How To... A step-by-step guide to tweaking your PC Experience

INSTALL A PERFECT Wireless Network

Anyone can add a wireless network to their home quickly and easily. But if you do it the *Maximum PC* way, you'll own the fastest, most reliable, and most secure network on the block

Without a doubt, wireless networking is the easiest way to share Internet access. And finally—*finally*!—the technology has emerged from the realm of the mundane corporate IT weenie to occupy the living rooms of regular folks. Anyone who wants Internet access throughout his or her house, or who's fed up with the Ethernet cables running into the living room for his or her game console, can use Wi-Fi.

The Wi-Fi elite don't want you to know this, but all you need to get a wireless network running is an access point (AP) and a wireless card. Most wireless access points also include a router, which lets you share a single Internet address with all the computers in your home. It's really that simple. If you still need some more reassurance, turn to page 60, where we show you everything you need to know to get your network up and running.

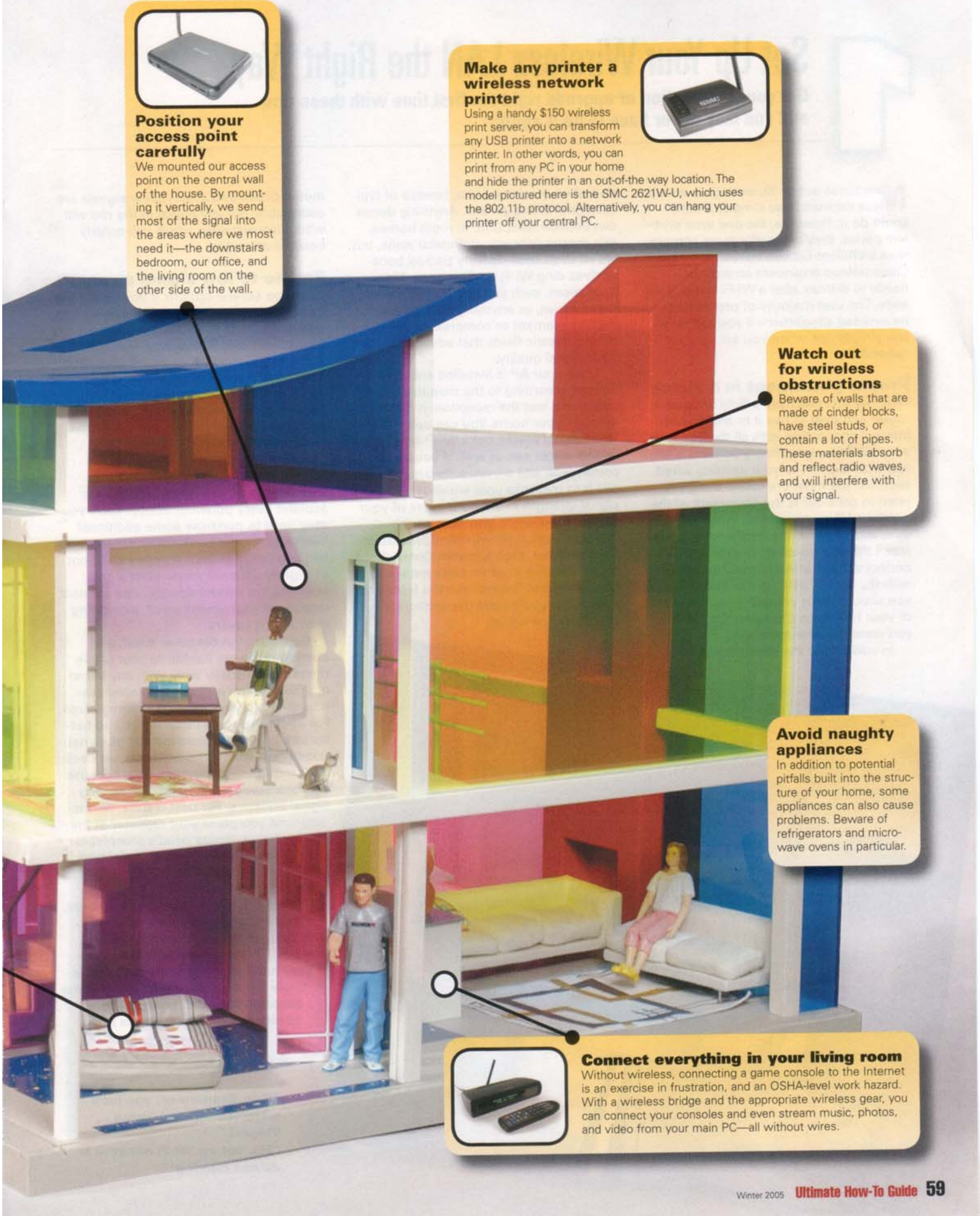
Although the new generation of wireless devices (more on them later) are a snap to configure and use, setting them up can still be intimidating to the uninitiated. And if something goes wrong—well, look out. If you're having trouble getting your wireless network up and optimally running, we've included a troubleshooting guide on page 64.

