

What to Buy

The next step in building your network is to determine what you need to buy. Based on the planning diagram and tables you did in Chapter 4, “Planning Your Wireless Network,” you should have a good idea of the basic device types you need to get your network up and running.

Determining Network Readiness

We’ll follow the example started in Chapter 4. We first need to take inventory of the type of NICs we have already in the different computers we want to participate in the wireless home network. Make a table like that shown in Table 6-1, recording how we need to connect the computer in the Need column, and what we have today in the Have column.

Table 6-1 Network Readiness

Computer or Device	Need	Have	Type to Buy
Today			
Desktop PC (Spouse)	Wired NIC and wireless NIC	Wired NIC	
Desktop PC (Son)	Wireless NIC	Wired NIC	
Laptop 1 (Work)	Wireless NIC	Wired NIC Wireless B/G NIC	
Future			
Laptop 2 (Daughter)	Wireless NIC	None	
Xbox video game console	None	Wireless NIC	

Based on the table, we have wireless capability in one of the laptops (as a reminder, Chapter 4 showed you how to determine if your computer has wireless capability). This leaves us with one laptop and two desktop computers that need additional equipment to support wireless.

In addition to outfitting the computers with the right equipment, you also need a wireless router, which will communicate with all the computers and provide them access to the Internet via the cable or DSL modem.

In addition, you may want to consider some extra bells and whistles (such as game adapters or wireless cameras) at some point, so we’ll cover them here as well.

Wireless Router Options

Because we will be putting together a G-based network, the router we chose—WRT54G—is the base G router with no extensions, shown in Figure 6-4. If you plan to have the router sit out in the open and you want something a little smaller (and nicer looking), you can go with the compact router (WRT54GC), shown in Figure 6-5.

Figure 6-4 Linksys Wireless-G Broadband Router (WRT54G)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Figure 6-5 Linksys Compact Wireless-G Broadband Router (WRT54GC)



These materials have been reproduced by Cisco Press with the permission of Cisco Systems, Inc.
COPYRIGHT ©2007 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Wireless Router Setup

The wireless router is really the brains, or at least the heart, of your home network. The wireless router provides a number of functions, including

- Enabling several computers to connect to your home network either through a wired Ethernet cable or a wireless signal
- Providing a gateway to your broadband Internet connection so that several computers can share it
- Enforcing security policies to protect your home network from unauthorized access

This chapter provides the steps necessary to set up your wireless router, starting with connecting the wireless router to your broadband service. Chapter 8, “Wireless NIC Setup,” then walks you through getting wireless NICs to join the wireless network, to get your wireless home network up and running.



