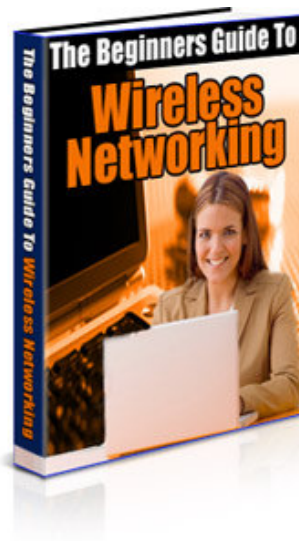


The Beginners Guide To Wireless Networking



What is Wireless Networking?

Wireless networking is just what it sounds like -- a way of creating networks without any wires! If this sounds exciting to you, then read on.

With a wireless network, you can create radio connections between computers that let them communicate and connect to the Internet without you having to go to all the trouble of connecting them with wires. The computers don't even need to have a clear path for the signal, as the wireless signal can go through walls and between floors easily.

Where Did It Come From?

The story of wireless networking is a rather strange one. It is basically an application of a technology called frequency hopping which was, believe it or not, invented by the actress Hedy Lamarr and a musician named George Antheil, back in the 1940s. Seriously, do a web search -- I promise I'm not pulling your leg here.

They received a patent for their invention, which was intended to help in the war effort. Hedy was Jewish, but had been made to hide it and socialise with Hitler as a young woman -- she had to drug her husband and run away to London to escape her native Austria. The importance of what they'd done, however, wasn't recognised until many years later.

The U.S. military adopted the technique in the '60s, using it during the Cuban Missile Crisis. Hedy never saw any money from it as the patent had expired (don't worry, she was a film star!), but she was given a Pioneer Award by the Electronic Frontier Foundation in 1997, three years before her death.

Wireless at Home.

When most people talk about wireless networks, they are talking about wireless LANs (local area networks). A local area network doesn't mean that it covers your whole neighbourhood -- the 'local area' in question can be only one building, such as your house. So if you want wireless networking in your home, you want a wireless LAN.

Once people have wireless in their home, they always seem to act as if there's been an absolute miracle. After years of drilling holes in the walls and running wires all over the place, suddenly seeing them gone is really amazing.

The Myths.

Wireless networking is expensive. Well, wireless networking used to be expensive when it was new, but now the prices have come way down thanks to competition and mass production. There are hundreds of manufacturers of wireless equipment, with something for every budget. Your costs will depend on how many computers you want to connect and how far apart they are, but a typical family should still be able to do it for less than \$100 overall. If you're willing to leave one of the computers on whenever you're using the other one, you could do it for as little as \$20! Best of all, once you've spend the money, there's nothing more to pay after that.

Wireless networking is hard. Again, this myth is a holdover from the early days of wireless. It used to be very difficult, with you needing to fiddle endlessly with the configuration on each computer just to get the simplest things to work. Now, though, Windows supports wireless out of the box, and setting it up is easier than ever. You can usually plug in what you've bought, put the CD in the computer and then sit back and watch it all work perfectly!

Wireless networking is insecure. You might think it's dangerous to have all your personal data floating around in the air for anyone to read. Well, if you want, it's dead easy to enable encryption for your wireless signals. It's already difficult for outsiders to intercept wireless signals at all, and they certainly won't be able to decode them as well.

Not Just at Home.

It was home users that were quickest to adopt wireless technology, willing to pay any amount to finally be free of needing to run wires all over their house. Since then, though, the technology has started to spread to offices, universities, and all sorts of other places.

Chains of coffee shops and cafes have found that their customers will stay for hours if they offer wireless Internet access, and it's also becoming more common in hotels and airports. This means that once you set up a laptop for wireless, it becomes far more portable than it ever was before.

How Do Wireless Networks Work?

Wireless networks work using radio waves instead of wires to transmit data between computers. That's the simple version. If you're curious to know what's going on in more detail, then it's all explained below.

Ones and Zeros.

I'm sure you know that computers transmit data digitally, using binary: ones and zeros. This is a way of communicating that translates very well to radio waves, since the computer can transmit ones and zeros as different kinds of beep. These beeps are so fast that they're outside a human's hearing range -- radio waves that you can't hear are, in fact, all around you all the time. That doesn't stop a computer from using them, though.

Morse Code.

The way it works is a lot like Morse code. You probably already know that Morse code is a way of representing the alphabet so that it can be transmitted over radio using a dot (short beep) and a dash (long dash). It was used manually for years, and became a great way of getting information from one place to another with the invention of the telegraph. More importantly for this example, though, it is a binary system, just like a computer's ones and zeros.

You might think of wireless networking, then, as being like Morse code for computers. You plug a combined radio receiver and transmitter in, and the computer is able to send out its equivalent of dots and dashes (bits, in computer-speak) to get your data from one place to another.

All About Frequencies.

You might wonder, though, how the computer could possibly transmit enough bits to send and receive data at the speed it does. After all, there must be a limit on how much can be sent in a second before it just becomes useless nonsense, right? Well, yes, but the key to wireless networking is that it gets around this problem.

First of all, wireless transmissions are sent at very high frequencies, meaning that more data can be sent per second. Most wireless connections use a frequency of 2.4 gigahertz (2.4 billion cycles per second) -- a similar frequency to mobile phones and microwave ovens. As you might know, though, a frequency this high means that the wavelength must be very short, which is why wireless networking only works over a limited area.

In addition, wireless networks make use of a technique known as 'frequency hopping'. They use dozens of frequencies in the range they are given, and constantly switch between them. This makes wireless networks more immune to interference from other radio signals than they would be if they only transmitted on one frequency.

Access Points.

The final step is when it comes to all the computers on a network sharing Internet access. This is done using a special piece of wireless equipment called an access point. Access points are more expensive than wireless cards for one computer, as they contain radios that are capable of talking to around 100 computers at the same time, and sharing out access to the Internet between them. Dedicated access points are only really essential for larger networks, though -- if you only have a few computers, it is possible to use one of them as the access point, or you could just get a wireless router.

They Understand Each Other.

That's all well and good, then, but how does wireless equipment made by entirely different companies manage to work together when this is all so complicated? Well, the answer is that there are standards that all wireless devices follow. These standards are technically called the 802.11 standards, and are set by the IEEE (Institute of Electrical and Electronics Engineers). It is thanks to people sticking to their standards that wireless networking is so easy and cheap to use today.

You Don't Need to Worry.

If all this talk of frequencies has you a little worried, you don't need to be -- wireless networking hardware and software handles all of this automatically, without you needing to do a thing. Don't think that you're going to have to tell one wireless device what frequency another is using, because it's just not going to happen, alright? Wireless networking, for all its complicated workings, is really far more simple to use than you'd ever expect.

5 Reasons Why You Need a Wireless Network.

As far as I'm concerned, wireless networks are one of the best inventions in history -- they really are the best thing since sliced bread. I mean, really, bread is easy enough to cut yourself, but have you ever tried to wire up a network? So, in the spirit of spreading the word, I'm going to give you five reasons why you need a wireless network.

Share Internet Access.

Wireless networking gives you a cheap and easy way to share one Internet connection between multiple computers, eliminating the need for more than one modem. You can even add new computers to your network simply by plugging in a wireless card and switching them on -- they get an Internet connection straightaway! There aren't many wired networks that can say that.

Share Files and Printers.

A wireless network gives you access to your files wherever you are in your home, and makes it easy to synchronise the data on a laptop with a home computer. It is much easier to send files between computers with a wireless network than it is to send them by email, or even by burning them to a CD.

Plus, with the printer connected, you can also write things wherever you want, press print, and go and collect them from a printer connected to another computer -- printers that are plugged into one of the computers on the network are shared between all the computers automatically.

Play Games.

You might have seen an option in your favourite game to play over a LAN. Well, wireless networks are LANs, which means that your whole family can play that game together -- without needing the computers to be anywhere near each other. It's far more fun to play against real people you know than to play against random people over the Internet, not to mention that the game will work much faster. You could even invite your friends to bring their computers and join in -- a 'LAN party'!

An added benefit is that wireless equipment lets you easily connect any games consoles you or your kids might have to the Internet, and start playing online. It's far easier to play online with a wirelessly connected Xbox or PlayStation 2 than to have to connect it to your modem every time.

Always On.

A big factor in the spread of broadband was that it let Internet connections be always-on, without needing to dial in. Well, wireless networking lets network connections be always-on, meaning that any of your computers can connect to the Internet whenever you want! You can take laptops from room to room, and it doesn't matter -- they'll always have access. Plus, there's not even any need to set up a username and password system, as wireless networks work without logging in. It's just so convenient!

No More Wires.

This, of course, is the biggest reason why you should switch your network over to wireless. Wires are inconvenient, expensive, ugly and dangerous -- you'll be delighted to see the back of them.

The average Ethernet wire doesn't cost that much per metre, but once you've bought enough metres to do whatever you need to do, well, it tends to add up quickly. Not only that, but if you want to run your wire between rooms or floors, you have to knock holes in the walls -- which might not even be allowed if you're renting. I know plenty of people in rented apartments who had to keep their network confined to one room until they went wireless. With wireless networking, well, you can even take your computer outside, if you want to!

No more wires also means no more spaghetti all over the floor and in the corners. Not

only does this improve the safety of your home, as it's all too easy to trip over exposed wires, but it also means that you don't have to go to all the trouble of packing all the wires up and re-connecting them at the other end when you move. It also means that you don't have to examine every wire for damage if your Internet connection breaks down.

Convinced?

If you're excited, then that's great -- keep reading this ebook for advice on how to set everything up. If you don't think it's for you yet, well, don't give up on it -- I'm sure you'll come round when you realise just how easy and cheap wireless really is.

Confused Yet? Wireless Jargon.

Wireless networking, like so many things in life -- and especially the ones that have anything to do with computers -- is filled with jargon. Don't be intimidated, though: here's a quick computer-speak to English guide to help you get by.

802.11. The name of the wireless networking standard, set by the IEEE. Ensures that wireless devices are interoperable.

Driver. A piece of computer software that tells the computer how to talk to devices that are plugged into it. For wireless networking, the drivers you need to install will come on a CD with any equipment you buy.

Ethernet. The most common way of connecting to a LAN. Any wires you might have connecting your computers together now are Ethernet wires, and the cable connecting your modem to your computer is probably an Ethernet wire too.

Ghz. Gigahertz. A measurement of frequency -- one gigahertz is one billion cycles per second. You may recognise the measurement from computer processor speeds, which are now also measured in Ghz.