And no Wi-Fi setup is complete unless you've taken the time to secure your connection from evildoers. After all, you don't want your neighbors to mooch off of your expensive broadband connection just because you didn't read our security guide on page 65.

Ready to learn about wireless? Turn the page and we'll hook up your hardware, optimize your network, and get you on the road to wireless bliss.

Browse the net from anywhere in your house
This is the number one reason most people buy into wireless. Whether you're sitting on your couch or lounging in bed, you can still connect to the Internet. It's so handy, it's hard to imagine a time when there wasn't a laptop in the living room.

Shut out Wi-Fi banditos
Protect your wireless network from would-be Wi-Fi thieves by enabling WEP and preventing unknown wireless cards from connecting to your network. By using the Cantenna Wi-Fi booster (**www.cantenna.com**, $20), broadband thieves can pick up wireless signals from several hundred feet away. Don't be a victim.



Position your access point carefully

We mounted our access point on the central wall of the house. By mounting it vertically, we send most of the signal into the areas where we most need it—the downstairs bedroom, our office, and the living room on the other side of the wall.

Make any printer a wireless network printer

Using a handy $150 wireless print server, you can transform any USB printer into a network printer. In other words, you can print from any PC in your home and hide the printer in an out-of-the way location. The model pictured here is the SMC 2621W-U, which uses the 802.11b protocol. Alternatively, you can hang your printer off your central PC.

Watch out for wireless obstructions

Beware of walls that are made of cinder blocks, have steel studs, or contain a lot of pipes. These materials absorb and reflect radio waves, and will interfere with your signal.

Avoid naughty appliances

In addition to potential pitfalls built into the structure of your home, some appliances can also cause problems. Beware of refrigerators and microwave ovens in particular.

Connect everything in your living room

Without wireless, connecting a game console to the Internet is an exercise in frustration, and an OSHA-level work hazard. With a wireless bridge and the appropriate wireless gear, you can connect your consoles and even stream music, photos, and video from your main PC—all without wires.

1 Set Up Your Wireless LAN the Right Way

Get your installation or upgrade right the first time with these tips, and you may never have to do it again!

Nine times out of 10, setting up a wireless network is so simple, a baby could do it. However, the one time problems arise, they're usually more complex than a William Gibson novel. We've seen Cisco-trained engineers scratch their heads in dismay after a Wi-Fi install gone awry. The vast majority of problems can be avoided altogether—if you follow a few simple tips when you set up your network.

Proper placement is a virtue

Whether you purchase a fully fledged router and plan to use it to share your Internet connection with all the PCs in your home, or you simply connect a wireless access point to your existing wired network, the most important thing you need to consider is the placement of the wireless AP in your home. When situating your access point, it's important to understand that the coverage area won't be a perfect sphere. Instead it will be flattened, with the access point in the center. Ideally you should place your AP near the center of your home, on the same floor where you want the best coverage.

In addition to the physical location of your access point, beware of typical signal-killing pitfalls. Anything dense can impede reception. In most homes, this means concrete and metal walls, but we've even seen densely packed bookshelves ding Wi-Fi performance. Many appliances, such as refrigerators, ovens, microwaves, or anything with an electric heating element or compressor, create strong electric fields that adversely affect your signal quality.

Once your AP is installed and configured according to the manufacturer's directions, test the reception in different areas of your home. You can use a fancy Wi-Fi signal meter, but a Wi-Fi-equipped laptop works just as well. If your card comes with site survey software, you can use it to measure your wireless network's signal strength in different areas of your home. If it doesn't, you can use the monitor that's built into Windows. Go to Control Panel, then Network Connections, then right-click your wireless network card and go to Status. Take the laptop to each room you'll want to connect from, and check the signal meter. Green and even yellow signals are acceptable, but any signal in the red will work inconsistently, which will quickly become annoying.

