Wireless Local Area Networks (WLAN)

The last few years has been characterised by considerable interest, business activity and general hype surrounding Wireless technologies. The Wireless market has seen rapid expansion and considerable development with a plethora of products and a number of very similar sounding standards. This paper will focus on Wireless LAN and the issues surrounding its implementation.

What is a wireless local area network?

Before answering what a wireless LAN is, it is helpful to define both what a Local Area Network (LAN) is, and what a wired LAN is.

In its simplest form a LAN is two or more computers linked together. The LAN allows data and applications to be shared on multiple computers connected to the network. A LAN also typically allows applications and/or files to be accessed on a central server.

A wired LAN uses cabling to link together computers in a room, building, or site to form a network. With a wired LAN, computers are connected by fixed network of wires. Once in place, a wired LAN can be difficult to move and expensive to change.

A wireless LAN enables a local network of computers to exchange data or other information by radio waves and without the use of cables. It can either replace or, more usually, extend a wired LAN.

A wireless LAN is made up of two key components:

- An access point, or base station, that is usually, but not necessarily, physically connected to a LAN.
- A wireless card that is either built into or added to a computer device, be it a handheld (PDA), tablet, laptop or desktop computer.

With a wireless LAN in place, portable computers can be used on the move while remaining connected to the network. Any device with a wireless adaptor within range of an access point can potentially connect to the wireless LAN. This provides greatly increased freedom and flexibility compared to a wired network. With suitable configuration in a school environment, teachers and pupils could be enabled to access information from anywhere within the school grounds.

Extending the Wireless LAN to include additional users often only requires that the user has a Wireless enabled computer device and is in range of an access point. Increasing the overall network coverage of the Wireless LAN can often be achieved by adding further access points.

Increasingly, portable devices are being sold with wireless LAN connectivity as a standard feature. Most new laptop and tablet PC models for example have in-built wireless and this is also now included on many PDAs. As wireless becomes a standard feature on portable devices, so setting up a wireless network should become a logical progression for schools. A school which has invested in wireless enabled laptops can immediately set up wireless ad hoc networks; while the purchase of access points can permit the creation of a larger or more complex infrastructure.

Currently, Wireless LAN technology is significantly slower than wired LAN. Wireless LANs have a nominal data transfer rate of between 11 and 54 Megabits per second (Mbps) compared to most wired LANs in schools which operate at 100Mbps. Newly installed wired networks can now operate at up to 1,000Mbps (1Gb).
A wireless LAN has sufficient bandwidth to handle a wide range of applications and services. It is often quoted that some multimedia functionality may not run smoothly over wireless, for example, live unstreamed video content; however, a number of factors can affect network capabilities and this is equally true of wired networks. With wireless networks, different standards have different capabilities - this will be discussed in more detail in the section below ‘What are the standards relating to Wireless LANs’. Ongoing advances in wireless standards continue to increase the data rates achievable with new equipment.

Whilst the data rates for wireless LANs are considerably lower than for a wired LAN, it is worth considering that nominal wireless LAN speeds at 11Mbps or 54Mbps compare very favourably with broadband internet access at, for example, 2Mbps.

How does a wireless local area network work?

A wireless network can range from a very simple network of two or more computer devices in ad hoc mode to a more complex network infrastructure (basic or extended service set) with hundreds of computers on the network.

Basic and Extended Service sets

In a typical wireless LAN, a transmitter/receiver (transceiver) device, called an access point, is normally physically connected to the wired network using standard Ethernet cabling. It acts as a bridge between the wired network and the remote computer(s). At a minimum, the access point receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure, using radio frequencies to transmit data to each user. A single access point can support a small group of users, normally within a range of up to 100 metres depending on the local environment. A network with a single access point is referred to as a Basic Service Set; when two or more access points are used to extend the wireless coverage and thus permit more users, this is referred to as an Extended Service Set.

To access a wireless LAN via the access point, users need a computer device (a desktop computer, laptop, tablet PC or handheld (PDA)) with a wireless Network Interface Card (wireless NIC) either built in, or installed. Wireless NICs are available in different forms and with different interfaces. The first NICs had PCMCIA or PCI interfaces. Compact Flash 802.11b NICs are now available as are SD (Secure Digital) cards and wireless USB network adaptors. In all cases the necessary software drivers may also need installing.

Ad hoc networks

It is also possible to create an ad hoc network by joining two or more computers or computer devices together wirelessly without the need for a wireless access point. This can be done by adding a wireless NIC to each computer device if they do not already have one inbuilt. It is also possible for one of the computer devices in the ad hoc network to be joined to a LAN and to provide Internet access for the other computers in the network. These types of WLANs are particularly useful for creating small dynamic networks.

Where are WLANs being used?

2003 saw a substantial increase in uptake of wireless equipment. A recent study suggested that Worldwide wireless sales increased 40% during 2003.

The DfES ‘Survey of Information and Communications Technology in Schools 2003’ report indicated that, of the secondary schools with a network, 32% had some wireless LAN provision. For primary and special schools this figure was 12%.

