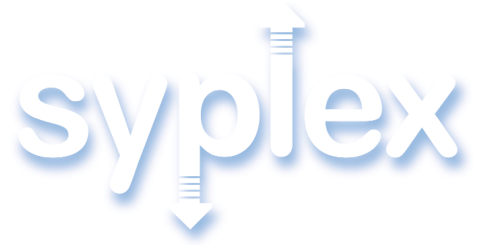


White Paper



Wireless Local Area Networks

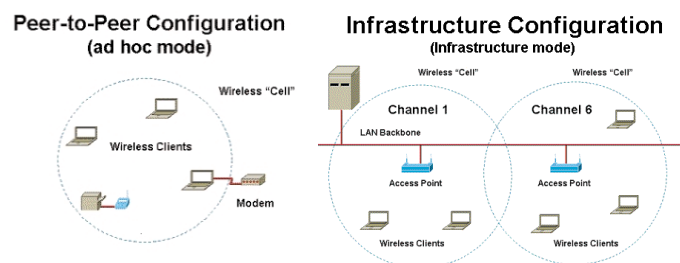
This White Paper is designed to provide an overview for IT Managers and other executives of the impact of wireless technology on the Local Area Network (LAN) and to identify its organisational benefits. It defines Wireless LAN technology, explores areas such as suitability, security, standards and installation, and provides a glossary of terminology. Wireless devices have been hugely successful in other markets, most obviously telephony, making it increasingly important to have a clear understanding of how wireless technology can be integrated and used to advantage within the LAN environment.

What is a Wireless LAN?

In essence Wireless LAN (WLAN) is a technology that enables you to connect PCs to the network without cables. As such it has two distinct benefits over a conventional wired network: it allows users to continue working whilst away from their desks - increased mobility; and it reduces the dependence on fixed cabling infrastructure - increased flexibility.

WLANs offer all of the functionality of hard-wired networks, and usually interoperate with conventional wired Ethernet backbones, offering mobility and simplified network installation in specific locations. Once the WLAN is set up, there are no service or air fees, and users access network servers and the Internet in exactly the way they are accustomed to, at comparable speed. After many years of waiting, the portability of the laptop finally has support for equally mobile networking.

Client computers ("nodes") are connected to the WLAN by the installation of a wireless networking adapter, replacing the conventional Ethernet adapter, and can then operate in one of two configurations illustrated below.



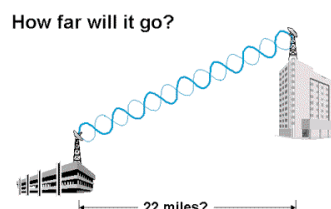
In Peer-to-Peer (also called "ad hoc") mode the wireless clients connect directly to one another to form a self-contained 'wireless only' network, useful perhaps for an off-site team with laptops. In Infrastructure mode they connect to one or more access points, which direct traffic and provide gateways to a wired network backbone. The latter is the more effective implementation for permanent installations and this mode is assumed as the main focus for this document.

Usually WLAN nodes will connect with an access point, the wireless equivalent of a wired network's hub, which is connected to the wired network by a standard 10/100 Ethernet interface. The access point (AP) has an external antenna which must be positioned to optimise the area of coverage, so will typically be mounted on a wall or ceiling. The wireless transmission is able to travel through walls and other obstacles, but the effective range and bandwidth (transfer speed) reduce as the signal deteriorates. Within a building a node should be able to maintain a full-speed connection up to 50m from an access point with a maximum range of up to 120m at lower speed (figures based on an 802.11b compliant network). Further coverage can easily be achieved by using multiple access points to create adjoining microcells (wireless reception areas).

Any devices with appropriate wireless network cards will automatically connect to the WLAN when they come within range of an access point. The number of nodes each access point can support is limited by the required connection speed, as APs are effectively hubs all nodes have to share the available bandwidth.

In some environments, a WLAN may be the best way of installing a computer network - for instance, where conventional network cabling would prove too costly or impossible because of structural hurdles. However, in a normal office environment it is also the ideal way of supplementing the conventional wired network, greatly increasing support for workers with laptop computers and personal digital assistants (PDAs).

