Wireless Networking Brief

Produced By:	John Chapman
Reviewed By:	Leonard Veenendaal
Service:	Education ICT
Date:	19th May 2005
Version	2.1

Cambridgeshire County Council
Children & Young People's Services

Education ICT Service

SIMS Accredited Support

QA naace Consultancy for ICT Development Planning

Table of Contents

Executive Summary

This paper is intended for school leaders who are investigating the possibility of extending or complementing their Local Area Network (LAN) using Wireless LAN (WLAN) technology.

Information has been taken from BECTA quite extensively throughout this document, as they are the Government's leading agency for ICT in Education.

Many education establishments are now starting to reap the many benefits of wireless networking technologies. Standards are however changing rapidly, with new equipment being brought out with alarming regularity. It is important therefore to consider the options carefully.

ICT Service can help you ensure the investment you make in this technology is future-proofed as far as possible by ensuring adherence to standards.

Benefits	Drawbacks
• No more cables to drag around with you • Move from classroom to classroom whilst still being connected to the network, without having to take cables with you • Work outside, retaining your network connection	• Somewhat slower than cabled network connection • Needs adequate security mechanisms • Needs to be properly planned and installed

Introduction

Wireless systems are becoming more and more popular; standards are rapidly being ratified, new standards are being introduced, and prices are slowly coming down. There are a number areas to consider, and we as a ICT Support provider recommend you invest in a site survey by a professional, external consultant; the cost of this will be refunded provided you:

a) Purchase equipment and installation through ICT Service
b) Have a survey carried out by one of our recommended partners

Our procurement team at Waterbeach are able to assist in getting a survey carried out. Contact details may be found in Appendix D.

Remember your fixed, wired network is likely to perform at speeds of 100 Mb/s, a leased line Internet connection (i.e. Broadband/CCN) will perform (initially) at 2Mb/s, and a Wireless LAN can perform at up to between 11Mb/s and 54Mb/s.

Wireless hardware vendors may promise extended range or increased bandwidth, above and beyond the standards listed in this document. Purchasing such equipment will effectively tie you in to a specific vendor, as the equipment will not be interoperable.

What is a Wireless LAN?

A Local Area Network (LAN) links computers in a building, or across a school, office or campus. The LAN allows data and applications to be shared on multiple computers. A LAN also allows applications and/or files to be accessed on a central server via wired or wireless connections. With a wired LAN, computers are connected by a solid and fixed network of wires. It can be difficult to move and expensive to change.

A wireless LAN enables a local network of computers to exchange data or other information without the use of cables. It can either replace or extend a wired LAN, and data can be transmitted through the air, through walls, ceilings and even cement structures, without wired cabling. With a wireless LAN in place, laptop or handheld computers may be carried from place to place while remaining connected. Any device 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.

A wireless LAN is made up of two key components:

a) An access point, or base station, that is usually physically connected to a LAN
b) A wireless card that is either built into or added to a handheld, laptop or desktop computer.

With a wireless LAN, additional users and access points can be added as necessary. Students and teachers can stay connected as they move throughout the school and, depending on how it is configured, access information anywhere in the school or in the school grounds.

The most common wireless standard, 802.11b, has a data transfer rate of 11 Megabits per second (Mbps) - much slower than current wired LANs, which operate at 100Mbps. Newly-installed wired networks now operate at up to 1,000Mbps (1Gb). 802.11b devices are often branded with a WiFi mark to indicate interoperability.

A wireless LAN has sufficient bandwidth to handle a wide range of applications and services. However, it has a limited ability to deliver multimedia applications at sufficient quality and a wired LAN is probably needed to access these. The 802.11g (54Mb/s) standard has recently been ratified. This describes wireless equipment running in the 2.4 GHz radio spectrum, making it backwards compatible with 802.11b (11Mb/s).

