Update: Wireless Networking

Wireless networking could be invaluable for certain applications, such as bridging wired LANs and connecting portables. We discuss current issues and the state of the market.

By Bryan Betts
IT Journalist

Wireless local area networks are on the ascent, thanks to the emergence of 11 Mbits/sec high-rate wireless Ethernet and the formation of a body dedicated to maintaining wireless Ethernet compatibility. However, they bring new problems, especially in the area of network security and management. Previous generations of wireless Ethernet were significantly slower than wired LANs, and wrangles among the manufacturers meant that interoperability was limited. As a result, their take-up was limited. The latest version of wireless Ethernet has been improved in both areas, matching standard Ethernet on speed and with an industry consortium to verify interoperability. Called IEEE 802.11b, the high-rate wireless Ethernet standard was ratified in 1997 after seven years' work. It is maintained by the Wireless Ethernet Compatibility Alliance (WECA) which carries out cross-vendor compatibility testing. Verified manufacturers are listed on the WECA Web site (**www.wi-fi.com**) and can use WECA's Wi-Fi logo in their advertising.

Wireless Ethernet operates on the 2.4 GHz ISM (industrial, scientific and medical) band, which is licence-free, but has regulations on power and bandwidth. Initially there were problems with its usage in certain countries, notably France and Japan, but these have now been resolved. The network can provide 11 Mbits/sec over a range of up to 30 m indoors or 150 m in the open although, as with other shared networks, the real data transfer rate may be around half this. It can cover longer distances and combat interference by dropping back to lower speeds. Its range is greatest at 1 Mbit/sec, when it can cover 50 m indoors or 400 m outdoors. Speed is increasing, too, with a 22 Mbits/sec version of 802.11b due by the end of 2001. Beyond that are IEEE 802.11a and HiperLAN/2, both of which will support 54 Mbits/sec and operate on the 5 GHz band. These two are rivals, but they also have a lot of technical similarities, so there are proposals to merge them, or at least to provide some interoperability.

The potential problems with wireless Ethernet revolve around the frequencies used. The 2.4 GHz band is also used by Bluetooth, and while the two can co-exist they will affect each other's data rates and connection quality. In addition, 22 Mbits/sec devices should be backwards-compatible with 11 Mbits/sec, but 54 Mbits/sec devices will not be, unless they are dual-mode. Lastly, a higher frequency brings greater bandwidth but it also means shorter range and less ability to pass through solid objects. It is possible that 5 GHz signals may have difficulty passing through even a thin wall. Conversely, a lower frequency, such as the 900 MHz used for GSM phones, brings greater range but a lower bandwidth.

Applications

Typical wireless Ethernet applications include the creation of *ad hoc* LANs, the linking of portables into a wired infrastructure, and wireless LAN bridging - for example, between two offices separated by a road. In a peer-to-peer network, PCs with wireless cards can exchange data directly. Alternatively, an access point allows them to communicate with the fixed Ethernet too, via a 10 Mbits/sec Ethernet hub or a 10/100 switch port. Internet connection is possible via a fixed or dial-up link: for example, an ISDN or DSL router. A wireless LAN also means users can roam inside the company. This did not work in the original 802.11 wireless Ethernet as the protocol was not clearly defined, but this has been fixed in 802.11b, which therefore permits roaming between different base stations.

Although WLAN cards are still more expensive than ordinary cable-based Ethernet cards, they bring savings in other areas. A wireless LAN has far lower infrastructure costs, with no cabling or hubs to be installed, except perhaps for a central file and print server. The wireless Ethernet NICs available are interoperable, not least because there are only two silicon manufacturers worldwide, and they all use a similar MAC. In addition, 802.11b developers have ignored the 2 Mbits/sec frequency-hopping radio and infrared options to concentrate on DSSS (Direct Sequence Spectrum Spread) radio.

Reliability

DSSS spreads the signal over several frequencies and can switch channels to avoid interference. Each network can be set to one of 13 available radio channels, though as the channels overlap it is not possible to have more than three wireless Ethernets in the same space. Bluetooth frequency-hops across the whole ISM band, whereas any individual 802.11b cell only uses one-third of the available spectrum, making the two less likely to conflict. In addition, Bluetooth only transmits when it has data to send, and is quiet most of the time. Research suggests that interference between 802.11b and Bluetooth is only a major problem when the transmitters are close together, for example if a single PC has both, and even then wireless Ethernet should still be reliable, although its effective range will be reduced.

