Wireless Advantages versus Disadvantages

Wireless Local Area Network (WLAN)

Advantages vs. Disadvantages

Mike M. Khayat

INNS 690, Professional Seminar

Mr. John Meinke

March 12, 2002

Table of Contents

Abstract

This paper addresses the Wireless Local Area Network (WLAN) for companies in European countries. The wireless system for Local Area Network (LAN) is an important landmark in the history of the Internet and electronic applications. It opens up existing systems, databases and intranets to mobile equipment such as telephones and hand-held terminals through a graphical customer interface. The most important benefit of WLAN is that it is independent of different mobile technologies that are used in different parts of the world.

The recent increase in mobile computing technologies and projects in the enterprise environment has resulted in extensive use of numerous point-to-point products that cover only a small part of the total mobile and wireless infrastructure that is required.

This paper is intended to be used as a recommendation for any company involved in building more effective use of commercial WLAN in European countries. Much of what is required to build an enterprise WLAN standard has been already defined years ago. It is critical that this be synthesized and summarized so that network managers and managements can have a better understanding of how to manage this great WLAN technology in the commercial environment. This paper attempts to fill in that space and concludes with an opinion of the WLAN technology based on the research.

Research statement

Challenges exit which will prevent wireless networking from becoming feasible in Europe in the short-term.

Introduction

Wireless LAN is a networking technology that allows the connection of computers without any wires and cables, mostly using radio and infrared frequency (RF) technology. It's called LAN because the range targets within an office, a building, a store, a small campus, or just a house.

The description of a WLAN is a mobile data communication connectivity system installed and configured as an alternative in some cases for traditional LAN. The WLAN equipment is capable of receiving and sending data over an adequate range. In the United States, the WLAN business is increasing in areas like the airports, health-care, warehousing and manufactures. Several research companies are predicting a healthy increase in WLAN business market in the coming years. The WLAN provides advantages over traditional LAN technology such as buried cables in the ground, hidden cables behind walls, and long cable runs measured in feet or miles. Without restrictions, the new technology infrastructure can easily be installed and ready to be used.

Current growth concerning network communication technology in the enterprise communication environment has resulted in widespread deployment of numerous products that cover only a small part of the total mobile and WLAN infrastructure required. The WLAN industry has experienced phenomenal increase over the past ten years. The U.S. wireless industry posted revenue of $40 billion in 1999, according to the Cellular Telecommunications Industry Association, and employed 156,000 workers (Palazzo, 2002). Most manufacturer companies offer WLAN equipment to improve field productivity, increase customer approval and reduce operational costs by shifting the way field workers and dispatchers perform their jobs.

Figure 1. WLAN Topology, source WLANA, 2000

Using the WLAN technology has already increased the speed from 1 to 11 Mbps with the introduction of the IEEE 802.11b (Frank, 2002). Office and field workers can now send and receive data wirelessly over the intranet, using state-of-art leading edge equipment. With the latest product and service, there is no need to invest in costly computer services and products or

suffer through a lengthy installation and implementation project. The objective is to rapidly provide customers with data network solutions and mobile equipment for enhanced connectivity, mobility, and flexibility, while at same time, maintain acceptable security. Customer influence was measured with WLAN systems that can be provided at anytime, anywhere and cost less, see figure 1 for WLAN topology.

Mobility

The most important benefits of WLAN are flexibility, mobility and portability, but no industry standard currently addresses the tracking or management of mobile equipment in its Management Information Base (MIB). This omission would reject customers from roaming between WLAN APs that cover a common work area, such as a complete floor of a building. The manufacture has engineered this problem, offering its own solutions of flexibility algorithms that facilitate roaming within an IP domain such as a floor with an eye towards optimizing roaming across IP domains.

The WLAN equipment can provide customers with connectivity to real-time information anywhere in their work areas. This flexibility supports productivity and service opportunities not possible with traditional wired networks. Installation of WLAN equipment can be fast, easy and can eliminate the need to pull cable through walls and ceilings.

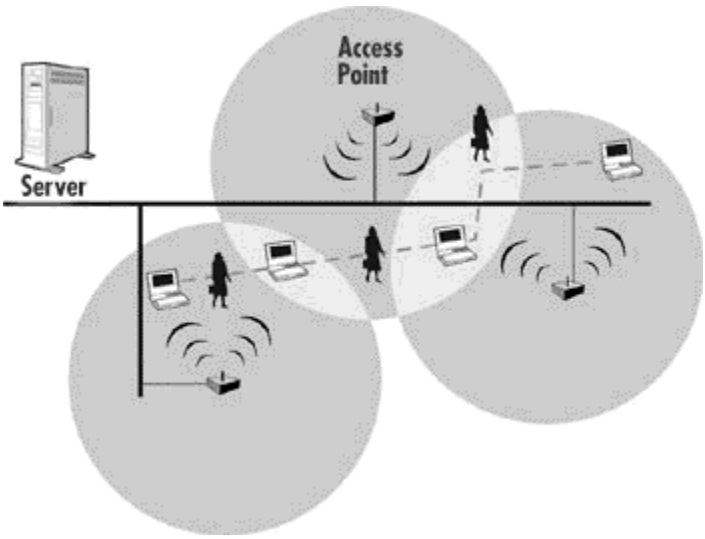

Figure 2. Handing off the WLAN Connection Between APs. (Source WLANA, 2000)

This new equipment enables technology, through a gateway infrastructure deployed in mobile operator's network, this will bridge the gap between the mobile world and the intranet, bringing sophisticated solutions to WLAN customers, independent of the bearer and network. When a customer sends data using WLAN equipment, it sends low energy radio waves to a local antenna site, which connects the customer with the landline or wireless location from where the customer is dialing. That same antenna also sends signals back to the customer wireless equipment. The WLAN equipment has the ability to move from one area to another within an adequate range. This technology allows services to derive the function and added value of the WLAN network. There is a key set of general functions and basis services that must be supported to have a viable service offering. This key set of functions and services includes the ability for the customer’s

computer to register, transmit which is to send, receive, and maintain data via one or more different media types. These features can be provided to the customer within a reasonable time if a tactical mission is on the horizon. The RF result is low power, and works with an AP that sends the radio waves to several customers. High expand antennas and multiple APs are required to send the signals over thousands of feet, see figure 2. Handing off the WLAN Connection Between APs.

