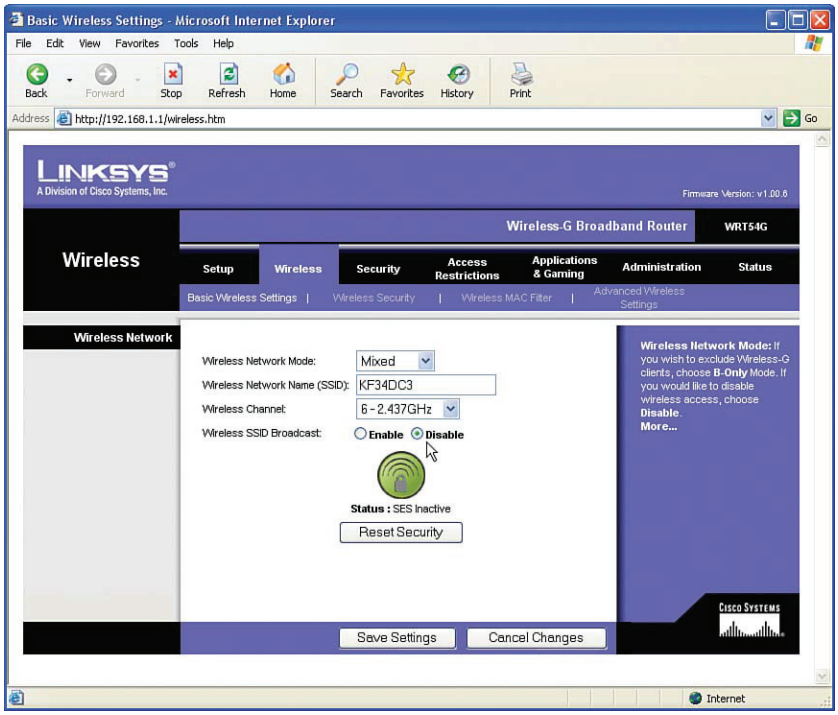
Stop Advertising Your Wireless Network

By default, wireless routers are set up to broadcast their SSID to make it easy for wireless cards to locate the wireless network without having to know information in advance. Nice feature, bad security practice. Broadcasting the SSID of our wireless home network is entirely unnecessary. So, one step to securing our network is to shut it off. To do so, follow these steps:

Step 1 Access the wireless router using your Internet browser. Click the **Wireless** tab.

Step 2 For Wireless SSID Broadcast, click the **Disable** radio button (see Figure 9-59). Click **Save Settings**.

Figure 9-59 Disable SSID Broadcast on the Wireless Router



Just by taking these simple steps, you have made your wireless network relatively invisible and fairly anonymous so that people looking for signals will not see a router with your name on it.



Note: As a reminder, do not use the default SSID that the wireless router is set up with. (For Linksys products, the default SSID is linksys.) If the SSID is not being broadcast but is easily guessed by intruders, your wireless network is still vulnerable. Change the SSID to something else, such as a random series of upper- and lowercase letters and numbers. Write it down.

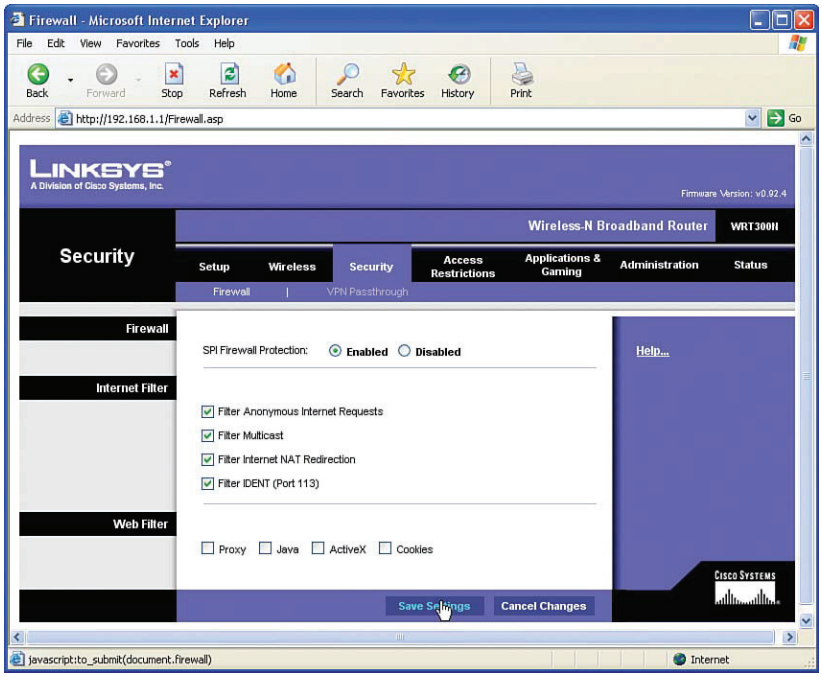
Turn On the Firewall

Most (Linksys Brand) wireless routers are shipped with a Stateful Packet Inspection (SPI) firewall. An important step to securing the wireless network is to make sure this firewall is enabled. To enable the firewall, follow these steps:

Step 1 Access the wireless router using your Internet browser. Click the **Security** tab.

Step 2 For SPI Firewall Protection, click **Enabled**, as shown in Figure 9-60. Click **Save Settings**.

Figure 9-60 Enable the Firewall on the Wireless Router



By enabling the firewall, you have added another level of protection for your wireless network.



Note: Firewalls are beyond the scope of this book. For more information on the use of firewalls and other security steps you need to take to properly protect your home network, pick up a copy of *Home Network Security Simplified*.

Prevent Unintentional Roaming

Wireless networks are a bit like cell phones. Your cell phone tries to find the closest cell tower so that you can get the most bars of signal strength to have high-quality voice calls. Wireless NICs work in a similar way in that they try to find the wireless router that has the strongest signal. The assumption is that the router the NIC finds is yours because it is the closest and therefore has the strongest signal.

However, that is not always true. If you have poor signal strength in a particular room of your house and your neighbor's router actually has a better signal in that room, your wireless NIC might try to roam onto your neighbor's router, unless you instruct it not to.

You do not want your laptop unintentionally hopping over to your neighbor's wireless router whenever it sees a stronger signal or for whatever reason loses connectivity with your own router. Using the Linksys NIC management utilities (such as WLAN Monitor), avoiding such hopping is pretty easy. Simply do not add your neighbor's wireless SSID as a profile. When using Windows to manage wireless connections, an additional step is required. This is another good reason to change your SSID, because chances are that at least some of your neighbors will leave their SSID at the default of linksys, which may cause confusion later.

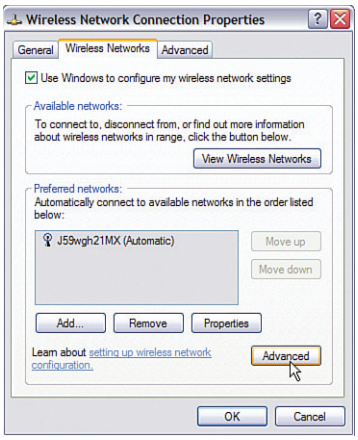
Another type of unintentional roaming is to inadvertently permit ad hoc wireless connections. As discussed in Chapter 4, "Planning Your Wireless Network," we recommend for security reasons that you operate your wireless home network in infrastructure mode, meaning a wireless router provides the central point of the network and all wireless computers communicate only with the central point, and not with each other directly (which is called *ad hoc*). This is a relatively low security risk, but there is a small possibility that those sitting next to us in an airport or other public location may try to make an ad hoc connection directly between their laptop and ours.

Because we plan to only ever use our laptop computers connected to a wireless router in infrastructure mode, we should disable ad hoc networking mode so that it is not possible for another laptop computer to attempt to make a connection directly to our laptop at all. Using the Linksys NIC management utilities (such as WLAN Monitor), we do this by selecting infrastructure mode. Again, when using Windows to manage wireless connections, an additional step is required.

The following steps describe how to take care of both issues:

Step 1 Access the properties for the wireless NIC by choosing **Start > Connect To > Show All Connections**, select the wireless NIC, and click **Change Settings for This Connection**. Click the **Wireless Networks** tab, as shown in Figure 9-61.

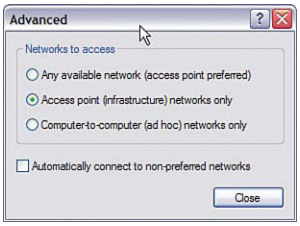
Figure 9-61 Verify the Preferred Networks List



Step 2 Make sure that only your wireless network profile appears in the Preferred Networks list. If other networks are listed that you do not recognize, delete them.

Step 3 Click the **Advanced** button. Click **Access Point (Infrastructure) Networks Only** and make sure that Automatically Connect to Non-Preferred Networks is *not* checked (see Figure 9-62).

Figure 9-62 Verify Network Access Settings



Step 4 Click **Close** and then click **OK**.

Now, if the wireless NIC sees your neighbor's wireless router, it will not try to connect to it because it is not in the list of preferred networks. Similarly, if we encounter another computer with a wireless NIC that attempts to set up an ad hoc connection, our wireless NIC will not respond to the attempt, keeping our wireless network (and laptop) secure.

MAC Address Locking

One additional wireless security measure that you can take that has not yet been discussed is MAC address locking (often called MAC address filtering). Because each wireless card has a unique identifier called a MAC address, we could instruct the wireless router to accept connections only from the wireless cards that we know. This is called *MAC address locking*.

Turning on MAC address locking is not trivial and can be a bit of trouble. Remember, with every security measure enabled, you typically lose some flexibility. For example, with MAC address locking enabled, you need to change the configuration on the wireless router if you buy a new wireless card or device. Also, if you have visitors who want temporary Internet access, you would have to grant them access by adding their MAC address to the permission table. MAC address locking does provide an additional level of protection. If you want to enable it, see Appendix A, "MAC Address Filtering."

Top Troubleshooting Tips for Wireless Encryption

Chapters 10, 11, and 12 are dedicated to troubleshooting problems with wireless networks, including encryption-related issues. However, here are the top tips to follow if any of the computers do not re-establish communication. Items to check include the following:

- Make sure the encryption method chosen on both the wireless router and *all* wireless NICs is the *same*.
- Make sure the passphrase for WEP key generation (or WPA) is entered exactly the *same* on both the wireless router and *all* wireless NICs. The passphrase is case sensitive, which means that *p* is different from *P*. Take care to make sure the entered phrase matches *exactly*, including lower- and uppercase letters.
- If all else fails, disable encryption on both the wireless router and all wireless network adapters, reverify the connections without encryption turned on, and then start the encryption setup from scratch.

Summary

Wireless networks are extremely beneficial, but you must take some simple steps to protect them. Failing to take the steps in this chapter is the equivalent of locking the front door and leaving all windows and back doors unlocked and standing open. It is pretty easy (and *so* critical) to add appropriate security. Here's a quick checklist to refer to:

- Change the password on the wireless router from the default (for example, admin).
- Change the SSID from the default (for example, linksys) to a random series of lower- and uppercase letters and numbers.
- Enable WEP or WPA encryption on the wireless router and all wireless network adapters. Use the strongest encryption level that all devices support.
- Use a WEP or WPA passphrase that is a random series of lower- and uppercase letters and numbers.
- Disable SSID broadcast on the wireless router.
- Disable ad hoc wireless networking on all network adapters (applies to Windows XP).
- Disable autoconnection to nonpreferred networks on all wireless network adapters.

The steps in this chapter are what most people need to take to keep their wireless network secure in all but the most extreme cases. The fact is that your SSID can be guessed or discovered, encryption schemes can be cracked (especially WEP), and MAC addresses can be spoofed (via a method called MAC address cloning); but doing all of this takes a great deal of skill, time, and money. If you want more protection than that described in this chapter, you can get it, but if you are still worried about wireless security, your best solution might be to stick with a wired network. Another good tip that we strongly recommend is to just turn off your wireless router and modem when you leave the house for an extended period or even over night. If it's not turned on, it can't be hacked.

Where to Go for More Information

The following are good sources of information for additional learning about wireless security:

Wikipedia has an entry for wireless security: http://en.wikipedia.org/wiki/wireless_security

Practically Networked is a good source for additional wireless security information: www.practicallynetworked.com/support/wireless_secure.htm

Tony Bradley has a helpful article on about.com titled *Introduction to Wireless Network Security*: http://netsecurity.about.com/od/hackertools/a/aa072004b.htm

You might also want to check out *Home Network Security Simplified*, one of our other books (Cisco Press, 2006)



PART IV

PART IV

"Honey, This Stupid Wireless Thing Is Not Working"

Chapter 10 Troubleshooting: I Can't Connect at All

Chapter 11 Troubleshooting: I Can Connect Sometimes

Chapter 12 Troubleshooting: I Can Connect, but It's Slow

Problems? We don't need no stinking problems.

Okay, so we would like to be able to say that wireless networks are so darn easy that you won't run into any issues. Unfortunately, we cannot do that. Wireless networks are a relatively new and fast-moving technology, which is the high-tech industry's way of saying stuff changes quite a bit, and stuff does not always work the way it's supposed to.

So invariably if you build a wireless home network of any kind, sooner or later you are going to hear those eight words: "Honey, this stupid wireless thing is not working." What do you do then? Because we cannot promise there won't be any problems, we give you some skills to figure out the most common problems and solve them. If nothing else, you will learn enough to be able to talk intelligently to a professional, should you need to call one in. That's what Part IV is all about.

Chapter 10, "Troubleshooting: I Can't Connect at All," shows you how to troubleshoot basic communications issues. We cover how to figure out why a wireless NIC and wireless router are not talking, and how to figure out who the likely culprit is. Then we show you what to do to get them talking again.

Chapter 11, "Troubleshooting: I Can Connect Sometimes," shows you how to troubleshoot range issues, meaning problems related to signal strength. Wireless networks are a lot like cell phones: no bars, no "workie." We cover how to figure out if you have dead spots in your house and give some tips for improving coverage.

We wrap up Part IV with Chapter 12, "Troubleshooting: I Can Connect, but It's Slow," which shows you how to get the best performance out of your wireless network. It may work, and you may get Internet access from the deck, but are you getting the speed you should be? We cover how to examine the speed you are getting between your computers and wireless router and give some tips for improving performance. We also show you how to figure out if your wireless network or broadband service is creating the slowdown.

The first step to figuring out what is wrong is to determine the type of problem you are having. Then, based on that determination, you can dive into the right troubleshooting steps. Here's a quick reference table to get you started:

Type of Problem	Start Here
My computer will not connect over wireless.	Chapter 10
My computer connects over wireless in certain places in my house but it won't connect in others.	Chapter 11
My computer connects over wireless but drops the connection at times.	Chapter 11
My computer connects over wireless but the connection is slow.	Chapter 12
My computer connects over wireless but cannot reach the Internet.	Chapter 12

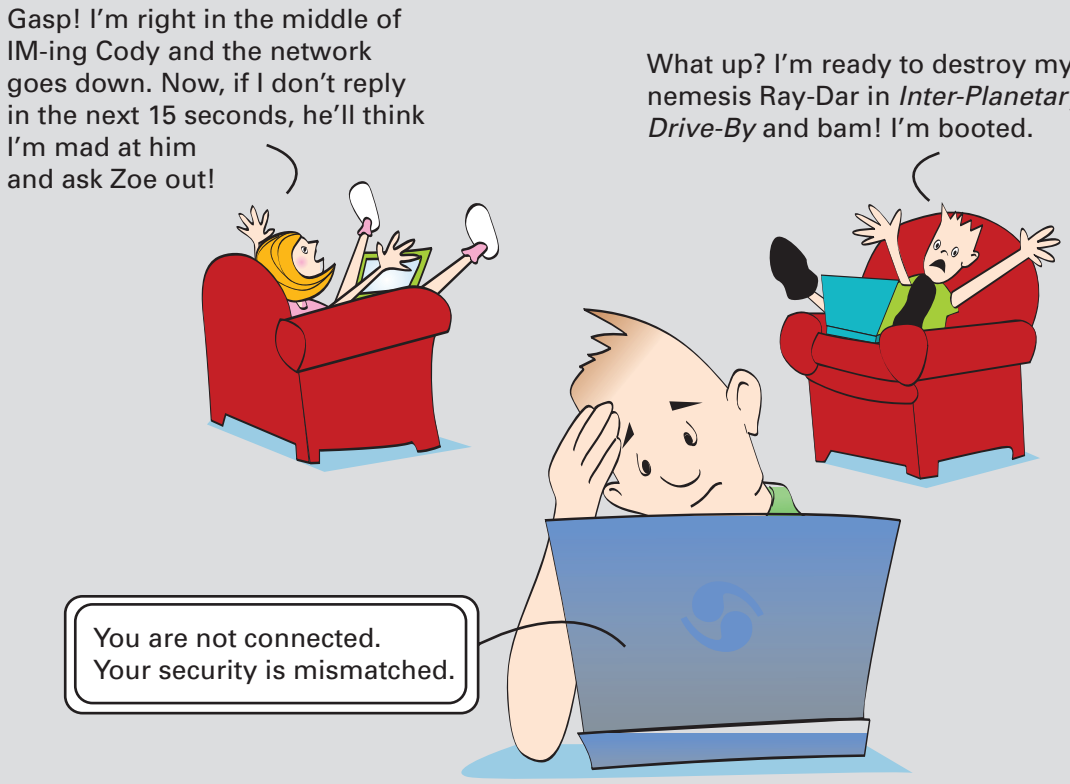
This page intentionally left blank

CHAPTER 10

Troubleshooting: I Can't Connect at All

Usually, wireless networks are pretty easy to set up and connect to, but, as we said earlier, due to the fast-moving nature of the technology, sometimes the network does not work as it is supposed to. In this chapter we will cover what to do if you cannot get a computer or laptop to connect over the wireless connection to the wireless router. Start here if you cannot get the computer and router to connect at all. If you can connect sometimes but not others, skip to the next chapter.

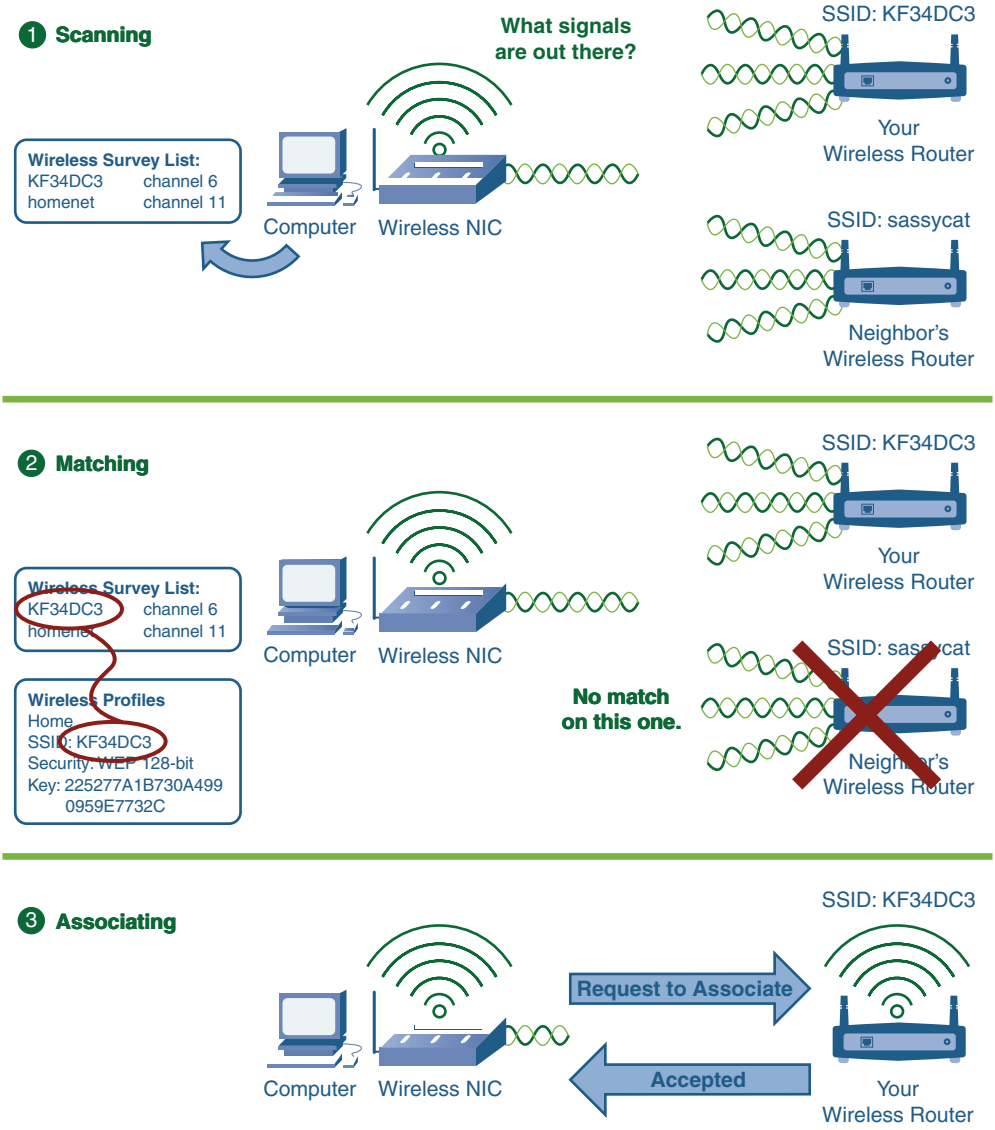
Before jumping into troubleshooting, let's first take a look at what happens during the steps when your wireless NIC connects to your wireless router and at what can go wrong during that process.

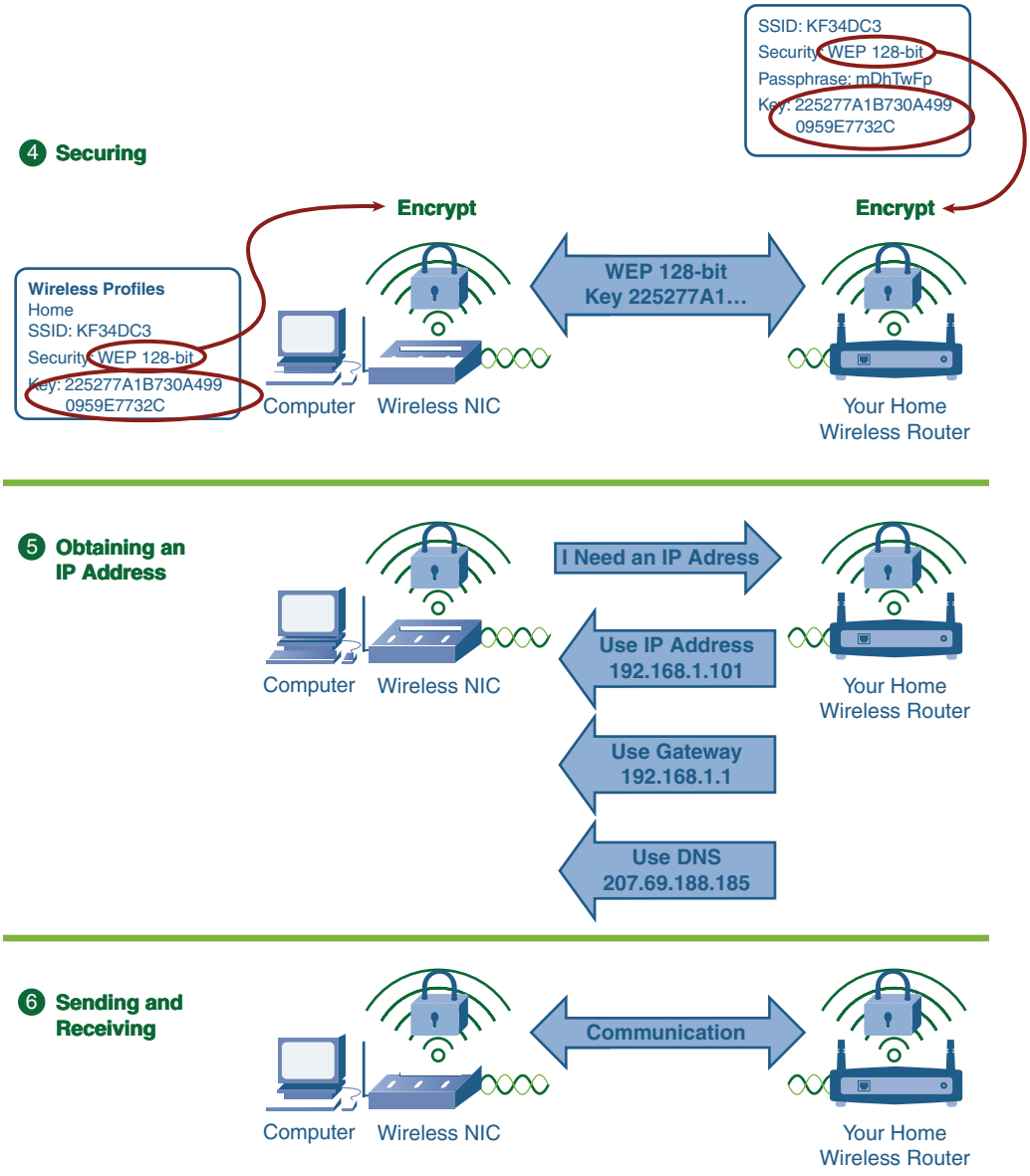


Steps to Connecting

When a wireless NIC and wireless router want to establish a connection, several steps need to occur, as shown in Figure 10-1 and described in the following sections. The example assumes your wireless NICs can see signals from two wireless routers, KF34DC3, which we have been using in previous examples as your router, and a second system named homenet, which is a neighbor's wireless router.

Figure 10-1 How a Wireless NIC Joins a Wireless Network




SSID: KF34DC3
Security: WEP 128-bit
Passphrase: mDhTwFp
Key: 225277A1B730A499
0959E7732C
4 Securing
Encrypt
Encrypt
Wireless Profiles
Home
SSID: KF34DC3
Security: WEP 128-bit
Key: 225277A1B730A499
0959E7732C
WEP 128-bit
Key 225277A1…
Computer
Wireless NIC
Your Home
Wireless Router
5 Obtaining an
IP Address
I Need an IP Adress
Use IP Address
192.168.1.101
Use Gateway
192.168.1.1
Use DNS
207.69.188.185
Computer
Wireless NIC
Your Home
Wireless Router
6 Sending and
Receiving
Communication
Computer
Wireless NIC
Your Home
Wireless Router

Scanning

First, the wireless NIC must perform a scan for available wireless signals, similar to the way your cell phone searches for a network when you turn it on. The NIC makes a list of the available wireless networks, including their SSID and channel. In this example the systems found were KF34DC3 and homenet.

Matching

Second, the wireless NIC checks the list of available signals to its wireless profiles to see if there is a system it recognizes, again much like your cell phone tries to match the cellular systems it sees with your provider. The NIC matches the SSID, in this example KF34DC3. There is no match on the other system, homenet.

Associating

Third, the wireless NIC selects the system that was matched *and* with the highest signal strength (this will become important in Chapter 11, "Troubleshooting: I Can Connect Sometimes"). In this example, there is only one match, so signal strength is not a factor. The wireless NIC sends an association request to the wireless router, which basically says, "Hey, mind if I join your wireless network?" Assuming it is permitted, the wireless router responds with an acceptance. The wireless NIC is then associated with the wireless network.

Securing the Connection

Next, the wireless NIC and wireless router both use the security information they have been programmed with, such as a WEP key or WPA key, and start sending information between them using encryption. If the security information matches and each side is using the correct key, the conversation is understood and can proceed. Now the wireless NIC and wireless router can freely, and securely, send and receive packets to and from each other.



Note: Technically speaking, with WPA there is an additional step that happens called *authentication*, where the two sides of the communication (the NIC and the router) exchange a WPA key to verify the identity of the NIC. We are combining that step with the securing step, for simplicity.

Obtaining an IP Address

Next, the wireless NIC needs to be assigned an IP address that it can be known by on the home network. We have set up the wireless router to assign IP addresses dynamically (as they are needed) to the home network, from a pool of addresses in the range of 192.168.1.100 to 192.168.1.149. This is the recommended way to set up home networks. In this step, the wireless NIC requests an IP address and is assigned 192.168.1.101.

Typically, a couple other important pieces of information—the gateway and DNS addresses—are passed to the NIC as well. The gateway is the address the NIC will always send traffic to in order to reach the Internet. The DNS is the server that will translate URLs such as http://www.cnn.com into the actual IP address on the Internet. The gateway is typically the wireless router, and the DNS is provided by your Internet service provider (ISP).

Sending and Receiving

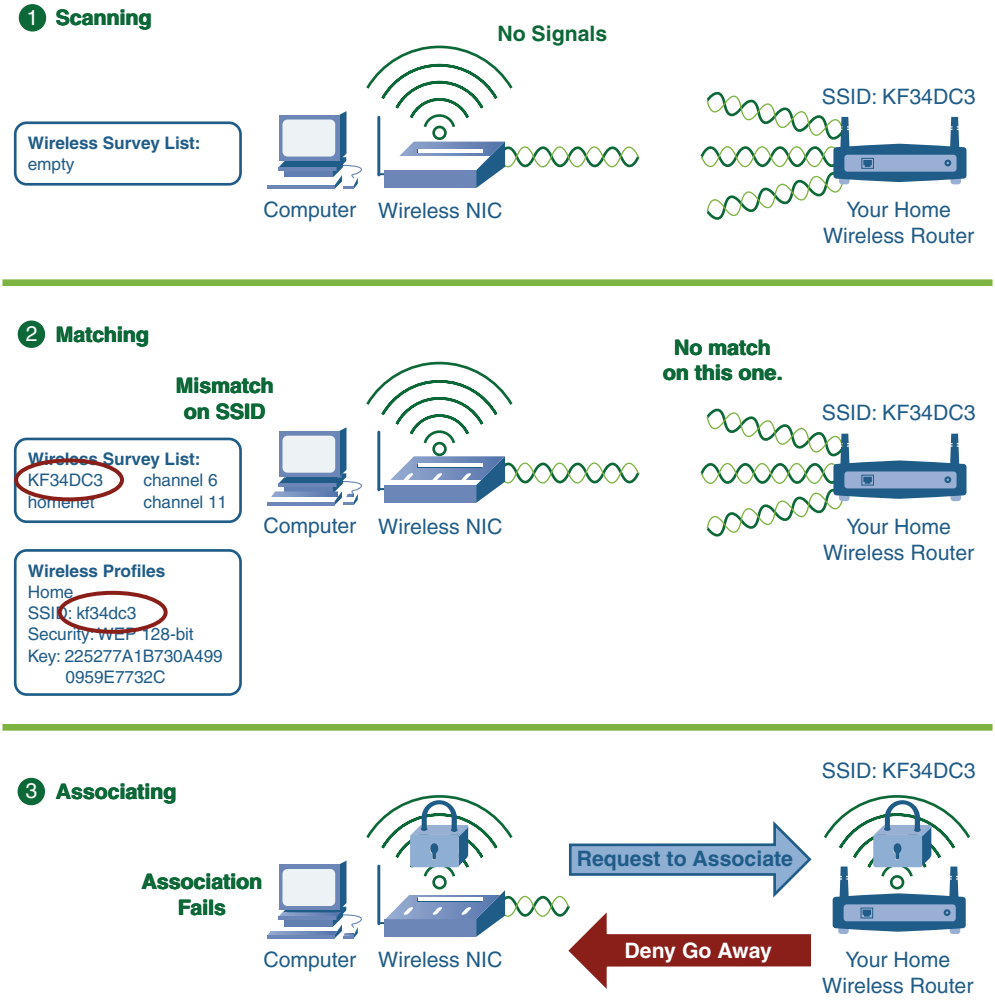
With the connection fully established, the computer with the wireless NIC can send and receive information to and from the home network, as well as the Internet.

What Can Go Wrong

Sounds pretty easy, right? In most cases it is, but joining a wireless network is a little like traveling on a trip with a very tight itinerary: If one leg of the journey does not go as planned, you miss a connecting flight, and it can mess up the whole trip.

What can go wrong? Well, during each of the steps discussed in the previous section, something can go wrong. Some of the issues are shown in Figure 10-2 and described in the following sections.

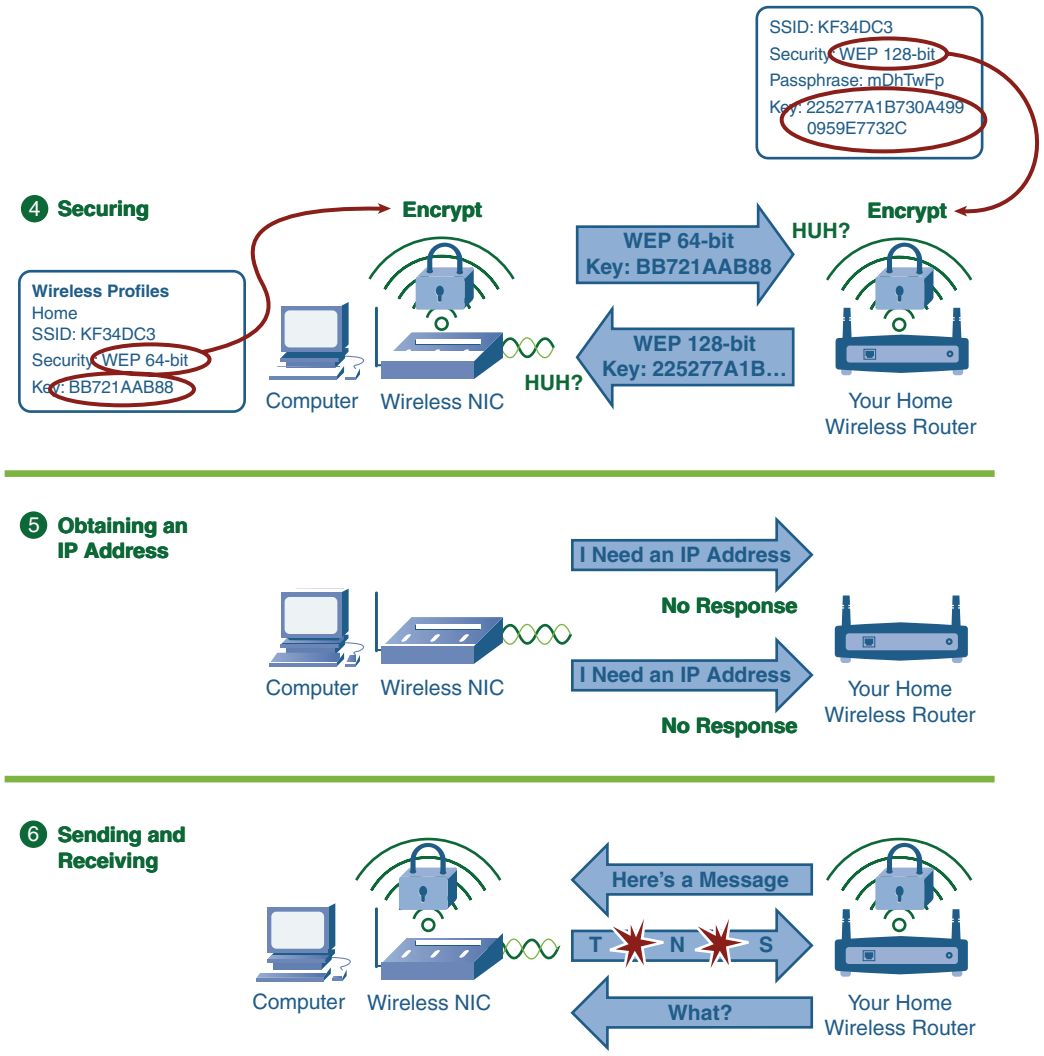
Figure 10-2 Things That Can Go Wrong Joining a Wireless Network



Problems During Scanning

If your wireless NIC does not see any wireless signals from a wireless router, you are pretty much dead in the water. Reasons for this could be that you are using the wireless NIC in a room of your house (or outside) with poor coverage. Another very common reason is that your laptop has a switch that turns the NIC on and off to save power, and you forget to turn it on. Unfortunately, most laptop built-in NICs we have seen do not alert you that you simply forgot to switch it on, but instead just give you an indication that there are no wireless signals in range. Quite maddening.

Don't worry if you have the SSID broadcast turned off on your router. When the NIC scans for a router, it will find it even if the broadcast function is turned off. If this is confusing, think of it this way: When broadcast is on, the router will continuously shout out to every NIC that is in range "I'm here! I'm here! I'm here!" When the broadcast function is turned off, the router will only answer "I'm here!" when the NIC first shouts "Are you there?"



Problems During Matching

During the matching step, it is possible that the wireless networks "in range" do not match those in the wireless profiles. In this example, we made an error setting up the wireless NIC. The wireless router is set up with an SSID of KF34DC3 but the wireless NIC is set up with an SSID of kf34dc3. You may be staring at the page saying, "Huh? These look the same to me." They are similar, but capitalization matters, so from a wireless network point of view, these are two different SSIDs. There are no indications or help in this case from the wireless NIC. It will not attempt to associate with the other SSID (KF34DC3) that is not in its wireless profiles and will keep scanning for one it recognizes.

Problems During Association

During the association step, it is possible the wireless router may not accept our association request. One reason could be that when we enabled MAC filtering/blocking as a security measure on the wireless router, we either configured it incorrectly or perhaps typed in the MAC address of the wireless NIC incorrectly. Again, there will be little indication of a problem by the wireless NIC. If you are lucky you may get a message from the wireless NIC manager utility you are using saying that the association failed. More than likely you will not be told anything, and the wireless NIC will go on about its merry way, scanning for another system.

Problems Securing the Connection

During the securing step, a couple of things can go wrong. The most likely problem has to do with mismatched security settings between the wireless NIC and wireless router. If you set the security type differently—for example, 64-bit WEP on the NIC and 128-bit WEP on the router—that is a problem. Another example is if you made an error typing in the WEP key or WPA key, such as mDhTwFp on the router but MDhTwFp on the NIC. These look the same, but the difference between "m" and "M" is huge from a WEP or WPA key perspective.

Once again, you will not get an indication that there is a security mismatch. The NIC and the router will be unable to communicate, so the association will simply fail, and the NIC will move on to try another system. From a security point of view, giving no indication of the failure is actually what we want it to do. After all, we do not want the wireless router or wireless NIC giving hints to a hacker trying to join our wireless network uninvited. But this has the consequence of not being much help to us in diagnosing our own legitimate wireless joining problem.

Problems Obtaining an IP Address

In most cases, once we make it past the securing step, establishing a connection goes pretty smoothly. However, for whatever reason, the wireless NIC might be unable to obtain an IP address from the wireless router. Fortunately, when this error occurs we can at least see an indication that it has happened, although we do not receive much else in the way of why it happened.

Problems Sending and Receiving

With the connection fully established, we are in the clear, right? Not always. Sometimes you can associate and get connected, but then your data gets garbled during sending and receiving, possibly from interference from other wireless devices, like a cordless phone, microwave, or even a neighbor's wireless network. In this case, usually the result is slower performance. Problems sending and receiving can also occur when you are just on the edge of coverage, so sometimes you get a good enough signal, and the next minute you don't. Sound familiar? Yes, your cell phone has probably given you similar fits. We can see when this is happening with a wireless network, and Chapter 11, "Troubleshooting: I Can Connect Sometimes," and Chapter 12, "Troubleshooting: I Can Connect, but It's Slow," discuss these problems more in depth.

Five Things to Look At First

Before you roll up your sleeves to troubleshoot in depth, you may want to take a look at the five most common things that keep people from getting connected to the Internet on their wireless network:

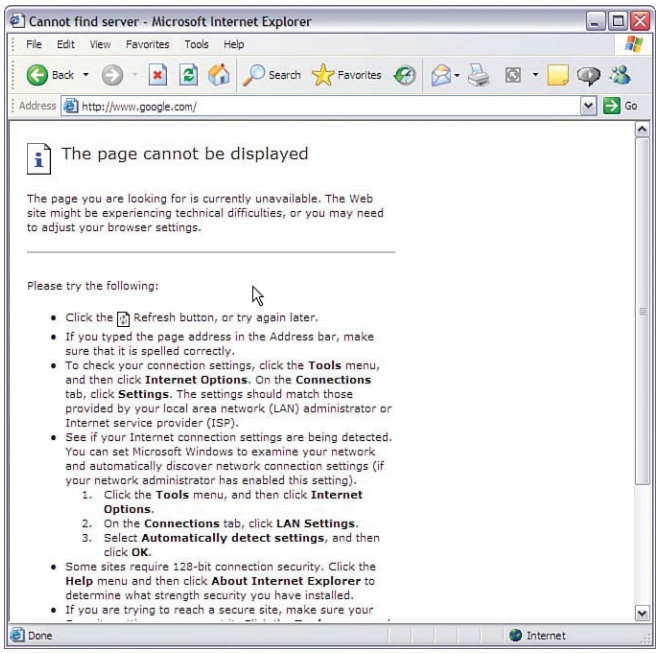
- **Check whether you have a working Internet connection**—Using a computer that has a wired network connection to the ports on the back of the wireless router, confirm that you can access the Internet by trying to browse a web page. If you cannot access the Internet from the wired computer, you are not going to be able to access it from a computer that is wireless either. See the section "How to Tell if You Do Not Have a Connection" that follows for more information.
- **Make sure the wireless NIC is turned on in your PC**—If you have a laptop, it usually has a way to power off the wireless NIC to save battery life (and for required shut-off on airplanes during flight). Make sure it is turned on. See the section "Wireless Turned Off" later in this chapter for more information.
- **Check for a good wireless signal**—Using the wireless NIC management utility (such as the Windows Wireless Network Connection utility, Linksys WLAN Monitor, Boingo, and so on), confirm that you can get a wireless signal. Sit the laptop next to the wireless router. If you still see no signal or a weak signal, something else is wrong. Make sure you are trying to connect to the right wireless router (SSID) and that the wireless router is functioning. Try rebooting the wireless router and laptop also.
- **Check whether you have disabled SSID broadcast**—Disabling SSID broadcast is a good security measure, but it makes troubleshooting more difficult. Enable SSID broadcast on the wireless router and leave it enabled until you have a well-functioning wireless network with no connection issues.
- **Check whether you can connect with the security disabled**—Turn off the wireless security measures, including WEP or WPA, on both the wireless router and wireless NICs. Can you make a wireless connection without security enabled? If so, that gives you a good indication that security settings are mismatched somewhere. See the section "Security- and Encryption-Related Issues" later in this chapter for more information.

Once you have confirmed that none of these is the issue, it is time to try some more in-depth diagnosing of the problem, which is the topic of the rest of this chapter.

How to Tell if You Do Not Have a Connection

The most common way to determine whether or not you have a wireless connection is to try accessing the Internet with an Internet browser, such as Internet Explorer, on the computer with the wireless connection. If you get the infamous "The page cannot be displayed" message, as shown in Figure 10-3, that is a good indication that you have some kind of problem.

Figure 10-3 Internet Browser Cannot Access the Internet



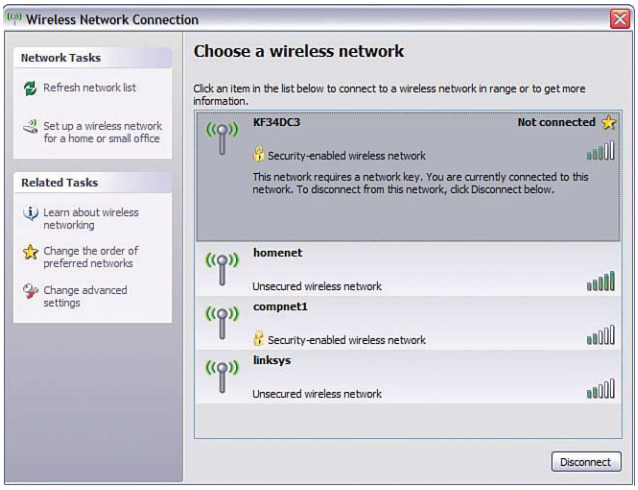
Before you go any further in troubleshooting the computer with the wireless connection, walk over to a computer that has a wired connection to the wireless router and try to access the Internet first from that computer. Many perceived wireless network issues turn out to be just a general problem with the broadband service.

If you cannot access the Internet from a wired computer, troubleshoot getting your wireless router to properly connect to the broadband modem, and so on. Start with Chapter 7, "Wireless Router Setup." If you need more in-depth help getting the wireless router to work with your broadband service, pick up a copy of *Home Networking Simplified*, which contains more information.

Once you have confirmed that your Internet access is working from a wired computer and that it is still not working from your wireless-connected computer, the next thing to check is to see if you have a wireless connection. Depending on which wireless connection manager you are using to manage your wireless NIC, each has a slightly different way to tell if you have a good connection to the wireless router. They generally display a fairly straightforward visual indicator that tells you if you have a connection or not.

If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **View Wireless Networks**. Figure 10-4 shows that the wireless network with SSID KF34DC3 has a few bars of signal strength, but the status listed is Not Connected.

Figure 10-4 Verifying a Wireless Connection with Windows XP



If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Figure 10-5 shows that there is no connection to the wireless router. Very clearly, the utility tells us there is "No association with access point," meaning the NIC and the router are not communicating.

Figure 10-5 Verifying a Wireless Connection with Linksys WLAN Monitor



Figuring Out Why It Will Not Connect

Earlier in this chapter we talked about the steps that a wireless NIC and wireless router go through to connect to each other, and also what can go wrong. Here is the secret to figuring out where the trouble is: follow the connection steps and find out which step is not occurring correctly. This seems simple, but we have seen many people trying random remedies. Eventually they may get it, mainly by accident, but sometimes they walk away frustrated. Trust us, and we may save you a lot of time and frustration with the methodical approach we have put together here.

Let's review our six connection steps: scanning, matching, associating, securing, obtaining an IP address, and sending/receiving. This section covers each of these steps, describes how to recognize a problem, and offers some remedies.

Scanning-Related Issues

During the scanning phase, the wireless NIC searches for available wireless networks. The wireless router sends out a "beacon" letting wireless NICs know that it is there (this is what SSID broadcast is, and the beacon only works when the feature is enabled). When the NIC detects and reads the beacon, it makes a record of this network as being available.

If you perform a "survey" using your wireless NIC manager (Windows Wireless Network Connection utility, Linksys WLAN Monitor, or one of the other options such as Boingo; see Chapter 14, "Wireless to Go") and do not see your home network wireless router SSID in the list of available networks, this is a scanning issue.

Why would your wireless NIC not be able to see your wireless router? There are three common issues that can occur, including incompatible wireless standards, a disabled wireless NIC, or poor signal coverage.

Incompatible Wireless Standards

In Chapter 2, "Wireless Standards: What the Letters Mean," and Chapter 3, "Selecting the Right Wireless Standard for Your Network," we covered the different wireless standards, including which standards are compatible and which are not. As an easy rule of thumb, 802.11b, 802.11g, and 802.11n work together, and 802.11a is special. If you have an 802.11a wireless NIC and an 802.11g router, your NIC will never see the router.

Some NICs and routers that support multiple standards offer the ability to limit the modes in operation. For example, an 802.11b/g router may allow you to set it to function as g-only, meaning disable the 802.11b mode and thereby accept only 802.11g wireless NICs. If you then try to connect with an 802.11b NIC, it will not see the router.

Here is another example where a wireless NIC supports 802.11a, b, and g, but the NIC has been inadvertently set to a-only. Under Windows XP, choose **Start > Connect To > Show All Connections**. Select the wireless NIC, click **Change Settings of This Connection**, and then click the **Configure** button. Figure 10-6 shows the result on a laptop with a built-in Intel 802.11a/b/g NIC.

Here we can see that the NIC is set to 802.11a only. If we are connecting to an 802.11g router, this NIC will never see the router. Figure 10-7 shows the corrected setting of 802.11b and 802.11g.

Figure 10-6 Checking the Wireless Mode on a Multi-Standard NIC

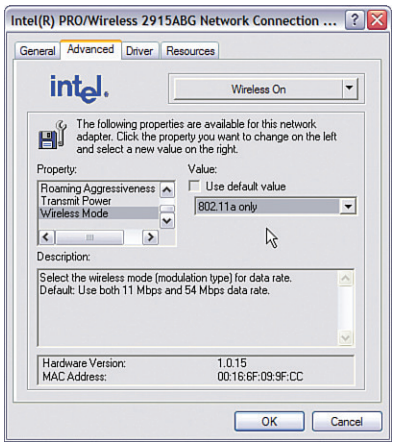
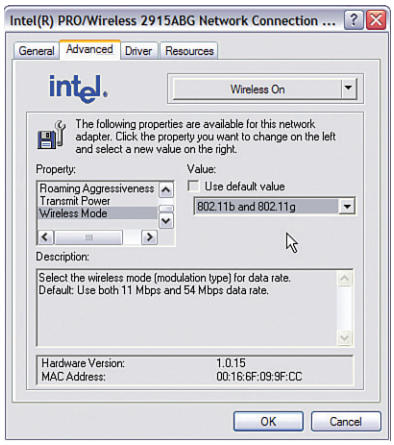


Figure 10-7 Correcting the Wireless Mode on a Multi-Standard NIC



By the way, you do not have to check this setting every time you have a wireless connection issue. Just check it the first time you are trying to set up your network and have an issue.

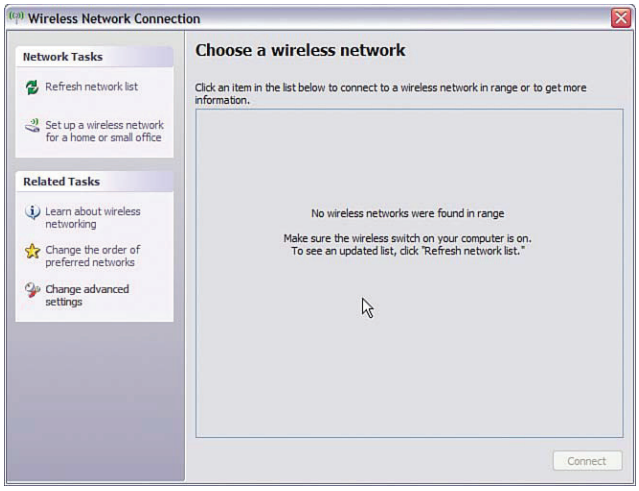
Wireless Turned Off

It seems like a pretty foolish mistake, but not turning on your wireless NIC is probably the single biggest cause of wireless network problems. You may be reading this thinking, "No way! Do they think I'm stupid or something?" Trust us, we have done it ourselves many times, as have those around us. No matter how stupid it may seem, please check it, and check it again.