In education, when wireless LANs have been deployed, schools have found that they can
• integrate ICT more effectively into teaching as lessons can be held in any classroom; teachers no longer need to ‘book’ specific time in the ICT suite to incorporate ICT into their lessons.

• allow students to work outside with a laptop for example to undertake fieldwork whilst also being able to access the school network

• take computers (and so access to the school network) to the pupils more easily than taking the pupils to the computers.

In the health service, wireless networks can and have been introduced into a number of hospitals in the UK

• in order to reduce cabling and thereby improve safety for patients

• to enable doctors and nurses to have an immediate network connection at the patient’s bedside allowing access to patient records and permitting data entry and/ or retrieval via a laptop or handheld computer.

In business, wireless LANs are quite well established as a networking technology, particularly where staff physical mobility is an issue; examples include large warehouses and the stock exchange.

In the wider community.

• Wireless networks can be used for public access to the Internet. Commercially available public access wireless networks are more commonly known as ‘hotspots’ and there are now thousands of these throughout the UK; located at railway stations, airports, hotels, in certain public libraries, in cafés and eating establishments, and at underground stations in London.

On transport

• Several airlines have in-flight WLAN availability (notably Lufthansa, Scandinavian Airlines).

• Wireless access is available on certain trains in many countries of the World. In the UK, several train operators have on board wireless services but these are usually only available to first class passengers.

What are the advantages and disadvantages of a Wireless LAN?

A Wireless LAN has some specific advantages over wired LAN:

• It is easier to add or move devices to the network

• Small dynamic ad hoc networks can be created very quickly and relatively easily.

• It is easier and quicker to provide connectivity to the network in areas where it is difficult or undesirable to lay cable or drill through walls. Instances might be:-
  o where a school is located on more than one site or is made up of several buildings.
  o when implementation is anticipated to be temporary or semi-permanent
  o when only one device is required at a remote part of a building or site
  o in historic buildings where traditional cabling would compromise the façade

• Access to the network can be from anywhere in the school within range of an access point
• Where wireless enabled laptop computers are used, any classroom in range of an access point can become a ‘computer suite’.

• While the initial investment required for wireless LAN hardware can be similar to the cost of wired LAN hardware, installation expenses can be significantly lower.

• Wireless provides increased flexibility for teachers. A teacher with a wireless enabled laptop can access the wireless network to show students work, share resources, obtain information from the internet from anywhere within the classroom. They do not need to teach from the front of the class. This flexibility is further enhanced when combined with an interactive whiteboard.

• Portability. They allow computer devices to move around the school with the pupil rather than the pupil going to a specific place to use a device. This allows for outdoor field work and work in non-classroom spaces (library, canteen, gymnasium/sports hall, playground).

Wireless LANs also have some disadvantages:

• As the number of devices using the network increases, the data transfer rate to each device will decrease accordingly – although this is equally true with wired LANs, wireless LANs usually have lower bandwidth to start with so it is more noticeable.

• As wireless standards change, it may be necessary, or at least desirable, to upgrade to higher specifications of wireless which will mean replacing wireless equipment (wireless NICs, access points etc). Currently wireless standards are more likely to change than wired standards in the near future.

• Current lower wireless bandwidth on 802.11b equipment means some activities such as video streaming will be more effective on a wired LAN.

• Security is more difficult to guarantee.

• Devices will only operate at a limited distance from an access point, with the distance determined by the standard used. Obstacles between the access point and the user, like walls, glass, water, trees and leaves can also determine the distance of operation. Poor signal reception has been experienced around reinforced concrete school buildings; these may require higher numbers of access points which in turn increases overall cost.

• In practice, a wireless LAN on its own is not a complete solution and will usually still require a wired LAN to be in place to provide a network backbone. Exceptions might be in smaller schools or for smaller networks.

• Data speeds drop as the user moves further away from the access point and may be as low as 1Mbps at the outer range of coverage.

• It is easier to make a wired network ‘future proof’ for high data transfer.

• They are not currently as reliable as wired LANs.

• As the number of people using wireless devices increases, there is the risk that certain radio frequencies used for wireless will become congested and prone to interference; particularly the 2.4GHz frequency.

What are the standards relating to Wireless LANs?

Any equipment used for a wireless LAN in the UK must be certified by the OFCOM and meet European regulations. The specifications that are currently in use, along with those that are expected to become available in the near future, are explained below.
The Institute of Electrical and Electronics Engineers (IEEE) is the leading authority in the specification and ratification of standards relating to technology. Current Wireless standards have originated from the IEEE; thus IEEE 802.11a, IEEE 802.11b etc.

In the field of wireless LAN there are currently three main standards; the 802.11a, 802.11b and 802.11g. There are also a number of other standards that are still under development, 802.11h, Hiperlan2 and Ultrawideband, as well as 802.11i which is concerned with security over wireless LAN; and 802.11e which is concerned with Quality of Service (QoS) issues. The IEEE has set up a High Throughput Working Group to develop the 802.11n standard which will look to develop higher bandwidth over wireless LAN (between 100-320Mbps).

