

INTELLIGENT DATA & POWER SOLUTIONS

WIRELESS LANS

Wireless LANs allow workstations to communicate and access the network using radio propagation as the transmission medium. The wireless LAN can be connected to an existing wired LAN as an extension, or can form the basis of a new network. Wireless LANs are especially suited to indoor locations such as; Office Buildings, Manufacturing, Hospitals and Universities.

The basic building block of the wireless LAN is the 'cell'. This is the area in which the wireless communication takes place. The coverage area of a cell depends upon the strength of the propagated radio signal, type and construction of walls, partitions and other physical characteristics of the indoor environment. In general, a cell covers a more-or-less circular area. PC-based workstations, notebook and laptops computers can move around freely in the cell.

An Access Point (AP) connects the cells of the wireless LAN with one another and connects wireless LAN cells to a wired (cabled) Ethernet LAN via a cable connection to an Ethernet LAN outlet e.g. an outlet as part of a structured cabling system.

The two main radio solutions used for Wireless LAN (WLAN) are: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). By transmitting the message energy over a bandwidth much wider than the minimum required, Spread Spectrum modulation techniques present two major advantages for Wireless Local Area Networks (WLAN):

Low power density relates to the fact that the transmitted energy is spread over a wide band, and therefore, the amount of energy per specific frequency is very low. The effect of the low power density of the transmitted signal is that such a signal will not disturb (interfere with) the activity of other systems' receivers in the same area.

Redundancy relates to the fact that the message is (or may be) present on different frequencies from where it may be recovered in case of errors. The effect of redundancy is that Spread Spectrum systems present

a high resistance to noises and interference; messages are recoverable even if noise is present on the medium.

Low power density and immunity to noise allow for license free use of the technology and make Spread Spectrum the technology of choice for (unlicensed) WLANs. One of the frequency ranges allocated for use with Spread Spectrum technology is 2.4 GHz to 2.4835 GHz, the same as the Industrial, Scientific and Medical (ISM) band. Most of the WLAN products currently available on the market operate in the ISM band.

The main differences between the two technologies are:

	FHSS	DSSS
Data Rate	up to 3Mbps	up to 11Mbps
Net throughput	up to 2.4Mbps	up to 5.5Mbps
No co-located cells /systems	26*	max 3 channels

*max 26 in any one hopping set. There are 3 sets of 26.

WIRELESS SECURITY

As the use of wireless LANs develops; businesses are becoming increasingly concerned about network security. The users need freedom and mobility without offering intruder's access to the WLAN or the LAN it is connected to.

With any WLAN, a client within an AP service area can receive the data transmitted to or from the AP. If security measures are not put into place, installing a WLAN can be the equivalent of putting Ethernet outlets everywhere, including the car park !

Basic WLAN security includes the use of Service Set Identifiers (SSID), open or shared key authentication, static WEP keys and optional MAC authentication (WEP keys are used to encrypt and decrypt transmitted data).

The SSID is a simple common network name for devices in a WLAN. This prevents access by any client that does not have the SSID. However, the AP broadcasts

INTELLIGENT DATA & POWER SOLUTIONS

the SSID and therefore can be detected by an intruder. The 802.11 standards for WLANs support two means of client authentication: open and shared-key. Open authentication is little more than supply of the correct SSID. With shared key authentication, the AP sends a challenge text packet that the client has to encrypt with the correct WEP key and return it to the AP. If the client has the wrong key or no key then authentication will fail. Shared-key authentication is not considered secure.

Static WEP keys are often used. It is defined by the network administrator on the AP and all clients that communicate with the AP. If a device that uses a static WEP key is lost or stolen, the processor of the stolen device can access the WLAN!

Specific manufacturers of WLAN equipment have developed additional security features based on a new IEEE standard for authentication – 802.11n.

WIRELESS LAN BRIDGES

A wireless bridge enables high-speed long-range outdoor links between buildings. It can be used with associated antenna to create a radio frequency (RF) link between two or more buildings. A maximum data rate of 54Mbps is achievable to provide a low cost data link eliminating the need for expensive dial-up services, leased lines, fibre installations and LAN extension services.

POINT-TO-POINT WIRELESS BRIDGE SOLUTION

A point-to-point solution can utilise a WLAN to create a network link between two remote premises. Products such as the Cisco Aironet Wireless bridge and the Motorola-Orthogon (Near Line of Sight) can be used to create this link and it can provide network links of up to eight miles in the UK with speeds that can exceed the standard 54Mbps.

Utilising a point-to-point wireless bridge overcomes logistical issues such as digging across public roads and highways. Unlike leased lines where costs are incremental and monthly, once installed and configured, the costs of such bridges are quickly recovered.

FREE SPACE-OPTICS

INS Sudlows can also offer Free Space Optical systems, such as the Sunflower which have the ability to communicate between two fixed points with extremely large bandwidth capabilities without the necessary

licensing requirements in traditional microwave and radio links.

FSO Systems, such as the Sunflower can be quickly deployed used either internally (Window to Window) or externally to suit the environment. Any installations can be either permanent or simply used as a temporary connection and quickly removed and installed to any new site or location with minimum fuss or effort.

NEXT GENERATION

802.11n wireless networks let you create a seamless working environment by combining the mobility of wireless with the performance of wired networks. Cisco has innovative, next-generation wireless solutions that offer greater performance and extended reach for pervasive wireless connectivity. 802.11n technology delivers unprecedented reliability and up to five times the throughput of current 802.11a/b/g networks. It makes wireless networks an integral part of every type of organization by offering the following benefits:

- Data rates of up to 300 Mbps per radio support more users, devices, and mission-critical, bandwidth intensive applications
- New multiple-input, multiple-output (MIMO) technology provide predictable WLAN coverage and reliable connectivity
- Next-generation wireless provides the greatest investment protection to support emerging mobility applications

802.11n is due to be officially ratified as a new standard in September 2008.

Data Speeds and Standards	
802.11	2Mbps
802.11b	11Mbps
802.11a/g	54Mbps
802.11n	300Mbps

In partnership with our consultancy experts ANS Group, INS Sudlows have successfully completed a number of significant Wireless LAN installations in Business and Healthcare Sectors. INS Sudlows have the experience to design, install and encrypt vital information systems, where flexibility and confidentiality are paramount.