Tests using audio, when the Bluetooth devices are continuously transmitting, show that if the two transmitters are placed on top of each other and physically in contact, the wireless Ethernet can drop right back to 1 Mbit/sec, while the Bluetooth sound becomes clicky as packets are lost due to collisions with 802.11b. Once the transmitters are more than a few inches apart the wireless Ethernet returned to its normal speed. However, the Bluetooth sound remains clicky (but comprehensible) during Ethernet file transfers.

Wireless Ethernet is much faster than Bluetooth, which has a maximum data speed of around 750 Kbits/sec, but Bluetooth is cheaper and uses less power, so it will be the preferred method of linking-in devices such as mobile phones, audio headsets, Palms and Pocket PCs. It can be used as a network, but for office use a proper LAN is far preferable. The relevant standards bodies are also working on ways to harmonise 802.11b and Bluetooth. One possibility would be to have both use the same radio chip within a PC, thereby avoiding many of the interference issues.

Security

There have been reports that listening in to WLANs is an increasingly popular pastime among US crackers. Whether this is true or not, the fact is that a radio-based LAN is far more open to interception than a wired LAN. It is essential therefore to secure the network, not only to protect the LAN but also to avoid providing free access to your Internet link.

For a small LAN, the basic scheme of maintaining a list of permitted NICs works well. A list of MAC (media access control) identities is programmed into the access point, with most access points allowing these lists to be maintained via a Web interface, so updates can be made from anywhere in the network. Any other NIC

"A radio-based LAN is far more open to interception than a wired LAN. It is essential therefore to secure the network."

Wireless Ethernet Suppliers

Wireless Ethernet products are available from almost all the major network suppliers, although in many cases they are not the original manufacturer. For example, Xircom's adapter card is a rebadged version of the Aironet 340 which is now owned by Cisco, Intel gets its products through a deal with Symbol Technologies, and the Symbol Spectrum24 access point also looks suspiciously similar to the 3Com AirConnect equivalent.

Other suppliers include Apple, Enterasys Networks, Avaya (formerly part of Lucent Technologies), D-Link, NoWiresNeeded, Buffalo Technology, SMC Networks, Zoom Telephonics and Proxim. In addition, Far Eastern manufacturers are now getting involved, with a number of new companies showing 802.11b hardware at this year's CeBIT exhibition in Germany.

will be unable to access the wireless network, although it may be able to listen in to network traffic, so the use of encryption is advisable. As an alternative to MAC lists there are schemes which use RAS-type security, for example 3Com's SuperStack. This takes advantage of the fact that most laptop users will already have some form of access control set up for dial-in access, such as Radius, which can also be used to control wireless access. Not all access points support Radius, however.

The standard encryption level shipped with most wireless Ethernet systems is 40-bit, but 128-bit upgrades are available. This is still crackable, but cracking it requires greater resources, not least because 128-bit encryption randomly changes keys. For greater security, other encryption schemes can be added on top, as they can with a wired Ethernet. For example, the wireless access point could be located outside the firewall and all LAN access routed through a VPN (virtual private network) gateway.

Site Survey

Manufacturers supply site survey software with their NICs and access points. This is designed to help assess the area to be covered, and work out how many access points will be needed and where they should be located. Thick walls, metal obstacles, doorways and other features can all affect radio propagation for better or worse. The network designer will also need to consider how many users there will be, as each access point has a limited capacity. Each wireless LAN cell comprises several PCs sharing a single access point. In theory, there can be any number of PCs per cell, but in practice a maximum of 20 is recommended. This is because, as with wired Ethernet, performance falls as the network load increases, plus there is the added problem of radio noise.

It is possible for cells to overlap, in which case network load-balancing software can log new users onto a less heavily loaded access point, even though it is not the closest to the user. Alternatively, a second cell can be overlaid on the first at a different frequency, bearing in mind that the 13 available radio channels overlap, so you can only have three cells in a given area.

WLAN Equipment

Some portable Macintoshes and a growing number of laptop PCs have 802.11b built in - or at least an antenna for it. Most PCs will need a wireless NIC, though; these are usually 16-bit PC Cards, so a desktop PC will need a PC Card adapter before it can use one, and they cost between US$100 and US$200. NICs have an internal aerial, although some also have a socket for an external aerial to improve the range, which is advantageous for desktop PC use. Software drivers are available for Microsoft Windows 95 (note that OSR2 or later is preferred), 98, ME and 2000, also for MacOS, Linux and Windows CE. NICs are also becoming available for PDAs and other handheld devices: Xircom has demonstrated an 802.11b adapter in Springboard form for a Handspring Visor PDA, and CompactFlash cards are on the way.