**Current standards**

**IEEE 802.11b**

The 802.11b standard derived from the 802.11 standard, and was ratified by the IEEE in 1999. The 802.11b standard operates in the 2.4GHz spectrum and has a nominal data transfer rate of 11Mbps. In practice the actual data transmission rate is approximately 4 to 7.4-7 Mbps is adequate for accessing most data or applications including Internet access but might be insufficient for multimedia applications or for instances when a large number of simultaneous users want to access data in a single wireless LAN.

The 2.4GHz frequency is also used by other electronic devices, notably Bluetooth computer devices, domestic portable telephones and microwave ovens. 802.11b can encounter electromagnetic interference in the presence of these devices or other 802.11b equipment.

IEEE 802.11b equipment, (laptops, access points, wireless NICs etc), is still the most commonly used for establishing wireless LANs in education and business. Initially, not all 802.11b items of equipment were compatible with each other. To rectify this, an alliance of manufacturers and interested parties was set up (Wireless Ethernet Compatibility Alliance – (WECA). WECA officially changed its name to the Wi-Fi Alliance in December 2002) and a distinct Wi-Fi certification mark was established. (See picture)

In principle, any item with the Wi-Fi certification mark should be compatible with other equipment (even from other manufacturers) bearing the Wi-Fi certification mark. In practice, this may not always be the case. Newly purchased equipment should bear the Wi-Fi certification mark. If using equipment form different manufacturers, you should check for interoperability before purchasing.

The Wi-Fi mark has now been extended to the 802.11a and 802.11g standards and denotes that equipment of the same standard is compatible (though not interoperable with different standards). From August 2003, to receive Wi-Fi approval, new 802.11b and 802.11g products were required to conform to the new WPA security standard. This also applied to all 802.11a products from September 2003.

**IEEE 802.11g**

The 802.11g standard was ratified in June 2003 and the first devices to receive Wi-Fi approval were announced in July 2003. Originally intended to offer the same bandwidth as 802.11a
(54Mbps) whilst working in the same frequency range as 802.11b (2.4GHz) and with a view to be backward compatible with 802.11b, the final outcome achieves some but not all of these goals.

802.11g

- operates in the 2.4GHz spectrum so offers up to three non overlapping channels
- is backward compatible with 802.11b equipment. All Wi-Fi certified 802.11g equipment should permit the use of 802.11b equipment.
- has nominal data speeds of 54Mbps
- has actual data speeds of 10-20Mbps which drop to an actual data speed of around 10Mbps in the presence of 802.11b equipment
- uses Orthogonal Frequency Division Multiplexing (OFDM) so benefits from reduced electromagnetic interference compared to 802.11b, (though will still suffer from interference from other devices in the 2.4GHz frequency) and the higher data rates associated with OFDM.

IEEE 802.11a

The 802.11a standard was ratified by the IEEE in 1999 and adopted in the USA and other parts of the World. However, 802.11a equipment was restricted in UK and the rest of Europe because it uses the 5GHz frequency, parts of which are traditionally used by national governments for defence purposes. In the UK, a temporary user licence from the Radiocommunication Agency (now a part of Ofcom) was required to use 802.11a equipment.

The Radiocommunication Agency granted licence exemption in two of the three bands in the 5GHz spectrum. Band A (5150MHz to 5350 MHz) and Band B (5470 MHz to 5725 MHz) are open for wireless LAN services. However, this is restricted to indoor usage; 802.11a access points should not be mounted outside.

Band C at 5725 MHz to 5875 MHz has recently been made open for the installation of Fixed Wireless Access (FWA) services, especially in areas where broadband is unavailable through standard delivery platforms. (Band C is subject to certain restrictions. For further information about Band C see ‘5.8 GHz Band C Authorisation Regime’ available from Ofcom. http://www.ofcom.org.uk/licensing_numbering/radiocomms/pbr_licensing/5.8_fwa_index/5.8_auth_reg.pdf)

802.11a has nominal data speeds of 54Mbps with actual data speeds of between 25-30Mbps. 802.11a has a signal range of about 50 metres from an access point and data rates begin to drop at a range of 10-15 metres from the access point.

The 802.11a standard incorporates Orthogonal Frequency Division Multiplexing (OFDM) which is designed to be less prone to electromagnetic interference. It is suited to environments where:

- there can be a significant amount of signal reflection, such as environments with many metal surfaces
- other devices of the same standard are likely to be present (because is has greater available capacity to share. See diagram below).

