JITTA
JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

HARNESSING THE POTENTIAL OF WIRELESS LOCAL AREA NETWORKS

HEMANT K. SABAT, Sabre Holdings
Dallas, Texas, USA. Email: Hemant.K.Sabat.2000@alumni.indiana.edu

ABSTRACT

Wireless Local Area Networks (WLANs) are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers. In this paper, the author has discussed the current state, the value proposition and the future potential of WLANs under four broad heads: business applications, technology options, network topologies, and prevalent industry standards.

INTRODUCTION

Mobile computing can be performed within the confines of a corporate or campus environment as well as over longer distances with the assistance of wireless bridges like cellular phones or WLAN services. A WLAN is a flexible, on-premise data communication network system implemented as a supplement, extension, or alternative to a wired Local Area Network (LAN; see Glossary of terms in Table 1) within a building or campus. Portable PCs or notebooks equipped with their own WLAN adapters can allow users to log onto a LAN infrastructure merely by getting within the range of a server-based WLAN adapter or wireless hub (Goldman 1998; Rupley 1999).

This paper discussed WLANs from the following three perspectives:

- The current state of WLANs
- The value proposition of WLANs
- The future potential of WLANs

THE CURRENT STATE OF WLANS

WLANs use radio or infrared electromagnetic waves to communicate information from one point to another without relying on any physical connection. WLANs consist of a number of nodes, or stations (STAs), that use a wireless interface to communicate with other nodes and with Access Points (APs; see Table 1) that connect WLANs with wired media. A WLAN tunes in (or selects) one radio frequency while rejecting all other radio signals on different frequencies. The primary standard governing this relatively new technological phenomenon was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in 1997.

Sabat, H.K., “Harnessing the potential of Wireless Local Area Networks ,” *The Journal of Information Technology Theory and Application (JITTA),* 2:2, 2000, pp. 13-29.

Table 1. Glossary of Items

Access Point

A device that transports data between a wireless network and a wired network infrastructure.

Ad hoc network or Basic Service Set (BSS) or Independent WLAN

An ad-hoc network is a simple network where communications are established between multiple stations or Basic Service Sets (BSSs) in a given coverage area without the use of an access point or server.

Authentication

Authentication is the means by which one station is verified to have authorization to communicate with a second station in a given coverage area. Authentication can be either Open System or Shared Key. In an Open System, any wireless node may request authentication. The receiving node either has authority to grant authentication to requests from any node, or to grant authentication only to requests from a select list of nodes. In a Shared Key system, a node must have an encrypted key in order to have its requests authenticated.

Basic Service Set or Independent WLAN

A Basic Service Set (BSS) consists of two or more wireless nodes, or stations (STAs), which have recognized each other and have established communications.

Client/server network or Extended Service Set (ESS)

The client/server network uses an AP that controls the allocation of transmit time for all stations and allows mobile stations to roam from cell to cell. An ESS consists of a series of overlapping BSSs (each containing an AP) connected together by means of a Distribution System (DS).

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

CSMA/CA requires each station to listen for other users. If the channel is idle, the station may transmit. However, if it is busy, each station waits until transmission stops, and then enters into a random back off procedure. This prevents multiple stations from seizing the medium immediately after completion of the preceding transmission.

Encryption

Encryption is intended to provide WLANs with a level of security comparable to that of wired LANs. Wired Equivalent Privacy (WEP) encryption from RSA Data Security, Inc. was selected because it meets the following criteria:

- Reasonably strong encryption
- Self-synchronizing
- Computationally efficient
- Exportable
- Optional
- Timing and Power Management

ETSI

European Telecommunications Standards Institute, headquartered in Southern France, is a governing body that works closely with the International Telecommunications Union. The website for this group is http://www.etsi.org/. Working with Broadband Radio Access Network to develop standards for 54 Mbps WLANs in the 5GHz band that would work integrate voice, data, and video transmission across ethernet, IP or ATM platforms.

Table 1. Glossary of Items (Continued)

IEEE 802.X

A set of specifications for Local Area Networks (LAN) from The Institute of Electrical and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5 the specification for token ring networks. There is an 802.11 committee working on a standard for 1 and 2 Mbps WLANs. The standard will have a single MAC layer for the following physical-layer technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infrared (IR). Draft versions of the specification are in process.

HiperLan2 Global Forum

Bosch, Dell, Ericsson, Nokia, Telia and Texas Instruments have joined to form a consortium to promote the adoption of HiperLAN2 as the global broadband wireless technology in the 5 GHz band. This group is using a standard developed by the ETSI BRAN group, and hopes this will integrate with 3G mobile wireless and many types networking equipment, like ATM and ethernet. www.hiperlan2.com

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 access point. In this environment, the access point not only provides communication with the wired network but also mediates wireless network traffic in the immediate neighborhood.

Local Area Network (LAN)

A LAN is a combination of hardware and software technology that allows computers to share a variety of resources such as: printers and other peripheral devices, data, application programs or storage devices. LANs also allow messages to be sent between attached computers, thereby enabling users to work together electronically in a process often referred to as collaborative computing. In general, LANs are confined to an area no larger than a single building or a small group of buildings. LANs can be extended by connecting to other similar or dissimilar LANs, to remote users or to mainframe computers. This process is generally referred to as LAN connectivity or internetworking.

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, 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.

Network Operating Systems (NOSs)

Network Operating Systems is concerned with providing an interface between LAN hardware, such as network interface cards, and the application software installed on a particular client or server. The job of NOS is to provide transparent interoperability between client and server portions of a given application program.

Table 1. Glossary of Items (Continued)

Roaming

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

Wireless Node or station (STA)

A user computer with a wireless network interface card (adapter).

Wireless Ethernet Compatibility Alliance (WECA)

WECA's mission is to promote the IEEE 802.11 High Rate Standard for applications in the enterprise, home, and small office and to provide certification of interoperability. To make this promise a reality, WECA has developed a strict compliance matrix and has commissioned an independent test lab.