Say no to low signal strength

You have several options if you've got the low-signal-strength blues. The easiest and cheapest trick is to relocate or reorient the access point. Leave your test laptop in the trouble spot, then move your AP a few feet and recheck the signal strength in the trouble spot and the rest of the house. (Make sure you check your other points as well before you make the new location permanent.)

But what happens if relocating the access point does no good? If you've tried several different rooms and have avoided every potential trouble spot, you may need to purchase some additional hardware. Signal boosters and repeaters will add range to your wireless LAN, but in slightly different ways. Most signal boosters are vendor-specific, and connect directly to your access point, expanding the range it covers.

Repeaters, on the other hand, add another coverage bubble to your LAN's range. They usually work with any brand of access point, and can be placed anywhere within your existing coverage area. For about the same price, we've had better luck using repeaters instead of signal boosters. It seems the hardware vendors have found the same to be true, because very few companies are still producing signal boosters. For best results, we recommend you place your repeater at the edge of your access point's acceptable coverage area, and nearest the rooms that need improved connection quality. We like D-Link's DWL-800 repeater.

In addition to access points, routers, repeaters, and signal boosters, Wi-Fi bridges are useful for connecting wired Ethernet devices to your wireless network. Most bridges available today are used to convert wired game consoles and other consumer electronics devices into wireless ones.

"Hey, Readerman, you look different. Are you using Viagra?"
"No, but my Wi-Fi network is *up* and running!"

3 Logically Troubleshoot Your Wi-Fi Woes

We present three easy steps to wrangle your Wi-Fi network into working order

Typically, setting up a Wi-Fi network is so easy, a poorly trained dyslexic monkey could have the whole thing up and running in 15 minutes. Of course, those rare instances when everything goes wrong can be frustrating for even a highly trained network engineer. Follow these steps to tackle even the gnarliest Wi-Fi mess.

PROBLEM:

My PC shows a strong signal, but I can't connect to the Internet.

WE SAY:

Three or four factors can cause a connection with no data transfer. First, try upgrading your access point's firmware. We've spent hours trying to configure and re-configure a dead Internet connection, only to discover that a firmware update was all we needed. (The firmware is like your access point's operating system.)

If that doesn't work, check for a misconfigured WEP (wired equivalent privacy) or WPA (Wi-Fi protected access) key. If you have other wireless PCs that are operating properly on your network, re-enter your WEP or WPA key on the machine that's not working.

If you live in an apartment complex with several other wireless access points, you may need to prevent your PC from connecting to other APs. Go to Start, Control Panel, Network Connections, then right-click your wireless network card and choose Properties. Go to the Wireless Network tab, then click the Advanced button and ensure that "Automatically connect to non-preferred networks" is not checked.

The final potential pitfall is an IP address misconfiguration. Go back to the Network Connections Control Panel, right-click your wireless network card, and then select Status. Go to the Support tab and check the IP address. For most IP addresses, the address type should be listed as "Assigned by DHCP." If that field lists "Auto-configuration IP address," it's easy to fix: Just press the Repair button to get a current dynamic address.

If the address-type field says "Static IP address," you'll probably need to change it to dynamic. First click Network Connections, and press Properties. Click the General tab, then double-click the Internet Protocol item. Make sure that "Obtain an IP address automatically" and "Obtain DNS server address automatically" are checked.

PROBLEM:

My access point is on and configured, but my wireless computer says there's no available wireless network.

WE SAY:

First, try moving your computer closer to your access point. If you're sitting three feet away from the AP and don't have a connection, either your device or the AP is misconfigured. Make sure your access point and PC are using the same type of security, either WPA or WEP. You also need to ensure that the security key is the same on the AP and the PC.

Make sure your card and access point are using the same spec. While 802.11g is backward-compatible with 802.11b, some access points allow the user to lock the AP into 802.11g-only mode, preventing connections from older 802.11b hardware.

If you've checked the security and compatibility settings, but still have no connection, check your AP manufacturer's web site for a firmware update. Many times, incompatibility issues between access points and wireless networking cards can be quickly resolved with firmware updates.

PROBLEM:

I've tried everything above, but I still can't connect to the Internet.

