Technofile: wireless networks

Wireless networks are both convenient and, in the long run, cost effective. Simon Williams explains their key benefits, the technologies involved and how to link up your PCs without draping ugly cables over floors and around the walls. Welcome to the future of networking

One PC on its own is an invaluable asset, but by connecting it to an entire network of computers you gain access to a range of powerful functions. Resources like printers and the internet can be shared among machines, while files can be stored at a central location and easily swapped between desks. Common information can also be held on network servers and accessed quickly by any PC linked to it.

However, the logistics of running cables to each PC from a central networking hub are far from trivial. Housing the cables is no small task and, in an open-plan office, the frequent need to run cabling to the centre of the floor can result in unsightly channels running along the ceiling or the expense of a raised floor with sockets.

Of course, you can have all the advantages of a network without the inconvenience of cables. It's much easier to fit each networked PC with an unobtrusive expansion card. All your data is then transmitted between systems wirelessly on low power. If you need to move a PC to a different place in the office, there's no network rewiring to consider. Equipment may cost more initially, but the increased efficiency of this type of network more than compensates.

Wireless networking has plenty in common with its cabled equivalent, but there's plenty of new terms and, above all, networking standards to learn. Let's start at the beginning.

Wi-Fi: the common standard

There are a number of wireless networking standards that govern how equipment is built and most of these fall within the less-than-memorable 802.11 category. The most popular standard is currently 802.11b, also known as Wi-Fi, which was drawn up by the IEEE (Institute of Electrical and Electronics Engineers).

This standard operates at a frequency of 2.4GHz and offers data transfer rates of up to 11Mbps (megabits per second). This throughput is roughly equivalent to a 10BaseT-cabled ethernet link and, although it's fast enough for general-purpose office networks, it may prove slow when transferring large amounts of data – for example, high-resolution graphics or video.

As you increase the distance between transceivers – that is, computers or devices on the network – the data rate under 802.11b will gradually drop. Full-speed data transfer at 11Mbps will typically be restricted to a range of around 25-50m indoors, although outdoors the range can easily be twice this. At a distance of more than 50m you will still get full error correction but the data transfer rate may fall to 5.5Mbps, 2Mbps or, at the furthest extremes can plummet to 1Mbps.

Beware of manufacturers who quote ranges of 'up to 300m' and data transfer rates of 'up to 11Mbps', as it's very unlikely you'll see both these maximums together. When comparing different suppliers' wireless networking equipment try and make sure all quoted ranges are at the kits' maximum data rate.

The range of an 802.11b wireless network can be extended by adding a better aerial and positioning it high up on a wall or ceiling. Alternatively, you could try adding extra 'access points'. Generally these are standalone devices that, when plugged into a network, act like wireless hubs. By handing the user from one access point to another, the effective range can be significantly increased. Indeed, with the correct use of access points and careful positioning of aerials, an 802.11b network can cover a considerable distance.

When positioning aerials in a large network it's also vital to avoid multipath propagation. Although, ideally you want each radio signal to reach its destination without interruption – in an office or home environment there are any number of obstacles (chairs, walls, office partitions, reflective surfaces) that can get in the way and bounce the signal from one part of a room to another. This results in the signal frequently breaking up into several pieces, which isn't good as it takes the receiver time to stick the pieces back together. Worse still, one of the portions may arrive at the same time as an entirely different signal causing even more disruption. To cut down on multipath propagation, try and position aerials so that there are as few obstacles in the line of sight as possible.

This isn't the only form of interference since the 2.4GHz frequency band, in which 802.11b operates, is a busy section of the radio spectrum. In particular, microwave ovens, Bluetooth devices and cordless phones may all be fighting for airspace. If interference from these is causing too many problems, there are other networks you can turn to.

→ A wireless router handles the connection between the modem/terminal adapter and your network

← A wireless network card normally takes the form of an elongated PC Card. It fits directly into a PC Card slot with a small protrusion outside the slot which forms the wireless network aerial

802.11: the alternatives

The lack of intrusion from such devices is a significant factor in the rising popularity of 802.11a wireless networks. This newer standard offers data transfer rates of up to 54Mbps. While this is only half the data transfer rate of a 100BaseT ethernet link, it's still nearly five times as fast as 802.11b. With this extra capacity an 802.11a wireless network can typically handle more PCs than its 802.11b equivalent without affecting performance.