Wireless LAN-LAN bridge

A wireless LAN-LAN bridge is an alternative to cable that connects LANs in two separate buildings.

Wireless Local Area Network (WLAN)

A WLAN is a flexible, on-premise data communication network system implemented as a supplement, extension, or alternative to a wired LAN within a building or campus.

Wireless Personal Area Network (WPAN)

A WPAN typically covers the few feet surrounding a user's work space and provides the ability to synchronize computers, transfer files, and gain access to local peripherals.

Wireless Metropolitan Area Network

A WMAN is a packet radio often used for law-enforcement or utility applications.

Wireless Wide Area Network

A WWAN is a wide-area data transmission over cellular or packet radio. These systems involve costly infrastructures, provide much lower data rates, and require users to pay for bandwidth on a time or usage basis.

Wireless Local Area Network Alliance (WLANA)

WLANA is a non-profit educational trade association, comprised leading WLAN vendors. WLANA provides information about wireless local area networking applications, issues and trends. WLANA's website (http://www.wlana.com/) includes industry studies, white papers, case studies of WLAN applications, and links to related topics and member web sites.

This section describes the following:

- Business applications of WLANs
- The basic components, the underlying radio technology options of WLANs and how WLANs differ from other wireless technologies
- The network topologies/configurations (how WLANs operate independently as well as integrate with wired network infrastructure)
- Handling of multiple access
- The factors that customers must consider when evaluating WLANs to fulfill the needs of their business applications
- Issues concerning network security

Business applications of WLANs

As a general-purpose connectivity alternative for a broad range of business customers, WLANs have gained strong popularity in a number of vertical markets, including the health-care, retail, manufacturing, production/warehousing, and academic arenas (Total Telecom, 1999). Table 2 summarizes the use of WLAN in a range of industry sectors. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing (Ruber 1999).

How WLANs operate

WLANs use electromagnetic waves (radio and infrared) to communicate information from one point to another without relying on any physical connection. The data being transmitted is superimposed on the radio carrier (i.e., radio carrier is modulated by the information) so that it can be accurately extracted at the receiver. Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. A WLAN tunes in (or selects) one radio frequency while rejecting all other radio signals on different frequencies.

WLAN technology options

Two technologies commonly used in WLANs are radio frequency (RF) and infrared frequency (IRF). RF can be based on either narrowband or spread spectrum technology. A narrowband radio system transmits and receives user information on a specific radio

Table 2. Business Applications of WLANs

Health care	Doctors and nurses in hospitals are more productive because hand-held or notebook computers with WLAN capability deliver patient information instantly. WLAN will allow health care professional to make use of mobile handheld computers to input and access patient information real-time. This will help to eliminate any duplicate or outdated information as well as any treatment delays.
Consulting	Consulting or accounting audit engagement teams or small workgroups increase productivity with quick network setup.
Education	WLANs facilitate convenient untethered access to information. The usage of notebook computers has been very popular lately for many Universities. WLAN will be able to fully leverage of such mobile connectivity to allow a more fluid connection by students.
Older buildings	WLAN installation is much less invasive than LAN installation. This is valuable when historical preservation and aesthetics are important. Also, LAN installation is more likely to release asbestos or other unsafe materials into the environment. Network managers installing networked computers in older buildings find that WLANs are a cost-effective network infrastructure solution.
Retail	Stores use WLANs to simplify frequent network reconfiguration, monitor inventories, and provide shoppers with point-of-purchase product information. Food orders can be input directly from the table while retail outlets will be able to set up extra registers during peak seasons.
Satellite offices & trade show	WLANs minimize setup requirements by allowing network managers to install pre-configured networks.
Warehouse & production facilities	Workers use WLANs to exchange information with central databases and increase their productivity. Portable terminals are used for real-time stock count and inventory tracking. With the assistance of barcode reader, the wireless data links are used to locate and maintain pallets and boxes locations.
Backup for wired LANs	WLANs can provide backup for mission-critical applications running on wired networks.
Network management	Network managers in dynamic environments minimize the overhead of moves, adds, and changes with WLANs, thereby reducing the cost of LAN ownership. Network managers implement WLANs to provide backup for mission-critical applications running on wired networks.
Training	Training sites at corporations and students at universities use wireless connectivity to facilitate access to information, information exchanges, and learning.
Executive information	Senior executives in conference rooms make quicker decisions because they have real-time information at their fingertips.
Corporate	With a WLAN system, corporate employees can take advantage of mobile networking for web browsing, email and file sharing within the office
Manufacturing shop floor	WLAN will help shop floor workstation to communicate with the company main network. This is especially so where the workstation need to be mobile.
Building-to-building	It is often more economical to use a wireless bridge between buildings rather than physically laid cable or telecommunication lines.
Finance	Using handheld PC, financial traders are able to receive up-to-date financial information. It is helpful when the trader has to be mobile.

frequency. Narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. On the other hand, spread spectrum is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. More bandwidth is consumed than in the case of narrowband transmission. The receiver knows the parameters of the spread-spectrum signal being broadcast. Spread Spectrum can use either Direct Sequence Spread Spectrum (DSSS) or a Frequency Hopping Spread Spectrum (FHSS) technique to transmit data. FHSS uses a narrowband 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. DSSS generates a redundant bit pattern (called chipping code or chip) for each bit to be transmitted. The longer the chip, the greater the probability that the original data can be recovered (and the more bandwidth required). Infrared (IR) systems use infrared frequencies in the electromagnetic spectrum to carry data. IR system use either directed (line-of-sight) or diffuse technology (Table 3). Inexpensive directed systems provide very limited range (3 feet) and typically are used for Personal Area Networks (PANs) but occasionally are used in specific WLAN applications. Diffuse technology-based WLAN systems do not require line-of-sight, but cells are limited to individual rooms.