WE SAY:

Either your Internet connection is down, or your router isn't talking to the Internet via your Internet Service Provider. If your access point is built into a router, make sure the router is actually working by plugging a PC into one of the wired Ethernet ports. If you can't connect using the wired port, then your router may be misconfigured. Make sure your router is configured as your ISP recommends. Check the IP address and your PPPoE settings. Some ISPs used to tie your connection to a single MAC (media access control) address, but that's increasingly rare. If you're concerned that there's some ISP funny business going on, check your access point's documentation to see how to clone your desktop PC's MAC address onto your router.

If it still doesn't work, try connecting your PC directly to your DSL or cable modem. If you can connect to the Internet when plugged directly into your modem, then your router is misconfigured. If you can't, contact your ISP to get your broadband connection working properly. ■

IN THE LAB: HOW TO TEST WI-FI PERFORMANCE

We use several benchmarks to test Wi-Fi performance, but the simplest method is to measure the length of time it takes to move a large file from a wired machine to a wireless machine and then back again. We use an FTP server for our tests, but it's entirely acceptable for a home user to just use Windows file-sharing by dragging and dropping files between directories. To test performance, you'll need a stopwatch and a file larger than 200MB. When the file is finished transferring, divide the size of the file by the length of time it took to download. We generally find 802.11g networks transfer at about 1.2MB/sec, or about 10Mb/sec, from a wired to wireless network in a best-case scenario.

How To... A step-by-step guide to tweaking your PC Experience

PROTECT YOUR Wireless LAN

MAXIMUM PC
TIME TO COMPLETION
00:40
HOURS MINUTES

Keep the neighborhood snoops, sniffers, and data thieves off your 802.11 network

Every month, you pay five sawbucks for a broadband Internet connection, and your favorite way to savor the lightning-fast downloads is via a wireless Internet connection. But danger lurks in this high-speed, free-range utopia. Just consider how many seedy online guides explain how to get "free broadband" by leeching off someone else's precious Wi-Fi bandwidth!

Stolen bandwidth isn't the only problem. Once thieves can leech your net connection, they can also get access to files on your PC, track the sites you browse, and even read your private e-mails and instant messages. Yikes! *It sucks to be you.*

But that's where we come in. We're here to save you from bandwidth pirates and other pimply ne'er-do-wells. Whether you use 802.11b or 802.11g, the precautions for wireless safety are about the same. We'll show you how to lock down your data and minimize the chances that a wireless snooper will leech from your LAN.

Wireless networking entails that every data packet to and from your PC be broadcast over the airwaves, so there's always a chance that someone will be able to sniff your data. If you want to make your LAN 100 percent secure, you'll have to disconnect it from wireless technology entirely. Still, the tips in this article will protect you from all but the most determined miscreants.

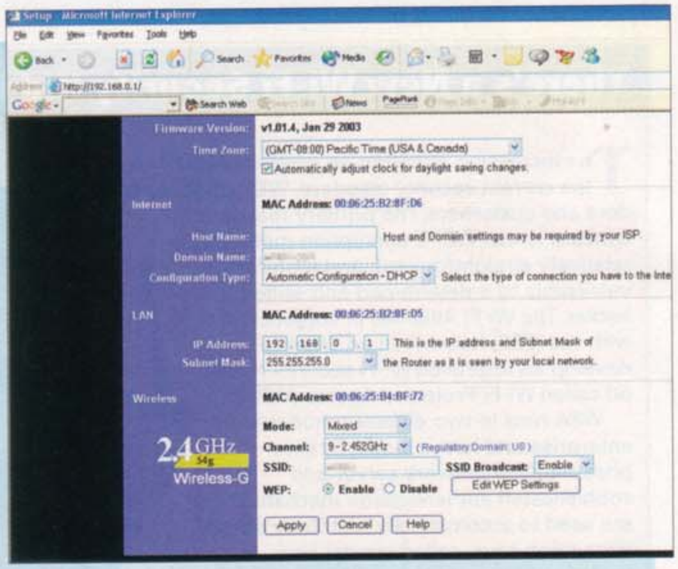
What You'll Need

- ▶ 802.11b or 802.11g access point
- ▶ 802.11b or 802.11g cards to access the LAN
- ▶ 100Mbit Ethernet hub
- ▶ NetStumbler (www.netstumbler.com)
- ▶ Laptop computer

Give Your Network a New Name

Your network's name can actually be a weak spot. In order to gain access to your network, an intruder has to know its name—commonly called an SSID. Most access points from a single manufacturer ship with the same SSID (preset at the factory), and the easy setup programs that come with the hardware don't always encourage users to change the SSID.