IEEE. The Institute of Electrical and Electronics Engineers. In charge of the wireless networking standard, as well as many other computer-related standards (including the Ethernet standard). They ensure that computer equipment made by different manufacturers can work together.

Interoperable. Means that two pieces of equipment are compatible -- you can use them together, because they stick to the standards. You should not get any wireless equipment that isn't interoperable.

LAN. Local Area Network. A network that is generally confined to one building, such as a home or office. A wireless LAN is also known as a WLAN.

Linux. An alternative operating system to Windows. Computers running Linux can run many programs and connect to the Internet without needing Windows. Linux is free to download and you are allowed to give it to friends to use. A lot of wireless devices run Linux, or are compatible with it.

MAN. Metropolitan Area Network. A network that covers a larger area, for example a town or city. Wireless MANs (men?) spread Internet access all over the area, but are expensive to set up. They are sometimes used on university campuses.

Mbps. Megabits per second, a measurement of connection speed. Not to be confused with MBps, megabytes per second. There are eight megabits in a megabyte.

PAN. Personal Area Network. These are networks made up of devices connected together in one small area. For example, your computer with a USB keyboard and mouse connected is a PAN. PANs can be wireless, using a technology called Bluetooth.

PCI. Peripheral Component Interconnect. This is a way of installing new devices inside your computer, such as graphics cards and network devices. If you want to install a wireless card inside your computer, you will be using PCI.

PCMCIA. Personal Computer Memory Card International Association (some say it should stand for 'People Can't Memorise Computer Industry Acronyms'). A standard for plugging credit card-sized devices into a laptop, to give it extra capabilities. PCMCIA is a great way of adding wireless networking to your laptop as easily as inserting a disk.

USB. Universal Serial Bus. A port used for connecting all sorts of devices to a computer, including keyboards, mice, printers, external drives, and almost anything else you can think of. If you don't want to open up your computer and you don't have a laptop, you can get a USB wireless device.

WAN. Wide Area Network. A network that is connected over more than one physical site, such as a business that has its computers in two countries connected on one network.

The Internet, for example, is a WAN -- the biggest WAN in the world.

WEP. Wired Equivalent Privacy. The old standard for encrypting wireless networks. Unfortunately, it was found to be insecure back in 2001, and so should no longer be used.

WPA. Wi-Fi Protected Access. Basically an upgrade of WEP to fix its security problems. WPA-encrypted networks change their encryption method often, to avoid becoming vulnerable, and also shut down for thirty seconds if they detect a suspected attack.

Could You Already Have Wireless and Not Realise It?

More and more laptops and desktop computers are coming pre-equipped with wireless networking devices -- it's so cheap that they might as well put it in, to have another thing to list in the system specifications.

If you're anything like me, though, you probably don't even know how much memory your computers have, never mind whether any of them came wireless-enabled. When you don't know what wireless networking is, it's easy to ignore it in a computer's specifications, and never take the time to set it up and get it working. Here are some things to look for if you want to check your computer's wireless capabilities.

Intel Centrino.

If your laptop came with something called 'Intel Centrino mobile technology', then it's good news for you! Computer manufacturers seem a little bad at explaining what this technology is or does, but it basically means that your laptop has wireless networking built right in, without you needing to do a thing. It is a marketing name for a combination of the Intel Pentium M processor and Intel's Pro/Wireless card.

Your computer should have a 'Centrino' sticker on it somewhere if it is Centrino enabled. If you think you might have taken the sticker off, you can check the name of your processor by right clicking the My Computer icon on your desktop (or in the Start Menu) and choosing Properties from the menu that appears. Take a look at what it says after the word 'Computer' on this screen.

If you're interested, Centrino technology also increases battery life and allows computers to be smaller. Don't worry, though, if you didn't buy a Centrino laptop -- as long as your laptop has a free card slot, installing wireless on it will be no trouble.

Desktop Computers.

If you're not sure whether your desktop computer has a wireless connection, the easiest thing to do is to turn it around and look at it. If a wireless connection is present, you should usually be able to see a small aerial sticking out of the back of the computer, towards the bottom.

If there's nothing there, then it's still possible that you have a wireless device in the computer, especially if you bought it recently and you think you do. It's not a good idea to try to open up your computer just to check something, though, so you should probably try and figure it out using Windows.

Checking in Windows.

Instead of fiddling around with your computer hardware to see what you've got, you can check easily enough using Windows' Device Manager. To use it, right click My Computer, and choose Manage from that menu. Now click Device Manager.

You should see a list of all the different kinds of things you can install on your computer. Take a look under 'Network adapters'. Ignore anything that says '10/100' or 'Ethernet' -- they're normal network connections, but not wireless ones. If there's anything else there, it could be a wireless device.

If you think you have a wireless device, but it has a yellow warning sign next to its name in the Device Manager, you should take a look at it to see what's wrong by double clicking its name. Windows should tell you why the device is not working at the moment, and may suggest that you go through its troubleshooter program. Do that before you do anything else.

If it turns out to be a driver problem, you should insert the drivers CD that came with your computer. Of course, as is always the way, you probably won't be able to find that CD -- but don't worry, you should be able to find drivers online. First, you should look on the website of the computer's manufacturer, and then you should try searching for the name that the wireless device had in Device Manager.

Of course, you might find after all this that you don't have a wireless device after all. Hard luck. It's better to figure that out now than to buy wireless equipment and then realise you had some already, though, isn't it? Of course, even if you did find a wireless device in one of your computers, you probably still need more. Don't worry either way -- they're getting cheaper all the time!

5 Things You Must Do Before You Buy Any Wireless Equipment.

Before you buy any wireless equipment, you need to be sure about what you're doing. There's nothing worse than having everything there and finding that it doesn't work in your house, or with your computers, or over the distances you need. Here's a handy checklist of the things that you really ought to do before you go out and spend any of your hard-earned cash on wireless networking equipment.

Check What Your Walls are Made Of.

Wireless can, in theory, pass through walls and other partitions easily. In practice, though, some walls are more solid than others, which means that they are more likely to block some of the signal. Note that it's only your interior partitions that matter, not the exterior ones. This does, however, include your floors, if you want the connection to work between levels.

Wireless does well with partitions made from: drywall, plywood, other wood (including doors), glass.

Wireless has trouble with: brick, plaster, cement, metal, stone, double-glazed glass.

Basically, it's all to do with how porous the materials are -- ones that let more of other things through also let more of your wireless signal through.

If you have a wall made of one of the 'bad' materials, it's not the end of the world. It just means that your wireless connection might have a slower speed or a shorter range. You may want to spend more than you otherwise would to get better equipment and overcome this problem.

Check for Possible Interference.

While it won't stop a wireless network from working altogether, interference in its frequency range can slow it down significantly, as well as reducing its range. If something is causing interference, the first thing you'll know about it is when your connection stops working -- unless you know what to look for.

There are two very common causes of wireless interference: wireless phones and microwave ovens. 2.4Ghz, the most common wireless networking frequency, is also a commonly-used wireless phone frequency. It is possible, though, to find phones that use other frequencies. Microwave ovens, on the other hand, operate at around 2.4Ghz by definition. It should be alright to have devices like these in your house, but certainly not in the same room as any computer that you plan to use a wireless connection with.

Decide Your Budget.

You need to stand back, take a look at your needs, and decide how much you're going to spend. Do you have long distances to cover? Do you want your connection to go through stone walls? Each factor will help you decide how much you should be looking to spend -- remember that the more problems you have, the more power you will need. On the other hand, if you live in a small wooden house, you can probably just go for the cheapest thing you can find.

Read Other People's Reviews.

It's well worth searching a site like amazon.com for wireless equipment, and taking a look at people's reviews to see what the different brands out there are like, and what you can get for your money. It is always a very bad idea to buy something without getting a second, third and fourth opinion, especially if you're buying it online. If you can, try to get to a computer shop and see some wireless networking equipment in action before you commit yourself.

Install and Update Windows XP.

Finally, your wireless life will really be improved if you have the latest version of Windows. Because wireless is such a new technology, it wasn't really around in any

significant way back when Windows 98, ME and 2000 were released, and support for them wasn't built in to the system. You'll have a lot more trouble getting wireless to work on systems like these than you would on Windows XP.

Even if you've got Windows XP, though, that doesn't solve the problem entirely. Windows XP Service Pack 2 (an updated version of Windows XP) contains much easier-to-use tools for configuring and using wireless than the un-updated versions do. If you've been using your copy of Windows for a while without updating it, you should really make sure you've got all the latest updates from <http://windowsupdate.microsoft.com> before you go any further.

Ports and Cards: How to Tell What You Need.

There are all sorts of different devices you can buy that will give your computer wireless networking capabilities. If you've taken a look around, though, you might have been confused by all the kinds of equipment being offered -- how things that look so dissimilar do the same task?

Essentially, the main difference between wireless devices is in how they connect to your computer. There are three main connection methods: PCI, PCMCIA and USB.

Desktops: PCI Cards.

PCI stands for Peripheral Component Interconnect. It is an old and established way of installing new equipment in a desktop computer. If you find a wireless card that looks like a green rectangle with something sticking out of the end, then what you've got is a PCI card.

To install a PCI card, you need to -- horror of horrors -- actually unscrew your computer, take the cover off, and plug the card in inside it. Scary as that might sound, it is designed to be very easy, and once it's done your computer will have internal wireless networking capabilities for the rest of its life.

You should go for this option, then, if you own a desktop computer, and you're not afraid to get your hands dirty (perhaps literally -- I've seen years worth of dust in those things) by installing it yourself. Or, of course, if you're willing to pay someone to do the installation for you.

Laptops: PCMCIA Cards.

PCMCIA stands for Personal Computer Memory Card International Association. A PCMCIA slot is a small slot in your laptop that allows you to insert these cards and so add functions to your laptop quickly and easily. They were originally for memory expansion, but are now more often used for networking.

Almost all laptops have PCMCIA slots. If you're not sure whether yours does, take a look at the side of the machine -- you should see a slot there, probably near the CD drive. Even if you do have a slot, you need to make sure it's free, by pressing the button to eject anything that might be in there. If it's an Ethernet card then, well, not to worry, as you can just replace that, but if it's anything else then you might want to consider using USB instead.

For 99% of laptop owners, at least, it's best to use PCMCIA -- the only reason some go with USB is because they didn't know they had an alternative.

The Third Way: USB.

Whether you're using a desktop computer or a laptop, you can use USB (Universal Serial Bus). USB ports look like very small slots, and could be almost anywhere on your computer -- but it will help you to locate them if you remember that they very rarely appear in groups of less than two. Computers have come with these USB ports for years now, and newer computers often come with four or even more. If you need more space, you can buy a splitter (a USB hub) that allows you to use more devices than you have ports for.