A WLAN has some specific advantages:

- It is easier to add or move workstations
- It is easier to provide connectivity in areas where it is difficult to lay cable
- Installation can be fast and easy and can eliminate the need to pull cable through walls and ceilings
- Access to the network can be from anywhere in the school within range of an access point
- Portable or semi-permanent buildings can be connected using a wireless LAN
- Where laptops are used, the ‘computer suite’ can be moved from classroom to classroom on mobile carts
- 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
- Where a school is located on more than one site (such as on two sides of a road), it is possible with directional antennae, to avoid digging trenches under roads to connect the sites
- In historic buildings where traditional cabling would compromise the façade, a wireless LAN can avoid drilling holes in walls

- Long-term cost benefits can be found in dynamic environments requiring frequent moves and changes
- They allow the possibility of individual pupil allocation of wireless devices that move around the school with the pupil.

WLANs also have some disadvantages:

- As the number of computers using the network increases, the data transfer rate to each computer will decrease accordingly
- As standards change, it may be necessary to replace wireless cards and/or access points
- Lower wireless bandwidth means some applications such as video streaming will be more effective on a wired LAN
- Security is more difficult to guarantee, and requires configuration
- Devices will only operate at a limited distance from an access point, with the distance determined by the standard used and buildings and other obstacles between the access point and the user
- A wired LAN is most likely to be required to provide a backbone to the wireless LAN; a wireless LAN should be a supplement to a wired LAN and not a complete solution
- Long-term cost benefits are harder to achieve in static environments that require few moves and changes
- It is easier to make a wired network 'future proof' for high data transfer.

Speed

The most common wireless standard, 802.11b, has a data transfer rate of 11 megabits per second (Mbps), much slower than current wired LANs, which operate at 100Mbps. Newly installed wired networks now operate at 1000Mbps (1Gb).

With a wireless LAN, bandwidth is sufficient to allow the use of a wide range of applications and services. However, it has a limited ability to deliver multimedia applications at sufficient quality, and a wired LAN is likely to be necessary to access these.

Benefits	Drawbacks
• No more cables to drag around with you • Move from classroom to classroom whilst still being connected to the network, without having to take cables with you • Work outside, retaining your network connection	• Somewhat slower than cabled network connection • Needs adequate security mechanisms • Needs to be properly planned and installed

Security

Bearing in mind a wireless network has no wires, and transmits data over radio, it should be obvious that there is a big security issue here. Setting up a WLAN without any security essentially means any passer-by with a wireless card in their laptop can "steal" your bandwidth, and use it to browse the web, download email etc. A more experienced "hacker" could then set about gaining access to your data.

It is therefore important to understand some of the security mechanisms available for wireless equipment.

Wired Equivalent Privacy (WEP)

WEP provides one level of security. It can be either a 64 or 128-bit key entered onto your Access Points and Wireless Cards to slow down an attacker. Tools are however readily available for download from the Internet which will allow a serious hacker to gain full access to your network within 24 hours.

Extensible authentication protocol (EAP)

EAP changes the WEP key at regular time intervals so that even if someone is able to break the code and determine the key, it will be changed by the time they try to use it. A cracker who is able to intercept an encrypted signal for the length of time it takes to crack the code could break though this system by recording and decoding each key as it is used. Someone using the network would have to be connected and using the network for the full amount of time it takes to break the code.

Media Access Control (MAC) Authentication

The MAC address is the unique hardware address burnt onto every network card installed in your PCs and laptops. Although this can be changed, you can add another layer of security by limiting the PCs that can use the device by listing authorised MAC addresses.

Standards and Certification

There are a number of standards ratified by the Institute of Electrical and Electronics Engineers (IEEE) Task Group. Certification by IEEE is important to users as it means products that have passed interoperability tests are compatible with one another.

802.11a

Transmits in the 5 GHz band
This standard faces regulatory problems outside the USA due to the existence of legacy systems. This is not compatible with either 802.11b or the new 802.11g standards.

