

No strings attached

Dan Cole, head of product management at THUS, discusses the types of wireless technologies available to small businesses

Considering the proliferation of wireless 'hot-spots' across the UK's towns and cities, it is easy to forget that wireless technology is something of a newcomer to the world of broadband access. It was only eight years ago that the first wireless networking standard left the laboratories and became available to home and business users alike. 802.11b, or WiFi as it is more commonly known, provided organisations with the possibility of an efficient and cost effective broadband access which promised to do away with the cumbersome wiring that litters most offices. The dream was of a clean and uncluttered access to a business' broadband service, providing a convenient and flexible means of connecting to the office LAN and World Wide Web. To some extent this vision was realised.

One of the key benefits of wireless technology is the ease with which it can be updated and improved. Upgrades are a simple affair requiring nothing more than new base stations and wireless cards. This is a world away from the re-cabling needed to upgrade a fixed line broadband network, with its implications of high cost and considerable disruption. This begs the question: what new wireless technologies are available to businesses and what do businesses need to know about them?

WiFi on steroids?

These days, WiFi is hard to miss. The ubiquitous wireless standards have found use in a wide range of devices: from computers to mobile phones and even in MP3 players such as the latest iPods. It is important to note, however, that WiFi comes in a number of 'flavours' and these can affect the uses to which a business can put the technology. The older standard (802.11b) can provide broadband access up to 11Mbps. This is suitable for most small businesses that primarily use the technology for email applications, data networking and possibly internet telephony. The updated version of WiFi (802.11n), on the other hand, can provide data rates of up to 248Mbps. These faster transfer rates would suit businesses in niche sectors, such as the media or architectural professions, where very 'heavy' data files routinely need to be sent between locations. WiFi standards are backwards compatible, so a machine which supports 802.11n will drop down to slower data rates if required.

WiFi does, however, have quite a short range (in the tens of meters). This means that in the office environment deployments usually involve a number of base stations being placed in strategic places throughout the building, which connect to the main fixed line network. It should be seen, therefore, as complementing, rather than replacing, fixed line networks.

WiFi is not alone in the world of wireless connectivity. One standard in particular is causing much interest within the telecoms industry and has been labelled 'WiFi on steroids'. WiMAX (Worldwide Interoperability for Microwave Access) places its emphasis on long physical range in an effort to create a wireless standard capable of replacing the 'last mile' of cable into a building. Due to this, some are speculating that the technology might be a possible alternative to cable or DSL, rather than a direct replacement for WiFi. The WiMAX standard, known as 802.16e, is capable of up to 70Mbps, less than the maximum for the fastest WiFi, but its range can be as much as 10km with high data rates from a single base station.

Why go wireless?

The primary benefits of wireless lie in its low cost and great flexibility. Fixed line broadband is not always easy to provision, and the cost of connecting to the network can be prohibitive if there are no fixed floor boxes or where new cable needs to be laid. Wireless means you have less need to densely run cables throughout your building, and can instead rely on having wireless access points covering areas where there's either lower usage or fewer employees.

For employees, wireless networking delivers greater flexibility too. Rather than having their machines tied to their desks, they can carry laptops around the building while retaining good connectivity, meaning more flexibility around meetings.

What's more, wireless makes it easier to construct a flexible working system based around "hotdesks". These are workspaces which are allocated not to a specific employee, but through a pool system. While it's possible to create a hotdesk system using fixed networks, wireless offers more flexibility about the type and structure of the physical spaces you can use.

Complementing fixed networks

It must be emphasised, however, that wireless (regardless of whether it is WiFi or WiMAX) is not a direct replacement for fixed or cable networks. The reasons for this are twofold. Firstly, wireless will never be able to compete with fixed-line Ethernet access in terms of speed. Gigabit Ethernet runs at more than four times faster than even the most up to date WiFi network, and over distances where wireless cannot come close.

Secondly, there is the question of reliability. Although wireless networks are, by and large, reasonably reliable, like any radio-based system they can be affected by interference, either from atmospheric conditions or from poorly shielded electrical equipment.

However, the flexibility of wireless makes it an ideal complement to a fixed network infrastructure. If your wired network acts as the reliable, fast workhorse then an additional wireless network can extend your infrastructure into places which would otherwise be impossible to reach.

Are wireless networks secure?

The question of security is one that has plagued the wireless standards since their inception eight years ago. Any signal which can be received inside the office is in danger of being eavesdropped from outside the office. The fact is, anyone can listen in to your WiFi connection if it is not secured properly.

Thankfully, there are many ways of making a wireless network secure. Firstly, ensure your network uses the stronger, more recent WPA encryption rather than the older WEP standard. WEP has been broken many times, allowing any determined hacker to easily compromise your data.

Secondly, enable MAC filtering. This allows you to specify which MAC addresses – unique codes embedded in every networking interface – are allowed to connect to the network, effectively locking out unauthorised machines. However, be aware that a determined attacker can get round this: there are ways to fake MAC addresses, which means an attacker could get through by guessing a correct address.

An obvious element of security, and one that is often overlooked, is that of

passwords. It is easy to be complacent when it comes to regularly changing the password, but it is vital to do this if the security of the WiFi connection is not to be compromised.

With the correct safeguards in place, WiFi and WiMAX will continue to offer great benefits to businesses choosing to network through them. Its flexibility can offer businesses new ways of working, while making the most of the available office space. They will not replace fixed line networks in their entirety; nevertheless organisations of all sizes should be looking to leverage the benefits of going wireless.