

Share an Internet connection

Never pay for anything you can get for free. *by Russell Shaw*

If you have more than one PC at home, even if that second machine is a notebook computer, there's absolutely no reason you should be paying for more than one connection to the Internet (although your Internet service provider would dearly love you if you did).

We're assuming, of course, that you have a broadband Internet connection (DSL, cable, or satellite). A dial-up Internet connection is just too slow to share.

And although some Internet service providers (ISPs) will provide this service for an extra monthly fee (as much as \$10 per month), you can easily set it up yourself for a very small initial investment of time and money—and zero ongoing financial investment. After all, why should you pay for what you can get for free?

As an added bonus, the equipment you need to share an Internet connection is the very same gear needed to build a local-area network (LAN). In other words, when you set

up the hardware to share an Internet connection, you're building a LAN at the same time. And once you've set up a LAN, you can not only share your Internet connection, but you can share your printer, scanner, and many other expensive peripherals, too.

Your network can be either wired or wireless, but we'll show you how to set up the latter. After all, who wants to deal with stringing cable all over the house? As you might expect, all the devices connected to a LAN need to speak the same language. Fortunately, the industry has established standards for this very purpose.

Unfortunately, constant advances in technology have forced the industry to create more than one standard. This means you'll still need to make sure all your gear is compatible when you go shopping. Here's what to look for:

WIRELESS STANDARDS

Wireless networking equipment based on the IEEE-802.11b standard is the most common and least expensive gear you'll find. (Refer to the sidebar "Wireless Standards" for a definition of IEEE.) In theory, an 802.11b network can

→ A USB wireless NIC, such as this Netgear model WG-121, can outfit any computer with wireless networking capabilities.



transmit data at rates up to 11 megabits per second (Mb/sec).

Gear based on the newer 802.11g standard can theoretically transmit data up to 20Mb/sec, and it's backward compatible with 802.11b gear. That means if you happen to already own a bunch of 802.11b gear, you won't need to throw it out if you add equipment based on the newer, faster 802.11g standard. (Both standards are commonly referred to as Wi-Fi, which stands for wireless fidelity.)

The actual performance of your LAN will depend on a lot of environmental factors, including where in your house the equipment is placed, what other wired and wireless equipment and appliances (particularly, wireless telephones and microwave ovens) are



→ Not sure if your desktop computer is set up for wireless networking? See if there's an antenna sprouting out its back.

SET UP YOUR WIRELESS ACCESS POINT The EasyWay



1 Turn off the power supplying your computer and your Internet gateway; unplug both devices from their electrical outlets. Place your wireless access point in close proximity to your Internet gateway.



2 Remove the Ethernet cable connecting the Internet gateway to your PC's NIC from the Internet gateway.

3 Plug that same cable into Port 1 on your wireless access point, leaving the other end connected to your PC's NIC.



4 Take one end of a short length of Ethernet cable and plug it into the Ethernet port on your Internet gateway.



5 Plug the other end of that short Ethernet cable into the WAN port on your wireless access point. Plug both devices into electrical outlets and turn them on.

operating in the house, and even the construction materials used in your home.

The radio waves that wireless networks use travel much more easily through wood and wallboard than they do concrete and steel. The number of walls—or floors, in a multistory home—will also have an impact on their effectiveness.

In an open-space environment without *any* physical obstructions, the signal from a wireless access point (we'll explain this term shortly) can travel as much as 175 meters (signals from wireless access points based on the 802.11g standard can travel about 50 meters). In a more real-world environment, with walls, ceilings,

furniture, and other obstructions, the distance the signal can travel will be considerably shorter.

If you need to provide coverage to a very large area, install multiple access points (either wired or wireless models).

ELEMENTS OF A WIRELESS LAN

In order to set up a wireless LAN that can share a broadband Internet connection, you'll need a wireless access point to physically connect to your DSL, satellite, or cable modem (also known as an Internet gateway). Access points are about the size of a paperback book and contain a radio transceiver (which transmits and receives data), an

antenna, communications and encryption (security) software, and one or more Ethernet ports.

You'll also need a wireless network interface card (NIC) for each computer you plan to put on the network. (If you're locating the access point in close proximity to one of your computers, on the other hand, you can simply hardwire the PC's NIC to the access point.)

Wireless NICs can fit inside your PC, plug into an available USB (Universal Serial Bus) port, or—in the case of a notebook computer—fit into a PC Card slot. Some notebooks even have built-in wireless NICs. Many handheld computers, such as those that use Microsoft's Pocket PC operating

LOCK DOWN YOUR WIRELESS LAN The Easy Way

Securing your wireless LAN is a three-step process, accomplished using your wireless access point configuration software. We've chosen a Linksys product for illustration purposes, but you'll need to use the utility that's provided with your particular router.

