Wireless Local Area Networks

Edward C. Prem,

This paper is designed to give the layman a basic understanding of Wireless LANs. Discussed topics are an introduction of Wireless LANs, and their Physical and Medium Access Control Layers. IEEE 802.11 Wireless Networks Standard (unapproved draft) is discussed in the Medium Access Control Section.

Other Reports on Recent Advances in Networking
Go to Raj Jain's Home Page

Table of Contents

1 Introduction

For some time now, companies and individuals have interconnected computers with local area networks (LANs). (Note- because of the many acronyms, there is a list at the end of the paper.) This allowed the ability to access and share data, applications and other services not resident on any one computer. The LAN user has at their disposal much more information, data and applications than they could otherwise store by themselves. In the past all local area networks were wired together and in a fixed location as in figure 1 below.

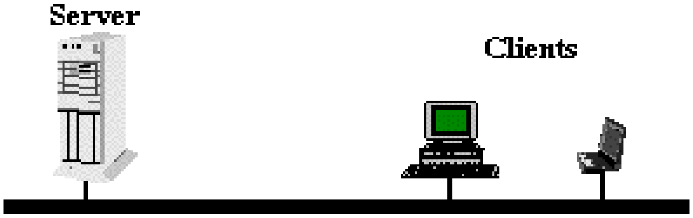


Figure 1: Traditional Wired LAN

Why would anyone want a wireless LAN? There are many reasons. An increasing number of LAN users are becoming mobile. These mobile users require that they are connected to the network regardless of where they are because they want simultaneous access to the network. This makes the use of cables, or wired LANs, impractical if not impossible. Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room. This ease of installation makes wireless LANs inherently flexible. If a workstation must be moved, it can be done easily and without additional wiring, cable drops or reconfiguration of the network. Another advantage is its portability. If a company moves to a new location, the wireless system is much easier to move than ripping up all of the cables that a wired system would have snaked throughout the building. Most of these advantages also translate into monetary savings. Ad Hoc networks are easily set up in a wireless environment. Ad Hoc networks will be discussed later. Figure 2 is an example of a wireless LAN.

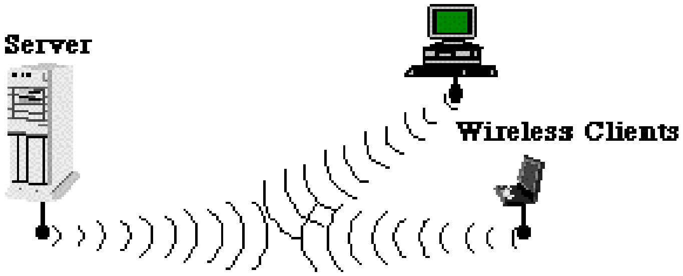


Figure 2: Wireless LAN

Return to Table of Contents

2 Physical Media

There are three media that can be used for transmission over wireless LANs. Infrared, radio frequency and microwave. In 1985 the United States released the industrial, scientific, and medical (ISM) frequency bands. These bands are 902 - 928MHz, 2.4 - 2.4853 GHz, and 5.725 - 5.85 GHz and do not require licensing by the Federal Communications Commission (FCC). This prompted most of the wireless LAN products to operate within ISM bands. The FCC did put restrictions on the ISM bands however. In the U.S. radio frequency (RF) systems must implement spread spectrum technology. RF systems must confine the emitted spectrum to a band. RF is also limited to one watt of power. Microwave systems are considered very low power systems and must operate at 500 milliwatts or less.

2.1 Infrared

Infrared systems are simple in design and therefore inexpensive. They use the same signal frequencies used on fiber optic links. IR systems detect only the amplitude of the signal and so interference is greatly reduced. These systems are not bandwidth limited and thus can achieve transmission speeds greater than the other systems. Infrared transmission operates in the light spectrum and does not require a license from the FCC to operate, another attractive feature. There are two conventional ways to set up an IR LAN. The infrared transmissions can be aimed. This gives a good range of a couple of kilometer and can be used outdoors. It also offers the highest bandwidth and throughput. The other way is to transmit omni-directionally and bounce the signals off of everything in every direction. This reduces coverage to 30 - 60 feet, but it is an area coverage. IR technology was initially very popular because it delivered high data rates and relatively cheap price. The drawbacks to IR systems are that the transmission spectrum is shared with the sun and other things such as fluorescent lights. If there is enough interference from other sources it can render the LAN useless. IR systems require an unobstructed line of sight (LOS). IR signals cannot penetrate opaque objects. This means that walls, dividers, curtains, or even fog can obstruct the signal. InfraLAN is an example of wireless LANs using infrared technology.