Currently, however, 802.11a network cards and access points are around 25 percent more expensive than their 802.11b counterparts. This cost difference will gradually reduce, though, as more and more manufacturers release dual-standard equipment.

It's not hard to imagine 802.11a/b dual-standard wireless network cards becoming as commonplace as 10/100BaseT dual-standard cabled ethernet cards are now. There's another player in the 802.11 camp known as

Connecting to the internet

It makes very little difference from a networking point of view whether you choose to connect to the internet from a fixed, cabled or wireless network. In each case you need a router to handle the connection between the modem/terminal adapter and your network and to distribute messages to the appropriate recipients at individual computers. You'll also need an appropriate terminal adapter or modem for the kind of internet connection you're using.

On cabled networks you can buy a network hub or switch with a built-in router. The idea is very similar on a wireless network, except that here you would buy an access point with the router built in. If you have a hybrid (part-cabled, part-wireless) network, the router you may already have for the cabled part of your network can usually be made to work via the access point for any wirelessly networked machines.

As with a cabled network, you must assign IP (internet protocol) addresses to all the connected PCs. This can be done with an automated DHCP (dynamic host configuration protocol) server or by manually typing in all of the numbers. For a small network you may find the latter approach more stable, but on a larger network the automated solution would prove more workable.

Also remember that, with the increased resources of the internet comes decreased security. For more information on protecting your network against unwanted visitors, see *Protect your network* on page 71.

Protect your network

Anybody wanting to hack into a cabled network must either break through its firewall security or obtain physical access to one of the networked PCs. But with a wireless network the latter restriction is removed. Anybody falling within range of the wireless coverage can potentially connect to the network. The only defences are an effective network firewall, good network encryption and measures taken to ensure the RF (radio frequency) range drops off steeply outside the intended coverage area.

The practice of 'warchalking' started last year and has since caused wide controversy. Wireless network coverage is marked on public footpaths and walls by interested individuals. These may be potential hackers or even security consultants keen to show why companies might choose to use their services.

If you have a notebook or a PDA (personal digital assistant) with wireless network capabilities it's simple enough to walk around checking where there's a compatible signal that could be used to link to a wireless network. As well as the possibility of hacking into the network itself, it can also be used as a free connection to the web via the network's internet gateway. It's very important when setting up a wireless network, therefore, to consider access from a 'false node' of the network itself, as well as guarding against hacking from the internet.

Two of a kind

Of the two kinds of wireless network structure – ad hoc and infrastructure – an infrastructure network is implicitly more secure. It requires a recognisable domain name and password before any PC can gain access to network services, whereas an ad hoc network is designed specifically to connect new devices with a minimum of fuss.

Although security measures can still be applied to ad hoc networks, the infrastructure approach is designed specifically with the security of a fixed network structure in mind.

802.11g. While this standard, which is still at a draft stage, offers a maximum data transfer rate of 54Mbps (like 802.11a), it still operates at 2.4GHz (like its 802.11b sibling). It may have a higher throughput but 802.11g is still likely to suffer from the same interference problems as the common 802.11b standard. Not only that, it also lacks the extra capacity that 802.11a enjoys through its higher frequency band.

→ SMC aims its 7004AWBR access point at home and small business users alike

The advantage of 802.11g is that, unlike 802.11a, it's backwardly compatible with the slower 802.11b. When the standard is finally ratified, newer 802.11b access points may even be upgradable through firmware. For those who have already made an investment in an 802.11b wireless network, the route to 802.11g may prove cheaper.

The 802.11 category doesn't stop there, though, as there are other varieties currently being developed.

First up is a variant of 802.11a, known as 802.11h. The main difference is its TPC (transmission power control) feature which ensures the network only ever uses the minimum power needed to transfer data between its most extreme nodes.