Standards, media access and network topologies

Standards and media access

Table 4 summarizes key currently approved standards for WLANs. The majority of these standards were developed by European Telecommunications Standards Institute (ETSI; see Table 1).

Table 3. Technology options for WLANs

(A) Radio frequency (RF)	There are two variations of the RF technology: narrowband and spread spectrum.
(1) Narrowband	A narrowband radio system transmits and receives user information on a specific radio frequency. Narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. Undesirable crosstalk between communications channels is avoided by carefully coordinating different users on different channel frequencies. Privacy and noninterference are accomplished by the use of separate radio frequencies. The radio receiver filters out all radio signals except the ones on its designated frequency. The global spectrum allocation for radio technology at 2.4 GHz is as follows: *Region* *Allocated Spectrum* US 2.4000 - 2.4835 GHz Europe 2.4000 - 2.4835 GHz Japan 2.471 - 2.497 GHz France 2.4465 - 2.4835 GHz Spain 2.445 - 2.475 GHz
(2) Spread spectrum	It is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. More bandwidth is consumed than in the case of narrowband transmission. The receiver knows the parameters of the spread-spectrum signal being broadcast. There are two types of spread spectrum radio: frequency hopping and direct sequence. *(1) Frequency Hopping Spread Spectrum (FHSS)* FHSS uses a narrowband 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. *(2) Direct Sequence Spread Spectrum (DSSS)* DSSS generates a redundant bit pattern (called chipping code or chip) for each bit to be transmitted. The longer the chip, the greater the probability that the original data can be recovered (and the more bandwidth required).
(B) Infrared frequency (IRF)	Infrared (IR) systems use infrared frequencies in the electromagnetic spectrum to carry data. These systems use either directed (line-of-sight) or diffuse technology. *(1) Directed (line-of-sight) IRF technology* Inexpensive directed systems provide very limited range (3 feet) and typically are used for Personal Area Networks (PANs) but occasionally are used in specific WLAN applications. High performance directed IR is impractical for mobile users and is therefore used only to implement fixed sub-networks. *(2) Diffuse (or reflective) IRF technology* These WLAN systems do not require line-of-sight, but cells are limited to individual rooms.

Table 4. Approved WLAN standards

Country	*Approved standards*	*Documents*	*Approval authority*
Europe	European Telecommunications Standards Institute	ETSI 300-328, ETSI 300-339	National Type Approval Authorities
France	La Reglementation en France por les Equipements fonctionnant dans la bande de frequences 2.4 GHz "RLAN-Radio Local Area Network	SP/DGPT/ATAS/23, ETSI 300-328, ETSI 300-339	Direction Generale des Postes et Telecommunications
Japan	Research and Development Center for Radio Communications (RCR)	RCR STD-33A	Ministry of Telecommunications (MKK)
North America	Industry Canada (IC), Canada Documents: GL36 Federal Communications Commission (FCC), USA	CFR47, Part 15, Sections 15.205, 15.209, 15.247.	Industry Canada (Canada), FCC (USA)
Spain	Supplemento Del Numero 164 Del Boletin Oficial Del Estado (Published 10 July 91, Revised 25 June 93)	ETSI 300-328, ETSI 300-339	Cuadro Nacional De Atribucion De Frecuesias

Note: Operation in countries within regions outside Japan or North America, may be subject to additional or alternative national regulations.

The IEEE 802.11 standard

Seeking to provide a uniform set of standards that enable interoperability among WLAN products from different vendors, IEEE has formulated a standard—the IEEE 802.11. The IEEE 802 Standards Committee formed the IEEE 802.11 WLAN Standards Working Group in 1990. The membership of the committee consists of individuals from a number of companies and universities, who research, manufacture, install and use products in WLAN network applications. Manufacturers of semiconductors, computers, radio equipment, WLAN systems solution providers, University research labs and end-users make up the core group. The Working Group consists of companies from the United States, Canada, Europe, Israel and the Pacific Rim. The IEEE 802.11 Working Group took on the task of developing a global standard for radio equipment and networks operating in the 2.4 GHz unlicensed frequency band. Currently, IEEE 802.11 supports 1 Mbps data rates for FHSS, and both 1 Mbps and 2 Mbps for DSSS. The standard does not specify technology or implementation; it states the specifications for Physical and Media Access Control (MAC; see Table 1) layers of the Open Systems Interaction (OSI) model. The IEEE 802.11 Working Group has completed the standard in 1997. More details on the 802.11 specification can be obtained from the IEEE P802.11 Working Group site (IEEE P802.11 Working Group 1999).

Media access. WLAN accesses the shared media or the network through Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA; see Table 1) protocol. The standard also enables WLAN users to roam between WLAN transmission ranges without interruption—a feature currently not offered by all vendors.

Ad hoc standards - WLAN Interoperability Forum (WLAN Forum). The IEEE 802.11 Working Group has been working to develop higher speed standards in the 2.4 GHz and 5 GHz frequency bands. However, due to the long-time shortcoming of the WLAN standardization, many vendors have already developed their proprietary standards. WLAN Interoperability Forum (WLAN Forum) is one of the multi-vendor consortiums (Wireless LAN Interoperability Forum 1999). The WLAN Forum is funded by Hewlett-Packard, IBM, Motorola and Sharp. The Forum provides a standard called OpenAir, which offers standards for data communications, roaming, set up, security, configuration and coexistence. OpenAir is interoperable with IEEE 802.11.

Ad hoc standards - Wireless Ethernet Compatibility Alliance (WECA). Recently, 3Com, Aironet, Intersil, Lucent and Nokia announced the formation of Wireless Ethernet Compatibility Alliance (WECA) to facilitate adoption of high-speed WLAN networking. The WECA, claiming to be compliant with

IEEE 802.11 High Rate standard, is working towards multi-vendor interoperability within the same wireless infrastructure. However, the new consortium may produce another ad hoc extended standard.