The 5 GHz band provides much greater (between three to seven times as much) spectrum as the 2.4 GHz band, and 802.11a provides almost five times the data rate of 802.11b solutions. This results in 802.11a being able to deploy eight non overlapping channels in the UK compared to only three in an 802.11b/g environment. In practice, a school with an 802.11b/g solution could use a maximum of three non-interfering access points in the same area whereas an 802.11a solution can use up to eight non-interfering access points.
This means that 802.11a is better suited to environments with multiple users using applications with high data throughput. In a school environment this might be a class group using multimedia, digital video, Computer Aided Design (CAD) or databases packages.

| Maximum available shared bandwidth with 802.11b, 802.11g and 802.11a WLAN solutions |
|---------------------------------------|-------------------------------------|--------------------------------------|
| 802.11b                               | 802.11g                             | 802.11a                              |
| no individual device will exceed 11Mbps | no individual device will exceed 54Mbps | no individual device will exceed 54Mbps |
|                                      |                                      |                                      |

Some comparisons and issues relating to these standards

At present 802.11a experiences few of the signal interference and congestion problems (multiple devices using the same frequency and therefore having to share the available spectrum) experienced by 802.11b users. The 802.11a congestion problems may increase as more 802.11a equipment is used. As mentioned previously 802.11a and also 802.11g experience less electromagnetic interference because they both use OFDM which is inherently resistant to interference.

Because 802.11a operates in a different frequency to 802.11b and 802.11g, it is incompatible with them. Schools or organisations that have already deployed 802.11b networks have several choices if they want to improve their wireless data rates

- build a new 802.11a wireless LAN alongside their existing 802.11b network
- purchase new dual or tri band access points to allow for equipment with different wireless cards to co-exist
- purchase Wi-Fi approved 802.11g equipment
- find out if existing equipment can be upgraded; some manufacturers offer upgrade kits for 802.11b access points to make them 802.11g compliant. There are also companies who offer proprietary solutions when all devices on the network are the same to enable 802.11b equipment to receive a nominal 22Mbps.

Schools, whether upgrading or deploying a wireless solution for the first time, should consider

- Who will be using the WLAN and how will it be used? Is it primarily aimed at a small number of people being able to move around a site with wireless equipment connected to the network; or will there be a higher numbers of people wanting to use high data throughput applications. In the first case, a 802.11b/g solution may be adequate, in the second an 802.11a solution may be more appropriate.
- For what purpose will the WLAN be used? If it is to permit an entire site to be wirelessly enabled, an 802.11b/g solution may be cheaper, and provide better coverage. In general
both 802.11b and 802.11g (as they work in the 2.4GHz frequency) have greater range, theoretically up to 100 metres from an access point; while 802.11a has a theoretical range of about 50 metres but only has optimum range at between 10-15 metres from the access point. In practice, to obtain the same network coverage, the user may require up to four times as many access points when using an 802.11a network. This may be more expensive as not only do you require more access points, but 802.11a access points are still currently more expensive than both 802.11b and 802.11g access points.

- The 802.11g is effectively an upgrade to the 802.11b specification; 802.11b equipment should begin to drop in price as 802.11g becomes more widely adopted. As 802.11g is backward compatible with 802.11b devices, it may be that in the longer term, manufacturers will stop producing 802.11b only devices (though analysts currently forecast that 802.11b equipment will continue to out sell 802.11g or a equipment for at least the next three years).

- Manufacturers now provide, dual mode and tri-mode equipment (access points, NICs) which support both 802.11a and 802.11b and 802.11a/b/g respectively. Whilst more expensive, this does provide considerable flexibility.

- Most new notebook, laptop and tablet PCs ship with wireless connectivity as standard. Schools should consider this when purchasing new equipment and ensure that it is compatible with their existing wireless set up. For schools without wireless provision, purchasing new computers with wireless connectivity might be a good opportunity to consider trialling a wireless network.

- There is a belief that the 2.4GHz frequency will become cluttered in the long term as it only has a small spectrum (compared to the 5GHz bands). With the widespread adoption of 802.11b and as equipment, like higher powered Bluetooth devices come onto the market, there is the risk that long term, the 2.4GHz frequency will become unreliable.

- If schools want to run a mixed 802.11b/g network there are a couple of issues relating to data rates, notably that the actual data rates for 802.11g devices drop in the presence of 802.11b equipment.

  If 802.11g devices and a 802.11b devices are in dialogue with each other then the data rates will be dictated by the 802.11b device.

  If two or more 802.11g devices are in dialogue with each other but there are 802.11b devices in the same network, then 802.11g data rates will drop but may well still be more than the practical rates of 802.11b.

  There are 802.11g access points, or dual or tri-band access point incorporating 802.11g which can be set to only recognise 802.11g equipment. This obviously prevents the 802.11b equipment from working on the 802.11g network but there are times when this may be desirable.

Future standards

IEE 802.11h
This is a modification of 802.11a being developed to comply with European regulations governing the 5GHz frequency. 802.11h includes Transmit Power Control (TPC) to limit transmission power and Dynamic Frequency Selection (DFS) to protect sensitive frequencies. These changes protect security of military and satellite radar networks sharing some of this spectrum.

As 802.11h needs to implement DFS in Europe it means that the technology involved is more complex which will make it expensive in the short term.

Hiperlan2
The European Telecommunications Standards Institute (ETSI) has developed High Performance Radio Local Area Network Type 2 (Hiperlan2). It was developed to operate in the 5GHz band at
54Mbps, a data rate similar to 802.11a and g. The future for Hiperlan2 is uncertain especially if the 802.11h standard is widely adopted.