So where's the problem? Well, you wanted a wireless network, right? With USB, your network won't be entirely wireless, as there will still be a small wire between your computer and the USB device -- it might not sound like much, but it makes USB wireless on laptops a bit of a joke.

Another factor is that small USB devices are very easy to break -- when I used to use USB wireless, I went through three new receivers inside a year. This is offset, of course, by the fact that USB wireless cards are usually the cheapest ones, and are far simpler to install than PCI.

Essentially, if you're a laptop user without a free PCMCIA slot, or you're a desktop user

who doesn't relish the prospect of opening up your PC, then USB is a good 'third way' for you.

If you do go the USB route, however, and you have a reasonably new computer, you should check whether the device you're buying supports USB2. Most newer computers have USB2 ports, and using specially-designed USB2 devices with them can give you a significant speed boost.

What to Look For: Range, Speed and Standards.

Not sure what you're doing in your wireless card shopping? Want to make sure you're buying the right thing but just have no idea what it is you're looking for? Well, you've come to the right place. When you're looking to buy a wireless network card, I can tell you right now that you're looking at three key issues: range, speed, and standards.

A Typical Specification.

This is a specification for a Linksys wireless PCMCIA laptop card I just bought:

11 Mbps high-speed transfer rate; interoperable with IEEE 802.11b (DSSS) 2.4Ghz-compliant equipment; plug-and-play operation provides easy set up; long operating range (up to 120m indoor); advanced power management features conserve valuable notebook PC battery life; rugged metal design with integrated antenna; compatible with virtually all major operating systems; works with all standard Internet applications; automatic load balancing and scale back; model no. WPC11. (source: amazon.com).

Now, some of those things can be pretty much ignored. Really, 'virtually all major operating systems'? That means nothing. The reason I've put it here, though, is so you can see which things are important to keep an eye out for.

Range.

See where it says 'up to 120m indoor'? This tells you that the maximum range of the wireless card you're looking at is 120 metres -- that's what it would be if everything was perfect. In practice, thick walls and interference can reduce this number by as much as 90%.

Without enough range, your wireless network is going to be pretty useless. It's not much fun having no wires when you have to keep all the computers in the same room to get them to connect to each other.

As a rule of thumb, unless your walls are made of drywall or wood, it's best to buy about four times the strength you'd think you'd need. Even in perfect conditions, get twice as much, to be safe. If you need to convert from metric to imperial units, remember that there are 30 centimetres (0.3 metres) in a foot and about 2.5 centimetres in an inch -- you shouldn't have too much trouble.

Speed.

Do you see where it says 'Mbps' in that description? That number is the speed of the wireless connection. 11 Mbps is about one and a half megabytes per second -- to convert megabits (Mb) to megabytes (MB), just divide by eight. 802.11b wireless cards all have a speed of 11Mbps, while 802.11g ones run at 54Mbps -- the next generation will be even faster.

Speed is important to your wireless network because it's going to directly influence how long you have to wait for things like files to transfer from one computer on the network to the other. It is less important for Internet use, however, because there are currently very few Internet connections running at speeds over 11Mbps -- it's really as much as you need, at least for now.

Standards.

Somewhere in the specification of what you're looking at, you should see the number '802.11', followed by a letter 'a', 'b' or 'g'. This is the standard that the wireless device conforms to, and tells you whether you will be able to use it with your other wireless devices.

Basically, 802.11b and 802.11g are compatible with each other. 802.11a is not compatible with either and is quite a bad standard all round, so you shouldn't buy 802.11a. Out of b and g, b is cheaper but slower, while g is more expensive but faster. It's worth considering that adding a b-speed device to a network that has g-speed devices will often slow the whole network down to b-speed, making the g-devices

pointless.

If your wireless device doesn't conform to the right standards, it's not going to be much good to you. I often see naive people bidding for used wireless equipment on eBay, not realising that it's going to be terribly slow and not work with any other equipment they might have. Always make sure that you check what standard the wireless equipment is -
- if you don't know the 802.11 letter, don't buy it!

Wireless Alphabet Soup: What's the Difference Anyway?

At this point, you might have read a few feature lists for wireless cards, and you're about to ask a very common question: what's the difference anyway? Well, answering that question requires a brief rundown of the history of wireless networking so far.

The Beginning: 802.11.

The first wireless networking standard was simply called 802.11, without a letter after its name, and was released in 1997. It is now sometimes called 'legacy 802.11' -- no-one uses the original 802.11 standard any more.

The 802.11 standard was never really popular to begin with, in fact, mainly because it offered wireless equipment manufacturers so many different choices on which parts of the standard to implement. This left users in a situation where they were more-or-less stuck with one set of wireless devices, and interoperability was hard to come by.

A Breakout Hit: 802.11b.

With the revision of the standard in 1999, 802.11 became 802.11b, and that's when things really started to take off. 802.11b streamlined the standards to provide greater interoperability, without making too many changes -- existing wireless devices were easily upgraded to the new standard, which meant that 802.11b wireless appeared on the market quickly.

Many advantages came with the upgrade to 802.11b. It was over ten times faster than 802.11 (11Mbps instead of 1Mbps), and yet cheaper. People loved 802.11b, and it was around this time that wireless networking technology started to take off in a big way.

Oops: 802.11a.

As a counterpoint to the 802.11b success story, consider 802.11a. The a and b standards were originally intended to present a choice to the consumer, with a offering higher speeds than b in exchange for reduced range. As it turned out, though, 802.11a was an utter failure.

Why? Well, 802.11a's downsides were simply too great to bear. Sure, it gave speeds of 54Mbps -- almost five times faster than 802.11b -- but it would only work if you had a clear line of sight between the two wireless devices. If there's nothing between the devices then, well, why not just use a wire?

As a final nail in the coffin, 802.11a products didn't start to appear on the market until 2001. By then, people were used to 802.11b, and no-one was interested in getting a speed increase in exchange for such a dramatic range decrease.

Speed With No Downsides: 802.11g.

In 2003, with the lessons of the 802.11a failure learned, a new standard was created -- 802.11g. The aim of this standard was to combine the best of both worlds, giving the speed of 802.11a with the range of 802.11b.

Well, it was some time in the making, but they managed it. 802.11g devices run at 54Mbps, but are otherwise the same as 802.11b ones. Even better, 802.11g devices are backwards compatible with 802.11b ones, meaning that you can use them together in your network.

What to Choose.

So you know the advantages and disadvantages of everything, but what should you choose if you're buying a wireless device today?

Well, first of all, avoid legacy 802.11 (if you somehow find it) or 802.11a. They will not work with your other wireless equipment, and are generally quite useless.

That leaves you with the choice of 802.11b or 802.11g. Considering that most broadband

connections run well below the speed of 802.11b (11Mbps), which you choose probably won't make any difference to your external Internet access. The area where it matters is when you transfer things around within your network -- if you're sending a file from your laptop computer to your desktop one, for example, it will happen five times faster with g than it would with b.

There is another consideration in your decision, however, and that's price: g devices are still quite a lot more expensive than b ones. If you're mainly planning to use your wireless network to connect to the Internet then b will do everything you need, but that hasn't stopped lots of people upgrading to g who didn't really need to. This means that the market is flooded with cheap 802.11b wireless equipment that still works perfectly!

If you want to know the secret of wireless networking on a budget, then that's it: get 802.11b equipment for a few dollars, then sit back and watch your network work just as well as the ones that cost hundreds.

10 Steps to Install a PCI Wireless Card.

Installing a PCI wireless card might seem like a bit of an adventure -- after all, you have to open the case, find where to put the thing, close it again... and then you have to deal with the software! Even if you've never opened your computer before, though, you shouldn't have too much trouble with it if you follow these steps.

Step 1: Look at the Manual. Yes, I know it seems like a dull thing to do, but you really need to at least skim the manual for things if you're going to go putting them in your computer. It's much better to do it now than to realise afterwards that you missed an essential step in the installation. A few cards, for example, require you to install the software before installing the card -- do this now if you need to.

Step 2: Switch the Computer Off. Before you even think about opening the computer, you've got to switch it off. You should use the 'Shut Down' option to make sure that the computer will start fresh next time, and wait for it to shut down completely.

Step 3: Unplug the Computer. To be safe, you should disconnect the computer from the power supply now. If there is anything connected to the computer, you should unplug that from the power too, as well as unplugging the wires from the back of the computer. If you're nervous that you won't remember which wire goes where when it's time to put them back again, you could draw a diagram before you start this step.

Step 4: Remove the Case. To avoid damaging your computer's parts or electrocuting yourself, you should be wearing an anti-static wristband (also known as a ground strap) whenever you open your computer. If you're not sure how to get the case off, consult your computer's manual. It's usually just a matter of unscrewing, though -- but make sure you keep the screws somewhere where they won't get lost.

Step 5: Find an Empty PCI Slot. PCI slots are long, rectangular slots inside the computer. Some of the available PCI slots might be used by existing modems or Ethernet cards. If there's no space for your new wireless card, then you might need to remove some of this old equipment.

Step 6: Insert the PCI Card. If you're using a PCI slot that hasn't been used before, you'll need to unscrew the piece of metal filling the gap in the back of the computer created by there being no card there. Make sure you store this piece in a safe place, in case you ever need it again.