What can you do to fix this? Change your network's SSID! Open up the configuration program that was provided with your access point, and change the SSID to something completely unique and obscure. We recommend that you *not* use anything obvious, such as your hardware manufacturer's name, or words like "default," "wireless," "802.11," "network," "home," or anything else that may be easily guessed after just a few tries.


Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.1/
Google Search Web News PageRank
2.4GHz 54g Wireless-G

Firmware Version: v1.01.4, Jan 29 2003
Time Zone: (GMT-08:00) Pacific Time (USA & Canada)
☑ Automatically adjust clock for daylight saving changes.

Internet
MAC Address: 00:06:25:B2:8F:D6
Host Name: Host and Domain settings may be required by your ISP.
Domain Name:
Configuration Type: Automatic Configuration - DHCP Select the type of connection you have to the Inte

LAN
MAC Address: 00:06:25:B2:8F:D5
IP Address: 192 . 168 . 0 . 1 This is the IP address and Subnet Mask of
Subnet Mask: 255.255.255.0 the Router as it is seen by your local network.

Wireless
MAC Address: 00:06:25:B4:BF:72
Mode: Mixed
Channel: 9 - 2.452GHz (Regulatory Domain: US)
SSID: SSID Broadcast: Enable
WEP: ● Enable ○ Disable Edit WEP Settings
Apply Cancel Help

While you're changing the SSID, make sure to change the password for your AP's administration account. No matter how secure you make your AP, it's wide open if a cracker can just log in using the username and password printed in the instruction manual.

Changing your SSID is the first step you need to take, but it's certainly not the end of your lockdown routine.

Get WEP Working

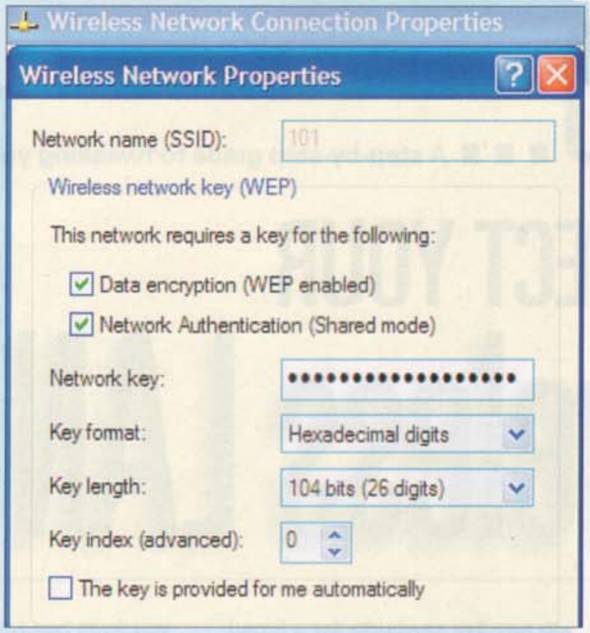
Enabling WEP—wired equivalent privacy—is the second-most important thing you can do to stymie would-be wireless freeloaders. WEP isn't 100 percent secure, but cracking the encryption technology isn't a simple exercise. In fact, it presents more trouble than most common bandwidth thieves are willing to wrestle with.

First things first: If your access point and your Wi-Fi card support 128-bit encryption, use 128-bit encryption. A 128-bit key can indeed be cracked, but even under perfect circumstances, a cracker will have to sniff packets from your wireless network for six or more hours in order to get enough data to generate a WEP key. And we repeat: That's in an *ideal* situation. It can actually take days or longer to sniff enough packets to crack a 128-bit key.

Of course, a 128-bit key won't help you if it's just 1111 1111 1111 1111 1111 1111 11. Interfaces for entering keys will differ from access point to access point. Some APs require that you enter the key in hexadecimal, while others prefer plain ASCII text. Luckily, the Windows wireless control panel lets you enter your key in either format, so make sure you enter the key in the same format in both places!

When you create your key, remember that hex keys can include the digits 0 through 9 and A through F. ASCII keys can be any letter of the alphabet or any number. For maximum security, avoid repetition or any kind of pattern.