**IEEE 802.11e**

This proposed standard aims to improve the QoS (Quality of Service) of wireless networks. 802.11e proposes that information packets to be sent over a wireless connection are categorised as one of eight traffic categories and prioritised accordingly. Voice, audio and video data will be given a higher priority (as it is important that the data stream arrives un-interrupted, in the correct order and within the correct time frame) than other forms of data (eg email, text documents). This prioritisation will help improve the transmission quality of video, audio and voice over wireless networks.

All 802.11e certified products are expected to be backward compatible with existing 802.11 wireless LAN products (a, b and g). It should be possible to upgrade existing 802.11 access points to comply with 802.11e through relatively simple firmware upgrades once they are available. Final ratification was due in late 2003 but has been delayed and there is no current date for final ratification. The first manufacturers began to ship products based on the draft specification of the 802.11e standard in December 2003. Schools should exercise caution when purchasing draft specification equipment as the standard may change before final ratification.

**802.16 and WiMAX**

An emerging group of standards which may impact on Wireless LAN deployment in the future is the IEEE 802.16 family of standards relating to broadband wireless. The original 802.16 standard specified fixed point-to-multipoint broadband wireless systems operating in the 10-66 GHz licensed spectrum. An amendment, 802.16a, approved in January 2003, specified non-line-of-sight extensions in the 2-11 GHz spectrum. The 802.16a standard will be capable of nominal speeds up to 70Mbps at distances of up to 25 miles; operating in the 5.8GHz band, under light licensing arrangements from Ofcom.

802.16 standards are expected to complement 802.11 (Wireless LAN standards) by enabling a wireless broadband alternative, connecting offices to each other and the Internet. Although the first amendments to the standard are only for fixed wireless connections, a further amendment, 802.16e, is expected to enable connections for portable and mobile devices. This may lead it to become a competitor to 802.11 rather than complementary.

The WiMAX group comprises wireless industry companies such as Alvarion, Proxim, Fujitsu, Intel, Nokia, Airspan and others who advised on the 802.16 standard. The group aims to promote and certify compatibility and interoperability of devices based on the 802.16 specification.

**Wireless Personal Area Networks (WPANs)**

There are a number of other wireless technologies which are used over a short distance (usually up to about 10 metres) to connect devices to each other. As such networks are based on the immediate area around the individual user; they are called Wireless Personal Area Networks. Examples of WPAN technologies are Bluetooth, Ultrawideband and Infrared. For more detailed information see the Becta technical paper Personal Area Networks (PANs) – January 2004. [www.becta.org.uk/technicalpapers](http://www.becta.org.uk/technicalpapers)

**Bluetooth**

This is a low-cost radio solution that can provide links between devices. Originally, and more typically the range of these devices is up to 10 metres. Newer Bluetooth devices are coming on to the market with a range of up to 100 metres. Bluetooth has access speeds of up to 780 Kbps; considerably slower than the various 802.11 Wireless LAN standards. Bluetooth technology is embedded in a wide range of devices, eg mobile phones, printers, video cameras, computer mice and keyboards etc. Within a school environment, it would be useful in the classroom over short distances.
Bluetooth, as a Wireless Personal Area Network (WPAN), should not be confused with 802.11 wireless as it is not intended to do the same job. Bluetooth is primarily used as a wireless replacement for a cable to connect devices assuming they are configured to share data. Although Bluetooth was not originally intended to be used for 802.11 wireless networking, it is now possible to buy access points for Bluetooth LAN and combined 802.11b/Bluetooth access points. The Bluetooth standard is relatively complex and it is therefore not always easy to determine if any two devices will communicate. Any devices should be seen to communicate successfully before purchasing.

Bluetooth operates in the 2.4GHz band so can cause interference with Wireless LAN (802.11b and 802.11g) equipment. Bluetooth Version 2 is currently in development and should see data rates increased to 10Mbps. Version 2 is expected some time in 2004.

**Ultrawideband**

UWB is a high-bandwidth (100Mbps and up), and initially, a short-range (less than 10 metres) specification for wireless connection designed to connect computers, or computers and consumer-electronics devices such as handhelds and digital cameras, with the potential to become a high-bandwidth connection. There is some uncertainty whether UWB equipment will become commercially available.