For good measure, don't forget to check that the wireless router is turned on and wireless is enabled, too. It may seem like a silly thing to do, but it beats troubleshooting for two hours only to find out your router was turned off.

If you are using the Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **View Wireless Networks**. Figure 10-8 shows an example.

Figure 10-8 Determining if the Wireless NIC Is Turned On in Windows XP



Here we see that the NIC has detected no networks within range, and Windows XP suggests that we make sure the wireless NIC is on. It could mean either that the NIC is off or (unfortunately) that the NIC is on and there are really no signals detected. Windows XP does not have the ability (apparently) of telling us definitively if the NIC is on or off. So, we just have to go check it ourselves.

Many laptops have a hard switch on the outside to turn the NIC on and off (to save battery life or on airplanes where it is required to be turned off). Most laptops also have a "soft" switch, where you press a function key to toggle the NIC on and off. For example, on an IBM ThinkPad, simultaneously pressing the blue Fn key and the F5 key shows the NIC toggle function display, as shown in Figure 10-9. We can see that the wireless NIC is off. Clicking the Turn On button will power the NIC on, where it will immediately begin the scanning step.

Some laptops also have an LED indicator that tells you if the wireless NIC is on or off. Consult the user guide for your laptop.

Figure 10-9 Toggling the Wireless NIC On and Off with an IBM ThinkPad

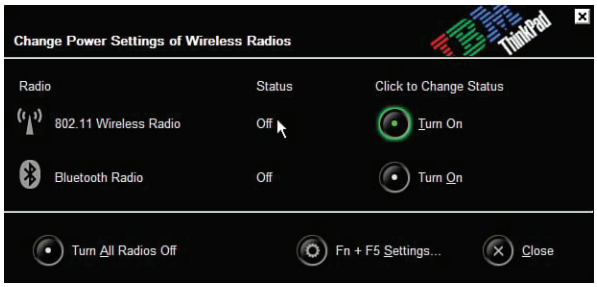
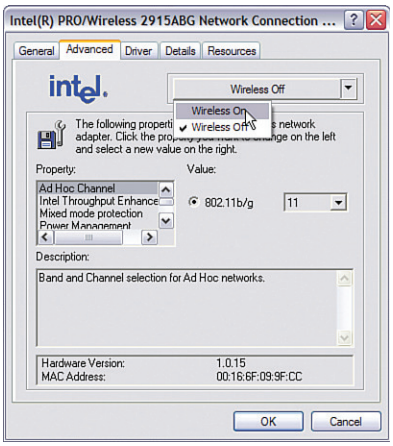


Figure 10-10 shows the result for a built-in Intel 802.11 a/b/g NIC. Choose **Start > Connect To > Show All Connections**. Select the wireless NIC, click **Change Settings of This Connection**, and then click the **Configure** button. Figure 10-10 shows that the wireless NIC is off, and we can use the selection list to turn it on by choosing **Wireless On**.

Figure 10-10 Toggling the Wireless NIC On and Off with Windows XP



Each laptop manufacturer provides a slightly different method, so check the user manual for your laptop to see how your particular wireless NIC can be turned on and off.

Poor Signal Strength

Another very common issue with wireless networks is signal coverage. Think of it as being similar to your cell phone and the cell tower. As you are driving away from the cell tower, you see the number of bars shrinking on your cell phone display. Sometimes, if you take your cell phone into the interior of a building or into an elevator, you lose the signal altogether. Wireless networks function in the same way. Wireless routers reach only so far, and the more objects, such as floors and walls, between your computer and the router, the more *attenuated* the signal becomes.

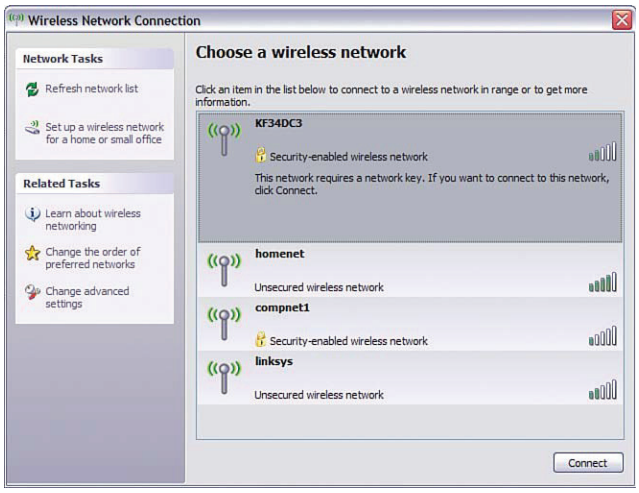
Attenuation refers to how much of the wireless signal gets absorbed by natural objects while it is traveling from the transmitter (wireless router) to the receiver (wireless NIC). In general, 802.11a networks have more attenuation than 802.11 b/g/n networks, so the distance away from the router in which you can receive a strong signal is not as far for 802.11a networks.

The ranges printed on the boxes of the routers do not take attenuation into account and are "idealized" ranges.

How do you tell if you have a weak signal? Most NIC utilities have an indicator much like your cell phone that displays a series of bars indicating a weak or strong signal. If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **View Wireless Networks**. Figure 10-11 shows an example.

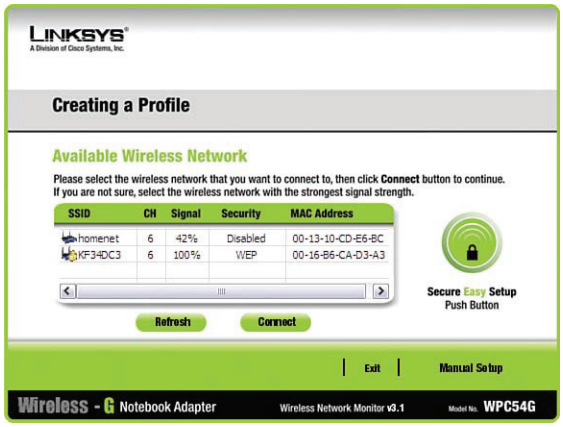
In this example we can see that for the wireless network with SSID KF34DC3, we have two out of five bars of signal strength. We do not necessarily need five bars to make a good connection, but if the signal shows only a single bar (or, with some NICs, even two bars) of signal strength, the signal could be too low to make a good connection.

Figure 10-11 Checking Wireless Signal Strength with Windows XP



If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Site Survey** tab. Figure 10-12 shows an example of a strong signal.

Figure 10-12 Checking Wireless Signal Strength with Linksys WLAN Monitor



In this example we see that the signal strength for the wireless network with SSID KF34DC3 is 100 percent. This is a good, strong signal. You do not need 100 percent to have a good connection, but if you see between 0 percent and about 20 percent, the signal could be too low to make a good connection.

One remedy to try if you see very low signal strength is to move the laptop or computer much closer to the wireless router, preferably in the same room. You should see a much stronger signal strength. If not, you may have some other issue and may want to check if the wireless router is functioning correctly. Make sure the wireless is enabled on the wireless router, and try rebooting it.

If the problem was a very low signal strength in the room you were trying to use the laptop in, before going much further in this chapter, you should probably take a look at Chapter 11, which focuses on signal strength and coverage issues.

You may also want to click the **Refresh** button (or **Refresh Network List** in the case of Windows Wireless Network Connection utility) a few times and note if the signal level changes. If the signal strength fluctuates between good and poor, you may have some form of interference that is causing trouble for your wireless network. In this case you may want to take a look at Chapter 12, which focuses on intermittent problems and performance issues.

If you have a strong, steady signal and the darn thing just will not connect at all, proceed with the rest of this chapter.

Matching-Related Issues

Once you have confirmed that the wireless NIC is scanning properly and detecting the wireless router, move on to the matching step. During matching, the wireless NIC compares the list of wireless SSIDs it has detected during scanning to the list of wireless SSIDs that are set up in the wireless profiles on the laptop or computer. A wireless profile (as you recall from Chapter 8, "Wireless NIC Setup") is a set of the characteristics for a wireless network that you previously connected to, or that you programmed in advance of connecting to.

Why would your wireless NIC not match on your wireless router? Two common issues can occur, including an SSID mismatch and a "bug" related to SSID broadcast.

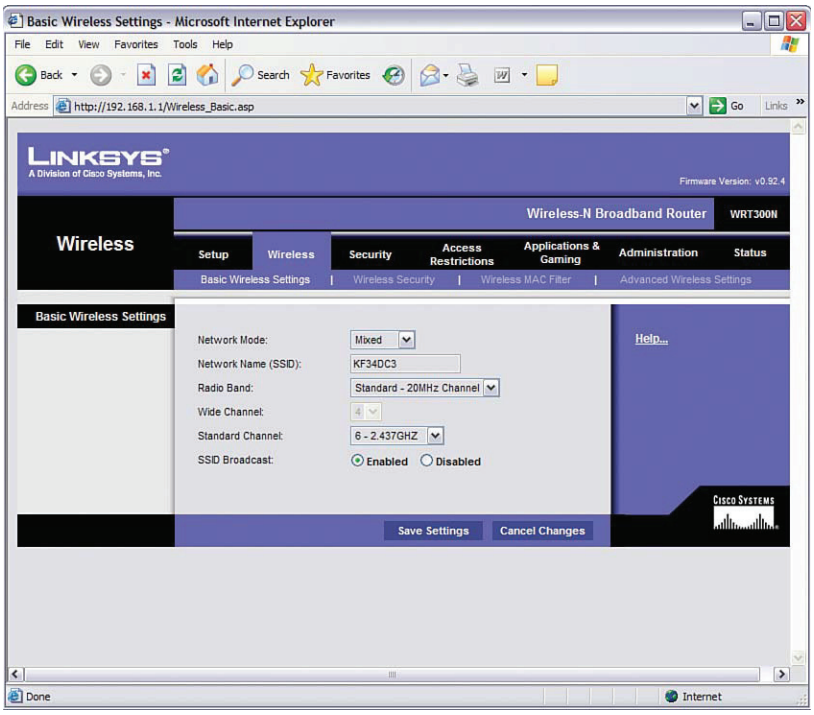
SSID Mismatch

A common problem in matching on a wireless network is a mismatched SSID. This is especially true if you had to manually type in the SSID to set up the wireless NIC. If you used a more automated setup process, such as the Linksys EasyLink Advisor utility, the SSID can be programmed into the NIC automatically.

The most common error people make is to overlook that the SSID is case sensitive and that the wrong case has been used, or to overlook that a number and letter have been confused, such as the letter *O* being used in place of the number 0.

To verify that the SSIDs match in your wireless network, first double-check that you have written down the exact SSID that is set up in the wireless router. To do so, access the router using an Internet browser. Click the **Wireless** tab, as shown in Figure 10-13.

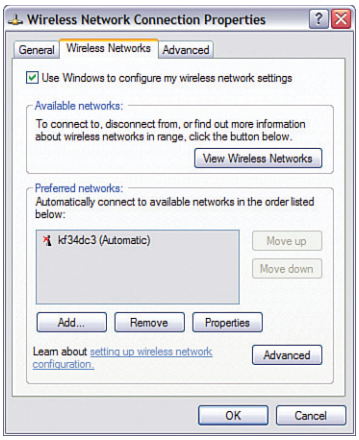
Figure 10-13 Verifying the SSID on the Wireless Router



We can see that the router is set up with an SSID of KF34DC3. Write it down *exactly* as it appears, paying attention to upper- and lowercase letters.

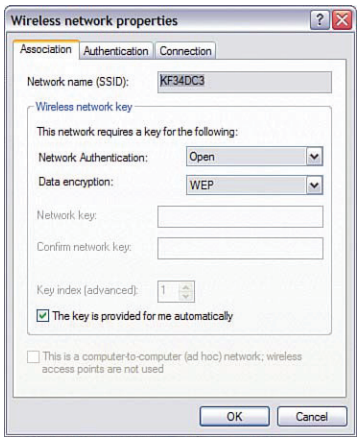
Now let's check the wireless NIC to make sure it has that exact SSID programmed into the wireless profile. If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Click the **Wireless Networks** tab. Figure 10-14 shows that the SSID is set to kf34dc3. This is not the same SSID entered on the wireless router, because of the difference in case, so the NIC will never match on the wireless network.

Figure 10-14 Verifying the SSID on the Wireless NIC Using Windows XP



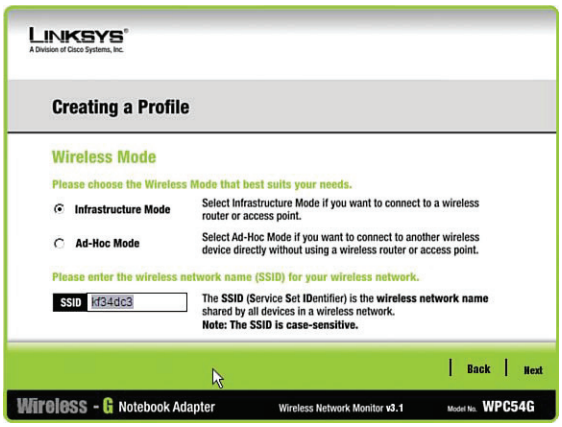
Unfortunately, in Windows XP, there is no way to edit the SSID for an existing wireless profile. Instead, you have to click **Remove** to delete the wireless profile and then click **Add** to create a new one with the right SSID. Figure 10-15 shows an example, with the correct SSID of KF34DC3.

Figure 10-15 Correcting the SSID on the Wireless NIC with Windows XP



If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Wireless Profiles** tab. Select the profile for your home wireless network and click the **Edit** button. Click **Next** until you find the SSID, as shown in Figure 10-16 (to save space, all the preceding dialog boxes are not shown here).

Figure 10-16 Verifying the SSID on the Wireless NIC with Linksys WLAN Monitor



Similar to the Windows XP example earlier, we can see that the SSID is set to kf34dc3, which is a case mismatch with the SSID of the wireless router. In this case, though, we can simply change the setting to the correct value of **KF34DC3**, click **Next** several times until we reach the Confirmation dialog box, and then click **Save** to save the settings in the wireless profile.

With the SSID corrected, and with any luck, the wireless NIC may find the wireless router and connect properly now. If not, unfortunately, there is no conclusive way to verify that the SSID matching is occurring correctly. We can only verify it, double-check it, and move on (or perhaps call someone else into the room, a different pair of eyes, to triple-check it for you).

SSID Broadcast

In Chapter 9, "Wireless Security Setup," we told you that it is a good security practice to disable the SSID broadcast function on your wireless router. This instructs the wireless router not to "beacon" the SSID, effectively to stop advertising your wireless router to anyone in the immediate vicinity.

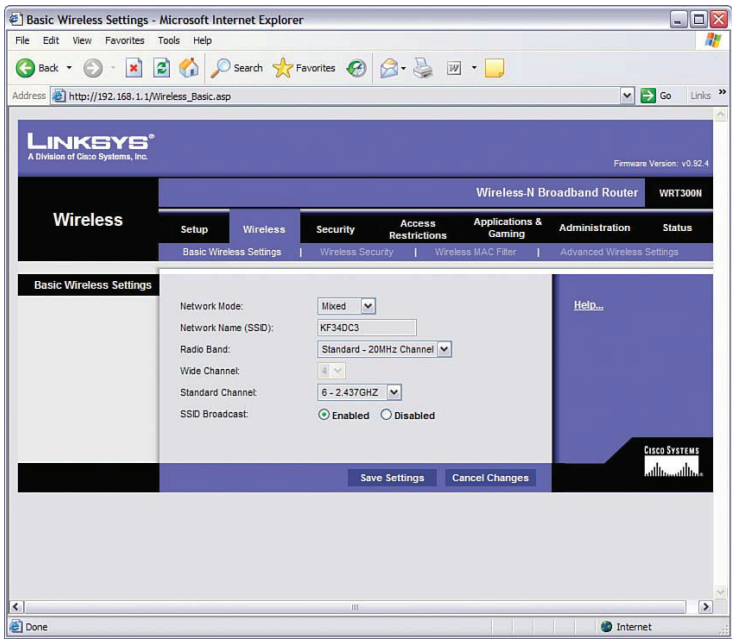
However, if you are having wireless connection issues, you *definitely* want to enable SSID broadcast on the wireless router. First of all, troubleshooting is more difficult if SSID broadcast is disabled. If you are having connection issues, enable SSID broadcast and leave it enabled until you have no more issues and are confident you can disable it.

Depending on the wireless connection manager you are using, wireless routers with the SSID disabled may not show up in the list. So if you have a mismatch in SSID, knowing that would be difficult because you won't be able to actually see the router.

Secondly, we have seen a few NICs that simply cannot locate a wireless router if the SSID broadcast function is disabled, even if the SSID is programmed perfectly into the wireless profile of the NIC. This is actually a "bug," an error in the product. So again, enabling SSID broadcast will uncover if this is the situation with the wireless NIC you are using.

To enable SSID broadcast on your wireless router, access the router using an Internet browser. Click the **Wireless** tab, as shown in Figure 10-17. On the **SSID Broadcast** line, click **Enabled** and then click **Save Settings**.

Figure 10-17 Enabling SSID Broadcast on the Wireless Router



Retry the laptop or computer you were having an issue with and see if it can now connect to the wireless router successfully.

Association-Related Issues

After the wireless NIC locates the wireless router's signal and matches the SSID, it sends an association request to the router to formally join the wireless network. Without this association, a computer or laptop is not permitted to send packets to or receive packets from the wireless network. It can only stand outside looking in the windows at the party.

Why would the wireless router refuse an association request? There are not very many reasons, actually. The most common reason is that MAC filtering (a form of security), which we referred to in Chapter 9 and discuss more in depth in Appendix A, "MAC Address Filtering."

MAC filtering, which you can enable on the wireless router, restricts the computers and laptops that can join the wireless network, by keeping a list of the authorized MAC addresses—the unique identifier of each wireless (and wired) NIC. Each NIC on planet earth has a unique MAC address.

MAC filtering can examine the MAC address of a computer trying to join the wireless network, and refuse entry if it is not on the preauthorized list. It makes for a pretty good additional security measure, but it can cause problems.

The three most common errors people make when enabling MAC filtering are as follows:

- Enabling Prevent instead of Permit, effectively reversing the function of MAC filtering to exclude a list of MAC addresses instead of authorizing them
- Forgetting to add a MAC address for a new device or computer to the authorized list
- Making an error when manually typing the MAC address into the authorization list

To see if MAC filtering is causing an issue, the best thing to do is turn it off and see if the problem goes away. To disable MAC filtering, access the wireless router using an Internet browser. Click the **Wireless** tab and then the **Wireless MAC Filter** subtab, as shown in Figure 10-18. Click **Disabled** and click **Save Settings**.

If it was already disabled, MAC filtering is not the problem; move on to the next troubleshooting step. If it was enabled and turning it off corrects the issue, then something is wrong with the way MAC filtering is set up on your wireless router.

When checking the MAC filtering setup, first see if the Prevent/Permit option is set correctly. On the same Wireless MAC Filter subtab of your wireless router, make sure that the Permit PCs Listed Below to Access the Wireless Network radio button is selected, as shown in Figure 10-19. If **Prevent PCs Listed Below from Accessing the Wireless Network** is selected, it will reverse the operation and keep your computers from accessing the network. Don't forget to click **Save Settings** if you change the setting.

Figure 10-18 Disabling MAC Filtering on the Wireless Router

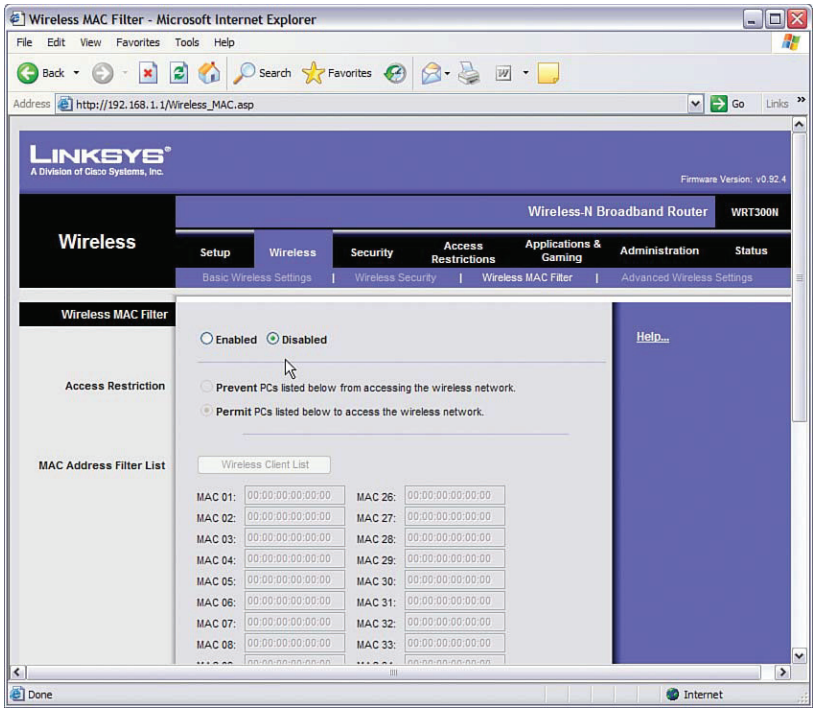
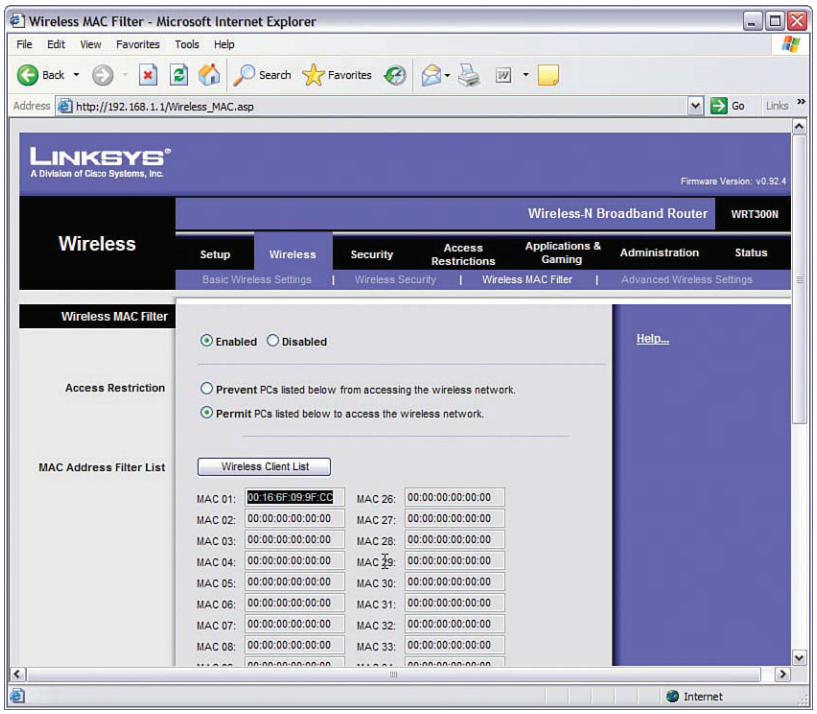


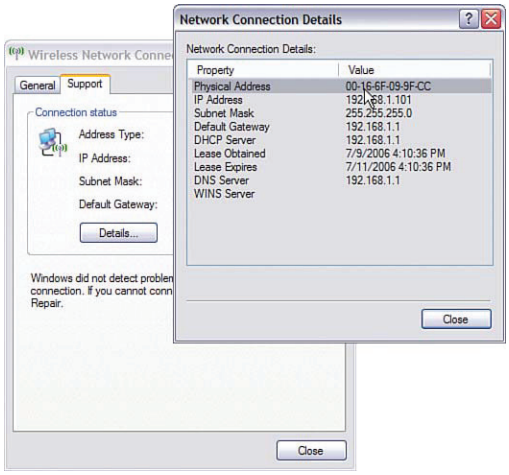
Figure 10-19 Verifying the MAC Filtering Setting on the Wireless Router



Next, we need to verify that the MAC address is correctly entered. Find the MAC address for the wireless NIC again. It is usually printed on the NIC itself, the packaging, or on a label on the underside of the laptop.

You can also find the MAC address with Windows XP. Choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **View Status of This Connection**. Click the **Support** tab and then click the **Details** button. Figure 10-20 shows an example.

Figure 10-20 Finding the MAC Address with Windows XP



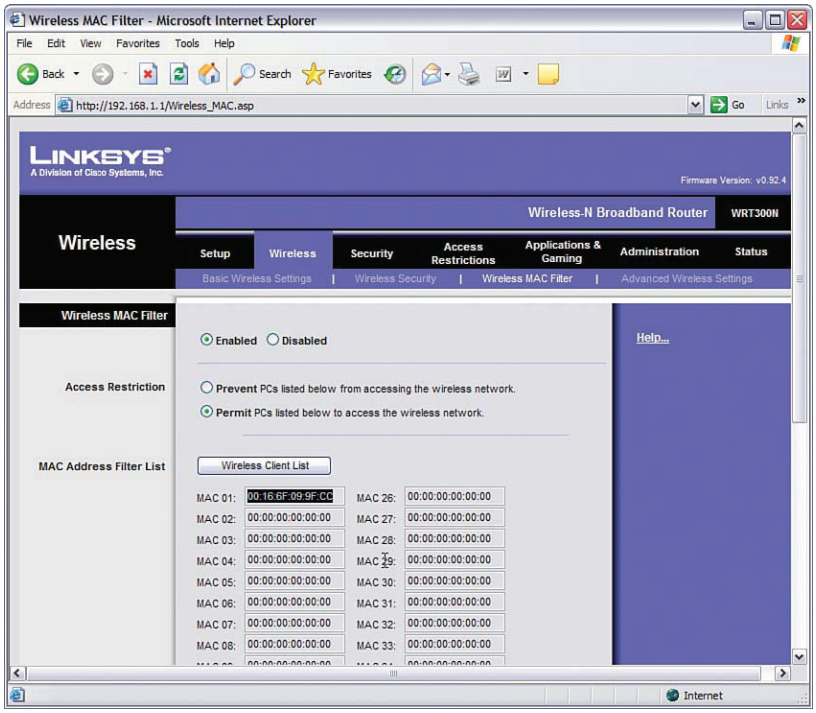
The physical address is the MAC address, in this example 00-16-6F-09-9F-CC. Write it down. MAC addresses are not case sensitive, so 6f is the same as 6F.

On the same screen on the wireless router, double-check that the MAC address in the authorization list is identical, as shown in Figure 10-21.

If it is not correct, then click **Edit MAC List** and correct the entry. Note that ":" is substituted for "-" in this case. If you change anything, remember to click **Save Settings**.

As discussed earlier, if MAC filtering is on, start by turning it off and seeing if the problem is corrected. Then, if you want to turn it back on, check and correct the settings as discussed.

Figure 10-21 Verifying the MAC Address on the Wireless Router



Security- and Encryption-Related Issues

After the wireless NIC successfully locates, matches on, and associates with a wireless router, the next step is to secure the connection with encryption. As we discussed in Chapter 9 and several times earlier, it is essential that you turn encryption on in your wireless network to protect against casual eavesdroppers and others. Turning on encryption is getting easier, but it can still be a little tricky.

If encryption is causing an issue on your wireless network, you will unfortunately not get a very good indication from either the wireless NIC or the wireless router. You may see the wireless NIC associate briefly, but then not "stay on" the wireless network, and start scanning again. You most likely will not receive a message such as "WEP key does not match" or "Wrong WPA key." Whenever you try to connect, the result after attempting will be "Not connected."

What kinds of problems would cause security and encryption not to work properly? There are three primary reasons: a mismatch of encryption type, a mismatch of the encryption key, or a mismatch of Windows XP authentication settings.

Encryption Type Mismatch

The first major step to troubleshooting security is to make sure you are using the same encryption type throughout the wireless network. As discussed in Chapters 5, (Wireless Security: What You Need to Know,) and 9, currently there are two major types of wireless encryption available: WEP and WPA.

You have to run the same encryption on both the wireless router and *all* wireless NICs. You cannot mix and match. So the first step is to verify on the wireless router and all wireless NICs that you are

using the same encryption type. WPA is preferred over WEP because it is more secure. Some older NICs may not support WPA.



Note: Wired NICs do not have or need encryption, so just ignore those.

Encryption Key Mismatch

WEP and WPA each have two additional settings that are critical to making encryption work, as described in the following sections.

WEP Key Length Mismatch

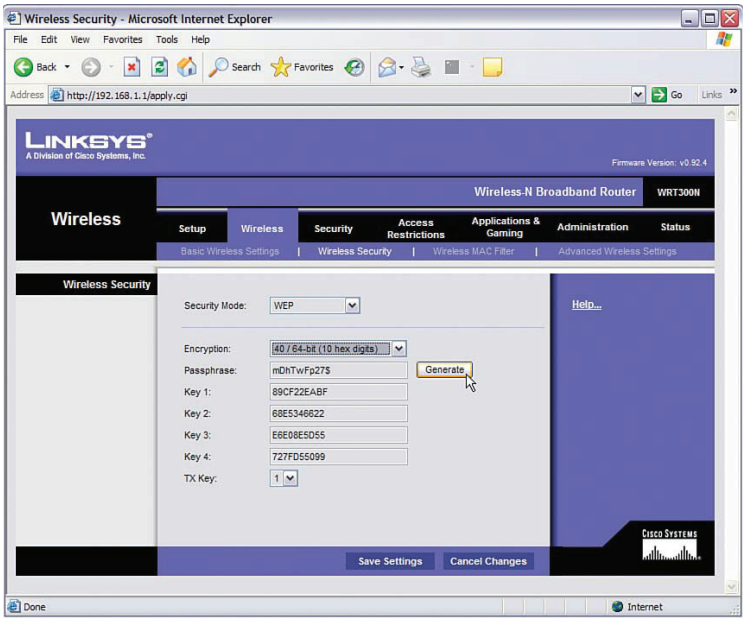
If you are using WEP to encrypt your wireless network, there are essentially two types of WEP: 64-bit WEP and 128-bit WEP. The only difference is the length of the key used to encrypt and decrypt the packets being sent and received on the wireless network. The longer the key, the more secure the encryption is. If the wireless router and wireless NIC are using different WEP key lengths, they will not be able to understand each other and the connection will fail.



Note: 64-bit WEP is pretty obsolete and very easily compromised. It's better than nothing, but use it only if no other form of encryption is available.

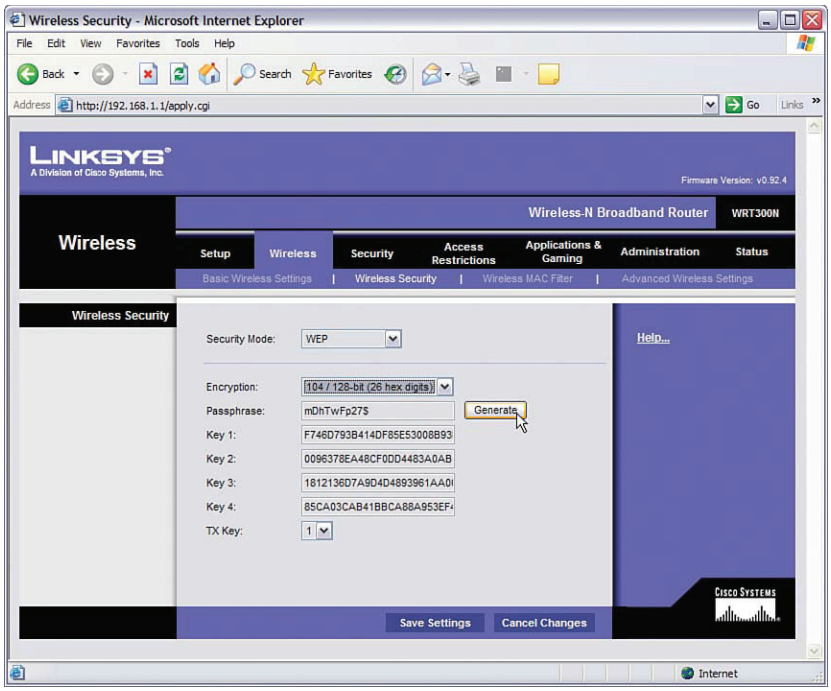
Let's say we have decided to use 128-bit WEP on our wireless network. To see if WEP key length is causing an issue, start by checking the setting on the wireless router. Access the wireless router using an Internet browser. Click the **Wireless** tab and then the **Wireless Security** subtab, as shown in Figure 10-22.

Figure 10-22 Verifying WEP Key Length on the Wireless Router



In Figure 10-22, we can see that the WEP key length is set to 64 bits, not 128. If our wireless NICs are set to use 128-bit WEP, this will cause them to be unable to join the wireless network. Click the drop-down arrow of the Encryption field and choose the setting for 128-bit WEP, as shown in Figure 10-23. Click **Save Settings** if you changed the setting.

Figure 10-23 Setting WEP Key Length to 128 Bits on the Wireless Router



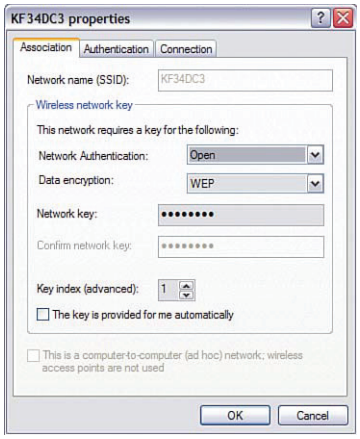
Now let's take a look at the wireless NICs to verify that their WEP key length is set correctly.

If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Select the home network profile and then click **Properties**. Figure 10-24 shows an example.

In Figure 10-24, we can see that for the wireless network with SSID KF34DC3, WEP is correctly set as the encryption type. Unfortunately, though, with Windows XP, we cannot actually see an indication of whether we set the key length correctly. The key length is determined based on how long the key is when you type it in. If you type in a key using 10 hexadecimal digits, the key length will be set to 64 bits. If you type in 26 hexadecimal digits, the key length will be set to 128 bits.

So if we want to make sure the key length is correct, we simply would have to type the key again. Fortunately, when you type the key in, Windows XP forces you to enter either 10 digits or 26 digits. If you have any doubt about whether you entered the full 128-bit WEP key, enter it again into both the **Network Key** and **Confirm Network Key** fields and click **OK**.

Figure 10-24 Verifying the WEP Key Length Setting in Windows XP



If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Wireless Profiles** tab. Select the profile for your home wireless network and click the **Edit** button. Click **Next** until you find the **Wireless Security** dialog box, shown in Figure 10-25 (to save space, all the preceding dialog boxes are not shown here). Similar to the Windows XP example earlier, we can see that the encryption type is correctly set to WEP. Click **Next**.

Figure 10-25 Verifying WEP on the Wireless NIC with Linksys WLAN Monitor

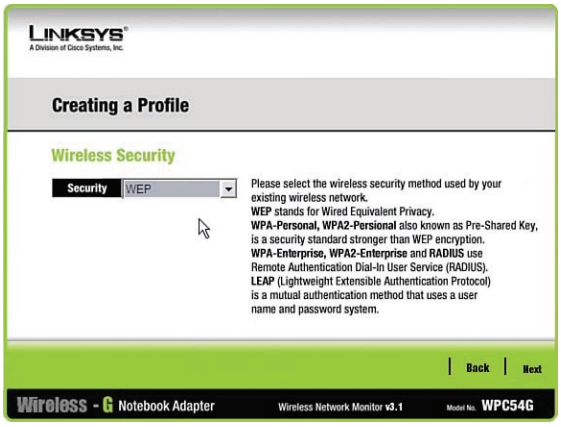
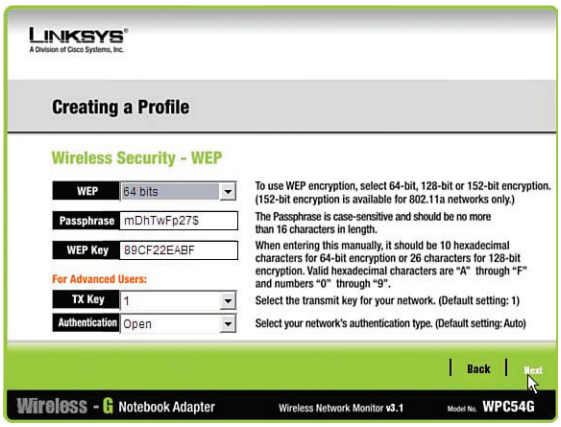


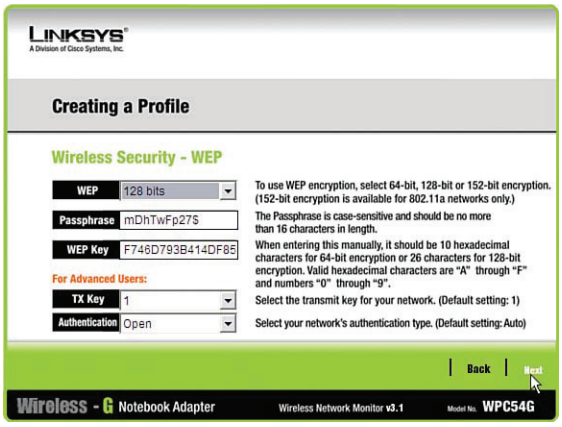
Figure 10-26 shows that the WEP key length is incorrectly set to 64 bits. This will cause a mismatch with the wireless network if the wireless router is set to use 128-bit WEP.

Figure 10-26 Verifying WEP Key Length with Linksys WLAN Monitor



Click the drop-down arrow of the WEP field and set the value to **128 Bit**, as shown in Figure 10-27.

Figure 10-27 Correcting WEP Key Length with Linksys WLAN Monitor



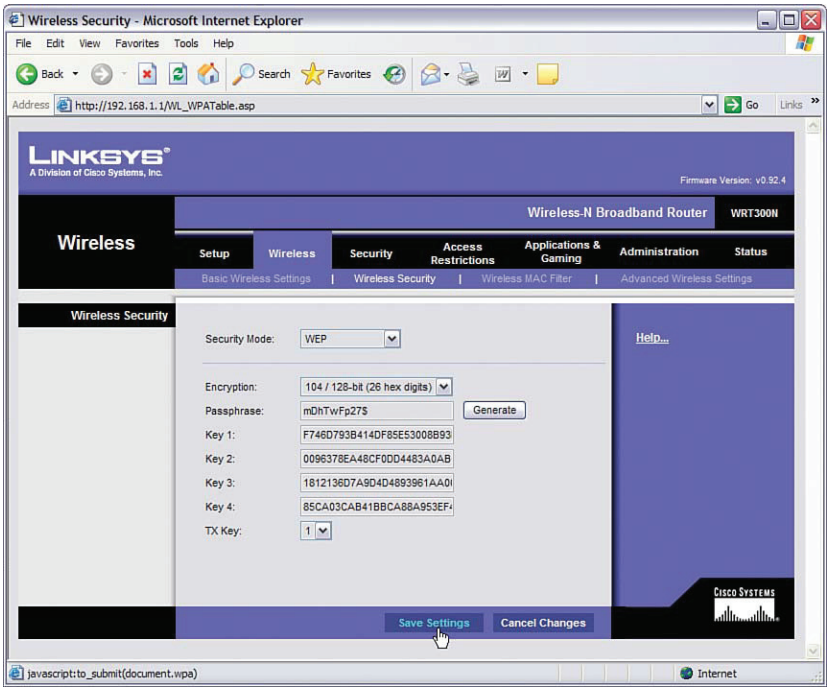
Click **Next** several times until you reach the Confirmation dialog box. Click **Save** to save the settings in the wireless profile.

WEP Key Mismatch

Once you verify the correct encryption type and key length, the other problem that can occur is that the key itself does not match. If the wireless router and wireless NICs are using a different key, they will not be able to understand each other and the connection will fail.

First, double-check the WEP key on the wireless router. Access the wireless router using an Internet browser. Click the **Wireless** tab and then the **Wireless Security** subtab, as shown in Figure 10-28.

Figure 10-28 Verifying the WEP Key on the Wireless Router



Here we can see that the WEP key passphrase is set to mDhTwFp27$ and the WEP key (Key 1, which is the important one) is set to F746D793B414DF85E53008B93E. These are the values we created in Chapter 9 when we secured the wireless network. Recall that the WEP key was actually generated by the router after we created and entered a passphrase.

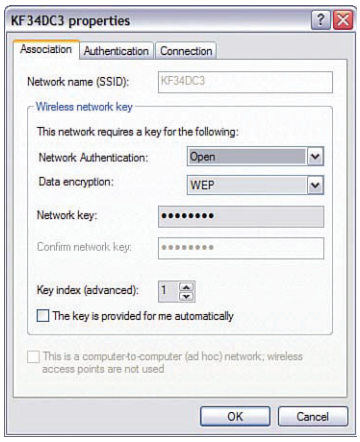
Write down both the WEP passphrase and the WEP key. The passphrase is case sensitive, so pay attention to the upper- and lowercase letters.

The WEP key is *not* case sensitive (so 6A is the same as 6a). But, the key is a lot of digits (10 or 26), so make sure to write it down accurately, not missing any digits or getting any out of order.

Now, let's confirm the WEP key on the wireless NICs. If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Select the home network profile and then click **Properties**. Figure 10-29 shows that for the wireless network with SSID KF34DC3, WEP is correctly set as the encryption type.

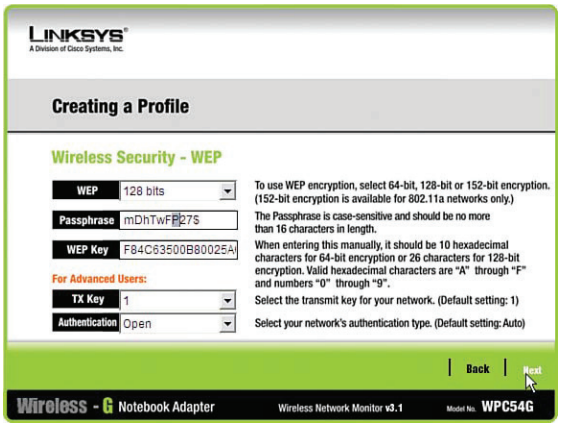
With Windows XP, we cannot see whether we typed in the WEP key correctly, because the display is masked for security purposes (presumably so someone cannot look at it over your shoulder or something). So if we want to make sure the WEP key is correct, we simply have to type the key again. Type the key that you previously wrote down from the router (the key, not the passphrase) into both the **Network Key** and **Confirm Network Key** fields, and click **OK**.

Figure 10-29 Verifying the WEP Key in Windows XP



If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Wireless Profiles** tab. Select the profile for your home wireless network and click the **Edit** button. Click **Next** until you find the Wireless Security – WEP dialog box, shown in Figure 10-30 (to save space, all the preceding dialog boxes are not shown here).

Figure 10-30 Verifying the WEP Key with Linksys WLAN Monitor

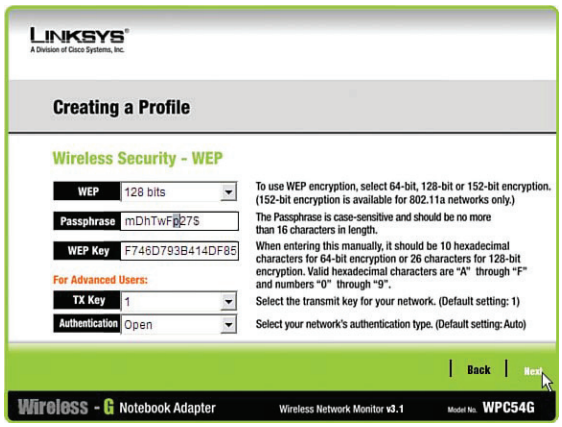


We can see that the WEP passphrase is incorrectly set to mDhTwFP27$, causing a mismatch with the wireless router. The router WEP passphrase has a lowercase *p* as one of the characters, whereas the NIC WEP passphrase has an uppercase *P*. That small difference is enough to render the wireless connection inoperable.

Also notice the WEP key just below the passphrase. That small difference in the passphrase completely changed the WEP key that was generated.

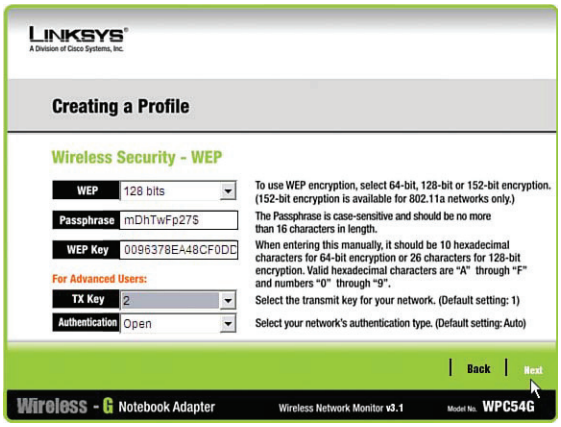
Edit the WEP key passphrase to the correct value, as shown in Figure 10-31. Notice that the WEP key generated now matches what was generated on the wireless router. That is a good way to double-check that you have entered the passphrase correctly.

Figure 10-31 Correcting the WEP Key with Linksys WLAN Monitor



As a final note on WEP keys, make sure the WEP TX Key field is set to **1** on both the wireless router and the wireless NICs. Changing this value will change the WEP key used. For example, Figure 10-32 shows that changing the value to 2 means a completely different WEP key will be used, and again there will be a mismatch with the wireless router.

Figure 10-32 Verifying the WEP Key Number with Linksys WLAN Monitor



Although possible, we do not recommend messing around with the TX key number. It is a feature that is meant to be able to generate multiple WEP keys from a single WEP passphrase. Instead, if you want to use a different WEP key, we recommend that you just create a new WEP passphrase on the wireless router and generate a new key.

Click **Next** several times until you reach the Confirmation dialog box. Click **Save** to save the settings in the wireless profile.

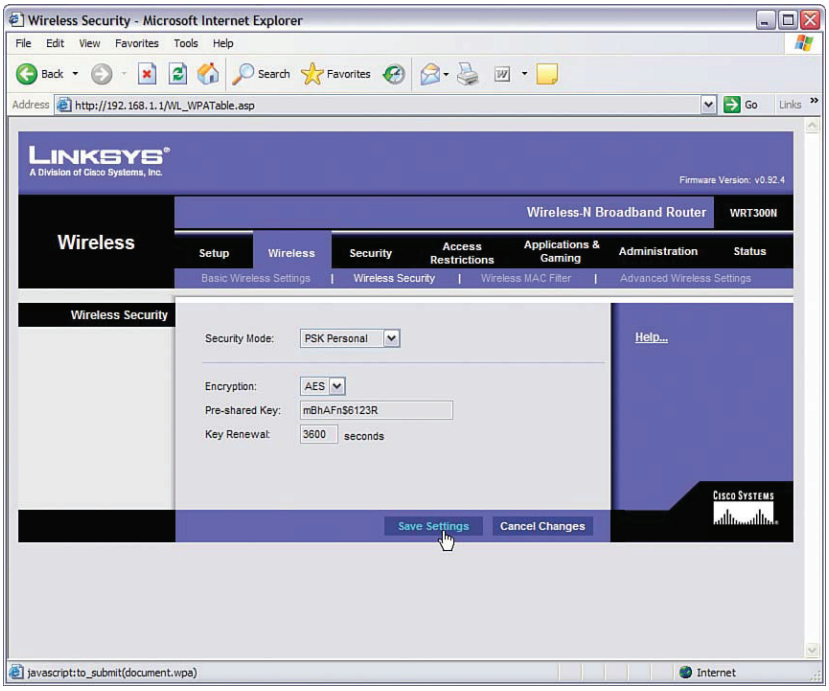
WPA Type Mismatch

If you are using WPA to encrypt your wireless network, there are essentially two types of WPA: TKIP and AES. The difference is the type of encryption used to encrypt and decrypt the packets being sent and received on the wireless network. AES is considered more secure than TKIP, but not

all wireless routers and wireless NICs support AES yet. If the wireless router and wireless NIC are using different WPA types, they will not be able to understand each other and the connection will fail.

Let's say we have decided to use WPA with AES on our wireless network. To see if the WPA type is causing an issue, start by checking the setting on the wireless router. Access the wireless router using an Internet browser. Click the **Wireless** tab and then the **Wireless Security** subtab, as shown in Figure 10-33.

Figure 10-33 Verifying the WPA Type on the Wireless Router



Here we can see that the WPA type is set to AES, as we intended. Now let's take a look at the wireless NICs to verify that their WPA type is set correctly.

If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Select the home network profile and then click **Properties**. Figure 10-34 shows an example.

WPA can be a little confusing because there are two ways to provide a key for WPA networks:

- Sharing the key in advance with all NICs
- Providing a key when you join from a central authentication server

In general, home networks use the *preshared key (PSK)* method, while corporate networks use the *key provided* method.

Figure 10-34 Verifying the WPA Type Setting in Windows XP

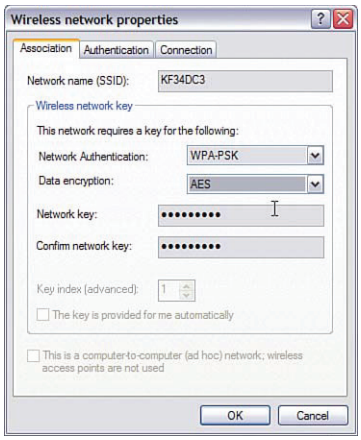


Wireless routers and wireless NICs may refer to these methods slightly differently. With Linksys wireless routers, you want to select WPA-Personal or Personal-PSK. With Linksys wireless NICs managed with Linksys WLAN Monitor, you want to select WPA-Personal. For NICs managed using Windows, the option is WPA-PSK.

In this example we can see that for the wireless network with SSID KF34DC3, WPA-PSK is correctly set as the encryption method. However, we can see that the WPA type is set incorrectly to TKIP.

Click the drop-down arrow for the Data Encryption field and set the encryption type to the correct value of **AES**. Figure 10-35 shows an example. Click **OK** to save the settings.

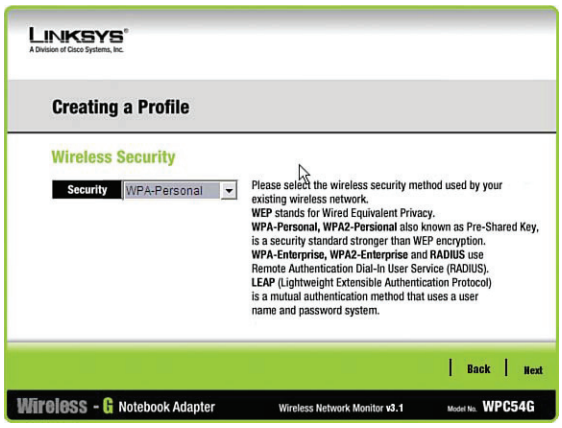
Figure 10-35 Changing the WPA Type Setting in Windows XP



If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Wireless Profiles** tab. Select the profile for your home wireless network and click the **Edit** button. Click **Next** until you find the **Wireless Security** dialog box, shown in Figure 10-36 (to save space,

all the preceding dialog boxes are not shown here). We can see that the encryption type is correctly set to WPA-Personal. Click **Next**.