The maximum rate for 802.11a (54M bits/sec.) is much faster than 802.11b (11M bits/sec.) But speed and distance are inversely related. It is likely that 802.11a throughput will drop to around 21Mb/sec. at 65 feet. However, that's still 4 times faster than 802.11b under similar conditions.

802.11b

Transmits in the 2.5 GHz band
This is certified for use worldwide
802.11b has an edge when it comes to maturity, per-station pricing, availability, and interoperability. Over 500 802.11b products have been certified by the Wi-Fi Alliance since March 2000. By mid-January 2003, just seven 802.11a products were Wi-Fi certified.

A single radio cannot support 802.11a and 802.11b simultaneously, so migrating from b to a requires hardware upgrade. Even if you're starting a new WLAN, many laptops and PDAs exist with embedded 802.11b. These "legacy" stations will be around for a while.

802.11g

The IEEE standards board has also approved 802.11g, which will most likely replace 802.11b. 802.11g allows the same speed as the 802.11a (54Mbps), but operates in the 2.4GHz waveband. This is interoperable with 802.11b, but not 802.11a

802.1x

This is a new security standard which allows the Wireless network to be hardened by the use of external authentication servers (RADIUS). This is an additional level of security for your WLAN.

On the horizon

As if having the 802.11a, 802.11b, and 802.11g wireless specifications weren't confusing enough, there is yet another variation that should be finalised soon: IEEE 802.11e. This specification is the first wireless standard to support both home and business applications, and incorporates multimedia support to the existing 802.11a and 802.11b wireless standards. This standard adds Quality of Service (QoS) features to provide channel robustness and an improved way to manage time-sensitive traffic for multimedia applications.

There are other new development standards in the works, including:

802.11i will offer a new version of the Wired Equivalent Privacy (WEP) security protocol that uses a 128-bit key instead of the 40-bit key currently in use.
802.1x will offer port-based network access control for the entire range of 802 technologies.

Performance

Although the standards listed above ratify the bandwidth of wireless devices as being either 11Mb/s or 54Mb/s, the real life scenario will probably see you achieve around 50% of that performance.

Keep in mind the following questions when considering a WLAN:

How many of your users require mobility, and where do they need to go?
What user applications will run over the WLAN?

Think where you are going to mount your Wireless access points; remember they need power and a physical network connection. If you are mounting on the ceiling, think about going for a unit that provides power over CAT5 Ethernet, removing the need for a separate power supply.

Remember also that Wireless is a shared medium; meaning if you have a single 802.11b Wireless access point, and 5 clients, they all share the maximum possible bandwidth of 11Mb/s.

What distances need to be covered?

Access points offer clients multiple data rates for the wireless link. For 802.11b, the range is from 1 to 11 Mbps in four increments, while for 802.11a the range is 6 to 54 Mbps in seven increments. The client cards will automatically switch to the fastest possible rate of the access point; how this is done varies from vendor to vendor. Because each data rate has a unique cell of coverage (the higher the data rate, the

smaller the cell), the minimum data rate for any given cell must be determined at the design stage.

While the size of the coverage area is the most important determining factor for antenna selection and placement, it isn't the sole criterion. Building construction, ceiling height, internal obstructions, available mounting locations, and physical aesthetics all must be considered.
Cement and steel construction have different radio propagation characteristics and are therefore factors when determining antenna strength. Internal obstructions, such as product inventory and racking in warehouse environments, are also factors. For example, any product with high-water content will absorb 2.4-GHz RF energy. In a warehouse, shelves stacked with paper or cardboard products can, due to their high water content, create RF "shadows" or dead spots.

Configuration Guidelines

This section is intended for technicians involved in configuring wireless access points (AP) and associated cards in schools. Decisions regarding the physical location of APs should already have been made during the Wireless survey that Education ICT Service, or our current cabling supplier, has carried out

This section is not intended to provide an exhaustive list of configuration settings for every AP you are likely to come across, instead it is a generic guide to enable you to follow recommended standards of installation to help ensure a secure and stable wireless network.