Range

In the analysis of WLAN range, there is marginal theoretical difference in the range capabilities of Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) systems. The largest range difference will be caused by two sources; the type and location of the antenna system not the spread spectrum modulation used and the environment that the equipment is operating in. The antenna diversity is one of the most important influences on the range and performance of equipment, particularly near the edge of the range profile, the marginal area. The antenna diversity is the use of multiple antennas that are physically separated. This is done because the radio waves will reflect off all objects, walls, buildings, bridges, cars, hills, trees, etc and cause nulls and peaks arbitrarily distributed in the air (OCBN, 2001).

It is significant for a good path to have a high height for the antenna. Basically, a better antenna elevation means better connectivity range, with all other things being equal. An appropriate antenna height would be required to “shoot over” path obstructions like hills or trees and also to reach suitable “Fresnel” zone permission, see figure 5 on WLAN frequency & range. This is much the same as the peaks and troughs that are seen on the surface of water when separate waves encounter each other and are called "Multipath" in the radio environment. With two antennas separated by a quarter of a wavelength, a few inches for 2.4 GHz band, it is statistically very unlikely that both antennas will be in a null or wave trough at the same time, whereas a single antenna will be realistically possible to be in a null in a highly reflective environment, such as an office building (Proxim,1998).

Figure 3, WLAN range between client and AP. (Source Proxim, 2000).

For a better performance, large antennas placed high above the ground will always provide better range than small antennas that extend marginally from a Personal Computer (PC) card and are low down on the side of a notebook computer. The range of the different equipment

components is therefore different. Single PC cards have the shortest range, 100-500 feet depending on the environment, see figure 3. An AP with elevated, efficient antennas will achieve up to 3000 feet. Fortunately in most communication equipment the client card will communicate with an AP and the overall link will benefit from the better antenna on the AP, though it will still have a shorter range than two APs communicating with each other.

The environment that the equipment is used in has a very significant influence on the range and performance. This should be of a little surprise to everyone that has used a cordless phone, as they suffer from similar range and performance problems as WLAN. When the environment is outside, in line of sight (LOS), with little to reflect off and cause multi-path, the range is at its best. When the environment is in a solid walled building, such as an old stone house or in the building basement, the range is greatly reduced. This is the same for WLAN, however the multi-path problem can significantly degrade megabit communications where it will not significantly affect connectivity quality.

Every WLAN configuration is different, when engineering an in-building solution, varying facility sizes, construction materials, and interior divisions raise a host of transmission and multi-path considerations. When implementing a building-to-building solution, range, physical obstructions between facilities, and number of transmission points involved must be accounted for. Several factors come into evaluation when measuring radio transmission range like, transmitter power, receiver sensitivity, antenna gain, antenna height, RF cable attenuation (RF connection from transmitter to antenna), and terrain. Since WLAN equipment operates in the 2.4 GHz band they need a LOS transmission path. The link range will be severely degraded if trees, hills, walls, heavy fog, or other obstructions are in the radio transmission path. It is very difficult to predict link range achievement for non-LOS paths.

Most office environments are constructed of materials that are relatively "translucent" to radio waves at 2.4 GHz so the range will not be greatly limited, however they do tend to present very reflective and refractive environments and the ultimate limitation will probably be caused by severe multi-path problems. Range up to 80 meters was achieved in point to multipoint tent configurations. Indoor range is considerably less and depends on the physical layout. Equipment based on the “Bluetooth” WLAN technology interferes with IEEE 802.11b WLAN. For most cases, Germany and European cities in general, support 2.4 Gbps transmissions to 100 mw:

100mw = 1mw transmitter * 20 dbi Dish Antenna
100mw = 5mw transmitter * 14 or 15dbi Yagi Antenna
100mw = 50mw transmitter * 2dbi monopole antenna

The standard IEEE 802.11b data is encoded using DSSS technology. The DSSS works by taking a data stream of zeros and ones and modulating it with a second pattern, the chipping sequence. The standard IEEE 802.11, that sequence is known as the Barker code, which is an 11-bit sequence (10110111000) that has certain mathematical properties making it ideal for modulating radio waves. The basic data stream is exclusive OR'd with the Barker code to generate a series of data objects called chips. Each bit is "encoded" by the 11-bit Barker code, and each group of 11 chips encodes one bit of data (Conover, 2000).

Communication network managers often find that WLAN fall short of expected range. Even though a vendor's specifications may say that the equipment has a range of 300 feet, obstacles such as walls, desks and filing cabinets can significantly reduce the range in some directions.

This results in an irregular propagation pattern of the radio signal. To provide adequate radio coverage throughout work areas, communication network manager needs to perform a RF site survey that determines the number and location of APs, as well as uncover potential RF interference (Geier, 2001).

Frequency

The FHSS uses a slim band carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short duration impulse noise (NDC Communications, 1999).