Figure 10-36 Verifying WPA on the Wireless NIC with Linksys WLAN Monitor



As shown in Figure 10-37, we can see that the WPA type is incorrectly set to TKIP. This will cause a mismatch with the wireless network if the wireless router is set to use AES.

Figure 10-37 Verifying WPA with Linksys WLAN Monitor

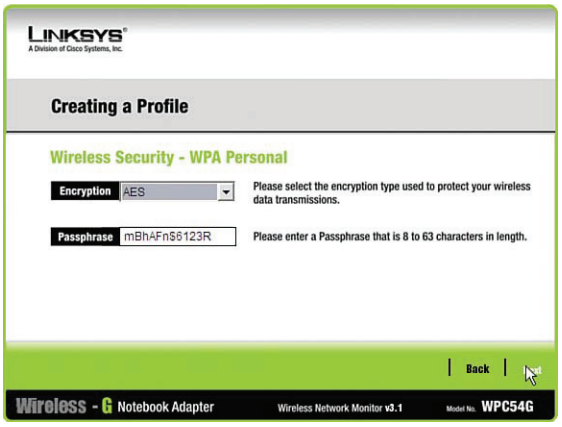


Click the drop-down arrow for the Encryption field and set the value to the correct **AES** setting, as shown in Figure 10-38.

Click **Next** several times until you reach the Confirmation dialog box. Click **Save** to save the settings in the wireless profile.

You can use either TKIP or AES as the WPA type. Both are very secure methods for encrypting your wireless network. The critical thing, though, is that you have to choose a single method on both the wireless router and all wireless NICs, because otherwise the wireless router and NIC will not understand each other and the connection will fail.

Figure 10-38 Correcting the WPA Type with Linksys WLAN Monitor

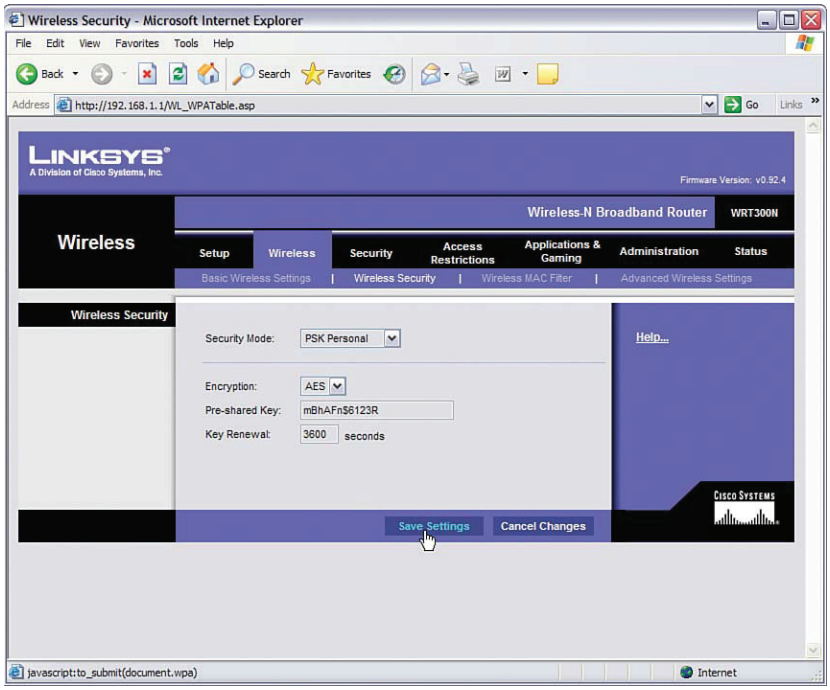


WPA Preshared Key Mismatch

Once you verify the correct WPA type, the other problem that can occur is that the WPA key itself does not match. If the wireless router and wireless NICs are using a different WPA preshared key, they will not be able to understand each other and the connection will fail.

First, double-check the WPA preshared key on the wireless router. Access the wireless router using an Internet browser. Click the **Wireless** tab and then the **Wireless Security** subtab, as shown in Figure 10-39.

Figure 10-39 Verifying the WPA Preshared Key on the Wireless Router



Here we can see that the WPA preshared key is set to mBhAFn$6123R. This is the value we created in Chapter 9 when we secured the wireless network. Recall that, unlike WEP, WPA uses just a passphrase key; there is no additional key that is generated by the router from the passphrase.

Write down the WPA preshared key. Make sure to pay attention to the upper- and lowercase letters.

Now, let's confirm the WPA key on the wireless NICs. If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Select the home network profile and then click **Properties**. Figure 10-40 shows an example.

Figure 10-40 Verifying the WPA Preshared Key in Windows XP



In Figure 10-40, we can see that for the wireless network with SSID KF34DC3, WPA-PSK is correctly set as the encryption type. With Windows XP, we cannot see whether we typed in the WPA key correctly, because the display is masked for security purposes (presumably so someone cannot look at it over your shoulder or something).

So if we want to make sure the WPA preshared key is correct, we simply have to type the key again. Type the key that you wrote down earlier from the router into both the **Network Key** and **Confirm Network Key** fields (or cut and paste it from the router dialog to the NIC dialog if you have both up on your screen), and click **OK**.

If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Wireless Profiles** tab. Select the profile for your home wireless network and click the **Edit** button. Click **Next** until you find the Wireless Security – WPA Personal dialog box, shown in Figure 10-41 (to save space, all the preceding dialog boxes are not shown here).

We can see that the WPA preshared key is incorrectly set to MBhAFn$6123R, causing a mismatch with the wireless router. The router WPA preshared key has a lowercase *m* as the first character, whereas the NIC WPA preshared key has an uppercase *M*. That small difference is enough to render the wireless connection inoperable.

Edit the WPA key to the correct value, as shown in Figure 10-42.

Figure 10-41 Verifying the WPA Preshared Key with Linksys WLAN Monitor

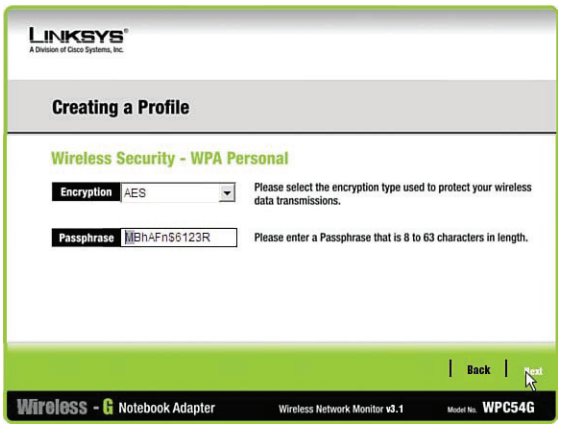
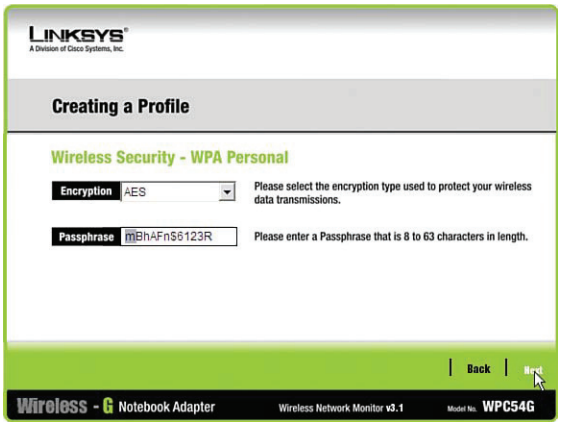


Figure 10-42 Correcting the WPA Key with Linksys WLAN Monitor

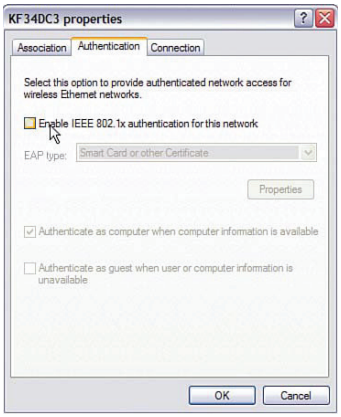


Windows XP Authentication Setting Mismatch

Windows XP has an additional setting that can be problematic. For corporate networks, many companies are implementing a security method that requires their employees to provide a user ID and password to log in to the wireless network. This login process uses a technology standard called IEEE 802.1x. How it works is beyond the scope of this book, but suffice it to say that for home networks, 802.1x is not used (at least not yet). Windows XP typically disables or enables this setting automatically based on the encryption method you choose. However, we have seen at least one case where it was incorrectly set and prevented a wireless network connection.

Here is how to confirm that it is disabled on the wireless NIC. Using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Select the home network profile and then click **Properties**. Click the **Authentication** tab. Verify that the **Enable IEEE 802.1x Authentication for This Network** setting is *not* checked, as shown in Figure 10-43. If it is, then uncheck it and click **OK** to save the settings.

Figure 10-43 Verifying the Authentication Setting in Windows XP



IP Address Assignment–Related Issues

After you have confirmed that the wireless NIC is now making a connection properly to the wireless router, including encryption, it's time to move on to the last step in the connection process: obtaining an IP address. Joining the wireless network allows the NIC to send and receive packets to and from the router. To be a part of the home network, the NIC also needs an IP address.



Note: IP addressing is a fundamental networking concept that is not covered in detail in this book. The 30-second description is that each device (computer, laptop, and so on) in a home network needs to have an IP address, which is how the device is known on the network. IP addresses have four numbers, separated by a dot (.). Most home networks use IP addresses in the range of 192.168.1.100 to 192.168.1.149, and the router assigns each device an address from this pool when it boots. This is called *dynamic IP addressing*, or Dynamic Host Configuration Protocol (DHCP). To learn more about how IP addressing works, pick up a copy of *Home Networking Simplified*.

With dynamic IP addressing, or DHCP, enabled on the wireless router, when a NIC establishes a new wireless connection, it then requests an address from the router, and the router assigns the next available one from the pool. The wireless NIC can then use the address until the computer is shut down or the laptop leaves the wireless network.

Why would an IP address not be assigned correctly? There is not really a good reason; let's just say that DHCP does not seem to always work properly. Sometimes a wireless NIC gets "stuck," thinking it already has an IP address (maybe from the last network it joined). Also, in very weak signal conditions, the request could get lost, never reaching the router.

On the router side, it's also possible that all the available IP addresses in the pool have been assigned. This is usually not the case, but, depending on how many devices you have on your home network and the size of the address pool, it could be an issue. Occasionally, if one or more devices are having an intermittent connection issue in which they keep losing the signal and then coming back onto the network, they could be requesting a new IP address each time, and the router could exhaust its pool.

Finally, depending on the wireless NIC, sometimes with WPA encryption, if the WPA key does not match, the NIC will appear to connect to the wireless signal just fine but will not be able to properly

acquire an IP address from the router. In other words, it looks like a DHCP problem, but it's really a mismatched WPA key.

It's important to be able to recognize when a problem with the IP address assignment is happening, and you may be able to take some actions to remedy the problem. The next few sections give some tips.



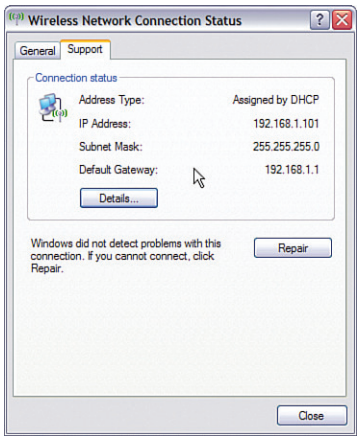
Note: Static IP addressing, which is when you turn off DHCP and assign your home network addresses manually, is quite problematic. Problems include duplicate addresses, errors in manually entering IP addresses, and others. We do not recommend using static IP addressing in home networks. If you do, prepare yourself for some frustration.

Determining if an IP Address Is Assigned

You first need to figure out whether you are getting an IP address assigned. Here is how to tell.

If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then right-click and select **Status** from the list. Click the **Support** tab. Figure 10-44 shows an example.

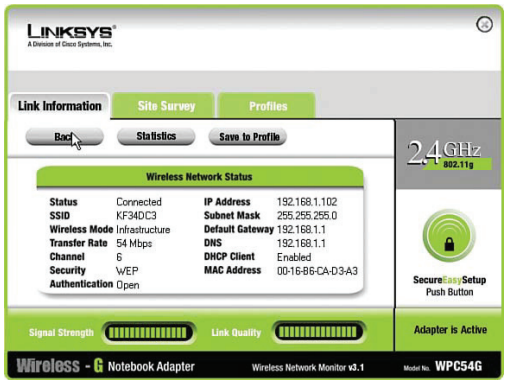
Figure 10-44 Verifying IP Address Assignment with Windows XP



In Figure 10-44, we can see that the IP address 192.168.1.101 has been assigned to the wireless NIC. We can also see that a default gateway IP address has been assigned, 192.168.1.1. This is good. We have both an IP address to use for the NIC and a gateway to which to send requests to access the Internet. This should be a complete connection now for us to access the Internet from the laptop or other computer that is connected over the wireless connection.

If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **More Information** button on the Link Information tab. Figure 10-45 shows the resulting link information.

Figure 10-45 Verifying the SSID on the Wireless NIC with Linksys WLAN Monitor



Again, we can see that this wireless NIC has been assigned an IP address of 192.168.1.102 and a default gateway of 192.168.1.1. This should be a completely established connection, and we should be able to access the Internet. If not, then something may be wrong with the broadband Internet connection itself, or the wireless router may not be reaching the Internet for some reason. Try accessing the Internet from a computer with a wired connection. Also try rebooting the wireless router, broadband modem, and computer with the wireless NIC.

Determining if IP Address Assignment Is Failing

There are some indications you can look for to tell if the wireless connection is failing due to an IP address assignment malfunction.

In Windows XP, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then right-click and select **Status** from the list. Figure 10-46 shows that the wireless NIC is trying to acquire an address from the wireless router. Even though the wireless signal shows five bars, and we see a few packets being sent and received, we can see that the overall status is **Acquiring Network Address**.

If the NIC stays in that status for a relatively long time, say 3 to 5 minutes or more, chances are the address assignment is not going to work. When it ultimately times out and stops trying, you will likely get an indication like that shown in Figure 10-47.

Figure 10-46 Checking the Status of IP Address Assignment in Windows XP

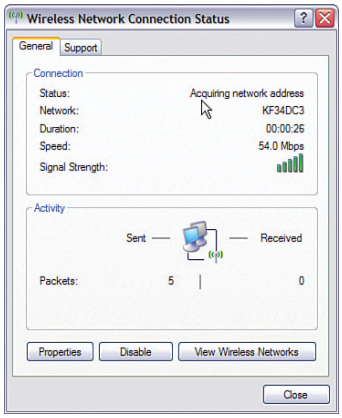
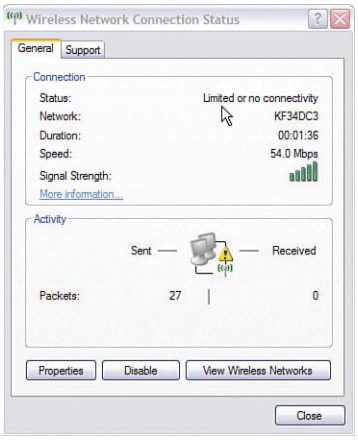


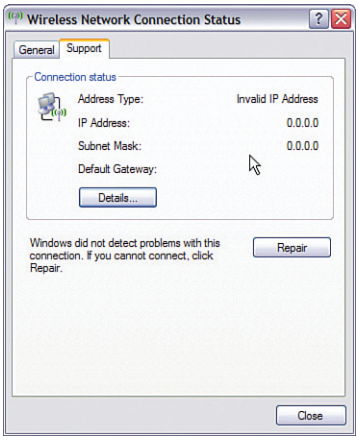
Figure 10-47 Indication of IP Address Assignment Failure in Windows XP



If the status shows **Limited or No connectivity**, that is usually an indication that IP address assignment has timed out and the laptop or computer has no IP address assigned to use. Consequently, the computer is not going to be able to do a whole lot on the home network, including access the Internet.

Clicking the Support tab enables you to get a further indication of what is wrong, similar to the example shown in Figure 10-48. Here you can see that the status is **Invalid IP Address**. This is another indication that something did not work correctly with dynamic IP address assignment.

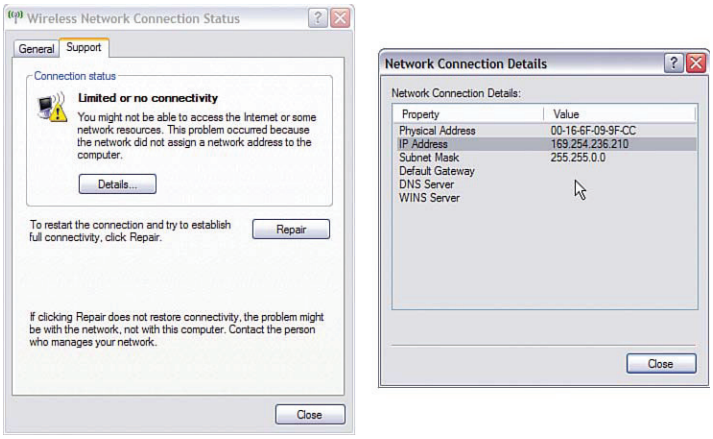
Figure 10-48 Checking If IP Address Assignment Failed in Windows XP



Clicking the Details button displays a little bit more information, as shown in Figure 10-49.

You can see that it appears that an IP address is assigned, 169.254.236.210. This is not a "real" IP address from the home network; this is the default IP address that occurs when IP address assignment has failed. If you see an address assigned like this, the computer is not going to be able to access the Internet.

Figure 10-49 IP Address Assignment Failure Details in Windows XP



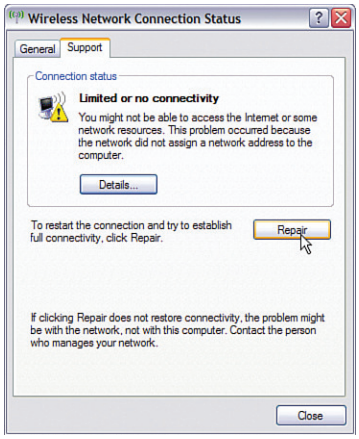
Trying the Windows XP Repair Function

Windows XP has a pretty slick built-in function to attempt to repair a networking connection. The function essentially disables the NIC and then re-enables it, effectively restarting the NIC in a "fresh" state.

Whenever you are having issues with IP address assignment, Windows XP Repair seems to have a pretty good success rate, assuming nothing fundamental is wrong, such as a mismatched WPA key. We have found Windows XP Repair fairly useful to solve DHCP-related problems.

To invoke the Repair function in Windows XP, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then right-click and select **Status** from the list. Figure 10-50 shows an example.

Figure 10-50 Repairing a Network Connection in Windows XP



Click the **Repair** button. Windows XP will go through a series of steps and advise you of progress, including disabling the wireless NIC, enabling, connecting to the wireless network, and acquiring an IP address. One of the advisements is shown in Figure 10-51. When it completes, the Repair function will advise you whether it was successful in completing a connection to the wireless network.

Figure 10-51 Repairing a Network Connection in Progress

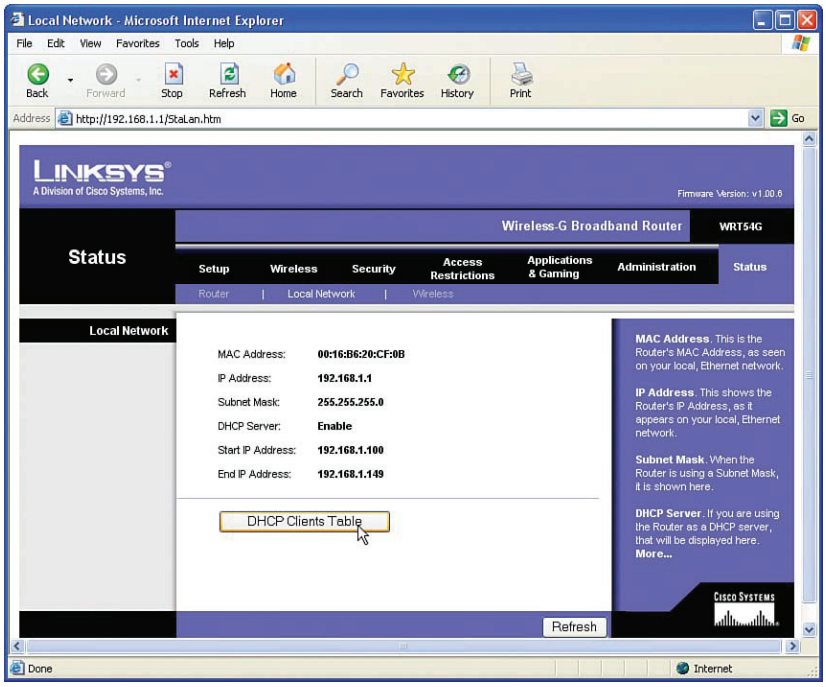


This remedy may correct the issue. If it does not, then chances are something else is wrong, and you should recheck some of the earlier steps. It also does not hurt to try shutting down and rebooting the laptop, and even the wireless router.

Checking the Router's DHCP Client Pool

Once you have pulled enough of your hair out (you be the judge of that), you may want to see what is going on from the wireless router's perspective as well. Access the wireless router using an Internet browser. Click the **Status** tab and then the **Local Network** subtab, as shown in Figure 10-52.

Figure 10-52 Checking the DHCP Status on the Wireless Router

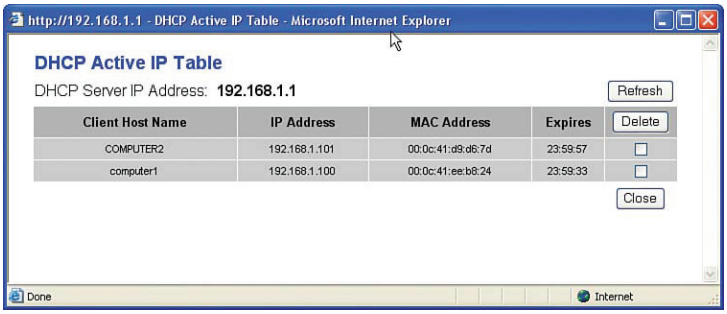


We can see that the DHCP server function is enabled on the wireless router. We can also see the IP address pool that is being used, in this case 50 IP addresses from 192.168.1.100 through 192.168.1.149. That should be plenty for most home networks.

Click the **DHCP Clients Table** button (on some Linksys routers this may be named slightly differently). A table of currently assigned IP addresses will be displayed, like the example shown in Figure 10-53.

We can see two addresses being used: 192.168.1.100 by Computer1 and 192.168.1.101 by Computer2. There does not appear to be anything out of the ordinary.

Figure 10-53 Checking the DHCP Clients on the Wireless Router



If you see one of the computers listed many times, or a whole list of devices you do not recognize, that could certainly be an issue. In that case, you may want to try rebooting the router and see if the issue clears up.



Note: Checking the DHCP clients table on your wireless router periodically can be a good security practice. If you see computers or other devices listed in the client table that are not yours, it could be a sign that someone is joining your wireless network without your permission. You can then take appropriate measures, such as changing your SSID and WPA key, or turning on MAC filtering. If you see them on again, it's time to take more active measures such as involving the authorities. Many states are starting to pass laws that make it a crime to join wireless networks without an owner's permission. Check the laws in your state (or province, county, parish, planetary body, and so on…).

For more information about security measures for home networks, pick up a copy of *Home Networking Security Simplified*.

Wireless Connection Made

Now that we have made it through all the steps, we need to check if we have a wireless connection yet.

If you are using the Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **View Wireless Networks**. Figure 10-54 shows that we are now connected successfully to the network with SSID KF34DC3, having passed all the steps up through obtaining an IP address.

If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Figure 10-55 shows that we are now connected successfully to the network with SSID KF34DC3, having passed all the steps up through obtaining an IP address.

Figure 10-54 Verifying a Wireless Connection with Windows XP

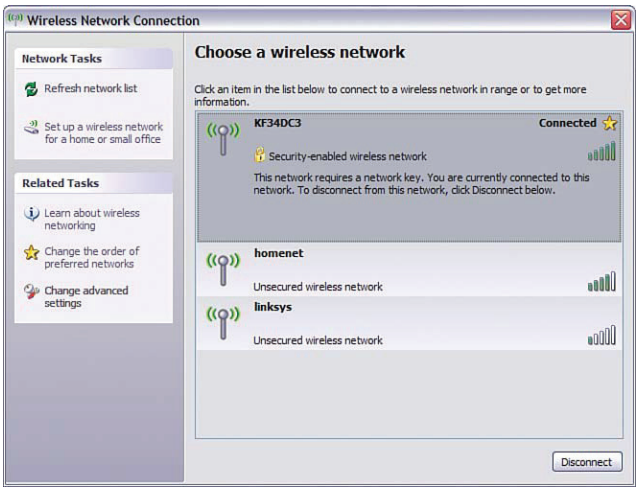
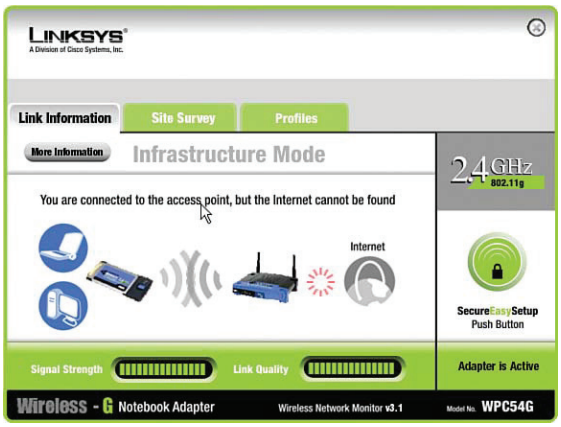


Figure 10-55 Verifying a Wireless Connection with Linksys WLAN Monitor



If you do not have a connection at this point, return to the start of section "Figuring Out Why It Will Not Connect," and try again. You may also want to shut down everything, restart it, and see if that auto-magically fixes the issue.

Oops, How Embarrassing!

Okay, so you have tried everything and nothing seems to be working. Here are a few other things to double-check. Some of them may seem silly, but trust us, we have seen it or we wouldn't list it:

- Is the wireless router actually plugged in and powered on?
- Do you have security turned on in the wireless router but not the wireless NIC?
- Have you tried connecting with a wired connection to see if the computer and the Internet are working?
- Can you connect to the wireless router with any other wireless laptop or computer (in other words, are you sure the wireless router is working at all)?
- Is the wireless NIC actually powered on, plugged in, enabled, and working?
- Can you make a wireless connection without security? Try turning off wireless security (WEP or WPA) on both the wireless router and all NICs and then connecting.

The 10-Minute Miracle

Many professionals who fix computers and networks for a living tell us to always include what they call the "10-minute miracle." Put simply, it means shut everything down, turn everything off, and go have your favorite beverage (they say coffee, we prefer beer, although we have also found that too many 10-minute miracle breaks for beer can be somewhat counterproductive to troubleshooting). Come back in 10 minutes, power things back up, and start looking at it again.

You may be surprised that whatever was not working is now working. Try it, it works sometimes.

Summary

You may read through these steps and say, "No, it can't be that, I am skipping that step." Trust us, do every step no matter how confident you are. Even we have spent 20 minutes trying to figure out why we can't get a connection, only to find out the wireless NIC in our laptop was shut off.

If all else fails, call in help from the kids, a smart neighbor, or a professional service.

Where to Go for More Information

For more home networking and home network security information, refer to our other books, *Home Networking Simplified* (Cisco Press, 2005) and *Home Network Security Simplified* (Cisco Press, 2006).

Microsoft provides an article titled "How to Troubleshoot Wireless Network Connections in Windows XP Service Pack 2" on its website: http://support.microsoft.com/kb/870702.

Bradley Mitchell has an article titled "Troubleshooting, Tips and Tweaks" at About.com: http://wireless.about.com/cs/wirelessproducts/a/howtobuildwlan_5.htm.

CHAPTER 11

Troubleshooting: I Can Connect Sometimes

Sometimes, your wireless network works well when you set it up, but then when you try to use your laptop over a wireless connection, say in the living room, it does not always connect. You might be experiencing a wireless signal coverage issue. Before assuming so, make sure you have successfully connected your computer to the router via a wireless connection at least once, even if your computer is right beside the router.

If you have never connected to the wireless router successfully, start with Chapter 10, "Troubleshooting: I Can't Connect at All." If you have connected before but are not able to use the wireless network in locations inside your house where you want to, take a look at the rest of this chapter.

How Wireless Coverage Works

Wireless networks are similar to cell phone networks:

- The more bars of service you have, the better the call sounds.
- When you have very few bars of service, you may be able to place a call, but it probably does not sound very good.
- When you have zero bars of service, you cannot make or receive calls.

Wireless networks operate the same way, as shown in Figure 11-1. When you are within the coverage area of your wireless network and have good signal strength (shown in the green area), you will have a good wireless connection and also have at or near the maximum data rate your wireless router supports (54 Mbps for 802.11g, 108 Mbps or higher for 802.11n, and so on).

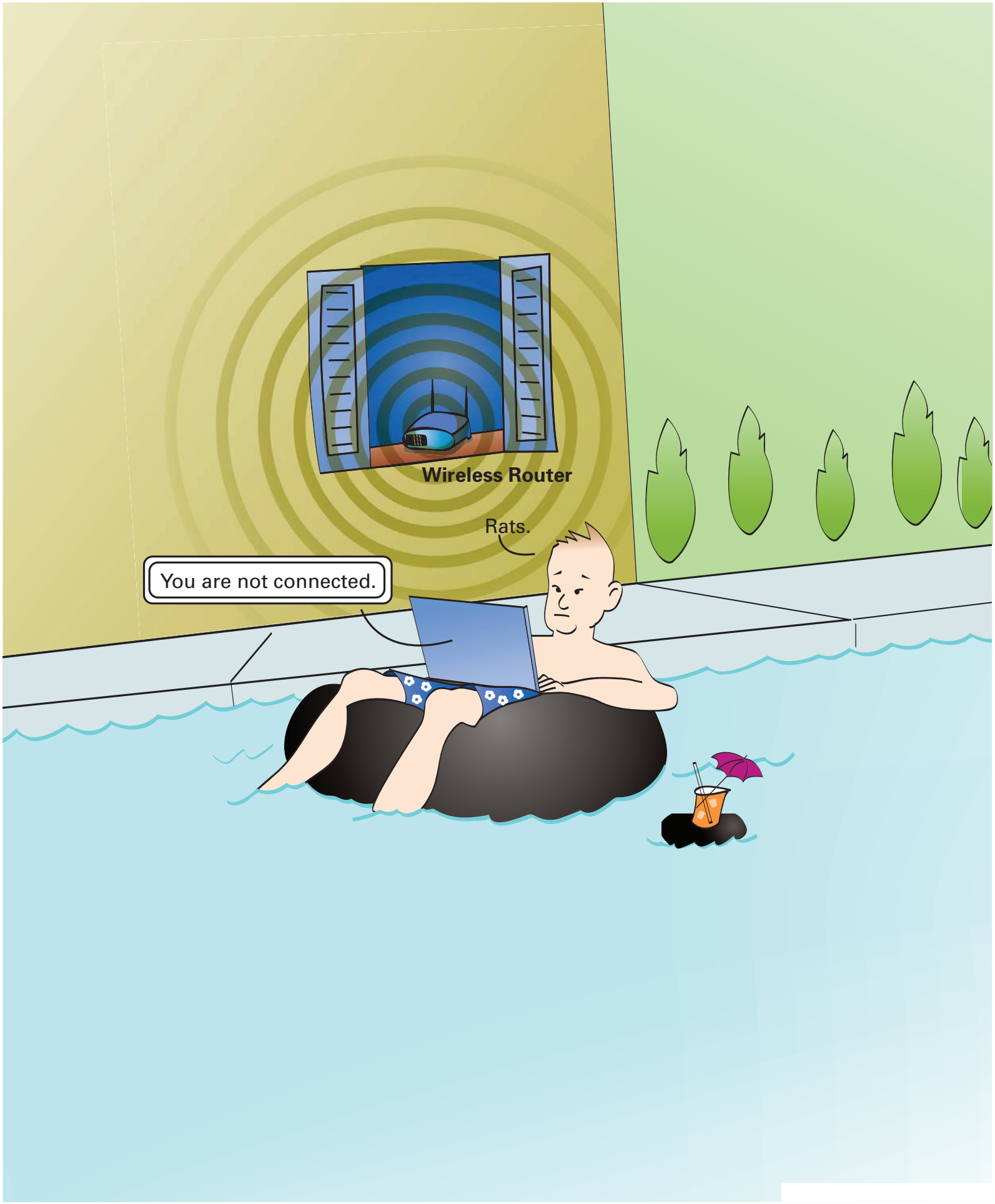
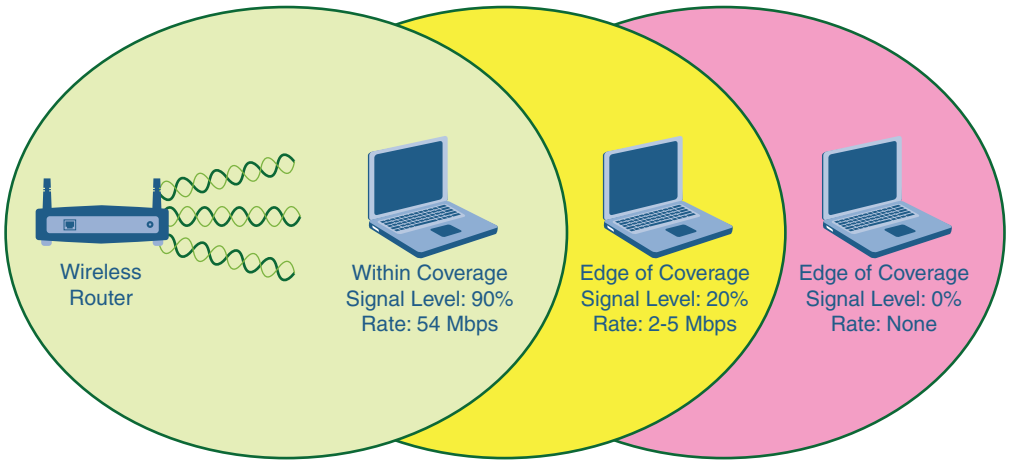

Wireless Router
Rats.
You are not connected.

Figure 11-1 How Wireless Network Coverage Affects Usage



When you are at the edges of your wireless network coverage, you will have relatively low signal strength, say between 5 and 20 percent of signal or 1 to 2 bars, depending on how your wireless NIC displays signal strength. At the edges, you will typically see a lower data rate than your wireless router supports, such as 5 Mbps or 2 Mbps, and you may also see that sometimes the signal strength goes to zero. You may also periodically see the signal disconnecting and then reconnecting. Keep in mind, though, that this is only at the edge of the usable range, and that if you are in the usable range, your performance should be fine.

When you are outside your wireless network coverage, you will have zero signal strength, and the wireless NIC will show a status of disconnected from the wireless network.

Tuning Your Wireless Coverage

Most wireless routers being sold today that are based on the 802.11g or 802.11n standard have pretty good range to cover the average house.

As discussed in Chapters 2, "Wireless Standards: What the Letters Mean," and 3, "Selecting the Right Wireless Standard for Your Network," 802.11a typically provides somewhat less coverage because it operates at the 5-GHz band, where wireless signals inherently just do not travel as far as they do on the 2.4-GHz band (where 802.11g and 802.11n operate).

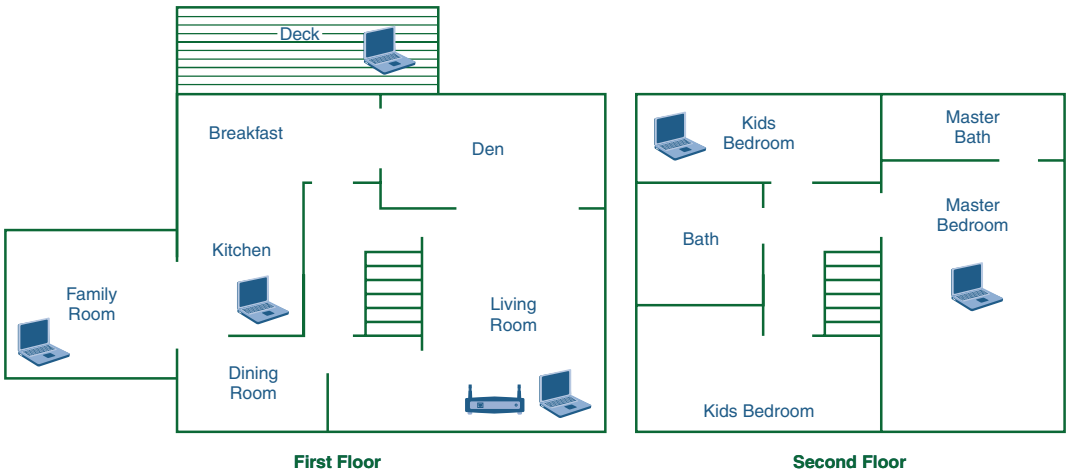
Quite often when you have coverage issues, you might have done something that is causing the range of the wireless network to suffer unnecessarily. Often, by following a few basic tuning rules, you can get the most out of your wireless router. The rest of this chapter tells you how.

Performing a Wireless Survey

After setting up the wireless router in the preferred location, the next step is to perform a survey of the wireless coverage in your house. Start by thinking about in which locations in your house you

want to use a laptop to connect over wireless, and which desktop computers are connected with wireless as well. It may be helpful to make a rough floor plan drawing like we did in Chapter 4, "Planning Your Wireless Network," marking where you expect to use wireless, such as that shown in Figure 11-2.

Figure 11-2 Sample Floor Plan for Conducting a Wireless Survey



Also make a quick chart, such as that shown in Table 11-1, with the different locations within your house listed in the first column and then a column for current signal strength and one or two columns for modified signal strength. In the sections that follow, we will fill in the chart while taking some readings.

Table 11-1 Wireless Survey Chart—Empty

	Current	Change 1	Change 2
Living Room			
Kitchen			
Back Deck			
Master Bedroom			
Kid's Bedroom			
Family Room			

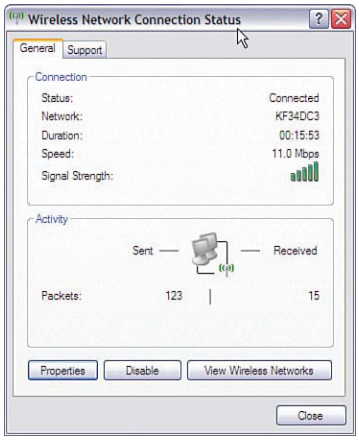
Next, we are going to take a laptop from room to room, check the signal strength we see from the wireless router, and record it in the table. Two surveys are shown in the sections that follow: one performed with the Windows Wireless Network Connection utility, and one performed using the Linksys WLAN Monitor utility.

Wireless Survey Using Windows XP

If you are using Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Select the home network profile and then click **Properties**.

For each room in the house, take the laptop to the room, put it in the location in which you plan to use it, and wait a few seconds for the display to update. Figure 11-3 shows an example for the living room. Write down in Table 11-1 that we have five out of five possible bars of service, which is a very good signal level.

Figure 11-3 Living Room Wireless Survey Using Windows XP



Move to each room in your house, each time waiting a few seconds for the reading to update, and write the figure down. Figure 11-4 shows the reading on the back deck: three out of five bars.

Figure 11-4 Back Deck Wireless Survey Using Windows XP

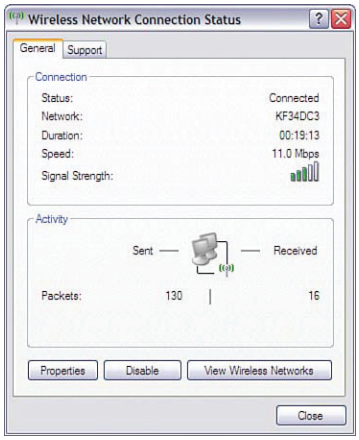
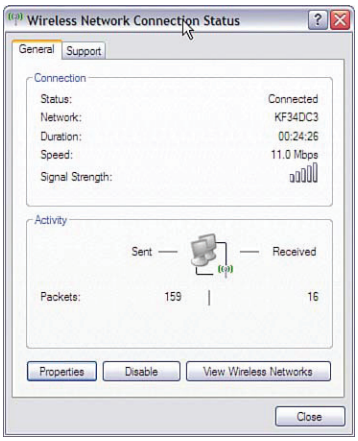


Figure 11-5 shows the reading upstairs in the family room: no bars, which indicates a very weak signal. Using wireless in this room is going to be a problem.

Figure 11-5 Family Room Wireless Survey Using Windows XP



Keep going through the rest of the house, each time recording the reading in your table. The completed example table is shown in Table 11-2.

Table 11-2 Wireless Survey Chart—After First Survey

	Current	Change 1	Change 2
Living Room	5		
Kitchen	4		
Back Deck	3		
Master Bedroom	4		
Kid's Bedroom	2		
Family Room	0		

We can see from the Table 11-2 that for most of the rooms in the house, we should have a fairly good wireless signal. Any room with a single bar of service or less is a likely problem area. In our example survey, the family room, which is the farthest room away from the wireless router, looks like it will be a problem.

Wireless Survey Using Linksys WLAN Monitor

If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Link Information** tab and then the **More Information** subtab.

Again, for each room in the house, take the laptop to the room, put it in the location in which you plan to use it, and wait a few seconds for the display to update. Figure 11-6 shows an example for the living room. Write down in Table 11-1 that we have 15 out of 15 possible bars of service, which is a very good signal level.

Figure 11-6 Living Room Wireless Survey Using Linksys WLAN Monitor



Move to each room in your house, each time waiting a few seconds for the reading to update, and write the figure down. Figure 11-7 shows the reading on the back deck: 5 out of 15 bars.

Figure 11-7 Back Deck Wireless Survey Using Linksys WLAN Monitor

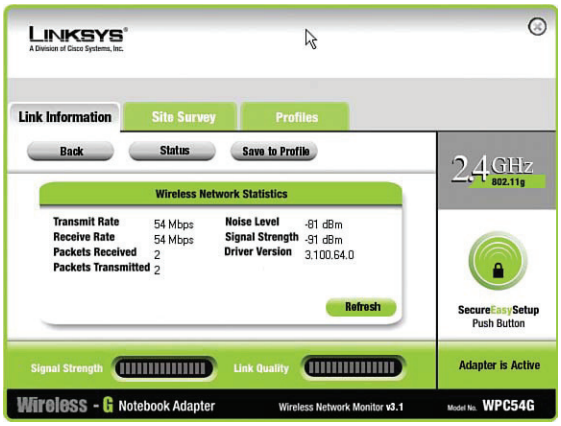




Note: You may notice that the Linksys WLAN Monitor displays two indicators: Signal Strength and Link Quality. Signal Strength is a measure of how well the wireless NIC can "see" the wireless router's wireless signal. Link Quality measures how well the wireless router signal can be understood. The vast majority of the time, the two go hand-in-hand, so don't get too bogged down worrying about which one to look at. Just record signal strength.

Figure 11-8 shows the reading upstairs in the family room: no bars, which indicates a very weak signal. Using wireless in this room is going to be a problem.

Figure 11-8 Family Room Wireless Survey Using Linksys WLAN Monitor



Keep going through the rest of the house, each time recording the reading in your table. The completed example table is shown in Table 11-3.

Table 11-3 Wireless Survey Chart—After First Survey

	Current	Change 1	Change 2
Living Room	15		
Kitchen	6		
Back Deck	5		
Master Bedroom	7		
Kid's Bedroom	3		
Family Room	0		

Again, we can see from the table that for most of the rooms in the house, we should have a fairly good wireless signal. Any room with about two bars of service or less is a likely problem area. In our example survey, the family room, which is the farthest room away from the wireless router, looks like it will be a problem.

What to Conclude from Your Wireless Survey

Looking at the wireless survey, you want to make a couple of decisions. First, verify that your survey shows you have the strongest signal in the room closest to the wireless router. The farther away you get from the router, the weaker the signal becomes. Second, determine whether you have adequate signal coverage in the areas of your house where you want to use a wireless connection. If not, then you may want to take some actions to improve the coverage.

Based on where you plan to use wireless the most within your house, you next need to determine if you've placed the wireless router in the optimal location in your house. (See the "Improving the Location of the Wireless Router" section later in this chapter.)

To some extent you are limited to locations in your house that have the possibility to connect to the broadband Internet service you have (DSL or cable), but you may have some flexibility. DSL can generally be placed anywhere inside your home where there is a phone jack. Cable is a little more restrictive, but can usually be placed anywhere there is a cable jack. In some situations, you may need to have the DSL or cable provider install a more centralized phone or cable jack for the broadband service.

Do keep in mind, though, that you do not need to have the maximum signal strength in every room where you want to use your wireless. We do not recommend installing new DSL or cable jacks unless the room where you want to use wireless gets very bad coverage or no coverage at all.

You can try several remedies to improve your signal coverage. These are described in the rest of the chapter.

What You Can Do to Improve Coverage

Here are the three primary reasons why coverage might not be as good as it can be:

- The wireless router setup or location is not optimal.
- Other devices in your house are interfering with the wireless network.
- The wireless router equipment you have is not adequate for the coverage you need.

If you determine that your coverage is not what you need, what can you do? There are a few things to try. The next few sections give some possible remedies for these limitations. Each time you try one of these remedies, repeat the wireless survey process described in the previous section to see if the change improved the network. Be aware that one change may improve a room that has zero coverage, but then cause another room to suddenly have coverage problems. You may need to attempt a couple of remedies to get the best overall coverage for all the locations in the house in which you want to use wireless.

Improving the Location of the Wireless Router

One of the most important determining factors of how your wireless network will perform is where you locate the wireless router itself. Table 11-4 gives you five simple do's and don'ts for wireless router location in your house.

Table 11-4 Five Simple Guidelines for Wireless Router Location

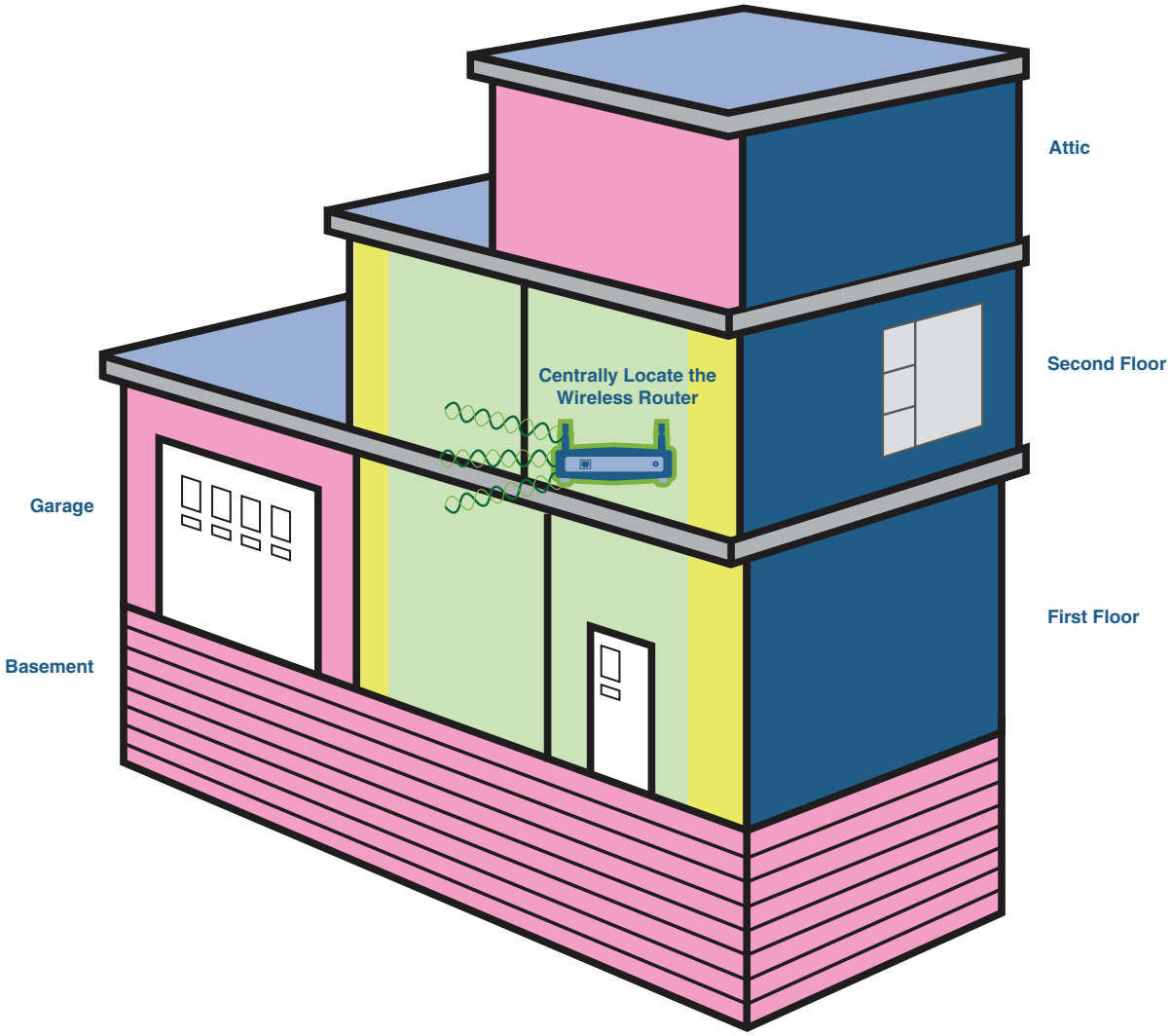
Do	Don't
Choose a site for the router in a central location in your house, considering all three dimensions (see Figure 11-9). Note the bigger the house, the more important this becomes.	Put the router in the basement, attic, garage, closet, or other isolated part of your house.
Place the router on a wooden table or desk where the router (and especially the antenna) is not obscured.	Place the router on the floor, in a metal bookcase, in a metal enclosure, or in a drawer.
Keep away from potential interfering devices like microwave ovens, cordless phones, and baby monitors.	Keep a cordless phone base or handset next to the router.
Plug into a power strip with a surge protector, and plug the power strip into an empty outlet.	Plug into an outlet along with other electrically "noisy" devices, such as hair dryers, blenders, toasters, and so on.
Keep the antennas free from obstructions, including wires and cables.	Drape electrical cords or cables over the router or antennas, or wrap extra wires around the antennas.