Figure 7-28 EasyLink Graphical View of Your Network

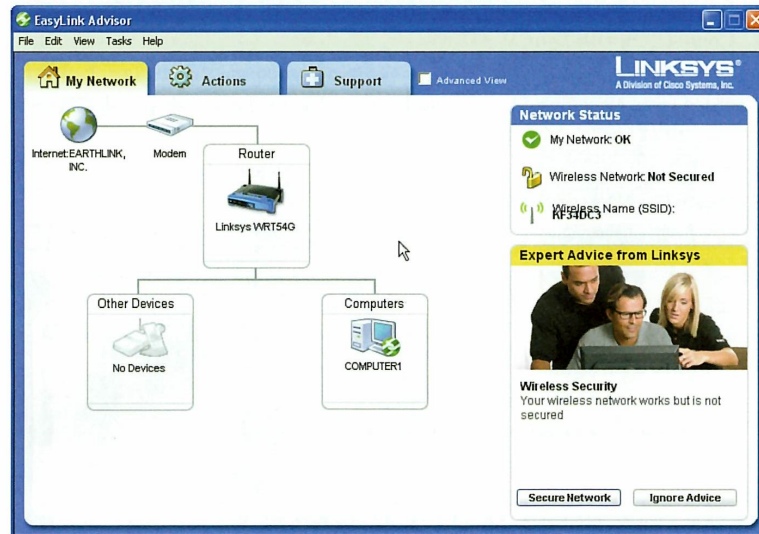
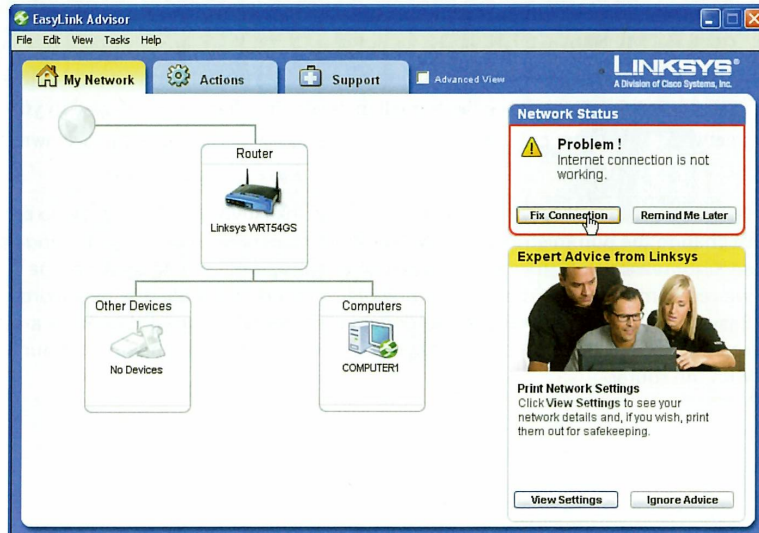


Figure 7-28 shows what the initial network should look like if things are working properly, including connectivity to the Internet. EasyLink Advisor can also help troubleshoot when something is not quite right. If, for example, the Internet connectivity is not working properly, EasyLink tells you, as shown in Figure 7-29.

Figure 7-29 EasyLink Advisor Notices the Internet Connection Is Not Working



Wireless NIC Setup

Each computer or device that you want to join your wireless network needs a wireless network interface card (NIC). A wireless NIC provides a number of functions, including

- Enabling a computer (or device) to connect to your home network through a wireless signal
- Securing the communications path between the wireless router and your computers and devices connected over wireless
- Providing a way for you to connect your computer to other wireless networks outside your home

This chapter provides the steps necessary to set up your wireless NICs, getting them to communicate with your wireless home network. The starting assumption is that you have already completed the wireless router setup in Chapter 7, “Wireless Router Setup.”

Installing the Wireless NIC

There are several types of wireless NICs to consider (as introduced in Chapter 6), including