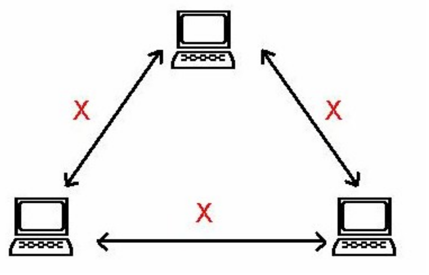
Ad hoc standards - Bluetooth. Bluetooth is an ad hoc industry technical standard for wireless devices (Judge 1999; Mitchell 20000; Ruber 1999). It has been developed by its Special Interest Group, which is founded by Ericsson, Lucent, IBM, Intel, Nokia, and Toshiba. Bluetooth is a short-range radio technology that allows high-speed data transmission between devices like mobile phones, Personal Digital Assistants (PDAs). It is aimed at instant data exchange and other communications among Net devices, and between devices and the Internet. However, Bluetooth is competing with WLAN standards since its technology can be applied to connection of PCs, mobile phone and other peripherals.

Challenges. The existence of these ad hoc standards, in addition to IEEE 802.11, is influencing customers' investment decisions in WLAN technology. This has set a premium on interoperability among these standards. More importantly, the industry itself might encounter confusion due to these multiple standards. These two forces have the potential to stall the accelerated growth of WLAN technology thereby reducing the use of full potential of this technological phenomenon.

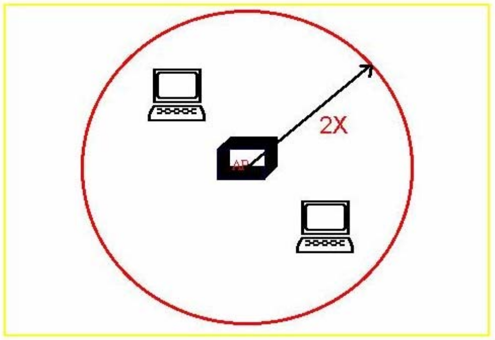
Network topologies

The standard defines protocols for two ypes of networks: ad hoc and client/server networks.

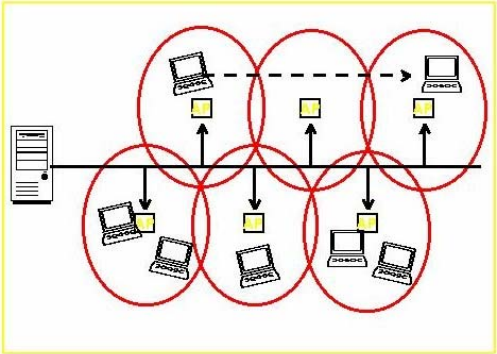
Ad hoc network (or Independent Basic Service Set or Independent WLAN). In an ad hoc network, communications are established between multiple nodes or STAs, or Basic Service Sets (BSSs), in a given coverage area without the use of an AP or server (Figure 1). Two or more wireless nodes use wireless adapters to communicate as peers within a shared cell coverage area.



Extended-range independent WLANs. The range of an ad hoc WLAN can be extended using an AP that functions as a repeater (Figure 2). The main function of the AP is to form a bridge between wireless and wired LANs. The AP is analogous to a base station used in cellular phone networks. When an AP is present, stations do not communicate on a peer-to-peer basis. All communications between stations or between a station and a wired network client go through the AP. APs form part of the wired network infrastructure; they are not mobile. A BSS in this configuration is said to be operating in the infrastructure mode (Table 1).



Client/server network (or Extended Service Set). In a client/server network, an AP controls the allocation of transmission time for all network nodes and allows mobile nodes (such as laptop computers) to roam freely from cell to cell. The network consists of a series of overlapping APs (Figure 3). The APs route data among nodes and between nodes and servers, ensuring the coordination of data traffic. These overlapping APs form a Distribution System (DS), which is typically built on an Ethernet LAN backbone.



Security

IEEE 802.11 provides for security via two methods: (i) authentication, and (ii) encryption.

Authentication. Authentication is the means by which one station is verified to have authorization to communicate with a second station in a given coverage area. In the infrastructure mode, authentication is established between an AP and each station.

Authentication can be either Open System or Shared Key. In an Open System, any STA may request authentication. The STA receiving the request may grant authentication to any request, or only those from stations on a user-defined list. In a Shared Key system, only stations which possess a secret encrypted key can be authenticated. Shared Key authentication is available only to systems having the optional encryption capability.

Encryption. Encryption is intended to provide a level of security comparable to that of a wired LAN. The Wired Equivalent Privacy (WEP) feature uses an algorithm from RSA Data Security, Inc. The WEP algorithm was selected to meet the following criteria:

- reasonably strong
- self-synchronizing
- computationally efficient
- exportable
- optional

Timing and power management

All station clocks within a BSS are synchronized by periodic transmission of time stamped beacons. In the infrastructure mode, the AP serves as the timing master and generates all timing beacons. Synchronization is maintained to within four microseconds plus propagation delay (or latency).

Timing beacons also play an important role in power management. Two power saving modes are defined: awake and doze. In the "awake" mode, stations are fully powered and can receive packets at any time. Nodes must inform the AP before entering doze. In the "doze" mode, nodes must "wake up" periodically to listen for beacons, which indicate that AP has queued messages.

Roaming

The standard identifies the basic message formats to support roaming, but everything else is left up to network vendors. (Roaming is movement of a wireless node between two microcells. Roaming usually occurs in infrastructure networks built around multiple access points.) In order to fill the void, the Inter-Access Point Protocol (IAPP) was jointly developed by Aironet, Lucent Technologies, and Digital Ocean. Among other things, IAPP extends multi-vendor interoperability to the roaming function. It addresses roaming within a single ESS and between two or more ESSs.

