

Wireless Networks



The use of mobile phones has had a major impact on the way people communicate. Other mobile devices, such as laptop computers and handheld devices have also become an integral part of everyday life. The portability and flexibility of these devices has succeeded in placing mobile technology in the realm of mainstream technology, both in the workplace and the classroom.

The development of wireless networking solutions represents a significant evolutionary step in this arena, as devices can now be fully networked even though they are not physically connected with cables.

What is a Wireless Network?

When the term '*wireless network*' is used today, it usually refers to a wireless local area network (WLAN). A WLAN connects computers together through radio technology using standard network rules or protocols, but *without* the use of cabling to connect the computers together.

A WLAN can be installed as the sole network in a school or building. However, it can also be used to extend an existing wired network to areas where wiring would be too difficult or too expensive to implement, or to areas located away from the main network or building. The most obvious difference between wireless and wired networks, therefore, is that the latter uses some form of cable to connect computers together. A wireless network does not need cable to form a physical connection between computers. Wireless networks can be configured to provide the same network functionality as wired networks, ranging from simple peer-to-peer configurations to large-scale infrastructures accommodating hundreds of users.

Wireless Network Components

There are certain parallels between the equipment used to build a WLAN and that used in a traditional wired LAN.

- Both networks require a network interface card (NIC) that is either built-in to or added to a handheld, laptop or desktop computer. There are two main types of plug-in card available: PCMCIA which is inserted into the relevant slot in the side of a laptop and PCI which is inserted into one of the internal slots in a desktop computer. Wireless NICs contain an in-built antenna to connect with the network.
- In a wireless network, an '*access point*' (AP) has a similar function to the switch in wired networks. It broadcasts and receives signals to and from the surrounding computers via their wireless NICs. It is also the point where a wireless network can be connected into an existing wired network.

Wireless Network Configurations

Wireless networks can be configured in ad hoc or infrastructure mode using access points.

Ad Hoc Configuration

This is the most basic wireless network configuration and is the equivalent of a wired peer-to-peer network. This arrangement requires nothing more than wireless NICs in each of the connecting computers which associate through use of a common network name. However, the range of this configuration is limited and administration becomes an issue with more than just a few nodes. Thus, ad hoc configurations should only be used for the smallest of wireless networks where scalability and security are unimportant.

Infrastructure Configuration using Access Point(s)

With the installation of an access point, the range over which the network is accessible increases to approximately 150m indoors and 350m outdoors (optimum performance within 30m indoors). It is possible for an access point to support up to 30 clients, but in practice more access points are needed to support large numbers of wireless PCs. Access points are connected together via a wired LAN. The access point can also act as a bridge, allowing the wireless network to connect to a wired network.

In a situation where users need to be mobile and still retain their connection to the network, the coverage provided by the access points should overlap. As the user moves from one area of coverage to another, the network connection is transferred from one access point to the next, without the user noticing.

Two other pieces of equipment may be required to support a wireless LAN:-

- Extension points which act as wireless relays extend the range of an access point
- Directional antennae may be used as a means of connecting two separate buildings so that the network is shared between buildings.

Benefits and Educational Uses

- Installation time and costs are significantly reduced.
- Network is accessible in places where wiring would have been difficult.
- The space over which a wireless network operates is not planar but spherical providing access in rooms above or below the access point in a multi-level site without the need for additional infrastructure.
- Teachers and students can have continuous access to the network, even as they move with their equipment from class to class.
- Computers fitted with wireless network cards can be placed on trolleys and moved from location to location within a school in order to facilitate group work, sharing of files, printers and Internet access.
- Wireless range can be extended beyond the main school building to allow students and teachers use wireless devices to gather and record data outside, e.g. as part of a science experiment or individual performance data from a PE class.