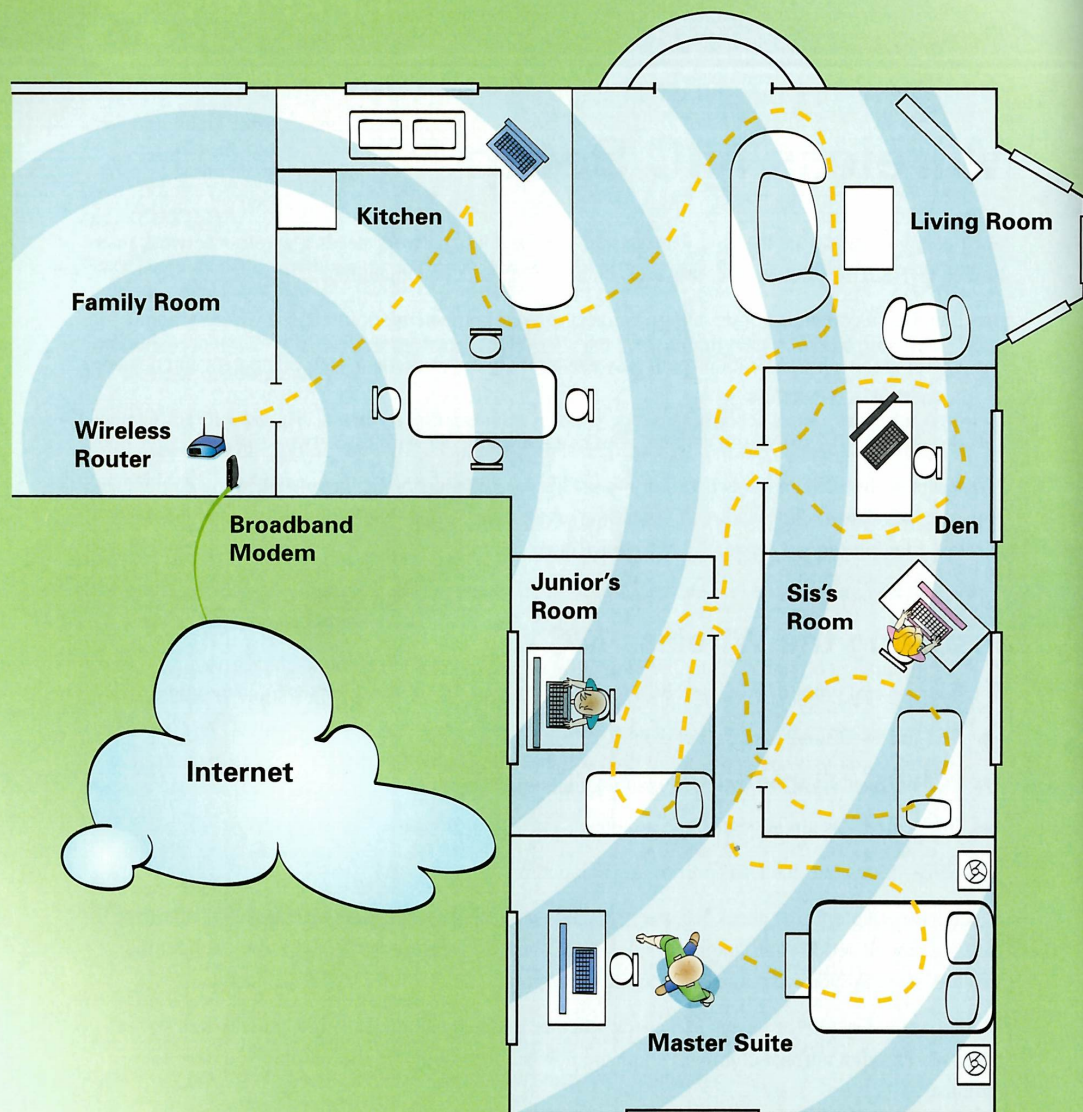
- **PCI card**—Installs inside a desktop PC
- **PCMCIA or ExpressCard**—Plugs into a laptop
- **Integrated**—Is already built into a laptop
- **USB**—Plugs into the USB port of any computer

If you have a laptop, first check whether it already contains an integrated wireless NIC. If it does, then you are all set. If your laptop does not have a built-in wireless NIC (or if it does but not the wireless standard you want to use), then the best option is to buy a PCMCIA wireless card.

If you have a desktop (or tower) PC, check whether it already contains an integrated wireless NIC, because (although not that common) some are now shipped with one. If not, then you have two options:

- Buy a PCI wireless card that installs inside the computer in an open card slot
- Buy a USB wireless NIC that plugs into any open USB port

USB NICs are handy because you can avoid opening up a computer to install them, but they do provide another box (albeit a little one) to add to a cluttered computer desk. USB is also an option for laptops, but they are a bit unwieldy on the go, so most people opt for a PCMCIA card.



Wireless association is very similar. The wireless NIC sees a signal that has the same SSID as one in its set of profiles. It attempts to associate by starting a conversation with the wireless router, sending certain signals to let the router know the NIC is there and wants to communicate. The wireless router may grant access or may not. In addition to the SSID, if wireless security is enabled, those parameters must match also (including type of encryption, encryption key, and so on). We will cover more on wireless security in Chapter 9.

If the wireless router grants access, it then typically assigns the NIC an IP address to use on the wireless network, at which point we can begin exchanging data. If it denies access for some reason (maybe we are not speaking the same wireless security language or are not authorized to use that wireless signal), the association fails and we must keep trying other wireless router signals until we find one to associate with.