Note: We omitted some pretty obvious guidelines from Table 11-4, but we have heard of these happening, so they are worth mentioning. The funny part is, you will probably read this and think we are kidding:

- You have to actually remove the router from the store packaging and plug it in somewhere in your house for it to work. It's not so much the shrink wrap that causes the problem, but the lack of electricity is hugely limiting.
- Don't put the router in a wet or damp area. This includes an area where pets are likely to urinate on it. By the way, urination on electrically powered devices, such as routers, can be just as detrimental to your pet as it is to the wireless network.
- Aluminum foil generally does not make a good antenna booster, although there is something to be said for empty Pringles cans, and a lot of "research" seems to have been done in this area.
- Unless specifically designed for use outdoors, the vast majority of wireless routers are for use indoors only, and bad things happen if they get rained on. This is true of most things with an electrical plug, by the way.
- A dark, cool, corner room of the basement or root cellar is a great place to store wine. Great places to store wine are not good places for wireless routers.
- You need to be at *home*, or close by, to use your wireless *home* network. If you are out of state on vacation, it is extremely unlikely you will get a signal from your *home* network.
- You may be tempted to mount your router on the ceiling (like they do in the office), but keep in mind that your office has a false ceiling to allow cable runs and, more importantly, your company has people who do this type of installation for a living. We're not saying it wouldn't be cool to do, but you are signing up for a lot of work (and a mess) if you try this at home.

Figure 11-9 Choose a Central Location for the Wireless Router



If you follow the guidelines described in this section, you will get the most coverage from your wireless router. If you do not follow them, and do something like putting the wireless router in a metal bookcase or computer desk cubby hole, no amount of tuning is going to help.

Next, let's move on to some other tips to help you get the most from the wireless network coverage.

Trying Different Channels

Wireless networks operate today in what are called *unlicensed frequencies*. The U.S. Federal Communications Commission (FCC), or the equivalent in your country, manages who uses which radio frequencies for what purposes. For example, television broadcasters, FM radio stations, police and fire radios, and cellular phone companies all must be licensed by the FCC to use a particular set of radio frequencies. If the FCC did not regulate this, no one would be able to rely on such services because everyone would be transmitting all over each other, and none of the services would work very well.

However, the FCC designates certain sets of radio frequencies as unlicensed, and as long as a certain set of general guidelines is followed, anyone can build devices that operate at these frequencies. The common public unlicensed frequency bands (in the United States) are 900 MHz, 2.4 GHz, and 5.1 GHz.

Approximately 5 to 10 years ago, cordless phones, baby monitors, and many other home wireless devices commonly used the 900-MHz band. More recently, most home wireless devices are built to operate in the 2.4-GHz band, somewhat because of overcrowding of the 900-MHz band. Finally, many new devices are being built to operate in the higher 5.1-GHz band.

There are not a lot of differences or advantages to frequency bands, except the number of other devices that share the band. Most home wireless networks use the 2.4-GHz band, with a few built for the 5.1-GHz band.

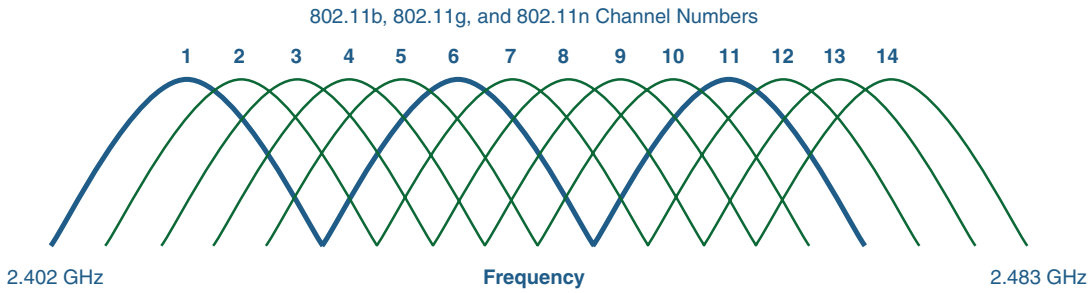
Each band is broken up into a number of usable channels. Table 11-5 shows the band and possible channels for each of the wireless standards.

Table 11-5 Possible Wireless Channels

Standard	Band	Channels	Default
802.11b	2.4 GHz	1–11	6
802.11g	2.4 GHz	1–11	6
802.11a	5.1 GHz	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	52
802.11n	2.4 GHz	3–9	5

802.11b, 802.11g, and 802.11n networks all operate in the 2.4-GHz band. There are 11 channels (in the United States), as shown in Figure 11-10 (Channels 12, 13, and 14 are valid in a few countries outside of the United States.)

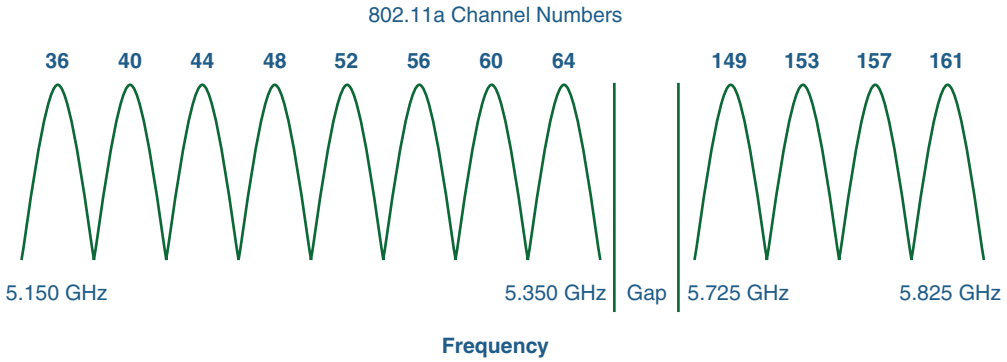
Figure 11-10 Channels for 802.11b, 802.11g, and 802.11n Standards



These channels are "overlapping," which means that part of the signal for one channel spills over a bit into the channels above and below it. This means there are three unique channels: 1, 6, and 11. If you have one wireless router using channel 1 and another nearby wireless router on channel 2, these channels partially overlap, so they could cause each other interference.

802.11a networks operate in the 5.1-GHz band (which ranges from 5.150 GHz to 5.825 GHz). There are 12 channels (in the United States), as shown in Figure 11-11.

Figure 11-11 Channels for 802.11a Standard



These channels are "nonoverlapping," which means that one channel does *not* spill into channels above and below it. This means that all 12 channels are unique channels for a wireless network. Nearby routers may use channels 44 and 48, for example, without interfering with each other.

Whenever you purchase a wireless router, the manufacturer has preconfigured it to use a particular default wireless channel. For Linksys wireless routers that are built for the 802.11b and 802.11g standards, the default channel is 6. The other defaults are shown in Table 11-5.

Many times, the default channel works very well and you do not need to think about it any further. Sometimes, though, there can be interference from other devices or something in your home that makes the default channel not work as well as possibly another one of the channels.

The types of devices in your home that can interfere with the wireless network include

- Microwave ovens (2.4 GHz)
- Cordless phones (2.4 GHz or 5.1 GHz) depending on which band they are built for
- Bluetooth devices, like wireless cell phone headsets (2.4 GHz)
- Room-to-room wireless audio/video extender (2.4 GHz)
- Wireless USB (2.4 GHz)
- Home automation sensors and controls (2.4 GHz)
- Your neighbor's wireless router (2.4 GHz or 5.1 GHz)

The most common two are microwave ovens, particularly older ones with less than adequate shielding, and cordless phones. As we discussed earlier in this book, we highly recommend that if you have an 802.11b, 802.11g, or 802.11n wireless home network, purchase 5-GHz cordless phones. This way the phones and wireless network will not interfere with each other.

Other than eliminating the source of the interference (preferred, but sometimes you just cannot), another possibility is to try changing the wireless channel that the router uses. It is very easy to do, here's how:

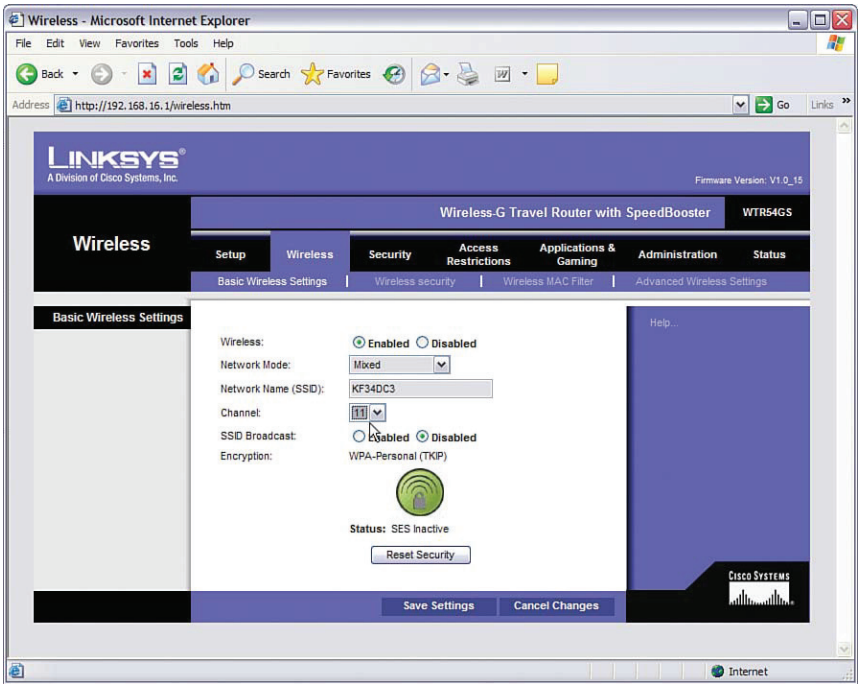
Step 1 Access the wireless router using an Internet browser.

Step 2 Click the **Wireless** tab, as shown in Figure 11-12.

Step 3 From the **Channel** field, change the channel to an alternative channel. If the router is set to the default channel 6, try channel 1 or 11. For this example, we set it to channel 11.

Step 4 Click **Save Settings**.

Figure 11-12 Changing the Channel on the Wireless Router

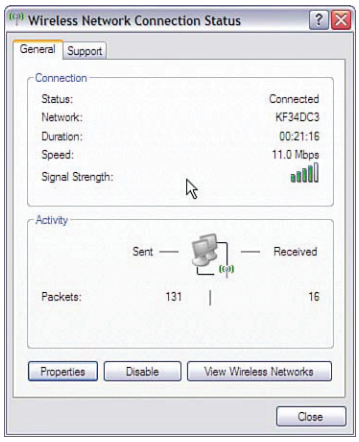


Once you click Save Settings, all wireless NICs on the network will lose connection with the wireless router and start scanning for a wireless network. They should simply re-establish a connection to your wireless network on the modified channel.

After changing the channel, you should conduct another wireless survey, as described earlier in this chapter, to see if the change had a positive or negative impact on your wireless network coverage.

If you are using Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Select the home network profile and then click **Properties**. Figure 11-13 shows an example.

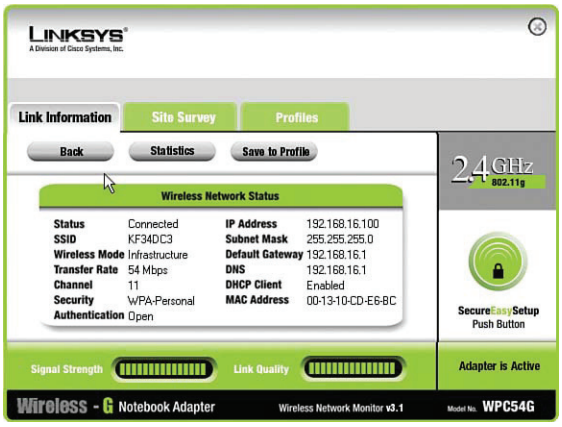
Figure 11-13 Surveying the Channel Change with Windows XP



We cannot see the actual wireless channel number in Windows XP. We can just look at the wireless signal level (in terms of bars of service) and visually inspect whether it is improved or not. Here we can see that changing the wireless channel had a positive effect on the wireless signal in the family room, where we were having trouble before.

If you are using the Linksys WLAN Monitor utility, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Link Information** tab and the **More Information** subtab. Figure 11-14 shows an example.

Figure 11-14 Surveying the Channel Change with the Linksys WLAN Monitor



With the Linksys WLAN Monitor, we can see the actual wireless channel, now channel 11. Once again, the wireless coverage in the family room improved in this example.

Update the table we made earlier with the new wireless survey data you collected after the channel change. Sample data for our example is shown in Table 11-6.



Note: When you change the channel on the router, you do not need to make any changes on the wireless NIC, because it automatically searches for and finds the new channel. This is one of the only times you need to change something on the router only and not on the NIC.

Table 11-6 Wireless Survey Chart—Channel Change

	Current	Channel Changed to Channel 11	Change 2
Living Room	15	15	
Kitchen	6	11	
Back Deck	5	10	
Master Bedroom	7	1	
Kid's Bedroom	3	1	
Family Room	0	15	

We can see from the new wireless survey after the change that we improved the coverage in the family room, kitchen, and back deck (very important for surfing by the pool). However, coverage in the master bedroom and kid's bedroom now may be a problem.

This is one of the challenges with wireless networks. They are a bit like squeezing a balloon: You squeeze on one side and the bubble pops out another side.

Assess from your wireless survey whether the channel change addressed the problems adequately. If not, you could try another channel or move on to some other possible remedies.

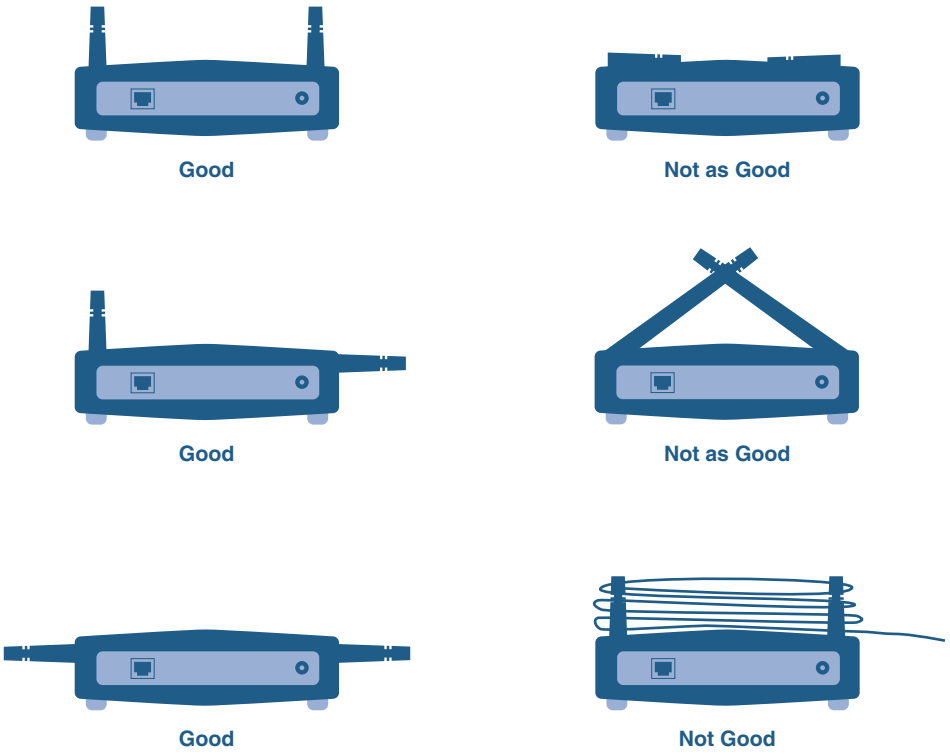
Trying Different Antenna Positions

Sometimes, simply changing the direction of the antennas on the wireless router can make a big difference in wireless coverage. There is no simple rule for which antenna positions will be best for your network, but there are some general guidelines.

As discussed earlier, first make sure that the location of the wireless router leaves the antennas with open air around them. Putting the router inside a bookcase or enclosure, or where antennas are near a bunch of electric wires or cables, will likely cause the network range to suffer.

Figure 11-15 shows some possible positions that work pretty well. In general, keep the antennas pointed in a direction where they are not folded onto each other or obstructed by other objects (including the router itself). You may have to experiment a bit to see if changing the antenna position has an effect on your wireless coverage, and if it is a positive or negative effect.

Figure 11-15 Possible Wireless Router Antenna Positions



Conduct a wireless survey as before to see what the overall effect on the network was. Table 11-7 shows some sample results for our example.

Table 11-7 Wireless Survey Chart—Channel Change

	Current	Channel Changed to Channel 11	Antennas Moved Upward
Living Room	15	15	12
Kitchen	6	11	9
Back Deck	5	10	9
Master Bedroom	7	1	7
Kid's Bedroom	3	1	8
Family Room	0	15	5

Suppose that the antenna changes had the effects shown in Table 11-7. Now the wireless network is a fairly healthy balance of signal strength in all the locations in which we want to use wireless. This would be a pretty good result. Note the change you made in your notebook in case you need to remember later what tuning steps you performed.

Upgrading the Antenna

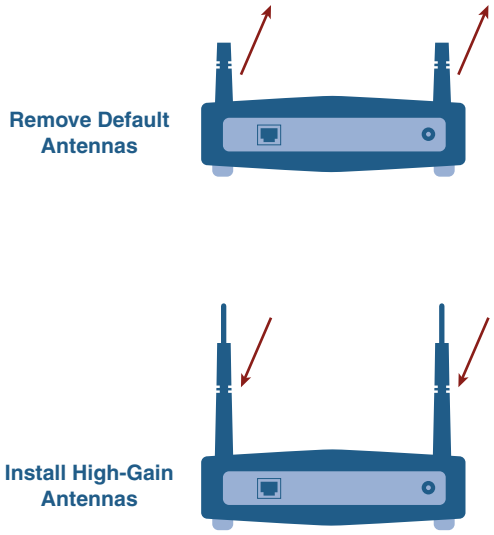
Depending on the type of wireless router you have, it may be possible to improve the antennas it uses to expand your wireless home network coverage. Antennas are a bit like ears for your wireless router: You get a default set of ears like everyone, but you can buy a hearing aid if you want.

Most wireless routers are shipped with a default set of antennas that have the type of performance most typically needed by the majority of customers. Sometimes it is possible to purchase a higher-performance antenna for your wireless router.

Before investing in this option, we recommend you exhaust the other options at your disposal. Make sure you have gone through Chapters 10, 11, and 12 to ensure that you do not have some other issue that is much cheaper to correct.

If you decide ultimately that you want to try upgrading the antennas, check with the manufacturer to see what the options are. For example, if you have a Linksys WRT54G wireless router, you can purchase a supplemental antenna set, model HGA7T, that provides two high-gain antennas to replace the default antennas that come with the router. Figure 11-16 shows that upgrading is pretty easy.

Figure 11-16 Upgrading the Wireless Router Antennas



High-gain antennas can certainly give your home wireless network an added boost in terms of range and coverage. However, this option is a bit expensive. High-performance antennas can cost as much as the router itself.

Using Wireless Range Extenders and Additional Access Points

Other options for improving coverage include installing a range extender or additional access point. Range extenders connect to the wireless router with an Ethernet cable, and they act like a wireless bridge, extending the wireless signal out farther.

Access points are wireless routers, without the router part. They provide an additional point of access for wireless NICs in another room and can extend your wireless coverage.

Both of these options are beyond the scope of this book. If you need to go this route, talk to someone who knows what they are doing and has experience with wireless networks, such as the folks at your neighborhood electronics store. The most common cause for needing a range extender is when you have a huge house. In general, you should try all the other options we mention here first. If you have a very large house and have tried all the other options presented here with no success, then a range extender may be called for.

Upgrading the Wireless Router

In general, 802.11b and 802.11g wireless networks have similar coverage ranges, which adequately cover the average house. 802.11a tends to provide a bit less coverage due to its operation at a higher frequency (5.1-GHz band) that causes the radio waves not to travel as far.

802.11n is a whole new ballgame. The wireless N standard was designed with specific range-improvement technologies that can provide up to four times farther range and reduce what are called "dead spots," areas where coverage suddenly dips to near zero in your house.

Upgrading to a wireless N router, such as the Linksys WRT300N product, could certainly be an effective option to extend your wireless network coverage. We evaluated one of the Linksys WRT300N routers, and in an average house size, we had nearly 100 percent signal strength in all rooms of the house.

Summary

When your wireless coverage is intermittent and causing issues with connecting, there are a number of steps you can take to remedy the problem and improve coverage throughout your house. When the remedies do not work, it may be time to take more serious measures, such as upgrading your network to an 802.11n wireless system.

If the remedies here improve your wireless coverage and you now have good performance, enjoy your wireless network and start surfing from poolside.

If you improve the coverage so that you now have pretty good signal strength in all rooms but still have issues with slow or intermittent connection problems, read the next chapter.

Where to Go for More Information

Check out Bradley Mitchell's article "Top 7 Tips for Improving a Wireless Home Network" on About.com: http://compnetworking.about.com/od/wifihomenetworking/tp/improvehomewifi.htm.

You also might find Microsoft's article "10 tips for improving your wireless network" (by Tony Northrup) helpful: www.microsoft.com/athome/moredone/wirelesstips.mspx.

This page intentionally left blank

CHAPTER 12

Troubleshooting: I Can Connect, but It's Slow

What if you can connect to your wireless network, it stays connected just fine, but it seems like it is slow? To answer that, we first need to understand what to expect from a wireless network. Is it living up to its potential, or is some problem keeping the network from being as fast as it could be?

A wireless network can be slower than expected for a few different reasons:

- Broadband speed limits Internet access speed
- Operating at a slower wireless standard than expected
- Signal degradation due to interference

We explore each of these possibilities in this chapter.

Is the Broadband Internet Connection the Bottleneck?

There is a lot of competition between wireless home networking equipment makers. As a result, faster and faster wireless routers are all the rage. 802.11b started out with 11 Mbps and then 802.11g (and 802.11a) increased the speed to 54 Mbps. Extensions to 802.11g as well as the newest 802.11n standard are increasing the speed even more to 100 Mbps and beyond.



Note: Incidentally, 100 Mbps is the speed of most wired networks today. Some are still 10 Mbps. So wireless networking has caught up to, and in some cases surpassed, wired networking in terms of speed. Wired networking is already starting to move toward 1 Gbps, which equals 1000 Mbps.

So, using a faster router means faster Internet access, right? Well, maybe. The Internet access speed really depends on more factors than just the wireless router speed. Figure 12-1 shows why. We have an 802.11g home wireless network, which provides up to 54 Mbps of speed. This means that within the home network, computers and devices can communicate with each other pretty fast. But when accessing the Internet, the speed is limited by the broadband connection to your house in most cases rather than by your router. The speed between the wireless device and wireless router stays the same, 54 Mbps, but the broadband services today typically only offer in the neighborhood of 384-kbps to 2-Mbps uplink speed (toward the Internet) and between 2-Mbps and 6-Mbps downlink speed (from the Internet).

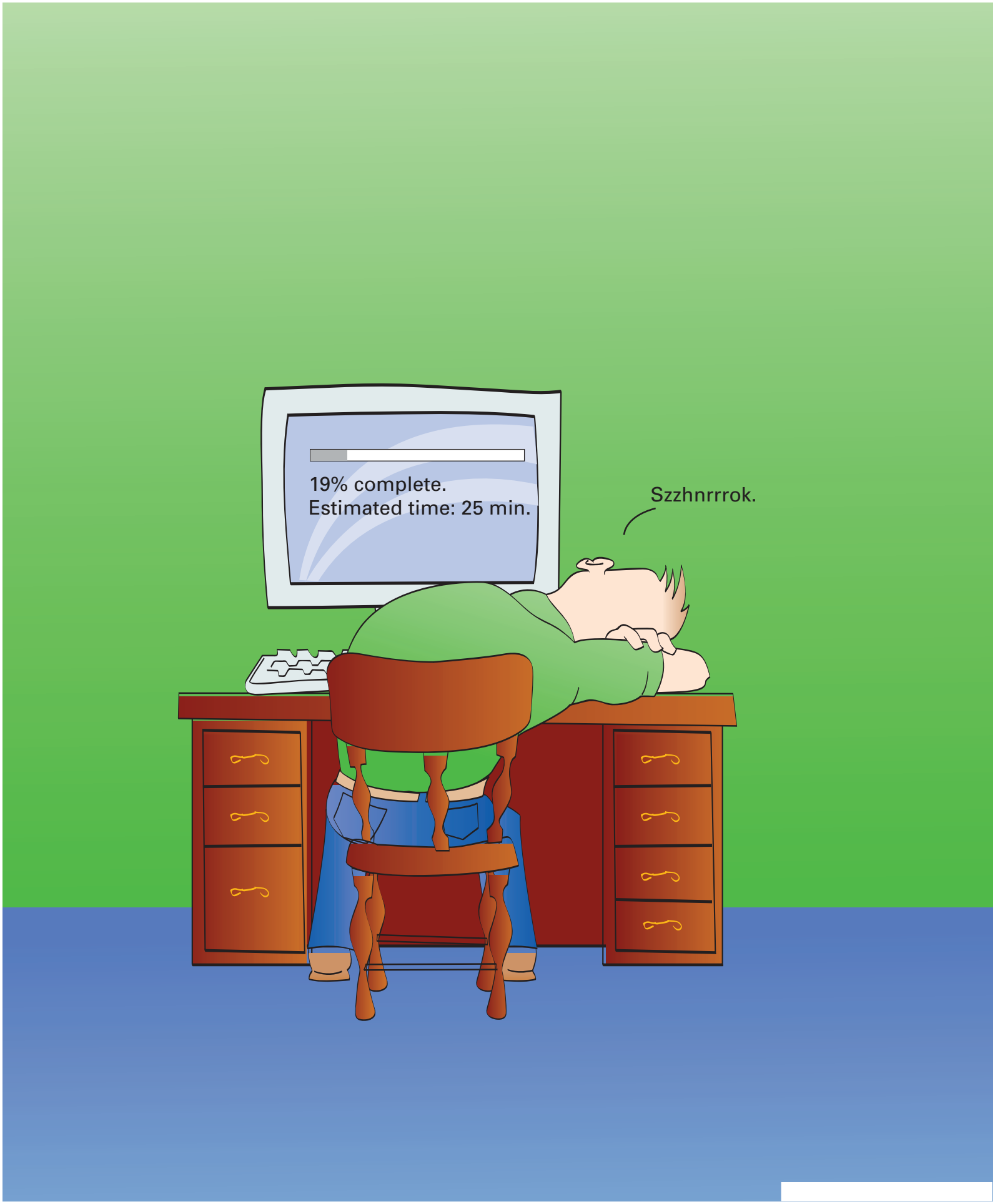
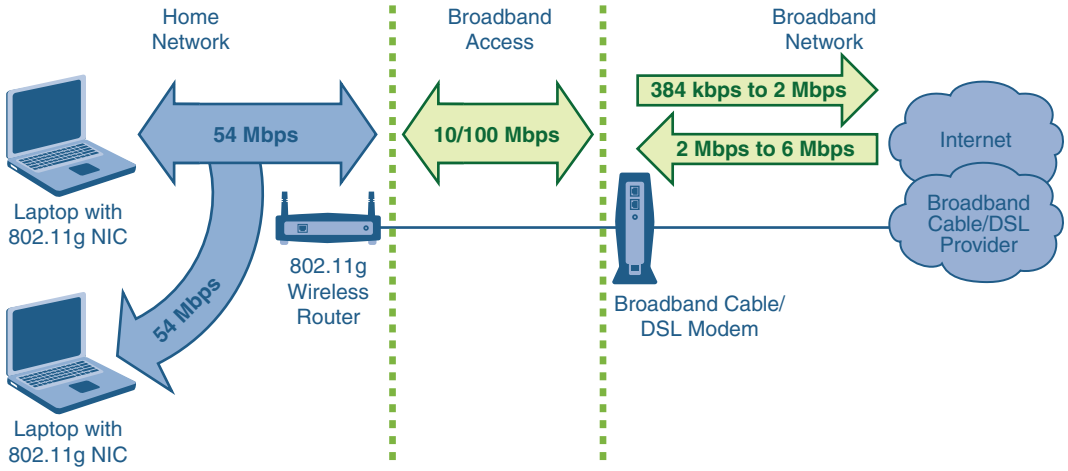

19% complete.
Estimated time: 25 min.
Szzhnrrrok.

Figure 12-1 Networking Speeds Inside and Outside the Home Network



The point is that buying a wireless router capable of 54-Mbps or 100-Mbps speeds does not mean that you get that speed when accessing the Internet. You are limited by the broadband speed.

Checking the Broadband Connection

Sometimes, you can experience issues with your broadband connection that cause your service speed to be slower than you are paying for. This can be caused by an intermittent connection or wiring problem, as well as just general congestion on the broadband service.

We can check whether the router seems to have a good connection to the broadband service. Linksys routers have a built-in utility called *ping* (Windows XP also has this utility) that you can use to perform a rudimentary connection test.

Access the wireless router using an Internet browser. Click the **Administration** tab and then click the **Diagnostics** subtab, as shown in Figure 12-2. Click the **Start to Ping** button.

The wireless router creates and sends a number of test packets to the address in the IP or URL Address field, measuring the success rate and time it takes to receive a response. The results displayed appear similar to the example shown in Figure 12-3.

Figure 12-2 Linksys Router Built-In ping Utility

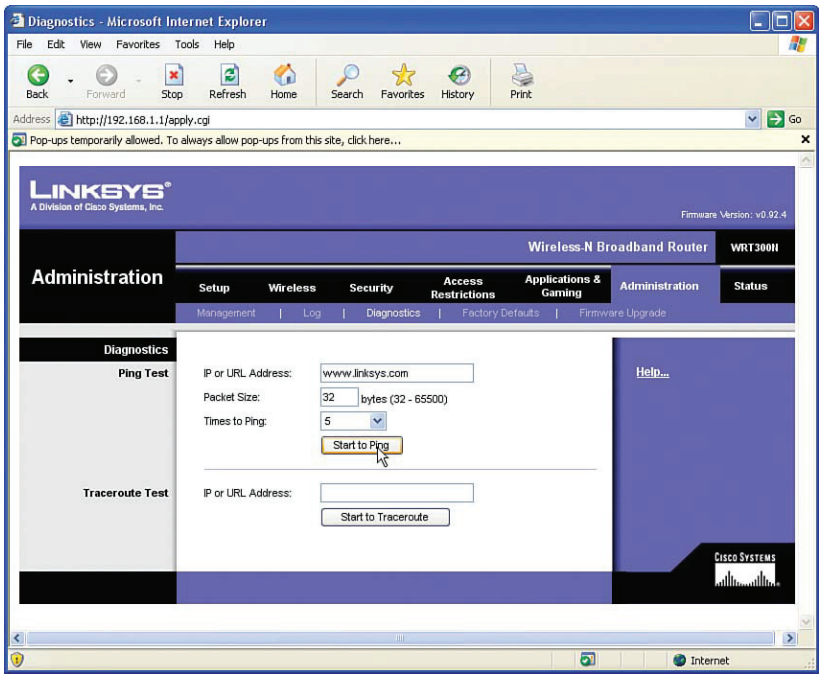
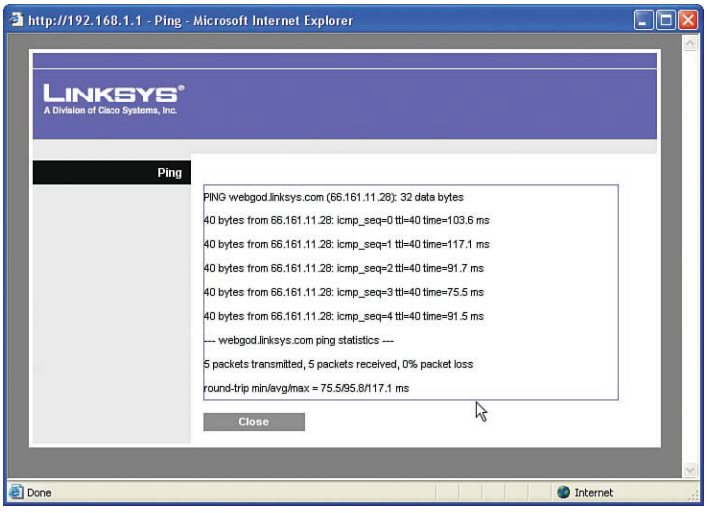


Figure 12-3 ping Test Result



We can see from the results displayed that five test packets were sent and all of them were successful (5 packets transmitted, 5 packets received, 0% packet loss).

We can also see that the time it took for the test packets to travel from our wireless router, across the broadband network, across the Internet to the destination, and back to the wireless router ranged from 75.5 milliseconds (ms) to 117.1 ms. This is pretty good. If you see time delays of 500 ms or 1000 ms (1 second), that could point to a problem in either the broadband network or your broadband connection.

From the Diagnostics screen shown in Figure 12-2, try increasing the Times to Ping field to 20 or 100 and see how the test works. If you see packets being lost, or excessive delays (say, greater than about 500 ms), this could be causing slowdowns on your network. In this case, you may want to talk with your broadband provider about fixing the problem.



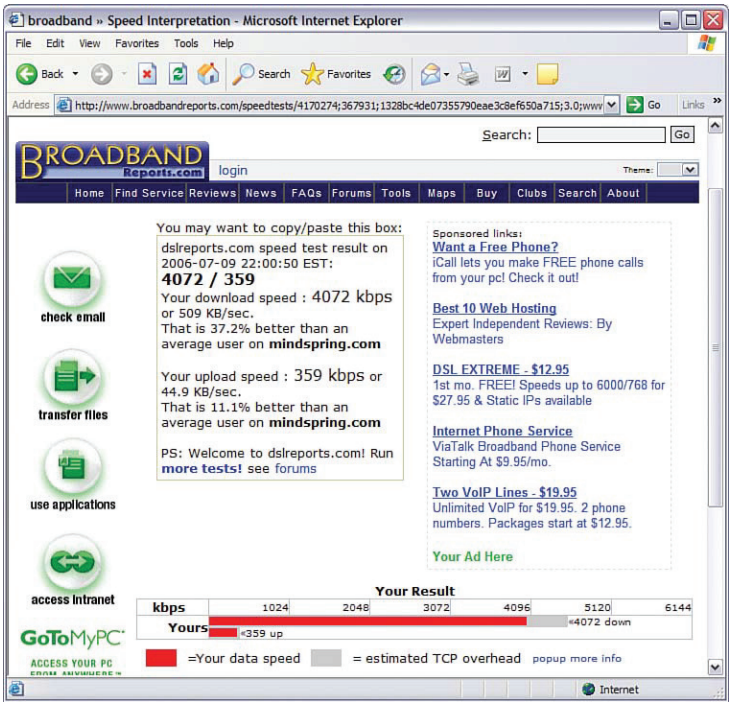
Note: You can ping any website you regularly use, although some website administrators disable responding to ping, so do not be alarmed if you do not get any response. Instead, try a few different websites. Also, if the website being pinged (or some Internet router on the path to the site) is having issues, you may see some ping failures that are not related to your provider. If you do see failures, try a few different ping sites to narrow down the issue. If you get the same issues with multiple sites, then you probably have an issue with your provider network.

Testing Your Broadband Speed

If the connection looks good (no packets being lost and short delay times), next check whether your broadband service is operating at the speed you have subscribed to. There are a few good online broadband speed tests you can do. We like the one at Broadbandreports.com: www.broadband-reports.com/speedtests/.

After you execute a speed test, results are displayed such as the example shown in Figure 12-4.

Figure 12-4 Broadband Speed Test Example



Here we can see that the uplink speed measured was 359 kbps, and the downlink speed measured was 4072 kbps (or 4 Mbps). This matches the broadband subscription in this case of 384 kbps/4 Mbps broadband cable service.

If you see speeds much slower than your subscription speed, you may want to talk to your broadband provider about fixing a problem, or possibly upgrading to a faster service. Make sure someone else in the house is not downloading a big file. You may also want to check your system for spyware, which could also slow down your system or connection.

Is the Wireless Network Too Slow?

After you verify that your broadband service is not creating a bottleneck, you are ready to take a look at the wireless network. As mentioned in the previous section, faster wireless networks do not always mean faster Internet access. But there are times when the wireless network can be an unexpected bottleneck.

Understanding Wireless Standards and Speeds

In Chapter 2, "Wireless Standards: What the Letters Mean," we talked about the wireless standards and the different speeds that they can provide. In Chapter 3, "Selecting the Right Wireless Standard for Your Network," we discussed how mixing different wireless NICs and wireless routers affects the overall network speed. Just to recap:

- 802.11b provides up to 11 Mbps
- 802.11g and 802.11a provide up to 54 Mbps
- 802.11n provides 100 Mbps and higher

One of the most common mistakes people make is that they upgrade their wireless router from 802.11b to 802.11g, increasing the network speed from 11 Mbps to 54 Mbps, but they do not upgrade the wireless NICs in the PCs and laptops. Because the NICs are still 802.11b, the network will continue to operate at 11 Mbps, and of course no noticeable increase in performance will be seen.



Note: The good news here is that, unlike encryption, which forces the whole network down to the lowest standard, the various network standards can work on the same network (assuming they are compatible). This means that if you buy a G-based router and you have one computer with a G NIC and one with a B NIC, both computers will work at the standard of their respective NIC. In other words, the computer with the G NIC will get G performance and the computer with the B NIC will get B performance.

In general, 802.11b wireless networks typically achieve around 5–6 Mbps of throughput speed. This is right on the edge of what is required to fully utilize the typical broadband connection (typically between 2 and 6 Mbps). Upgrading to 802.11g could very well provide a noticeable difference.

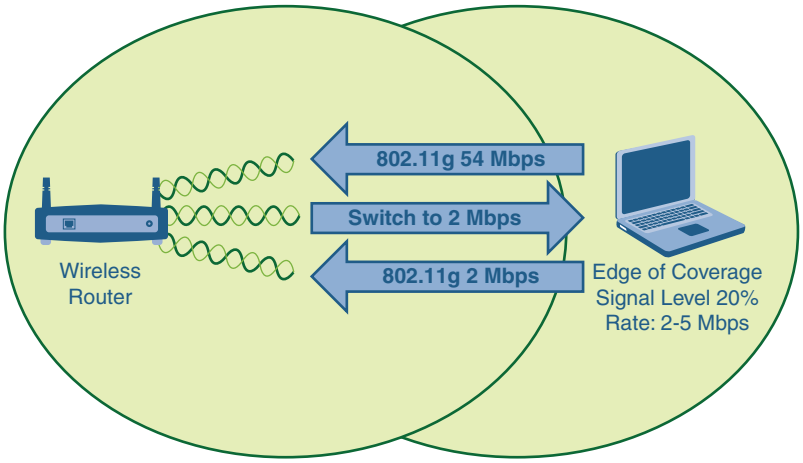
Upgrading to 802.11n may or may not provide a speed benefit. Speeds within the home network will certainly be accelerated to 100 Mbps and above, assuming that you upgraded both the wireless router and wireless NICs to 802.11n. However, the broadband service is still between 2 and 6 Mbps, so it is unlikely you will see any performance improvement for accessing the Internet.

The key point to understand is what you should expect from your wireless network. Do not fall into the trap of thinking that faster routers and faster wireless standards automatically mean faster Internet access.

Verifying Wireless Network Speed

One condition that can occur which dramatically slows down the speed of a wireless network is called *automatic speed negotiation.* An example of speed negotiation is shown in Figure 12-5.

Figure 12-5 Automatic Speed Negotiation



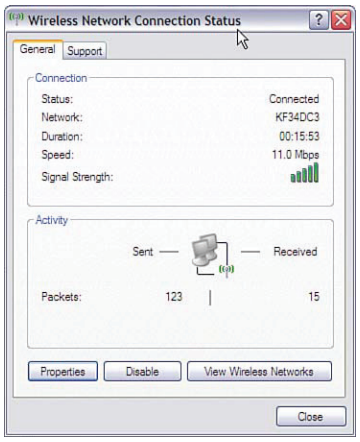
When the wireless router detects that a signal from a wireless NIC is weak or degraded, it "determines" that it is not possible to continue sending and receiving at the maximum speed supported by the standard. So the wireless router reduces the speed of the data between it and the wireless NIC. This automatic behavior is built in to all 802.11 wireless standards and cannot be disabled. But this is preferable to the alternative, which is for the wireless connection to simply drop or work intermittently.

As depicted in the example shown in Figure 12-5, suppose that we have an 802.11g wireless router and NIC. The NIC is on the edge of the coverage area and has a fairly weak signal. First, the NIC tries to transmit to the router at the maximum speed of 54 Mbps. The wireless router determines that there are many errors in the transmission, so it instructs the NIC to "back off" the speed, lowering it in this example to 2 Mbps. It determines that at this rate, transmissions have far fewer errors.

Automatic speed negotiation is a very nice feature that self-corrects many wireless network issues. However, if your wireless laptop is only getting 2 Mbps when you thought it was getting 54 Mbps, that's a problem.

How can you tell if this is occurring? Pretty easily, actually. Here is how. Suppose we have an 802.11g wireless router. Now suppose we have an 802.11b wireless NIC and we are using Windows Wireless Network Connection utility. Choose **Start > Connect To > Show All Connections**. Right-click the wireless NIC and choose **Status**. Figure 12-6 shows an example.

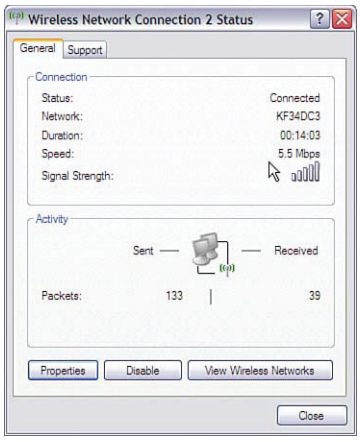
Figure 12-6 Checking Wireless Connection Speed with Windows XP–Good Signal



We can see from Figure 12-6 that we have pretty good signal strength, and we are getting the full rate that the wireless NIC is capable of. Note that even though the router supports up to 54 Mbps, the NIC shows it is connected at 11 Mbps, the maximum rate for an 802.11b NIC.

Suppose now that we take the same laptop with the 802.11b NIC to a room of the house with much weaker signal strength, as shown in Figure 12-7.

Figure 12-7 Checking Wireless Connection Speed with Windows XP–Poor Signal



We can see from Figure 12-7 that we have poor signal strength. As a consequence, the wireless router and NIC have auto-negotiated the data rate down to 5.5 Mbps, essentially 50 percent of the maximum NIC speed.

Next let's look at an 802.11g NIC where we are using the Linksys WLAN Monitor utility. Double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Link Information** tab and then the **More Information** subtab. Figure 12-8 shows an example.

Figure 12-8 Checking Wireless Connection Speed with Linksys WLAN Monitor–Good Signal



We can see from Figure 12-8 that we have good signal strength, and we are getting the full rate that the wireless NIC is capable of. Note that in this case both the router and NIC support up to 54 Mbps. The NIC shows it is connected at 54 Mbps, the maximum rate for an 802.11g NIC.

Suppose now we take the same laptop with the 802.11g NIC to a room of the house with much weaker signal strength, as shown in Figure 12-9.

Figure 12-9 Checking Wireless Connection Speed with Linksys WLAN Monitor–Poor Signal



We can see from Figure 12-9 that we have poor signal strength. As a consequence, the wireless router and NIC have auto-negotiated the data rate down to 18 Mbps, essentially only 33 percent of the maximum NIC speed.

Is the Wireless Network Signal Getting Degraded?

One of the reasons that you can experience either poor signal coverage or slower speeds even in good signal coverage is that the wireless signal is being degraded. This means that although the wireless router is sending out a clear and strong signal, something is causing the signal quality to diminish by the time it reaches your wireless NIC (and vice versa).

How can you have a strong signal but the connection is still poor quality? Think about being in a drive-through restaurant and placing your order at the speaker. Often the person taking your order is loud, but you cannot understand what they are saying because they sound muffled or are so close to the microphone that the sound is distorted.

The same is true of wireless networks. You may be able to see a very strong signal, but something may be causing the signal to be garbled, creating errors in the connection. Possible sources of signal degradation include

- Interference from nearby wireless routers
- Interference from other devices, including cordless phones, microwave ovens, Bluetooth headsets, and so on
- A malfunctioning wireless router or wireless NIC

Let's look at a couple of these issues, how you can recognize if one is occurring, and what you can do about it.

Interference from Other Wireless Routers

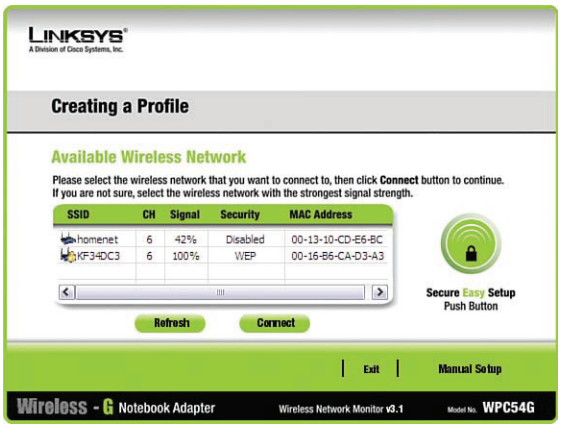
Every wireless router manufactured is set up to use a default wireless channel when you take it out of the box and plug it in. For Linksys routers designed for the 802.11b and 802.11g standards, it is channel 6. For Linksys routers designed for the newer 802.11n standard, the default channels are 5 and 7. (802.11n uses two channels in wideband mode. See Appendix B, "802.11n Wireless Channels," for more information.)

Every Linksys wireless router manufactured is set up to use these channels, unless you change them. This means that if you and your neighbor both buy a Linksys router (or any other router), there is a good chance you will be running your wireless networks on the same channel. If your houses are far enough apart, using the same channel is not necessarily a problem. However, if your houses or apartments are near each other, it can cause issues.

Checking for Conflicting Wireless Routers

So how can we see if other routers are using the same channel as ours? With Linksys WLAN Monitor it is pretty easy. Double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Site Survey** tab. Figure 12-10 shows an example.

Figure 12-10 Checking for Conflicting Wireless Routers with Linksys WLAN Monitor



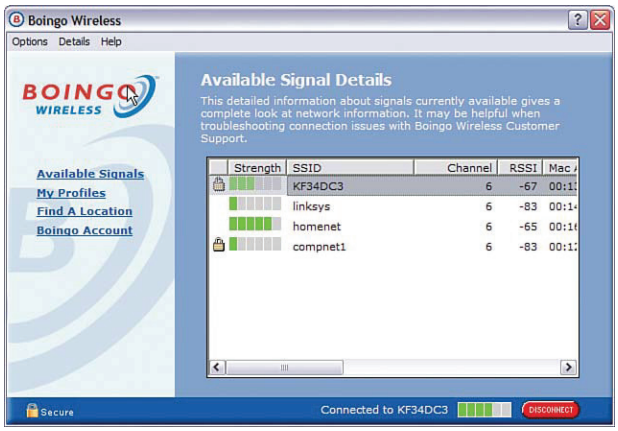
We can see from this example that there are two wireless network signals within range of the wireless NIC, with SSIDs KF34DC3 and homenet. KF34DC3 is our wireless network, so homenet must be the neighbor's. Both are operating on channel 6, the default channel.

If you are using Windows Wireless Network Connection utility to manage your wireless connections, checking for conflicts is not easy, because XP does not display the channel currently connected or the channel of other wireless networks. In this case, you need to add another wireless connection manager, such as Boingo, that can provide the information.

Boingo Wireless offers a free downloadable wireless connection manager that you can use as an alternative to the Windows Wireless Network Connection utility or Linksys WLAN Monitor to manage your wireless profiles. The free program is available here: www.boingo.com/download.html.

After you download and install the program, double-click the icon on the desktop to start it or choose **Start > Programs > Boingo > Boingo** to launch the application. Choose **Details > Available Signal Details**. An example is shown in Figure 12-11.

Figure 12-11 Checking for Conflicting Wireless Routers with Boingo



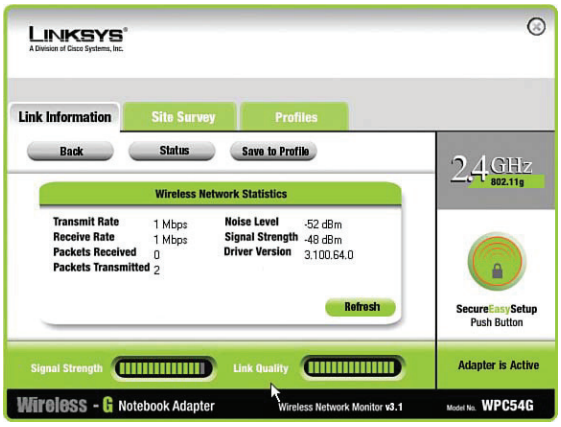
We can see from this example that there are four wireless signals with SSIDs: KF34DC3, homenet, linksys, and compnet1. The linksys and compnet1 signals are weak, so they should not be an issue. However, you can see that the homenet signal is strong, even stronger than our own wireless network (KF34DC3). All four are using channel 6, the default wireless channel.

Determining Whether the Conflicting Wireless Router Is Causing an Issue

Seeing that there is another wireless router using the same channel is one thing, but is it causing a problem? It's a little tough to answer. There are some telltale signs you can look for, though.

If you are using Linksys WLAN Monitor, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Link Information** tab and then click the **More Information** subtab. Figure 12-12 shows an example.

Figure 12-12 Detecting Signal Degradation with Linksys WLAN Monitor



Here, we see strong signal strength, but the data rate is only 1 Mbps. In this situation (with an 802.11g wireless router and NIC), we should be able to have a data rate of 54 Mbps. The reduced rate in spite of a strong signal strength could indicate that the other wireless router operating on the same channel is causing signal degradation.

If you are using Windows XP, you may need to use Boingo again. Double-click the Boingo icon on the desktop or choose **Start > Programs > Boingo > Boingo** to launch the application. Choose **Details > Signal Performance**.

Wait a few minutes and let Boingo monitor the wireless signal for a bit. Boingo will produce a nice graph of the wireless signal level. What we would like to see is a consistent wireless signal like that shown in Figure 12-13.

Now look at the example shown in Figure 12-14.