If you still don't feel secure enough, check into WPA-based wireless products (see sidebar below). The setup process for WEP and WPA security is nearly identical.


Wireless Network Connection Properties
Wireless Network Properties
?
X

Network name (SSID): 101

Wireless network key (WEP)

This network requires a key for the following:

☑ Data encryption (WEP enabled)

☑ Network Authentication (Shared mode)

Network key: ••••••••••••••••••••

Key format: Hexadecimal digits

Key length: 104 bits (26 digits)

Key index (advanced): 0

☐ The key is provided for me automatically

You Gotta Keep'em Separated

Now that your access point is reasonably secure, it's time to separate your networks. By separating them, you'll deny access to your wired LAN even if a cracker manages to break into your wireless LAN. The separation process involves getting a second hub and a second IP address from your ISP, and then setting up a firewall on your wired network.

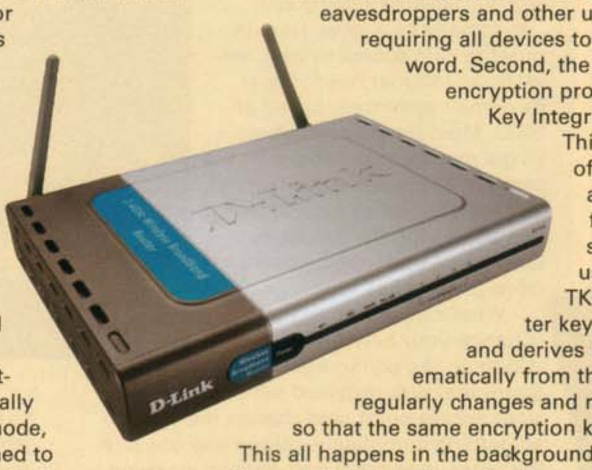
First, you'll need to rewire your wired network. Connect your new hub to your DSL or cable modem, then connect your wired LAN to one port on the hub and your access point to another port. Next, configure your access point with the new IP address. Now you have two separate networks—one wired and one wireless—running off the same broadband modem.

Of course, none of this will do any good if you don't have a firewall on your wired LAN, so make sure you at least have *ZoneAlarm* running on your router.

There's a New Wi-Fi Security Kid in Town: WPA

The increasing attention on wireless security issues has the current security standard, WEP, under scrutiny by vendors and customers. The primary reason for concern is that WEP's encryption method is relatively straightforward, and therefore, vulnerable to a determined and skilled hacker. The Wi-Fi Alliance, in conjunction with the IEEE, has driven an effort to develop an improved Wi-Fi security method called Wi-Fi Protected Access (WPA).

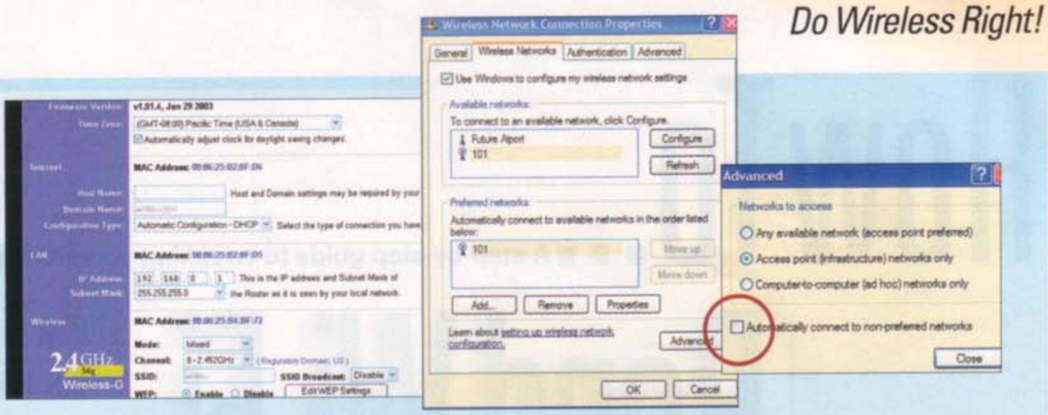
WPA runs in two different modes–enterprise and home mode. In enterprise mode, a network server and sophisticated authentication mechanisms are used to automatically distribute special encryption keys, called master keys. In a home environment, where there are no network servers, WPA allows the use of manually entered keys or passwords, instead. This mode, also called Pre-Shared Key (PSK), is designed to be easy to set up, and the process is quite similar to what we've described for WEP. You enter a password (also called a master key) into your access point or home wireless gateway and into each PC that is on the Wi-Fi wireless network. After you enter the password, WPA keeps out eavesdroppers and other unauthorized users by requiring all devices to have the matching password. Second, the password kicks off the encryption process, called the Temporal Key Integrity Protocol (TKIP).