Wireless Connection Managers

Wireless connection managers are programs that let you manage the wireless profiles in your computer, and which one you are currently connected to. If you use your computer only at home, such as a desktop PC or some other device that does not leave your home, you will typically use the wireless connection manager when you first set up your wireless network, and maybe again if you make changes. In this case you will likely also have only a single wireless profile: your home network.

If you own a laptop, chances are you will have several wireless profiles, including your home wireless network and several other profiles for traveling. Chapter 14, "Wireless to Go," covers how to use wireless outside your home.

There are several types of wireless connection managers, including

- Windows Wireless Network Connection utility
- Linksys WLAN Monitor utility
- Other programs such as Boingo

In this chapter we show the Windows Wireless Network Connection utility and the Linksys WLAN Monitor utility. We cover other programs such as Boingo in Chapter 14.

Starting with Windows XP and continuing with Vista (also available via patch updates for Windows 2000), it is possible to manage wireless connections within Windows, and not require an add-on program. This is the long-term direction for wireless NIC management: letting Windows manage the devices just like most other devices in the PC or laptop.

If managing your wireless NIC using Windows is supported, it is probably the best option. For those NICs that you cannot manage with Windows, you need an add-on program from the NIC manufacturer. These cases include

- NICs that use a very new wireless standard or type of wireless security that is not yet supported by Windows
- Wireless NICs from manufacturers that force you to use their specific software

Wireless Security Setup

With the wireless router set up and all the computers now communicating with it, it is time to turn our attention to securing the wireless network.



Note: The starting assumption is that you have already been successful in setting up the home wireless network without security in Chapters 7, “Wireless Router Setup,” and 8, “Wireless NIC Setup.” If not, stop and do that first. Turning security on in a wireless network that is already having issues is only going to increase the problem, not solve it.

As discussed in Chapter 5, “Wireless Security: What You Need to Know,” wireless networks have no security enabled when you buy the router and NICs. This is necessary because the wireless router and NICs have to be set up with the same security information (that you choose) to communicate with each other. For the reasons discussed in Chapter 5, it’s very important to take the few extra steps that are necessary to properly secure your wireless network. The steps are pretty easy:

- Enable encryption (either WEP or WPA) between the wireless router and wireless NICs.
- Disable SSID broadcast on the wireless router.
- Prevent unintentional roaming on all wireless NICs.
- Turn on the firewall on the wireless router (applies to any router, wireless or otherwise).
- Change the wireless router’s administration password (applies to any router, wireless or otherwise).

This chapter shows how to set up wireless security.

Setting Up Wireless Encryption

The first (and most important) step to securing your home network is to turn on encryption between the wireless router and the computers in your home network. In order for the computers on your home network to communicate with the wireless router, both sides of the wireless connection (wireless router and wireless NICs) must be using the same type of encryption and the same encryption key.

Figure 9-1 shows what the security options look like before and after.

- 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."

CHAPTER 10

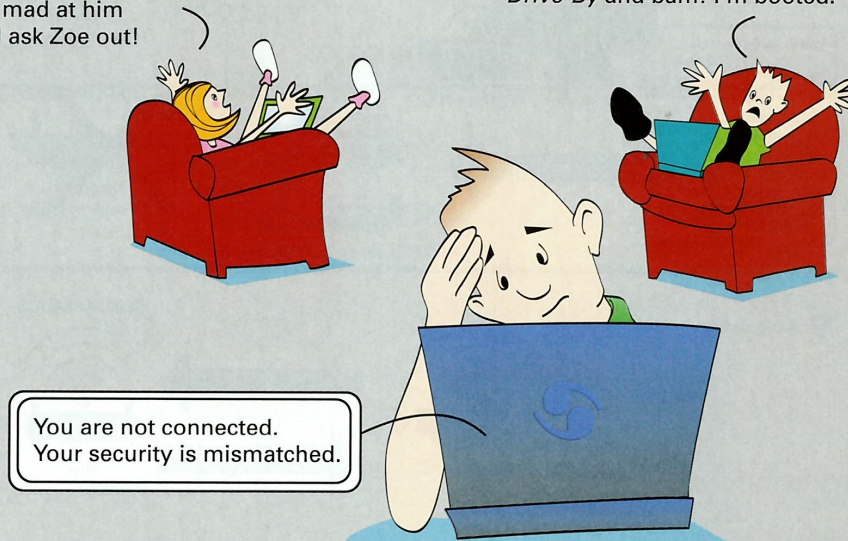
Troubleshooting: I Can't Connect at All

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.