The second in the pipeline, known as 802.11i, improves the encryption used in earlier members of the standard. Known as WEP (wired equivalent privacy), this feature was shown to have some weaknesses. The new encryption in 802.11i should improve security in wireless networks and may well be available as a firmware upgrade to equipment using earlier versions of the standard.

Bluetooth

The Bluetooth standard is named after the blueberry-loving viking King Harald (he liked the fruit so much that they stained his teeth) who, unusually, preferred talking to fighting.

Originally envisaged as a wireless connectivity standard for mobile phones and peripherals, Bluetooth has recently been mooted as a suitable candidate for wireless networking, where this standard excels is in its immunity to interference.

By using a clever technique of automatic frequency hopping between 79 allocated frequencies, Bluetooth devices can continue talking to each other – even when there's a lot of other traffic in the same frequency band. Most Bluetooth processors can handle up to seven information channels simultaneously, so a single device in a PC or PDA (personal digital assistant) can potentially communicate with several peripherals at the same time.

Unfortunately, when it comes to general networking, Bluetooth simply isn't up to the task. For a start it has a comparatively short maximum range of 10m, making it suitable only for small-scale networks in a home or small office. An even bigger restriction, though, is the maximum data transfer rate of just 2Mbps – around a fifth of 802.11b's capacity.

While this is adequate for passing information to printers or headsets, it

would leave you waiting an uncomfortably long time when transferring standard network data. It's best to leave Bluetooth for what it was designed for – that is communicating with individual printers and peripherals rather than PCs.

HiperLAN

The alternative to the 802.11 clan is HiperLAN, a European wireless network specification aimed at two different frequency bands – 5.15-5.25GHz and 17.1-17.3GHz. Power output for HiperLAN transceivers is restricted to 1W in the lower band and 100W in the higher.

← 3Com's 3CRWE20096A is a great choice if you're looking for basic 802.11b wireless LAN extensions that won't strain your budget

The HiperLAN 2 standard uses the 5.15-5.25GHz band to provide a wireless network that can deliver up to 54Mbps or a range of up to 150m, although not at the same time. It works in a similar way to 802.11 networks, with one or more access points communicating with wireless network cards fitted to PCs.

However, HiperLAN is less well-developed than its main rival and while some major players continue to support it – Canon, Ericsson, LG, Motorola, Nokia, Panasonic and Sony among them – others such as Philips, have decided not to make chipsets for this standard.

HomeRF

As the name suggests, the HomeRF standard is intended primarily for use in the home. As well as providing wireless data transfer, it also offers wireless voice transfer so you can use wireless headsets for answering phone calls. Up to four separate voice conversations can be carried out simultaneously through a HomeRF network.

The new HomeRF 2 standard has increased the data transfer rate from 1.6Mbps to 10Mbps – with a further increase to 20Mbps planned – making it suitable for most home uses. It hosts the same 2.4GHz frequency band as 802.11b and Bluetooth but, once it has established the frequency of the unwanted signals, it implements a frequency-hopping regime to try and block any interference.

Suppliers of HomeRF kits are still few and far between but the technology has several advantages that may see it grow in popularity as wireless networking becomes more attractive to home consumers.

Setting up a wireless network

There are two ways of setting up a wireless network: both techniques involve a similar set of hardware, they're just connected in different ways. It depends on whether you're adding a wireless component to an existing cabled network or creating a wireless network from scratch.

The key components – you will need at least one example of each in a wireless network – are the wireless network card and the access point. An access point (a small box about the size of a paperback book) provides the housekeeping functions of the wireless network. It connects to one of the PCs in your wireless network or directly to a cabled network hub/switch. It provides automatic name and IP (internet protocol) address allocation, as well as communicating with other network hardware such as ethernet hubs.

A wireless network card normally takes the form of an elongated PC Card. It fits directly into a PC Card slot with a small protrusion outside the slot which forms the wireless network aerial. This is fine for notebook PCs, but if you want to network desktop PCs wirelessly you'll also need a PCI adapter.