WLAN versus other wireless networks

WLAN configurations include independent networks, offering peer-to-peer connectivity, and infrastructure networks, supporting fully distributed data communications. Point-to-point local-area wireless solutions, such as LAN-LAN bridging and Personal Area Networks (PANs), may overlap with some WLAN applications but fundamentally address different user needs.

- A wireless LAN-LAN bridge (see Table 1) is an alternative to cable that connects LANs in two separate buildings.
- A Wireless Personal Area Network (see Table 1) typically covers the few feet surrounding a user's work space and provides the ability to synchronize

computers, transfer files, and gain access to local peripherals.

- A Wireless Metropolitan Area Network (see Table 1) is a packet radio often used for law-enforcement or utility applications.
- A Wireless Wide Area Network (see Table 1) is a wide-area data transmission over cellular or packet radio. These systems involve costly infrastructures, provide much lower data rates, and require users to pay for bandwidth on a time or usage basis. In contrast, on-premise WLANs require no usage fees and provide 100 to 1000 times the data transmission rate.

The value of WLANs

This section describes a decision matrix comparing wireless to wired LANs and the business value of WLANs. Table 5 compares the two technologies, WLAN and LAN, based on a variety of factors related to installation, cost, functionality, and maintenance. WLANs offer the following productivity, service, convenience, and cost advantages over traditional wired networks:

Table 5. Wired LANs versus WLANs

Factors	***Wired LANs***	***WLANs***
Mobility	Not to the same extent	Access to real-time information anywhere in their organization; this supports productivity and service opportunities
Installation speed and simplicity	More difficult and time-consuming to install	Fast and easy; eliminates the need to pull cable through walls and ceilings
Installation flexibility	The network, being tethered, is limited by the media accessibility	Wireless technology allows the network to go where wire cannot go.
Costs	Higher maintenance and support costs.	Initial investment required for WLAN hardware can be higher. Installation expenses can be significantly lower. WLANs eliminate the direct costs of cable installation. Netowork maintenance costs are reduced. WLANs can easily be transferred from one location to another, Scalability and flexibility of WLANs reduces user downtime and administrative overhead costs. Long-term cost benefits are greatest in dynamic environments that require scalability and flexibility.
Scalability and Flexibility	Not as easy to scale.	Configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed. Network managers can preconfigure entire networks before installing them at remote locations. Once configured, WLANs can be moved from place to place with little or no modification.
Security Considerations	Physical security User authorization and external eavesdropping Attacks from within network	Security considerations are similar to that of wired LANs. However, because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic. WLAN addresses security via authentication and encryption (see Glossary)
Range/coverage	Depends on wire media used.	Varies between less than 100 feet to more than 300 feet for an individual cell.

Table 5. Wired LANs versus WLANs (Continued)

Throughput	11 mbps is typical for a wired ethernet LAN, though maximum speeds can be close to gbps, depending on the network.	1 to 10 Mbps
Multi-path effects		Reflections of the signals can cause them to become stronger or weaker, which can affect data throughput.
Integrity and reliability	Wires can be tapped; physical damage to wires reduces reliability in data transfer.	Radio interference can cause degradation in throughput. Designs of proven WLAN technology and the limited distance over which signals travel result in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.
Interoperability	Easy interoperability.	Dependent on vendor's technology choice and method of implementation. Products from different vendors employing the same technology and implementation are typically interoperable.
Interference and co-existence	Less interference.	Other products that transmit in the same frequency spectrum can potentially interfere with a WLAN system.
Battery life for mobile platforms		WLAN vendors typically employ special design techniques to maximize the host computer's energy usage and battery life.
Safety		The output power of WLAN systems is much less than that of a hand-held cellular phone. Since radio waves fade rapidly over distance, users are exposed to very little radio frequency (RF) energy.

Range/coverage

The distance over which RF waves can communicate is a function of product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects can affect how energy propagates, and thus what range and coverage a particular system achieves. Most WLAN systems use RF because radio waves can penetrate many indoor walls and surfaces. The range (or radius of coverage) for typical WLAN systems varies from under 100 feet to more than 500 feet. Coverage can be extended. Roaming, which can be provided through microcells, can increase mobility.

Throughput

As with wired LAN systems, actual throughput in WLANs is dependent on products and set-up. Factors that affect throughput include airwave congestion (number of users), propagation factors such as range and multipath, the type of WLAN system used, as well as the latency and bottlenecks on the wired portions of the WLAN. Typical data rates range from 1 to 11 Mbps.

Multipath effects

A radio signal can take multiple paths from a transmitter to a receiver. This attribute is called multipath (see Table 1). Reflections of the signals can cause them to become stronger or weaker, which can affect data throughput. The effects of multipath depend on the number of reflective surfaces in the environment, the distance from the transmitter to the receiver, the product design and the radio technology.

Integrity

While radio interference can cause degradation in throughput, such interference is rare in the workplace. Robust designs of proven WLAN technology and the limited distance over which signals travel result in connections that are far more robust than cellular phone connections. So, WLANs provide data integrity performance equal to or better than wired networking.

Interoperability with wireless infrastructure

Several types of interoperability are possible between WLANs depending on technology choice and on the specific vendor's implementation. Products from different vendors employing the same technology and the same implementation typically allow for the interchange of adapters and access points. An eventual goal of the IEEE 802.11 specification is to allow compliant products to interoperate without explicit collaboration between vendors.

Interference and coexistence

The unlicensed nature of radio-based WLANs means that other products that transmit energy in the same frequency spectrum can potentially provide some measure of interference to a WLAN system. Microwave ovens are a potential concern. But most WLAN manufacturers design their products to account for microwave interference.

Another concern is the co-location of multiple WLAN systems. While co-located WLANs from different vendors may interfere with each other, others coexist without interference. Individuals are addressing this issue.