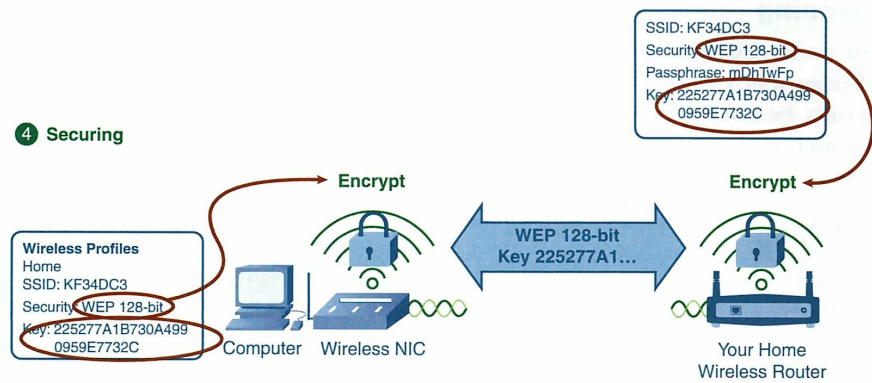
Before jumping into troubleshooting, let's first take a look at what happens during the steps when your wireless NIC connects to your wireless router and at what can go wrong during that process.

Gasp! I'm right in the middle of IM-ing Cody and the network goes down. Now, if I don't reply in the next 15 seconds, he'll think I'm mad at him and ask Zoe out!

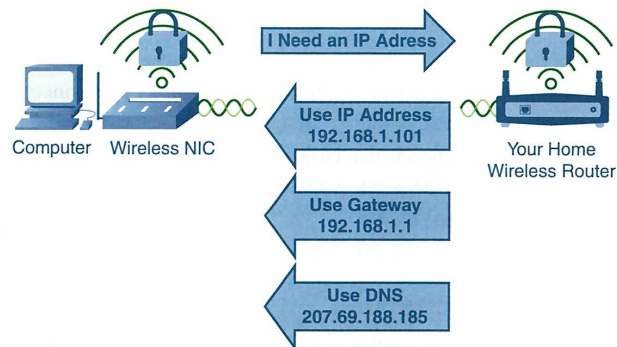
What up? I'm ready to destroy my nemesis Ray-Dar in *Inter-Planetary Drive-By* and bam! I'm booted.



4 Securing



5 Obtaining an IP Address



6 Sending and Receiving

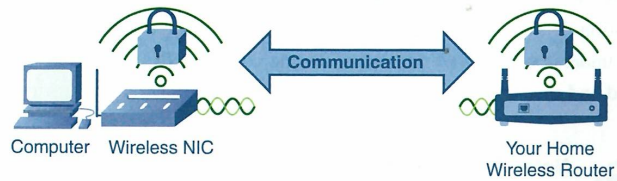
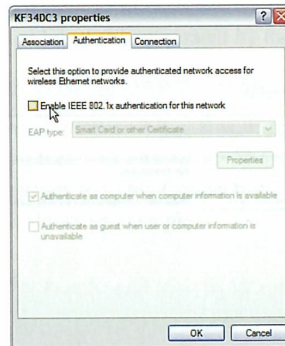


Figure 10-43 Verifying the Authentication Setting in Windows XP



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.



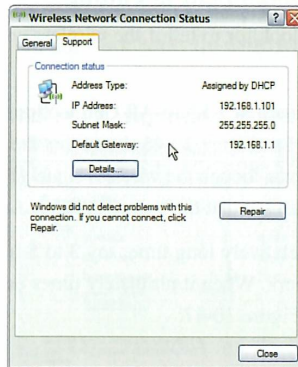
Note: Static IP addressing, which is when you turn off DHCP and assign your home network addresses manually, is quite problematic. Problems include duplicate addresses, errors in manually entering IP addresses, and others. We do not recommend using static IP addressing in home networks. If you do, prepare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

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).

