Wifi without worries

Alan Stevens offers solutions to the 20 most common problems encountered with wireless networks

Wireless networks are great – until they go wrong, that is. For example, you want to connect a new wireless client to your network but can't remember, or don't know, the type of encryption or keys required. And then, when you check the settings on the wireless router or access point, you're asked for a username and password and can't remember those either. Of course, you should have changed the default administrator account and password, and made a note of the new settings, but a lot of us don't – in which case you might want to try some of the common defaults.

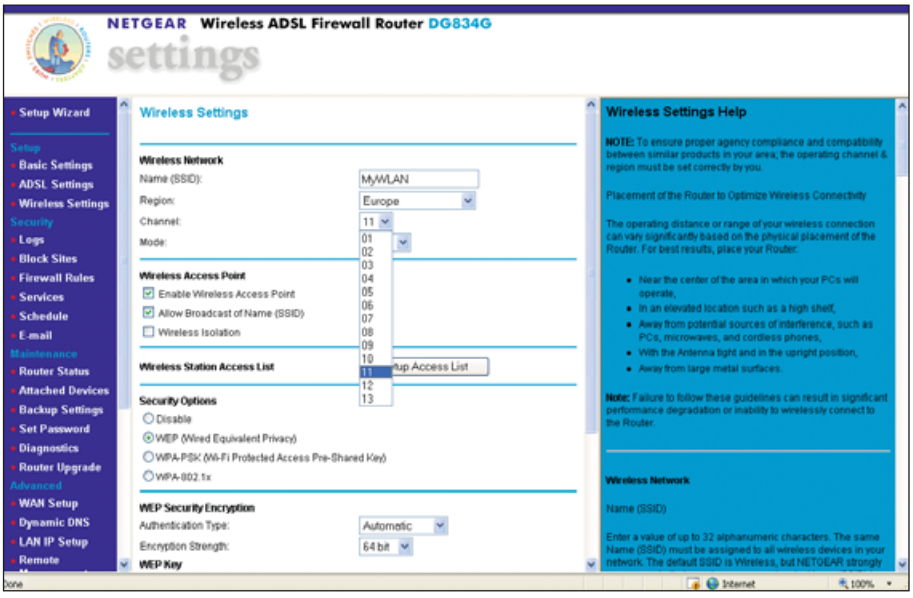
1 Blankety blank

A username of 'admin' and password of 'admin' will often get you into a router's setup page, as can 'admin' and either a blank password or the word 'password' itself. You might also try a password of '1234', or on some devices a blank username and password of 'admin'.

If all else fails, you can reset most wireless routers back to their factory defaults, typically by pressing a small reset button at the back or underneath. However, you will then have to reconfigure all its settings from scratch.

2 Up-to-date software

Wireless networking is relatively new and the technology is still evolving. As a result, you can solve a lot of connectivity and other problems simply by downloading and installing the latest firmware or drivers for your wireless devices. Some of the latest security enhancements are only available if you're running up-to-date software.



The version of Windows involved can also have a big effect. Microsoft didn't really start getting its wireless act together until Windows XP was launched, which means that if you're running anything earlier you're dependent on the software provided by hardware vendors.

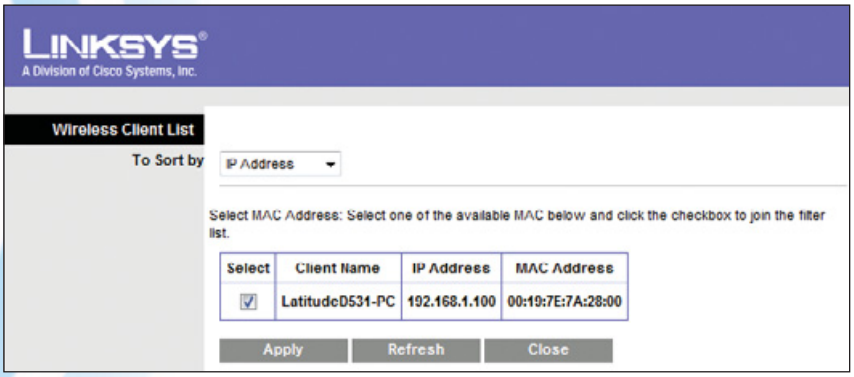
Windows Vista has the most up-to-date wireless support, but if using Windows XP it's worth making sure Service Pack 2 (SP2) is installed as the wireless options were greatly enhanced in this update and it addresses a lot of connectivity and security issues.