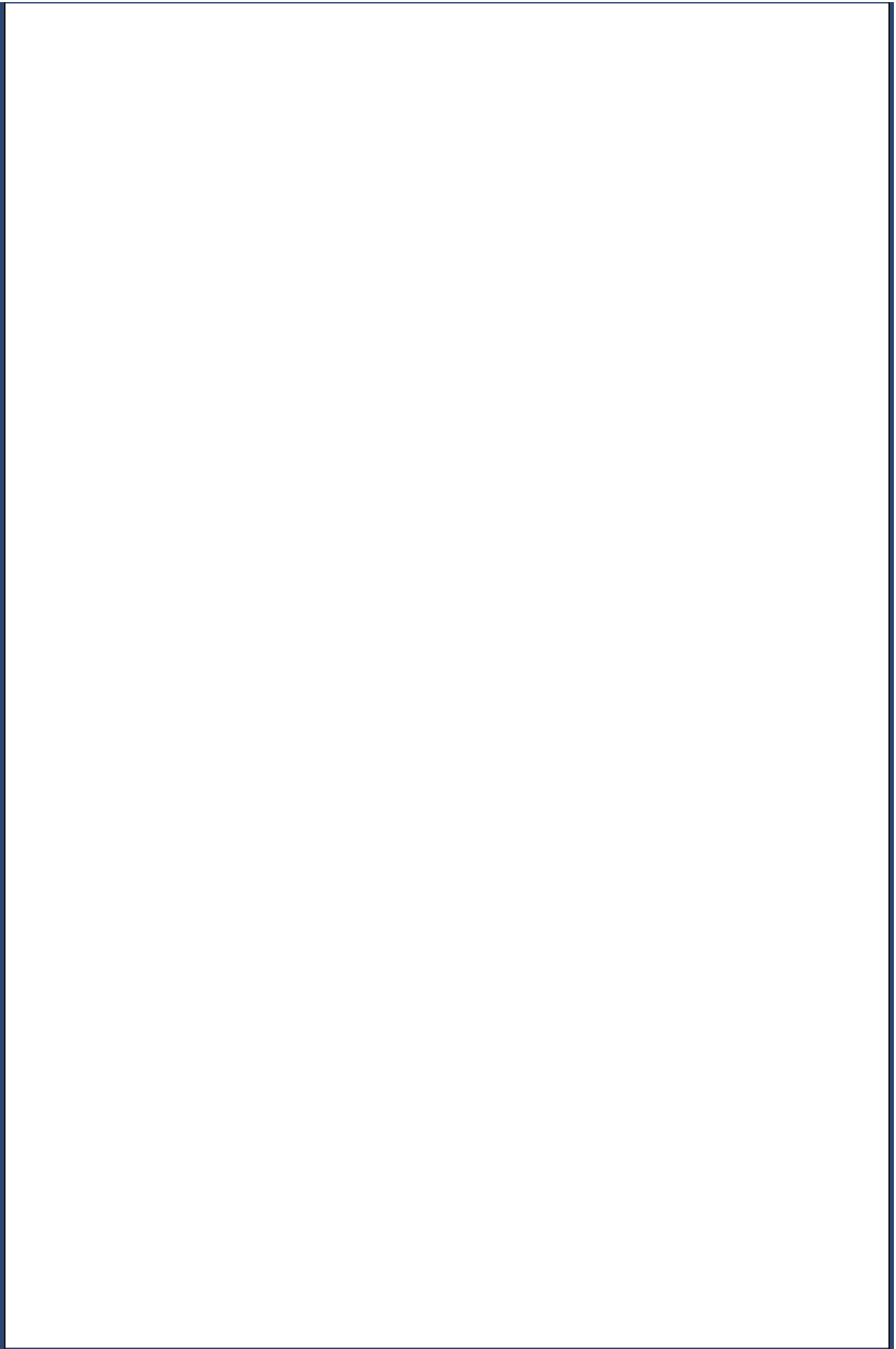
When you insert the PCI card into the slot, do it as carefully as you can. Try not to touch any of the circuits on the card. Once it's in the slot, you will need to press firmly, but don't use too much force. You should also make sure that you point the wireless card's antenna upwards.

Step 7: Close the Case. Just do what you did in step 4 in reverse -- put it all back together.

Step 8: Plug In and Start. You need to plug your computer back in and start it. If you don't want to re-attach all your wires right now, you will at least need to plug in the keyboard, mouse and monitor. Many people are scared when they turn on their computer again after installing a PCI card and it doesn't work -- only to find that the error was caused by them not reconnecting their keyboard!

Step 9: Install Drivers and Software. Once the computer's done starting, it should notice it has some new hardware. This is when you should insert the CD that came with the card, and leave Windows to do its thing. If everything's gone to plan, the PCI card should be set up automatically. If things don't happen automatically, try inserting the CD before you panic.

Step 10: Configure Your Network. Your PCI wireless card gives your computer a permanent wireless connection. The first time you use it, you should be asked which wireless network you want to connect to. Choose your wireless network from the list, and you're ready to go!



Ad-hoc or Access Point? Network Structures Explained.

What happens to many people is that they're just about to buy some wireless equipment, and then they have a sudden realisation -- they have no idea how their network layout is going to work with a wireless connection. Well, there are a few things you need to think about when you decide how you're going to connect up your computers with all that great new wireless stuff.

Ad-hoc Networks.

Ad-hoc networks are the ones your wireless devices create more-or-less on their own -- they are also known as peer-to-peer networks. In an ad-hoc network, each computer on the network acts as an equal 'peer', with each one sending data to any other. This arrangement is most often used in place of a real LAN, to allow employees in a company, for example, to exchange files. You can create ad-hoc wireless networks between any computers that have wireless equipment -- access to the Internet is not required.

These networks work using something called an 'SSID' (Service Set Identifier). Essentially, this is the network's name, decided on the computer that was the first to connect to the network (yes, a network consisting of just itself). The other computers that connect to the network can then simply connect by finding the network with the name (SSID) they want.

This is powerful. You can put your wireless-enabled laptop next to a friend's, and the two computers can create a little network for themselves on the fly. Thanks to the way wireless networking works, they keep the connection even if you move them around -- the only thing that will force the computers to disconnect from each other is if they go out of range. For many people, this spells the end of messing around with CDs and floppy disks -- they can finally use their laptop just like a briefcase, carrying everything from one place to another.

Arriving somewhere with your laptop and being automatically included in the wireless network also gives you access to shared resources, such as printers. Imagine being able to take your computer to somewhere where there's a printer, press print, collect the document and walk away again. Ad-hoc networking makes this a reality.

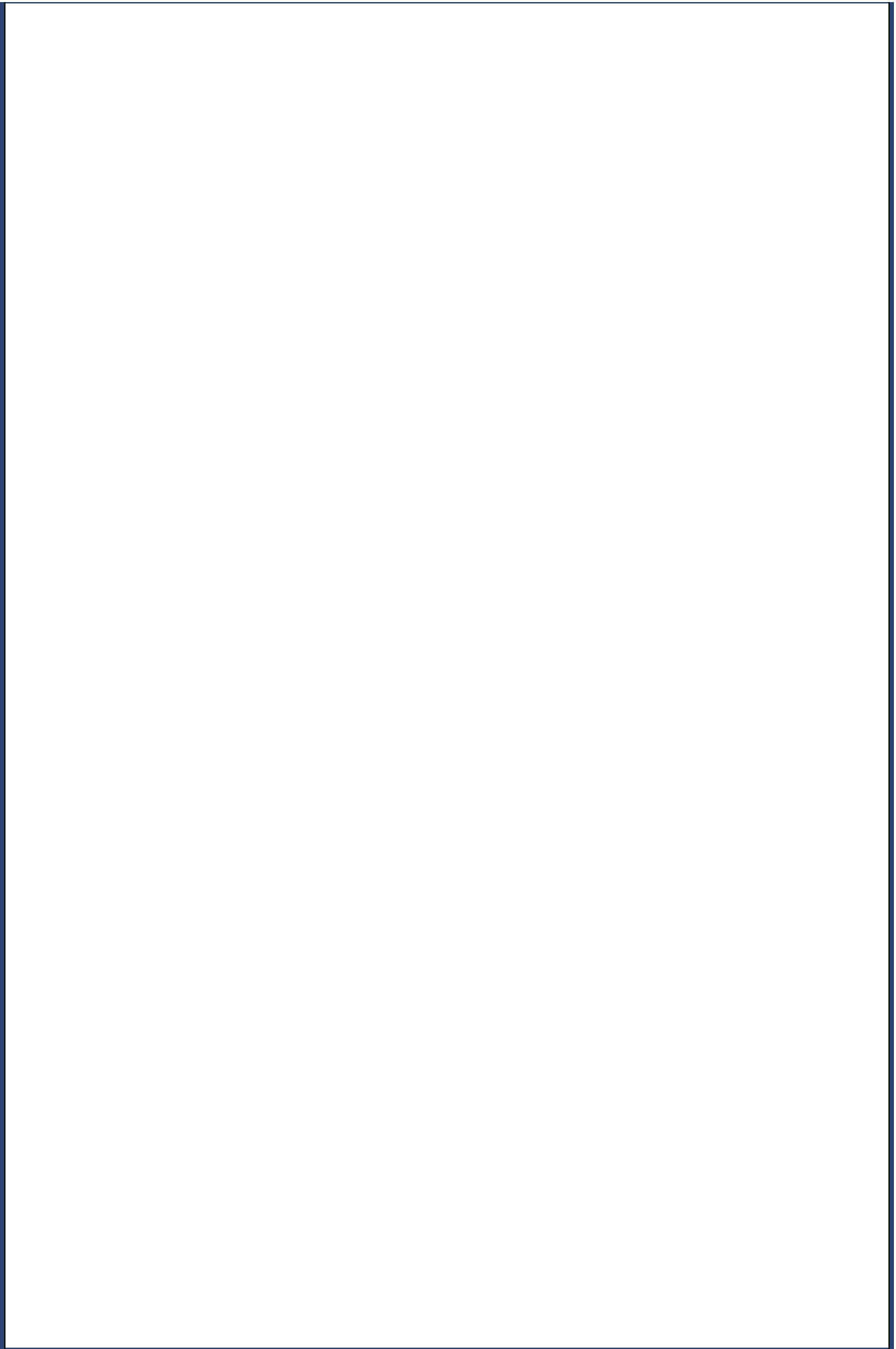
Access Points.

An access point, on the other hand, is a way of connecting your ad-hoc wireless network to a real, wired network. Note that this network could just be a LAN, or it could be the entire Internet. There are hardware access points and software ones, with either kind allowing you to connect your wireless device to a wired network. Internet Connecting Sharing, for example, is a software access point to the Internet, while a wireless router is a wired one. If you have wireless access at your office, the chances are it is provided as a wireless access point to the wired network, to let people bring in wireless devices and connect them to the office LAN.

A network that contains an access point is sometimes called an 'infrastructure' network, as opposed to an ad-hoc one. It's worth remembering, though, that part of the infrastructure network still consists of the ad-hoc network between the computers -- they can still communicate just the same as they could before.

If you think about it, you can see that the access point structure allows you to create a series of networks, all interconnected. The Internet, in this scheme, is just another wired network. You can connect your wired network to the Internet, connect your wireless network to an access point to your wired network -- whatever you want.

The string of networks is potentially never-ending, with wired networks being able to break out into wireless ones as often as they need to. This concept is sometimes called lilyypad networking, because it lets your computer be like a frog, hopping from lilyypad to lilyypad. Even though the whole area of the water isn't covered with lilypads, the frog can still get through -- and you can make wireless networks work the same way.



Fighting with Windows: Getting Wireless Set Up.