Return to Table of Contents

2.2 Microwave

Microwave (MW) systems operate at less than 500 milliwatts of power in compliance with FCC regulations. MW systems are by far the fewest on the market. They use narrow-band transmission with single frequency modualtion and are set up mostly in the 5.8GHz band. The big advantage to MW systems is higher throughput achieved because they do not have the overhead involved with spread spectrum systems. RadioLAN is an example of systems with microwave technology.

Return to Table of Contents

2.3 Radio

Radio frequency systems must use spread spectrum technology in the United States. This spread spectrum technology currently comes in two types: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). There is a lot of overhead involved with spread spectrum and so most of the DSSS and FHSS systems have historically had lower data rates than IR or MW.

2.3.1 Direct Sequence Spread Spectrum (DSSS)

With direct sequence spread spectrum the transmission signal is spread over an allowed band (for example 25MHz). A random binary string is used to modulate the transmitted signal. This random string is called the spreading code. The data bits are mapped to into a pattern of "chips" and mapped back into a bit at the destination. The number of chips that represent a bit is the spreading ratio. The higher the spreading ratio, the more the signal is resistant to interference. The lower the spreading ratio, the more bandwitdh is available to the user. The FCC dictates that the spreading ratio must be more than ten. Most products have a spreading ratio of less than 20 and the new IEEE 802.11 standard requires a spreading ratio of eleven. The transmitter and the receiver must be synchronized with the same sreading code. If orthogonal spreading codes are used then more than one LAN can share the same band. However, because DSSS systems use wide subchannels, the number of co-located LANs is limited by the size of those subchannels. Recovery is faster in DSSS systems because of the ability to spread the signal over a wider band. Current

DSSS products include Digital's RoamAbout and NCR's WaveLAN.

Return to Table of Contents

2.3.2 Frequency Hopping Spread Spectrum (FHSS)

This technique splits the band into many small subchannels (1MHz). The signal then hops from subchannel to subchannel transmitting short bursts of data on each channel for a set period of time, called dwell time. The hopping sequence must be synchronzied at the sender and the receiver or information is lost. The FCC requires that the band is split into at least 75 subchannels and that the dwell time is no longer than 400ms. Frequency hopping is less suceptible to interference because the frequency is constantly shifting. This makes frequency hopping systems extremely difficult to intercept. This feature gives FH systems a high degree of security. In order to jam a frequency hopping system the whole band must be jammed. These features are very attractive to agencies invovled with law enforcement or the military. Many FHSS LANs can be co-located if an orthagonal hopping sequence is used. Because the subchannels are smaller than in DSSS, the number of co-located LANs can be greater with FHSS systems. Most new products in wireless LAN technology are currently being developed with FHSS technology. Some examples are WaveAccess's Jaguar, Proxim RangeLAN2, and BreezeCom's BreezeNet Pro.

Return to Table of Contents

2.4 Multipath

Interference caused by signals bouncing off of walls and other barriers and arriving at the receiver at different times is called multipath interference. Multipath interference affects IR, RF, and MW systems. FHSS inherently solves the multipath problem by simply hopping to other frequencies. Other systems use anti-multipath algorithms to avoid this interference. A subset of multipath is Rayleigh fading. This occurs when the difference in path length is arriving from different directions and is a multiple of half the wavelength. Rayleigh fading has the effect of completely cancelling out the signal. IR is not effected by Rayleigh fading because the wavelengths used in IR are so small. Figure 3 shows the problem of multipath fading.