Figure 12-13 Determining a Steady Wireless Signal with Boingo

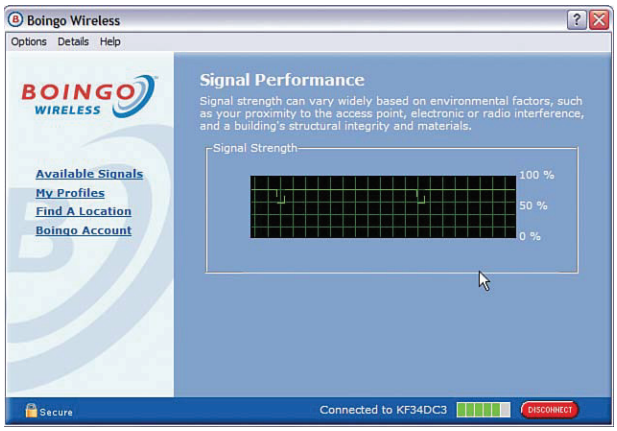
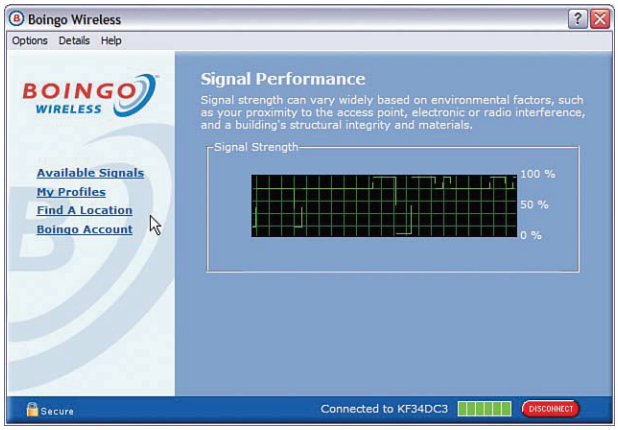


Figure 12-14 Detecting Signal Degradation with Boingo



Here you can see that the wireless signal is all over the place, sometimes high and sometimes low, not very consistent. This could be an indication that the other wireless network operating on the same channel is causing a problem.

Correcting a Conflicting Wireless Router Situation

If you detect a potential conflicting wireless router and suspect it may be causing your network to suffer, the best fix is to try changing your wireless network to operate on a different channel.

Follow the procedure described in Chapter 11, "Troubleshooting: I Can Connect Sometimes," to change the wireless channel and then conduct a follow-up wireless survey in your house to confirm that it had a positive effect.

Choose a wireless channel that you do not see another wireless router using. Also see Chapter 11 for more discussion on available wireless channels you can choose from.

Interference from Cordless Phones and Other Devices

As we have mentioned a few times now, cordless phones can be another source of problems for your wireless network. How do you know if your cordless phone system may be incompatible with your home wireless network? The first step is to understand which wireless radio frequency bands each device uses. Table 12-1 shows a very easy rule of thumb.

Table 12-1 Wireless Network and Cordless Phone System Compatibility

	900-MHz Cordless Phones	2.4-GHz Cordless Phones	5-GHz Cordless Phones
802.11b	No problem	Potential problem	No problem
802.11g	No problem	Potential problem	No problem
802.11a	No problem	No problem	Potential problem
802.11n	No problem	Potential problem	No problem

The green areas of the table indicate that there is not a possibility for interference between the type of wireless network and cordless phone system you have. Areas in yellow indicate that there could be an issue—not always, but possibly.

In general, if you have an 802.11b, 802.11g, or 802.11n wireless network, try to buy 5-GHz cordless phones.



Note: We mention cordless phones through this section, but baby monitors, garage door openers, walkie-talkies, and other wireless types of devices can cause the same problem. The actions you take will be the same, although you have a little less control when it comes to testing the devices for interference (especially if it's your neighbor's garage door opener).

Determining Whether the Conflicting Cordless Phone Is Causing an Issue

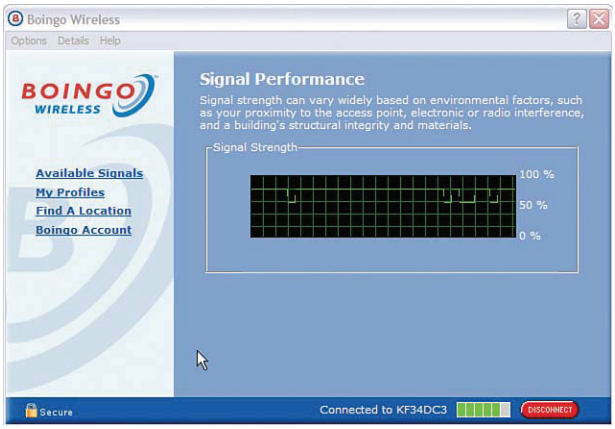
If you do think you have the possibility for a conflict between the wireless network and your cordless phone, how can you tell if it's causing an issue? One simple way is to unplug the cordless phone for a while and see if the issue goes away.

Another way is to try detecting the issue using Boingo. Suppose in this example that we have an 802.11g network and a 2.4-GHz cordless phone system.

Double-click the Boingo icon on the desktop or choose **Start > Programs > Boingo > Boingo** to launch the application. Choose **Details > Signal Performance**.

Wait a few minutes and let Boingo monitor the wireless signal for a bit. Boingo will produce a nice graph of the wireless signal level, like the example shown in Figure 12-15.

Figure 12-15 Detecting Signal Degradation with Boingo–During a Call

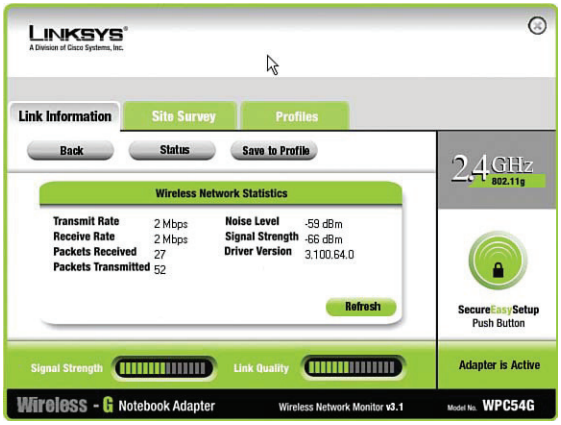


You can see that the wireless signal is quite consistent. Now place a call with your cordless phone. If you look on the right side of the signal chart, you can see that while we made a call, the signal was degraded a bit. The degradation is not terrible, but it is there. It may or may not be causing an issue; it is difficult to say.

To further investigate the issue, we can check whether we see a slowdown in the data rate of the connection. Place a call again using the cordless phone.

If you are using the Linksys WLAN Monitor, double-click the icon on the desktop to launch the utility or choose **Start > Programs > Linksys Wireless Card > WLAN Monitor**. Click the **Link Information** tab. Figure 12-16 shows an example.

Figure 12-16 Checking the Wireless Data Rate with Linksys WLAN Monitor–Phone On



We can see that despite having a pretty good signal level, the data rate has dropped to 2 Mbps during the duration of the call.

Now hang up the phone. As shown in Figure 12-17, the wireless data signal has gone up significantly, and the wireless data rate is also increased back up to 54 Mbps.

Figure 12-17 Checking the Wireless Data Rate with Linksys WLAN Monitor–Phone Off



If you see a degradation of either the signal level or wireless data rate, or both, when you place a test call with the cordless phone, you probably have a conflict. Also keep in mind that interference works both ways, so your router can degrade the sound quality of your cordless phone.

Correcting a Conflicting Cordless Phone Issue

If you detect a potential conflict between your wireless network and your cordless phone system, you have several options:

- Move the base and handset of the cordless phone system well away from the wireless router and where you will use the wireless computers.
- Change the channel of the wireless router (see Chapter 11).
- Upgrade your cordless phone system to a type that does not conflict with your wireless network (see Table 12-1).
- Upgrade your wireless network to a type that does not conflict with your cordless phone system (see Table 12-1).

Whichever change you make, follow the procedures described in Chapter 11 and then conduct a follow-up wireless survey in your house to confirm that it had a positive effect.

You can try the same experiment outlined in this section with your microwave, Bluetooth headset, and other devices that may conflict with your wireless network. Just check the signal level and wireless data rate with the device off and then check it again with the device in use.

Summary

Signal degradation can occur with your wireless network, causing slowdowns or difficulty making connections at all. The most common causes are a nearby conflicting wireless router or another device in your home, such as a cordless phone, that causes interference.

Before assuming the wireless network is causing a slowdown, make sure your broadband service is performing the way your subscription says it should. Also make sure your perceptions are accurate—are you making a bad assumption that upgrading to a faster router will give you faster Internet access?

If you determine that your wireless network is experiencing some issues due to interference, take some steps to correct the problem, using the wireless survey procedure from Chapter 11.

Where to Go for More Information

Read Bradley Mitchell's article titled "Top 6 Reasons Why WiFi Network Connections Drop" at About.com: http://wireless.about.com/od/wifihomenetworking/tp/connectiondrop.htm.

Bradley Mitchell has also written an article titled "Change the WiFi Channel Number to Avoid Interference," also available at About.com: http://compnetworking.about.com/od/wifihomenetworking/qt/wifichannel.htm.

Joseph Moran has a tutorial at Wi-Fi Planet titled "Wireless Home Networking, Part V—Interference and Range Extension": www.wi-fiplanet.com/tutorials/article.php/1497111.

This page intentionally left blank



PART V

PART V

Bells and Whistles

Chapter 13 Wireless Video and Entertainment

Chapter 14 Wireless to Go

Chapter 15 The Future of Wireless Networking

Whew. Now that we've designed, built, and debugged our wireless network, it's time to do some cool stuff with it. Let the good times roll.

Chapter 13, "Wireless Video and Entertainment," shows you how to use your home wireless network for entertainment. We cover how to add a wireless video camera to the network. Then we show you how to network your video game console (like an XBox) and a Digital Video Recorder (DVR).

Chapter 14, "Wireless to Go," shows you how to take wireless networking with you when you travel. Wireless networks are becoming about as common as electric lights. We cover how to use wireless hotspots when you travel, how to set up your own portable hotspot, and how to give your guests access to your wireless home network.

We wrap up Part V with Chapter 15, "The Future of Wireless Networking," which gives a glimpse into what we think is the future of wireless home networking. We don't have a crystal ball or anything, we just give our best guesses. The technology is moving quickly, so we will probably look foolish in five years, but what the heck. We love to give these little glimpses into the future. It at least gives the appearance that we know what we are talking about.

CHAPTER 13

Wireless Video and Entertainment

Now that we have a well-functioning, secure wireless network, what do you do with it? Well, lots. You can of course use it to surf the Internet and read your e-mail from the back deck. But there is a lot more you can do.

One general category is wireless video and entertainment, including wireless video cameras, media gateways that can display pictures and send music to your TV entertainment system, online gaming, networking your digital video recorder (DVR), and wireless digital jukeboxes.

We cannot begin to cover all the things you can do with your wireless network here, but let's take three pretty cool things to do and see how you would set up and use them:

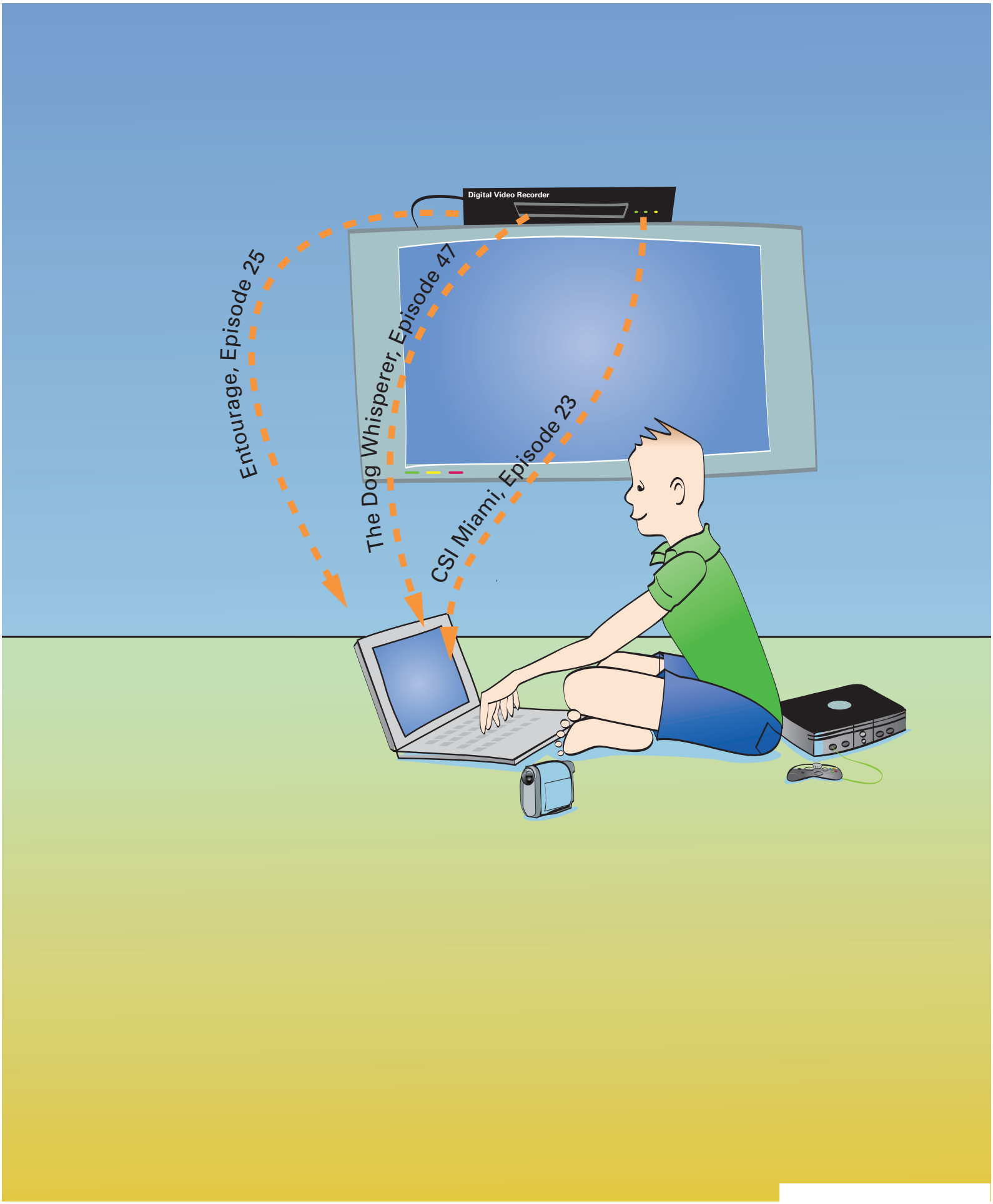
- Wireless video cameras
- Online gaming
- Networking a DVR, like a TiVo

The network capacity (or bandwidth) within your home network is much greater (three times or more) than the fastest upload/download speeds you will get from your high-speed connection to the Internet. All this excess capacity exists on your home wireless network because many in-home applications—including the three described in this chapter—typically require more bandwidth than is required for Internet browsing or e-mail. This chapter shows you how to set up these three options in your network.

Wireless Video Cameras

Once limited to very expensive closed-circuit television (CCTV) systems, video cameras for fun or for surveillance are now pretty affordable. If you already have a wireless network in your home, a decent wireless video surveillance system costs you only $100 or so. (We say "only" because a basic CCTV system costs more than $1000.)

Wireless video cameras have all sorts of practical uses, including home surveillance for security and nanny cams.


Digital Video Recorder
Entourage, Episode 25
The Dog Whisperer, Episode 47
CSI Miami, Episode 23

Finding Uses for Wireless Video Cameras

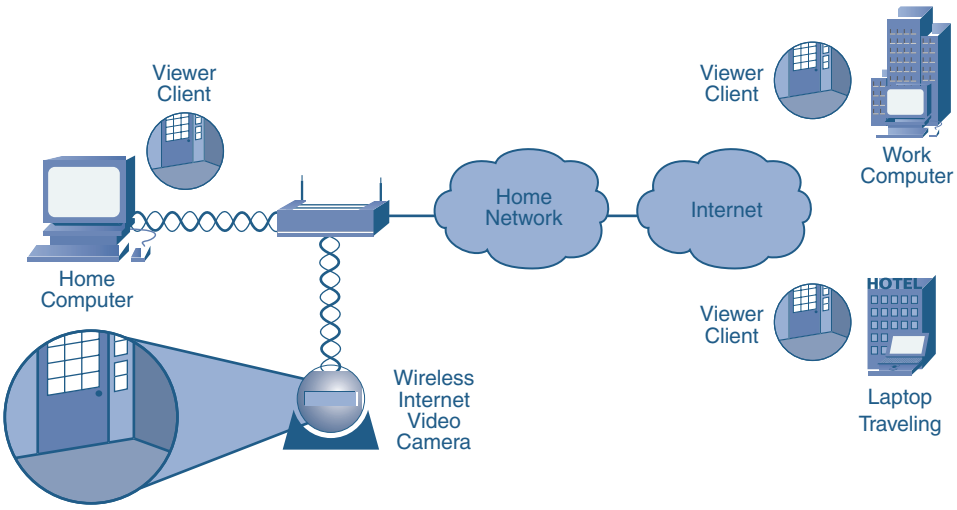
Video cameras that attach to computers are very common, usually used for communicating with other people that have similar video cameras. Also popular recently have been very inexpensive wireless cameras that can be placed anywhere in your house.

The ability to use either of these video cameras for live surveillance while you are not at home is limited. However, newer products like the Linksys wireless Internet video cameras have several distinct advantages:

- No computer is required for them to operate, so they can be located anywhere in your house (or outside, for that matter) where there is an electrical outlet.
- Images from the camera are viewable with any computer from inside your house, or from anywhere outside your house where there is Internet service.

In Figure 13-1, we placed a wireless Internet video camera in a house with a view of the front door.

Figure 13-1 Home Surveillance Using a Wireless Internet Video Camera



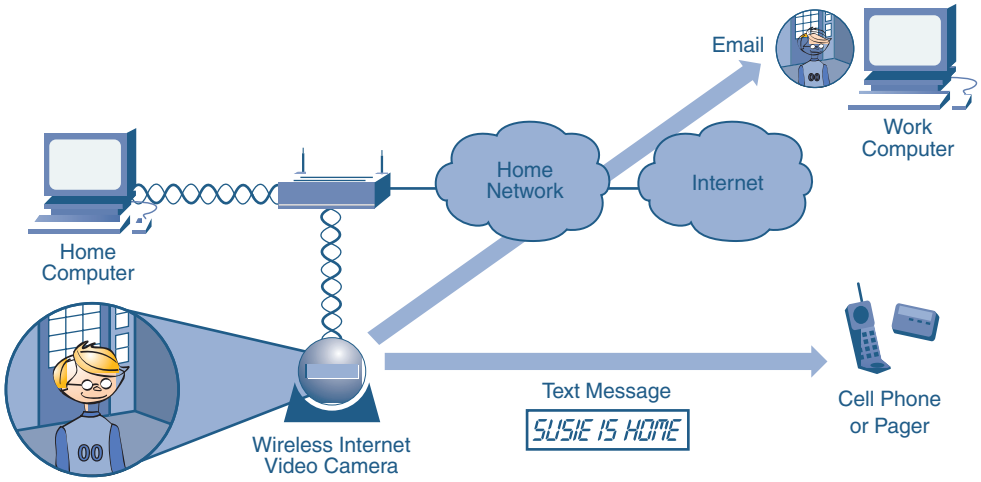
Now, we can use a viewer client to view the real-time video feed. So from upstairs, we could check who is at the front door. We could also use the viewer client on a computer at work to periodically check the residence or to see that the kids got home at the expected time from school. In a similar way, you could even use your laptop to check on the house while traveling on business.

To avoid the need for constant surveillance, you can set up the camera to act as an automated sentry, and notify you only when there is something worth seeing.

You can program the camera to send a signal to a pager, cell phone, or e-mail account to notify you if motion has been detected. You can even have the camera send you a video clip that it captures of the event.

In Figure 13-2, when little Susie arrives home, the camera detects the motion of her entering the front door. It then can send a notification e-mail (including a video clip) so you can verify that it is her. Or the camera could send a text message to your cell phone (via Short Message Service [SMS]) or to your pager (alphanumeric) with a message such as "Susie is home."

Figure 13-2 Automatic Notification of a Child Arriving Home



We will walk through how to set up your camera for viewing and as a motion detector later in the chapter. First, we need to pick a camera. Linksys offers a few different camera products. Table 13-1 shows the wireless video camera products from Linksys that we recommend.

Table 13-1 Linksys Wireless Internet Video Cameras

Model	Capability	Wireless Standard	Wireless Encryption Supported
WVC54G	Audio, video, and motion detection	802.11g Also works with 802.11b, 802.11n	64-bit WEP 128-bit WEP WPA-PSK
WVC54GC	Audio, video, and motion detection Compact size	802.11g Also works with 802.11b, 802.11n	64-bit WEP 128-bit WEP
WVC11B	Video and motion detection	802.11b Also works with 802.11g, 802.11n	64-bit WEP 128-bit WEP

The next few sections go through the steps to install a wireless Internet video camera on your home network. Here's an overview of the steps we will go through:

- Connecting the video camera to your wireless network
- Determining who can access the video camera

- Viewing video from within your house
- Viewing video over the Internet
- Using the video camera as a motion detector

Connecting the Video Camera to Your Wireless Network

The first step is to set up the wireless Internet video camera so that it can communicate with the wireless home network. Similar to the wireless NICs we added in Chapters 8, "Wireless NIC Setup," and 9, "Wireless Security Setup," you must tell the video camera how to join your wireless network.

For almost every device or computer we add to the network, it's advantageous to let the wireless router choose and manage the IP addresses for the devices on your network. IP addresses can be assigned as needed, and the actual addresses assigned are not important to us. However, for the wireless Internet video camera, it will be necessary for us to assign a fixed IP address, so that we may access the camera images via the Internet.

The steps to install the wireless Internet video camera are as follows (the example shown is for the Linksys WVC11B Wireless-B Internet Video Camera):

Step 1 Connect the Linksys wireless Internet video camera to the wireless router using an Ethernet cable (ordinary, not crossover), and plug in the power adapter. The LAN LED light on the front should light up.

Step 2 Put the CD that came with the Linksys video camera into a computer on the network (one that is wired is preferred). The Setup Wizard should start automatically. If not, use My Computer to browse the CD and double-click **Setup.exe**. Click the **Setup** button.

Step 3 The Setup Wizard instructs you to connect the video camera to the wireless router. Click **Next**.

Step 4 The Setup Wizard searches for the new video camera on the network (see Figure 13-3). Click **Next**. If it does not locate the camera, try clicking **Search Again**. If it still does not show up, check your cabling. Make sure the LAN LED light is lit on the video camera.

Figure 13-3 Setup Wizard Searches for and Finds the New Video Camera



Step 5 You are prompted for the camera administrator name and password. Enter **admin** for both the Administrator Name and Administrator Password fields and click **OK**.

Step 6 Enter a device name (this is something you can just make up) for the video camera (we used Camera_1 in Figure 13-4). Enter the time zone, date, and time. Click **Next**.

Figure 13-4 Enter the Basic Camera Setup Settings



Step 7 Click **Static IP Address** and then click **Next**.



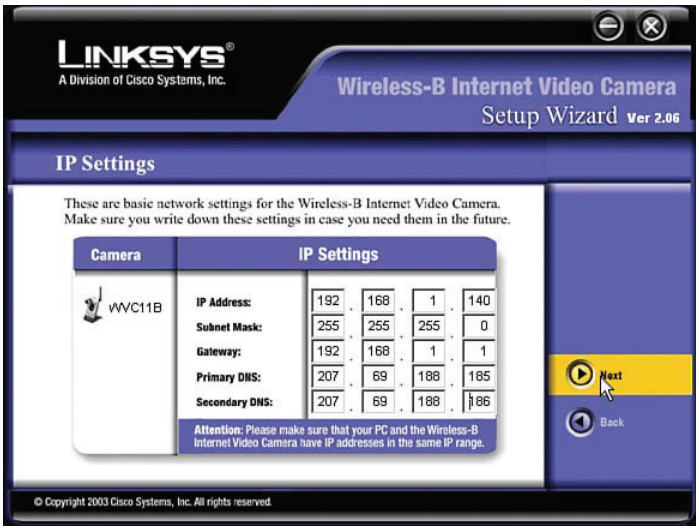
Note: The Setup Wizard recommends choosing **Automatic Configuration—DHCP** if you are connecting the camera to a router. However, if you want to access the camera over the Internet, you need a fixed (static) IP address.

Step 8 Enter an IP address that is unlikely to be assigned on your network by the wireless router (for example, 192.168.1.140). (See Figure 13-5.)

The subnet mask will be 255.255.255.0. The gateway will be 192.168.1.1. For the primary DNS and secondary DNS, enter the addresses listed on the sheet of paper or e-mail you received from your ISP when you subscribed. If you can't find them, access the wireless router using an Internet browser and click the **Status** tab.

After entering all the settings, click **Next**.

Figure 13-5 Configure the IP Address Settings





Note: The IP address you choose needs to be in the range of IP addresses for your home network. In Chapter 7, "Wireless Router Setup," we set up the router to use the address range 192.168.1.2 through 192.168.1.254 for our home network (.0, .1, and .255 are reserved). In addition, we set up the router to dynamically assign IP addresses in the range 192.168.1.100 through 192.168.1.149 to computers and devices requesting an address.

The IP address just needs to be unique on the network and within one of these ranges. We chose 192.168.1.140 for this example. Whatever address you choose, write it down, because this will be the address needed when accessing the camera. If you forget the address, you probably have to do a factory reset and start over.

Step 9 The next wizard page asks if your network is ad hoc or infrastructure (meaning based on a wireless router). Select **Infrastructure** and click **Next**.

Step 10 Enter the SSID for your wireless network (see Figure 13-6). For this particular example, the home network is using an SSID of J59wgh21MX. Click **Next**.

Step 11 Set the wireless security setting to **WEP 128 Bit Keys** (or the encryption you are using), as shown in Figure 13-7. Enter the WEP passphrase for your wireless network. In this example, the WEP passphrase is 64Gx3prY19fk2. Click **Next**.

Figure 13-6 Enter the SSID for Your Wireless Network

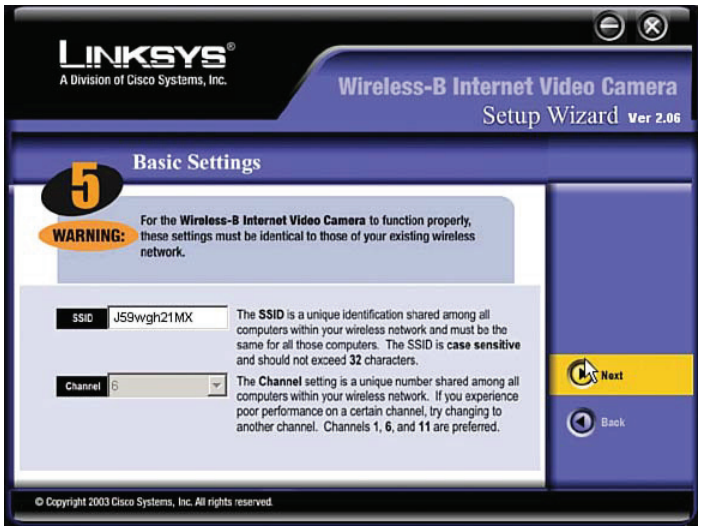
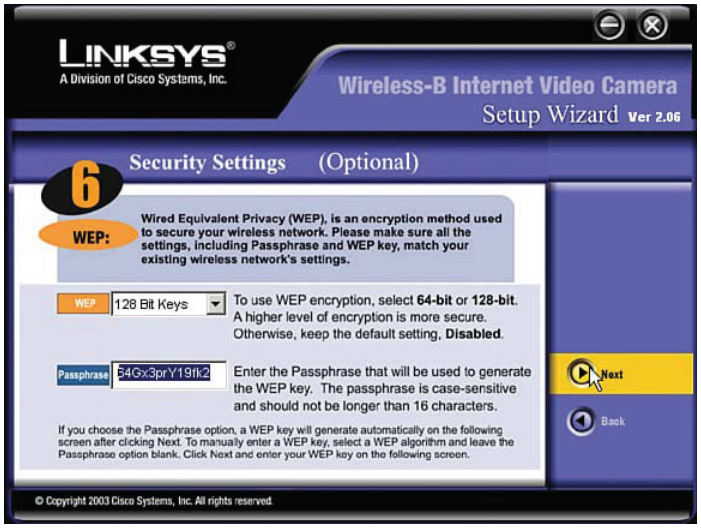


Figure 13-7 Enter the Wireless Security Settings

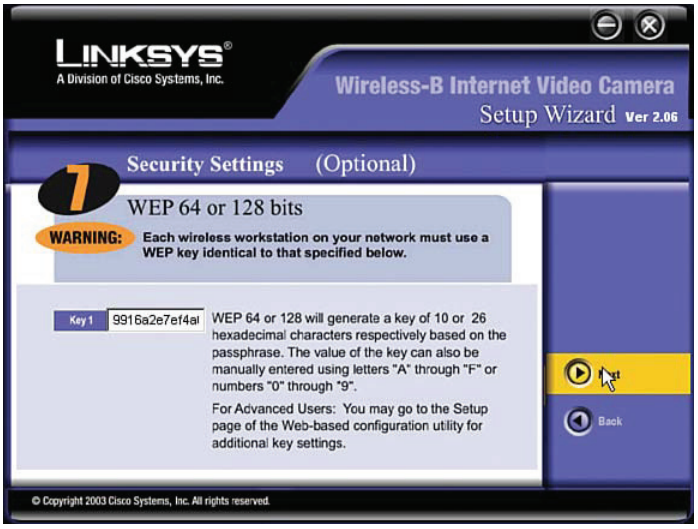


Step 12 The camera generates a WEP key from the WEP passphrase you entered (if it is a Linksys product, that is). Check the WEP key to ensure it matches the key being used on the wireless router (see Figure 13-8). Do not modify the key! Click **Next**.



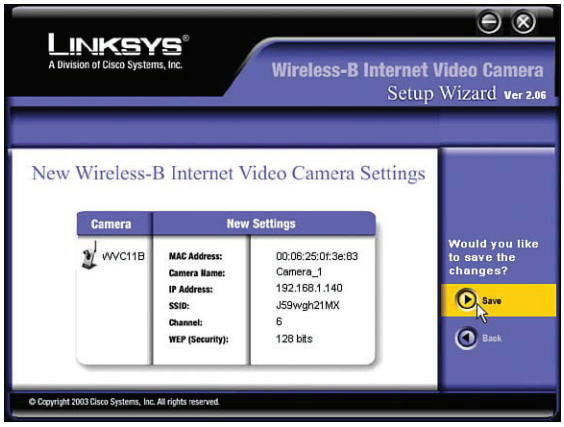
Note: If the two keys do not match, modify the key value to match what is being used on the wireless router. Normally, the keys will match as long as the wireless video camera and wireless router are both Linksys products.

Figure 13-8 Confirm the Generated WEP Key



Step 13 The Setup Wizard then displays a summary of the new settings. (See Figure 13-9.) Click **Save**. Click **OK** on the double-confirmation dialog box that appears next.

Figure 13-9 Settings Confirmation



Step 14 You're all done. Leave the Setup Wizard for now. We have to come back to it later.

Unplug the Ethernet cable from the video camera, power it off, and then power it back on. After you complete these steps, the WLAN LED indicator light on the front of the wireless Internet video camera should be lit. You can now unplug the video camera and move it to the location of your choice.



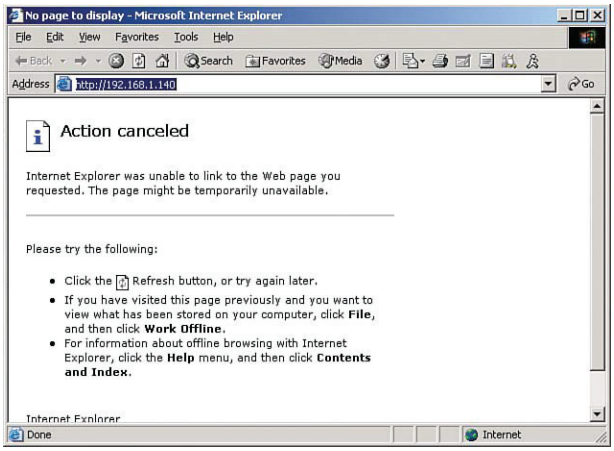
Note: By the way, if you have MAC address filtering turned on in your wireless network as a security feature, you will need to add the wireless video camera MAC address to the list of devices permitted to join your wireless network. This is true of any device you add to the wireless network. Most people remember to add laptops and computers, but they often forget to add other devices.

Determining Who Can Access the Video Camera

Now that the wireless Internet video camera is communicating properly with the wireless network, you need to perform a few steps to finish setting up the security for the camera. You want to change the administrator password for sure. You also may want to restrict who can access the camera, essentially who can view the image. Here is how:

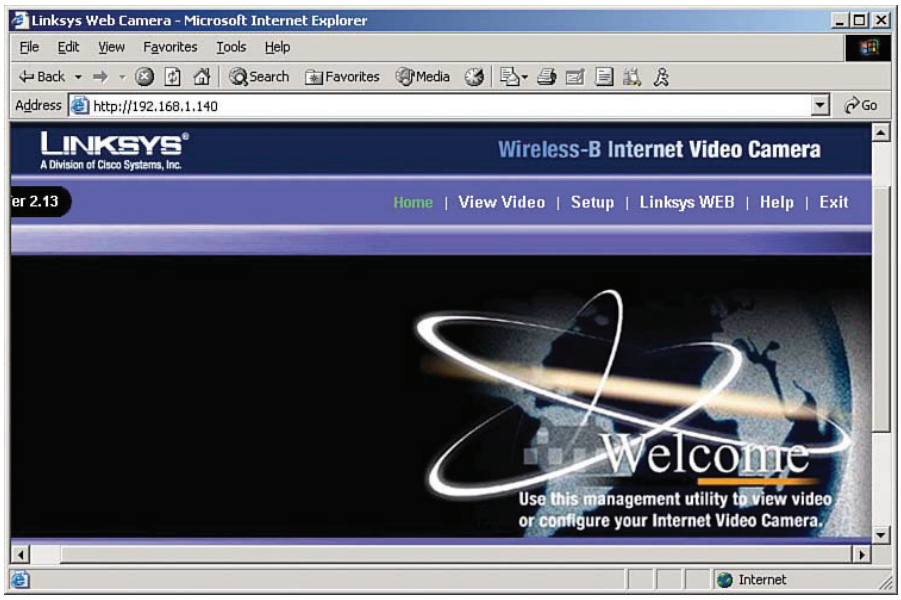
Step 1 Open your Internet browser and type in the IP address that you selected for the video camera (for example, 192.168.1.140, as shown in Figure 13-10). Press **Enter**.

Figure 13-10 Access the Video Camera with Your Internet Browser



Step 2 The main menu for the video camera should appear (see Figure 13-11). If it does not appear, go back to the installation steps in the previous section.

Figure 13-11 Video Camera Main Menu



Step 3 Click the **Setup** option and then click **Password**. Enter a new password on both the **Password** and **Verify Password** lines. Write it down in the notebook you have been keeping for your network. Click **Apply**.

Step 4 Immediately, the video camera will reauthenticate (you will be logged out and will have to log back in again). Enter **admin** for the user ID and the new password you created. Click **OK**.

Step 5 Click **Users**. It is possible to set up video camera users who have only viewing privileges and not the authority to modify the video camera itself (see Figure 13-12). Never give out the master administration password. Click **Add**.

Step 6 Enter a username and corresponding password (see Figure 13-13). Do *not* use the same password as the administrator. Click **Apply**. Repeat this step for as many user accounts as you want to add. Click **Close** when you're finished.



Note: The usernames and passwords here are different from your Windows usernames. This is a list of users who are going to have access to your video camera and will have to log in to the camera itself. This prevents people from viewing your camera without your permission.

Figure 13-12 List of Authorized Camera Users

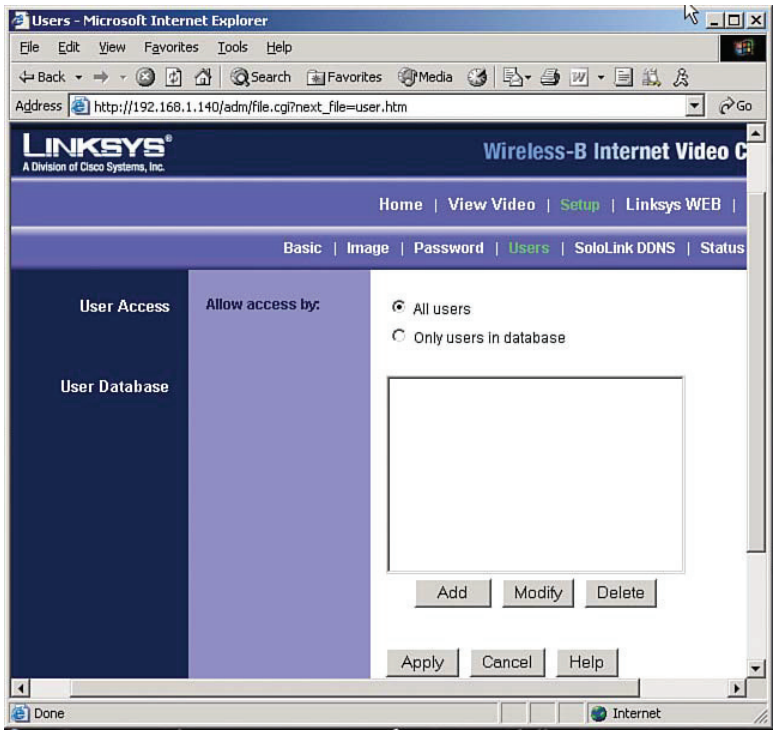
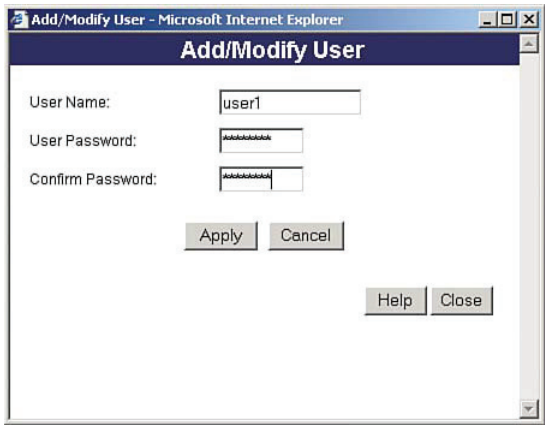
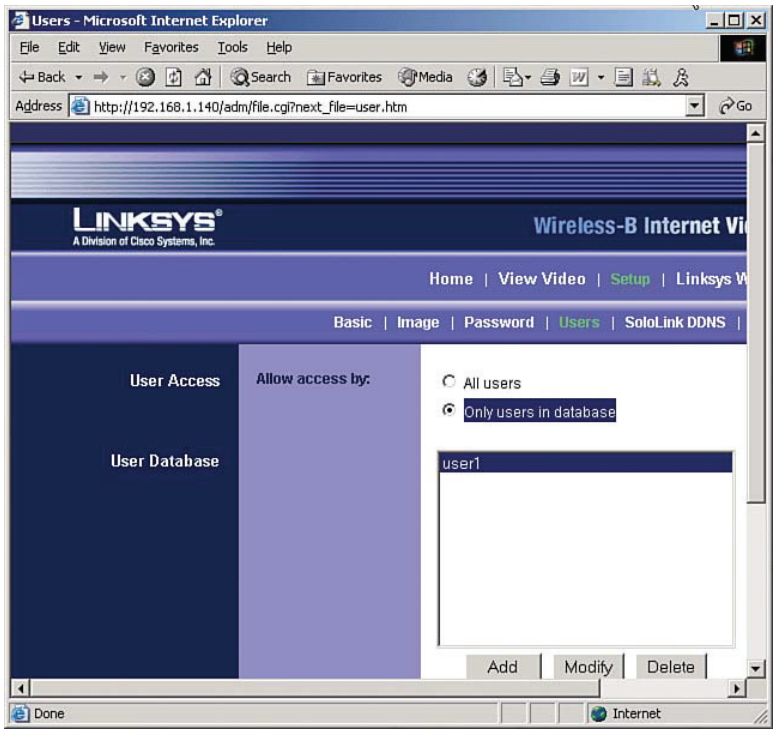


Figure 13-13 Add New Users with Viewing Privileges



Step 7 THIS STEP IS CRITICAL! If you do not complete it, anyone who tries to access your video camera over the Internet will be granted access. Click **Only Users in Database** (see Figure 13-14). Click **Apply**.

Figure 13-14 Restrict the Video Camera to Authorized Users Only



Now the wireless Internet video camera is installed, set up, and ready for use.

Viewing Video from Within Your House

Now that the wireless Internet video camera is set up completely, we can start using it to view video images. There are two ways to view video:

- **Internet browser**—This method is more involved than using the Viewer Client, but you can view video using any computer with an Internet browser, which is useful when trying to check your camera from a friend's house or from a public computer. (Extra steps are required for viewing the camera from outside your home network. See the section "Viewing Video over the Internet," later in the chapter.) With the Internet browser, you can access the other administrative features of the camera, such as setting up motion detection.
- **Viewer Client**—The Viewer Client is software provided on the CD that came with the camera. It is easier to use than the Internet browser and offers a recording feature. However, the Client must be installed on every computer you wish to view the video feed from. The Linksys Viewer Client software works only on computers running Windows XP or 2000, not Windows 98.

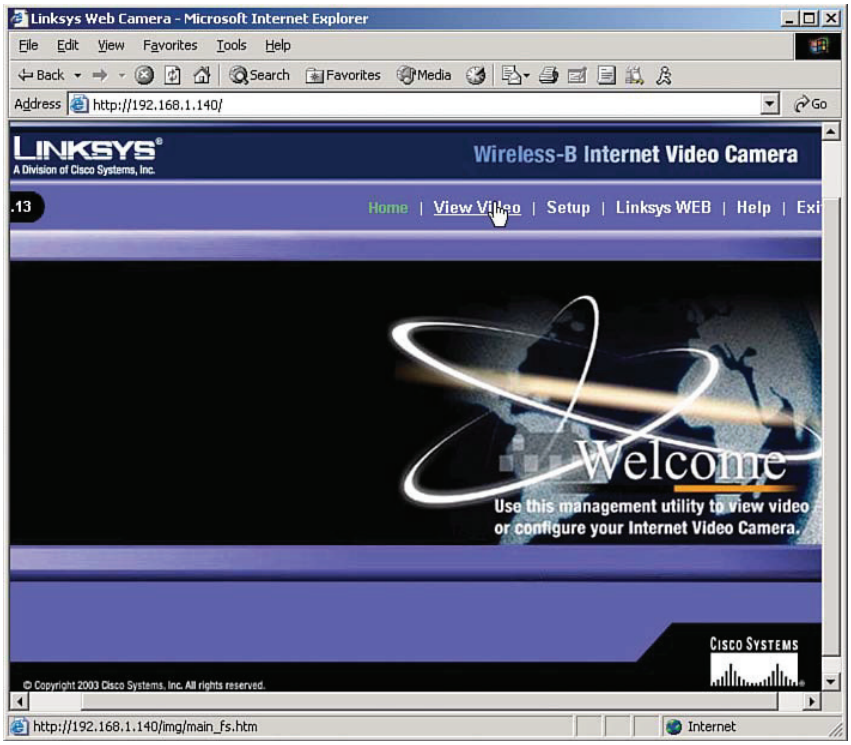
Let's look at an example of viewing the video image using an Internet browser:

Step 1 Point an Internet browser to the video camera by entering the IP address (for example, http://192.168.1.140) in the Address field of the browser, as shown in Figure 13-15, and press **Enter**. The main camera dialog box appears. Click **View Video**.



Note: For this example, Microsoft Internet Explorer is assumed to be the Internet browser. Other browsers such as Netscape or Firefox may require additional plug-ins to use them.

Figure 13-15 Access the Camera Using an Internet Browser



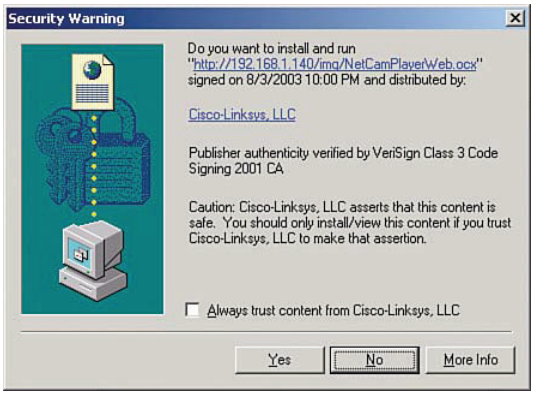
Step 2 Enter a username and password that you created with viewing privileges (see Figure 13-16).

Figure 13-16 Enter the Username and Password of the Viewer Account



Step 3 The first time you want to view video with your browser, a special "plug-in" is downloaded automatically and installed into the Internet browser. You'll see the dialog box shown in Figure 13-17. Click **Yes**.

Figure 13-17 Plug-In Is Automatically Downloaded the First Time



Step 4 It works! (See Figure 13-18.) Isn't she beautiful? Now, you're all done.

Figure 13-18 Viewing a Video Image



At this point, you can do a couple of things to save yourself some time in the future. Add the Video Viewer to your Favorites list by bookmarking the URL in your Internet browser. The next time you use the Internet browser, you can then simply go to the Video Viewer in the Favorites list instead of remembering the IP address.

You also may want to create a shortcut on the Windows Desktop. While still in the Viewer mode, click **File > Send To > Desktop Shortcut** in the Internet browser menu. This puts an icon on the desktop of your computer that you can simply double-click to jump into the Video Viewer mode.

Viewing Video over the Internet

Viewing video from within your home network (which we did in the previous section) is fairly straightforward. Viewing video over the Internet is a bit trickier. First, your home network is set up for access from inside-out, not from outside-in. Second, the actual IP address of your broadband service most likely changes over time (which is normal). It's a little like trying to deliver mail to someone whose address changes each week. Fortunately, there are a couple slick solutions to these potential problems.

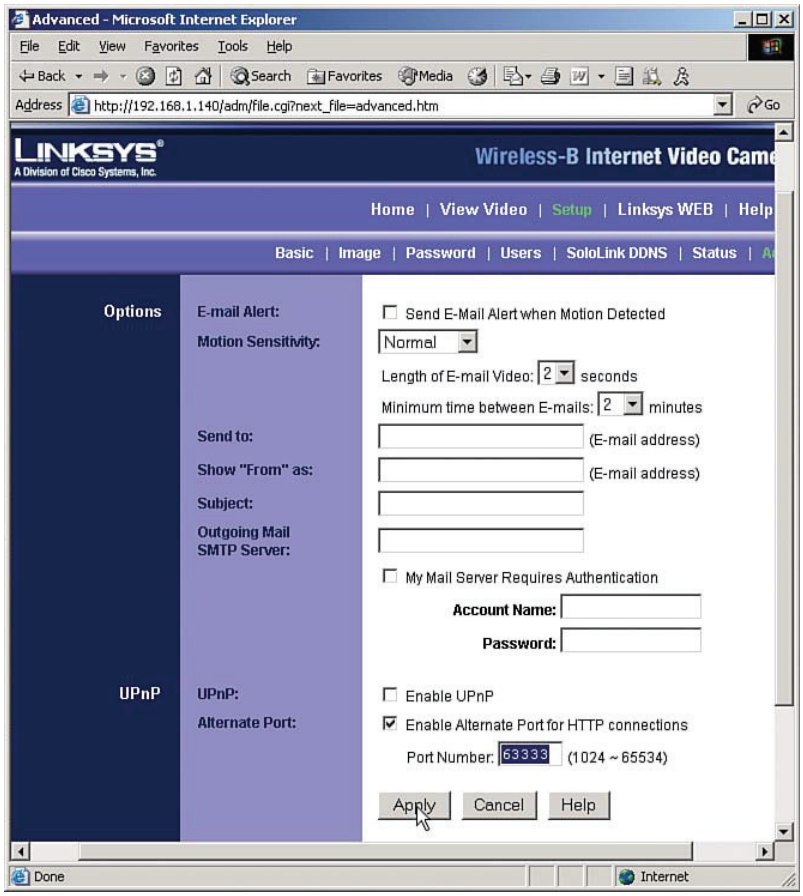
First, let's tackle the inside-out/outside-in problem. How do you provide outside-in access to the video camera without compromising the security of your home network? Further, how do you reach the video camera, whose IP address on the home network is unknown to you? From the Internet's perspective, the video camera's IP address of 192.168.1.140 is not accessible. Remember, this is by design from a security perspective.

Setting Up the Wireless Router for Internet Camera Viewing

The trick to being able to access the video camera over the Internet is to use a feature on the Linksys wireless router called *port forwarding*. Using this feature, the wireless router can recognize incoming attempts to access the video camera, and can forward those requests directly to the video camera. Here's how to set up port forwarding on the wireless router:

Step 1 Point an Internet browser to the video camera by entering the IP address (for example, http://192.168.1.140). When prompted, enter **admin** for the user ID and the administrator password. Click **Setup** and then **Advanced**. Check the **Enable Alternate Port for HTTP Connections** check box (see Figure 13-19). Choose an IP port number that you want the camera to use (for example, 63333). Write it down. Click **Apply**.