Simplicity/ease of use

Users need very little new information to take advantage of WLANs. Because the wireless nature of a WLAN is transparent to a user's Network Operating System (NOS; see Table 1), applications work the same as they do on tethered LANs. WLAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system. However, products are designed so that most users rarely need these tools. WLANs simplify many of the installation and configuration issues that plague network managers. Since only the APs of WLANs require cabling, network managers are freed from pulling cables for WLAN end users. Lack of cabling also makes moves, adds, and changes trivial operations on WLANs. Finally, the portable nature of WLANs lets network managers preconfigure and troubleshoot entire networks before installing them at remote locations. Once configured, WLANs can be moved from place to place with little or no modification.

Security

Because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. So, WLANs are more secure than most wired LANs. It is extremely difficult for unintended receivers (eavesdroppers) to listen in on WLAN traffic. Complex encryption techniques make it impossible for all but the most sophisticated to gain unauthorized access to network traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

Decreased cost of ownership

Intense competition and rapid technological advancements are driving organizations to cut costs and operate more efficiently. WLAN technology offers a cost-effective networking solution that minimizes large capital investments in wiring and cable infrastructure. According to a survey conducted by the Wireless Local Area Network Alliance (WLANA; see Table 1), the average total cost per user for a WLAN solution is $4,550 (ROI/Cost-Benefit Study 1999). However, organizations installing an average of 300 client cards reaped annual savings of up to $4.9 million, which translates into per user savings of $15,989. WLANs drive costs out of the system through easier installations that avoid construction and wiring in buildings.

Scalability

Wireless networks can support large numbers of nodes and/or large physical areas by adding APs to boost or extend coverage. WLAN installations are scalable and flexible because they are easily configured to serve as a standalone network or as a complement to installed wired LAN topologies. WLANs can be strategically placed throughout a network to provide connectivity in areas where wired

LANs simply cannot service. For example, due to the size and layout of some manufacturing warehouse facilities, forklifts contain wireless transmitters that enable drivers to gather and communicate information through laptop computers. Network managers have the flexibility to design wireless networks that are extremely simple or quite complex.

Battery life for mobile platforms

End-user wireless products are capable of being completely untethered, and run off the battery power from their host notebook or hand-held computer. WLAN vendors typically employ special design techniques to maximize the host computer's energy usage and battery life.

Safety

The output power of WLAN systems is very low, much less than that of a hand-held cellular phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a WLAN system. WLANs must meet stringent government and industry regulations for safety. No adverse health affects have ever been attributed to WLANs.

Increased mobility and network speed

The fundamental value proposition of a WLAN solution is that it enables mobility of the workforce. Computers and handheld devices access real-time information without a physical connection to an outlet. The benefits of mobility and speed are immense. For example, customer requests for information (such as an order status) are delivered in near-real time through WLAN speeds reaching 11 Mbps. At these rates, customers enjoy data transmissions rates equal in speed to some wired LAN environments. Inventory stocks are tracked and monitored more closely with the use of wireless scanners, avoiding stock outs and delivering customer satisfaction.

Rapid return on investment

With declining hardware prices and advancements in wireless networking, WLANs are an increasingly attractive alternative to LANs. Payback periods required to cover initial investment in WLANs average 6-12 months (Table 6).

Table 6. Return on investment from WLANs in industries

(In Millions)	*Retail*	*Manufacturing*	*Health-care*	*Office automation*	*Education*
Benefits per company ($)	5.6	2.2	0.94	2.5	0.5
Costs per company ($)	4.2	1.3	0.90	1.3	0.3
Payback (No. of months)	9.7	7.2	11.4	6.3	7.1

Source: "ROI/Cost-Benefit Study" conducted by WLAN Alliance.

The following are two case studies that describe how Ocean Spray and Indiana Statehouse (Kilgore 1999) have benefited from implementation of WLAN systems.

Ocean Spray: A case example

Ocean Spray operates several manufacturing warehouses. Each warehouse manufactures fruit juice and distributes Ocean Spray's full product line throughout regions of the country. Before the implementation of a WLAN, employees at the Kenosha, WI warehouse manually processed inventory and shipments made to and from the site. The manual process was labor-intensive and unreliable. Ocean Spray product delivered to the 300,000 square-foot facility required two full-time employees to survey the warehouse on foot for locations to store inventory. In addition, inventory-tracking procedures were entirely paper-based which generated high administrative costs and led to inaccurate inventory records.

When the managers of the Kenosha warehouse experienced a 15 percent increase in product volume and a 10 percent increase in stock keeping units (SKUs), they decided to implement a WLAN in the facility. Radio frequency data communication (RFDC) terminals were placed on every forklift in the building, allowing ease of communication with forklift operators. Every pallet and storage location was bar coded so that empty storage slots and incoming pallets could be matched electronically in near real-time.

Enormous productivity gains were achieved following the WLAN implementation. The system increased warehouse shipments by 1.8 million cases, while reducing the number of worker hours by 2,200. Productivity increased from 451 to 550 cases handled per worker. Further, inventory turns dramatically increased due to reductions in inventory levels made possible by 98 percent accuracy in inventory tracking.

Indiana Statehouse: A case example

In 1992, the Indiana Statehouse installed a WLAN to serve 150 users. A WLAN was chosen because it proved less costly to install than a wired LAN, and a WLAN did not compromise the need to preserve the historic architecture and aesthetics of the building's interior. The Statehouse elected to install a Digital Equipment Corporation WLAN system of ten Access Points connected with 10Base T cable. The WLAN uses Direct Sequencing Spread Spectrum (DSSS) transmission to support the network needs of 150 laptop computer users. The laptop computers are equipped with PCMCIA network interface cards called Roamabouts, which enable state legislators to remain connected to the network as they move from the Chambers to a committee room, and elsewhere throughout the building.