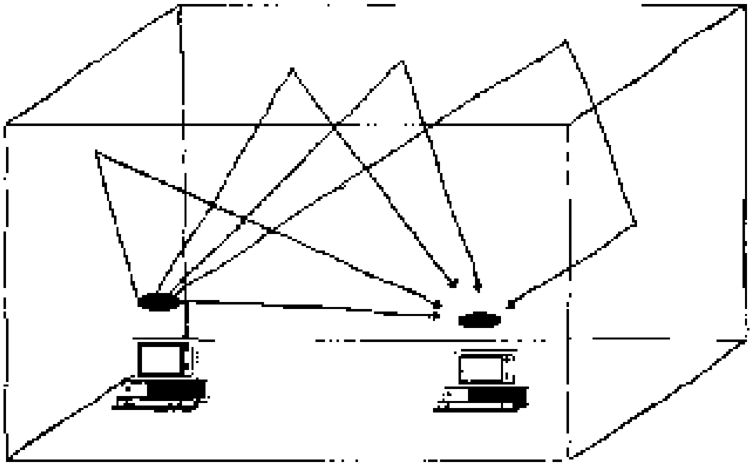


Figure 3: Example of Multipath Fading

Return to Table of Contents

3 Medium Access Layer

With more and more companies and individuals requiring portable and mobile computing the need for wireless local area networks continues to rise throughout the world. Because of this growth, IEEE formed a working group to develop a Medium Access Control (MAC) and Physical Layer (PHY) standard for wireless connectivity for stationary, portable, and mobile computers within a local area. This working group is IEEE 802.11. Because 802.11 will eventually become the standard for wireless networking, (I have only seen an unapproved draft), I will use 802.11 terminology in the rest of this paper.

3.1 802.11 Architecture

Each computer, mobile, portable or fixed, is refered to as a station in 802.11. The difference between a portable and mobile station is that a portable station moves from point to point but is only used at a fixed point. Mobile stations access the LAN during movement. When two or more stations come together to communicate with each other they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block.

A BSS which stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is refered to as an Ad-Hoc Network. An ad-hoc network is a network where stations communicate only peer to peer. There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-Hoc or IBSS networks are characteristically limited both temporally and spatially.

When BSS's are interconnected the network becomes one with infrastructure. 802.11 infrastructure has several elements. Two or more BSS's are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable. So data moves between the BSS and the DS with the help of these access points.

Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, the Extended Service Set or ESS. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSS's transparently to the LLC.

One of the requirements of IEEE 802.11 is that it can be used with existing wired networks. 802.11 solved this challenge with the use of a Portal. A portal is the logical integration between wired LANs and 802.11. It also can serve as the access point to the DS. All data going to an 802.11 LAN from an 802.X LAN must pass through a portal. It thus functions as brigde between wired and wireless.

The implementation of the DS is not specified by 802.11. So a distribution system may be created from existing or new technologies. A point to point bridge connecting LANs in two seperate buildings could become a DS. While the implementation for the DS is not specified, 802.11 does specify the services which the DS must support. Services are divided into two sections, Station Servies (SS) and Distribution System Services (DSS).

There are five services provided by the DSS. Association, Reassociation, Disassociation, Distribution, and Integration. The first three services deal with station mobility. If a station is moving within its own BSS or is not moving, the stations mobility is termed No-transition. If a station moves between BSS's within the same ESS, its mobility is termed BSS-transition. If the station moves between BSS's of differing ESS's it is ESS transition. A station must affilliate itself with the BSS infrastructure if it wants to use the LAN. This is done by Associating itself with an access point. Associations are dynamic in nature because stations move, turn on or turn off. A station can only be associated with one AP. This ensures that the DS always knows where the station is. Association supports no-transition mobility but is not enough to support BSS-transition. Enter Reassociation. This service allows the station to switch its association from one AP to another. Both association and reassociation are initiated by the station. Disassociation is when the association between the station and the AP is terminated. This can be initiated by either party. A disassociated station cannot send or receive data. Notice that I have not mentioned ESS-transition. That is because it is not supported. A station can move to a new ESS but will have to reinitiate connections. Distribution and Integration are the remaining DSS's. Distribution is simply getting the data from the sender to the intended receiver. The message is sent to the local AP (input AP), then dstributed through the DS to the AP (output AP) that the receipiant is associated with. If the sender and receiver are in the same BSS, the input and out AP's are the same. So the distribution service is logically invoked whether the data is going through the DS or not. Integration is when the output AP is a portal. Thus 802.x LANs are integrated into the 802.11 DS.