Features comparison: access points

Model	Phone	Website	Typical street price (ex VAT)	Wireless standard	Wireless nodes	Maximum data rate	Router included	Print server included
3Com 3CRWE20096A	01442 438 000	www.3com.com	£109	802.11b	up to 128	11Mbps	no	no
Buffalo WLA-L11G	01753 555 000	www.buffalo-technology.com	£94	802.11b	up to 128	11Mbps	no	no
Intel Pro Wireless 5000 Starter1	01793 403 000	www.intel.co.uk	£399	802.11a	up to 64	54Mbps	no	no
Netgear MR314UK	0870 112 1206	www.netgear.co.uk	£99	802.11b	30-70	11Mbps	yes	no
SMC 7004AWBR	01932 866 553	www.smc-europe.com/english	£115	802.11b	up to 128	11Mbps	yes	yes
Zoom Hayes ZoomAir 4165-72-00	01493 748 904	www.zoom.com	£169	802.11b	approx 30	11Mbps	yes	yes

Features comparison: wireless network cards

Model	Phone	Website	Typical street price (ex VAT)	Product format	Compatible PCI adapter	Wireless standard	Range at full data rate	Operating system compatibility
3Com 3CRDW696	01442 438 000	www.3com.com	£65	PCI card	standalone	802.11b	100m	Windows 98 to XP
3Com 3CRSHEW696	01442 438 000	www.3com.com	£49	USB	external	802.11b	300m	Windows 98 to XP
Belkin F5D6020u	0800 2235 5460	www.belkin.co.uk	£46	PC Card II	external	802.11b	180m	Windows 95 to XP
Buffalo WLI-CB-G54	01753 555 000	www.buffalo-technology.com	£45	PC Card II	n/a	802.11g	20m	Windows 98 to XP
Buffalo WLI-CF-S11G	01753 555 000	www.buffalo-technology.com	£69	CompactFlash	n/a	802.11b	25-50m	Windows 98 to XP, CE3
D-Link DBT-120	020 8731 5550	www.d-link.co.uk	£30	USB	external	Bluetooth	10m	Windows 98 to XP

Rather than making two different types of wireless network card, many manufacturers produce only PC Cards (which fit notebooks as standard) and provide PCI adapters for anyone wishing to use the network cards on desktop PCs. The only disadvantage of this approach is security, as it's comparatively easy to remove a PC Card.

The simplest wireless network consists of one PC connected directly to an access point communicating with a second PC equipped with a wireless network card. Under most recent versions of Windows the software supplied with wireless networking equipment automatically sets everything up and it works, in all respects, like a cabled ethernet link. You can establish shared resources and allow access to your files from other networked PCs in exactly the same way you would with a cabled connection.

You can add other PCs to a wireless network by simply equipping them with wireless network cards up to the limit supported by the access point – usually between 128 and 256 devices. Once up and running, a wireless network is much easier to expand than a cabled one and maintenance is very similar with both types of connection.

↓ Netgear's MR314UK wireless router enables Cable/DSL modem sharing via built-in four-port 10/100Mbps switch

→ Wireless network cards come in many shapes and forms – USB, PCI, PC Card and flash memory. This Buffalo model is a USB version

If you want to add wireless facilities to an existing cabled network, you must equip every PC with a wireless network card. You'll also have to connect an access point to your network hub or switch. The access point takes the place of one of the PCs in your cabled network so you'll also need a spare port available to make the connection.

Setting up the wireless network mainly involves ensuring that every PC has a unique IP address and name. For a brand new wireless-only network you can leave this to the automated address and name servers. If you're integrating a wireless network within an existing cabled one, though, you'll have to ensure the wireless PCs have addresses and names which are consistent with those already allocated.

Verdict

Wireless networking is growing in popularity, with improved data access rates and ranges being announced virtually every month. The many varieties of the 802.11 standard provide the basis for quick-and-easy network setup and offer performance approaching that of ethernet cabled equivalents.

Alternative standards – for example, HomeRF – may be particularly appealing in certain markets such as for consumers who have specific usability, security and multimedia requirements. In our opinion, though, Bluetooth, a valuable technology for interconnecting PCs, PDAs and peripherals, is not really fast or versatile enough for wireless networking. ■

Find out more about the advantages of wireless networks in our *Wireless primer* feature on page 98