It was supposed to be so easy, wasn't it? Well, usually it is -- but sometimes, for some reason, Windows just doesn't want to play ball. Here's a quick guide to what to do when you've plugged in all your wireless equipment but it's not connecting yet.

Insert the CD.

It's not enough to just plug in your wireless card the first time you use it -- you need to put in the CD it came with and install the drivers. If you've already done that and there's still nothing, then you might need to update your drivers by paying a visit to the manufacturer's website.

Note that the instructions below apply to Windows XP. If you're determined to use Windows XP, then what you need to do next will be different depending on your wireless equipment's manufacturer -- you should take a look at your manual.

Use the Wireless Network Setup Wizard.

While it's easy to use Windows to connect to an existing wireless network, you still need to create the wireless network to begin with. Don't worry -- once you've created it once, your whole network will be able to connect to and remember it, even if the computer you used to create the network is never switched on again.

The easiest way to open the Wireless Network Setup Wizard is through the Start Menu: go to All Programs, Accessories, then Communications, and you'll find it there. If you can't find it, you might need to visit Microsoft's Windows Update at <http://windowsupdate.microsoft.com> to get it.

The first thing to do when the wizard appears is read the welcome message, and click Next. Type a name for your network -- anything will do, as long as it's relatively unique to you. You're allowed up to 32 letters to express yourself, but remember that your neighbours might get to see this name at some point! If you bought equipment with WPA (stronger encryption), tick that box. Click Next again.

Unless you have a USB flash drive (it's unlikely), choose the option for manual setup. Don't worry -- it's just a matter of printing out some settings and entering them into your other computers. If you don't use encryption, you can usually skip this step.

It Still Doesn't Connect.

On one of your other computers, right-click on the wireless icon in the bottom-right corner of your screen -- it looks like a small computer with two lines on the right of it. On the menu that appears, click 'View Available Wireless Networks'. Now, you should see a list of the wireless networks your computer is in range of. Look for the name of your own network. This will be the name you typed in the setup wizard earlier or, if you use a router, it will probably be the name of your wireless equipment's manufacturer.

Note that this is the screen to come to if you ever want to connect to a wireless network other than your usual one -- just double click the one you want, wait a while, and it should work.

The most common problem is to find that your computer is trying to connect to another network near you, usually one belonging to your neighbours. If their wireless network has an unnecessarily wide range, it's not at all unusual for you to be able to receive their signal in your house -- I sometimes find as many as five networks in my area available to connect to. Fun as it would be, though, to go through all their shared files, your priority right now is getting their wireless network out of the way to let you connect to your own.

Getting on Your Network.

To make sure Windows knows which network is yours, you need to click 'Change the order of preferred networks' on the left of the available networks screen. You should click the 'Add' button to add the name of your network to this list, and use 'Remove' to take

away any that aren't yours.

When you've highlighted your network, click Properties, and then go to the Connection section. Make sure 'Connect when this network is in range' is ticked. If all else fails, you might have to take your printout from the Wireless Network Setup Wizard and enter that information on each computer.

Sharing an Internet Connection over a Wireless Network.

Once you've got your wireless network set up, I've no doubt that one of the first things you'll want to do with it is share an Internet connection -- after all, that's why most home users put in a wireless network to begin with. Well, the good news is that Windows has Internet Connection Sharing built in. The bad news is that setting it up can sometimes be a little less than fun.

How Internet Connection Sharing Works.

When you set up Internet Connection Sharing, you set up one of your computers as a 'gateway' to the Internet, and then use this gateway to access the Internet with your other computers. Essentially, requests for data from the Internet are being sent out through the gateway, and the responses are being sent back across the network ('routed') back to your computer. The gateway computer is still the only one that's directly connected to the Internet.

If you have trouble visualising what's happening, imagine for a second that the computers are people. Let's call the computer-people Bob, Fred and Alice. They're all in a bar together, but Bob is the only one with money for drinks (we could say he has a 'connection' to the bar). Fred and Alice can ask Bob to buy them a drink, and Bob can bring over the drinks, for them to have as they usually would. At no point, however, can Fred or Alice go and order a drink at the bar.

Setting It Up: The Gateway.

Note: this guide assumes that you have already set up your wireless network, but you have not connected it to the Internet yet.

The computer with the modem connected to it is the one you need to set up first -- as the gateway, it's going to be providing Internet access to all your other computers. On this computer, go to the Control Panel, then click Network Connections. From here, you can run the Network Setup Wizard by clicking 'Set up a home or small office network'.

Click next through the wizard until you get to a screen called 'Select a connection method'. On this screen you need to select 'This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer'. From here on, you should be able to click next again until you get to the finish. Say 'yes' to turn on file and printer sharing when you're prompted.

Your computer is now ready to be a gateway to the Internet.

The Network.

The next step is setting up the other computers on your network to make use of the gateway you just created. Run the Network Setup Wizard on each of these computers, but this time through choose 'This computer connects to the Internet through another computer on my network or through a residential gateway'.

If the computer that will now be using a shared Internet connection was using a dial-up connection before, then there are a few things left to do -- you need to change some settings in the web browser Open Internet Explorer, then go to the Options screen (in the Tools menu). Click the Connections tab. You should click 'never dial a connection', and untick three boxes: 'automatically detect settings', 'use automatic configuration script' and 'use a proxy server'.

The Trouble With Internet Connection Sharing.

To go back to our bar for a moment, imagine Bob leaves. Oh dear. Looks like Fred and Alice can't get any more drinks, doesn't it? The same thing applies to the computers on your network -- if the gateway computer is switched off, they will lose all their access to the Internet.

That's not the only problem, though. While Internet Connection Sharing works fine for the web and email, it can be more problematic when it comes to doing other things.

Downloading files from filesharing networks, for example, or using videoconferencing, requires you to mess around with the gateway computer's settings. After a while, it can get quite frustrating. If you're in this position, you should really try a wireless router -- see the section 'Create Always-On Networks with a Wireless Router'.

Sharing Your Files and Folders Wirelessly.

Of course, once your computers are networked together and sharing Internet access, the next step is to make your internal network a little more useful. One of the best things you can do with your wireless network is use it to share your files and folders.

Look Out for Security.

Before I tell you how to share folders, a quick word of warning: if you don't have encryption set up on your network, then everything you share will be available for others to view. This means that anyone could bring their computer close enough to connect to your wireless connection (and in many cases, your neighbours are close enough), and they could see everything you've put in a shared folder.

How do you get around this? Well, unfortunately, there are only two things you can do: only share things that you wouldn't mind other people seeing, or turn on encryption for your network. If you want to change shared files from other computers as well as just uploading and downloading them, you definitely need encryption. For more, see 'Dealing with Security Threats: Wireless Encryption'.

Automatic Sharing.

Here's some good news: if you're happy to put your shared files in a special folder, you don't need to do any extra configuration. Windows automatically shares your 'Shared Documents' folder when you create a wireless network, to give you a space to share pictures and music across your network. To access the Shared Documents folders, just open My Network Places using the Start Menu.

Sharing More.

Of course, most people want to share more than one folder. I, for example, want to be able to access Word documents I'm working on from any computer on my network, without saving them outside My Documents. Luckily, you can access any files across the network, as long as they are in the same folder together.

To share an existing folder, simply right-click it and choose 'Sharing and Security'. Tick 'Share this folder on the network' in the box that appears. If you want to be able to change the files from other computers, you should also tick 'Allow network users to change my files' -- if you don't do that, then the files will be read-only when you use another computer to access them.

Remember that sharing files over the network can be slow, depending on how fast your wireless equipment is. Because of the way Windows works, you should try to avoid keeping lots of files in the same shared folder, as it can slow down the network more than you might expect.

You Can Even Share Drives.

You can share whole drives, if you want to. You should never do this for your whole hard drive, though, as it is very dangerous -- anyone who could get access to your network would be able to see everything on your computer, including all sorts of private information that you probably wouldn't want them to have. Worse, if you had it set to allow the network to change files, your computer could get messed up big time.

Where drive sharing becomes useful, then, is to share removable drives. You can right-click anything from a CD drive to a floppy drive, and share it over your network. The procedure is the same as turning on sharing for a folder, except that there is an extra step where you need to click to confirm to Windows that you understand the risks involved.

Once a removable drive is shared, you can do all sorts of things. You can use software that needs the CD to run as long as the CD is in one of your computers, or you can save to floppy disk from computers that don't have floppy disk drives -- the possibilities, as they say, are endless.

With a little lateral thinking, you can take this even further. Devices like digital cameras

and mp3 players almost always appear in My Computer as drives while they're plugged in -- turning on sharing for these drives basically means that you're sharing the devices across the whole network. It's really neat to be able to plug your camera into one computer and then download the photos on to all of them -- give it a go!

Create Always-On Networks with a Wireless Router.

If you're using a wireless network with Windows' built-in Internet Connection Sharing, you're probably quite happy with it -- but there's a problem. The problem is this: the computer the modem is connected to needs to be turned on before any of the other computers can get Internet access! It's alright for a while, but it gets annoying really fast.

So what should you do about it? Well, a wireless router is the answer to your problem.

What is a Wireless Router?

A wireless router is basically a small, low-powered computer dedicated to nothing but providing Internet access to your wireless network. Once you've got a wireless router, you can connect any of the computers on your network to the Internet anytime, regardless of which other computers are switched on! Because this is the only thing the wireless routers do, they don't usually need any configuration to get started.

Choosing a Wireless Router.

When you're choosing a wireless router, you should consider the same things as you would with any other wireless equipment: range, speed and standards. Remember, though, that speed is far more important with a router than it is with other equipment -- the router might be providing Internet access to more than one computer at once, meaning that it needs to have enough speed to share between them. When it comes to standards and range, on the other hand, it is pointless to get anything better than your current wireless equipment has -- you won't see any improvement.

It's probably worth noting here that the Linksys WRT54G router is fast becoming a standard. It's the most popular router out there, and it's the easiest to use out of the lot. It's not as cheap as some of the others, though, so it's still worth shopping around. As ever, the most important thing is to read as many reviews of what you're buying as you can.

Installing a Wireless Router.

Wireless routers are designed to work easily out of the box: in most cases, it should be a matter of plugging the router into the power supply and then connecting it to your cable, DSL or other modem. That's it -- in 99% of cases, you're ready to start using your wireless Internet.

Sometimes, though, there might be more things you need to do. The most common problem is that your ISP uses special software to confirm who you are before giving you access to the Internet. This is called PPPoE, which stands for Point-to-Point Protocol over Ethernet. It's basically a way giving you broadband access while still requiring you to enter a username and password first, and you need to go through a short process to use a PPPoE connection with a wireless router.