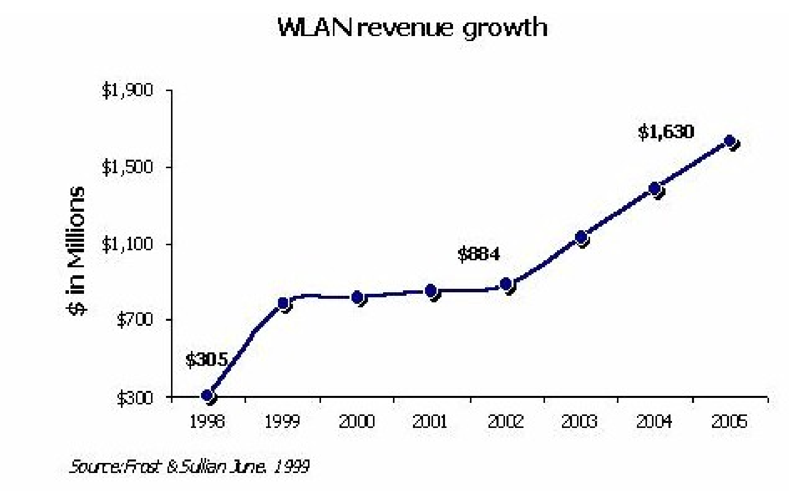
The Future Potential of WLANs

The future developments in the WLAN field will address the following issues:

- How to meet the demands for higher performance, higher data rates and higher bandwidths
- How to facilitate interoperability between WLAN products from different equipment manufacturers
- How to expand the WLAN applications horizontally

Future growth

Dan Mitchell (2000) projects the number of wireless users will be 1.1 billion by 2004. Strategy Analytics (2000) forecast the U.S. cellular penetration to be 80% (or 227 million) by 2005; at the end of 1999, it was 86 million. Not only this, according to the GartnerGroup, WLAN nodes comprise only a fraction of 1% of 43 million Ethernet nodes shipped today. Over the next ten years, this percentage is estimated to grow to between 5% and 10% of all Ethernet nodes. That is, a growth rate of 600% over the next ten years. Frost & Sullivan estimate that by 2005, WLAN industry will be worth $1.63 billion in annual sales (Figure 4). Growth will depend on three key factors: transmission speed, interoperability and standards compliance, and Internet demand (Gillooly 1999; Edwards 1999).



Source:Frost &Sullian June, 1999

Transmission rates, and interoperability among standards and technologies

Table 7 states the interdependence between transmission rates, and interoperability among standards and technologies (Ruber 1999).

The IEEE 802.11 WLAN standard is one of the first generations of standardization for WLAN networks. This standard will set the pace for the next generation standard, addressing the demands for higher performance, higher data rates and higher frequency bands. Because of bandwidth and device constraints, Jupiter Communications (1999) maintains that mobile access is not suited to using the Web as such, but rather to using narrowly customized data services that may be delivered over the Internet.

(i) With the creation of a dozen ad hoc standards, interoperability among WLAN products from different equipment manufacturers will be important to the success of the standard.

(ii) Currently, WLAN applications are mostly in vertical markets hospitals, education, and manufacturing. It is expected that many horizontal applications will follow as 802.11 network infrastructure is installed.

(iii) Over time, increase in demand for 802.11 products is expected to increase competition. This will make WLANs more efficient and economical for all applications requiring wireless connectivity. For example, the need for higher data rates, for applications requiring wireless connectivity at 10 Mbps and higher will force WLAN vendors to manufacture products that match the data rate of the majority of wired LANs.

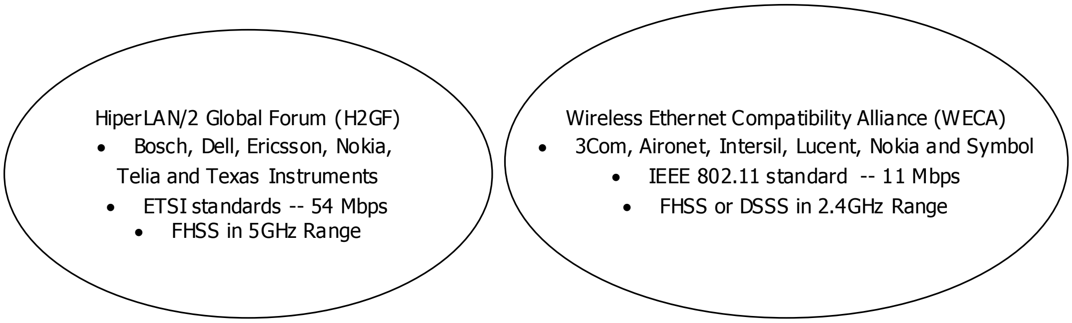
(iv) There is no current definition of the characteristics for the higher data rate signal. However, for many of the options available to achieve it, there is a clear upgrade path to maintain interoperability with 1 and 2 Mbps systems while providing a faster data rate as well. In the future, these upgrade paths will be refined to ensure complete compatibility across products from multiple vendors.

Today's WLANs transmit at 2 Mbps. This speed is low when compared to that of the wired counterparts. Transmission rates of 11 Mbps are appearing in the market. 24 Mbps WLAN products should be available within twelve months. A group of manufacturers, called the HiperLan2/Global Forum (H2GF), have joined together to develop a 54 Mbps model that works with ATM, Internet Protocol packets and Ethernet (CommunicationsWeek 1999; Moozakis 1999). This group uses a standard, which is developed by ETSI (Figure 5). It operates through FHSS in 5 GHz range (Dix 1999). By contrast, the IEEE standard uses the 2.4 GHz range. This standard allows for either FHSS or DSSS Ethernet. With two camps created, the immediate future of WLANs will be focused on negotiating and posturing for a dominant technology. Once these standards are settled and the faster transmission rates are available, the uses for WLANs will expand beyond their traditional segments towards a wider customer base.