WLAN technology can also be used for 'bridging' (connecting) between LANs, for example between buildings, where with specialised antenna and suitable siting the range can be as much as 20+ miles (802.11b), see below.



Suitability of Wireless Networks

The technology is equally valuable for organisations of all types and sizes. It is currently most widespread in healthcare, education, IT, retail, government, manufacturing and finance.

In any organisation wireless networking:

- Allows users of portable devices total mobility within the office, so mobile workers are not confined by the availability of fixed network connections
- Supplements an existing wired LAN infrastructure, wired and wireless operate seamlessly together
- Provides network connectivity in areas where it is inappropriate or too expensive to install cables (e.g. conference rooms, public areas, reception areas, outside areas, exhibition halls, manufacturing or warehousing environments) or where office configurations change on a frequent basis
- Allows small teams to set up their own ad-hoc private networks - for example in common areas such as conference rooms, or off-site at a client's office
- Enables office start-up in new locations without any wiring for either computer or telephone services
- Eliminates the expense and inconvenience of installing wiring, especially for organisations undergoing staff changes or relocation in short-term rented space
- Makes hot-desking a reality by creating common work areas for employees who are only occasionally in the office
- Provides a flexible bridge between existing static networks e.g. inter-site links

"You simply do not realise until you have the ability how valuable it is to be able to access the company data and the Internet during a meeting"

WLANs also have the potential to improve the way we work with PCs. As WLANs are more widely implemented the working methods they will facilitate include:

- People attending meetings, or just working away from their desks in non-wired rooms, can use their laptops to access the company network, the Internet or check e-mail – enjoying true in-house mobility
- Roving employees in a hot-desking environment can find desk space anywhere and readily access files, print documents, undertake research, write reports and presentations and check e-mail. People can even work outside where WLAN access points are available
- Staff and visitors at exhibitions and conferences can have Internet access from any area in the halls without the need for a telephone point

- Staff working in a large warehouse or factory can use WLAN technology to take inventory of supplies
- A business traveller can use a laptop to make a wireless broadband connection to the Internet at any hotel, airport, library, coffee shop or cybercafé with an 802.11 access point

Wireless vs Wired Networks

Wireless and wired networks are not mutually exclusive. Each technology offers a number of unique advantages, and a combination of both will often provide the optimum solution. The comparative features of wireless technology are:

- A notebook PC with a wireless network connection offers much greater mobility, availability and convenience than its wired equivalent
- A wireless LAN allows unbeatable flexibility, for both people and equipment, where an organisation is growing or frequently changing. New employees can be added to the network and offices rearranged without any rerouting of cables and time is saved on new installations when compared to structured cabling runs
- WLAN performance is more than sufficient for the most common office applications, but for the foreseeable future wired networks will continue to offer much greater bandwidth. However the seamless interoperability of wired and wireless networks allows a combined installation with a high-performance wired backbone supporting wireless connections to the desktop
- On costs, although wireless networking equipment tends to be more expensive than wired, there are substantial savings to be made in eliminating cabling and physical infrastructure space planning costs
- Wireless LANs are potentially more vulnerable to security breaches than wired, but when correctly configured with encryption they can actually be more secure
- WLAN technology shares the airwaves with other radio devices, including microwave ovens, some industrial and medical equipment, cordless phones and the new bluetooth devices. Interference from these or from other offices using WLANs can cause bandwidth congestion and slow the network

Standards & Technologies

WLANs use electromagnetic radio waves just like TV broadcasts or mobile phones, and currently operate in one of two wavebands, 2.4GHz or 5GHz. For a time, WLAN was not a standards based technology as each manufacturer created their own wireless networking protocols. However, most manufacturers equipment now complies with the IEEE 802.11 WLAN standards to ensure interoperability.

It is essential to install only equipment that is 802.11 compliant and advisable to stay with one manufacturer. Despite compliant devices being interoperable, inevitable differences in features and some security options make mixing and matching more complex than standardising on one vendor.

There are currently two ratified IEEE standards for wireless LANs: 802.11a and 802.11b. Both use the Ethernet transport protocol, making them compatible with higher-level protocols such as TCP/IP, with popular network operating systems, and with the majority of LAN applications.