Naming your wireless LAN with a Service Set Identifier (SSID) and enabling Wired Equivalent Privacy (WEP) will provide security that's pretty much equivalent to a hardwired network. That's because no one will be able to access your wireless LAN until you give them the LAN's unique WEP encryption key. At the very least, it will foil nosy neighbors and other casual snoops who might try to eavesdrop on your wireless network.

Domain Name: (Required by some ISPs)
 Firmware Version: 1.42.7, Apr 03 2002
 LAN IP Address: (MAC Address: 03-08-26-76-0E-97)
 192 168 1 1 (Device IP Address)
 255.255.255.0 (Subnet Mask)
 Wireless: (MAC Address: 00-00-4B-0C-C3-03)
 Enable Disable
 SSID: easytechguide
 Allow "Broadcast" SSID to associate? Yes No
 Channel: 6 (Domain: USA)
 WEP: Mandatory Disable WEP Key Setting

1 Name your wireless LAN with a Service Set Identifier (SSID).

Firmware Version: 1.42.7, Apr 03 2002
 LAN IP Address: (MAC Address: 03-08-26-76-0E-97)
 192 168 1 1 (Device IP Address)
 255.255.255.0 (Subnet Mask)
 Wireless: (MAC Address: 00-00-4B-0C-C3-03)
 Enable Disable
 SSID: easytechguide
 Allow "Broadcast" SSID to associate? Yes No
 Channel: 6 (Domain: USA)
 WEP: Mandatory Disable WEP Key Setting

2 Enable Wired Equivalent Privacy (WEP) on your wireless LAN.

Phrase: elabot432 Generate
 Key: NEBDA37B17FA973249EAB3
 Clear
 Apply Undo

3 Create a WEP encryption key by entering a password into the key-setter utility. Click "Generate," and the program will create an encrypted version of that password. Write down this encryption key, because you'll need to install it on each computer that you grant access to your wireless LAN.

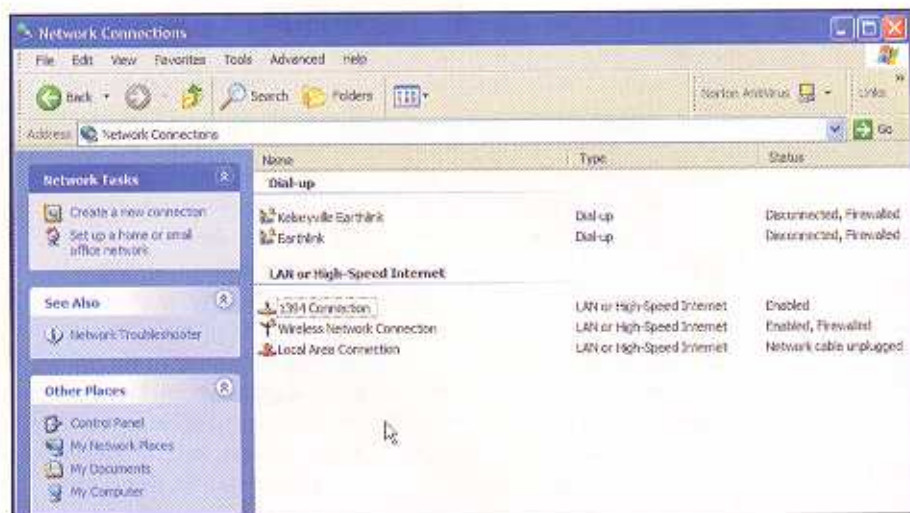
system—are also capable of wireless connectivity (using either built-in or add-on NICs).

You can mix and match equipment from different manufacturers, as long as all of it is based on either the 802.11b or 802.11g standards. You should note, however, that if your wireless access point is based on the 802.11b standard, the maximum speed of your entire network will be limited to 11Mb/sec (the maximum speed that standard supports).

By the same token, if you connect an 802.11g wireless access point to your Internet connection, but all your computers have 802.11b Ethernet NICs, the computers will be limited to data-transfer speeds of just 11Mbps.

So, which standard should you buy? We expect the older and slower 802.11b standard to eventually fall by the wayside. In the meantime, 802.11b equipment will be considerably cheaper than gear based on the newer, faster 802.11g standard.