This is where the mechanics of Wi-Fi Protected Access are substantially different from WEP, where the same static encryption key is used over and over again. TKIP takes the original master key only as a starting point and derives its encryption keys mathematically from this master key. TKIP then regularly changes and rotates the encryption keys so that the same encryption key is never used twice. This all happens in the background automatically, invisible to the user. Together, these features make Wi-Fi Protected Access a stronger security solution than WEP.

For more on WPA, go to http://www.wi-fi.org/opensection/.

Disable SSID Broadcasting



Firmware Version: v1.01.4, Jan 29 2003
Time Zone: (GMT-08:00) Pacific Time (USA & Canada)
☑ Automatically adjust clock for daylight saving changes
Internet
MAC Address: 00:06:25:02:8F:D6
Host Name: Host and Domain settings may be required by your
Domain Name:
Configuration Type: Automatic Configuration - DHCP Select the type of connection you have
LAN
MAC Address: 00:06:25:02:8F:D5
IP Address: 192 . 168 . 0 . 1 This is the IP address and Subnet Mask of
Subnet Mask: 255.255.255.0 the Router as it is seen by your local network.
Wireless
MAC Address: 00:06:25:04:8F:72
Mode: Mixed
Channel: 8 - 2.452GHz (Regulatory Domain: US)
SSID: SSID Broadcast: Disable
WEP: ● Enable ○ Disable Edit WEP Settings

Wireless Network Connection Properties
General | Wireless Networks | Authentication | Advanced
☑ Use Windows to configure my wireless network settings
Available networks:
To connect to an available network, click Configure.
Future Aiport
101
Configure
Refresh
Preferred networks:
Automatically connect to available networks in the order listed below:
101
Move up
Move down
Add... Remove Properties
Learn about setting up wireless network configuration.
Advanced
OK Cancel

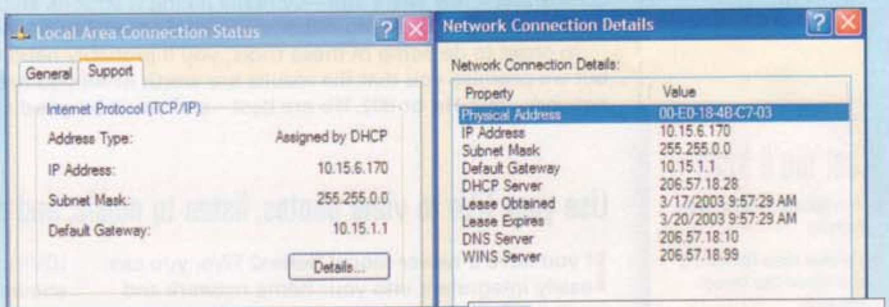
Advanced
Networks to access
○ Any available network (access point preferred)
● Access point (infrastructure) networks only
○ Computer-to-computer (ad hoc) networks only
□ Automatically connect to non-preferred networks
Close

The SSID is your network's name. By default, most access points are set to broadcast their SSIDs to a compatible Wi-Fi device in the vicinity. So not only can crackers discover vulnerable wireless LANs by driving around with Wi-Fi-enabled laptops, but they can also get network names at the same time!

Most access points, however, include an option to disable SSID broadcasting. It's generally a good setting to disable, but we have had some problems maintaining connectivity when using the Windows built-in wireless configuration interface to connect to Wi-Fi LANs with SSID broadcasting disabled. And this problem is exacerbated if other people in your neighborhood have wireless LANs set up.

If you're noticing interference after disabling SSID broadcasting, there's a setting you can change to minimize the problem. Right-click My Network Places and select Properties. Now right-click your specific wireless connection, and select Properties. Go to the Wireless Settings tab, and select the Advanced option. Uncheck the "Automatically connect to non-preferred networks" option.

Super Security



Local Area Connection Status
General | Support
Internet Protocol (TCP/IP)
Address Type: Assigned by DHCP
IP Address: 10.15.6.170
Subnet Mask: 255.255.0.0
Default Gateway: 10.15.1.1
Details...