Table 11-4 Five Simple Guidelines for Wireless Router Location

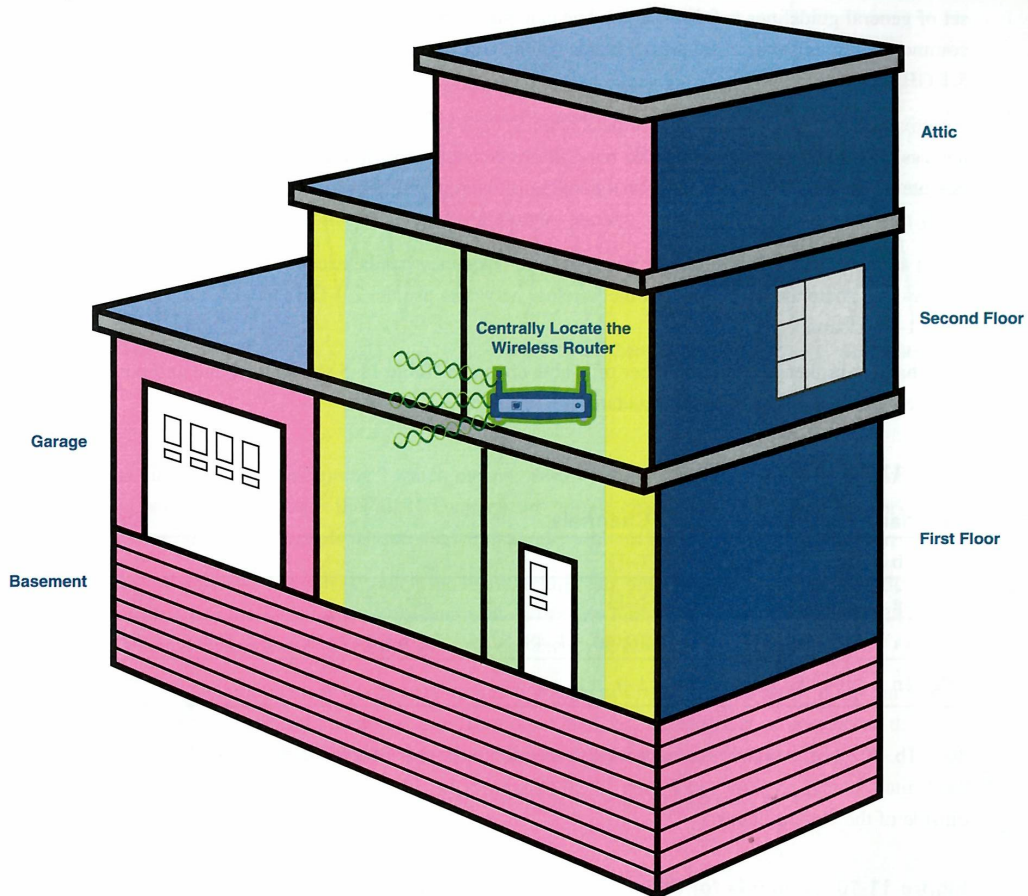
Do	Don't
Choose a site for the router in a central location in your house, considering all three dimensions (see Figure 11-9). Note the bigger the house, the more important this becomes.	Put the router in the basement, attic, garage, closet, or other isolated part of your house.
Place the router on a 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.

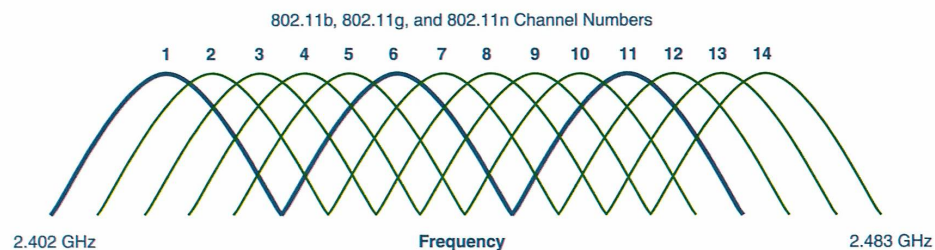
Each band is broken up into a number of usable channels. Table 11-5 shows the band and possible channels for each of the wireless standards.