3 A matter of range

There are lots of things you can try in order to improve the coverage of your network. First, locate your wireless router or access point as centrally and as high up as possible. You can also upgrade to high-gain antennas, although it's not always possible, especially on cheaper devices that don't have antenna sockets, and it's important to check compatibility before buying.

On a business network, install additional access points to improve coverage, while on

If you think interference might be causing you problems, try setting your wireless router/access point to use a different channel



You can limit access to your wireless network by MAC address, but you should still employ other security measures

a home Lan consider a Powerline range extender such as the WGXB102 from Netgear. This comprises two small wireless devices that plug into standard mains power sockets – one connects to the wireless router, the other acts as an access point and needs to be close to the client PCs. The mains wiring then acts as a backbone network joining them together.

Lastly, you might want to look at the latest 'Draft-N' products. Designed to conform to the forthcoming 802.11n specification, these offer greater throughput and range. However, you will need to upgrade all your wireless devices to get the full benefit.

4 Interference issues

If you're having trouble connecting to a wireless Lan or the connection becomes intermittent, interference could be a contributing factor. Wifi shares the 2.4GHz waveband with a lot of other technologies, including wireless TV senders, baby monitors, wireless alarm systems and Bluetooth devices. Microwave ovens can also cause problems. If you have any of these, try turning them off to see if the situation improves.

You may also want to experiment with the wireless channel used by your router/access point, especially if there are any other wireless networks nearby. Although there are 13 channels available for the most popular 802.11g technology in Europe, most routers and access points come configured to use channel 6. Try changing to a different channel number to see if that helps. Channels 1, 6 and 11 are completely separate and should be tried first; all the others overlap a little.

5 Controlling access by MAC address

Some wireless products include survey tools that can tell you which channels are being used by other devices.

For maximum protection, you will need a wireless router/access point and clients that support WPA2-Personal security with AES encryption

Routers and access points that support the Wireless Distribution System can be configured as wireless bridges/repeaters, but it's complicated and not a common option

You won't normally have to change the client setup, as most will simply use whichever channel they find your network on.

Most wireless routers/access points can be configured only to permit connections from clients with a known MAC address – a unique code hardwired into every Ethernet networking device. It's an easy-to-apply configuration option, and the only real issue is working out what your MAC address is. Fortunately, on a lot of routers and access points you can see the MAC addresses of clients trying to connect and simply authorise them directly. Otherwise, open a command window on the client itself and type in the command

```
ipconfig /all
```

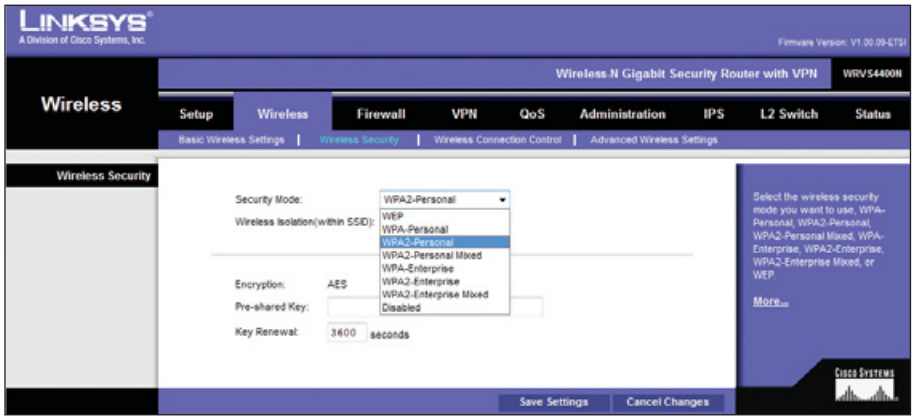
then look for the numbers listed as Physical Address, which will look something like 00-19-7E-7A-28-00.

On a home or small-business network, MAC address filtering is worth activating. On a larger network, however, management can be an issue, especially if you want to allow guests access to your WLan. Bear in mind that MAC addresses can be spoofed and you still need to encrypt your data to protect it from wireless 'sniffers'.

6 Wireless bridging

Wifi can be used to wirelessly connect networks (wireless bridging), but it's not always as easy as it sounds. That's because most wireless routers and access points are only designed to connect client devices, not act as bridges to other access points. In most cases, installing an extra access point in a remote part of your house and expecting it to propagate the signal from your wireless broadband router won't work.