Figure 13-19 Assign the Video Camera an IP Port Number



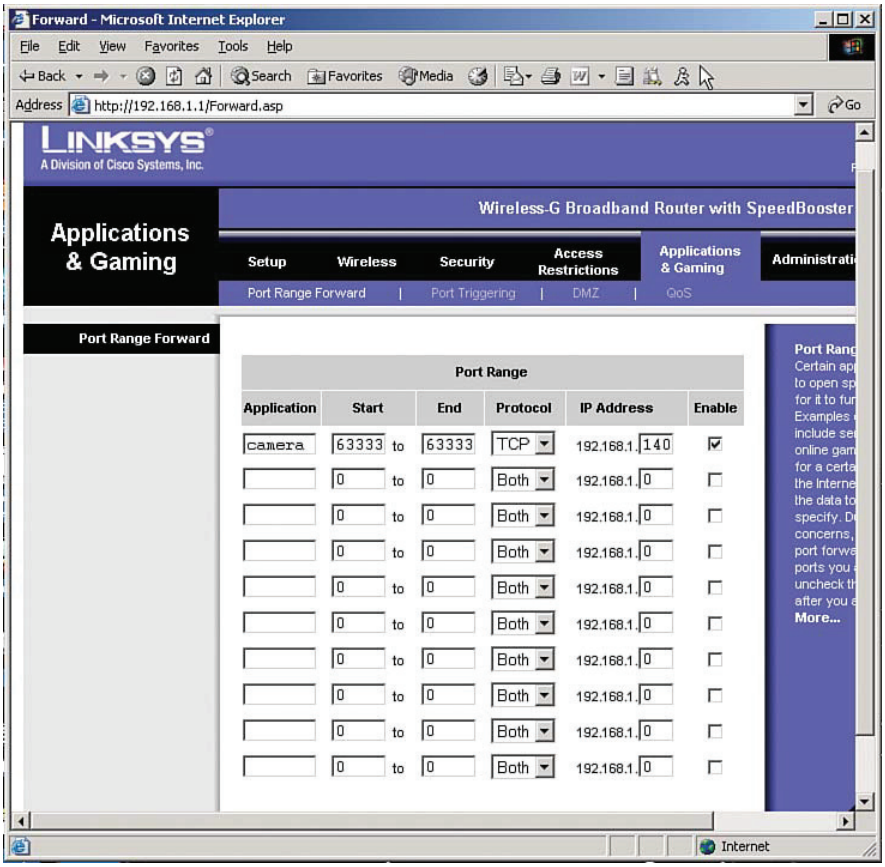


Note: We have not discussed IP port numbers very much. An IP port number is a number from 1 through 65535 that is used by applications (such as an Internet browser) to access the network. If an IP address is like your home address, think of an IP port number as being like a room of your house; it's adding another level of detail to the address.

Applications such as Internet browsers and e-mail programs use particular IP port numbers. We want to assign the camera to an uncommon number, such as between 60000 and 65535.

Step 2 Point an Internet browser to the wireless router by entering the IP address (for example, http://192.168.1.1). When prompted, enter the router's administrator password. Click the **Applications & Gaming** tab and then the **Port Range Forward** subtab (see Figure 13-20). Enter the chosen port number (from Step 1) in both the Start and End fields. Select **TCP** and then enter the IP address of the camera, for example, 192.168.1.140. Check the check box in the **Enable** column. Click **Save Settings**.

Figure 13-20 Set IP Port Forwarding on the Router



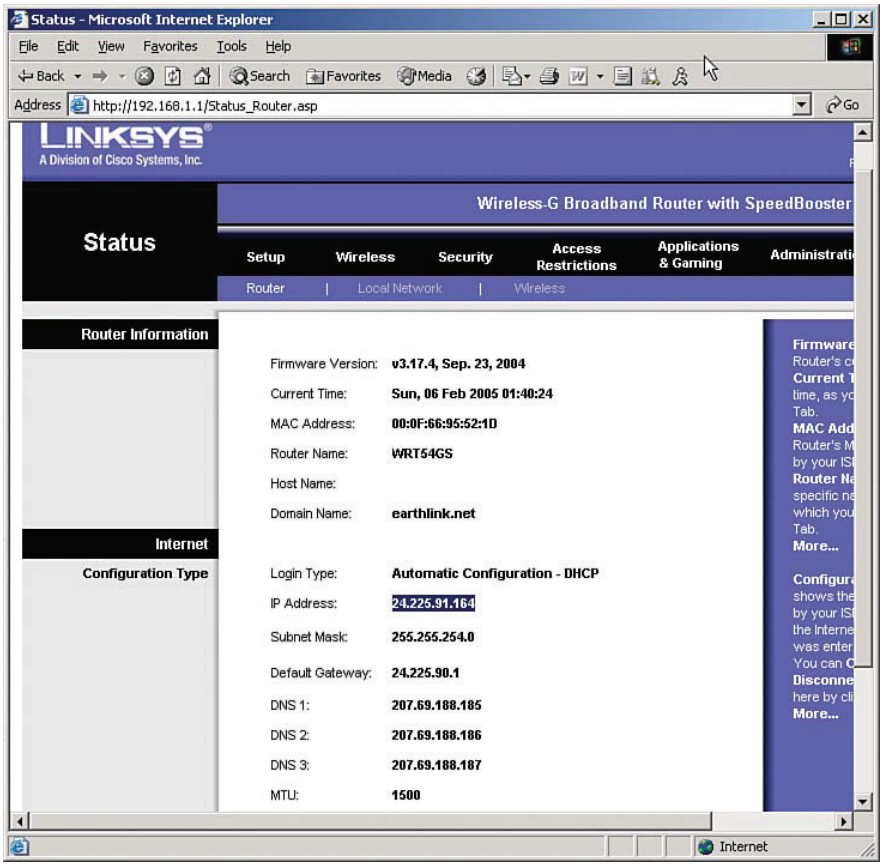
Now when packets are received from the Internet side of the wireless router with port number 63333 (assuming that is what you selected), they will be routed directly to the camera.

How to View the Camera over the Internet

Now we are ready to try to view the camera over the Internet. By the way, you will need to actually be outside your home network, at work or a wireless hotspot, to try this.

Step 1 While still on the wireless router, click **Status**. Find the Internet IP address (in Figure 13-21, it's 24.225.91.164). This is the IP address on the Internet to reach your wireless router (and your home network), so write it down.

Figure 13-21 Finding Your Internet IP Address



Step 2 Now, when you want to view the video images from a computer outside of your house, you access it in a similar way. Point the Internet browser to the Internet IP address plus the port number we chose, for example, http://24.225.91.164:63333. When prompted, enter the viewing username and password, and click **View Video**.

After completing these steps, you can reach the video camera from outside the home network.



Note: You can also use the Linksys Viewer Client to view video images over the Internet. The details of this process have been omitted here to save space. The procedure is very similar to using the Viewer Client from within your home network, as previously described. The major differences are

- Click **Internet** instead of **LAN**.
- Specify the Internet IP address.
- Specify the port number (for example, 63333).

Problems with Viewing Video over the Internet

There is one other potential issue with viewing your video over the Internet. The broadband networks typically assign a dynamic IP address to your broadband service. *Dynamic* means the IP address can change, typically only if you power off and on your broadband modem. This is usually not an issue because, typically, you will be assigned the same IP address for a long period of time.

If the IP address of your broadband modem does get reassigned, the new address may not match the address you wrote down for the camera. Then, when you try to access the camera, you will get an error message from the Internet browser saying "The page cannot be displayed." In this case, you need to access your wireless router, click the **Status** function, and write down the new Internet IP address.

If you rely on accessing your camera over the Internet, and the IP address changes too often, here are a couple of solutions:

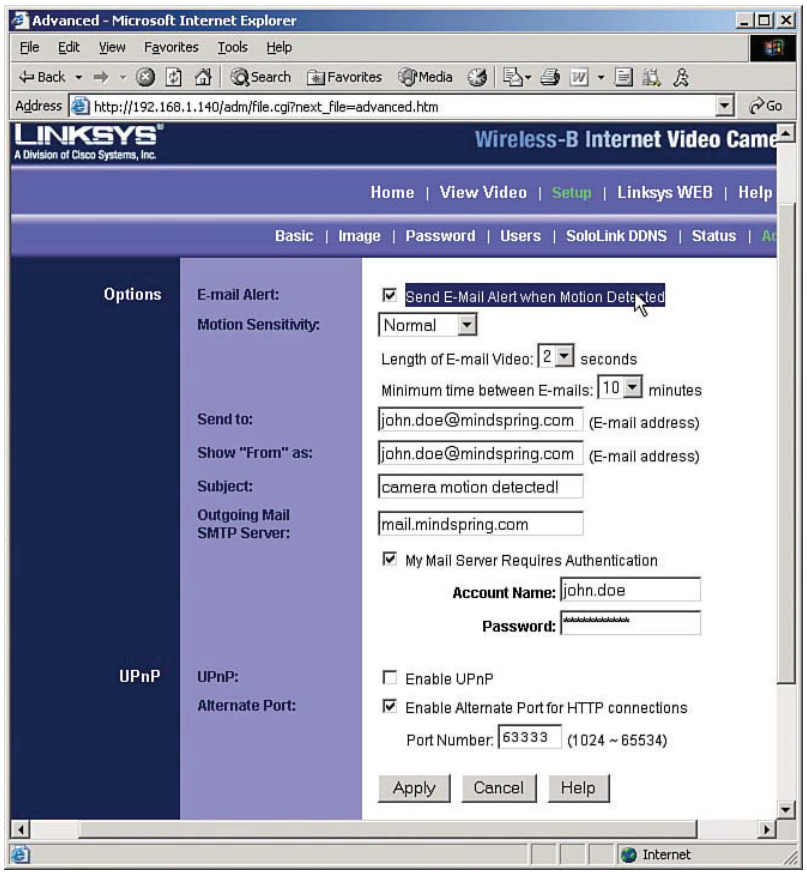
- Subscribe to a dynamic DNS service that automatically tracks your home network's IP address. Linksys offers a pay service called SoloLink. This service automatically tracks the address used to reach your video camera. (See http://www.linksys.com/sololink/. Further detail on dynamic DNS services is beyond the scope of this book.)
- Inquire with your ISP about upgrading your broadband subscription to a static IP address, which means that you pay a little extra per month, but your address never changes.

Using the Video Camera as a Motion Detector

Another very useful feature of the Linksys wireless Internet video camera products is the ability to act as a motion detector for active surveillance. Watching a video feed for hours waiting for something to happen is tedious. Depending on the reason for the video camera, it can be more effective to trigger on motion detected and then perform a notification action. Setting up the motion detector is pretty easy:

Step 1 Access the video camera using the administrator account. Click **Setup** and then click **Advanced**. Check the **Send E-Mail Alert when Motion Detected** check box (see Figure 13-22). Select a length in seconds for a video capture (2–5 seconds). Select the minimum time between e-mail alerts (2–30 minutes).

Figure 13-22 Enabling Motion Detection



Step 2 In the same dialog box, enter the e-mail account information, including

- Send-to e-mail address
- Show "from" e-mail address
- Subject
- Outgoing mail SMTP server (this is from your e-mail provider)
- E-mail login name and password

Step 3 Click **Apply**.

That's all there is to it. A word of caution, though: As soon as you enable the motion detector function (and until you shut it off), you will receive a video capture attached to an e-mail as often as you have specified. So take care not to leave it enabled for lengthy periods of time, because your e-mail account will promptly fill up.



Note: The Linksys WVC11B model provides video only, but the WVC54G and WVC54GC models provide audio and video.

You also can set up your motion detector to send alerts to a pager or cell phone. Most cell phones and pagers have an equivalent e-mail address that can be used to send a text message to. Simply supply that e-mail address as the alert address. If the camera product supports it, you may want to disable the audio/video clip attachment to cell phone and pager alerts. (The WVC11B camera does not support disabling, but the WVC54G camera does.)

When used properly, alerts based on motion detection can be very effective for verifying that latchkey kids have gotten home from school safely or that a spouse is home, or perhaps even as a security alarm if motion is detected while on vacation due to a home intruder.

Here are a few side notes on video cameras and the Internet:

- Take care where you point your wireless Internet video camera. It may not be a good idea to have an ongoing video feed of the inside of your home being offered up to the Internet. At a minimum, make sure you enable security, including passwords, to protect access to the camera.
- Be advised that Internet video cameras normally do not work well in low-light conditions. This may limit the camera's usefulness as a baby monitor, for example. Conversely, too much light or glare from nearby windows can also spoil images from these cameras.
- Review the laws in your state with respect to video taping of people without their knowledge. Your kids are most likely yours to tape whenever you deem necessary. However, using the video surveillance functions in this chapter to perform surveillance on the activities of an adult (such as a spouse or a babysitter) may be subject to local laws.
- Be careful about letting kids get into the web-cam game. You don't necessarily know who is on the other end watching.

Wireless Online Gaming

When we were 11 years old or so, we each got an Atari gaming system. We spent the entire summer indoors playing Pitfall Harry, and our mothers were constantly screaming at us to go outside and play like normal kids. In the years since, much has changed. The game systems are out of this world. You can play against people from all over the world, so after you whip everyone in your neighborhood, you can find some dude in Vancouver (or wherever) to play against. Our wives have stepped in for our moms and now they scream at us to turn that darn thing off. Good times.

This section walks you through the setup of an online gaming system. Our weapon of choice here is the Microsoft Xbox, which is easy to set up and use online. The online service from Microsoft is called Xbox Live. This system allows you to play one on one against a specific person or join an "open" game to play with or against other people. Some games also allow team play so that several people can cooperatively play the same game. Another feature of this system is audio chat, which allows you to speak live (via voice chat) with the other players during the game to strategize or talk smack (whatever the situation calls for). This feature uses VoIP chat technology. For a further discussion on VoIP, pick up a copy of *Internet Phone Services Simplified* (Cisco Press, 2006).

Gaming Servers

To play video games with other people online, gaming servers are required to provide the connections and communications between people playing the games.

Gaming servers work much like a videoconference bridge in that each individual inputs their own data, and all parties receive the combined stream of all the individuals. In a gaming server, each person on the server is assigned an entity in the program. This entity could be a car, a fighter, or a really mean duck. Within the game, you control the actions of this entity, which could affect other entities or the environment, as do all the other players in the game.

All the information from all the players is compiled in the server and then sent out to all the players in the game. A system like this requires a great deal of computing power and speed (both processing speed and connection speed if the players are remote). Fortunately, with dedicated game systems such as Xbox and broadband download speeds, high-end games lose nothing when you play online. Part of the reason for this is that the gaming server sends as little information as possible, just basic instructions to update the game.

It's important to understand the need for gaming servers, because different video game manufacturers offer varying degrees of online playing services. If you want to participate in online gaming, research the available options before you buy.

Options for Online Gaming

You have a few different options for online game playing, including using a computer or an actual video game console (such as Microsoft Xbox). Table 13-2 compares the options.

Table 13-2 Video Game Options for Online Play

Video Game Platform	Built-In NIC	Number of Online Games	Online Services	Online Play Costs	Voice Chat
Computer	Probable	Many	GameSpy (and others)	Free to $12.95 monthly	Yes
Microsoft Xbox	Built-in wired	Many	Xbox Live	$49.99 annual	Yes
Microsoft Xbox 360	Built-in wired	Many	Xbox Live	Free Silver Membership $49 annual for Gold Membership	Yes
Sony PlayStation 2	Built-in wired (starting Nov. 2004)	Many	Various game publishers	Free to $12.95 monthly	Handful
Sony PlayStation 3	Built-in wired One model has built-in 802.11g Wi-Fi	Many	Various game publishers	Free to $12.95 monthly	Handful

Table 13-2 Video Game Options for Online Play

Video Game Platform	Built-In NIC	Number of Online Games	Online Services	Online Play Costs	Voice Chat
Sony PlayStation Portable (PSP)	Built-in 802.11b Wi-Fi	Many	Various game publishers	Free to $12.95 monthly	No
Nintendo GameCube	Add-on wired NIC for $30-$40	Very few	Sega		No
Nintendo Wii (pronounced "we")	Promises built-in 802.11g Wi-Fi	Promises many	Promises Nintendo Wi-Fi Connection service	Promises Free	TBD

A computer with video game software installed is certainly an option. There are already hundreds of online games available, some for free and some requiring a fee. A good resource to find out what is available is GameSpy (http://www.gamespy.com). However, this type of online gaming device is not the focus of this chapter. This chapter focuses on dedicated video game consoles, because getting these connected takes a bit more work, and there appears to be much less information out there about how to do so.



Note: If you are truly interested in online gaming, Xbox and PlayStation are the leaders in the field. It does not appear that Nintendo is a serious player here yet, in our opinion. However, Nintendo is promising a major re-entry with the Wii platform (pronounced "we").

How to Connect Video Game Consoles to Your Wireless Network

In this section, we look at how to take video game playing to the next level: online.

The first step to online gaming is to have a network-capable video game console. You then can connect the console to the home network with an Ethernet cable, just as you can with any other computer or device. Because it is probable the video game console and television may be in an entirely different room of the house from the Internet connection, a wireless game adapter may also be incredibly useful. This device will allow a video game console to be connected to the wireless network.

So, let's get online. It is assumed that you have already installed your home wireless network and have high-speed broadband Internet service. The rest of this section goes through the steps to connect a video game over your home wireless network to an online gaming service.

Here's an overview of the steps to set up an online gaming system:

- Setting up the wireless game adapter for your wireless network
- Connecting a video game console
- Setting up an account and connecting to an online game provider

Setting Up the Wireless Game Adapter

After you have chosen your gaming console, you will want to connect it to your home network. If the console happens to be in close proximity to the wireless router, you could use an Ethernet cable and just connect it directly. Often, this is not the case, so in this section, we show how to use a wireless game adapter to connect the console from anywhere in your house.

Table 13-3 shows the Linksys wireless game adapter products that we can choose from.

Table 13-3 Linksys Wireless Game Adapters

Model	Wireless Standard	Wireless Encryption Supported
WGA54G	802.11g Also works with 802.11b and 802.11n	64-bit WEP 128-bit WEP
WGA11B	802.11b Also works with 802.11g and 802.11n	64-bit WEP 128-bit WEP



Note: The Linksys wireless game adapters will generally work with Microsoft Xbox and other game consoles. Another option is to purchase the wireless module made by the game console manufacturer. Check the instructions for your game console to make sure you can use any game adapter or if you need a specific one.

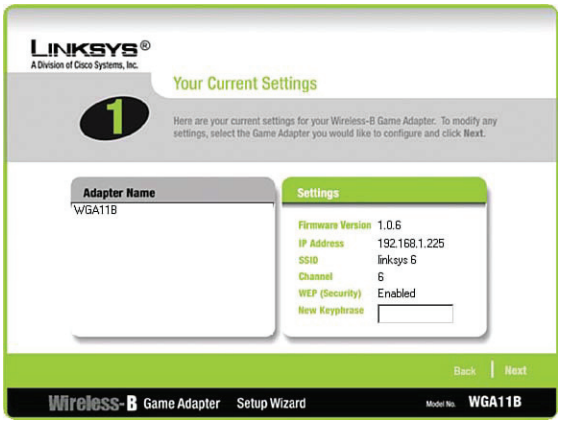
The steps to connect are as follows (in this example, we use the WGA11B product):

Step 1 Connect the Linksys wireless game adapter to the Linksys wireless router using an Ethernet cable, and plug in the power adapter. Set the X -|| switch to ||. The LAN LED light on the front should light up.

Step 2 Put the CD that came with the Linksys wireless game adapter into a computer on the network (a wired computer is preferred). The Setup Wizard should start automatically. If not, use My Computer to browse the CD and double-click **Setup.exe**. Click **Setup**.

Step 3 The Setup Wizard searches for the new game adapter on the network. If it is not detected, check the cabling and try powering the game adapter off and back on. Then, return to Steps 1 and 2. If the game adapter is located successfully, the current default settings for it are displayed (see Figure 13-23). Click **Next**.

Figure 13-23 Setup Wizard Searches for and Finds the Game Adapter



Step 4 Enter the default password, **admin**, and press **Enter**.

Step 5 Click **Obtain IP Address Automatically**. Change the password from the default (admin) to a random series of upper- and lowercase letters and numbers (see Figure 13-24). Write it down somewhere safe for keeping. Click **Next**.



Note: Note that this is the administration password for the wireless game adapter itself, not the wireless router. Wireless NICs generally do not have an administration password, but most other devices, including wireless routers, game adapters, print servers, and so on, have an administration password. You want to change it from the default, and make sure to write it down somewhere.

Step 6 Enter the SSID for your wireless network. (In Figure 13-25, we use J59wgh21MX.) Set the wireless security setting to **WEP 128 Bit** (or the encryption you are using). Enter the passphrase you have been using for your wireless network (in this example, 64Gx3prY19fk2). Click **No** to save the settings.

Figure 13-24 Change the Basic Settings

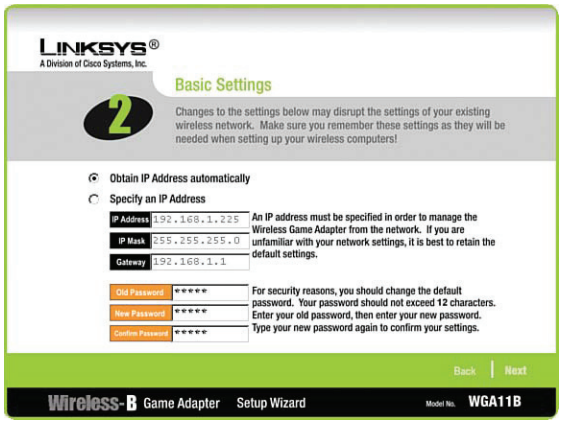
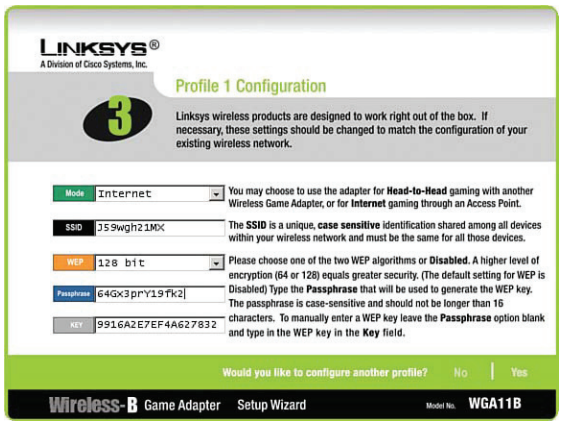


Figure 13-25 Set the Wireless SSID and Security Settings



Step 7 Two dialog boxes are displayed. These are normal; not very graceful, but normal. Click **OK** for both dialog boxes.

Step 8 Unplug the Ethernet cable connecting the game adapter to the wireless router. Power off the adapter (unplug it) and then power it back on.

Step 9 Press the blue button on the side of the game adapter repeatedly until the display on the front reads **P1** (see Figure 13-26). The wireless channel LED indicator light on the front of the wireless game adapter should be lit.

Figure 13-26 Select Wireless Profile P1



Connecting a Video Game Console

After you verify that the wireless game adapter is properly communicating with your wireless network, you can move on with setting up the rest of the online gaming system:

Step 1 Unplug the Ethernet cable to the game adapter (if it's still connected) and move the game adapter to the location in your house where you want the video game console to be. Because it is wireless, it can be placed anywhere there is an electrical outlet (and TV) nearby.

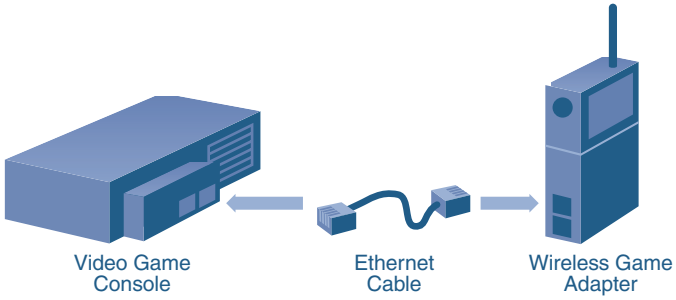
Step 2 Plug one end of an Ethernet cable into the port on the back of the wireless game adapter. Plug the other end into the Ethernet port on the back of the video game console, as shown in Figure 13-27.

Step 3 Connect the power cable to the wireless game adapter. After connecting the cables to both the game adapter and the video game console, remember to plug in the video game console to the electrical outlet.

Step 4 Turn on the video game console. After it boots, you should see both the LAN and wireless channel LED lights on the front of the wireless game adapter light up. If not, check the cabling and try powering off and on the game adapter. Also, try changing the X -ll switch setting.

Now we should have the game adapter joined to the wireless network, and the video game console connected and ready to access the network. The default settings may work and the game console may just connect at this point.

Figure 13-27 Connect the Game Console to the Game Adapter



Connecting to an Online Game Provider

Now that the wireless game adapter is on the network and your video game console has been connected, you need to set up the online game service. This will vary greatly depending on the particular service.

Here's a short example for Xbox Live service. First, we need to set up and verify the network settings:

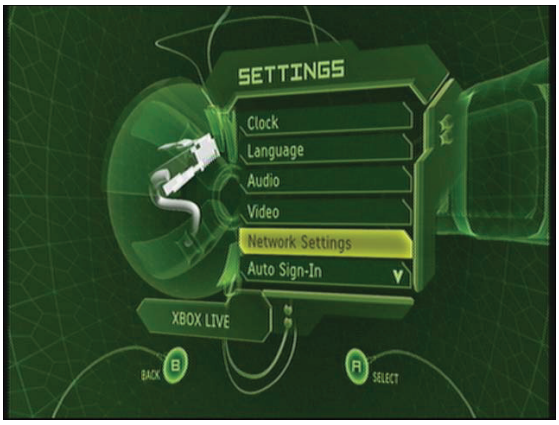
Step 1 Power on the Xbox. In the main window, scroll using the arrow pad until **Settings** is highlighted and then press the green **A** button (see Figure 13-28).

Figure 13-28 Xbox Main Menu



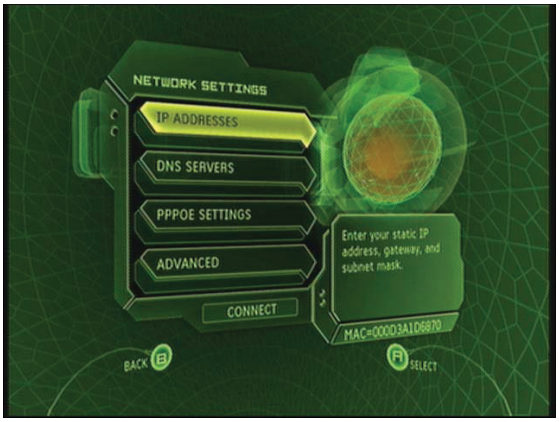
Step 2 Afer choosing **Settings** choose **Network Settings** (see Figure 13-29).

Figure 13-29 Xbox Network Settings Menu



Step 3 There are four Network Settings submenus (see Figure 13-30). Choose **IP Addresses**.

Figure 13-30 Xbox Network Settings Submenus



Step 4 Set Configuration to **Automatic** (see Figure 13-31). Click **B** to go back one menu.

Figure 13-31 Setting IP Address to Automatic



Step 5 Follow similar steps to set

- DNS Servers to **Automatic**
- PPPoE Settings to **Off**
- Advanced to **blank**

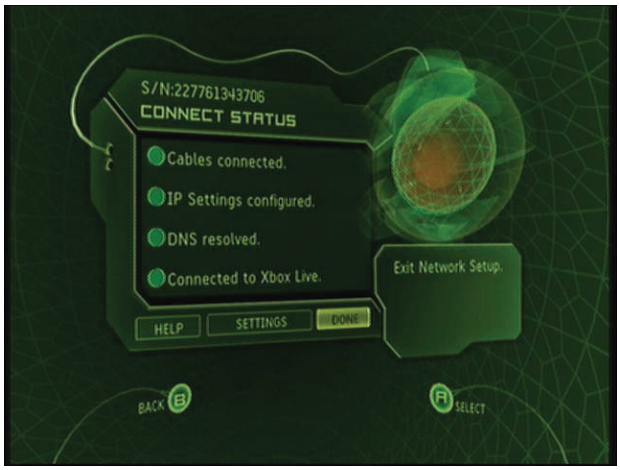
Step 6 After you verify the settings, select and click **Connect** (see Figure 13-32).

Figure 13-32 Test the Connection to Xbox Live



Step 7 The Xbox tests the connection by accessing the Xbox Live server. All four status indicators should appear as green (see Figure 13-33).

Figure 13-33 Connection to Xbox Live Is Successful



Now that we have set the network settings for the video game console, you can move on to setting up an account with the online gaming provider (we use Xbox Live for this example). Before continuing, you need to purchase a subscription to Xbox Live either from a retail store or online. The subscription comes with a code number that you need to enter during the setup process.

When you have completed the account setup, you are ready to jump into online gaming. Whenever you power on your Xbox game console, it automatically connects to the Xbox Live service. Now put in your games and go play!

We, the authors, do not assume liability for any marital or family problems or carpal tunnel syndrome caused by the (excessive) use of this technology.



Note: If you have trouble getting your gaming system online, check your firewalls. You might have to temporarily disable one or more security measures. Just remember to turn them back on when you are done.

Networking Your DVR

For those of you who, like us, have become TiVo or digital video recorder (DVR) junkies, we are about to show you something wicked cool you can do with your TiVo and your wireless network.

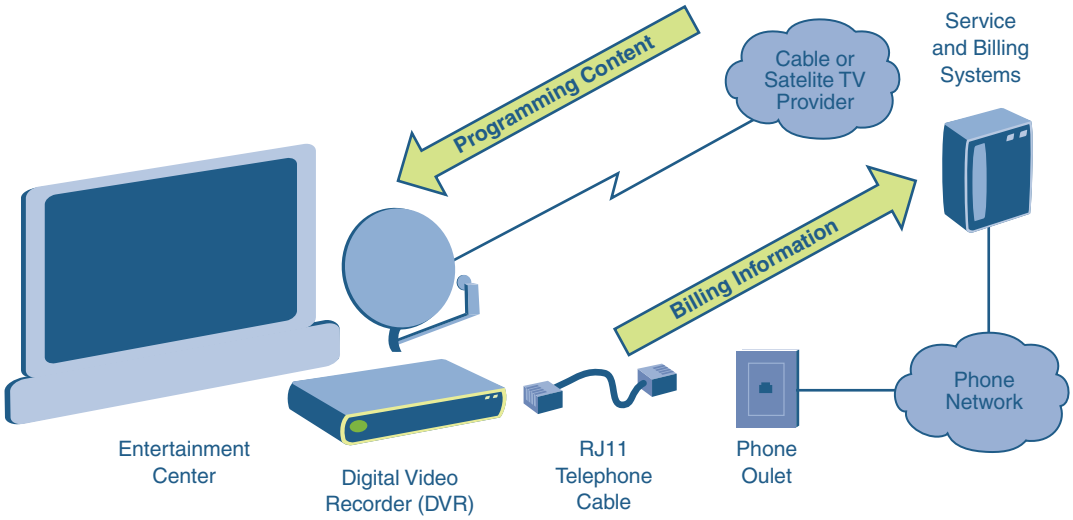
In case you have been living in a cave and have not heard of TiVo or DVR yet, here is a 30-second version. TiVo and DVRs allow you to record your favorite TV shows or movies to watch later. Big deal, VCRs can do the same thing, right? Well, not exactly. See, TiVo and DVR boxes are able to sit in between your television and the content provider (cable or satellite) box. Then, you can select what you want to record from an interactive programming menu, and the DVR records it digitally and stores it on its hard disk. Depending on the size of the hard disk, DVRs can store 40, 80, or more than 100 hours of shows.

Like a show a lot? TiVo lets you record a season pass, which means every time your favorite show is on, TiVo records it. At your leisure, you can simply go into the recordings list and watch your favorite shows whenever you feel like it.

Typical DVR Setups Today

The typical setup today for a TiVo or DVR is not networked, as shown in Figure 13-34.

Figure 13-34 Typical Non-Networked DVR Setup Today



The TiVo or DVR is connected to your television, either as a standalone box or integrated into your content provider's set top box (this is an increasingly popular option).

Programming content is transmitted by the provider, over satellite or cable, to your home. TiVo or DVR sits in the middle and records content you have specified. TiVo also requires a telephone connection that its internal modem uses to "call home" for billing and subscription service purposes.

With these basic requirements met, life is grand.

Reasons to Network Your DVR

So, if your TiVo or DVR is already recording your favorite shows and keeping you from missing *The Dog Whisperer*, why worry about networking it?

Well, networking your TiVo or DVR offers several distinct advantages. Remember that DVRs record TV episodes and movies in digital form. Essentially, they are computer files, sitting on a hard drive.

So what if we told you that you could do one of the following?

- Transfer movies and TV episodes from your TiVo to a laptop to watch when you travel
- Transfer movies and TV episodes to a portable player, like a video iPod

- Burn a DVD of your favorite TV episode
- Transfer movies and TV episode recordings between two different TiVo players
- Download a video file from your PC or laptop into the TiVo or DVR to watch later on your widescreen TV

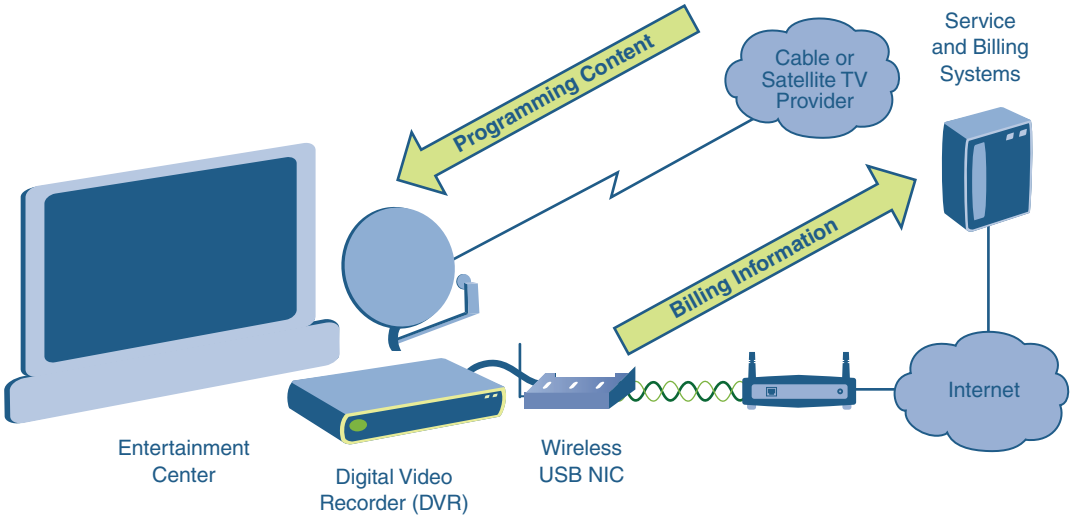
Does any of that sound interesting? Yeah, we thought so.

Further, now that you have a wireless network, you can put the TiVo or DVR anywhere in your house without worrying about a telephone jack. The DVR can just use the wireless network to do its "call home" function, over the Internet. Pretty sweet.

Networking Your DVR

It is relatively easy to connect your TiVo or DVR to your wireless home network. Figure 13-35 shows how it works.

Figure 13-35 Connecting a DVR to Your Wireless Network



Essentially, instead of having a telephone cable connecting the DVR to a phone jack, you add a wireless USB NIC that bridges your DVR onto your wireless network.

There are a couple of very important requirements to be met before you start. First, the TiVo Home Media feature is required for networking, which means you need a Series 2 TiVo box. If you are not sure which series your TiVo is, contact TiVo and ask a representative.



Note: If you are a DirecTV subscriber, the DirectDVR TiVo service uses integrated satellite receiver/TiVo DVR boxes. Unfortunately, DirecTV opted to disable the Home Media capabilities in its implementation, and has no specific plans at the time of this writing to include these cool functions. For more information, you can contact DirecTV at www.directv.com/DTVAPP/customer/howToReachUs.jsp.

Second, TiVo supports a specific list of wireless USB NICs, because there is a very limited user interface for you to configure them, and there is not really a way for you to load new NIC drivers. The list can be found at the TiVo support site: www.tivo.com/adapters/.

The Linksys WUSB11 is one of the supported wireless USB NICs. Check the list for the latest supported NICs.

As long as you have a Series 2 TiVo and can acquire a supported wireless USB NIC, you are all set. What are you waiting for?

Connecting your TiVo to the wireless network is relatively easy:

Step 1 Using a standard USB cable, connect a supported wireless USB NIC to an open USB port on the back of the TiVo.

Step 2 Using the TiVo menu, access the **Settings** menu. Locate the network settings. Choose **Wireless**.

Step 3 Using the TiVo remote control, enter the SSID for your wireless network, the security type (128-bit WEP), and the WEP key.

Step 4 Save the settings.

If you entered the SSID and WEP key correctly, the wireless USB NIC should connect to your wireless network.



Note: Don't forget, if you have enabled MAC address filtering as a security measure in your wireless network, you need to add the MAC address of the wireless USB NIC before it will be permitted to join the wireless network.

More detailed setup instructions for adding TiVo to wireless home networks can be found at the TiVo support site: http://customersupport.tivo.com/knowbase/root/public/tv2013.htm.

Using TiVoToGo

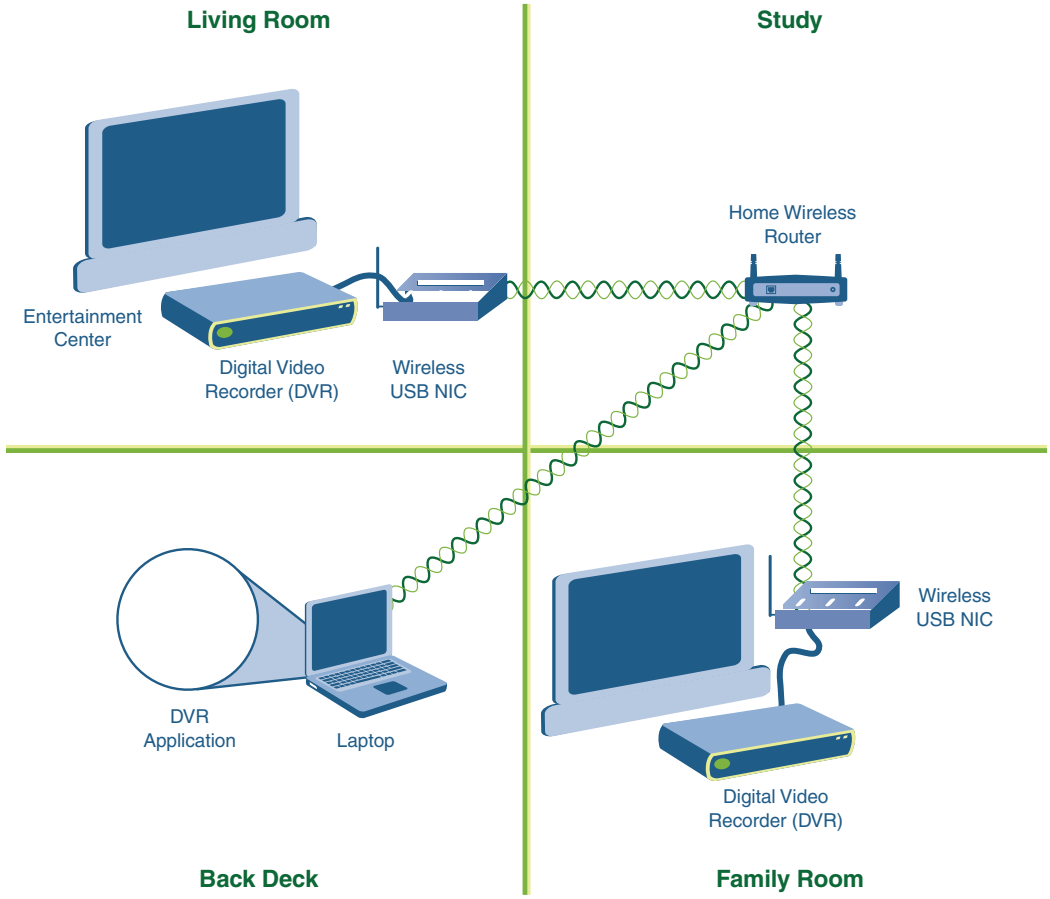
After your TiVo is networked, you can start taking advantage of the connectivity and freely move your favorite TV episodes and movies around. Figure 13-36 shows a couple possible scenarios.

Suppose you have two TiVo or DVR boxes: one in the living room downstairs, and one in the family room upstairs. Suppose you have recorded your favorite episode of *CSI: Crime Scene Investigation* (possibly the best show ever to grace the screen of a television) on the downstairs TiVo.

But you neglected to remember that your spouse is hosting a function downstairs and so you are kicked out. No problem, you can just transfer the episode over your home wireless network to the TiVo upstairs, and you are once again in business.

Another very useful function is TiVoToGo. As the name implies, TiVoToGo lets you transfer episodes recorded on a TiVo to a portable viewing device to take with you, such as a laptop or video-capable iPod.

Figure 13-36 What You Can Do with Networked DVR Boxes



To transfer between a DVR and a laptop, you typically need to download a software application. For TiVo, this is called the TiVo Desktop. The application is free and can be found at the TiVo website: www.tivo.com/desktop.

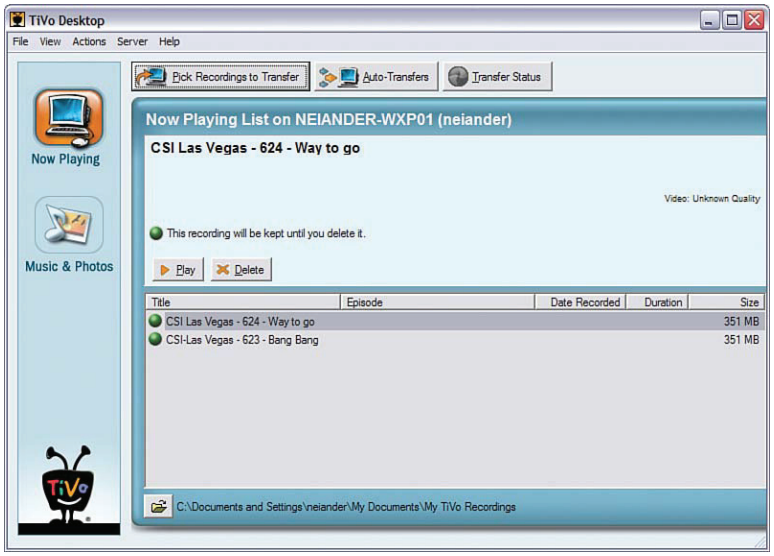
TiVo Desktop is a very straightforward application that lets you see what is on your TiVo and laptop, and then transfer episodes back and forth. Figure 13-37 shows an example of TiVo Desktop.

More information on getting started with TiVo Desktop can be found here: http://customersupport.tivo.com/knowbase/root/public/tv2178.htm?.

Help on transferring video files from your computer to TiVo can be found here: http://customersupport.tivo.com/knowbase/root/public/tv251080.htm?.

Get your DVR networked, and enjoy!

Figure 13-37 TiVo Desktop Example



Summary

Wireless home networks are for connecting more than just your computers and laptops. They can connect wireless video cameras, video game consoles like Xbox 360, TiVo and DVRs, home automation devices, and someday refrigerators, pantries, and maybe sock drawers. We have just barely scratched the surface here of what you can do with your wireless network. But we hope we have at least given you a glimpse and got you excited about the possibilities.

Where to Go for More Information

For more information about wireless video cameras, go to the Linksys website: http://www.linksys.com.

For more information about online gaming, go to the following websites:

- **Xbox and Xbox 360**—http://www.xboxlive.com
- **PlayStation 2 and 3**—http://www.playstation.com/
- **PlayStation PSP**—www.us.playstation.com/PSP/OnlineGaming
- **Nintendo Wii**—http://wii.nintendo.com/home.html

For more information about networking your TiVo, go to TiVo customer support: http://customersupport.tivo.com/userWelcome.asp?path=2&faq_node=Network.

For more information about voice over IP (VoIP), check out our book *Internet Phone Services Simplified* (Cisco Press, 2006).

This page intentionally left blank

CHAPTER 14

Wireless to Go

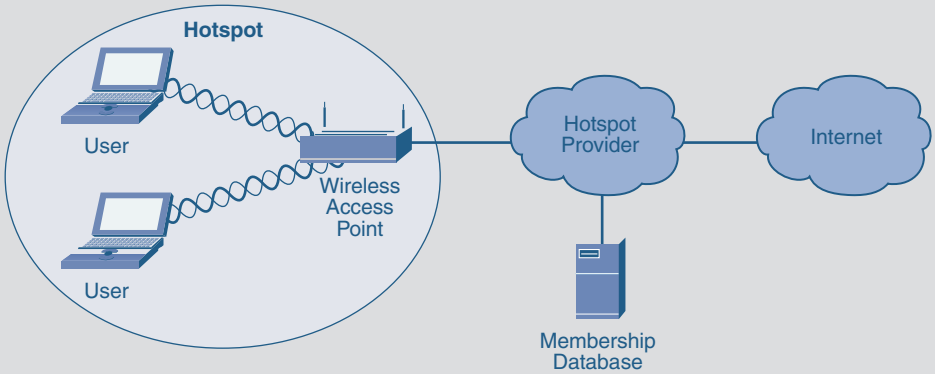
One of the biggest advantages of wireless technologies is the ability to easily take it on the road with you. Public Internet access was rare before the advent of Wi-Fi mostly because of cost and convenience. Allowing patrons of a coffee shop, airport, or bookstore to access the Internet meant expensive cabling retrofits to put Ethernet ports in, and—even if a lease holder were willing to put up the expense—there are only so many ports you can put where patrons can get to them.

Wireless, of course, removes the need for network cabling and provides vendors the same flexibility as home users of wireless. With virtually no need to cable outside access and power, a shop owner can provide Internet access to every patron in the store and even those sitting outside. No cables and no expensive retrofits are needed. In most cases, the actual Internet access is provided by a regional or national service provider who charges individual users directly.

What Is a Wireless Hotspot?

A *hotspot* is an area served by a Wi-Fi wireless access point to provide Internet service. Figure 14-1 shows the basic elements. A *hotspot provider* is the owner of the Internet service, and it can be a very large commercial operator, such as T-Mobile, or a small privately owned hotspot, such as a neighborhood shop. Some cities and communities are also starting to provide Wi-Fi service in downtown areas for use by citizens. Depending on whether the service is a free or pay service (which requires a subscription), the hotspot provider may have a membership database, which contains information about who is permitted to use the service.

Figure 14-1 Wireless Hotspot and Its Basic Elements




STARGATE
COFFEE
Like, are you, like, online right now?
Like, can you download my all-time favorite Celine Dion song, like, right now?

Connecting to wireless hotspot networks is similar to connecting to your wireless network at home, with some distinct differences:

- At home, we know the SSID of the wireless system; with a hotspot, we need to discover this crucial information. To make this easy, hotspots typically broadcast their SSID.
- For a home network, we want to provide access to *only* our computers, so we turn on very strong security measures. By their nature, hotspot networks are very open, using no encryption; otherwise, how would we be able to connect?
- Our home network is free to access (but you still need to pay your ISP), whereas hotspot networks may be free or may require a membership or subscription to use.
- We know that our home network is our own and can be trusted. We have to be far more careful with hotspot networks because, by their nature, we may not always be certain who is operating them. Currently, no regulations exist regarding who can and cannot operate wireless hotspots.
- Having secured our home wireless network, we know the users are "friendly." On a hotspot network, we have no idea what other people are also using the hotspot, whether they are "friendly" or are the source of a potential hack attack.

How to Find Wireless Hotspots

The first step to using wireless access while you're away from home is to find a hotspot. Hotspots are relatively easy to find (and it gets easier every day).

There are a few different ways to find out where wireless hotspots are, including

- Doing an online search
- Downloading a list to your PC
- Scanning

If you know you will be looking for a hotspot before you leave your home or office, your best bet is to do an online search prior to heading out. There are several sites that allow you to enter an address, airport code, or even a ZIP or postal code. For example, the search tool at JiWire, http://www.jiwire.com, allows you to sort by proximity, location, or by service providers (who pay for preferred placement on the site).

If you plan on using hotspots regularly, you may want to download a program to your laptop that contains a list of hotspots (regular updating is required). This can be of great benefit if you need to find a hotspot after you have already left home.

A third option for finding a hotspot is to do a scan for a hotspot at the moment you need one. To do so, you need a program that will go out and "sniff" for a wireless signal. Depending on the wireless NIC that you are using in your laptop, it may come with a scan function in the NIC's management utility (the Linksys products do). Windows XP has this functionality built into its wireless NIC management. There are also several programs available for free download with built-in scanning capability.

Table 14-1 lists some good resources and tools for finding Wi-Fi hotspots.

Table 14-1 Resources for Finding Wi-Fi Hotspots

Resource	Online Search	Download Location Database	Download Wireless Connection Manager	Website
Boingo	Yes	Yes	Yes	http://www.boingo.com
JiWire	Yes	Yes	No	http://www.jiwire.com
T-Mobile HotSpot	Yes (T-Mobile locations only)	Yes (T-Mobile locations only)	Yes (T-Mobile locations only)	http://hotspot.t-mobile.com
WiFi 411	Yes	No	No	http://www.wifi411.com



Note: Lists of hotspots in tools such as these may or may not be up to date. If you know where you are staying or going to be in advance, it's also helpful to check that location's website to see what they offer. For example, most hotels list on their website whether or not they provide Wi-Fi Internet access.

Wireless Hotspot Options and Costs

In general, hotspots are either free sites or pay sites. Free sites are typically offered by businesses such as hotels, coffee shops, and restaurants to attract customers. Pay sites are more numerous and widespread. Many business-like hotels are using them to extract an extra $10 from your wallet. Pay sites are also growing rapidly due to the entry of large wireless cell phone companies, such as T-Mobile, Cingular, and SBC. Four basic types of hotspot services exist, as shown in Table 14-2.

Table 14-2 Types of Wireless Hotspot Services

Type	What They Are	Where You Can Find Them	Examples
Free	A free connect-and-go hotspot service that is becoming rare these days.	Small neighborhood businesses, public libraries; provided to attract customers	Public library, local communities (increasing trend)
Free with registration	It's free, but you provide your name, address, e-mail address, and maybe answer a survey.	Hotels, coffee shops, restaurants; provided to attract customers	Schlotzsky's Deli, Bear Rock Cafe, Panera Bread, Holiday Inn Express
Subscription	You pay a monthly, annual, or per-usage fee to use the service, much like your cell phone.	Hotels, airports, coffee shops, restaurants, business service shops, planes (soon)	T-Mobile (at Starbucks, Borders, Kinkos), SBC (at UPS Store), Wayport (airports, McDonald's), Cingular (airports)

Table 14-2 Types of Wireless Hotspot Services

Type	What They Are	Where You Can Find Them	Examples
Roaming	Same as subscription service, except you are roaming on another provider who has an agreement with your provider.	Same as subscription	Same as subscription

Ironically, the initial popularity of wireless network hotspots was the idea of free Internet access. Despite attempts at an organized citizen-led mosaic of free hotspots, it seems inevitable that the sizeable market opportunity is just too attractive for the traditional telecommunications companies to pass up.

The upside is that to make money, these companies will invest the cash to put hotspots everywhere you need them. Soon, any place that people can stand or sit for more than 60 seconds will be a hotspot.

One growing trend worth mentioning is that many local communities are starting to invest in city-wide wireless hotspot networks. Most have two aims: provide high-speed access for public-sector agencies such as police, fire, and so on, and provide access to citizens themselves.