802.11b

The “b” standard (also called “Wi-Fi” for wireless fidelity) is currently the dominant wireless standard, with a wide range of fully featured products available at lower cost than 802.11a. It uses the unregulated 2.4GHz part of the radio spectrum and offers up to 11Mbps (megabits per second) of bandwidth, typically over a radius of from 50m up to 120m from an access point. It supports 3 non-overlapping channels so a maximum bandwidth of 33Mbps¹ can be achieved if required. Another reason for its wide acceptance is that 802.11b can use 128-bit encryption, thus allowing secure transmission of corporate data. The Wireless Ethernet Compatibility Alliance (WECA), which comprises several key manufacturers including Cisco, sets the Wi-Fi standard and tests new products to ensure they conform.

802.11a

The “a” standard operates in the relatively interference free 5GHz frequency band offering data transfer speeds of up to 54 Mbps but with a limited range of about 15-20m from the access point. Eight non-overlapping channels are available giving a maximum bandwidth of 432Mbps¹. In the UK using the 5GHz band requires a licence from the Radiocommunications Agency, although this may soon change, and only three channels are currently available.

The IEEE is also working on several new standards to improve WLAN performance and security:

802.11g

Work on the “g” standard is not yet complete but the intention is to provide greater bandwidth (from 20-50Mbps) over the 2.4 GHz frequency and maintain backward compatibility with 802.11b equipment to protect existing investment.

802.11h

This standard aims to develop 802.11a to improve international harmonisation in the 5GHz band, particularly relevant for using 5GHz products in Europe.

802.11i

This standard aims to tackle the issues of authentication and security on wireless LANs.

The European Telecoms Standards Institute (ETSI) has also developed a wireless networking standard:

Hiperlan

This is an alternative to the IEEE 802.11a/h standard and offers similar performance, but it is designed taking account of the different allocations in the European 5GHz RF band. In many respects it is a very advanced specification but at present there are no products available and no support from the major US manufacturers like Cisco.

Case Study – Business Consultants

This Business Consultancy supplemented its existing wired network with WLAN when it increased its personnel numbers from eight to fifteen in early 2002. The Managing Director believes it has had a measurable impact on productivity: *Meetings are a case in point. With the WLAN, we can take our portables into the conference room and still have access to everything we had at our desks. You simply do not realise until you have the ability how valuable it is to be able to access the company data and the Internet during a meeting. You can also type notes directly into your computer instead of handwriting them, arrange appointments with other people and send and receive e-mails. Another boon is that, if you have back-to-back meetings, you do not need to print out everything you need for every single meeting before you disappear into the first one. The amount of time saved is phenomenal.*

Installing a WLAN

Theoretically, a WLAN can be installed by anyone with moderate IT knowledge, although they are more complex to implement than a wired computer network due to their configuration options. When designing a WLAN installation one of the most important issues is to establish the optimum cell coverage pattern in the required area. This determines the performance of the connections and the number of access points required to implement the WLAN. In a small office where one access point will suffice this obviously is not too complex, but in larger installations a site survey should be carried out and this will normally require an external specialist.

Essentially the physical components of a WLAN are similar to those of a conventional wired network, minus the cables.

Client Adapters/Wireless Interfaces

Wireless client devices (sometimes called client radio) are available as PCI or ISA cards for desktops (and potentially servers) and PC Cards for laptops and PDAs. Increasingly, notebooks are being manufactured with built-in wireless network adapters. The computers treat the wireless adapter exactly like any other network adapter, letting you bind normal network protocols and client software to it, and support Microsoft Windows.

¹802.11b current maximum bandwidth available is from three non-overlapping channels. Multiplying 11mb (the current maximum speed) with these three channels delivers 33mbps of bandwidth. For 802.11a using the same formula with eight channels of 54mb each gives a total bandwidth of 432mbps.

Access Points

The Access Point (AP) performs the equivalent function of a hub on a wired network in that it connects, wirelessly, to the client devices and is wired to the Ethernet backbone via a standard CAT5 cable. In the case of Cisco's Aironet products the CAT5 cable also carries power to the AP to ease installation. Once connected, wireless APs allow access to information or a network server that is located on the hard-wired LAN.