**NB.** A table of side by side comparisons of the various wireless standards is shown below

**How the standards compare**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Nominal Data Rate</th>
<th>Actual Data Rate</th>
<th>Typical Range</th>
<th>Frequency</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>11Mbps</td>
<td>4-7Mbps</td>
<td>Up to 100m</td>
<td>2.4GHz</td>
<td>Currently available for use without licence in the UK.</td>
</tr>
<tr>
<td>802.11g</td>
<td>54Mbps</td>
<td>10-20Mbps</td>
<td>Up to 100m</td>
<td>2.4GHz</td>
<td>Currently available for use without licence in the UK. An extension of 802.11b. Uses the same encoding technology as 802.11a (OFDM), increasing the data rate. Is backward compatible with 802.11b</td>
</tr>
<tr>
<td>802.11a</td>
<td>54Mbps</td>
<td>27-30Mbps</td>
<td>Up to 60m</td>
<td>5GHz</td>
<td>Currently available for use without licence in the UK.</td>
</tr>
<tr>
<td>802.11h</td>
<td>54Mbps</td>
<td>27-30Mbps</td>
<td>Up to 60m</td>
<td>5GHz</td>
<td>A modification of 802.11a being developed to comply with European regulations governing the 5GHz frequency. Protects security of military and satellite radar networks sharing some of this waveband. Includes transmit power control (TPC) to limit transmission power and dynamic frequency selection (DFS) to protect the sensitive frequencies.</td>
</tr>
<tr>
<td>Hiperlan2</td>
<td>54Mbps</td>
<td>42Mbps</td>
<td>Up to 100m</td>
<td>5GHz</td>
<td>Uncertain future due to widespread adoption of 802.11a as a world standard. The Hiperlan2 project, lead by the ETSI organisation is/ was an attempt to create a European standard in the 5GHz range.</td>
</tr>
<tr>
<td>Bluetooth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Used to replace cables for transferring data over a short distance between, for example, handheld devices, computers and printers.</td>
</tr>
<tr>
<td>Version 1</td>
<td>1 Mbps</td>
<td>780Kbps</td>
<td>Up to 10m</td>
<td>2.4GHz</td>
<td></td>
</tr>
<tr>
<td>Version 2</td>
<td>10Mbps</td>
<td></td>
<td>Up to 100m</td>
<td>2.4GHz</td>
<td>Expected 2004</td>
</tr>
<tr>
<td>Ultrawideband (UWB)</td>
<td>100Mbps+</td>
<td>n/a</td>
<td>Initially up to 10m</td>
<td>Initially 3-6GHz</td>
<td>Not expected on the market before 2005.</td>
</tr>
</tbody>
</table>
What issues should I consider when buying a Wireless LAN?

**Security**

Wireless LAN security has been widely publicised and remains a contentious issue.

Originally, Wireless LAN equipment shipped with a security mechanism called Wireless Equivalent Privacy (WEP), which was often not activated as a default. When activated, WEP provided a certain level of security which would deter most computer hackers. However, WEP is now considered insecure.

An interim solution called Wi-Fi Protected Access (WPA) has been introduced by the Wi-Fi Alliance. WPA is a subset of the forthcoming IEEE 802.11i Security Standard for Wireless LAN and is regarded as very secure.

In many cases, equipment bought with WEP security can be upgraded to WPA with a software upgrade.

From August 2003, to receive Wi-Fi approval, new 802.11b and 802.11g products were required to conform to the new WPA security standard. This also applied to all 802.11a products from September 2003.

WPA incorporates features of the future 802.11i standard. WPA runs in either enterprise mode or pre-shared key (PSK) mode:
- **Enterprise Mode** requires an authentication server using RADIUS protocol for authentication and dynamic key distribution
- **Pre-Shared Key Mode** does not require an authentication server. A shared key is entered once on the access point and the wireless client, to act as a starting point for the dynamic encryption process.

WPA is deemed by the industry to be very secure despite being an interim solution. It should be noted though that WPA offers no support for devices in ad hoc mode. For encryption to take place in this mode WEP will still need to be used. Schools can maximise the security of their wireless networks in a number of other ways which will be discussed in more detail in the ‘What are the implementation issues?’ section below.

**802.11i**
The 802.11i security standard ratification – June 2004) provides a very secure mechanism for wireless networks; it incorporates:

- a more secure security encryption protocol called Temporal Key Integrity Protocol (TKIP)
- 802.1x authentication (the same authentication used on many wired LANs)
- Advanced Encryption Standard (AES). For technical information on AES see reference section

To upgrade to 802.11i, current wireless users will need to replace their existing access points as it will not be possible to offer access point software upgrades. There are already access points on the market which incorporate 802.11i security based on the draft specification of the 802.11i standard. It is recommended to buy equipment which adheres to the ratified standard as there may be differences between the draft and final specifications.

**Performance**

It is important to remember that transmission speeds for all wireless LANs vary with file size, number of users and distance from the access point.
As the distance from the access point increases, the nominal data rate for 802.11a and 802.11g standard equipment drops from 54Mbps to 48, 36, 24, 18, 12, 9, or 6 Mbps.

802.11b standard equipment drops from 11Mbps to 5.5Mps, 2Mbps or 1Mbps.

Although 802.11b and 802.11g access point can potentially be accessed from up to 350 metres away outdoors, this is very much reduced indoors, the maximum distance attainable in ideal conditions being about 100m.

The performance of each standard varies considerably depending on the number of users, the local environment and any obstructions that are in the way. Buildings with many girders, thick walls, and concrete will often shorten the effective range and there may be areas that are effectively 'dead zones'. Water, glass and paper can also reduce a network’s range.