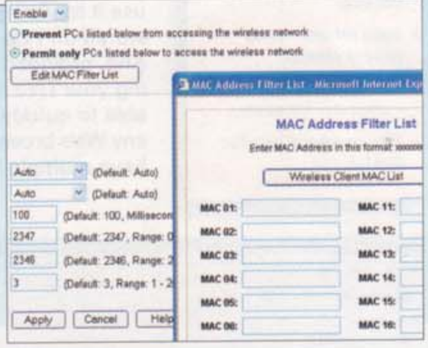
Network Connection Details
Network Connection Details:

Property	Value
Physical Address	00-E0-18-4B-C7-03
IP Address	10.15.6.170
Subnet Mask	255.255.0.0
Default Gateway	10.15.1.1
DHCP Server	206.57.18.28
Lease Obtained	3/17/2003 9:57:29 AM
Lease Expires	3/20/2003 9:57:29 AM
DNS Server	206.57.18.10
WINS Server	206.57.18.99

Most access points are able to deny wireless access to unknown computers. You see, each network card has a unique number assigned when it's manufactured. This "MAC address" is a 12-digit code, and no other piece of network hardware will share the same code. By telling your wireless LAN to grant access only to network cards that have known MAC addresses, you can prevent unknown users from gaining entry.

Each AP will handle MAC address filtering differently, so you'll need to consult your instruction manual. The Linksys interface is pictured above. Just remember, any time you want to add a new authorized user to your wireless LAN, you'll have to get the MAC address, go into your access point's configuration screen, and manually enter it.

To get the MAC address from a Windows XP system, right-click My Network Places and select Properties. Next right-click your wireless network connection and select Status. Go to the Support tab, and press Details. The MAC address is labeled Physical Address in the window that pops up.



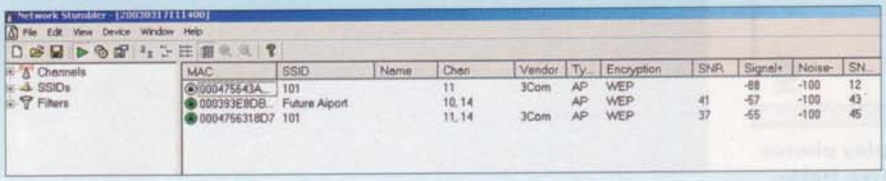
Enable
○ Prevent PCs listed below from accessing the wireless network
● Permit only PCs listed below to access the wireless network
Edit MAC Filter List
Auto (Default: Auto)
Auto (Default: Auto)
100 (Default: 100, Milliseconds
2347 (Default: 2347, Range: 0
2346 (Default: 2346, Range: 2
3 (Default: 3, Range: 1 - 2
Apply Cancel Help

MAC Address Filter List - Microsoft Internet Exp
MAC Address Filter List
Enter MAC Address in this format: xxxxxx
Wireless Client MAC List
MAC 01: MAC 11:
MAC 02: MAC 12:
MAC 03: MAC 13:
MAC 04: MAC 14:
MAC 05: MAC 15:
MAC 06: MAC 16:

Check Your Back

If you've followed all of our instructions, your wireless LAN should be reasonably secure. If the National Security Agency wants into your wireless LAN, there's not much you can do to stop it, but our tips should keep little Billy next door from using your DSL line to download gigabytes of Trent Reznor MP3s.

Regardless, you should still install *NetStumbler* (**www.netstumbler.com**) on one of your wireless PCs, and see if your LAN shows up. *NetStumbler* is the most common 802.11 network sniffer. Most likely, it's what your enemies will be using to discover and compromise your LAN. If you configured everything correctly, your access point shouldn't even show up in this utility's window. If you don't see it, the freeloaders probably won't either, and will just move on to easier prey. ■


Network Stumbler - [20030317111400]
File Edit View Device Window Help
Channels
SSIDs
Filters

MAC	SSID	Name	Chan	Vendor	Ty...	Encryption	SNR	Signal+	Noise-	SN...
000475643A...	101		11	3Com	AP	WEP		-88	-100	12
000393E8DB...	Future Aiport		10, 14		AP	WEP	41	-57	-100	43
0004756318D7	101		11, 14	3Com	AP	WEP	37	-55	-100	45