To provide wireless coverage for a whole building there will be a need for multiple APs on the network. Each AP will be assigned a different radio channel to provide overlapping coverage whilst preventing interference. Expanding the wireless coverage in this way enables WLAN users to move between different areas without any access problems (termed "roaming") as APs are capable of automatically transferring users to other APs that provide better reception, in the same way that cellular phones function. This means, for example, that a notebook computer user can move between wireless coverage zones without any interruption in the service. However, roaming functions work most effectively if all the APs installed are from a single manufacturer.

Antenna

The design of the antenna determines the range and direction of the radio signals. Specialised antennas are available to provide the most suitable coverage area for the installation, for example a wall mounted antenna will direct the signal back into the building whilst a directional antenna, designed for point-to-point links, can support a range of up to 25 miles. Specialist advice is required to ascertain how far a radio signal will propagate and installers will be able to advise on the most suitable antenna for an installation.

Wireless Bridges

Wireless bridges provide high-speed point-to-point links between two or more separate LANs using wireless LAN technology, for example between buildings. Bridges are normally connected to an antenna that is mounted outdoors as it needs a clear line of sight to the other bridge's antenna, located at the other site. With suitable antenna and correct mounting the link can reach for 10 miles at full speed or up to about 25 miles maximum (802.11b).

Case Study – Sales Team

This company's Regional Sales Manager has found that WLAN technology has transformed the way he works. *It is now commonplace for me to be able to take my laptop around to members of my sales team, or to my hardware buyers or warehouse staff. I can discuss meeting notes from a prospect visit, for instance, and get their feedback there and then without having to print anything out in advance. If someone needs hard copy, I can wirelessly connect to the nearest printer, or e-mail him or her a copy on the spot. I can also work in meetings where I am not required to participate in one session but need to hang around until I am required. In the pre-WLAN days I would either have sat there feeling bored or sneaked out and waited for someone to call me back in. WLAN has had a huge positive impact on my productivity and I cannot imagine working without it.*

Security Issues

It should be understood that broadcasting data through the air has potential implications for network security. Theoretically, hackers could infiltrate a WLAN from outside the building (just using a laptop with a wireless network card), just as they could break into a traditional network over the Internet. Such an attack would be "invisible" to the organisation as there is no activity log to show where the attack came from or what was accessed. Consequently, security has become a major concern for those considering the implementation of a wireless LAN and the manufacturers have responded by adding significant security features to their products.

Basically, wireless networking can be made as secure as hard-wired networks, provided the access points have been set up to encrypt traffic and reject unknown users. Too many non-professional installers are unaware of the need for security and attempt to install the WLAN "straight out of the box" without any security configuration at all.

Encryption

The 802.11b standard includes a built-in provision for encryption called WEP (Wired Equivalent Privacy). Depending on the manufacturer there are two levels of WEP available. One, based on a 40-bit encryption key, is now generally considered insecure but the other uses 128-bit encryption and provides good protection. However standard WEP is based on pre-determined static keys that do not change over time. If a key becomes compromised it is possible for an intruder to gain unauthorised access to the WLAN, but WEP does provide basic protection against being 'overheard' provided it is enabled and configured.

To improve security further there are two additional configuration options:

Dynamic WEP Keys and Authentication

The main weakness of WEP is that it uses pre-installed static (unchanging) keys which if compromised would allow unrestricted access to the WLAN by an external party. To counter this Cisco WLAN products offer IEEE 802.1x based access control requiring EAP (Extensible Authentication Protocol) authentication before a connection to the AP can be made. Once authenticated the AP passes dynamically generated WEP keys to the client, which are unique to that connection session. This delivers a much higher level of security than standard WEP as it verifies the identity of each node and avoids using static keys at all.

VPN over Wireless

Virtual Private Networking (VPN) has been used with great success for many years to secure connections over the Internet. In the same way, VPNs can be established over a WLAN which effectively treats wireless devices exactly like external sites connected over the Internet. Inevitably, building a VPN infrastructure adds complexity and some cost to the installation, but it will provide a layer of encryption and authentication that equips the WLAN to handle the most sensitive data.