It is possible that there may be issues of interference when using an 802.11b wireless LAN and where there are devices with Bluetooth connectivity such as handhelds and cordless phones in the same area. Reports by the Spectrum Management Advisory Group (SMAG) suggest the issue is a minor one, but it should be considered when discussing the site survey.

**Prices**
The costs for 802.11b wireless equipment typically range from about £50 to £350 for an 802.11b wireless LAN access point. The cost of a wireless card for a laptop or handheld computer starts at about £25 with average costs of around £55.

Prices for 802.11a equipment are generally more expensive than 802.11b equipment, with access points starting at around £130 and wireless cards starting at about £50 although 802.11a Wireless cards have significantly dropped in price in the last six months.

Prices for 802.11g equipment were initially on a par with 802.11a. There has been a tendency for 802.11g equipment to be dual (802.11b/g) or tri band (802.11a/b/g). Chip sets in computer laptops have moved towards a tri band model. Dual 802.11a/b dual access points are available from about £200 and tri band prices start at not much more.

The cost of access points depends on the quality and on built-in functionality, and includes:

- the quality of the antennae
- antennae directionality
- encryption included in the access point
- whether the access point has DHCP (Dynamic Host Configuration Protocol – allows automatic assignment of IP addresses to new devices on the network) built in
- DSL access (which allows internet access direct from the access point) this is designed for small home network or small business use
- the number of user devices that can be listed in the Access Control Lists; is the number limited and if so is it sufficient for your network?
- the ability to centralise the control and management of access points over the network
- whether the access point can act as a bridge between other access points and the network.

**Interoperability**
Purchasing Wi-Fi certified products *should* ensure that Wireless equipment is interoperable between products of the same standard (or where products are clearly sold as dual or tri mode). Where possible, it is strongly recommended that equipment is demonstrated to interoperate.
What are the implementation issues?

Planning
To determine the location of access points for Extended Service Sets, it is essential that a site survey is undertaken by a specialist in this area. A site survey will also determine the number of access points required to give the desired coverage, the range of each access point, and its channel designation. The access point, or the antenna attached to the access point, will usually be mounted high in a classroom. However, an access point may be mounted anywhere that is practical as long as the desired radio coverage is obtained. Larger spaces generally require more access points.

Before a site survey is undertaken, it is advisable to prepare a floor plan to show where coverage is required. Precise details should be sought from suppliers of ‘network coverage’ and ‘data transfer rates’ particularly towards the edge of the coverage area. You should specify the level of coverage you require, a supplier’s definition may be as low as 1Mbps. It is also a good idea, if possible, to ensure that the site survey is carried out with the equipment anticipated to be used in the school. It is also important that technical school staff assist with the site survey. There may be a charge for the site survey but the supplier will often refund this if the equipment is then purchased from them.

For schools upgrading, or adding to, an existing 802.11b wireless network, a further site survey may be required since the coverage is likely to be different when compared to 802.11b. More access points may be required to maintain or improve data rates.

Capacity
Planning a wireless LAN should take into account the maximum number of people who will be using wireless devices in the range of any access point. The recommended maximum number of devices simultaneously accessing each access point is 15 to 20 depending on the type of use and the standard of the equipment. Where light usage of the network occurs, such as with web browsing or accessing applications that require little exchange of data, this could rise to around 30 users, with some manufacturers suggesting their access points can support up to 250 simultaneous users. It is relatively easy to scale wireless LANs by adding more access points, but for an 802.11b or 802.11g network no more than three access points may operate in any one coverage area owing to frequency congestion. An 802.11a network can operate up to eight access points in one area, each using a different channel.

Network Management
Schools will need to allocate resources for network management in the same way as they would for a wired network. Tasks such as configuring MAC and IP addresses, monitoring network performance, upgrading access points and generally ensuring system integrity, will need to be undertaken on a relatively regular basis.

Security
Anyone with a compatible wireless device can detect the presence of a wireless LAN, however if appropriate security mechanisms are put in place, this does not mean that they can access any data.

The wireless LAN should be configured so that anyone trying to access the wireless LAN has at least the same access restrictions as they would if they sat down at a wired network workstation. All the suggestions below are practical steps that schools can put in place to improve wireless LAN security.

A school can
• ensure that the devices with WEP security are upgraded to WPA where possible and that the encryption is enabled. WPA provides a high level of security for a wireless network. If an upgrade to WPA is not possible, schools should ensure that WEP is enabled.

• restrict access to the Wireless network by only permitting devices with a recognised MAC (Media Access Control) address. Every computer has an individual alphanumeric identifier known as a MAC address. Within the software accompanying the access point, there is an Access Control List, which as its name suggests, controls access to the network. The access point can be configured to only permit recognised devices. This only gives an additional layer of security to the network, it is not a secure solution in itself.