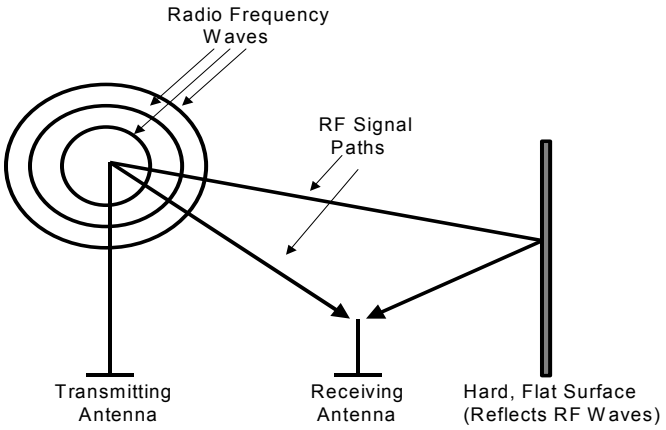

Figure 4, WLAN RF, source (Burd, 998)

There are two main technologies that are used for WLAN communications today, RF and infra red (IR). In general they are good for different applications and have been designed into products that optimize the particular features of advantage. The RF is very capable of being used for applications where communications are not LOS and over longer range. The RF signals will travel through walls and communicate where there is no direct path between the equipment. In order to operate in the license free portion of the spectrum called the industrial, Scientific and Medical (ISM) band, the radio system must use a modulation technique called Spread Spectrum (SS). In this mode a radio is required to distribute the signal across the entire spectrum and cannot remain stable on a single frequency. This is done so that no single customer can dominate the band and collectively all users look like noise (NDC Comm.,1999).

The SS communications were developed during World War II by the military for secure communications links. The fact that such signals appear to be noise in the band means that they are difficult to find and to jam. This technique lends itself well to the expected conditions of operation of a real WLAN application in this band and is by its very nature difficult to intercept, thus increasing security against unauthorized listeners, see figure 5 for WLAN frequency and range.

The WLAN uses RF or IR instead of copper or fiber optic cable to connect customers together into a LAN. The WLAN is appealing because it allows customer mobility, flexibility can easily be reconfigured, and requires no cable infrastructure. The WLAN is particularly useful when mobile access to data is necessary, such as in health care environments and warehouses. It is also appropriate in situations where a temporary LAN is needed but no communication infrastructure is available, such as when hosting conferences at hotels or community clubs, or when providing computer based training in ad-hoc classrooms, exercises, and emergency missions. Frequency hopping addresses a significant problem with RF "transmission-Multipath" distortion, which occurs when an RF signal bounces off the stationary objects.

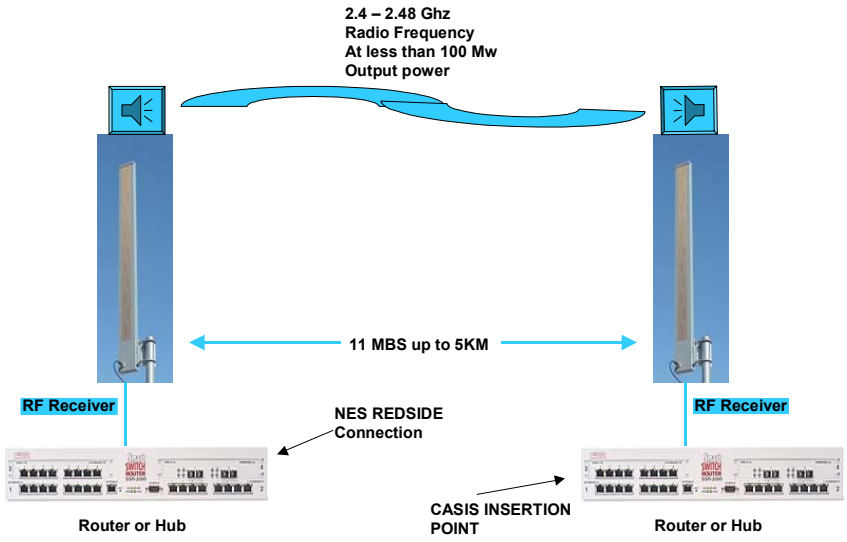

Figure 5. WLAN frequency and range

A receiving antenna can receive multiple copies of the same signal at slightly different times, figure 4, WLAN RF, which blurs or smears the signal content causing bit detection errors. The problem is especially severe in-door where there are numerous hard, flat surfaces to "bounce" RF signals (Burd,1998).

Equipment Cost

An analysis reveals savings can be measured in terms of equipment cost for WLAN compared to what customarily is in used for wired LAN connection. In order for two customers to communicate over the wired network, the following are required for installation, network cable installation with, data drop ($500), PC LAN card ($50), a hub ($100), small router ($2,500), a network T1 modem ($1,300), and cable conduit between customer buildings, bringing the total to $9,000. For the WLAN, connecting two customers to a LAN, the total cost is not more than $7,000 that to include the bridge 100Mw output ($1,400), ceiling antenna ($82.00), 11Mbps DSSS AP ($990) and cable ($120). The big savings is that there is no need to open a trench to bury network cable

beneath the ground, quick installation, and can easily to be removed, see table 1 on equipment cost, range and performance for three types of WLAN equipment. The relatively high cost of transmission equipment and licenses makes short wave radio a rare method for a signal user or company; instead, companies are formed to purchase and maintain the required licenses and infrastructure (Burd,1998).

Feature	Type 1	Type 2	Type 3
distance (feet):	500	1000	1000
(meters):	150	300	300
speed/protocol:	full duplex 10 T3 to 100 Mbps Ethernet FDDI & Fast Ethernet to 155 Duplex 10 Mbps Ethernet	from 4/16 Mbps Token Ring to full Mbps ATM	from 45Mpbe
Remote management:	no	yes	yes
List price ($US):	$6,995	$8,995	$16,995

Table 1, Equipment cost, range and performance

For usual wired LAN connectivity, the immediate cost is high, the installation site requires extra money compared to the WLAN connectivity, this is not to include the wired cable is a lease line, and switched line rates, the actual rates for dedicated leased lines may vary from one country to another. In the U.S. the rates are based on range, see table 2 for leased line rates and table 3 for switched line rates in the U.S (Stamper,1999).