Additional simple precautions can be taken to reduce the potential security risks, such as having access points located towards the centre of each building rather than near the windows. Using external installers who can periodically survey each site using a detection tool is another sensible approach: they can locate unauthorised access points and monitor signal strength outside the building.

Health & Safety

WLANs are considered inherently safe to use (certainly safer than cellular phones). Only one transmitter is active at any given point in time meaning that the total radiated power of a total network is equivalent to the radiated power of a single transmitter. This would typically be about 35 milliwatts (mW). This contrasts with a cellular phone, which will have an output power of up to 600mW whenever it is in use.

"WLAN has had a huge positive impact on my productivity and I cannot imagine working without it."

What are the benefits of WLAN?

Major studies have now demonstrated beyond doubt that there are numerous quantifiable and qualitative benefits for end-users from WLAN implementations.²

- **Productivity.** A WLAN user can save up to eight hours per week when compared to a wired LAN user. WLANs enable users to save the most time when responding to e-mail as they can access and respond to them while undertaking other tasks (such as attending meetings or otherwise away from their desks). Other productivity gains arise from the ability to access the LAN for information that may otherwise be sought from a colleague, and rapid access to applications and the Internet
- **Flexibility.** WLAN users are able to access information on the LAN while on the move inside and (if required) outside their building. These include conference/ meeting rooms, training rooms, shipping/receiving areas, warehouses and staff rest areas. A business with a WLAN can also rapidly move its network from a smaller facility to a larger one, or vice versa, without costly and time-consuming rewiring
- **Quality of work.** WLAN users frequently cite improved accuracy as a benefit of WLAN usage. This is particularly noticeable in areas where wireless scanners can be used for stocktaking (where the data is downloaded directly into an appropriate server-based application)
- **Quality of Working Life.** Many WLAN users report reduced stress as a result of being able to access information on demand, regardless of their location. For example, bringing the wrong version of a presentation to a meeting is no longer a problem – the correct one can be accessed on the server wirelessly. Similarly, users can receive and deliver vital information via e-mail whether or not they are close to a wired connection (from the rest area, for instance)

- **Competitive advantage.** Enabling key members of staff to respond from anywhere within the company to an important query (say, from a customer or prospect) will deliver competitive advantage over other suppliers

Network managers are also finding that WLANs deliver quantifiable benefits, including lower overall installation costs and reduced cost of ownership. There is no longer a need to install hundreds of metres of hub-to-workstation wiring through walls and ceilings. In management terms, new users can be added instantly to the LAN with no extra cabling required, plus the WLAN can be made both highly reliable and secure and is fully scalable and adaptable to meet changing needs.

About Syplex

Syplex Ltd are a dedicated team of Information Technology professionals based in Cambridge, England, one of Europe's centres of technological excellence.

Our aim is to provide first-class services to companies and organisations in the Eastern Region by combining proven expertise in the leading technologies, accreditation from the foremost manufacturers and a sound understanding of the commercial drivers for IT solutions.

We are a Cisco Premier Certified Partner with Wireless LAN Specialisation, demonstrating that we have the technical competence to provide WLAN solutions from the world's leading manufacturer of networking equipment.

Cisco WLAN products

Syplex Ltd supplies the full range of Wireless LAN products from Cisco Systems, Inc, the worldwide leader in networking. Cisco design and manufacture a complete range of WLAN products which offer the following benefits to our customers:

- A wide range of wireless products to provide the optimum solution for all types of environment from offices to warehouses and factories
- Excellent support for roaming between access points
- The best security features which are being continually enhanced, including LEAP
- In-line power to ease installation of Access Points
- Compatibility with 802.11b, and seamless migration to future technologies such as 802.11g
- Support for enhanced enterprise ready features like load balancing and redundancy
- Full range of antenna available for specialised installations and remote bridging
- Wireless firmware is flash upgradeable to allow easy upgrading as new enhancements are developed

Syplex offers the following WLAN services: site survey, network design and deployment planning, supply and installation and ongoing support.

²Wireless LAN Benefits Study. Conducted by NOP World Technology on behalf of Cisco Systems (Fall 2001); Wireless LANs: Improving Productivity and Quality of Life. Prepared by Sage Research, Inc. (May 2001)

The Future of Wireless Networking?