If wireless bridging is what you want, then look for custom wireless bridge solutions, some of which can be used to link networks over several kilometres. They can be expensive, however, and for home use you might want to consider routers/access points that support the Wireless Distribution System (WDS). These can be configured to act as either dedicated bridges or repeaters, where they can also connect to wireless



If you're only going to use 802.11g, it's worth disabling support for earlier technologies on the wireless router or access point, to stop neighbouring networks slowing you down

clients. However, WDS implementations are complex and can differ, so mixing products from different vendors may not always be possible, and since the same channel is used for each wireless 'hop', bandwidth can be significantly reduced.

7 Improving performance

Still something of a dark art, there are several simple things you can try to boost wireless throughput. For example, where you only have 802.11g clients, try turning off support for older, slower, 802.11b devices on your access point. Wireless networks tend to step down and operate at the speed of the slowest connected device, so this will help stop neighbouring networks slowing down your Lan. Likewise, if you've gone for an all 802.11n setup, turning off support for earlier technologies may help optimise performance.

The new 802.11n products use Mimo (multiple input, multiple output) aerial technology to enhance both throughput and range. This is also available on a lot of 802.11g products and upgrading to Mimo is a good idea, but you will need Mimo both on the wireless access point and on all its clients to get the benefit – and with 802.11g Mimo products there's no guarantee of interoperability between vendors. Some Mimo speed improvements come from combining signals reflected off nearby walls and other surfaces, therefore locating a client too close to an access point can sometimes be counterproductive.

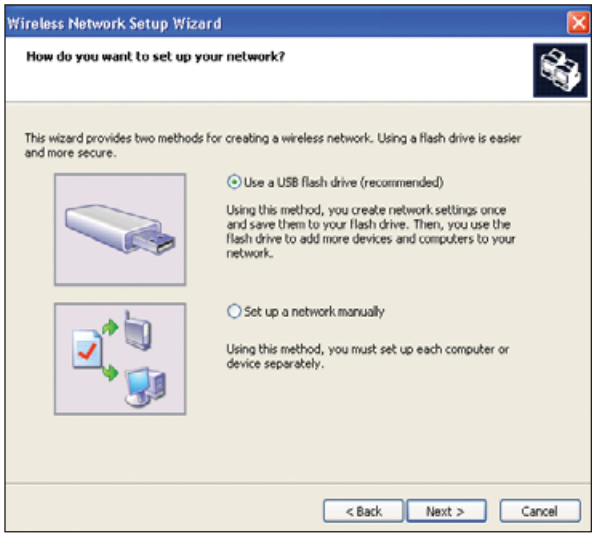
8 Which security technology?

With several different authentication and encryption technologies to choose from , it can be difficult deciding how best to protect your wireless Lan. In order of preference, here's what to consider. The most secure option is Wifi Protected Access 2 (WPA2) with AES (Advanced Encryption Standard) encryption. On a small network, you should use WPA2-Personal, sometimes called WPA2-PSK (Pre-shared Key), where you type in the same security key on the wireless router/access point and client PCs. WPA2-Enterprise requires additional authentication server components and isn't suitable for small networks.

If WPA2 isn't available on all your devices, check to see if it can be added by upgrading the firmware or driver software. If it can't, consider the slightly less secure WPA-Personal technology which, because it has been around longer, is more widely supported. If AES encryption is available, use that here as well, otherwise use TKIP (Temporal Key Integrity Protocol). Some routers/access points can support both WPA and WPA2 clients at the same time.

Some older 802.11b devices will only offer Wep encryption. This is fairly easy to crack, but is better than no protection at all. Choose the highest level available – opt for 128-bit rather than basic 40-bit or 64-bit Wep encryption.

You can't usually mix different security technologies together, so you may have to upgrade or replace older devices to achieve the level of protection you require. Wireless security is a must – if you don't use one of the many available technologies anyone can connect to your wireless Lan. However, a lot of users have trouble with the keys required to encrypt wireless data. Here's how to troubleshoot such issues.



9 Trouble with keys

First, always start with an unencrypted (no security) setup to establish that a new client can connect successfully and that something else isn't causing the problem. Once encryption is turned on, you'll need to provide the same security key on both the router/access point and its clients. These can usually be typed in using either ordinary keyboard characters (it's best to stick with a-z and 0-9) or hexadecimal notation (that's 0-9 plus a-f).