Range	Rate
First 100 miles	$2.52 per mile
Next 900 mike (101-1000)	$0.94 per mile
Each mile over 1000	$0.58 per mile

Table 2 leased line rates in U.S. Source (O'Brien,1999)

Type of charge	Rate
Fist minute of connect time	$0.60
Each additional minute	$0.40

Table 3 switched line rates

Line type	Rate (year)	One time cost
E1 Speed	$87,732	$5,000
T1 Speed	$84,264	$5,000
Fiber 2 strands distance 40KM	$252,000	

Table 4 leased line rates in Germany

Factor in the price of a mobile device plus application software, wireless service, maintenance and support, each users' tally can reach $3000 annually (Bednarz, 2001). Table 5 shows the immediate and recurring requirements comparison for two LANs, the traditional wired LAN and WLAN. The difference between these two LANs is small.

Immediate Requirements	Wired LAN	WLAN
equipment upgrades:	X	X
documentation:	X	X
site preparation (AC, raised floor, etc..):	X	---
hardware installation:	X	X
installation applications:	X	X
testing:	X	X
training (users, operators, administrators):	X	X
installation of cabling:	X	---
equipment software installation:	X	X
creating user environments:	X	X
space required for new equipment:	X	---
supplies and spares:	X	X
backup:	X	X
Recurring Requirements:		
LAN management, personnel costs:	X	X
consumable supplies:	X	X
hardware and software maintenance:	X	X
training (new users, administrators):	X	X

Table 5, two types of LANs comparison

A WLAN implementation includes both infrastructure costs for the Wireless APs and user costs for the wireless LAN adapters. Infrastructure costs depend mainly on the number of APs deployed, APs range in price from $800.00 to $2,000.00. The number of APs typically depends on the required coverage region and/or the number and types of customers to be supported. The supported area is proportional to the square of the product range (WLANA, 2000).

Equipment bandwidth and performance

The WLAN protocol is engineered to reduce the demanded bandwidth and maximize the number of wireless network types that can deliver. Multiple WLAN networks within an area can be achieved, with the additional aim of multiple networks. In other words, an IP-networked world will enable the multimedia evolution to optimize the bandwidth required to support the multimedia applications demanded by the marketplace. This will reduce the cost to own or lease a dedicated LAN circuit. The WLAN equipment can go point-to-point (PPP), speed up to 100MB at range of a 3000 meters. The WLAN equipment speed is adequate among customers to send and receive e-mail messages, upload and download documents (PowerPoint briefing slides, spreadsheet, etc.) and small data files, see table 1 equipment cost, range and performance for WLAN performance.

The ISM spread spectrum bands do not offer a great deal of bandwidth, keeping data rates lower than desired for some applications. The IEEE 802.11 working group, however, dealt with methods to compress transmission data, making the best use of available bandwidth. Efforts are also underway to increase the data rate of 802.11 to accommodate the growing need for exchanging larger and larger bandwidths (Geier, 1999).

Type of Media	Maximum BPS (kilobits per sec)
Twisted pair – unshielded/shielded	2M-100M (million)
Coaxial cable – baseband/broadband	264M-550M (million)
Satellite/terrestrial microwave	100M (million)
Wireless LAN	3.3M (million)
Infrared LAN	4M (million)
Fiber optic cable	40G (Billion)

Table 6, types of media. Source (O'Brien,1999)

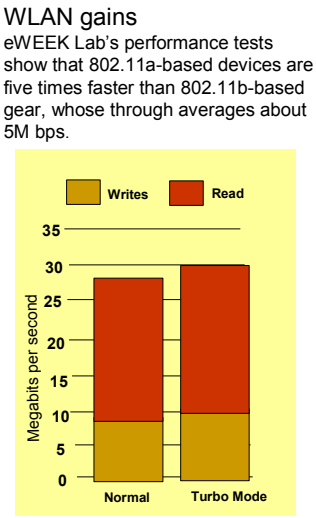

Fig 6 WLAN performance, source (Taschek, 2002)

The standard for WLAN networks is IEEE 802.11b. The 802.11b standard specifies the use of DSSS in the 2.4 GHz band. Most European countries have a maximum of 100mw power output. The data communications rate for this standard is at 1 and 2 Mbps. The 802.11b high-rate (HR) Wi-Fi version of the standard increases the throughput to 11 Mbps but the same power maximum applies in Europe. The WLAN equipment can theoretically support up to 200 customers. Table 7 compares the conventional wired LAN and WLAN. The evaluation performance rates criteria on a scale of 1 to 5, with 1 being Best.

Criteria	Wired LAN	WLAN
Number of workstations:	1	4
initial cost:	4	2
personnel costs:	5	1
operations/maintenance costs:	5	2

expandability:	1	4
microcomputer workstation support:	4	3
user transparency:	3	1
accommodation for multiple users:	1	1
ease of use:	3	1
ease of management:	3	1
interface to other networks:	1	5

Table 7, LANs comparison

The "Multipath" Fading problem is caused by a signal bouncing off the walls and other surfaces, as the signal arrives at the receiver, a reflection of the signal will arrive shortly afterwards. This causes interference as old signals arrive at the same time as the new data. Frequency hopping equipment is protected from this problem since a reflected signal arrives after the receiver has hopped to a new frequency and any signal on the old frequency is ignored. Direct sequence systems do not have this advantage, however a technique identified as antenna diversity allows them to show some improvement. Antenna diversity involves having two antennas built into the hardware. Two antennas allow the equipment to determine which signal is stronger (Canterbury Campus, 2001). Table 8 displays the IEEE series topologies and protocols:

Criteria	IEEE 802.3	IEEE802.5	IEEE 802.11
Speed:	10, 100, 1000Mpbs	4, 16, 100 Mpbs	vary
Medium:	twisted-pair wires Coaxial cable, fiber optic	twisted-pair wires	wireless
Range:	500 m for thick table up to 1000 m 185 m for thin-net cable up to 2500 m w/repeaters	366 m for the main ring 750 w/repeaters 400o m fiber optic	
number of stations:	802.3-100 per thick	260	200
cost for NIC and connectors only:	\$30 per thin-net \$50 per station	\$225 per station	N/A

Table 8, IEEE series comparison

Equipment procurement and installation

In view of wireless technology, cost reductions of network components will be possible compared to alternative technologies like traditional wired LAN. Cards that plug into PC or laptop are promptly available, and operate either Peer-to-Peer or Peer-to-AP Mode. The WLAN equipment can be configured in a matter of hours while customarily used equipment (hard wire) can take a week to a month if cable between customers is not available. For scalability, WLAN can be installed and configured in a variety of topologies to meet the needs of specific

applications and installations, see figure 7 on vendor equipment.

Vendor	Product	Type	Data Rate	Power	Maximum Range Indoor/Outdoor		Configuration	Host Nation?	Price ($US)	Miscellaneous
Aironet	PC3500	FH	Up to 2 Mbps	100 mW	150 m	600 m	PCMCIA Type II	U	-	IEEE 802.11
Aironet	PC4500	DS	1 or 2 Mbps	50/100 mW	75 m (2 Mbps) 100 m (1 Mbps)	300 m (2 Mbps) 500 m (1 Mbps)	PCMCIA Type II	U	-	IEEE 802.11 compliant
Lucent	WaveLAN PC-AT Wireless Adapter	DS	2 Mbps	88 mW	240 m	-	ISA card	U	545	-
Lucent	WaveLAN PCMCIA Wireless Adapter	DS	2 Mbps	88 mW	240 m	-	PCMCIA Type II	U	495	-
Proxim	RangeLAN2 7100 ISA	FH	1.6 Mbps	100 mW	150 m	300 m	ISA card	U	595	15 channels. OEM version available.
Proxim	RangeLAN2 7401/02 PC Card	FH	1.6 Mbps	100 mW	150 m	300 m	PCMCIA Type II	U	695	15 channels. Several antennas

Figure 7, WLAN vendors

The WLAN configurations are easily changed and range from peer-to-peer networks suitable for a small number of customers to full infrastructure networks of thousands of customers that enable roaming over a broad area, as used in several U.S airports and hospitals. Micro cells (the physical areas covered by each of the LAN AP) are established to provide coverage to all customers, figure 8 shows a notional WLAN configuration.

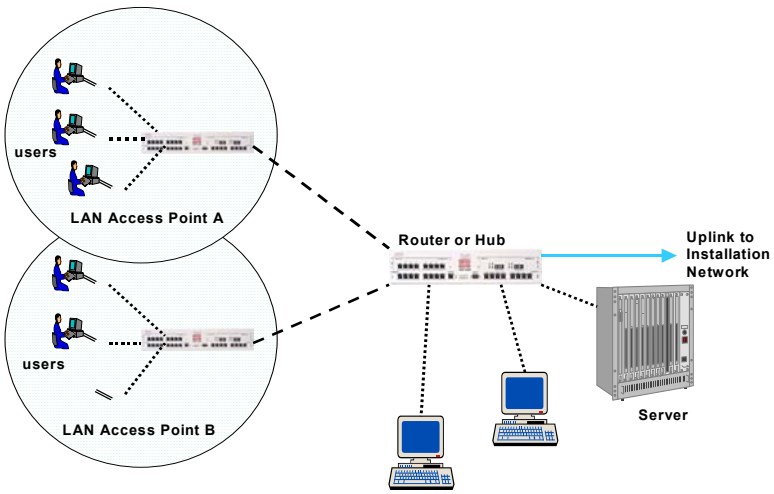

Figure 8. WLAN Configuration

The range a WLAN can be from a LAN AP depends on many factors including the types and numbers of obstructions (such as walls, hills, trees, etc.), the data rate, and the equipment used.

The LAN AP serves as the LAN hub for the WLAN customers and as connection points into normal building LANs. Each LAN AP typically supports large number of customers, depending upon their network use.

A variety of factors must be considered when selecting type equipment for LAN connectivity. The company should decide whether a wired LAN is required or an alternative like WLAN will be sufficient. Factors, which must be considered, include cost- effectiveness, hardware, application software, security, training, etc. The weight associated with each selection criterion may differ among companies. In making the right selection, company management and IT analysts need to evaluate the alternatives from the perspective of their companies' immediate short-term and long-term communication objectives, see evaluation criteria below.

Criteria	WLAN	others
cost:		
number of concurrent users:		
medium:		
short-term and long term objectives:		
expandability:		
software and hardware:		
vendor support (just-in-time):		
number of workstations:		
type of use:		
mobility and flexibility:		
environment		
maintenance:		
life cycle:		
speed:		
equipment connectivity:		
vendor on site:		
manageability:		
type of workstations:		
number of printers:		
applications:		
connectivity with other networks:		
type of mission, location, country:		
adherence to established standards:		
security:		
host nation approval:		
range:		
frequency:		

Table 9, criteria selection

Security

The WLAN service cannot be perfectly secured, but the wireless industry has made significant investments to prevent intruders and hackers. The WLAN equipment can support session layer protocols that establish the connection between applications, enforces rules for

carrying on the dialogue, and tries to re-establish the connection if a failure occurs. The WLAN manufacturing companies claim that the current IEEE 802.11b standard contains an optional 40-bit encryption algorithm to ensure data sent over the air is scrambled and remains private.