If you want to future-proof your network, buy an access point based on 802.11g. Each time you upgrade or replace a computer, make sure it has an 802.11g wireless NIC and you'll get the most speed out of your access point and your network as a whole. If you're more interested in saving money, on the other hand, buy an 802.11b access point;



➔ If you see a listing for a **Wireless Networking Connection** in your Control Panel, then your PC is already equipped with a wireless network interface card. Congratulations!

especially if the wireless NICs in all your computers are based on the slower 802.11b standard anyway.

INSTALLING YOUR ACCESS POINT

The first step in sharing your broadband Internet connection is to configure your wireless access point. As a general rule, you won't be able to rely on your Internet service provider to help you with this process—unless you've signed up for one of their monthly service plans, that is. In all fairness to ISPs, however, you really can't expect them to help you install a product that you didn't purchase from them.

But you needn't worry, anyway. Attaching your Internet gateway

to your wireless access point is a simple process. And once you've configured your wireless access point, you can plug a wireless NIC into your computer and move the machine anywhere within the access point's range. Imagine being able to print documents and pictures, access files stored on your other computers, check your email, and surf the Web from the comfort of your bed, your kitchen table, or even out on your backyard patio!

Keep two things in mind when you choose a location for your wireless access point. First, you'll want to place it in close proximity to your Internet gateway, because you'll need to hardwire it (physically connect it with an Ethernet cable) to that device. You'll also need electrical outlets to power (and perhaps a surge suppressor to protect) both devices.

Second, envision a "wireless sphere" around the access point. In other words, place it in a central location equidistant from all the devices that will access it, and with as few physical obstacles between them as possible. This will produce the maximum usable coverage.

As we mentioned, you'll need to hardwire a computer to the access



➔ If your notebook computer doesn't have built-in Wi-Fi capabilities, it's simple to add a PC Card that will do the job.

point—at least temporarily—in order to configure it with a network name and an encryption key. The manufacturer of your wireless access point will provide installation software, which you'll install on this machine, that will guide you through the configuration process for their hardware. During that installation process, you'll be asked to choose between two networking modes: Ad-hoc and infrastructure.

Since you'll most likely want to share peripherals that are hooked up to one computer on your LAN (you might have four computers sharing a single printer and scanner, for example), choose infrastructure mode. The only time you'd choose ad-hoc mode is in the unlikely event that your printer (and any other shared peripherals) had their own wireless Ethernet cards.

If you don't secure your wireless LAN, anyone with a wireless NIC in their computer who happens to be in range will not only be able to jump on and leech the Internet connection you're paying for, but they'll have access to your

entire LAN and all the computers connected to it, too. This could be your nosy neighbor, for example, or even someone running a laptop from a nearby parked car.

Fortunately, securing your LAN is an easy, three-step process that involves identifying it with a Service Set Identifier (SSID), enabling a privacy technology called Wired Equivalent Privacy (WEP), and creating an encryption key that each computer accessing the LAN must have before it will be granted access. Refer to the sidebar "Lock Down Your Wireless LAN" for detailed instructions on how to secure your wireless network.

After you've configured your wireless access point, you can either leave the computer where it's at, or install a wireless NIC (if it doesn't already have one) and move it anywhere in your house (as long as it's within range of the access point, that is). If you ever need to reconfigure the wireless access point, however, you'll need to temporarily re-hardware a computer to it for the task.

Refer to the sidebar "Set Up Your Wireless Access Point" and we'll take you through a sample configuration process step-by-step.

ADDING COMPUTERS TO YOUR WIRELESS LAN

Each computer you connect to your wireless LAN must be outfitted with a wireless NIC, although if one machine is in very close proximity and has a wired NIC, you could just as easily hook it up with an inexpensive Ethernet cable.

Many laptop and handheld computers are now being manufactured with this gear built in, but it's highly unlikely that your desktop machine is equipped this way. Here's how you can tell what's inside yours:

Spotting a wireless NIC in a desktop computer is easy—just look for an antenna sprouting out the back, near the expansion slots. (Turn to page 52 and you'll see a picture of an internal wireless NIC. The antenna portion would protrude from the back of the computer.) It's more difficult to find a wireless NIC

ENABLE ACCESS TO YOUR WIRELESS LAN

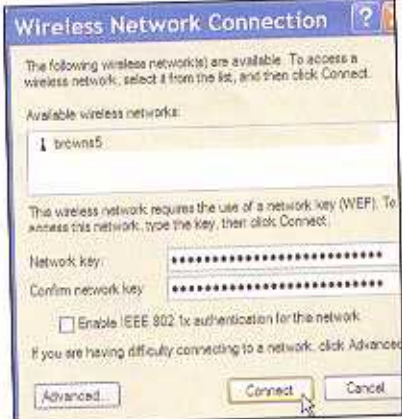
The Easy Way



1 Select your wireless LAN by clicking on the Start button on the Task bar at the bottom of the screen. When the menu pops up, click on the "Control Panel" menu item, then double-click on "Network Connections."