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.

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.

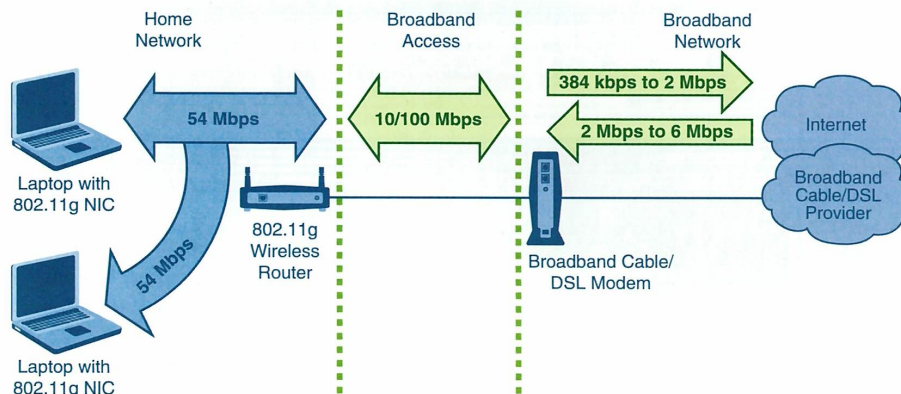
Is the Broadband Internet Connection the Bottleneck?

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).

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.

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.

Finding Uses for Wireless Video Cameras

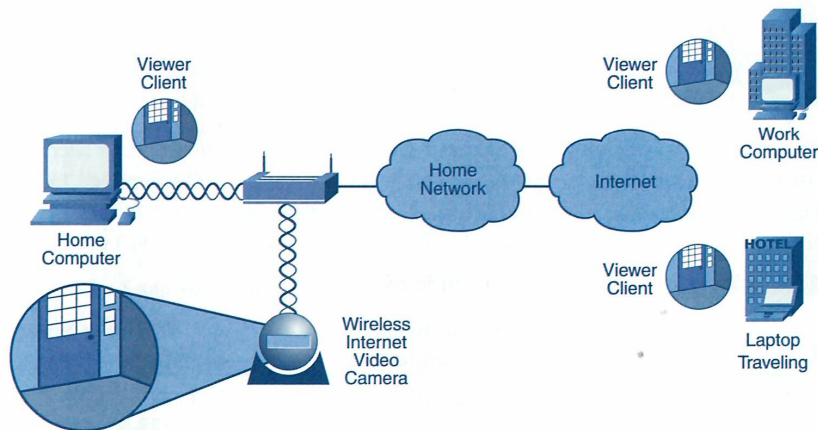
Video cameras that attach to computers are very common, usually used for communicating with other people that have similar video cameras. Also popular recently have been very inexpensive wireless cameras that can be placed anywhere in your house.

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.

Figure 13-5 Configure the IP Address Settings

LINKSYS
A Division of Cisco Systems, Inc.

Wireless-B Internet Video Camera
Setup Wizard Ver 2.06

IP Settings

These are basic network settings for the Wireless-B Internet Video Camera. Make sure you write down these settings in case you need them in the future.

Camera	IP Settings
WVC11B	IP Address: 192 . 168 . 1 . 140 Subnet Mask: 255 . 255 . 255 . 0 Gateway: 192 . 168 . 1 . 1 Primary DNS: 207 . 69 . 188 . 185 Secondary DNS: 207 . 69 . 188 . 186

Attention: Please make sure that your PC and the Wireless-B Internet Video Camera have IP addresses in the same IP range.

© Copyright 2003 Cisco Systems, Inc. All rights reserved.

Next

Back



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**.

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).

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

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.