The number of characters required will depend on the type of encryption. With ordinary keyboard characters you'll need to supply exactly five characters for a 48-bit Wep key and 13 for 128-bit Wep (10 or 26 if using hexadecimal). For WPA/WPA2, you can type between eight and 63 characters, and the longer the key the harder it will be to crack. Including upper-case characters will also make the key more secure.

Keys are easily forgotten so a lot of vendors let you type in a more memorable passphrase and use this to generate security keys. The wireless network setup wizards in Windows XP and Vista can generate security keys automatically and save them on a USB memory key ready for transfer to other client PCs, saving having to re-key the data or remember how many characters to type. The USB key can also be used to set up some wireless routers access points, although few have the necessary USB port to support this.

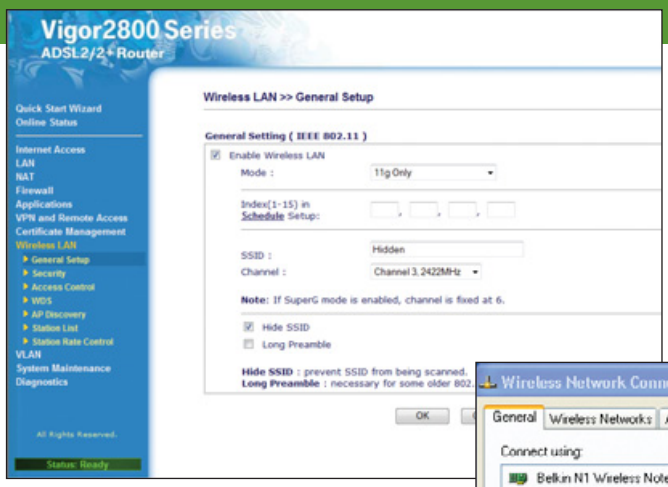
10 Hidden networks

Wireless routers and access points advertise their availability by broadcasting the network name (SSID). By turning off these broadcasts (an almost universal option) you can, in theory at least, hide the network and make it more secure. In practice, however, it's quite easy to discover hidden networks, making it a fairly worthless exercise. Also it makes it harder to connect to a hidden network, especially if running Windows XP, which will try to connect to a network broadcasting its SSID in preference to those that don't.

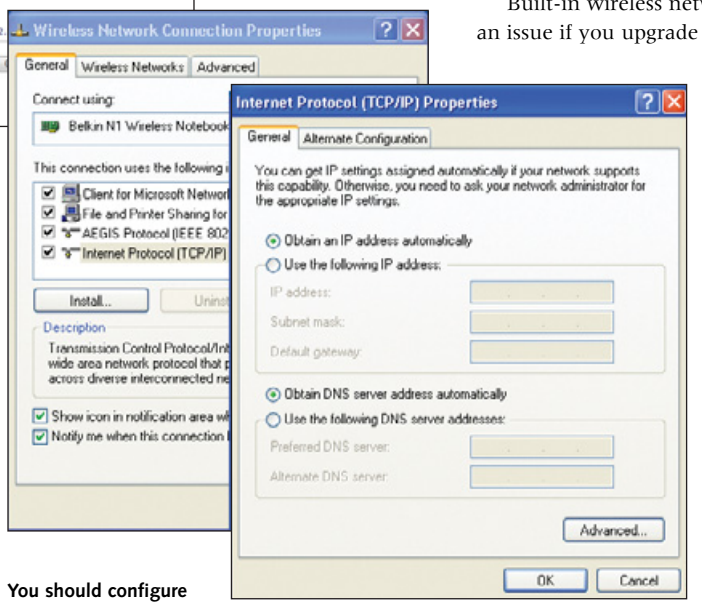
11 Sharing files and printers

Although mainly bought to share broadband internet services, wireless networks can also be used to share files and printers. Once

The Windows wireless network setup wizard can generate keys for you and save them to a USB memory key for easy transfer to other client PCs



Disabling broadcasts of the network name (SSID) may seem like a good security measure, but it's easily bypassed and can cause connectivity problems



You should configure wireless clients to get an IP address automatically from the DHCP server

the client PCs have been connected, the setup required is the same as it would be for a wired network.

You should first make sure that all the PCs are configured with the same workgroup name. Next decide on the folder you want to share, then in XP right-click on its icon and select Sharing and Security. Click the radio button marked Share this folder, then click the Permissions button to specify who is allowed access. Similarly, it's possible to share printers by right-clicking its icon and choosing the Sharing option.

File and printer-sharing problems can arise when mixing different versions of Windows together, but troubleshooting such issues is the same, irrespective of whether connected by cables or a Wifi network.