A small research group at the University of California at Berkeley in recent times put out a statement stating that they found flaws in the IEEE 802.11 standard (and IEEE 802.11b standard). Their statement says that they were able to intercept transmissions over the wireless network. These transmissions were encrypted, but the encryption was broken (Dunne, 2001).

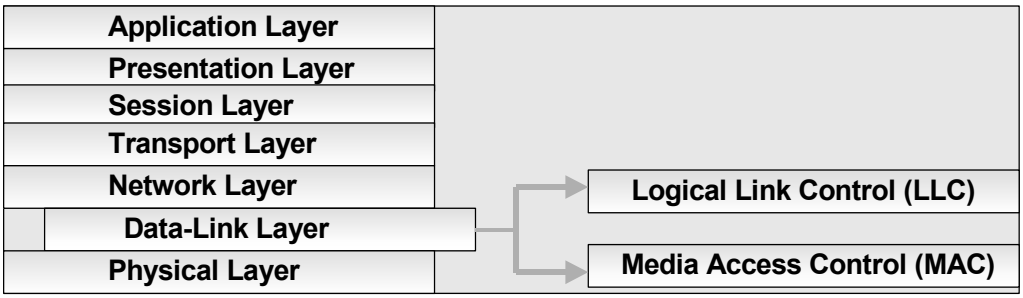

Figure 9, MAC layer

A company may implement WLAN for the customer's specific requirement, however, WLAN security is the most serious issue that a customer must consider. Most WLAN circuits enter European controlled areas; non-secure encryption device is a requirement. Throughput is the next most critical WLAN issue. WLAN should not be used for critical data transfer without a study on the maximum throughput requirement. The WLAN technology is considered an emerging technology, and therefore should be approached with caution. The technology is largely untested for the secure environment, and it introduces a potential for operational data-loss and yet-unknown security risks.

As with wired networks, the first line of security defense is the customer IDs and passwords in the operating system of client computers and servers. Additional security varies from one AP to another.

Many AP manufacturers allow network administrators to limit AP connections by creating a table of wireless client hardware media access control (MAC) addresses, see figure 9 above on MAC layer. There is no WLAN solution exists for sensitive data processing. Also, before any wireless equipment is procured or operated in Europe, the customer must verify that the specific wireless equipment used has host-nation approval to be used in the country where the LAN is to be set up. Although WLAN is a part of the Information Systems Architecture (ISA), there are numerous procedural guidelines processes that must be completed before they can be implemented, host-nation approval is required for any wireless application. Host-nation vendor equipment that is used out-of-the-box by anyone must be approved before use for company applications.

The WLAN is still considered an emerging technology. Several technologies (Fast Ethernet-Gig E, Cell Telecommunications) are in competition with this new technology and it is not determined that this technology wins out in any particular situation. It has promise and with faster data rates and longer reliable operating distance. This new technology may become a more

important player as these characteristics improve. All new implementations must meet minimum current standards of 3DES for security and 100mw at 2.4 GHz frequency requirements.

The WLAN can't send or receive signals over much larger areas than that of traditional wired media such as twisted-pair, coaxial cable, and optical fiber optic (FO). In terms of privacy, therefore, the WLAN have a much larger area to protect. To utilize security, the IEEE 802.11group have to organize their work with the IEEE 802.10 standards committee accountable for developing security mechanisms for all IEEE 802 LAN series (Geier, 1999).

Security mechanisms in IEEE 802.11b networks should be equivalent to existing mechanisms in wire-based networks. Traditional wired network jacks are located in buildings already protected from unauthorized access through the use of keys, badge access, facial recognition, finger printing and so forth. A customer must gain physical access to the network building in order to plug a client computer into a network jack. In contrast, a WLAN AP that is configured incorrectly may be accessed from off the grounds (for instance, from a parking lot next to the building). Properly designed WLAN secure access to the APs and isolate the APs from the internal private network prior to user authentication into the company network domain (Vector, 2000).

Empowering the customer with the ability to access a large quantity of information and services from WLAN equipment will create a new battleground. The WLAN industry will fight to provide their customers with sophisticated and value added services. As WLAN technology becomes a more secure and trusted channel by which customers may conduct their financial affairs, the market for WLAN will become even more lucrative.

Analysis

Advantages

- The WLAN Internet connectivity is great for any company whose site is not conducive to LAN wiring because of building or budget limitations, such as older buildings, leased space, or temporary sites.
- While the initial investment required for WLAN hardware can be higher than the cost of traditional wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
- The WLAN concept ensures the Internet customer, web-served mobile communication and field service productivity, the benefits of wireless communications sooner, and hard-dollar savings quicker than from any other commercial equipment available today. WLAN can provide network hardware for in-building and building-to-building data networks, as well as mobile communication equipment for information capture and display.
- WLAN mobility, i.e., a student attending class on a campus accesses the Internet, accesses information, information exchanges, and learning.
- Senior executive officers, managers can present their briefings using WLAN without carrying the data files, charts, and any storage equipment.
- Trade show and branch office workers minimize setup requirements with central database thereby increasing productivity.

- Most WLAN equipment is plug-and-play. This will help to reduce the total cost to include vendor technical installation, equipment maintenance and to eliminate equipment redundancy in case of system crash.
- WLAN technology allows the network to go where regular wire cannot go.
- The WLAN was clearly better then wired in setup/teardown time and effort.