WLANs are proving their worth in organisations and it is expected that Wi-Fi will increasingly be available in public spaces such as airports, railway stations, hotels, coffee shops – even trains and buses. With telephone technology the additional convenience and availability of wire-free connections has led to the huge growth of the mobile phone market and it seems likely that the wide availability of WLANs will result in a similar growth in mobile computing.

What seems certain is that next-generation devices, whether cellular phones, handheld PDAs or laptop computers, will be equipped to use multiple connection modes – Bluetooth, Wi-Fi, GPRS and 3G. This will enable users to seamlessly switch from cellular networks to Wi-Fi and vice-versa depending on which signal provides the best data link. Within the next few years this capability will enable people to use their portable devices in hitherto undreamed-of ways. Watch this space...the future is wireless.

How big is the market?

The Wireless LAN is already proving its worth as a mainstream network platform. Figures from Gartner Dataquest show that more than five million wireless network cards and almost two million wireless APs were sold in 2001.

For details on how Syplex Ltd can help you achieve your WLAN or other IT implementation objectives...

Call: 01223 422 355

E-mail: info@syplex.co.uk

Fax: +44 (0) 1223 422356

Or visit: www.syplex.co.uk

Syplex Ltd

St Johns Innovation Centre
Cowley Road
Cambridge CB4 0WS

© 2002 Syplex Limited. All rights reserved.

All trademarks acknowledged.

For information on Cisco WLAN products, see www.cisco.com

WLAN Glossary

Access Point (AP) A wireless hub, connects between wireless clients and a wired network (infrastructure).

Ad-Hoc Network A small wireless network composed only of network clients in peer-to-peer mode (i.e. without access points).

Antenna A device for transmitting or receiving a radio frequency (RF). Antennas are designed for specific and relatively tightly defined frequencies and radiation patterns i.e. an antenna designed for long range bridging will support only a very narrow radius.

Bluetooth A short-range wireless connection intended for use in personal devices like headsets.

Channel A communications path wide enough to permit a single RF transmission.

Client Any computer connected to a network that requests services (e.g. files, print capability) from another member of the network.

Direct sequence (DSSS) A method of wireless transmission that can provide higher data rates and greater robustness in radio-noisy environments than frequency hopping. The trade-off is higher cost and fewer users for a given area. Used in 802.11b.

EAP Extensible Authentication Protocol.

ETSI European Telecommunications Standards Institute, regulates telecoms standards in Europe.

Hiperlan/2 An ETSI standard for 5GHz WLAN equipment.

IEEE 802.1x A standard for Port Based Network Access Control defining user authentication, dynamic session based encryption keys and centralised user administration. Used to improve WLAN security.

Infrastructure Mode A client setting that provides connectivity to an access point (AP). Clients set in Infrastructure Mode all pass data through a central AP.

LEAP Lightweight Extensible Authentication Protocol, developed by Cisco to provide EAP on pre-Windows XP PCs.

Microcell A bounded physical space in which a number of wireless devices can communicate. Because it is possible to have overlapping cells as well as isolated cells, some rule or convention establishes the boundaries of the cell.

RF Radio Frequency.

Roaming Movement of a wireless node between two microcells. Roaming is relevant in infrastructure networks built around multiple APs.

Wireless Ethernet Compatibility Alliance (WECA) The standards body that developed the Wi-Fi interoperability standard. WECA's mission is to certify interoperability of Wi-Fi (IEEE 802.11b) products and to promote Wi-Fi™ as a global wireless LAN standard across all markets. See www.wirelessethernet.org

Wi-Fi (Wireless Fidelity) The trademarked name given by WECA to wireless networks operating with the IEEE 802.11b standard. See <http://www.wi-fi.org/>

Wireless LAN (WLAN) A Local Area Network where the physical layer (i.e. cabling) has been replaced by radio waves.

Wireless node A computer or other device with a wireless network interface card.

Wired Equivalent Privacy (WEP) Encryption mechanism defined within the 802.11b standard. Designed to make the link integrity of the wireless medium equal to that of a cable.