Return to Table of Contents

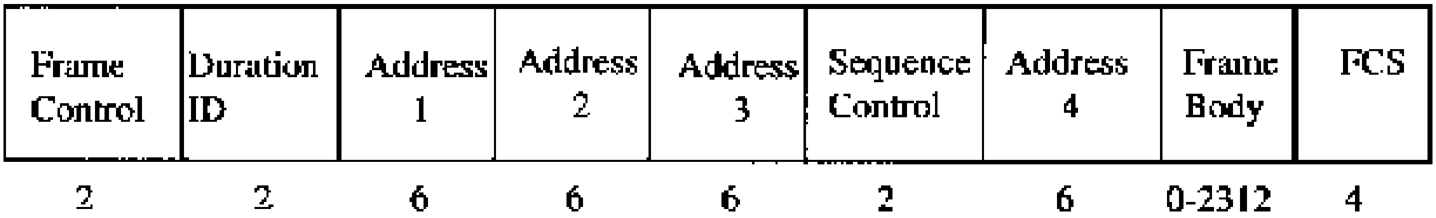
Station services are Authentication, Deauthentication, Privacy, and MAC Service Data Unit (MSDU) Delivery. With a wireless system, the medium is not exactly bounded as with a wired system. In order to control access to the network, stations must first establish their identity. This is much like trying to enter a radio net in the military. Before you are acknowledged and allowed to converse, you must forst pass a series of tests to ensure that you are who you say you are. That is really all authentication is. Once a station has been authenticated, it may then associate itself. The authentication relationship may be between two stations inside an IBSS or to the AP of the BSS. Authentication outside of the BSS does not take place. There are two types of authentication services offered by 802.11. The first is Open System Authentication. This means that anyone who attempts to authenticate will receive authentication. The second typw is Shared Key Authentication. In order to become authenticated the users must be in possesion of a shared secret. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm. The shared secret is delivered to all stations ahead of time in some secure method (such as someone walking around and loading the secret onto each station). Deauthentication is when either the station or AP wishes to terminate a stations authenication. When this happens the station is automatically disassociated. Privacy is an encryption algorithm which is used so that other 802.11 users cannot eavesdrop on your LAN traffic. IEEE 802.11 specifies Wired Equivalent Privacy (WEP) as an optional algorithm to satisfy privacy. If WEP is not used then stations are "in the clear" or "in the red", meaning that their traffic is not encrypted. Data transmitted in the clear are called plaintext. Data transmissions which are encrypted are called ciphertext. All stations start "in the red" until they are authenticated. MSDU delivery ensures that the information in the MAC service data unit is delivered between the medium access control service access points. The bottom line is this, authentication is basically a network wide password. Privacy is whether or not encryption is used.

Wired Equivalent Privacy is used to protect authorized stations from eavesdroppers. WEP is reasonably strong. The algorithm can be broken in time. The relationship between breaking the algorithm is directly related to the length of time that a key is in use. So WEP allows for changing of the key to prevent brute force attack of the algorithm. WEP can be implemented in hardware or in software. One reason that WEP is optional is because encryption may not be exported from the United States. This allows 802.11 to be a standard outside the U.S. albeit without the encryption.

Return to Table of Contents

3.2 Framing

Frame formats are specified for wireless LAN systems by 802.11. Each frame consists of a MAC header, a frame body and a frame check sequence (FCS). The basic frame can be seen in figure 4 below.