2 Double-click on "Wireless Network Connection."



3 Select the network name, and then enter the WEP encryption key in each of the two boxes provided. When you're finished, click on "Connect" and you'll be able to access your wireless LAN.

on a portable device, because their antenna is often tucked away inside the device.

Some manufacturers print the term "Wi-Fi" right on the device's case, but you can make an absolute determination by examining the Windows Control Panel.

Click on the Start menu and select Control Panel from the pop-up menu. Next, double-click on Network Connections. Under the Type heading, look for the words LAN or High-Speed Internet. If you see an item beneath that labeled Wireless Internet Connection, your computer has a wireless NIC. If it doesn't, you'll need to install one before you can continue configuring your LAN.

Add-on wireless NICs come in a variety of form factors, including circuit boards designed to fit in the expansion slot of a desktop PC, PC Cards that fit in specially designed slots in notebook computers, and USB adapters that can be installed in either type of computer. You'll find photos of each type of device elsewhere in this story.

Once you've installed wireless NICs in each of the PCs you wish to grant access to your wireless network, you'll need to configure each of them with the Wired Equivalent Privacy (WEP) key you created to protect your wireless LAN from outsiders. Refer to the sidebar "Enable Access to Your Wireless LAN" for details.

TEST YOUR INTERNET CONNECTION

Now that you've configured your wireless access point and all the computers you want to share your broadband Internet connection with, you're ready to test your network. Launch Internet Explorer on each of the computers on your network and either type in the address of any valid Website, or hit the Refresh button to reload your Home page.

WIRELESS STANDARDS

There are currently three different industry standards for building wireless networks. Governed by the Institute of Electrical and Electronic Engineers (IEEE), these standards (see the table below) ensure that all wireless networking equipment can function together regardless of who manufactured it.

The newest equipment is manufactured according to the IEEE 802.11g standard. This equipment isn't the fastest (that honor goes to equipment manufactured according to the 802.11a standard), but it is backward compatible with the older and more common 802.11b standard. That means you can mix and match newer 802.11g equipment with older 802.11b equipment on the same network without any experiencing any problems.

Equipment manufactured according to the 802.11a standard is much faster than equipment manufactured according to the 802.11b and 802.11g standards. But since 802.11a equipment is also incompatible with 802.11b and 802.11g equipment, we don't recommend it.

Confused? Don't be. When you buy your wireless networking equipment, just make sure it uses the 802.11g standard. It's a little more expensive, but it's much faster. And if you ever need to grant wireless network access to a PC outfitted with an older 802.11b NIC, you won't have a problem.

STANDARD	802.11b	802.11g	802.11a
SPEED	11Mb/sec	Up to 20Mb/sec	Up to 54Mb/sec
RANGE	Up to 175 meters	Up to 50 meters	Up to 175 meters
FREQUENCY	2.4GHz	2.4GHz	5GHz
CHANNELS	12	2	3

If you experience any problems, check the obvious possibilities first: Make sure all your cables—including your power cables—are securely plugged in. If that doesn't solve the problem, unplug each Ethernet cable and plug it back in again to make sure you have a secure connection. Still having problems? Turn all the equipment off and turn it back on again. This sort of power cycling often cures common problems.

You might also check to see that all the computers on the network are within the range of the wireless access point, and that there aren't any obstacles interfering with the signal path. These can be either physical (e.g., metal-clad doors or aluminum studs) or electrical (microwave ovens and wireless phones are common culprits).

If none of these troubleshooting tips solves your problem, contact the manufacturer of your wireless access point. The major manufacturers offer very good free tech support over the phone,

although you might have to wait on hold for a while before you get to speak with anyone.

You should also be aware that some manufacturers are putting time limits on their free tech support: They'll gladly help you configure the device within a certain window of time after you purchase it; wait too long, however, and you could discover that you're expected to pay for the manufacturer's tech support on a per-call basis.

And remember, your Internet service provider is unlikely to lend a hand in setting up an Internet-access sharing system—unless you've decided to pay their extra monthly service fee (and why would you ever do that?).

As with a lot of today's technology, once you've experienced the dual joys of a shared broadband Internet connection and having your own local area network, you'll soon wonder how you ever managed to get along without them. ■