Most routers support PPPoE, but you'll have to read the manual and do some fiddling. You may also have to download an update for your router's firmware (on-board software) from its manufacturer's website.

Problems with Wireless Routers.

Wireless routers generally solve more problems than they cause -- but there are still some problems that you may need to work around.

One that a lot of people run into sooner or later is that there are some programs that require a direct Internet connection for some functions. Using a wireless router instead of Internet Connecting Sharing at least lets you use these functions if you configure it, but it can be a pain. Wireless routers have built-in firewalls that only allow data through on certain ports (for example the web port, 80, and the email port, 110), while keeping all the others closed.

Although programs that require you to open ports become rarer every day, you might

need to do it at some point. Your router's manual will tell you how to do this if it comes up.

I hope you enjoy your new wireless router -- I know I enjoy mine!

Connecting to a Wired Network: Wireless Access Points.

Let's talk about something a little more complicated. What if you have a wired network already, and you're quite happy with the way it's laid out -- you see no point in dismantling it and making it wireless when it works fine as it is. You've got this laptop, though, that you'd really like to use wirelessly. Basically, what you want to do is make a wireless connection to a wired network, often referred to as a network bridge.

Well, as luck would have it, there's a very easy way to do exactly what you want. It's called a wireless access point.

Going Partly Wireless.

If you've got a lot of computers (on an office network, for example) and you can't switch them all over to wireless networking at once, installing a wireless router is a good way of doing it bit-by-bit. Once the router is part of the network, you could just remove one network wire per day or per week, replacing it with a wireless connection.

Software and Hardware.

There are two kinds of wireless access points: software and hardware ones. Wireless access point software runs on one of the computers on the wired network, and lets wireless devices connect to the network through that computer (the computer must obviously be wireless-enabled).

You can get wireless access software easily -- doing a web search will give you plenty of choices. Look for one that's open source, as you will be able to download it straightaway for free without breaking any laws. Unfortunately, though, the wireless devices will only be connected to the network while the computer in question is turned on and connected itself.

Hardware access points, on the other hand, are standalone devices that can be plugged in anywhere on the network -- you can either buy a dedicated access point, or convert an old computer to act as one and do nothing else. They connect to the wired network just as a normal computer would, except that they offer access to the network to any wireless receivers within range.

You can leave hardware access points connected to your network and turned on all the time, if you want. An advantage of dedicated devices is that they generally have a greater range, letting you use your wireless devices further away from the access point than you could with a software access point. Dedicated devices can be expensive, though -- prices are roughly similar to wireless routers.

How Wireless Access Points Work.

An access point sends requests for data on behalf of the wireless devices connected to it. In this way, it works a lot like a wireless router: basically, a wireless access point is to a wired LAN as a wireless router is to the Internet. The difference, though, is that the devices connected through an access point actually become part of the LAN -- other computers on the LAN won't distinguish between the wired computers and the wireless ones.

This is powerful, as it gives you the capability to dynamically extend your wired LAN, without wires. In theory, there shouldn't be anything you can currently do over your wired network that you won't be able to do over the wireless extension to it.

Configuring a Wireless Access Point.

You can usually configure a wireless access point as easily as plugging it into a connection to your network, using the cable that should be included. Your network should see the access point and give it a networking (IP) address automatically. If you need to do any more configuration on your access point -- for example, turning on wireless encryption -- then you'll need to open your access point's settings.

You can do this by going to the router's IP address in your web browser. If you're not

sure how to do this, refer to your access point's manual (you might have better luck reading the online version, which will be updated with the latest problems people are having). While you're playing with your access point's settings, you might find it worth disabling DHCP (dynamic network addressing) and giving your access point a static address instead. This helps to keep your wired network more stable.

Taking it Long-Distance: Wireless Extension Points.

How far can wireless go? Well, really, the answer is as far as you want it to, or as far as you can afford. You see, even though each wireless transmitter has a range limit, you can install things called wireless extension points, often called repeaters, to boost the signal and make your network's range even bigger.

What is a Repeater?

As you get further away from the origin of a wireless signal, it gets weaker and weaker, until eventually it is impossible to receive at all. No matter much you spend on high-powered wireless equipment, you will eventually reach a point where your network just won't stretch any further.

Some people solve this problem by running wires out as far as they want the network to go, and having it 'break out' into wireless every so often using a wireless access point. This can be more trouble than it's worth, though -- what's the point of installing massive lengths of wire just to cover an area with wireless access? You could just put ports in the wall, couldn't you?

Well, to fix this dilemma, some manufacturers have started to produce wireless repeaters, even though they're not part of the wireless standard. These 'extension points' work as a relay, simply taking the existing wireless signal and making it stronger, making the range of the signal larger each time.

If you place the repeaters correctly, this can make it so that you can move computers a long way away from the wired part of the network (the router or access point) without stopping them from working. The only requirement is that the ranges of the points must overlap -- after all, a repeater can't repeat a signal that it can't receive.

How Do They Work?

To understand how repeaters work, you must remember that wireless networking signals are really just radio signals. Repeaters simply take all the radio signals they receive on the frequency used by wireless communications (2.4Ghz) and use their power to amplify and re-broadcast them. This process does not degrade the signal, and can be done as many times as necessary.

In theory, you place wireless repeaters in a line for several miles and so extend a wireless network out that far. Because extension points don't need all the computer technology required in a router or an access point, they are relatively inexpensive, and so this possibility isn't as unlikely as it sounds.

Some companies, for example, use a combination of repeaters and directional antennas (antennas that focus a wireless signal in one direction) to connect two LANs that are miles apart. They find it's cheaper to do things this way than to worry about the problems that come with doing it over the Internet or to install their own underground wires. It is technology like repeaters that could, in the future, help to build wireless networks covering whole towns and cities.

Choosing a Repeater.

For the moment, you're limited to the bigger manufacturers when choosing a repeater, and even some of them have it missing from their product range. Different companies give their repeaters different names, such as 'Range Expander' (Linksys) or 'Range Extender' (D-Link).

When you're thinking of buying a wireless extension point, there are some things you need to think about. The most important thing is whether it will work with your existing equipment -- because there's no formal standard for wireless extension points, there's no guarantee that one you get will work on your network. It's best to stick to the same manufacturer that you have the rest of your equipment from, or at least do a web search to find other people who've made the combination work.

Another consideration is whether the extension point has any Ethernet ports. It's not an

essential feature, but it can be useful if you want to connect the extension to a wired network. This is mainly only important if you're trying to connect two LANs wirelessly, although Ethernet can also be useful for connecting devices if something breaks and you need to troubleshoot the network.

Wireless Everywhere: Talking Your Laptop for a Walk.

Sometimes it really does seem like wireless is being offered everywhere. If you know where to find so-called 'hotspots' (areas where there is wireless internet access), you can take your laptop for a little walk.

Public Hotspots.

When you take your laptop and go searching for hotspots, the first place to look is big public institutions. Libraries increasingly offer wireless access and, if you're a student, the chances are that your university campus is wireless-enabled, or will be soon.

Private Hotspots.

The real growth area in wireless hotspots, though, is in the private sector. Businesses are falling over themselves to provide free Internet access to their business customers -- cafes, hotels and airports are all starting to offer wireless access to anyone who happens to be around. All you need to bring is a laptop with Centrino technology or a wireless PCMCIA card.

But how does it benefit cafes to offer wireless Internet access for free? Well, think about it: instead of paying money to sit in some dingy Internet cafe, you can use the Internet for free in an otherwise normal cafe -- while still buying food and drinks, of course. Cafes are willing to pay the minimal cost of providing wireless Internet access in exchange for the new customers it gets them, especially in areas where Internet access is hard to come by any other way. The same goes for hotels and airports: customers see wireless access as a big value-add, and will vote with their feet for places that provide it.

Finding Them.

For some reason, even though there are thousands of hotspots, they don't get a lot of marketing. Doing a search for hotspots in your town could really surprise you -- you might think there aren't any, but if you live in a decently-sized place then it'd be surprising at this point if there weren't.

There are plenty of websites you can go to and find hotspots (try a search for 'wireless hotspots'). The most comprehensive, though, is generally thought to be at JiWire.com. You can see information from JiWire at their website, or alternatively by typing your postcode into Yahoo Maps and choosing 'WiFi Hotspots' from the menu over on the right of the screen.

If you can't be bothered with that, one tip is to just look out for a Starbucks. The things are everywhere, and almost all of them offer wireless Internet access in at least part of the shop. Borders and Kinko's are also good places to try. Failing that, just keep an eye out for a cafe -- it can't hurt to ask, after all.

Your Wireless ISP.

You might find, though, that some of the larger hotspot networks with more convenient locations require you to pay a small fee to a wireless ISP to use them. You can usually do this by buying a prepaid card at the place where the access is offered, though, so it isn't too much to worry about. If you want to stay free, just stick to the small independent places.

Hotspot Software.

Of course, it's a little useless to have to look for hotspots on the Internet, or go hunting for them on foot. It takes time and energy to go walking around searching, and if you had Internet access, well, why would you be looking for a hotspot? The solution, then, is download and install hotspot locator software on your computer.

Once you have this software, you have a database of known hotspots on your computer that you can search at any time, whether you're online or offline. Just type in a postcode or the name of the town where you are and the software will come back with the nearest hotspots, sorted by distance from you. Each time you do manage to get an

Internet connection, the software connects to its server and downloads the latest hotspot list, to make sure that your database doesn't get out of date.

Where can you get hotspot locator software? Well, it's offered for free from the hotspot providers' sites, for a start. T-Mobile Hotspot is currently the largest provider, and offers software for free download at <http://www.tmobile.com/hotspot>.

Wardriving and the Wireless Pirates.

Thanks to the manufacturers' default settings leaving wireless encryption switched off, thousands upon thousands of wireless connections everywhere are completely insecure. New breeds of wireless users have started to take advantage of this 'free' bandwidth appearing everywhere: the wardrivers and the wireless pirates.

Wardriving.

So what's wardriving? Well, to put it simply, it's when someone drives around with their laptop looking for unsecured wireless networks to connect to. This allows people to circumvent the physical security of large companies and connect to their networks: the network is said to be leaking out of the building. Wardriving used to be very difficult, but now there is easy to use software such as NetStumbler that searches for open networks automatically.

Wardriving works well because wireless networks, by default, are set up to provide access to any wireless-enabled computer that comes within range. This is very convenient and easy to use, but also extremely insecure.

The legal status of wardriving is dubious to say the least, but most of the people doing it don't have any malicious intent. There are some, of course, who will abuse the massive amount of bandwidth (download capacity) they can get access and download enormous files at amazing speed. There is also a small minority who may try to use access to a company's network -- or even an individual's -- for nefarious ends.