• incorporate a Virtual Private Network (VPN). A VPN is a secure private network that uses a public network like the Internet to connect remote sites or users together. Anyone wishing to access files on the WLAN would first need to log on to the network via the VPN using a User name and Password. Data sent between the client device and the network is secure as it is encrypted / decrypted using VPN encryption (for further information on VPNs see the Becta technical paper ‘Virtual Private Networks’ www.becta.org.uk/technicalpapers). Most VPN solutions entail installing VPN software on the client devices. A VPN for wireless would provide a relatively high level of security for a school. Users would need to ensure they use sensible (ie not obvious) Password and Log-on details otherwise this level is security is easily compromised.

• change the default Service Set Identifier (SSID or network name) and passwords. (SSID is the method wireless networks use to identify or name an individual wireless LAN.) Access points may be set to broadcast the SSID, this should be turned off where possible. This only adds an additional layer of security and is not a solution in itself. On access points where this is not possible, the network name can be made less recognisable by including non alphanumeric characters (like _*# etc).

• avoid wireless accessibility outside buildings where it is not required; directional aerials can be obtained to restrict the signal to 180° or 90° from the access point.

• switch off the power to the access point(s) ‘out of hours’ makes the wireless LAN unavailable at those times.

• make sure that the network is regularly checked to ensure that only legitimate wireless access points are connected to the network.

• put the Wireless LAN into its own DMZ so that all Wireless nodes pass though a firewall to access the educational network.

• The security measures a school would consider for a standard LAN implementation can also be incorporated in to a WLAN (eg installing a firewall, using a DMZ, administrator file restrictions etc)

More detailed technical information on how the different security protocols work can be found in the security references at the end of this paper.
Power Consumption
Wireless cards typically have a number of different settings related to their power usage. For example, ‘standby mode’, where the transmission of data occurs only when required, uses relatively little power and leads to improved battery performance. Wireless cards that have recently come on to the market tend to consume less power, and this trend is expected to continue as newer generations of cards become available.

Power over Ethernet
Access points require a power supply in addition to a wired network connection. Access points are often sited high on walls and away from existing power outlets. There are products on the market that will supply power to the access point via the network cable, removing the need to install additional power cabling.

Safety issues
For information on safety issues regarding wireless equipment, contact the National Radiological Protection Board (NRPB) (http://www.nrpb.gov.uk) or OFCOM (www.ofcom.org.uk).

Other sources of information

Becta
Becta’s Expert Technology Seminars - Wireless Networking for Education
A series of presentations given at Becta’s Expert Technology Seminar in February 2003
http://www.becta.org.uk/etseminars_presentations/index.cfm?seminar_id=1&id=2608

Becta/TC Trust Wireless Networks Project
http://www.becta.org.uk/leaders_leaders.cfm?section=3_2&id=396

Useful links

Case studies (wireless technologies in education)

Apple case studies
http://www.apple.com/uk/education/airport/

Bradford LEA ICT Team Wireless LAN Case Study
http://www.ergo.co.uk/bradford_wireless_lan.html

Microsoft Education case studies
http://www.microsoft.com/uk/education/products-education/case-studies/default.asp

The Cornwallis School. Presentation at Becta Expert Technology Seminar June 2003
http://www.becta.org.uk/etseminars_presentations/presentation.cfm?seminar_id=13&section=7_1&presentation_id=19&id=2608

News
CNET Communications News

Wi-Fi net news
http://wifinetnews.com

Wireless Week
http://www.wirelessweek.com

802.11 Planet
(for background and current information on 802.11 Wireless LANs)
http://www.80211-planet.com/tutorials
http://www.80211-news.com/

**Security**

‘Wi-Fi Protected Access. Strong standards based, interoperable security for today’s Wi-Fi Networks’ Paper from the Wi-Fi Alliance
http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf - April 2003

‘Securing Wi-Fi Wireless Networks with Today's Technologies’ Paper from the Wi-Fi Alliance
http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Networks2-6-03.pdf - February 2003

General question and answers from Wi-Fi alliance

Advanced Encryption Standard (AES)


A 60-minute Web cast regarding WPA and the Wi-Fi Alliance’s response to the need for improved WLAN security was held on 11 June 2003. Follow the link from
http://www.wi-fi.org/OpenSection/protected_access.asp

‘Wi-Fi Security’, Paper from Toshiba

**Standards, compatibility and safety issues**

Communications Electronics Security Group (CESG)
http://www.cesg.gov.uk

European Telecommunications Standards Institute
http://www.etsi.org/

Institute of Electrical and Electronics Engineers (IEEE) Wireless Standards Zone
http://standards.ieee.org/wireless

National Radiological Protection Board (NRPB)
http://www.nrpb.gov.uk

OFCOM
http://www.ofcom.org.uk

Wi-Fi Alliance (formerly Wireless Ethernet Compatibility Alliance (WECA))
http://www.wi-fi.org
Technical

5.8 GHz Band C Authorisation Regime – OFCOM
http://www.ofcom.org.uk/licensing_numbering/radiocomms/pbr_licensing/5.8_fwa_index/5.8_auth_reg.pdf

Wireless Networking in Schools (Australia)

http://mosquito.net.stanford.edu/software/802.11e/ipc84.pdf

‘802.11e brings QoS to WLANs’. Online article. Computerworld Malaysia. Aug 2003