Remember that a wireless network should Compliment The Wired Infrastructure. Where possible, the use of a wired connection is preferred because it is faster and it does not compete with other wireless stations (clients) for bandwidth.

Device Naming

The following device naming conventions should be used:

AP_*DfeSNumber.number*

So for example, the 3rd AP at Godmanchester Primary School would be:

AP_2209.3

Network Settings

Ensure you disable DHCP on the device
Also check that any settings permitting the AP to hand out IP addresses is also disabled.
Enter the Default Gateway IP address
Enter the relevant DNS server settings

Encryption

Ensure you configure 128-bit Encryption with a specified shared key.

Channels

The radio frequency channels used in 802.11b/g networks are listed below:

Channel	1	2399.5 MHz	–	2424.5 MHz
Channel	2	2404.5 MHz	–	2429.5 MHz
Channel	3	2409.5 MHz	–	2434.5 MHz
Channel	4	2414.5 MHz	–	2439.5 MHz
Channel	5	2419.5 MHz	–	2444.5 MHz
Channel	6	2424.5 MHz	–	2449.5 MHz
Channel	7	2429.5 MHz	–	2454.5 MHz
Channel	8	2434.5 MHz	–	2459.5 MHz
Channel	9	2439.5 MHz	–	2464.5 MHz
Channel	10	2444.5 MHz	–	2469.5 MHz
Channel	11	2449.5 MHz	–	2474.5 MHz
Channel	12	2454.5 MHz	–	2479.5 MHz
Channel	13	2459.5 MHz	–	2484.5 MHz

Note: All the above channels are supported in Europe. **It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.**

Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

SSID

The SSID should again contribute to the security of the WLAN infrastructure, and therefore should not be easily guessed by any passing unauthorised laptop user.

Enter a Network Name of "DfEsNumber_ Wireless" (note the single space before "Wireless").

DO NOT select Create a closed network. Select a Channel frequency suitable as per the above list.

Disable Broadcasting of SSID/ESSID

Administration

Protect the base station (access point) with a suitably complex password (not blanks or the default password)

Pass DHCP to the network (no NAT or IP address distribution)

Enter the DNS name, technical contact person's name, and physical location of the AP.

Appendix A - A Checklist

To what standards are your products certified?
The standards to consider are:

IEE 802.11a – not compatible with any other standard
IEEE 802.11b
IEEE 802.11g

Security

Is 128-bit WEP supported?
Is EAP supported?
Can SSID broadcast be turned off?
It is possible to restrict access by MAC address?

Performance

How many simultaneous client connections are you likely to need?
What type of traffic is likely to pass over the wireless network?
How many simultaneous wireless connections can the Access Point support?
How is performance affected by addition of more laptops/PC's accessing the access point?
How is growth in the numbers of PCs accessing the network via wireless handled/planned for?
How will you test performance within the school?
Are there other Wireless networks in your area?
What is the maximum distance that needs to be covered?
Where are you going to mount the Access Points?
Is power available?
Is a CAT5 Ethernet point available?

Future Proofing

Does the solution provide a migration path to the evolving IEEE 802.11 standard and other emerging radio technologies?
Is the equipment modular, allowing easy upgrades?

Support

What Warranty is provided?
What extended warranty may be purchased?

Appendix B - Advice

http://www.wirelessweek.com/

http://computer.howstuffworks.com/wireless-network.htm

Appendix D - ELH ICT Service Contacts

ICT Service Helpline
Tel: 01480 376650
Email: ict.helpline@cambridgeshire.gov.uk

ICT Service Tech Support Team Leader
Tel: 01480 376685
Email: john.chapman@cambridgeshire.gov.uk

Procurement & Installations
Tel: 01223 566456
Email: ken.pearce@cambridgeshire.gov.uk

References

BECTA
http://www.ictadvice.org.uk/index.php?section=te&cat=007000&rid=659

CISCO
http://www.cisco.com/en/US/tech/tk722/tech_topology_and_network_serv_and_protocol_suite_home.html