Wireless Piracy.

It is a point of contention among wireless users whether it is possible to 'pirate' wireless Internet access. Sure, if you go and sit outside someone's house in a car, you're probably doing something you shouldn't be. But what if you just use one of your neighbours' wireless networks instead of paying for your own ISP and Internet connection? Is that wrong?

The trouble is that it is impossible to tell whether an open network has been left that way intentionally or not. Many people have thought it through, and prefer to leave their network open for anyone to use, seeing no harm -- I am one of these people. Others just have no idea how to turn on security. The problem would be solved overnight if wireless equipment would come with encryption turned on by default (meaning that you would have to change the settings if you didn't want it). Unfortunately, the incompatibility of the two current encryption standards makes this unlikely to happen anytime soon.

In the end, until things change, the answer has to come down to your own individual ethics: you're probably not doing much harm if you use your neighbours' connections, as long as you don't download so much that you cause their connections to go slower.

The line is more blurred, of course, in areas where ISPs charge for access by the gigabyte. If you're not sure one way or the other, it's probably best to stick to your own network.

Should You Be Worried?

Some people are unnecessarily worried when someone tells them that their network is insecure: they think hackers are going to come and steal all their credit card numbers or something. You might even run into people trying to sell you 'wireless intrusion detection' software. Remember, though, that the Internet is designed to operate over wires that anyone could tap into: all sensitive data is encrypted anyway.

While you don't need to be scared about someone sniffing your web data, though, you should be a little more concerned about any files or folders you have shared. If you don't want to encrypt your network, you shouldn't share anything that you wouldn't want others to see, and you certainly shouldn't give the network write (change) access to anything you don't have a backup copy of.

Of course, if you really want to keep other people off your network, it's not like it's hard

to do yourself with a little configuration. Take a look at the next section, 'Dealing with Security Threats: Wireless Encryption', for a brief guide.

Dealing with Security Threats: Wireless Encryption.

If you don't want your network to fall victim to snooping or people 'borrowing' your bandwidth, then you're going to need to lock down your network. Luckily for you, all wireless technology has encryption built in -- it's just a matter of turning it on.

WEP Vs. WPA.

Security on wireless networks does have a flaw, though -- there are two completely incompatible standards, which makes it a pain to set up a whole network to use encryption.

How did this happen? Well, WEP (Wired Equivalent Privacy) was the original standard for encryption over 802.11 wireless networks. Back in 2001, though, a research paper was published called 'Weaknesses in the Key Scheduling Algorithm of RC4'. This paper demonstrated critical flaws in the security of WEP that made it trivial for someone to break into, if they wanted to.

Essentially, it is too easy to discover the secret 'key' used for WEP, and once you have the key, you can get into the network and stay in for as long as you want. People quickly recognised that it was almost useless to use WEP on their network -- but by the time its weaknesses were discovered, the WEP method was built into almost every piece of wireless equipment out there.

The WEP standard had to be replaced, and in 2003 WPA (Wi-Fi Protected Access) was introduced as its replacement, fixing most of its flaws. WPA is much more secure than WEP. Unfortunately, though, WPA took a long time to reach the market, and WPA devices were expensive when they were released. Combine this with the fact that WEP is still the default in a lot of software (because it's supported by more devices), and you end up in the confused situation we're in today.

Always Use WPA.

If you're going to enable encryption, always use WPA. Devices bought after 2003 or so should be compatible with it, as the upgrade was made a mandatory part of the standard.

It is true that WEP is better than nothing -- it will, at least, deter the casual intruder, who won't try any more than double-clicking to get onto your network. WEP can also make you less of a target for wardrivers, since there will be so many completely open networks that they might as well use instead. However, it's silly to use WE nowadays when WPA is so easily available.

Turning on Encryption.

Turning on encryption in Windows isn't too difficult, but it does involve quite a lot of clicking -- no wonder so few people bother.

The first step is to turn on encryption for your wireless router or access point. The exact method for this will vary between devices, but you can usually do it by visiting the router or access point's configuration page in your web browser, finding the encryption settings, and then choosing WPA. If you have any trouble, refer to your manual.

Once you've done that, you need to change the encryption settings on your computers. Open the 'View Available Wireless Networks' screen by right-clicking on your wireless connection in the bottom-right of the screen and choosing it from the menu that appears. Then click 'Change advanced settings'. Go to the Wireless Networks section of this box, click your network's name, and then click Properties.

Now, where it says 'Network authentication', select WPA. Click OK on everything you've opened. Once you've done that -- this is the really fun part -- you're going to have to do it for every computer on your network!

It's Easier for New Networks.

While the process is quite troublesome for existing networks, it's much easier for ones that haven't been set up yet. You'll still need to turn on encryption at the wireless router or access point, but once you've done that you can set up encryption as you set up the network using the Wireless Network Setup Wizard.

Unfortunately (and stupidly) Windows now turns on WEP by default when you set up your wireless network. This means that each time you go through the wizard, you need to remember to tick the box on the third screen that says 'Use WPA encryption instead of WEP'. Still, it's easier than changing the settings manually later on.

Wireless Troubleshooting: 5 Things to Try.

Wireless networks can be funny things. They'll work for weeks or months and then suddenly, one day -- bang! They're dead. But what can you do to try and resuscitate a dead wireless network?

The Simple Things.

Before you go to too much trouble to fix your network, you should try the simple solutions. No-one's quite sure why they work, to be honest, but they have a surprisingly high success rate.

To get Windows to attempt to fix problems with a wireless connection, double click the connection's icon in the bottom right corner of your screen. Go to the Support section of the box that appears, and then click Repair. Windows will deactivate and reactivate the connection in an effort to get it to work.

Once you've tried this, the last-ditch simple solution is that Windows classic: restart the computer. If that doesn't work either then, well, you'll have to try something else.

Has Your Wireless Card Come Loose?

If you have a USB or PCMCIA wireless card, you should check now to see whether it's come loose. The best way to do this is to disconnect everything and reconnect it. USB devices are especially vulnerable to gradually coming loose -- make sure you unplug your USB wire at both ends of the connection, if possible.

Of course, if you have an internal PCI wireless card, you might want to try a few other things first before you go to the trouble of opening the computer to take a look at it.

Have the Networks in Your Neighbourhood Changed?

Sometimes, if someone sets up a new network near you, it can cause some interference and take precedence over your own network, especially if you're in a part of your house where your network's signal is weak. Once your computer is connected, though, there's no guarantee your computer will be granted -- the other network could be set up in any number of strange ways. This leaves you in a position where your computer has connected to a network that it thought was 'better' without telling you, even though it turns out that network is useless to you.

You need to go to the 'View Available Wireless Networks' screen and take a look at what you're connected to. If it's something you don't recognise, you should double-click your own network in the list to connect to it. If this works, make sure you remove other networks' names from your 'preferred networks' list, to avoid connecting to them in the future.

Check for New Sources of Interference.

If you find that your connection will work if you put your computer right next to the source of the Internet signal, but stops working as you get further away, then the cause could be interference. You should consider any changes you've made to your home recently. For example, did you just get a new cordless phone? They can often interfere with wireless networks. Treat any equipment that uses radio waves as suspect -- try switching each thing off in turn and see if the performance of the wireless network improves.

Reset Equipment to Factory Settings.

With routers and access points, one thing that might work is to log in to their admin control panels (using a web browser) and click the option to restore to factory settings. This removes all your settings and makes the router or access point 'like new' again, meaning that any problems it was causing should be solved, unless it has been physically damaged.

If none of these things work, but the network was working fine before, the chances are

that you've got a hardware failure somewhere on your network. This could be as simple as someone having sat on a USB device, or knocked an antenna on a router. You need to try unplugging things in turn to figure out where the failure is, and then call the manufacturer to report the fault -- be prepared that you might need to replace the item yourself, though, if it's not their fault or the equipment is outside warranty. Even if it turns out not to have been a hardware failure, they should be able to help you fix your network.

Bluetooth: Personal Wireless.

If you've got a wireless network for your computers already, well, you might get a bit excited about what I'm going to say next. How would you feel if your PDA, your mobile phone, your mp3 player and almost everything else you connect to your computer could be wireless too? You'd like that? Well, it's already a reality. Read on...

Personal Area Network.

Using wireless networking with your personal gadgets is often called PAN, which stands for Personal Area Network. The idea is that, in the future, we'll all have laptop computers with their batteries charged and no more need to connect any wires to them at all -- you just place your Bluetooth device near the computer, and the computer sees it and can use it straightaway.

Bluetooth has been around and in-use since 1999, and it's only getting more popular. It was designed to be secure, low cost, and easy to use from day one.

There are two classes of Bluetooth that are in popular use: class 1 and class 2. Class 2 is the most common and cheaper standard, allowing you to use a device that is up to 10 metres (32 feet) away. Class 1 is rarer, but you can still find devices that use it easily enough, and it has ten times the range: 100 metres or 320 feet.

How Does It Work?

Bluetooth is more flexible than 802.11 wireless networking, in exchange for the shorter range. Essentially, a Bluetooth-enabled computer has one Bluetooth receiver installed in it, and this receiver can then be used with up to 7 nearby Bluetooth devices. On the other end, wireless devices do not need to have Bluetooth installed if they support it -- it is already integrated.

Like 802.11, Bluetooth works by using radio signals to create bandwidth. It is not, though, the same thing as an old-style wireless mouse or keyboard, which required a receiver to be plugged into one of your computers' ports, and didn't have range or stability anywhere near that of Bluetooth.

Many computers now come with built in Bluetooth, especially Apple Macs. If you want to add Bluetooth to a computer that doesn't come with it pre-installed, you should probably use a USB to Bluetooth adapter, although internal Bluetooth devices to install in your computer are available. If you have a laptop and a spare PCMCIA slot, you can get Bluetooth cards for that too.

What Can You Do With Bluetooth?

Mobile phones with Bluetooth are very popular, and so are PDAs -- the instant synchronisation of addresses and calendars to a computer is a useful feature. Other than that, almost anything that would usually use USB can be done using Bluetooth, including digital cameras, mp3 players, printers, and even mice and keyboards. If you take a look through the comprehensive list of Bluetooth 'profiles' (kinds of devices that could, in theory, be Bluetooth enabled), it includes cordless phones, faxes, headsets, and even video.

Basically, more than anything, Bluetooth is a replacement for USB: some say that while 802.11 wireless networking is wireless Ethernet, Bluetooth is wireless USB.

Not Just for Computers.