Disadvantages

- Due to the limited bandwidth, the WLAN technology cannot support Video Teleconference (VTC). However, experts believe that WLAN will support VTC within the next five years.
- Due to the security reason, using the WLAN equipment as a contingency model is not recommended.
- The WLAN operated within typical wired LAN parameters provides less downtime and an increased invisibility to the customer.
- The WLAN technology also have obvious potentials in customer mobility and configuration changes significantly worse then wired in the risk of jamming, in the potential for interference, and in the detection of customer location.
- The WLAN is not capable to download and upload large data files.
- The WLAN is significantly worse then wired in the risk of jamming, potential for inference, and in the detection of RF signal.
- Products from different WLAN manufacturers are often incompatible with each other.
- Interference from friendly network will likely effect WLAN operation as the popularity of this industry increases.
- The WLAN equipment is not capable of sending and receiving data successfully during field exercises in case of heavy fog or dust storm.
- The WLAN equipment have difficulties at time in sending and receiving data when a flying object passes over a WLAN field exercise.
- If too many people or businesses in the same area have WLAN, then the band of air that they transmit signals on can become overloaded. Problems with signal interference are already happening and there are no doubts that the airwaves will become overloaded (Dunne, 2001).
- Most office environment and modern homes are constructed of materials that are relatively "translucent" to radio waves at 2.4 GHz so the range will not be greatly limited, however they do tend to present very reflective and refractive environments and the ultimate limitations will probably be caused by severe "multipath" problems.
- The problem has been the lack of interoperability among WLAN products from different manufacturers. The classic Ethernet 802.11 standard was ignored in developing current WLAN products (Seymour 2000).
- The WLAN weakness is susceptibility to many forms of external interface and the cost of transmitting stations. In addition, United States, international authorities and treaties strictly regulate most of the bands that can support high-speed communication. Use of these bands requires an expensive license (Burd, 1998).

Conclusion

The architecture provides customers with a logical migration path to IP-based networking for achieving peer-to-peer and non-hierarchical communication while maintaining interpretability with the existing infrastructure. This architecture permits the partition of customer and the LAN network, enabling network managers the flexibility for deploying end-customer services and applications independent of wireless switch manufacturers. The Wireless architecture will provide the framework for innovative technology enhancements. It's important to look at the interoperability between different wireless technologies and the interfaces with one another.

Wireless manufacturers are adopting standards and conflicts could result from the use of different standards in equipment in the same area. The current use of cell phones is different from that of a WLAN; phones have higher power and lower bandwidth equipment than a WLAN. The WLAN has a limited range, but it can be used as an extension of a wired LAN. Those two can co-exist on the same network. As far as multiple standards go, there is IEEE 802.11a, which specifies 25mb/s at 5ghz and IEEE 802.11b, which specifies 11mb at 2.4ghz, and Home RF, which is at 1mb/s and could be raised to10mb/s. It is not clear which standard will be adopted in the WLAN market, but once one is developed, prices will fall as chipmakers develop specific ICs around the standards, and the FCC may open a spectrum bandwidth and faster equipment, for WLAN manufactures per cost, see figure 7.

Today, the WLAN has redefined what it means to be connected. It has stretched the limits of the LAN. It makes an infrastructure as dynamic as it needs to be. It's only just beginning, the IEEE standard is less than three years old, with the high speed IEEE 802.11b yet to reach its first birthday. With standard and interoperable WLAN products, LAN can reach scales unimaginable with a wired infrastructure. They can make high-speed interconnections for a fraction of the cost of traditional wide area technologies. In a WLAN world, customers should be able to roam not just within a campus but within a city, while maintaining a high speed link to extranets, intranets, and the Internet itself. The future of WLAN is imminent (OCBN 2001).

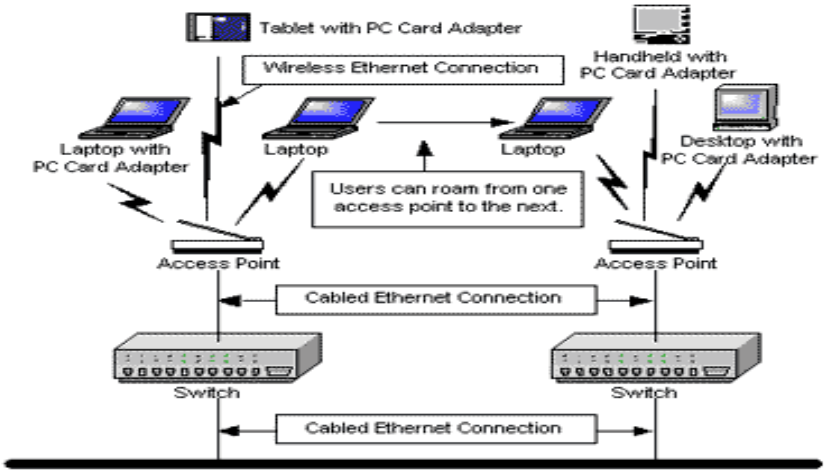

Figure 10, WLAN Architecture, source Smart Home Forum (2001)

The WLAN is “plug and play” equipment, open architecture built around a customary expensive wired LAN to eliminate interoperability problems. The WLAN architecture will serve as a reference to facilitate the efficient and effective coordination of common business process, technology, information flow, systems and investments among companies.

A proper WLAN architecture framework provides a structure to develop, maintain and implement an excellent operation environment and supports implementation of automated information systems, see figure 10 on WLAN architecture. The Intel personal Internet client architecture has been designed to keep pace with the arrival of next generation WLAN equipment and with the notion that hardware and software must be allowed to develop in parallel. The WLAN architecture will allow applications to be written to re-programmable microprocessors.

Data-rich applications and Internet content, including streaming audio and video (VTC), put intense demands on the data processing capabilities of handheld equipment, making re-programmable microprocessors more appropriate for the job. A preliminary requirement detailing the architecture has been distributed to key WLAN manufacturing companies, and a final specification and software developer kit will be accessible to the industry in the very near future (Johnson, 2000).

Today important emphasis on WLAN end-user satisfaction continues to encourage a departmental shortsightedness, creating vertical systems with their own proprietary data, software, and technology components (Cook, 1996).