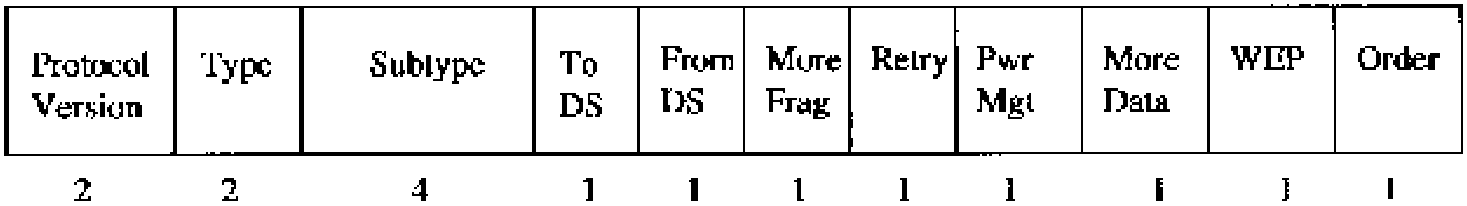


Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2	2	6	6	6	2	6	0-2312	4

Field Length is in Bytes

Figure 4: 802.11 Frame

The MAC header consists of seven fields and is 30 bytes long. The fields are frame control, duration, address 1, address 2, address 3, sequence control, and address 4. The frame control field is 2 bytes long and is compised of 11 subfields as shown in figure 5 below.



Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
2	2	4	1	1	1	1	1	1	1	1

Field Length is in Bits

Figure 5: 802.11 MAC Header

The protocol version field is 2 bits in length and will carry the version of the 802.11 standard. The initial value once 802.11 is approved will be 0, all other bit values are reserved. Type and subtype fields are 2 and 4 bits respectively. They work together hierarchically to determine the function of the frame. The remaining 8 fields are all 1 bit in length. The To DS field is set to 1 if the frame is destined for the distribution system. From DS field is set to 1 when frames exit the distribution system. Note that frames which stay within their basic service set have both of these fields set to 0. The More Frag field is set to 1 if their is a following fragment of the current MSDU. Retry is set to 1 if this frame is a retransmission. Power Management field indicates if a station is in power save mode (set to 1) or active (set to 0). More data field is set to 1 if there are any MSDUs are buffered for that station. The WEP field is set to 1 if the information in the frame body was processed with the WEP algorithm. The Order field is set to 1 if the frames must be strictly ordered.

The duration/ID field is 2 bytes long. It contains the data on the duration value for each field and for control frames it carries the associated identity of the transmitting station. The address fields identify the basic service set, the destination address, the source address, and the receiver and tranmitter addresses. Each address field is 6 bytes long. The sequence control field is 2 bytes and is split into 2 subfields, fragment number and sequence number. Fragment number is 4 bits and tells how many fragments the MSDU is broken into. The sequence nuber field is 12 bits an indicates the sequence number of the MSDU. The frame body is a variable length field from 0 - 2312. This is the payload. The frame check sequence is a 32 bit cyclic redundancy check which ensures there are no errors in the frame. For the standard generator polynomial see IEEE P802.11.

Return to Table of Contents

3.3 Medium Access Control Protocol

Most wired LANs products use Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the MAC protocol. Carrier Sense means that the station will listen before it transmits. If there is already someone transmitting, then the station waits and tries again later. If no one is transmitting then the station goes ahead and sends what it has. But what if two stations send at the same time? The transmissions will collide and the information will be lost. This is where Collision Detection Comes into play. The station will listen to ensure that its transmission made it to the destination without collisions. If a collision occured then the stations wait and try again later. The time the station waits is determined by the backoff algorithm. This technique works great for wired LANs but wireless topologies can create a problem for CSMA/CD. The problem is the hidden node problem.