If you fall into the category of a regular hotspot user, and you either can pick the hotspot location where your preferred provider has an access point or can always access from the same locations (such as your local airport), your best bet may be to get a monthly or annual subscription. If you are a casual hotspotter, you will probably be better off with a per-day or other pay-per-use option.



Note: Accessing a network that was unintentionally left open (such as your neighbor's) isn't very nice. On the other hand, there are many "unwired city" initiatives where local governments are providing free access. It's no problem to use free access when it is made available on purpose, but not when someone just forgot to set up security. It's usually easy to tell the difference.

Discovering and Connecting to Wireless Hotspots

Because hotspot locations want to advertise their willingness to accept your business, they broadcast their SSID and do not require an encryption key to connect. But you do need to discover or be told what the SSID is for the hotspot so that you can tell your wireless NIC how to connect to it.

You can use several methods to discover the hotspot's SSID, depending on the Windows operating system you use, the capabilities of the wireless NIC in your laptop computer, and the hotspot service to which you want to connect. In general, there are three possibilities:

- The wireless NIC management utility that ships with the NIC, such as Linksys WLAN Monitor
- Windows Wireless Network Connection utility
- A third-party wireless connection manager, such as Boingo or T-Mobile's Wireless Connection Manager software

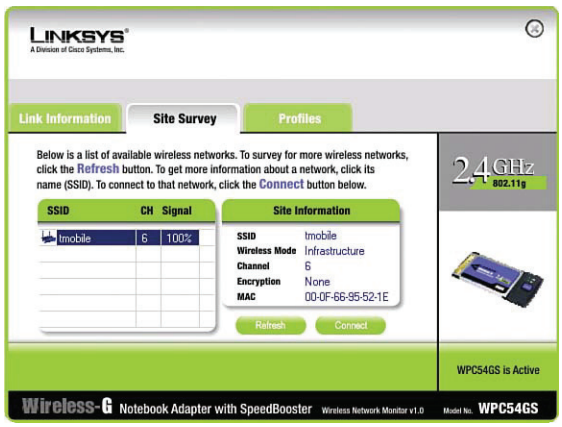
As discussed in Chapter 8, "Wireless NIC Setup," you are likely using Windows or the manufacturer's utility to manage your wireless NIC. These are also fine to use for connecting to hotspots. If you connect to hotspots a lot, you may want to consider using a connection manager from Boingo or T-Mobile (if you subscribe to one of them) for convenience. We cover connecting to a wireless hotspot with each of these possibilities in the sections that follow.

Connecting to Hotspots Using Linksys WLAN Monitor

If you are using the Linksys WLAN Monitor to manage your NIC, the following steps show how to find and connect to a hotspot:

Step 1 Launch the WLAN Monitor utility by double-clicking the icon on the desktop or by choosing **Start > Programs > Linksys > Wireless Notebook Adapter**. Click the **Site Survey** tab (see Figure 14-2). Click the **Refresh** button to perform a survey of what wireless networks are available.

Figure 14-2 Perform a Site Survey



Step 2 Click the hotspot that you wish to connect to. In our example, we found a T-Mobile hotspot. Click **Connect**. You should see the connection made to the hotspot (Signal Strength and Link Quality show green, as shown in Figure 14-3).

Figure 14-3 Successful Connection to Hotspot



Step 3 You can save this hotspot into your profiles so that the next time you use it, connection happens automatically. Choose **More Information > Save to Profile** (see Figure 14-4).

Figure 14-4 Save the Hotspot in Your Wireless Profiles



Step 4 A dialog box appears asking for a name for the new profile (see Figure 14-5). Enter a description you will remember, and click **OK**.

Step 5 The new profile just created now appears in the Profile list (see Figure 14-6). Now, whenever you encounter a hotspot with this profile, the wireless network adapter will automatically connect to it.

Figure 14-5 Enter a Name for the New Wireless Profile

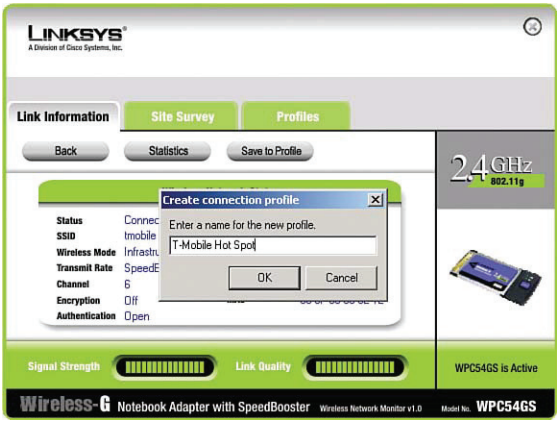
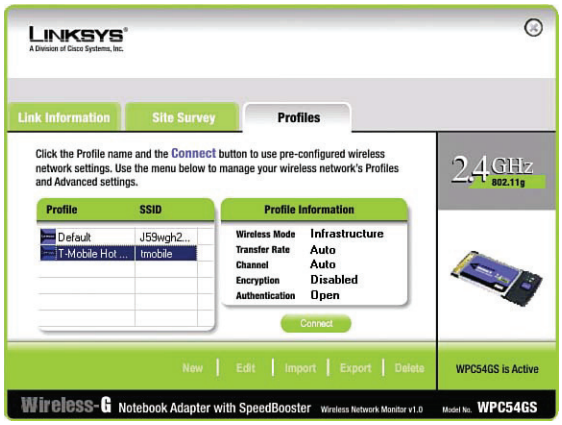


Figure 14-6 New Profile Is Listed





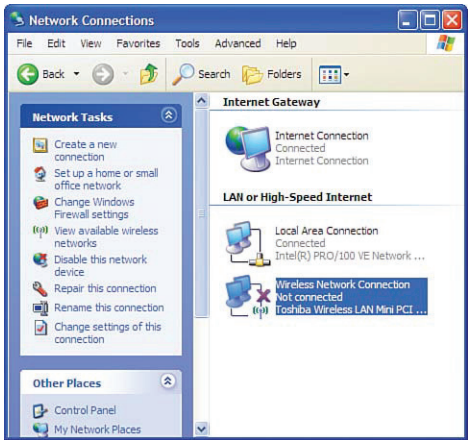
Note: Generally, after you create a profile for one hotspot on a provider's network, this allows you to connect to all the other hotspots on that provider's network. You do not need to create a new profile each time you connect to a hotspot in a different location, only when you use a new provider for the first time.

Connecting to Hotspots Using Windows XP

If you are using Windows XP to manage the NIC in your laptop, the steps for connecting to a wireless hotspot are as follows:

Step 1 Choose **Start > Control Panel > Network Connections**. Note the red X on the Wireless Network Connection icon. This is normal, because we have not yet established a connection to the wireless hotspot network. Click the **Wireless Network Connection** icon in the right section of the window and then click **View Available Wireless Networks** on the left. (See Figure 14-7.)

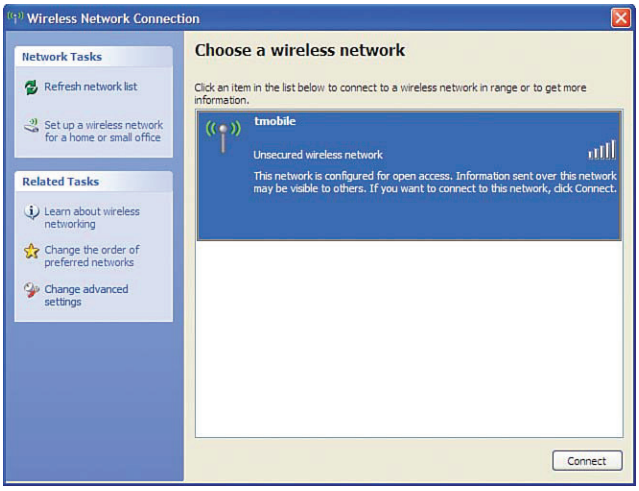
Figure 14-7 Perform a Site Survey with Windows XP



Step 2 Click the hotspot that you want to connect to (tmobile in this example), and click **Connect** (see Figure 14-8).

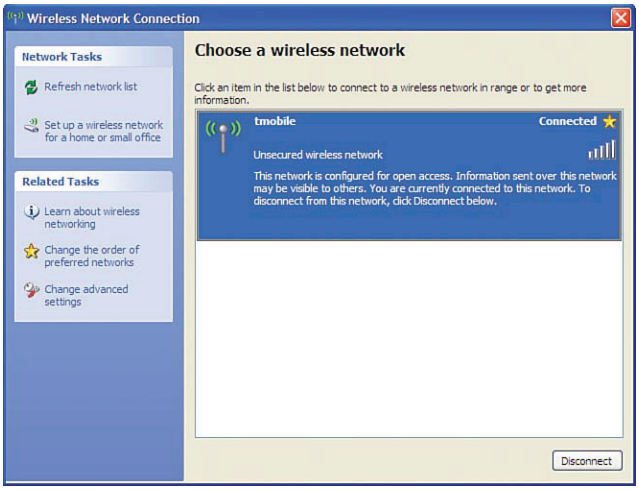
Windows may prompt you to verify that you want to permit a connection to an unsecured wireless network. This is normal, because the hotspot is not running encryption such as WEP or WPA. Acknowledge that you want to allow the connection.

Figure 14-8 Select an Available Hotspot



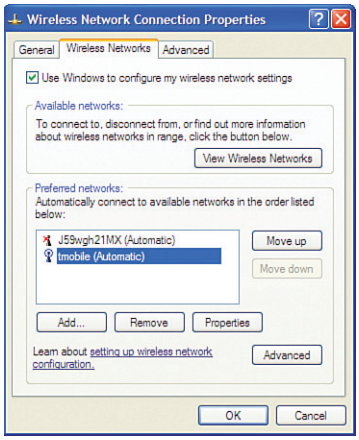
Step 3 In the Wireless Network Connection window, you can verify that you are connected successfully to the hotspot. (See Figure 14-9.)

Figure 14-9 Successful Connection to the Hotspot



Step 4 Windows XP typically adds the hotspot to the Preferred Networks list upon successful connection. To check this, in the Network Connections window, choose **Change Settings for This Connection > Wireless Networks**. You should see the hotspot in the Preferred Networks section (see Figure 14-10). Click **OK**.

Figure 14-10 Verify Hotspot Is Added to Preferred Networks





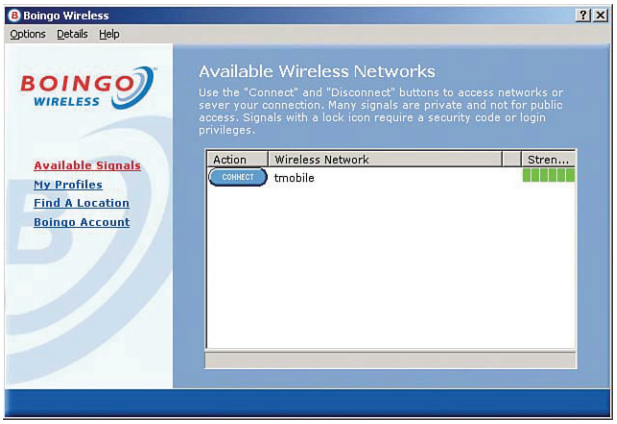
Note: Being in the Preferred Networks list in Windows means that your laptop will automatically connect to the wireless network in the future if encountered. This can be convenient if you use hotspots often. If you would prefer not to connect automatically, remove the entry from the Preferred Networks section.

Connecting to Hotspots Using Boingo

A third possibility for connecting to hotspots, which can generally be used on any of the Windows operating system versions (98, 2000, Me, XP), is to use a connection manager software program that is provided by the hotspot system provider you have a membership with. For example, if you subscribed to a T-Mobile or Boingo hotspot service, using the provided connection manager software can make location of and connection to hotspots literally just a click of a button.

Boingo Wireless operates through a collaboration of many different hotspot providers who choose to affiliate with Boingo Wireless and list their hotspots in the Boingo database. Figure 14-11 shows the connection manager program that Boingo provides.

Figure 14-11 Boingo Connection Manager Program



The Boingo application automatically detects wireless hotspots you encounter. To connect, you simply click the **Connect** button for the hotspot network you choose.

Boingo also provides a searchable database of hotspot locations. You can use the Boingo application if you have a paid membership with Boingo, or you can use it for free (limited functionality) as a general connection manager application, whether you are connecting to Boingo-affiliated hotspots or someone else's.

Passing the Membership Test

At this point, you have accomplished getting your laptop to talk properly with the wireless hotspot access point. But you are not yet to the point of being able to access the Internet. The next step is the *membership test*.

Whether using a free site or a pay site, the membership test is almost always started the same way: by launching your Internet browser. When your browser first attempts to access the Internet, you will be redirected to the membership page for that service. For free services, this web page may ask you to fill out some information about yourself and possibly hit you with a quick survey. For pay services, you typically must enter your user ID and password to prove that you have a valid subscription to their service.

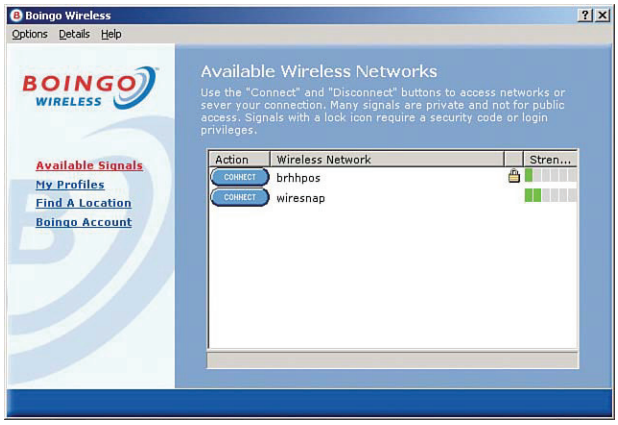
Following are two examples: one for a free service, and one for a pay service.

Example: Connecting to a Free Service at Bear Rock Cafe

The following is an example of using the hotspot service at a Bear Rock Cafe. In this example, access is free with registration. The registration process lets you create a user ID and password for easy repeat access in the future.

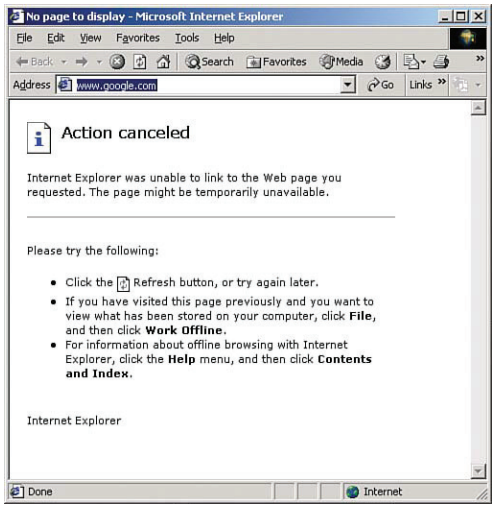
Step 1 Use your chosen connection manager program to connect to the hotspot. In this example, we used the Boingo free connection manager (see Figure 14-12). We can see that the SSID is wiresnap. Click the blue **Connect** button next to the wiresnap network.

Figure 14-12 Using Boingo to Connect to the Hotspot



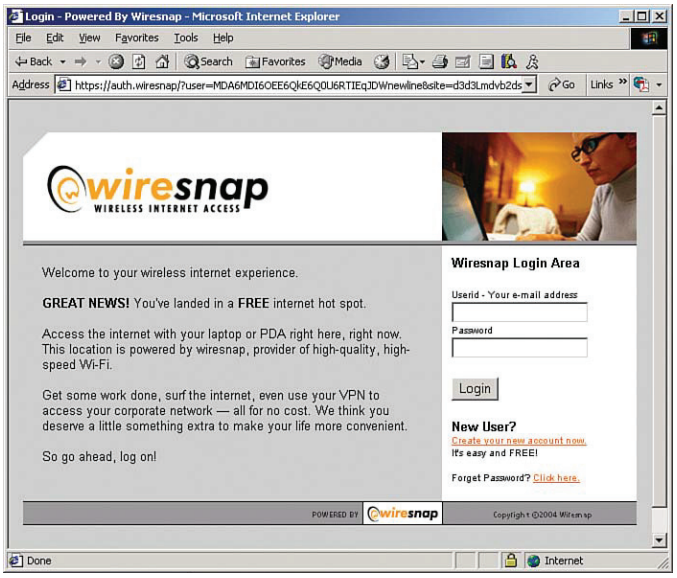
Step 2 Launch your Internet browser (such as Internet Explorer) and type in any web page address (see Figure 14-13).

Figure 14-13 Launch Internet Browser to Trigger the Redirect



Step 3 You are redirected to the membership test page, prompting for the user ID and password (see Figure 14-14).

Figure 14-14 Hotspot Membership Login Page



If you have already registered previously, you can enter the user ID and password and immediately log in.

If you have not already registered previously, you can click the **Create Your New Account Now link** . To register for a free account, you provide your name, address, e-mail address, and age. You also create a user ID and password.

After logging in to the free service, you can then use the Internet.

Example: Connecting to T-Mobile Service at Borders Book Stores

This section provides another example of using the hotspot service, this time at a Borders store. In this example, T-Mobile owns and operates the Borders hotspots as a pay subscription service. (This example assumes you have already signed up for service with T-Mobile.)



Note: It is never a good idea to sign up for a new hotspot subscription service over the hotspot. Remember, you are in a public location on a public network, and you do not want anyone to obtain your personal information or credit card number. Plan in advance where you are going, determine what hotspots you may want to use, and sign up from home or office.

Step 1 Use your chosen connection manager program to connect to the hotspot. In this example, we used the T-Mobile-provided Connection Manager (see Figure 14-15). The Connection Manager program indicates (with bars of service, much like a cell phone) when there is a T-Mobile hotspot in range. Click **Connect**.

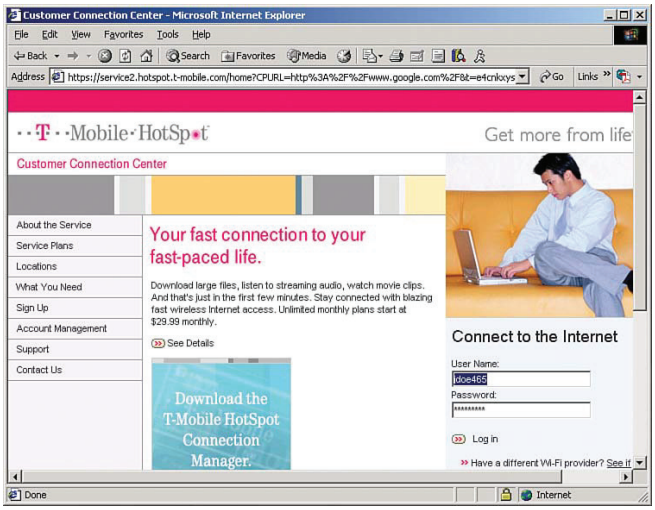
Figure 14-15 T-Mobile Connection Manager



Step 2 Launch your Internet browser (such as Internet Explorer) and type in any web page address.

Step 3 You are redirected to the membership test page, prompting for the T-Mobile login credentials (see Figure 14-16). Enter the user ID and password that you chose when you signed up for a T-Mobile HotSpot account.

Figure 14-16 T-Mobile Login Page



Step 4 A login confirmation box appears. Shrink this down to your taskbar and save it. When you are ready to log off, go back to this little box and click **Log Off** or simply click **Disconnect** in the main T-Mobile Connection Manager window.

After you pass the membership test, you can finally move on to using the Internet. Make sure to read the following section for some important security tips.

What Not to Do When Using a Wireless Hotspot

Okay, so you never thought you would actually need to use a hotspot when you suddenly find that you need to take a cross-country trip or go to visit family for a week and, to your horror, discover that they do not have broadband access in their home. We discuss how to deal with this so-called family of yours later, but in the mean time, you need to find a hotspot and reconnect.

Unfortunately, many people start using hotspots without advanced planning, which leaves them extremely vulnerable. Hotspots are convenient and kind of cool in a nerdy way, but you must protect yourself if you are going to use what is, by design, a very open and unsecure medium. Unlike a home or business network, a hotspot is wide open to allow maximum use through the provider's network.

In this environment, security is second to access, so you need to take some precautions. Using a hotspot is a bit like being out in public: You don't go leaving your credit card lying around, speaking loudly about a confidential topic, or handing out spare keys to your house.

Keep these commonsense things in mind when using hotspots:

- Be aware of what hotspot you are connecting to. Use known, reputable services like those listed previously. Sometimes you get what you pay for; free sites are very attractive, but if they are provided by individuals and not businesses, you should eye these with great suspicion.
- Do not shop online or enter your credit card information into websites over a hotspot connection. Exercise caution when reading e-mail, using instant messaging programs (chat), and other forms of personal communication. Assume everything you read or type might be read by others sitting next to you.
- If you use a pay hotspot service, change the password to your account frequently. Someone can grab the user ID and password "off the air," and then use your subscription on your dime. When you are typing passwords, take a quick look around to make sure no one is looking over your shoulder (or over your fingers).
- Make sure your laptop is running a personal firewall program (such as ZoneAlarm) and an antivirus program (such as Norton AntiVirus, McAfee VirusScan, or Trend Micro PC-cillin). For a more thorough discussion on security, pick up a copy of *Home Networking Security Simplified*.
- Turn off ad hoc wireless networking. Chapter 9, "Wireless Security Setup," discusses how to do this. Turn off all file sharing while using your computer in a public place. In the off chance that someone does access your computer, don't make it easy on them by sharing your entire C: drive. (You should never do this anywhere, ever.)
- If you have the need to use hotspots frequently, ask your provider about using a Virtual Private Network (VPN) software program. These programs encrypt all communications between your laptop, through the hotspot access point, and up to the Internet. Boingo Wireless provides a VPN service included with a pay subscription. Eventually, all service providers should do the same. If you already have access to a VPN service through your employer, use it!



Note: One of the biggest security issues with PCs is laptop theft. A big problem using hotspots can be the logistics of a bathroom break. Having to disconnect and reconnect can be a pain. Taking the laptop with you to the bathroom is an option, but obviously that creates some other "logistics issues."

The bottom line is, if you are in a public place, treat your PC the same way you treat your wallet. Don't walk away from it, or it will walk away from you.

Following these simple steps should keep you plenty safe while using public hotspots, especially because the vast majority of folks don't take these measures, and hackers hit the easy targets first. We do realize that some of this might be a pain, but if you have ever lost data on a hard drive, or had your identity stolen (and had to deal with fixing your credit), you know that the pain of prevention is far, far less than the pain of getting burned by a hacker or thief.

So go out there and surf the Internet while sipping a cappuccino-coffee-hot milk thingy—you hip thing you—but protect yourself and your PC first.

Setting Up Your Own Portable Hotspot

Wireless networking is pretty addictive. After you start using it, you will find very quickly that when you have to switch back to a wired connection, you feel like someone just leg-cuffed you to a ball and chain.

Fortunately, availability of wireless connectivity is increasing at a dramatic pace. But still, there are a significant number of places where it is not available. For example, many higher-end business hotels are installing wireless networks throughout their hotels, including room access. However, others are installing wireless only in common areas such as the lobby, and rooms are still wired-only.

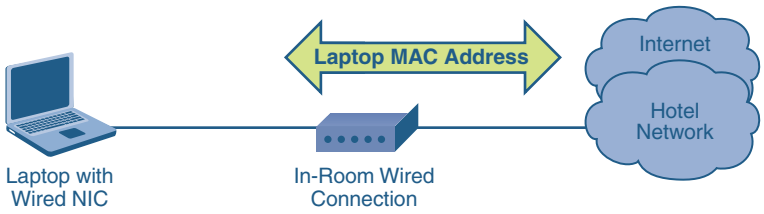
This can be fine. After all, do you really need wireless in your hotel room? Can you not just sit at the desk and use the wired connection? Well, maybe. But we are telling you, when you start using wireless, you will quickly forget how to plug in an Ethernet cable.

So what do you do if your favorite hotel, travel destination, family member you visit, and so on, does not have wireless access? The answer is: get a Linksys Wireless Travel Router.

How Wireless Travel Routers Work

Wireless travel routers essentially work just like your home wireless router, but they are more portable. When you use an Internet connection in a travel location, such as a hotel, what occurs is shown in Figure 14-17.

Figure 14-17 Wired Internet Access from a Hotel Room



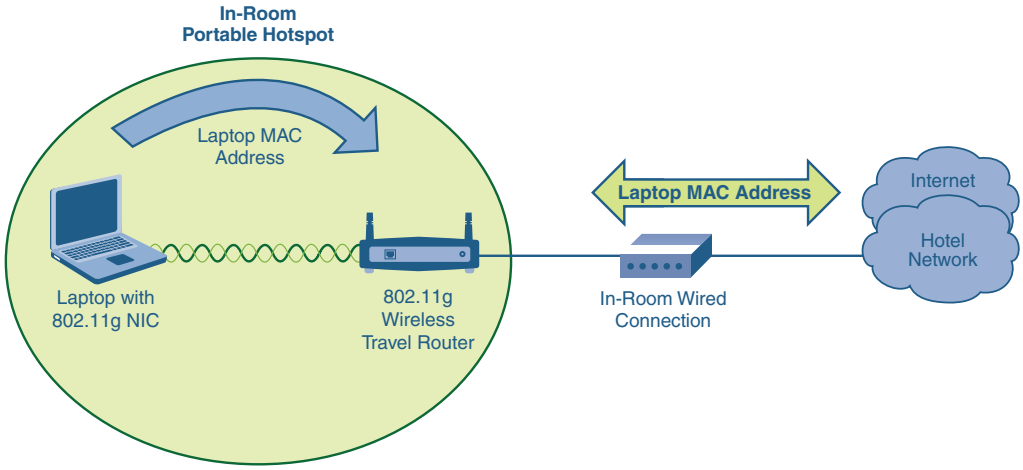
You connect your laptop to a wired Ethernet connection that is connected to the Internet through the hotel's network. You launch your Internet browser and are redirected to a membership page (very much like a wireless hotspot). After verifying your information, and possibly charging you a fee, your access is opened up and you can access the Internet.

How does the hotel network know that it is your laptop it needs to allow through to the Internet? It is based on your laptop's MAC address. As long as the hotel network sees that the traffic is coming from that MAC address, it is permitted and forwarded on to the network.

So now if we want to convert the wired connection to a wireless connection using a travel router, what needs to happen is shown in Figure 14-18.

We can simply connect the travel router to the wired connection instead of connecting the laptop to the wired connection. Then, the laptop can connect through the wireless router and onto the hotel network.

Figure 14-18 Wireless Travel Router in a Hotel Room



One very important point to remember is that the hotel network permission is based on the MAC address of our laptop. So, a critical function of the travel router is to be able to "clone" the laptop's MAC address and make the hotel network think that it is the laptop. It turns out that the Linksys Wireless Travel Router makes this extremely easy to do.



Note: Do not worry, the MAC cloning performed by the travel router is a perfectly legal thing to do. Essentially, it is just passing along the MAC address of your laptop's NIC to the hotel network.

After you establish a connection to the wireless router with the laptop, you can simply launch an Internet browser, get redirected, and enter the authorization or payment information, just as if you were connected over the wired connection. Very, very easy.

Setting Up a Wireless Travel Router

Before you travel, you want to set up the wireless travel router while you are still at home. This section explains the steps you need to take. Use the same laptop computer you plan to use when traveling, with a wired connection during the setup.

This example uses a Linksys WTR54GS Wireless-G Travel Router:

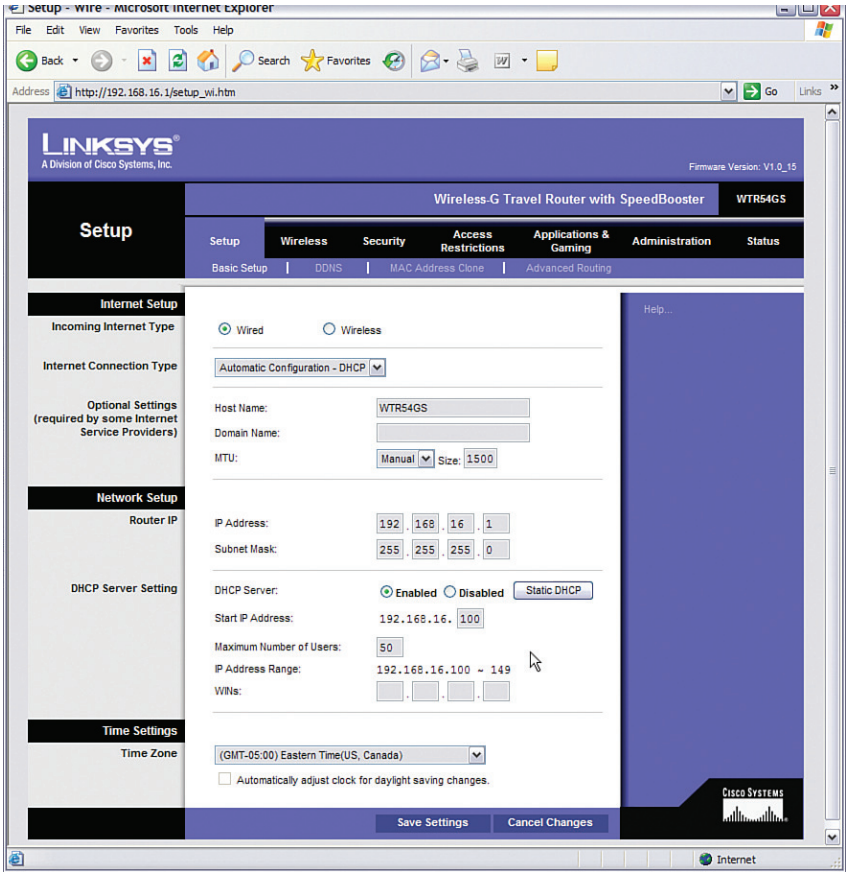
Step 1 Start an Internet browser and type the router's default address, **192.168.1.1**, into the Address field and hit **Enter**. When prompted for the username and password, leave the username blank and enter **admin** for the password.

Step 2 Click the **Setup** tab and the **Basic Setup** subtab, and set up the basic router setup information, as shown in Figure 14-19. Set the following parameters:

- Incoming Internet Type: **Wired**
- Internet Connection Type: **Automatic Configuration – DHCP**

Step 3 Click **Save Settings**.

Figure 14-19 Wireless Travel Router Basic Setup



Step 4 Click the **Wireless** tab and the **Basic Wireless Settings** subtab, as shown in Figure 14-20. Create an SSID for your travel router (see Chapter 6, "What to Buy," on how to choose SSIDs). For this example, we chose d92JdlPq. It is also a good idea to disable the SSID broadcast at this point. Click **Save Settings**.

Step 5 Click the **Wireless Security** subtab, as shown in Figure 14-21. We strongly recommend that you use either WPA or WPA2 wireless security, not WEP. For this example, we chose WPA-Personal, and created a WPA key of 3kD$df501nc0waZ. It is also a good idea to "tighten up" the key renewal period. The example here shows 300 seconds, or 5 minutes, for renewal. Click **Save Settings**.

Figure 14-20 Choose an SSID

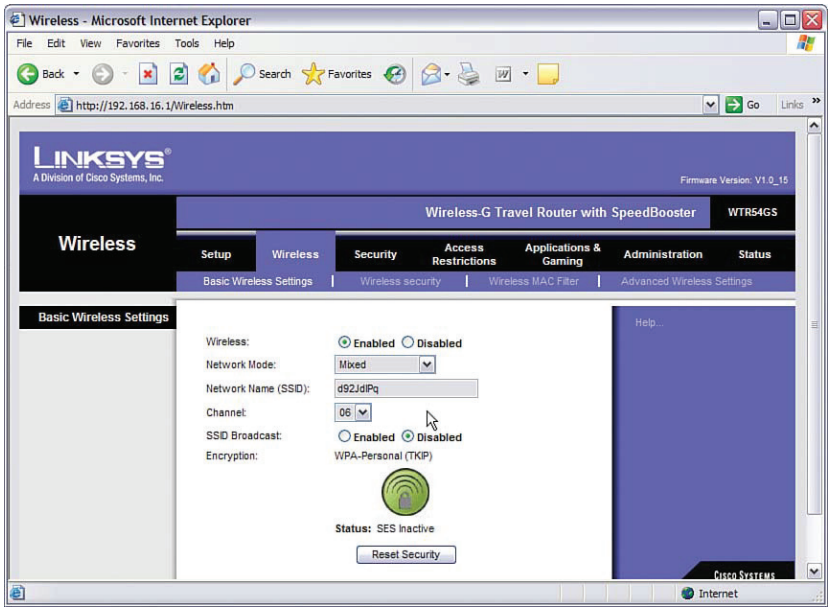
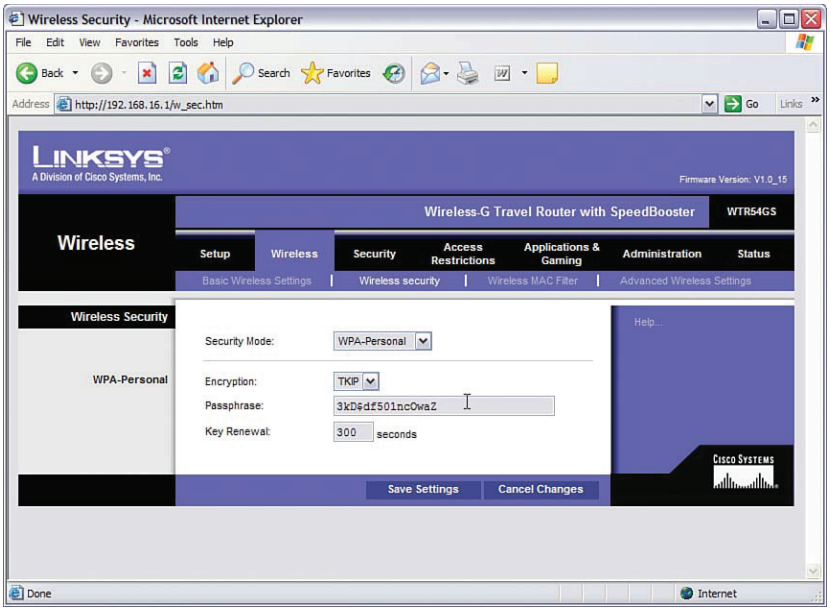
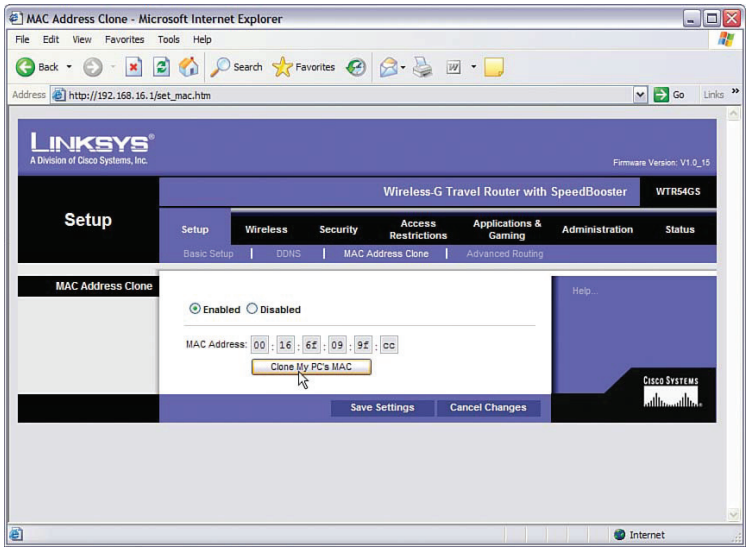


Figure 14-21 Turn on Wireless Security



Step 6 Click the **Setup** tab and the **MAC Address Clone** subtab, as shown in Figure 14-22. Click **Enabled** and then click the **Clone My PC's MAC** button. You should see the MAC Address field change from all 00s to the MAC address matching the wired NIC in your laptop. Click **Save Settings**.

Figure 14-22 Enabling MAC Address Cloning



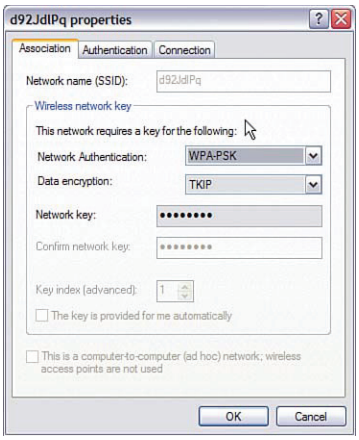
Step 7 Make sure to change the router's administration password.

Setting Up Your Laptop to See the Travel Router

Next, we need to create a wireless profile in the laptop for the wireless travel router. If you are using Windows Wireless Network Connection utility, choose **Start > Connect To > Show All Connections**. Select the wireless NIC and then click **Change Settings for This Connection**. Click the **Wireless Networks** tab and then click **Add**.

In Figure 14-23, we set the SSID to d92JdlPq, WPA-PSK as the network authentication method, and TKIP as the data encryption type. Then, we need to enter the WPA key twice, once in the Network Key field and again in the Confirm Network Key field. Take extra care to type in the WPA key exactly as we set it up on the travel router, paying attention to upper- and lowercase letters. For this example, we typed in a WPA key of 3kD$df501n0waZ. Click **OK** to save the settings.

Figure 14-23 Adding the Travel Router Profile in Windows XP



If we typed everything in correctly, the laptop should be able to connect to the wireless travel router. If it does not, then follow the troubleshooting suggestions in Chapter 10, "Troubleshooting: I Can't Connect at All."

Verify at home that you can connect to the wireless travel router with the laptop. You may even want to temporarily connect the travel router to your home broadband connection (through a wired connection on the home wireless router) to verify that you can reach the Internet on the laptop.

How to Use a Wireless Travel Router

When you have set up the travel router and laptop, using the travel router is very easy. Here is how:

Step 1 When you arrive at the location in which you need a portable wireless connection, plug the router into an electrical socket. The Linksys WTR54GS Wireless-G Travel Router has a plug built into the router instead of a cord, which is a very nice travel feature.

Step 2 Connect the Ethernet cable from the hotel's wired Internet connection to the port on the travel router marked "Internet."

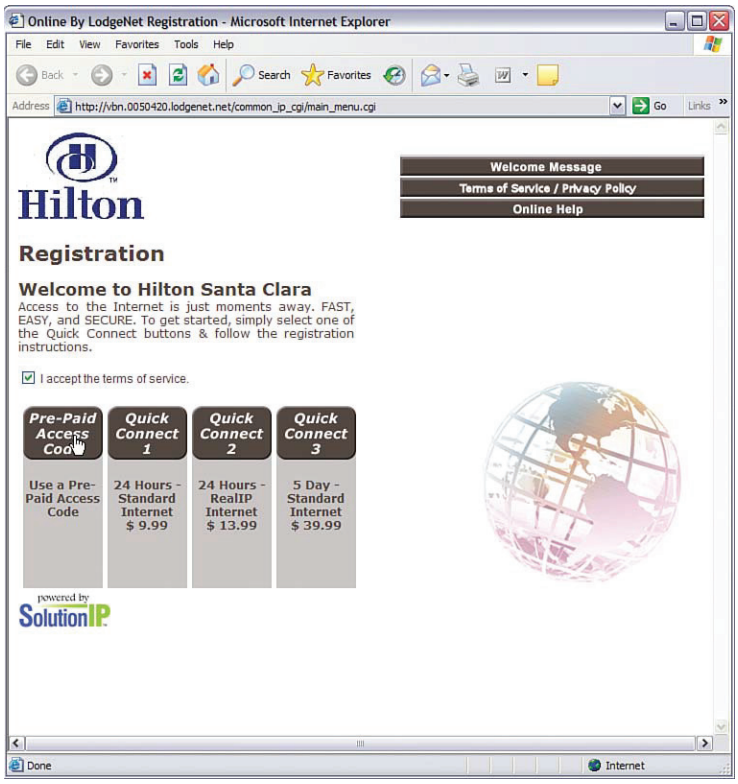


Tip: Pack your own Ethernet cable in the bag with your travel router. You cannot always count on a cable being in the hotel room.

Step 3 Turn the laptop on and use Windows XP (or your chosen wireless NIC manager) to connect to the wireless travel router.

Step 4 Launch your Internet browser. You should be redirected to the hotel's authorization page, such as the example shown in Figure 14-24. Enter the authorization code you received from the front desk, or click the appropriate pay option.

Figure 14-24 Hotel Connection Authorization Page Example



You should now be able to access the Internet over wireless within your hotel room. Coolness.

Summary

Wireless networking is addictive. When you use it at home, you will feel naked when you do not have wireless Internet access when you are away from home. Fortunately, there are many wireless hotspots where you can get connected when you travel. If you travel to a location that does not have a wireless hotspot, you can create your own portable hotspot with a wireless travel router. It's easy, and it's fun.

Where to Go for More Information

Microsoft provides an article titled "Tips for Working Securely from Hotspots" by Armelle O'Neal: www.microsoft.com/atwork/stayconnected/hotspots.mspx.

About.com offers an article titled "Top 10 Ways to Find a Hot Spot" by Catherine Roseberry: http://mobileoffice.about.com/od/locatinghotspots/tp/locatehotspot.htm.

For more information about JiWire, visit www.jiwire.com/.

For more information about T-Mobile HotSpot, visit http://hotspot.t-mobile.com/.

For more information about setting up security in your home network, check out our other book, *Home Network Security Simplified* (Cisco Press, 2006).

CHAPTER 15

The Future of Wireless Networking

The future of technology is always difficult to predict. Usually you get some pretty generic statements that do not really tell you anything, or wild predictions that are usually wrong and provide little insight for those trying to figure out if the $400 worth of stuff they just bought is going to be useless a year from now.

In this chapter, we try to give you some points to think about regarding where this technology is going in the near future (which we see as being 2 to 5 years out). We hope to avoid being too generic or making any wacky predictions. We see wireless networking evolving as follows:

- Wireless networks will be faster.
- Wireless networks will go farther.
- Wireless networks will be in more places.
- Wireless networks will move with you.
- More devices will connect to wireless networks.

This chapter explores each of these, including how it will affect your network and the stuff you just bought.

Wireless Networks Will Be Faster

There is no doubt that wireless users are addicted to speed. With perhaps the sole exception of security improvements, speed is where most of the R&D and engineering dollars get spent in companies that provide wireless equipment. The interesting thing is that most people's high-speed Internet connection is slower than the slowest wireless standard currently on the market (which is being phased out because consumers are demanding the faster standards).

Paying for extremely high speeds doesn't make sense unless you are using wirelessly enabled computers where the connections are faster (perhaps at the office or Internet cafés) or if you are using bandwidth-intensive applications within your network, such as music or video servers or head-to-head video or computer games. The funny thing is that most wireless users are not doing this, but folks are addicted to speed whether they are on the road or on their own network.

So, how fast will wireless home networks get? We are already up to 100 Mbps. That is as fast as most corporate wired computer networks have been for a couple of years. The next big jump would


Today.
The First Day
of the Rest
of Your Life.

then be to 1 Gbps (that's a billion bits per second), which is where corporate wired networks are moving today. But we don't think that home wireless networks will go that far any time soon (nor do they need to). They may double or triple in speed but we think that's about it. Given that most people have a hard time using up 54 Mbps with home-based applications, 300 Mbps should be a lot. Remember that if your downloads or uploads bog down, it's your broadband connection, not your wireless router, that is the choke point.

Another aspect of speed that will improve is latency, which is the delay of signals to and from the router. This improvement will have a big impact on the performance of online gaming and streaming video applications.

Wireless Networks Will Go Farther

Another aspect that is improving all the time with wireless networks is the range of wireless equipment. Most of the wireless routers claim that the usable distance is about 150 feet (for B, G, and A networks), but this is rarely achieved except in lab environments without obstructions such as floors or walls between the router and the computer. In the real world, the range is quite a bit less than that, and signal strength at that range is so low that the speed would noticeably drop. Even worse, the power drain would suck your laptop battery dry in no time.

The good news here is that the range is getting much better, and will continue to do so as more improvements come along, such as the 802.11n standard. The range will get a boost as computer manufacturers begin to embed 802.11n technology into the computer itself. This type of technology addition will improve range without decreasing battery performance. In others words, the distance that your computer will work away from your router will increase much faster than the rate your battery will drain due to the added power requirements of the wireless transmissions. If you are plugged in, even better.

So how far do we think it will go? The N standards claim a range of about 600 feet today (which we expect means about 300 to 400 or so in the real world). As the technology improves, we think the usable range (without signal-sucking obstructions such as metal framed buildings) could approach 800 to 1000 feet, which is great if you want to do e-mail from the neighborhood pool. By the way, this range will make turning on your security options even more important, because war-drivers who would usually sit in front of your house in a car will be able to access your network from around the block.

Wireless Networks Will Be in More Places

The general availability of wireless has been increasing for years from coffee shops to hotel rooms to airports. When it first appeared, it was always a pay-for-service model, but now many places are offering wireless connections for free. Now the race is on, as more and more places offer wireless access, and more and more of both the new and existing hotspots offer free access.

For any business that offers other types of services (such as hotels or coffee shops), the free wireless access is the hook that gets you to buy their coffee at a 5000 percent markup while you browse the

Internet. For business travelers, the choice between a hotel without wireless access and one with (even if the cost or quality of the hotel without is better) is almost an automatic decision.

The list of places offering wireless service is also growing to include RV parks, vacation resorts, and apartment complexes and underserved rural areas (no more dialup for those of you in the country). In addition, the phenomenon is growing in many countries, which is great if you are in Vietnam or Sri Lanka and want to check your e-mail. A good place to check for places with free wireless access is the Wi-Fi-FreeSpot Directory, at http://www.wififreespot.com.

The really interesting trend, though, is citywide free Wi-Fi, also known as muni Wi-Fi (short for municipality provided Wi-Fi). Several cities, including San Francisco, Portland, Chicago, and Philadelphia, are in various phases of planning or implementing citywide wireless networks. According to an article written by Michael Grebb at Wired.com, many city officials view free city-wide wireless as a form of public works, much like libraries and public schools. Others view city-wide wireless as a way to operate existing city services more cost effectively, such as meter reading, public safety, and city planning.

So, how far will it all go? The idea of coast-to-coast wireless is interesting, but it's a long, long way off. We do think that we will see a significant number of cities (both large and small) implement free wireless access in the next few years, despite the cost and complexity of implementing a network of that size. Some cities may offset the cost by asking people to agree to viewing advertising content while on the system. We think that within 3 to 5 years, many cities will either have it deployed or will be taking a serious look at it.

Wireless Networks Will Move with You

Most people think that wireless capability gives them the ability to be "mobile." To be specific, though, wireless in its current form allows portable access rather than mobile access. This means that you move to where you want to go and then you use your computer on the wireless system. When you want to go somewhere else, you disconnect your computer, move somewhere else, and then connect again. Many view this working model as "portable" or "nomadic" wireless access.

Our prediction is that in 3 to 5 years truly mobile wireless will start to become available. This means that while riding in a train, bus, or car (as a passenger only, please), you will be able to get connected and stay connected as you move from one place to another. The distance you can go and stay connected will be limited (usually to a city or along train routes between cities) but it will be a huge improvement, especially for long-distance commuters taking trains into major metropolitan areas.

One of the big difficulties that must be solved is roaming. Much like your cell phone, your computer will need to switch from access point to access point as you move between different coverage areas. The good news is that many of the technical issues here have long been solved by wireless companies. The bad news is that wireless ISPs (also known as WISPs) have a different cost structure, so some business issues (including roaming fees between companies) need to get sorted out. At this point, it's a toss up as to who will win: the current ISPs who have the speed and access or the mobile carriers who have the roaming (and billing) parts down. Chances are there will be consolidation in the form of mergers and acquisitions and both will win in parts.

By the way, some airlines (such as Germany's Lufthansa) offer Internet access on their flights today via satellite link, and more are expected to follow.

More Devices Will Connect to Wireless Networks

Probably the most significant change impacting wireless networks will be the number and types of devices that connect to it. A number of new devices have already come out, but these are network-specific types of gear like print servers and such.

In the next wave, we see all types of devices connecting to the network, including some obvious devices such as TVs, stereos, and digital recording devices (DVRs), but also appliances, home security systems, and electronics that can control home lighting, sprinkler systems, air conditioning, and answering machines.

Connecting these devices will have some pretty important implications on security and processing requirements for your wireless router. Because most routers are underutilized today, the processing power required should not be an issue. Even if processing power were an issue today, it wouldn't be an issue in 3 to 5 years given the pace of technology. Security is particularly important because in this scenario a hacker could really mess with you.

Having a handle on how this technology really works is also important. If you think it was annoying when the clock was blinking 12:00 on your VCR for 5 years, just wait until you have to upgrade the firmware on your toaster. That said, as manufacturers make it easier to connect, secure, and use this technology with tools such as EasyLink Advisor, adoption will increase.

Summary

This chapter provided not so timid but not too crazy predictions on where wireless networks are going. The capability for everything we mentioned in this chapter exists today. The issue is that the technology is too expensive. Technology costs are dropping all the time, however.

The real determining factor with wireless (and all technology for that matter) is its usefulness to the average consumer or business user. It is a rare event when a technology is broadly adopted within 5 to 10 years of its discovery. In fact, the history of fax machines, cellular phones, and the Internet suggests that the new technology adoption time frame is closer to 25 years than to 5. There are a lot of great "solutions" out there waiting for the right problem to come along. The day that the public demands wireless networking that is faster, goes further, exists in more places, moves with you, and connects to more stuff is the day someone will be standing there with a box that does it.

Where to Go for More Information

The Michael Grebb article for Wired is called "Cities Unleash Free Wi-Fi." You can find it at Wired.com: www.wired.com/news/technology/technology/wireless_special/0,68999-0.html.

This page intentionally left blank



Appendixes

APPENDIXES

Appendix A MAC Address Filtering

Appendix B 802.11n Wireless Channels

Appendix C 802.11 Additional Revisions

We end the book with a few appendixes. You do not need to read these unless you are curious about MAC address filtering, 802.11n wireless channels, or revisions to 802.11.

Appendix A, "MAC Address Filtering," shows you how to add MAC filtering to your wireless network security. MAC filtering can be a bit difficult to implement and maintain, so we chose not to make it a core part of the security steps you should take. Instead, it is offered as an optional security measure.

Appendix B, "802.11n Wireless Channels," contains a discussion on how the 802.11n standard uses wireless channels. If you want to set up a wireless network based on the 802.11n standard, it uses wireless channels differently from 802.11b or 802.11g.

Appendix C, "802.11 Additional Revisions," contains a list of other, lesser-known 802.11 standards. Most of them do not affect home networking, but they are included for completeness.