Issues to be aware of:

Before installing wireless networks schools should be aware of the following issues:

Health Considerations

- Some health concerns have been raised that wireless networks in association with wireless laptop computers in schools may pose a health risk to pupils, due to the levels of radiation emitted. The Government published the Report of the Expert Group on Health Effects of Electromagnetic Fields (EMF) on 22nd March, 2007, which examined a wide range of issues in relation to potential health effects of EMF, including those produced by mobile telecommunications. The Group concluded that *“so far, no adverse short or long-term health effects have been found from exposure to the radiofrequency (RF) signals produced by mobile phones and base station transmitters. RF signals have not been found to cause cancer.”* The Department of the Environment, Heritage and Local Government has assumed responsibility for the health effects of EMF with effect from 1 May, 2007. The full report can be accessed at the link below:

Wireless Speed and Reliability

- Wireless networks may seem to be a simpler alternative to networking a school than a cabled network, however schools should not install wireless networks unless they are aware of the potential issues and satisfied that it is the right decision for the school. Wireless networks are significantly slower than fixed networking, by a factor of approx 10. Wireless is also less reliable than cabled networks mainly due to issues such as the movement of mobile PCs and possible reductions in signal strength due to changes in the local environment. Wireless networks are typically not suitable for schools with thick walls, including many older schools.

Security of school data:

- As wireless data travels through the air, there is a risk it could be accessed by other parties at ranges of 100-300 metres outside of the school grounds. There is thus a risk that sensitive school or pupil data could be accessed by unauthorised parties. In order to prevent such an occurrence high quality wireless security software would need to be installed by qualified companies who can provide the appropriate level of technical support and maintenance to schools. Too often schools install wireless networks with either no or inadequate levels of security.

Technical and Purchasing Considerations

- If wireless is to be installed it is essential that that school receives a warranty and maintenance agreement, so that they understand the possible additional costs associated with the wireless network. The agreement should resolved issues such as reliability of signal, lack of coverage, security. A service level agreement (SLA) should be provided by the provider so that the school is aware of the extent of service provision and possible additional charges associated with the service.
- Wireless NICs are more expensive than their wired counterparts. The cost of the access points should be considered.
- Wireless networks typically work at 54Mbps which is shared between all the workstations using an access point whereas a hard-wired network connection is capable of running at 100Mbps (Fast Ethernet). A wireless network will be noticeably slower when a group of users are transferring large files. This should be considered if multimedia applications are to be delivered over the network to a significant number of users.
- Wireless data transmission rates are dependant on the number of users, the distance from the access point and the fabric of the building (metal structures in walls may have an impact).As the range of the network may extend beyond the walls of the building, it could become accessible from outside. Consideration should be given to what security features the equipment provides to ensure that only authorised users have access to the network and that data is protected.

Relevant Web Sites

Further information on wireless networks is available at:

In depth Wi-fi Information

http://www.wi-fi.org/knowledge_center_overview.php

The Wi-Fi Alliance have provided a downloadable document which outlines the five steps to setting up your Wi-Fi network: planning, equipment selection, set up, adding Wi-Fi to computers, and security.

Vicomsoft Wireless Networking Q & A

www.vicomsoft.com/knowledge/reference/wireless1.html#2

This website provides answers to the most commonly asked questions and uses clear descriptive diagrams.

Wireless Networking Information Sheet for Schools

www.edtech.co.nz/pages.asp?MenuID=2&DeptID=24&PageID=78

The Network Services department of Edtech (New Zealand based ICT company) has provided a useful, easy to read document which explains wireless networking from a schools' perspective

Report of the Expert Group on Health Effects of Electromagnetic Fields (EMF)

www.dcmnr.gov.ie/Press+Releases/Government+Publishes+Report+of+the+Expert+Group+on+Health+Effects+of+Electromagnetic+Fields.htm

This report published in March 2007, examined a wide range of issues in relation to potential health effects of Electromagnetic Fields (EMF), including those produced by mobile telecommunications. The report answers many questions commonly raised by the public in relation to the health effects of electromagnetic fields.

Note: While the advice sheets aim to act as a guide, the inclusion of any products and company names does not imply approval by the NCTE, nor does the exclusion imply the reverse. The NCTE does not accept responsibility for any opinions, advice or recommendations on external web sites linked to the NCTE site.

This Advice Sheet and other relevant information are available at:

www.ncte.ie/ICTAdviceSupport/AdviceSheets