12 Network addresses

Every PC on a network will need its own unique IP address so, by default, most wireless routers/access points will be configured to act as a Dynamic Host Configuration Protocol (DHCP) server. This will assign addresses automatically to each PC as it connects to the wireless Lan. However, there are one or two things to bear in mind. First, if you already have a DHCP server on your network, you'll need to disable the one in the wireless router/access point as you can't have two on one Lan.

Second, client PCs need to be configured to get their network addresses automatically. In XP, right-click the wireless connection and choose Properties, then double-click Internet Protocol (TCP/IP) and select the entry marked Obtain an IP address automatically. You can usually do the same for the DNS server address.

Lastly, if you configure servers or printers with fixed addresses, make sure they fall outside the scope automatically assigned by the DHCP server, otherwise conflicts will arise. On a lot of wireless routers/access points, you can set the range of addresses the DHCP server can use.

13 Checking your network address

If you have problems connecting to a wireless network, one of the first troubleshooting steps is to make sure you have a usable IP address. In XP right-click the wireless connection icon and choose Status, then the Support tab to see what IP address you have. Alternatively, open a command window and type

```
ipconfig
```

to display the current address.

Addresses formatted as 169.xxx.xxx.xxx are automatically generated and indicate that there was a problem obtaining an IP address from the DHCP server. Alternatively, you may have no address at all. Either way, the most common cause is a mismatch in terms of wireless encryption technology or security keys between the client and the host network. In other words, the client can connect to the network but can't unscramble data correctly to receive a proper IP address. Try turning the security off to see if you can get an address then, if you can, try to find out where the mismatch has occurred.

14 Built-in problems

A lot of notebook PCs now come with a wireless interface built-in (the Centrino brand indicates integrated wireless on Intel-powered products). This is great because you can connect to a wireless Lan straight away with nothing extra to buy, but it can also cause some problems.

Somewhat embarrassingly, one of the most common issues is being unable to connect to a wireless Lan because the built-in interface hasn't been turned on. Look for a small switch located at the front or on the side of the notebook or, in some cases, just above the keyboard. Turning the wireless interface off saves battery life, but will also stop you connecting to a wireless network.

Built-in wireless networking can also be an issue if you upgrade to a newer technology not supported by the integrated adapter. For example, first-generation Centrino notebooks will only support 802.11b networking and Wep encryption. Sometimes a firmware or driver upgrade can resolve this kind of problem, otherwise it's a matter of fitting another plug-in, adapter or, if all else fails, upgrading to a newer notebook.

15 Windows wireless management

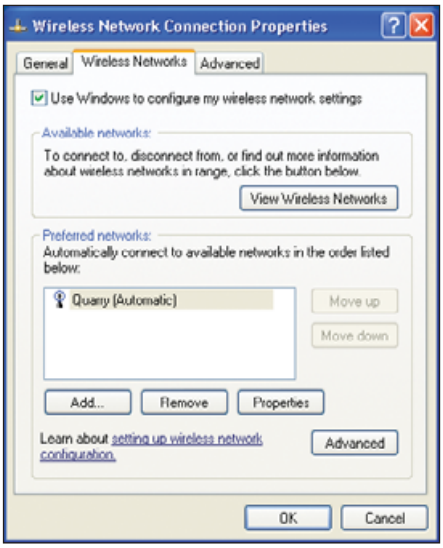
Vendors of wireless network adapters normally provide their own software to enable you to find and connect to a network. However, you can also opt to let Windows manage the wireless connection. There are pros and cons to both approaches.

Use Windows and you get a consistent interface no matter what hardware you're using, but proprietary utilities may offer greater functionality, such as identifying hidden networks and making it easier to prioritise connections. Some vendors provide their own tools to switch between the two approaches, but in XP simply open the wireless connection properties and click the Wireless Networks tab where you will find an option marked 'Use Windows to configure my wireless network settings'.

16 Standards matter

Wireless networking standards only guarantee a basic level of interoperability and many vendors also offer add-ons to, for example, boost performance or make it easier to configure security settings. These are proprietary and outside the common standards, so if you want to use them you'll need to build your wireless network using products from the same vendor.

Some care is also required with the new Draft-N products, which have been released before the 802.11n standard to which they are meant to conform has been ratified. ↘



Most adapters can be managed using either vendor-supplied software, or the tools that are included in Windows

They do work, but interoperability and conformance to the final standard, when it's finally agreed, can't be guaranteed.