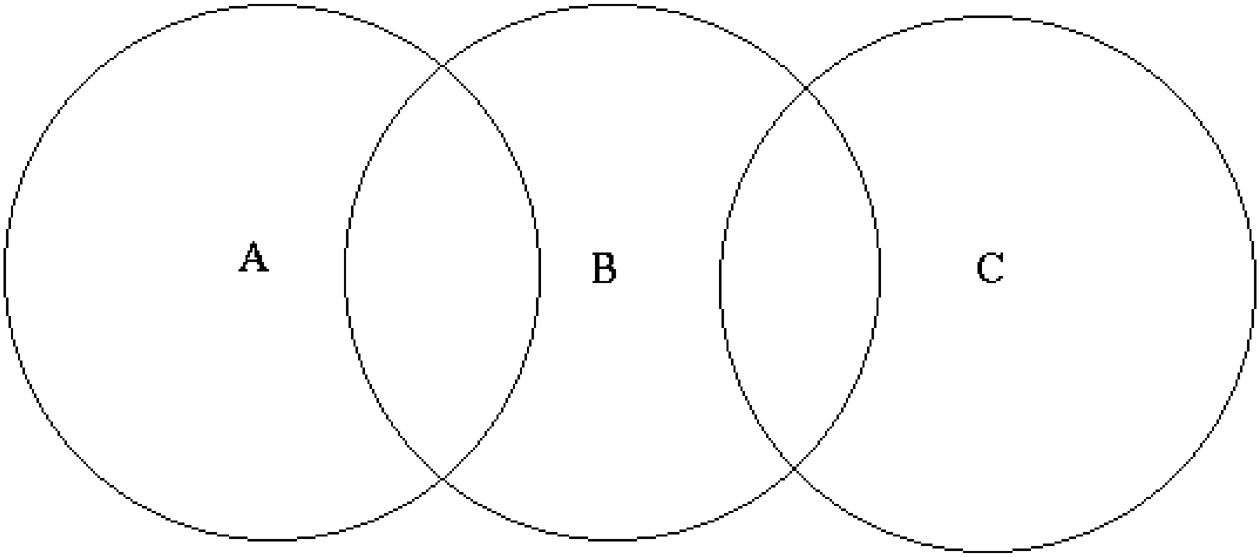


Figure 6: The Hidden Node Problem

The Hidden Node problem is shown in Figure 6 above. Node C cannot hear node A. So if node A is transmitting, node C will not know and may transmit as well. This will result in collisions. The solution to this problem is Carrier Sense Multiple Access with Collision Avoidance or CSMA/CA. CSMA/CA works as follows: the station listens before it sends. If someone is already transmitting, wait for a random period and try again. If no one is transmitting then it sends a short message. This message is called the Ready To Send message (RTS). This message contains the destination address and the duration of the transmission. Other stations now know that they must wait that long before they can transmit. The destination then sends a short message which is the Clear To Send message (CTS). This message tells the source that it can send without fear of collisions. Each packet is acknowledged. If an acknowledgement is not received, the MAC layer retransmits the data. This entire sequence is called the 4-way handshake as shown by figure 7 below. This is the protocol that 802.11 chose for the standard.

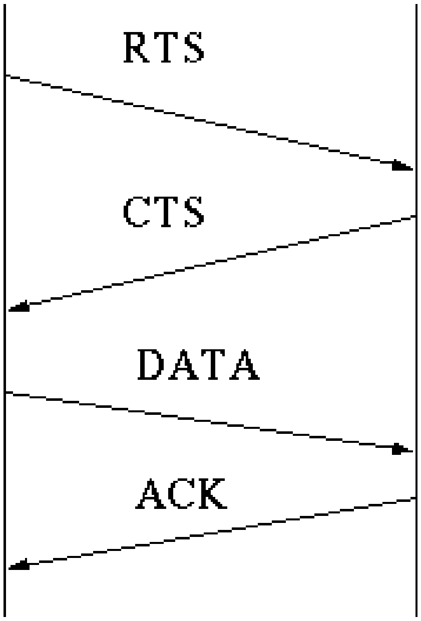


Figure 7: The 4-way Handshake

Return to Table of Contents

4 Summary

Wireless LANs come in many types: infrared, microwave, and radio. Radio is further broken down into direct sequence and frequency hoppping spread spectrum. The MAC layer protocol used by wireless LANs as standarized in 802.11 is CSMA/CA. The Negroponte Switch Theory states that all things wired will be wireless and all things wireless will become wired. This will certainly be true in the case of LANs. Traditional wired LANs will become a thing of the past as more and more users become mobile. LANs used to be defined by distance and spatial locality. Today, with the advances of wireless and virtual LAN technology, LANs are defined as a trust relationship regardless of location. Stationary users will become wireless once technology is able to increase throughput and data rate to levels which equal today's wired LANs.