In my opinion, WLAN technology is offering great opportunities for remote connectivity for in-door small businesses and for families connecting their PCs at home. However, the WLAN technology is not ready yet to offer to the big companies building-to-building or out in the field solutions due to numerous reasons that I stated earlier in my paper, these reasons are; range limitation, frequency availability, cost effective, bandwidth size, and security access. Once all of those challenges are resolved and meet the standard, the WLAN business will be ready to operate for any company size and for any mission anywhere in Europe. Today communication business requires VTC sessions, as well ability to upload and download large briefing slides and data. The WLAN technology can’t support the requirements. The WLAN manufacturers need to look at these features while trying to keep their product cost under control. Also, security is the most important element in communication networks today, and companies in Europe would not hesitate to spend the extra money to use the traditional wired LAN if the WLAN technology can’t support it. True, the traditional wired LAN costs more money to install hard wires inside the building and to lease a dedicated line from building-to-building. Doing that gives customers guarantee that their data will not be compromised. I predict that until the WLAN industry must work harder to get end-user satisfaction by resolving disadvantages, technical issues and the challenges.

Bibliography

Bednzrs, A. (2002), Growing pains slow wireless CRM rollouts, Network World, 18(45). p. 18.

Burd, D. (1998), Systems Architecture, (2nd edition), Course Technology.

Buy Domains. "Wireless LAN"
http://www.integrationwireless.com/IWWhitepaper.doc (2002).

Cisco Systems. "What is Wireless Local Area Networking"
http:// www.ocbn.com/MFG/CISCO/what_is_wireless_net.html (2002).

Conover, Joel. "Anatomy of IEEE 802.11b Wireless"
http://www.networkcomputing.com/1115/1115ws2.html (2000).

Cook, M (1996), Building Enterprise Information Architectures, Prentice Hall, p. 43

Dunne, D. "What is a Wireless LAN, Darwin Net"
http://europe.cnn.com/2001/TECH/ptech/05/10/what.is.WLAN.idg (2001).

Frank, Alan. "Wireless LANs Up-shift 10 11 Mbps"
http://www.networkmagazine.com/article/DCM20000426S0002 (2002).

Geier, J. "Overview of the IEEE 802.11 Standard, Wireless-Nets, Ltd"
http://www.wireless-nets.com/whitepaper_overview_80211.htm (2002).

Johnson, M. "IDG News Service\Washington Bureau" Intel Unveils Wireless architecture
http://www.idg.net/english/crd_intel_250266.html (2002).

NDC communications, Inc. "Wireless LAN System – Technology & Specification"
http://www.ndclan.com/Wireless/wlanW1.htm (1999),

Nouveau Solutions, "What is a Wireless LAN?"
http://www.cease-wire.co.uk/whatis.htm

O'Brien, J. A. (1999). Management Information Systems, (4th Edition). Irwin McGraw-Hill

OCBN, Inc. "What Is Wireless Local-Area Networking"
http://ocbn.com/MFG/CISCO/what_is_wireless_net.html (2001).

Palazzo, Anthony. "Wireless Communication Online", The guide to the Wireless World.
http://www.wireless-communication.org/ (2002).

Proxim. "Wireless distance", What is a Wireless LAN.
http://www.proxim.com/learn/library/whitepapers/wp2001-06-what.html (1998).

Seymour, J. "Lucent's Wirless LAN Play, The Solutions Group"
http://www.thestreet.com/comment/techsavvy/895571.html (2000).

Smart Home Forum. “Wireless LAN, Founder & Sponsor Intellicom Innovation” http://www.smarthomeforum.com/wlan.shtml (2001).

Stamper, D. A. (1999). Business Data Communications, (5th Edition), Addison-Wesley.

Vectors White Papers. “Deploying 802.11b (WI-FI) in the Enterprise Network”. http://www.dell.com/us/en/gen/topics/vectors_2001-wireless_deployment.htm (2001).

Wheeler T. ”Welcome to access wireless , CTIA’s World of Wireless Communications” http://www.wow-com.com/consumer/faqs/faq_general.cfm#one (2002).

WLANA papers. “What is WLAN? Wireless LAN” http://www.pulsewan.com/data101/wireless_lan_basics.htm (2000).

Glossary

Access Point : A hardware equipment that transports data between a wireless network and a wired network

HR: High-rate

IEEE 802.X: A set of specifications for Local Area Networks from The Institute of Electrical and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks. The 802.11 committee completed a standard for 1 and 2 Mbps WLAN in 1997 that has a single MAC layer for the following physical-layer technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infrared. IEEE 802.11 HR, an 11 Mbps version of the standard is expected to be completed by the end of 1999.

Independent network: A network that provides (usually temporarily) peer-to-peer connectivity without relying on a complete network infrastructure.

Infrastructure network: A wireless network centered about an AP. In this environment, the AP not only provides communication with the wired network but also mediates wireless network traffic in the immediate neighborhood.

IR: Infra Red

ISA: Information Systems Architecture

IR: infrared radiation

ISM: industrial, scientific and medical

LOS: line-of-sight

MAC: access control

MIB: Management Information Base

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

Multipath: The signal variation caused when radio signals take multiple paths from transmitter to receiver.

PPP: point-to-point

Radio Frequency (RF) Terms: GHz, MHz, Hz: The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One Mega-Hertz (MHz) is one million Hertz. One Giga-Hertz (GHz) is one billion Hertz. For

reference: the standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55 -1.6 MHz, the FM broadcast RF band is 88-108 MHz, and microwave ovens typically operate at 2.45 GHz.

RF: Radio Frequency

Roaming: Movement of a wireless node between two microcells. Roaming usually occurs in infrastructure networks built around multiple APs.

SS : Spread Spectrum

VTC: Video Teleconference