Access point prices range from under US$200, for the most basic, to well over US$1000. Most simply connect to an existing Ethernet hub or a switch, but there are also access points with integrated modems or ISDN TAs for linking branch offices. Alternatively, an access point could be connected to an ADSL router. One other area is voice telephony, where companies such as SpectraLink have developed 802.11b wireless handsets. These are expensive but could be a good choice for organisations which already have a wireless LAN or voice-over-IP infrastructure planned or in place.

"Each network can be set to one of 13 available radio channels, though as the channels overlap it is not possible to have more than three wireless Ethernets in the same space."

All of this equipment is interoperable, thanks to the Wi-Fi certification. For example, we had no trouble setting up a 3Com AirConnect access point and then connecting to it with either a 3Com NIC or an Intel PRO / Wireless 2011 card.

Higher Speeds

The first 54 Mbits / sec wireless networks operating at 5 GHz should reach the market later this year. They will be expensive to start with and will only be appropriate where the high data rate is needed, perhaps for applications such as multimedia or for high-speed wireless bridging. There are also plans to double the speed again, this time to 108 Mbits / sec, though obviously this is even further in the future.

The problem is that while the 2.4 GHz and 5 GHz bands are unlicensed, they are not unregulated, and different jurisdictions have attempted to set different standards for the next generation of wireless LANs. Europe's choice is ETSI HiperLAN/2 (**www.hiperlan2.com**), while the US and Japan have chosen IEEE 802.11a (**www.ieee.org**). The differences between HiperLAN/2 and 802.11a are in the MAC layer and in the fundamentals of how they work. While 802.11a comes from a data heritage and is Ethernet-based, HiperLAN/2 is designed to work in other environments too, providing high-speed access to ATM and 3G mobile phone networks, as well as IP networks. In particular, HiperLAN/2 is connection-oriented and includes quality of service features, which could make it a better option for the high-throughput applications that might need more than the 11 Mbits/sec of 802.11b, such as streaming video and multimedia. Conversely, 802.11a has a big advantage in being perceived, rightly or wrongly, as the natural follow-on to 802.11b, even though the two are technically different.

Fortunately, there is also a lot of similarity between Hiperlan2 and 802.11a, to the extent that there are companies working on chipsets and radios that will support both and may allow interworking. This is possible because they use the same physical layer, called Orthogonal Frequency Division Multiplexing (OFDM), for modulating data before transmission. The use of OFDM resolves many of the issues associated with operating a wireless LAN indoors. Homes and offices are awkward places because the radio system has to deal with phenomena such as multipath and fading. Multipath is receiving multiple versions of the same signal thanks to reflections from walls, ceilings, furniture, people, etc. Fading relates to the signal being blocked by an object or by the position of the device. As well as dealing with these issues and increasing the reliability of the wireless link, OFDM also uses the radio spectrum more efficiently than spread-spectrum, allowing it to offer better performance.

It is possible that the 802.11a versus HiperLAN/2 battle will be Ethernet versus ATM all over again, with the technically superior and more flexible system being crushed by a cheaper alternative that has wider industry support. Getting to market first should also seal victory for 802.11a, as by the time HiperLAN/2 products appear buyers will have already made their investments.

Conclusion

The choice of which wireless LAN to deploy today is easy, as 802.11b is here now and it works. It provides up to 11 Mbits/sec, depending on the range, and unlike the previous 802.11 specification, it pretty much guarantees compatibility between different network hardware. It should also be compatible with forthcoming 22 Mbits/sec 802.11b products. For anyone needing higher data rates, then 802.11a products should begin to appear late this year, but at relatively high prices. HiperLAN/2 products will follow, along with higher volumes of 802.11a, during 2002. Beyond that are proposals to double the peak data rate to 108 Mbits/sec, though this will almost certainly require new network hardware.

In terms of the target applications, the increasing speed of wired networks means that 802.11a and HiperLAN/2 will still be used primarily as extensions to a fixed LAN. By the time they arrive, Gigabit Ethernet will be commonplace, meaning that even 108 Mbits/sec will not be enough for a backbone. It might be useful for linking network segments together outdoors, though, or where fixed cabling is impossible or impractical.

"A wireless LAN has far lower infrastructure costs, with no cabling or hubs to be installed, except perhaps for a central file and print server."

One other factor is the demand for public access services, such as wireless LANs in airports, and for home networking. Wireless Ethernet has also been adopted as the ideal technology for building local broadband Internets such as Consume.net, which would be connected to the Internet but would be independent of the local loop suppliers.

PCNA

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.