Table 7. Transmission rates, interoperability and standards

Company	***Type***	***Planned technology***	***Standard***
Proxim	FHSS	24 Mbps	HiperLAN/2
Lucent	DSSS	2 Mbps add Turbo	IEEE 802.11
Aironet	DSSS	11-22 Mbps	IEEE 802.11
RadioLAN	Narrowband	10 Mbps - current	None uses unlicensed 5 GHz band
Nortel/Symbol	DSSS	11-24 Mbps Wireless Voice over IP	IEEE 802.11
Cisco		Coming soon	

Sources: Information for analysis and inference was obtained from http://www.symbol.com/, http://www.lucent.com/, http://www.nortel.com/, http://www.weca.cm/, http://www.radiolan.com/, http://www.proxim.com/, and Ruber, 1999.



HiperLAN/2 Global Forum (H2GF)

- Bosch, Dell, Ericsson, Nokia, Telia and Texas Instruments
- ETSI standards -- 54 Mbps
- FHSS in 5GHz Range

Wireless Ethernet Compatibility Alliance (WECA)

- 3Com, Aironet, Intersil, Lucent, Nokia and Symbol
- IEEE 802.11 standard -- 11 Mbps
- FHSS or DSSS in 2.4GHz Range

Most current WLANs are compatible only with Ethernet. New standards are emerging to make WLANs work with Asynchronous Transfer Mode (ATM), token ring, Fire Wire, and others (Mitchell 2000).

THE FUTURE RESEARCH

The future research will focus on improving transmission rates, developing standards for WLANs, interoperability of different standards and technologies, wireless Web access, among other things. Development of voice recognition technologies will make mobile transactions more ubiquitous. So, plentiful resources will be directed to this field of research.

Ricochet Mobile Internet Access: A case example

An example of how the Internet impacts the future of WLAN is seen with Metricom (Metricom 1996). This company offers Ricochet Mobile Internet Access. Ricochet operates in the unlicensed 902-928 MHz radio frequency, on streetlamps and other urban fixtures that transmit RF packets between user wireless modems and wired APs. These APs take the user directly to the Internet or company network. Offering Internet service to mobile PC users opens options to users who work in a variety of locations or who do not have consistent access to a wired phone line. This offering does not use either IEEE or ETSI standards. It is dependent on a checkerboard network of radio cells installed around a metropolitan area. However, Ricochet exemplifies a type of start-up company that can quickly implement a product while the larger players are occupied with speed and standards issues.

CONCLUSIONS

WLANs offer many technological and practical benefits. This technology provides mobility and sufficient scalability. Also, the freedom from physical connection between an AP and terminals reduces networking complexity and costs of ownership. Further, the benefit of wireless architecture eases network installation and shorten the installation lead-time.

However, delayed process of standardization in the industry has allowed the growth of multiple ad hoc standards in response to customers' demands. This has set a premium on interoperability between WLAN products. Another consequence has been the multi-directional growth of WLAN products. Currently, WLAN industry is catering to vertical markets. There is a need to expand horizontal business applications of WLAN technology. Due to soaring expectations of customers for better performance, in order to effectively compete or match with wired LAN industry, the focus is on increasing data rates through higher bandwidths.

The near future will see an increase in wireless augmenting wired networks in business use. Improvements will be made in niche wireless markets like wireless Internet. Only after standards, transmission speeds and interoperability among products are agreed upon can the WLAN more effectively compete with wired networks.

REFERENCES

Dix, J., “Effort underway for a new wireless LAN standard,” *Network World*, 20 September 1999, pp. 23-27.

Edwards, M., “Is it time to take another look at wireless LANs,” *Communication News*, June 1999, pp. 11-13.

Gillooly, C., “Wireless LANs set to take off,” *Informationweek*, 19 July 1999, pp. 15-17.

Gohring, N., “Wireless LANs to take on broadband access,” *Telephony*, 21 June 1999, pp. 12-14.

Goldman, J. E., *Applied Data Communications,* 8th ed., New York: John Wiley & Sons, 1998.

Editor, Industry Group Set to Drive Wireless. *Total Telecom,* August 1999. Available: www.totaltelecom.com, last accessed 20 November 1999.

Kilgore, R., Network Manager, Indiana Statehouse, Indianapolis IN, 20 November 1999, Phone.

Judge, P., “Networks: Bluetooth won’t eat WLANs,” *ZD Net UK*, July 1999. Available: www.zdnet.co.uk, last accessed 20 November 1999.

Graves, L., R. Leathern, S. McAteer, and K. Allard, “Mobile Web Access: Overcoming Wireless Walled Gardens,” Report by Jupiter Communications, July 1999.

Mitchell, D., “Waiting for wireless,” *PC Computing,* January 2000, pp. 72-77.

Moozakis, C., “Wireless poised to take on the enterprise—third generation IP products promise to make wireless applications more mainstream,” *Internetweek,* 13 September 1999, pp. 12-14.

Ruber, P., “Wires Not Included,” *Network Magazine,* November 1999, pp. 50-54.

Rupley, S., “The Untethered LAN,” PC Magazine, 19 October 1999.

Strategy Analytics Report, “*U.S. Wireless Voice Market Forecast,* February 2000.

Wireless LAN Interoperability Forum (1999). Available: www.wlif.com, last accessed 20 November 1999.

WLAN ROI/CBA Study (1999). Available: www.wlana.com, last accessed 20 November 1999.

“VoIP Push for Wireless LANs,” *CommunicationsWeek,* June 1999. Available: www.totaltelecom.com.

Ricochet Technology Overview, Metricom, Inc. Available: www.metricom.com/individuals/techover.htm, last accessed September 1999.

AUTHORS

Hemant K. Sabat is a Principal to Vice President at $3 billion Sabre in Dallas, U.S.A. Earlier, he was a Business Consultant to Vice President at Fannie Mae, a $32 billion Fortune 25 company, in Washington, D.C. He earned his MBA from Kelley School of Business, Indiana University, U.S.A. He has authored research papers on leadership, reengineering, corporate performance management and network systems. His current research interests include corporate strategy and business performance management. He lives in Dallas, Texas.