APPENDIX A

MAC Address Filtering

Just like a wired NIC, a wireless NIC also has a MAC address, which is a unique identification for every single NIC manufactured, much like a social security number or a set of fingerprints. It is possible to use MAC addresses as a security measure for your wireless network.

Because you know the MAC address for each wireless NIC you have purchased and planned to use on your network, it is possible to "lock" those into your wireless router and instruct it to let *only* those wireless NICs access your network. Then, if someone should try to access the wireless network using a laptop with a different NIC (that is, a different MAC address), the wireless router will deny access, even if the correct SSID and encryption key are provided.

Sounds great, right? Yes, but there is a trade-off. MAC address filtering can be difficult to manage and even harder to troubleshoot. Every time you add a new wireless NIC or another wireless device to your network, it won't work until you add the MAC address for it to the network. You receive no warning or reminder that you need to do so; the new device just won't work.

Another disadvantage occurs when a visitor, like a relative, comes to your house and wants to join your wireless network during her stay. You have to find out the MAC address for her wireless NIC and add it to your wireless router's permission table. Again, if you forget to do this, you and your visitor could spend hours trying to figure out why the laptop simply can't see your wireless network.



Note: MAC addresses can also be "spoofed" by hackers and clever users, so it's not a bulletproof solution, but it does add to your overall security if you choose to implement it.

Overall, we believe that the wireless security measures outlined in Chapter 9, "Wireless Security Setup," will make your wireless network secure enough about 99.77 percent of the time. If you want to spend the time (and potential frustration) to nail down the other 0.23 percent with MAC address filtering, this appendix is for you.

Enabling MAC Address Filtering

To enable MAC address flitering, you do not need to do anything on the computers with wireless NICs (or wireless devices) on the network. For the wireless router, it takes a couple steps.

First, make sure all the computers with wireless NICs (and devices) are configured for the wireless network (see Chapter 8, "Wireless NIC Setup") and the other security measures have been successfully turned on (see Chapter 9).

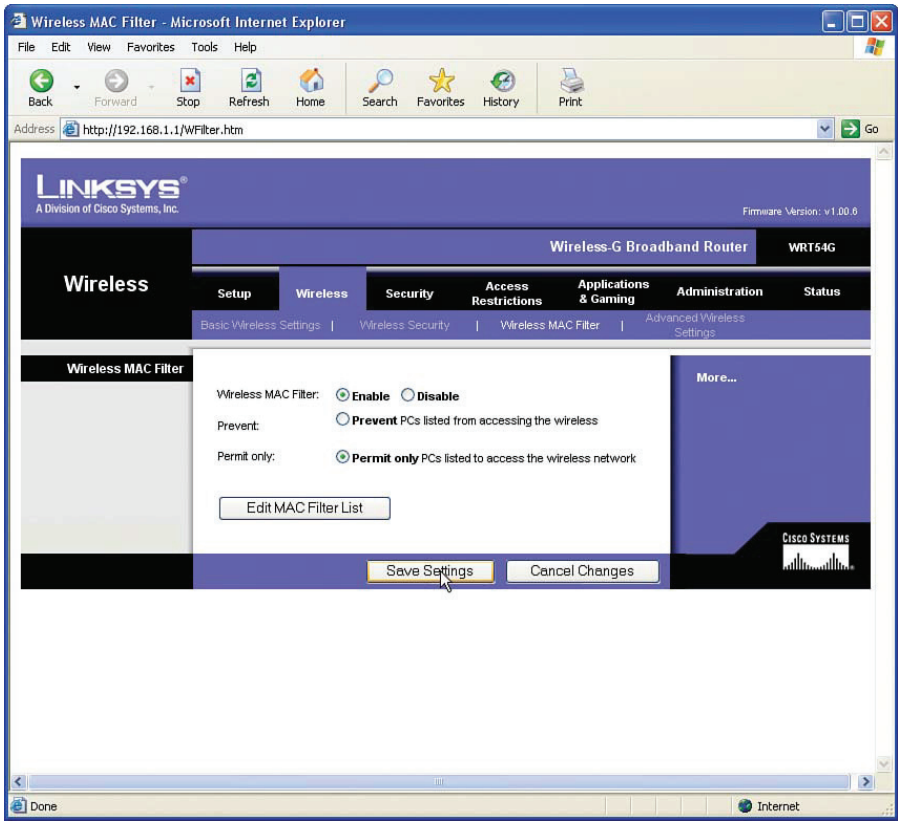
Then, access the router using your Internet browser as you have done before and perform the following steps:



Note: You will want to perform these steps from a computer that has a wired, not wireless, connection to the router. As soon as you do Step 1, your wireless NICs will not be able to access the wireless network any longer, until you complete Steps 2 and 3. However, you won't be able to do those steps because you have, as the saying goes, "sawed off the branch you were standing on" in Step 1.

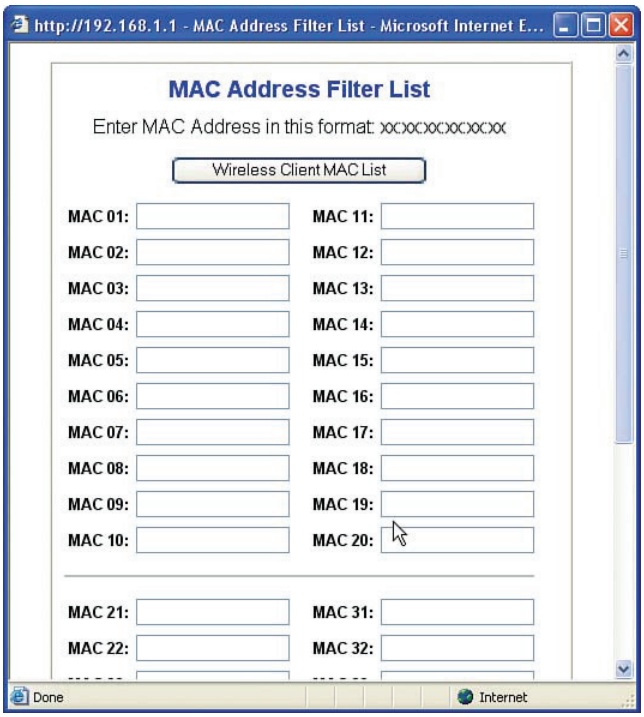
Step 1 Click the **Wireless** tab and click the **Wireless MAC Filter** subtab (see Figure A-1). (On some Linksys products, this is labeled Wireless Network Access.) Click **Enable** and select **Permit Only**. (On some Linksys products, this is labeled simply Restrict Access.) Click **Save Settings**.

Figure A-1 Enabling MAC Address Filtering



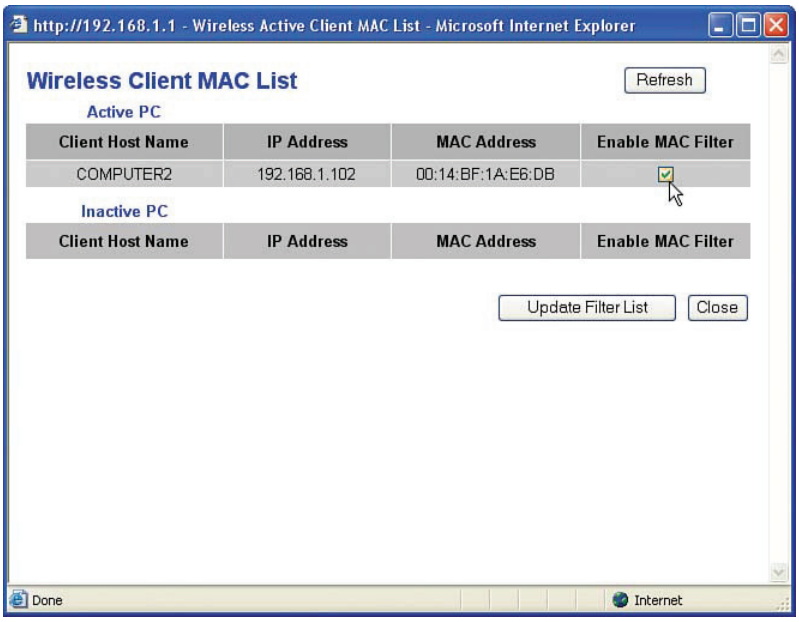
Step 2 Click the **Edit MAC Filter List** button. The MAC Address Filter List dialog box appears, but it is empty until we add addresses (see Figure A-2).

Figure A-2 Viewing the MAC Address Filter List



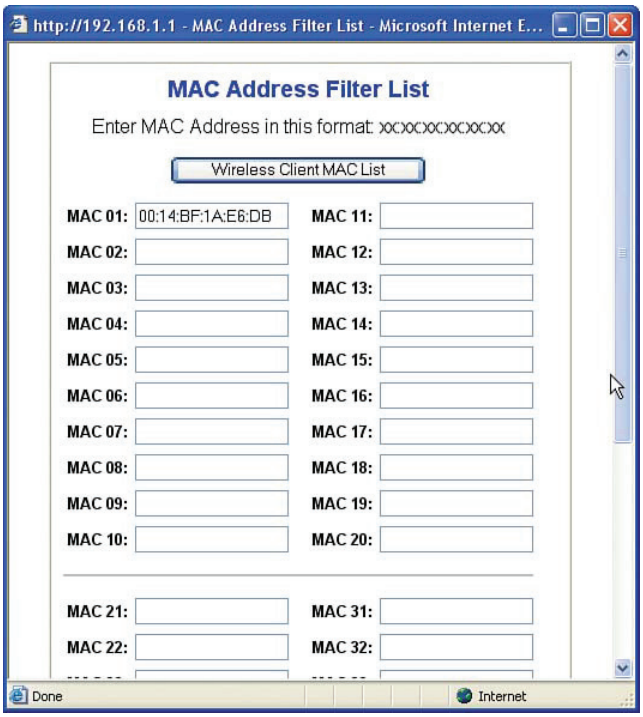
Step 3 Click the **Wireless Client MAC List** button. A list displays all the computers (by NIC) and their associated MAC addresses (see Figure A-3). Check each entry's check box in the **Enable MAC Filter** column. Click **Update Filter List** and then click **Close**.

Figure A-3 Adding a New MAC Address to the Filter List



Step 4 Back in the MAC Address Filter List dialog box (see Figure A-4), click **Save Settings**.

Figure A-4 Save the New MAC Filter List



Now the wireless network is "locked" to permit only our NICs to gain access. Check each of the computers with a wireless NIC to make sure it still can connect to the wireless router. If any of the computers can no longer connect, it is possible the MAC address for that computer did not make it into our "lock down" table.



Note: MAC address filtering only works for computers or devices trying to connect via wireless. A computer with a wired connection to the router will be able to connect even if the MAC address has been placed on the MAC Address Filter List.

Troubleshooting Tips for MAC Address Filtering

If any of the computers do not re-establish communication, check these items:

- Make sure the number of entries in the MAC address table on the wireless router is the same as the number of computers with wireless NICs in your network.
- Disable the MAC address restriction, reboot the computer that is not connecting properly, and see if it re-establishes a connection. If it does, repeat these instructions and add the “missing” MAC address from the computer.
- If all else fails, manually enter the MAC address for the computer’s wireless NIC. You can find the MAC address usually on a sticker label attached to either the NIC itself or the package it came in.
- Remember that if you upgrade your NIC or plug-in card, you need to update your MAC list with the new address because the list has the MAC address of the card and not the computer.

This page intentionally left blank

APPENDIX B

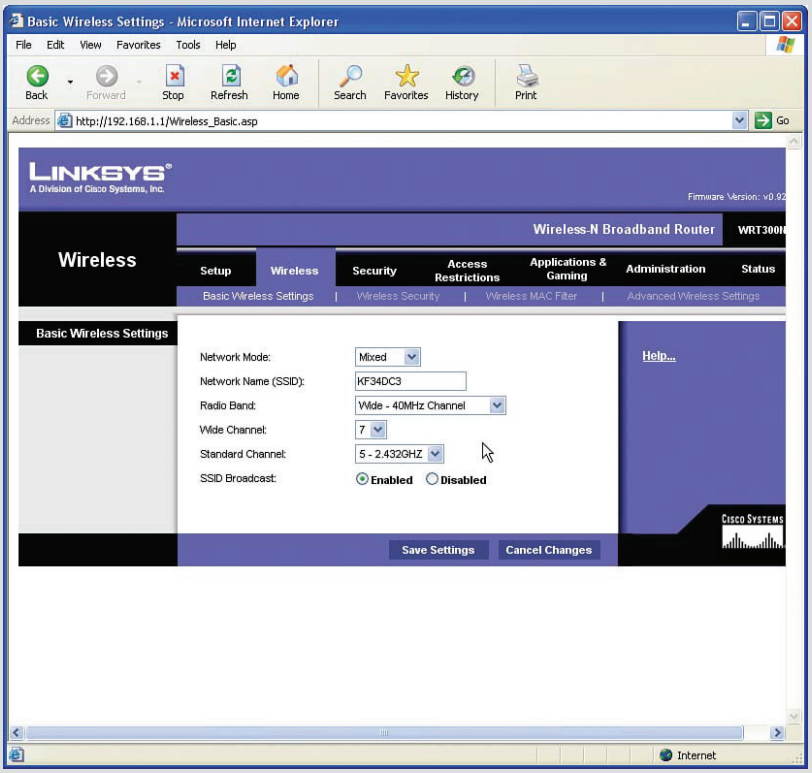
802.11n Wireless Channels

The 802.11n standard uses the same band (2.4 GHz) and channel plan (channels 1 through 11) as the 802.11b and 802.11g standards. However, 802.11n has two possible modes of operation: standard channel and wide channel. In the standard channel mode, 802.11n uses a single channel, very similar to 802.11b and 802.11g. In the wide channel mode, 802.11n uses a secondary channel to gain additional speed.

With the Linksys Wireless-N Broadband Router (WRT300N), you have the ability to choose between standard channel and wide channel modes. If you choose standard channel, then you are asked to select a wireless channel from 1 to 11, the same as 802.11b or 802.11g. In this case, the router acts like an 802.11g router, using only the single channel. In this mode you will not get the extra speed advantages of 802.11n wide channel mode.

If you choose wide channel, you are presented with the option to choose a wide channel as the primary channel and a standard channel as the secondary channel, as shown in Figure B-1.

Figure B-1 802.11n Wireless Channel Selection with the Linksys WRT300N Router



The Linksys WRT300N implementation of 802.11n restricts wireless channel selection to certain possible "pairs" of channels, as shown in Table B-1.

Table B-1 802.11n Primary to Secondary Channel Map

Channel	Possible Channel Pairs						
Primary (Wide)	3	4	**5**	6	**7**	8	9
Secondary(Std)	1 or 5	2 or 6	3 or 7	4 or 8	5 or 9	6 or 10	7 or 11

The default is wide channel mode, with channel 5 as the primary channel and channel 7 as the secondary channel.

When the 802.11n router is set to wide channel mode, wireless clients associate with the wireless router on the primary channel, and this channel is used during normal single-channel communications. When both the wireless router and the wireless NIC have 802.11n capability, they can additionally take advantage of the secondary channel to increase the data rate.

APPENDIX C

802.11 Additional Revisions

The following list outlines additional revisions to the 802.11 standard. Most of these revisions do not directly impact the home networking user.

- **802.11c, "Operation of Bridge Procedures"**—The 802.11c specification provides guidance for companies developing access points or hotspots.
- **802.11d, "World Wide Regulation Compliance"**—The IEEE created the 802.11d update to promote the widespread adoption of 802.11 by ensuring compliance with the regulations of more countries than the original standard. When the original 802.11 specification was written, only a few countries had regulations in place for wireless LAN transmissions. This amendment ensures that the rules for wireless LANs (WLANs) meet the restrictions of multiple countries. This specification was ratified in 2001.
- **802.11e, "QoS Enhancements"**—Quality of service (QoS) is a method for prioritizing certain types of traffic (for example, voice and video) that are prone to quality issues when delay occurs.
- **802.11f, "Access Point Roaming"**—802.11f provides rules for vendors to follow to ensure that computers that roaming (or switching) from one access point to another works, even when the access points are from different vendors. This enhancement was ratified in 2003.
- **802.11h, "802.11a Enhancements for Europe"**—802.11h addresses additional European regulatory requirements for the 802.11a standard. This was necessary because of the potential for 802.11a to interfere with satellite communications (which have priority on the frequencies in question). This enhancement was completed in 2003.
- **802.11i, "Security Improvements"**—802.11i is a security enhancement that makes it much more difficult for hackers to decipher wireless encryption keys. The original specification used static keys, which meant that hackers using automated programs (which could try millions of key combinations) would eventually stumble on the right key code. Once that happened, the user's security would be compromised. The updated standard (completed in 2004) addresses this issue and allows for dynamic key updates.
- **802.11j, "802.11a Enhancements for Japan"**—Much like the h update for Europe, the j update addresses regulations for the 5-GHz frequency band in Japan.
- **802.11k, "Radio Resource Measurement"**—802.11k provides rules for system management on commercial or enterprise network infrastructures.
- **802.11l (not used)**—The l standard was skipped due to possible confusion with the I standard (I and l look alike).

- **802.11m, "Documentation Upgrades"**—The 802.11m specification will update the documentation of the entire 802.11 standard.
- **802.11o (not used)**—The IEEE skipped 802.11o to avoid confusion with 802.110 (zero).
- **802.11p, "Wireless Access for the Vehicular Environment"**—This specification extends the 802.11 standard for use in moving vehicles and may be adopted in 2008.
- **802.11r, "Fast Roaming/Fast BBS Transition"**—This specification describes fast roaming support via Basic Service Set (BSS) transitions.
- **802.11s, "ESS Mesh Networking"**—This specification describes Extended Set Service (ESS) mesh networking for access points.
- **802.11t, "Wireless Performance Prediction"**—This specification describes wireless performance prediction (WPP) testing standards.
- **802.11u, "Interworking with External Networks"**—This specification describes internetworking with external networks such as 3G/cellular.
- **802.11v, "Wireless Network Management"**—This specification describes device configuration.
- **802.11w, "Protected Management Frames"**—The 802.11w specification provides security enhancements.
- **802.11y, "Contention Based Protocol"**—This specification describes interference avoidance.

GLOSSARY

2.4 GHz
Operating frequency shared by cordless telephones, wireless home networks (WLAN or Wi-Fi), and (unfortunately) microwave ovens and other devices that can cause interference.

5.8 GHz
Operating frequency for newer cordless telephones and wireless home networks (WLAN or Wi-Fi), with less interference (yet) from other devices.

802.11
IEEE working group and standards dealing with wireless networking.

802.11a
An IEEE wireless networking standard that specifies a maximum data transfer rate of 54 Mbps and an operating frequency of 5 GHz. Not compatible with 802.11b, 802.11g, or 802.11n.

802.11b
An IEEE wireless networking standard that specifies a maximum data transfer rate of 11 Mbps and an operating frequency of 2.4 GHz. Forward compatible with 802.11g and 802.11n.

802.11g
An IEEE wireless networking standard that specifies a maximum data transfer rate of 54 Mbps and an operating frequency of 2.4 GHz. Backward compatible with 802.11b and forward compatible with 802.11n.

802.11n
A fairly new IEEE wireless networking standard that specifies a maximum data transfer rate of 100 Mbps (and higher) and an operating frequency of 2.4 GHz. Backward compatible with 802.11b and 802.11g.

A

ad hoc mode
Refers to a wireless network that is computer to computer, without a wireless router.

Advanced Encryption Standard (AES)
A very secure encryption algorithm used as part of WPA2 wireless security encryption (and is also used for other types of data encryption).

B

bandwidth
The measure of how much data can be sent over a network connection, for example between your router and the broadband provider's network, at a point in time.

bit
Short for "binary unit"; this is a single digit of information, which is a 1 or 0.

broadband
A term used to describe high-speed Internet service. The term comes from the fact that a broad range of frequencies is used to attain high information exchange rates.

browser
A program used to access content on the Internet.

brute-force attack
Defeating a password or encrypted data by successively trying a large number of possibilities; for example, exhaustively trying password combinations using a dictionary attack program.

byte
A standard-size "chunk" of computer language or network information. A byte is made of 8 bits.

C

cable
A wire with connectors to connect two devices together. Also, the type of broadband service you get from your cable TV provider.

cable modem
A device that provides a broadband Internet connection to your home network by transmitting over the cable TV network.

chat
Instant messaging session where often there are three or more people involved.

D

delay
The length of time required to transmit packets from their origination point to their destination. Sometimes called latency.

denial of service (DoS) attack
An attack on a computer system or network that causes a loss of service to users, by consuming the bandwidth of the network or overloading the processor and memory of the computer system.

DHCP (Dynamic Host Configuration Protocol)
Protocol used by routers and similar network equipment to automatically assign IP addresses from a pool rather than assign permanent IP addresses to users.

Domain Name Service (DNS)
Fast computers at your ISP that can translate URLs (web links) into their actual IP addresses.

downlink
The connection and information flow from the service provider to your computer.

DSL (digital subscriber line)
A high-speed Internet connection that uses unused frequencies on phone lines to deliver very high data rates with the use of a specialized modem.

DSL modem
A device that provides a broadband Internet connection to your home network by transmitting over the public telephone network.

dynamic DNS
A service that tracks the dynamic IP address of your broadband connection and associates it with your own URL.

dynamic IP address
An IP address that is assigned by a device in the network (such as a wireless router for a private home network or a device at the ISP for public networks), which can change each time an address is requested. *See also* static IP address.

E

e-mail
An application used to exchange notes and files between two or more people. An e-mail address is identified by the username and the service provider, such as bob@network.com.

encryption
The manipulation of data to prevent accurate interpretation by all but those for whom the data is intended.

Ethernet
A protocol that defines the rules for computer communication over certain types of network cables and other physical media. It is the dominant protocol in use for both home and businesses.

F

firewall
A physical device or software program that prevents unwanted access into a private network from an outside location.

G

Gb (gigabit)
1 billion bits.

GB (gigabyte)
1,073,741,824 bytes.

GHz (gigahertz)
Measurement of a radio frequency equating to 1 billion cycles per second.

H

hack
A clever or elegant modification to computer software to gain unauthorized access or otherwise cause computer software to malfunction.

hacker
A person able to exploit a computer system or gain unauthorized access, usually by creating or modifying computer software.

hotspot
A wireless network available for use in a public place such as a coffee shop or airport.

HTTP (Hypertext Transfer Protocol)
The computer network protocol used to retrieve information from web pages written in certain "markup" languages.

I

IEEE
Institute of Electrical and Electronics Engineers, commonly pronounced "eye triple-e," is a group of professionals from many companies, governments, agencies, and so on that gets together to standardize different technologies.

infrastructure mode
A topology for deploying wireless networks in which a centralized "base station" (such as a wireless router) provides a common access point through which all computers and devices communicate.

Internet
The worldwide system of computer networks. Although many private networks connect to it, the Internet is public, cooperative, and self-sustaining.

IP (Internet Protocol)
Defines the communication rules for devices on the Internet. Communication within this protocol is based on the assignment of IP addresses.

IP address
Numerical address by which computers, web servers, and devices are known on the Internet. IP addresses have little bearing on geographic location.

ISP (Internet service provider)
A company that provides access to the Internet for residential or business use.

J–K-L

kilobit (Kb)
1000 bits. This is a standard transmission-rate unit for dialup modems when referred to over a portion of time such as kilobits per second (Kbps).

kilobyte (KB)
1024 bytes.

LAN (local-area network)
A small network within a house, department, or business.

loss
A measure of communication link quality, by measuring the number or percentage of packets that are lost between their origination point and destination.

M-N

MAC (Media Access Control) address
The unique physical serial number given by the manufacturer to every networking device used for network communication.

MAC address locking
A security measure for wireless networks whereby access through a wireless signal is restricted to specified MAC addresses, and others are rejected. Also called MAC filtering.

megabit (Mb)
1 million bits. When measured over time, this is the standard transmission-rate unit for high-speed modems, such as 2 megabytes per second (Mbps).

megabyte (MB)
1,048,576 bytes.

modem (modulator demodulator)
Device that translates computer language for transmission over a network media (phone line, cable, DSL, and so on) and back again.

Network Address Translation (NAT)

The technology by which a home router translates the private IP addresses used by computers on your home network into a single public IP address assigned to your broadband modem, providing the ability for multiple computers to share a connection, and also providing a degree of privacy because the computers on your home network are not able to be accessed directly from the Internet.

NIC (network interface card)

Provides the connection for a computer to either a wired or wireless network. Can be installed internally in the computer (PCI), connected externally to a USB port, or plugged into the PCMCIA slot of a laptop.

O-P

packet

A message containing data that is transmitted between an origination and destination in a network.

passphrase

Used much like a password, typically, to seed an ecryption key.

peer-to-peer

Another term for ad hoc wireless networking, whereby two computers establish a connection directly to each other without a wireless access point.

ping

Utility program on most PCs that can be used to test a network connection.

Point-to-Point Protocol over Ethernet (PPPoE)

Communication protocol commonly used on DSL broadband connections to communicate between your DSL modem and the DSL service hub.

Q-R

registry

A database that stores settings and options for the Microsoft Windows operating system, containing information and settings for all the hardware, software, users, and preferences of the PC.

RJ11

The connector on the end of a telephone cable, typically four wires, thinner than an Ethernet jack.

RJ45

The connector on the end of an Ethernet cable, typically eight wires, wider than a telephone jack.

router
A networking device that makes "intelligent" decisions regarding how traffic is moved across or through a network.

S

Skype
Popular free Internet-based voice chat service.

SSID (service set identifier)
A term used for the name of a wireless network.

SSID broadcast
An advertisement by a wireless router announcing its network's assigned SSID. Disabling SSID broadcasting can be one wireless networking security measure.

stateful packet inspection (SPI)
Examining each packet that flows through a firewall to make sure that the packet is both in response to a legitimate request by a computer on the home network and the correct packet in the expected sequence of packets.

static IP address
An IP address that is assigned by the ISP (or installed on a private home network) and that does not change. *See also* dynamic IP address.

T

TCP (Transmission Control Protocol)
A subset of the Internet Protocol (IP) set of rules to send data in the form of message units between computers over the Internet.

Temporal Key Integrity Protocol (TKIP)
A wireless encryption protocol that periodically changes the encryption key, making it harder to decode. Commonly used in WPA.

throughput
The amount of data moved successfully over a network connection, from one place to another in a given time period.

TiVo
A digital video recorder service that allows digital recording of live TV. Warning: The authors have found TiVo to be highly addictive.

U

uplink
The data flow from the computer to the service provider (and then to the Internet).

URL (uniform resource locator)
The official term for a link to a website or other material on the Internet; also known as the web address.

USB (Universal Serial Bus)
An interface that allows other devices to be connected and disconnected without resetting the system. Also a serial communication standard that allows high-speed data communication to many devices.

V

VoIP (voice over IP)
A protocol for transporting voice conversations across a data network. Also known as IP telephony.

VoIP chat
Using the Internet for voice conversations and phone calls, where there is typically no number to call but you reach others through their "handle," much like instant messaging. Online gaming systems, such as Xbox Live, often provide a voice chat feature for players to communicate during games.

W-X-Y-Z

WEP (Wired Equivalency Protocol)
Encryption security standard for 802.11-based wireless home networks.

Wi-Fi
A common reference to wireless networking; playing on the 1980s term for a high-fidelity (or Hi-Fi) stereo, Wi-Fi refers to wireless fidelity.

WiMax
A future wireless standard in the works that promises outdoor wide-area wireless networking, much like your cellular phone does today for voice.

WLAN
A wireless local-area network. *See also* LAN.

WPA (Wi-Fi Protected Access)

More recent encryption security standard for 802.11-based wireless home networks, considered more secure than WEP.

WPA2 (Wi-Fi Protected Access 2)

Latest encryption security standard for 802.11-based wireless home networks, considered more secure than WEP and WPA.

This page intentionally left blank

INDEX

A

access
- free Internet, 49
- hotspots
  - *Boingo, 305*
  - *configuring, 310-316*
  - *connecting, 299-300*
  - *Linksys WLAN Monitor, 300-301*
  - *membership tests, 305-308*
  - *searching, 297-298*
  - *services, 298-299*
  - *troubleshooting, 308-310*
  - *Windows XP, 302-304*
- networks, 328
- security, 47-50
  - *encryption, 52-55*
  - *SSID, 51*
- wireless access points, 11
- wireless video cameras, 268-275
- WPA, 53

ad hoc networks, 35, 54-55

adapters, wireless games, 282-283

adding
- computers, 114-120
- encryption, 123-135, 137
  - *Linksys EasyLink Advisor, 150-162*
  - *Linksys SES, 142-150*
  - *troubleshooting, 167*
  - *WPA, 137, 140-141*

addresses
- IP
  - *assigning, 177, 180, 210-216*
  - *dynamic, 277*
- MAC
  - *enabling filtering, 327*
  - *locking, 166*
  - *troubleshooting filtering, 329*

administration, passwords, 55. *See also* passwords

Advanced Encryption Standard. *See also* AES

advertising, stopping, 163

AES (Advanced Encryption Standard), 53

applications
- Linksys EasyLink Advisor, 91-98
- Viewer Client, 271-275

assigning
- IP addresses, 177, 180, 210-216
- IP ports, 275

associating
- NICs with routers, 105-111, 113-120
- routers, 176, 180, 193-195

attenuation, 187

authentication, 176, 209

automatic speed negotiation, 245-247

availability, future of, 319-320

avoiding proprietary extensions, 58

B

bad signals, verifying Windows XP, 246

base stations, 11

Boingo monitor, 252

Boingo utility, 305

bottlenecks, 239-242

broadband connections
- speed, 243
- testing, 239-242
- upgrading from dial-up, 75

broadcasts
- SSID settings, 51
- troubleshooting, 192-193

browsers. *See also* interfaces
- connections, 181-183
- routers, 84-90

C

cables. *See also* connections
- Ethernet, 263
- overview of, 4
- routers, 78

cameras, 259
- accessing, 268-275
- configuring as motion detectors, 277-279
- connecting, 263-268
- troubleshooting, 277
- uses of, 261-262
- viewing, 271, 276

cards, laptops, 59

channels
IEEE 802.11n standard, 331-332
interference
cordless phones, 252-254
troubleshooting, 248-251
characters, WEP passphrases, 125
clients, troubleshooting, 215-216
CNET.com, 67
combinations of standards, 21
comparing ExpressCards/PCMCIA, 59
compatibility
cordless phones, 252-254
standards, 24-26
computers
adding, 114-120
capabilities, 40-41
USB wireless NICs, 103-104
configuring
DVRs, 289
Encryption, 123-137
Linksys EasyLink Advisor, 150-162
Linksys SES, 142-150
Troubleshooting, 167
WPA137, 140-141
hotspots, 310-316
NICs99
associating with routers, 105-111, 113-120
installing, 99-104
routers, 75-77
connecting, 74-75
Internet browsers, 84-90
Linksys EasyLink Advisor, 91-98
Linksys Setup Wizard, 77-84
viewing wireless camera images, 274-275
topologies, 6
wireless online gaming, 282-283
wireless video cameras, 277-279
connections, 11-12
DVRs, 288-292
configuring, 289
uses of, 289
future of, 317
availability, 319-320
devices, 321
portability, 320
range, 319
speed, 317
hotspots, 299-300
Boingo, 305
configuring, 310-316
Linksys WLAN Monitor, 300-301
membership tests, 305-308
troubleshooting, 308-310
Windows XP, 302-304
Linksys Setup Wizard, 80
managing, 108-120
NICs
wired, 40
wireless, 40-41
overview of, 4
profiles, 106-108
routers, 74-75
security, 52-55
slow
degraded signals, 248-254
speed tests, 243
testing broadband connections, 239-242
troubleshooting, 239-245
verifying speed, 245-247
SSID, 51
Troubleshooting, 174-181, 218
assigning IP addresses, 177, 180, 210-216
associating, 176, 180, 193-195
detecting, 181-183
matching, 176-179, 189, 192-193
scanning, 176-178, 184-188
securing, 176, 180, 196-204, 206-209
testing, 216-217
Wi-Fi, 10-11
wireless online gaming, 281-288
wireless video cameras, 263-268
consoles, wireless online gaming, 284-285
cordless phones, interference, 252-254
costs
hotspots, 298-299
standards, 29
customizing routers, 76

D

data rates, 10
decoding keys, 52
default channels
cordless phones, 252-254
troubleshooting, 248-251
degrading signals, 248-254
desktops. *See also* computers
NICs, 101-102
PCI wireless cards, 101-102
USB wireless NICs, 103-104
detecting connections, 181-183

devices
future of, 321
interference, 252-254
purchases, 57
determining readiness, 57-61
selecting NICs, 63-65
selecting routers, 62-63
travel routers, 65-66
where to, 67-69
standards
IEEE 802.11, 16, 333-334
IEEE 802.11a, 17
IEEE 802.11b, 18
IEEE 802.11g, 19-20
IEEE 802.11n, 20-21, 331-332
wireless online gaming, 279
connecting, 281-288
options, 280-281
servers, 280
wireless video cameras, 259
accessing, 268-275
configuring as motion detectors, 277-279
connecting, 263-268
troubleshooting, 277
uses of, 261-262
viewing, 271, 276
DHCP (Dynamic Host Configuration Protocol), 210, 215-216
dial-up connections, upgrading to broadband, 75
digital video recorders. *See also* DVRs
disabling ad hoc networks, 54-55
drivers, war-drivers, 49. *See also* devices
dual-band products, 26
DVRs (digital video recorders), 288
configuring, 289
connecting, 290-292
uses of, 289
Dynamic Host Configuration Protocol. *See also* DHCP
dynamic IP addresses, 277

E

e-mail, overview of, 7
EasyLink Advisor, 76, 91-98
connections, 113-120
encryption, 150-162
enabling
encryption, 126-127
Linksys EasyLink Advisor, 150-162
Linksys SES, 142-143, 150
NICs, 130-137
Routers, 128-129
WPA, 137-141
firewalls, 164
MAC address filtering, 327-329
NICs, 185-186
encoding keys, 52
encryption, 52-55. *See also* security
configuring123-137
connections, 196-197, 199-209
Linksys EasyLink Advisor, 150-162
Linksys SES, 142-150
standards, 28-29
troubleshooting, 167
WPA137, 140-141
entering SSIDs, 82
episodes (TV), recording, 291. *See also* DVRs
Ethernets, 17, 263. *See also* connections
ExpressCards, 59
extending VoIP, 60
extensions, proprietary, 27, 58

F-G

filters (MAC addresses)
enabling, 327
troubleshooting, 329
firewalls. *See also* security
enabling, 164
encryption, 28-29
forwarding ports, 274
free Internet access, 49
frequency, unregulated ranges, 17
future of wireless networking, 317
availability, 319-320
devices, 321
portability, 320
range, 319
speed, 317

games, 279
connecting, 281-288
options, 280-281
servers, 280
good signals, verifying Windows XP, 246

H

hackers, war-drivers, 49. *See also* security
hotspots, 295-297
Boingo, 305
configuring, 310-316
connecting, 299-300
Linksys WLAN Monitor, 300-301
membership tests, 305-308
searching, 297-298
services, 298-299
troubleshooting, 308-310
Windows XP, 302-304

I-K

IEEE (Institute of Electrical and Electronic Engineers) standards
combinations of, 21
comparing to WLAN, 30-31
compatibility, 24-26
cost, 29
IEEE 802.11, 16, 333-334
IEEE 802.11a, 17
IEEE 802.11b, 18
IEEE 802.11g, 19-20
IEEE 802.11n, 20-21, 331-332
range, 28
security, 28-29
selection of, 23-24
speed, 27-28
images (wireless video cameras)
troubleshooting, 277
viewing, 271, 276
incoming messages, 7
incompatible standards, 184-185
infrastructure, 35
installing
NICs, 99-104
wireless video cameras, 263-268
Institute of Electrical and Electronic Engineers. *See also* IEEE standards
interfaces
connections, 181-183
NICs, 99
routers, 84-90
USB, 58
interference, 10, 17
cordless phones, 252-254
planning, 38
routers, 248-251
Internet
broadband connections
speed tests, 243
testing, 239-242
browsers, 84-90
connections, 80
images
troubleshooting, 277
viewing, 271-276
Wi-Fi, 305. *See also* Wi-Fi
wireless online gaming, 279
connecting, 281-288
options, 280-281
servers, 280
Internet Explorer, detecting connections, 181-183
Internet Protocol. *See also* IP
Internet service provider. *See also* ISP
Interoperability, 10
IP (Internet Protocol)
addresses
assigning, 177, 180, 210-216
dynamic, 277
ports, 275
ISP (Internet service provider), 7

keys
encryption, 52
mismatch, 197-208
selecting, 53-54
PSKs, 125
renewal periods, 137
WEP, 125

L

LANs (local area networks)
connections, 11-12
overview of, 4-11
laptops
cards, 59
hotspots, 302
NICs, 99
PCMCIA cards, 102-103
travel routers, 314
TV episodes, 291
layouts, planning networks, 37-39
leeching onto networks, 49
limitations of IEEE 802.11g, 19

Linksys. *See also* routers
EasyLink Advisor, 91-98
configuring encryption, 150-162
managing connections, 113-120
SES, 142-150
Setup Wizard, 76-84
wireless game adapters, 282-283
Wireless-N Broadband Router (WRT300N), 331
WLAN Monitor, 111-113, 300-301
WLAN utility, 131-132
local area networks. *See also* LANs
locking
MAC addresses, 166
Networks, 328

M

MAC (Media Access Control) addresses
enabling filtering, 327
locking, 166
troubleshooting filtering, 329
management
connections, 108-118, 120
profiles, 106-108
manually configuring encryption, 127
maps, channels, 332
matching SSIDs, 176, 179, 189-193
Mbps (megabits per second), 16
megabits per second. *See also* Mbps
membership tests, hotspots, 305-308
messages, 7. *See also* e-mail
methods, encryption, 53
Microsoft Xbox, 280. *See also* wireless online gaming
MIMO (multiple inputs, multiple outputs), 20
mismatch (encryption)
keys, 197-208
type, 196-206
modes, IEEE 802.11n standard, 331-332
monitoring
Boingo monitor, 252
Linksys WLAN Monitor, 300-301
motion detectors, configuring video cameras as, 277-279
multiple inputs, multiple outputs. *See also* MIMO

N

negotiation, automatic speed, 245-247
networks
computer capabilities
wired NICs, 40
wireless NICs, 40-41
connecting
assigning IP addresses, 177, 180, 210-216
associating, 176, 180, 193-195
detecting, 181-183
matching, 176, 179, 189-193
scanning, 176, 178, 184-188
securing, 176, 180, 196-209
testing, 216-217
troubleshooting, 174-181, 218
connections
degraded signals, 248-254
slow, 239, 244
speed tests, 243
testing broadband connections, 239-242
upgrading routers, 244-245
verifying speed, 245-247
disabling, 54-55
DVRs, 288
configuring, 289
connecting, 290-292
uses of, 289
encryption
configuring, 123-137
Linksys EasyLink Advisor, 150-162
Linksys SES, 142-150
troubleshooting, 167
WPA, 137-141
future of, 317
availability, 319-320
devices, 321
portability, 320
range, 319
speed, 317
hotspots, 295-297
Boingo, 305
configuring, 310-316
connecting, 299-300
Linksys WLAN Monitor, 300-301
membership tests, 305-308
searching, 297-298
services, 298-299
troubleshooting, 308-310
Windows XP, 302-304
layouts, 37-39

locking, 328
purchases, 57
determining readiness, 57-61
selecting NICs, 63-65
selecting routers, 62-63
travel routers, 65-66
where to, 67-69
readiness, 44
security, 47-50
enabling firewalls, 164
encryption, 52-55
optimizing, 162
preventing roaming, 164-165
SSID, 51
stopping advertising, 163
topologies, 35-37
wireless online gaming, 279
connecting, 281-288
options, 280-281
servers, 280
wireless video cameras
accessing, 268-275
configuring as motion detectors, 277-279
connecting, 263-268
troubleshooting, 277
viewing, 271, 276
worksheets, 43-44

NICs (network interface cards)
compatibility, 25
configuring, 99
associating with routers, 105-114, 117-120
installing, 99-104
connecting
assigning IP addresses, 177, 180, 210-216
associating, 176, 180, 193-195
detecting, 181-183
matching, 176-193
scanning, 176-188
securing, 176, 180, 196-209
testing, 216-217
troubleshooting, 174-181, 218
encryption
configuring, 123-137
Linksys EasyLink Advisor, 150-162
Linksys SES, 142-150
troubleshooting, 167
WPA, 137-141
hotspots
Boingo, 305
configuring, 310-316
connecting, 299-300
Linksys WLAN Monitor, 300-301
membership tests, 305-308
troubleshooting, 308-310
Windows XP, 302-304
locking, 328
proprietary extensions, 27
readiness, 57-61
selecting, 63-65
standards
costs, 29
ranges, 28
security, 28-29
speed, 27-28
topologies, 36
upgrading, 244
wired, 40
wireless, 40-41

O

omnidirectional signals, 47

optimizing
connections
degraded signals, 248-254
slow, 239, 244
speed tests, 243
testing broadband, 239-242
upgrading routers, 244-245
verifying speed, 245-247
security, 162
enabling firewalls, 164
preventing roaming, 164-165
stopping advertising, 163

options
hotspots, 298-299
routers, 76
wireless online gaming, 280-281

P

packets
firewalls, 164
SPI, 29

passphrases
generators, 53
selecting, 128
WEP, 125

passwords
routers, 80
wireless video cameras, 269

PCI wireless cards, installing on desktops, 101-102

PCMCIA (Personal Computer Memory Card International Association), 59-60, 102-103
peer-to-access point networks, 35
peer-to-peer networks, 35
performance, compatibility, 26
Personal Computer Memory Card International Association. *See also* PCMCIA
ping utility, 241. *See also* testing
planning
networks
computer capabilities, 40
layouts, 37-39
readiness, 44
topologies, 35-37
wired NICs, 40
wireless NICs, 40-41
worksheets, 43-44
purchases, 57
determining readiness, 57-61
NICs, 63-65
selecting routers, 62-63
travel routers, 65-66
where to, 67-69
pools, troubleshooting, 215-216
portability, 320
ports. *See also* connections
forwarding, 274
IP, 275
power of transmissions, 10
preshared keys. *See also* PSKs
preventing roaming, 164-165
primary channels, 332
privacy, WEP, 52
profiles, 106-108, 110-120
proprietary extensions, 27, 58
protocols
DHCP, 210, 215-216
Ethernet, 7
IP. *See also* IP
TKIP, 53
providers, connecting to online games, 285-288
PSKs (preshared keys)125
purchases (planning), 57
determining readiness, 57-61
selecting NICs, 63-65
selecting routers, 62-63
travel routers, 65-69

R

radio frequency. *See also* RF
ranges
future of, 319
standards, 28
transmissions, 10
unregulated frequency, 17
readiness
determining, 57-61
planning networks, 44
recording, DVRs, 291. *See also* DVRs
relationships, wireless standards, 25
renewal periods, keys, 137
Repair function (Windows XP), 214
revisions, IEEE 802.11 standards, 333-334
RF (radio frequency), 9-10
ring topology, 6
roaming, preventing, 164-165
routers, 6
associating, 176, 180, 193-195
broadband connections
speed, 243
testing, 239-242
compatibility, 26
configuring, 74-77
connections, 4, 11-12
encryption
configuring, 123-137
Linksys EasyLink Advisor, 150-162
Linksys SES, 142-150
troubleshooting, 167
WPA, 137, 140-141
extensions, 27
interference, 248-251
Internet browsers, 84-90
Linksys EasyLink Advisor, 91-98
Linksys Setup Wizard, 77-84
NICs, 105-114, 117-120
passwords, 80
purchases, 57
selecting, 62-63
travel, 65-66, 310-316
upgrading, 244-245

S

saving router configuration settings, 83
scanning signals, 176, 178-188
scrambling signals, 52-55

searching for hotspots, 297-298
secondary channels, 332
SecureEasySetup. ***See also*** **SES**
Security, 47-50
connections, 176, 180, 196-209
encryption, 52-55
configuring, 123-137
Linksys EasyLink Advisor, 150-162
Linksys SES, 142-150
troubleshooting, 167
WPA, 137-141
hotspots
Boingo, 305
configuring, 310-316
connecting, 299-300
Linksys WLAN Monitor, 300-301
membership tests, 305-308
troubleshooting, 308-310
Windows XP, 302-304
optimizing, 162
enabling firewalls, 164
preventing roaming, 164-165
stopping advertising, 163
SSID, 51
standards, 28-29
wireless video cameras
accessing, 268-275
configuring as motion detectors, 277-279
troubleshooting, 277
viewing, 276
selection
encryption keys, 53-54
IEEE 802.11n wireless channels, 331-332
NICs, 63-65
routers, 62-63
standards, 23-24
compatibility, 24-26
cost, 29
range, 28
security, 28-29
speed, 27-28
travel routers, 65-66
WEP passphrases, 128
servers, wireless online gaming, 280
Service Set Identification. ***See also*** **SSID**
services, hotspots, 298-299
SES (SecureEasySetup), 142-150
Setup Wizard, 263
setup. ***See also*** **configuring**
signals
Boingo monitor, 252
degrading, 248-254
omnidirectional, 47
RF, 9-10
scrambling, 52-55
scanning, 176, 178-188
troubleshooting, 187-188
Windows XP, 246
slow connections, 239, 244
degraded signals, 248-254
speed tests, 243
testing broadband connections, 239-242
upgrading routers, 244-245
verifying speed, 245-247
snooping, 8
SoloLink, 277
speed
broadband connections, 243
future of, 317
overview of, 244-245
standards, 27-28
verifying, 245-247
Speed Booster, 19, 58
SPI (stateful packet inspection), 29, 164
SSID (Service Set Identification), 11, 51
entering, 82
hotspots, 299-300
matching, 176, 179, 189-193
standard channel, 331-332
standards, 16
AES, 53
combinations of, 21
IEEE 802.11, 16, 333-334
IEEE 802.11a, 17
IEEE 802.11b, 18
IEEE 802.11g, 19-20
IEEE 802.11n, 20-21, 331-332
incompatible, 184-185
overview of, 244-245
selection of, 23-24
compatibility, 24-26
cost, 29
range, 28
security, 28-29
speed, 27-28
WLAN, 30-31
starting Linksys Setup Wizard, 78
stateful packet inspection. ***See also*** **SPI**
static IP addressing, 211

stopping advertising, 163
strength, troubleshooting signals, 187-188
surveillance, 261, 277-279
switches, 6

T

T-Mobile, connecting, 307. *See also* hotspots
telephones, troubleshooting interference, 252-254
Temporal Key Integrity Protocol. *See also* TKIP
testing
broadband connections, 239-243
connections, 216-217
hotspots, 305-308
TiVo, 288
configuring, 289
connecting, 290-292
TiVoToGo, 291
uses of, 289
TKIP (Temporal Key Integrity Protocol), 53
tools
Boingo, 252, 305
Linksys WLAN Monitor, 111-113, 300-301
Linksys WLAN utility, 131-132
ping, 241. *See also* testing
Windows Wireless network Connection utility, 109
Windows XP, 135-137
topologies
overview of, 6
types of, 35-37
transferring TV episodes (DVRs), 291
transmissions, power of, 10
travel routers, 65-66, 310-316
troubleshooting
connections, 174-181, 218
assigning IP addresses, 177, 180, 210-216
associating, 176, 180, 193-195
degraded signals, 248-254
detecting, 181-183
matching, 176, 179, 189-193
scanning, 176-178, 184-188
securing, 176, 180, 196-209
slow, 239, 244
speed tests, 243
testing, 216-217, 239-242
upgrading routers, 244-245
verifying speed, 245-247
cordless phones, 252-254
encryption, 167
hotspots, 308-310
MAC address filtering, 329
router interference, 248-251
wireless video cameras, 277
types
of encryption mismatch, 196-206
of NICs, 99
of topologies, 35-37
of wireless connection managers, 108

U

unregulated frequency ranges, 17
upgrading
dial-up connections to broadband, 75
NICs, 244
overview of, 244-245
routers, 244-245
USB (universal serial bus). *See also* connections
interfaces, 58
NICs, 103-104

V

verifying speed, 245-247
video
DVRs, 288
configuring, 289
connecting, 290-292
uses of, 289
wireless cameras, 259
accessing, 268-275
configuring as motion detectors, 277-279
connecting, 263-268
troubleshooting, 277
uses of, 261-262
viewing, 271, 276
Viewer Client, 271-275
viewing wireless video cameras, 271, 276
VoIP (Voice over IP), 17, 60
vulnerabilities, 50. *See also* security

W

W-Fi hotspots, 295-297
Boingo, 305
configuring, 310-316
connecting, 299-300
Linksys WLAN Monitor, 300-301
membership tests, 305-308
searching, 297-298
services, 298-299
troubleshooting, 302-310

war-drivers, 49
web sites, CNET.com, 67
WEP (Wired Equivalent Privacy), 52
keys, 125, 197-203
NICs, 130-137
passphrases, 125, 128
routers,128-129
Wi-Fi Protected Access. *See also* WPA
wide channel, 331-332
Windows XP
authentication, 209
hotspots, 302-304
Repair function, 214
speed, 246
WEP encryption, 135-137
Wired Equivalent Privacy. *See also* WEP
wired NICs, 40
wireless access points, 11
wireless devices
standards
IEEE 802.11, 16, 333-334
IEEE 802.11a, 17
IEEE 802.11b, 18
IEEE 802.11g, 19-20
IEEE 802.11n, 20-21, 331-332
wireless hotspots, 295-297
Boingo, 305
configuring, 310-316
connecting, 299-300
Linksys WLAN Monitor, 300-301
membership tests, 305-308
searching, 297-298
services, 298-299
troubleshooting, 308-310
Windows XP, 302-304
wireless LAN. *See also* WLAN
wireless networks, 317
availability, 319-320
devices, 321
portability, 320
range, 319
speed, 317
wireless NICs, 40-41
wireless online gaming, 279
connecting, 281-288
options, 280-281
servers, 280
wireless profiles, 106-108, 110-120
Wireless Security Wizard, 152
wireless travel routers, 310-316
wizards
Setup, 263
Wireless Security Wizard, 152
WLAN (wireless LAN)
connections, 11-12
Linksys Monitor, 111-113
Linksys WLAN Monitor, 300-301
overview of, 4-11
standards, 30-31
worksheets, planning networks, 43-44
WPA (Wi-Fi Protected Access), 53
enabling, 137, 140-141
preshared key mismatch, 207-208
PSKs, 125
type mismatch, 203-206

X

Xbox, 280. *See also* wireless online gaming