Return to Table of Contents

5 Products

Wireless LAN Products

Company	**Product**	**Type**	**Frequency**	**Speed**	**Range**
BreezeCom	BreezeNet Pro	Radio FHSS	2.4 Ghz	3 Mbps	3000 feet
Proxim	RangeLAN2	Radio FHSS	2.4 GHz	1.6 Mbps	1000 feet
Digital	RoamAbout	Radio DSSS and FHSS	915 MHz and 2.4 GHz	2 Mbps	800 feet
WaveAccess	Jaguar	Radio FHSS	2.4 GHz	3.2 Mbps	??? feet

IBM	IBM Wireless LAN (Withdrawn Apr 97)	Radio FHSS	2.4 GHz	1.2 Mbps	800 feet
Solectek	AirLAN	Radio DSSS	2.4 GHz	2 Mbps	800 feet
Windata	Freeport	Radio ??SS	2.4 and 5.7 GHz	5.7 Mbps	263 feet
NCR	WaveLAN	Radio DSSS	915 MHz and 2.4 GHz	2 Mbps	800 feet
Aironet	ARLAN	Radio DSSS and FHSS	2.4 GHz	2 Mbps	???
RadioLan	RadioLAN	Microwave	5.8 GHz	10 Mbps	120 feet
Motorola	Altair Plus II	Microwave	18 GHz	5.7 Mbps	???
Photonics		Infrared	N/A	1 Mbps	25' X 25' room
InfraLAN	InfraLAN	Infrared	N/A	16 Mbps	90 feet

Note: Motorola uses frequencies which require licensing from the FCC.

Return to Table of Contents

6 Abbreviations

AP	- access point
BSS	- basic service set
CSMA/CA	- carrier sense multiple access with collision avoidance
CSMA/CD	- carrier sense multiple access with collision detection
CTS	- clear to send
DS	- distribution system
DSS	- distribution system services
DSSS	- direct sequence spread spectrum
ESS	- extended service set
FCC	- Federal Communications Committee
FCS	- frame check sequence
FHSS	- frequency hopping spread spectrum
IBSS	- independent basic service set
IR	- infrared
LAN	- local area network

MAC	-	medium access control layer
MSDU	-	MAC service data unit
MW	-	microwave
PHY	-	physical layer
RF	-	radio frequency
RTS	-	ready to send
WEP	-	wired equivalent privacy

Return to Table of Contents

7 References

IEEE P802.11, Draft Standard for Wireless LAN
Medium Access Control and Physical Layer Specification
9 May 1997
This is the meat of the paper

Chen, Kwang-Cheng
Medium Access Control of Wireless LANs for Mobile Computing
IEEE Network Sep/Oct 1994 V8 N5
A good discussion of wireless MAC

Balakrishna, Saraswati
Network Topologies in Wireless LANs
IFSM 652 Dec 20 1995
A great intro to wireless topologgies

Pahlavan, Kaveh
Trends in local wireless data networks
IEEE Vehicular Techonology Conference v1 1996 p. 21-25
Good paper, he also has a book

Gibson, J.
The Communications Handbook
IEEE Press, CRC Press 1997
The bible for communications, regardless of type

Weber State U., www.weber.edu/ist/itfm/lanstren.ht

The Wireless LAN Alliance, www.wlana.com

BreezeCom, www.breezecom.com

WaveAccess, www.waveaccess.com

RadioLAN, www.radiolan.com

Davis, P.T. McGuffin, C.R.
Wireless Local Area Networks
McGraw-Hill 1994

Bates, B.
Wireless Networked Communications
McGraw-Hill 1994

Muller, N.
Wireless Data Networking
Artech House 1995

Santamaria, A.
Wireless LAN Systems
Artech House 1994

Rappaport, T.
Wireless Communications
Prentice Hall 1996

Garg, V. Wilkes, J.
Wireless and Personal Communications Systems
Prentice Hall 1996

Return to Table of Contents

This page was written by Edward C. Prem

Last Modified 13 August 1997