17 Firewall requirements

A common question on both wireless and wired networks is whether there's any need for a desktop firewall on individual client PCs when there's already one built into the shared internet router. The answer depends on how the PCs are going to be used. The firewall in the internet router will provide a basic level of protection, but only while the client PCs are connected to the local network. Take a notebook off site and connect to a wireless hotspot, for example, and you can't be certain what level of protection you will end up with.

A local firewall is, therefore, worth considering, but you don't have to buy into a third-party product. The firewall included with Windows XP and Vista is pretty good, especially when teamed up with a good anti-virus tool and anti-spyware software. Indeed, they're so easy to deploy you might as well use them on all your desktops anyway.

18 Wifi to the desktop

It's easy enough to connect notebooks to a wireless network, as most now come with integrated Wifi interfaces or slots to take readily available PC card adapters.

Desktop PCs are another matter entirely, and here you've got two choices. One is to find a compatible internal wireless Lan adapter, although that will involve opening up the PC and fitting the card. A far simpler alternative is to buy an external WLan adapter, available from all the leading vendors, designed to simply plug into a free USB port.

USB adapters are available for all the popular Wifi standards, including the latest Draft-N technology. Just make sure you install the software provided first, before plugging the adapter in, and installation should be a breeze.

Bear in mind, however, that wireless networking will almost always be slower than having a wired connection.

USB adapters can be used to connect desktop as well as notebook PCs to a wireless Lan

Once you've got a wireless network up and running you can connect a wide range of Wifi devices such as this VoIP phone to it

19 What about 802.11a?

Most home and small-business wireless products operate in the 2.4GHz waveband. Those labelled 802.11b, 802.11g all use this frequency, as do most Draft-N implementations. However, yyyou can also get devices that operate in the 5GHz waveband, the most common standard being 802.11a with some 802.11n products being developed to use this frequency.

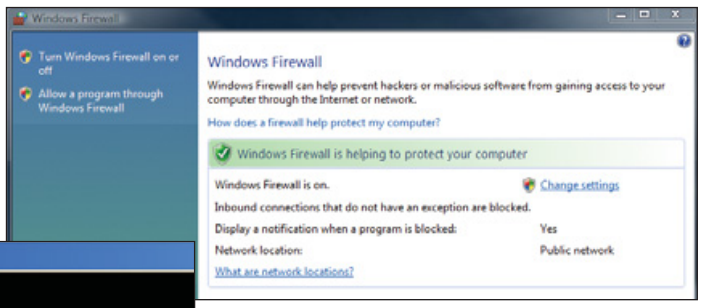
One benefit of 5GHz is reduced interference from other networks as it's a far less popular technology. As a result, however, the products tend to be a lot more expensive and there's much less choice, with very few 802.11a wireless routers, for example, on the market.

And, of course, there's no interoperability between the two wavebands, so buy a notebook with an 802.11g wireless interface and it won't be able to connect. As such, 5GHz wireless networking is probably best avoided for the time being.

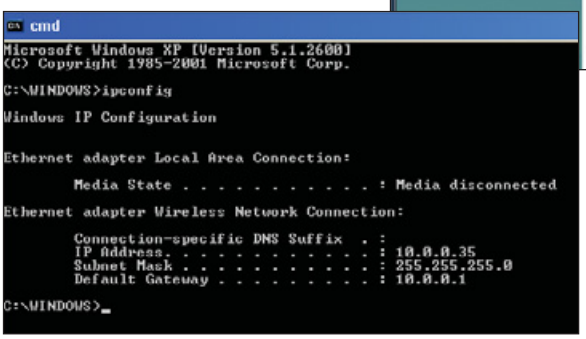
20 Wireless everywhere

Once you've got a wireless network, there's a lot more you can do with it beyond simple sharing of internet access. Wireless multimedia streaming, for example, is an increasingly common application, with Wifi-enabled audio systems on sale that let you beam music anywhere in the house. You can also buy appliances from companies such as Apple, Buffalo D-Link and others that are designed specifically to enable you to wirelessly stream music and video from your PC directly to a television in your home.

Likewise, wireless printers and print servers are increasingly common, along with wireless cameras and Wifi phones, all of which are designed to take advantage of your wireless network. **PCW**



Above: Although your wireless router probably has a firewall built in, it's still worth employing the Windows firewall on client PCs



Left: Use the ipconfig command to see if you've been assigned a valid IP address