Part of the power of Bluetooth is that it isn't just used to connect things to computers -- it can be used to connect almost anything to anything else, if both things are Bluetooth-enabled and recognise each other.

Mobile phones, in particular, take advantage of this. Hands-free headsets often use Bluetooth to communicate with the phone. Some cars, for example, now have on-board computers that will connect with a Bluetooth phone and allow you to make hands-free calls, regardless of where the phone is in the car (even if you've left it in your bag in the

trunk!)

On top of that, of course, Bluetooth devices can communicate with each other. This has led to some people sending messages from their Bluetooth PDAs to others in close range -- not an especially useful feature, but quite fun. This is called 'bluejacking', and the first recorded instance of it was a man who sent a Bluetooth message to another man's Nokia phone while they were in a bank together. What did the message say? 'Buy Ericsson'.

Since then, it has become possible to send images by bluejacking, and it is widely believed to be the newest advertising medium -- yes, it lets billboards send messages to your phone, a practice known as 'bluecasting'. Whether you think that's cool or annoying, of course, is your choice.

RFID: Wireless Shopping.

So wireless networking has got rid of your network wires and your USB wires... what can it do next? Well, the answer might surprise you: wireless is going shopping.

RFID: Electronic Barcodes.

Yes, that's right: RFID (Radio Frequency Identification) is a replacement for the barcode, using wireless radio technology. But what's wrong with barcodes, you ask? Well, they need to be scanned, for a start. Supermarkets and other shops have small armies of staff in their stores, in fact, doing almost nothing but scanning barcodes and taking money.

RFID lets barcodes be replaced with radio signals, which can automatically be scanned. In theory, you could have a shopping cart full of RFID-labelled products, put it near an RFID scanner, and the things in your cart would be detected and their prices added up instantly.

Imagine being able to stop in front of a machine at the supermarket's exit, and do nothing but put your credit card in a machine before you leave (if your credit card is RFID-enabled too, you might not even need to do that). You can checkout in a matter of seconds! It's a win-win situation: it saves you time, and it saves the supermarket money. The only people who lose out are the ones getting paid to sit around scanning barcodes, but hey, that's technology for you.

How on Earth Does It Work?

Believe it or not, RFID tags contain tiny antennas, allowing them to transmit small amounts of data by radio. The majority of tags in use today do not have their own power supply (a power supply makes the tag larger and more expensive), which means that they must rely on power they receive through the air by radio. This is such a tiny amount of power that it is only just enough to transmit an ID number. This does work, however, from as much as five metres away.

For shopping use, tags that send numbers are sufficient -- a barcode is just a number in the form of lines, after all. These tags are now as cheap as 40 cents, and mass production means the price is only going to come down -- RFID is likely to become widespread in the next decade. The smallest RFID tags are already thin enough to be almost invisible.

Privacy and Other Uses of RFID.

There are privacy concerns around the use of RFID, simply because it makes it so quick and easy to tag just about anything -- and the tags can be scanned without any human interaction. This, however, is also what makes the system very useful.

Pets are already implanted with RFID tags so that they can be identified if found, and the idea of humans being made to have RFID implants as a replacement for identity cards isn't as science fiction as it sounds -- it is possible today. As long ago as 1998, a professor was able to implant a tag in his arm. The technology is being considered for used on prisoners. In countries that already have ID cards or that will have them soon, RFID tracking probably won't be far behind.

If RFID shopping tags are left on things, then people could leave tags on their clothes or other products without realising it. This has all sorts of implications -- someone might be able to point an RFID scanner at your house and get a list of everything in it that still has a tag, for example.

RFID is already widely used in many industries. Warehouses use them to track pallets of goods, some libraries put them in books and airlines use them to track baggage. Usage is particularly common in building access control (the ID cards for employees that open the door automatically).

Travel is another growth area: many parts of the USA have the option of using RFID cards to pay at toll booth's, and the London Underground now uses RFID payment cards known as Oyster cards. There are even RFID car keys that can open the door while

they're still in your pocket, without you doing a thing.

Environmental Concerns.

As a footnote to all this, many people are concerned about the environmental impact RFID could have. Although they are small, using computer chips as a replacement for barcodes could lead to the equivalent of many thousands of computers being thrown away every year.

What Else Can You Do Over a Wireless Network?

Well, you'd be surprised. There really are all sorts of things you can do with wireless networks -- you're only really limited by your imagination! Here are a few weird and wonderful ideas to get you started, but don't be afraid to try out anything else you think of.

Store Files in Your Car.

If you put a small wireless-enabled hard drive in your car, you can use it as a mobile file server, avoiding the need to send files around on the Internet or burn them to a CD. This can be especially good if you often move large files around. You could, for example, upload your files to the car-server when you're at home, and then download them again when you get to work.

There are other uses of this too -- you could, for example, send music files from your computer to the car to play on your journey, without having to physically move anything at all.

Build a Real 'Network Neighbourhood'.

You can extend wireless networks as far as you want, using repeaters and directional antennas. If some of your neighbours put repeaters in their houses, then any networks in the area could be extended to cover a gradually larger range.

Ultimately, if you have co-operative neighbours, you could turn your whole street into a wireless hotspot: you could even all share one super-fast Internet connection, paying less per person than you usually would for a much slower one. There is even a name for this: a 'freenet' or 'community net'. People who have tried it find that it makes people feel much closer to each other, bringing back long-lost social ties within the local community.

Bear in mind, though, that you're basically running your own ISP if you decide to do this, with all the support issues that could involve. You might want to ask your ISP's permission first, in case they get upset about you sharing your connection so freely. Whole books have been written about this topic -- for more information, you might want to read one of them, such as Rob Flickenger's 'Building Wireless Community Networks'. If you live in a big city, you might even find that someone's already trying to do it in your areas.

Make Cheap Phone Calls.

If you get a Bluetooth-enabled headset, you can use your wirelessly networked computer to make cheaper (or free) phone calls. Voice over IP (VoIP) software such as Skype makes it easy to call anyone in the world, and using a headset makes it even more convenient than using a phone -- you can do whatever you want while you talk.

Most VoIP software is limited to calling other VoIP phones, which is free. Services like Skype, however, allow you to call real phone numbers too. Since the call is made in whatever country the number is in and then routed over the Internet to you, you can call worldwide for not much more than the cost of a local call. There are few things more fun than chatting to your friend half the world away for an hour and knowing it only cost you 50 cents -- and that all they had to do was pick up the phone.

Watch Media on Your TV.

There is a new wave of wireless media devices that connect to your TV like a cable box or a DVD player, but allows your TV to play media files you have shared on your wireless network. If you use an operating system like Windows Media Center Edition or similar, it's easy to watch videos from your computer on your TV -- you even get a remote control. On top of that, you can record shows from your TV, TiVo-style, and then share these recordings over your wireless network.

You want things you digitally record on one TV to be viewable on all your TVs? Now they can be. Simply get two wireless-enabled digital recorders and they'll form a network all

on their own -- simple as anything.

The Future of Wireless.

Wireless is a technology that's cheap, easy and useful right now, and yet it's a technology that's still very young. Here's a quick look at what the future could hold for wireless.

The Radio and the Phone.

Wireless networks will always win over wired ones, in the end, simply because it is cheaper for signals to travel through the free air than it is to install and maintain wires. If you want an example of this, consider that telephones were originally used for sending and receiving news reports. When radio was invented, this stopped almost overnight -- why bother going to all that expense when it's free over the air?

It's the same way with computer networking. Imagine you have a choice between a wired Internet connection and a wireless one. Why would you choose the wired one? Because it's cheaper? That will change soon. Because you know how to use it? Wireless is easier. There's no reason why anyone wouldn't switch in an instant, if they had the opportunity.

WiMAX.

You remember that wireless networking today uses a standard called 802.11? Well, WiMAX is 802.16 -- the next generation of wireless. It's still a work in progress, but the possibilities are exciting.

WiMAX stands for Worldwide Interoperability for Microwave Access, and is designed to complement existing wireless equipment rather than replace it. The biggest advantage of WiMAX is in its vastly increased range: instead of being measured in square metres, WiMAX ranges will be measured in square kilometres. Some say the strongest WiMAX stations could transmit for up to 50 kilometres -- over 30 miles!

This obviously opens up a whole new world of possibilities. Wireless access would move from LANs to MANs: Metropolitan Area Networks, covering a whole town or city with wireless access. The question would no longer be whether there was a hotspot in the area where you were, but which of the many WiMAX networks you wanted to connect to.

Other benefits of WiMAX include speed of up to 70Mbps (almost 10 MB per second), and stronger security. Imagine a future where ordering Internet access is as simple as connecting your existing wireless equipment to the network, opening your web browser, and buying a low cost subscription. That's it -- done. No more access points, no more routers, no more configuration... just wireless Internet, everywhere. WiMAX is going to take the world by storm.

For the latest news on WiMAX, take a look at the WiMAX Weblog at <http://wimax.weblogsinc.com>, or visit the WiMAX Forum (a non-profit industry group set up to promote WiMAX) at <http://www.wimaxforum.org>. WiMAX has been in development since 2001 now, and the first WiMAX equipment is currently expected to hit the market as soon as the end of 2005.

Bluetooth in Everything.

While Bluetooth's most obvious purpose is to replace USB, it is designed so that it can eventually replace almost every wire there is (except power cables). That means that someday your TV could be connecting to your DVD player by Bluetooth, or your speakers could connect to your radio with it, and so on and on.

As you get older, expect to see fewer and fewer wires. I know people said the same thing about paper, but it turns out people like paper and don't want a 'paperless society'. How many people do you know who have a thing for wires? Exactly. Once someone figures out a way to provide reliable wireless power (better batteries?) we'll be set!

A Simpler Life.

When you read about the potential of wireless technology for a while, one thing sticks

out in your mind: it all sounds so convenient. Wires have so many flaws, especially when they go long distances, and the overall wireless project is to remove them from our lives -- and then charge us less! That has to be worth supporting, doesn't it? I'll make a prediction now: I think that, within a decade, wireless access will be making everyone's life much easier, and they won't even notice it's there. That's the future of wireless. See you there.

Put Your Own Adverts Here



Join the Software Gold Club and you can put your own adverts on brand new Master Resale Rights ebooks and software tools just like this one every single month, then sell them or give them away.

As your ebooks and tools spread across the Internet, they will carry your adverts to an **ever increasing audience**.

You can advertise anything you want - your own products, affiliate programs or anything else.

You'll also get access to our superb collection of Premium Software which you can **private label**, sell and keep all the money.

Plus loads of niche products, special tools, training and much more.

[Click here now for more details](#)