

INTRODUCTION

Local Area Networks have evolved over the past 20 or so years to become a crucial ingredient in the success of businesses, large and small. From the smallest office to the largest multinational corporation shared access to information resources is an indispensable part of modern business processes. Local Area Networks (LAN) have been traditionally connected with wired infrastructure and a multi-billion dollar industry has grown up to supply customers needs for wired networking products. Companies like Cisco, 3Com, Bay Networks and Cabletron have developed a vast range of products to implement and manage Local Area Networks of all sizes and to interconnect them throughout the enterprise. Over the past ten or so years an alternative to wired LAN structures has evolved in the form of the Wireless LAN (WLAN). In a manner analogous to the growth of the wired LAN, initial application and market success of the WLAN was in specialized, vertical markets. Thus applications that highly valued the mobile, untethered connectivity were the early targets of the WLAN industry. These first generation products, which operated in the unlicensed 902-928 MHz ISM (Industrial Scientific and Medical) band had limited range and throughput, but proved useful in many factory floor and warehouse applications. These systems took advantage of emerging semiconductor processes developed for cellular telephone applications to enable inexpensive WLAN products. Unfortunately these same inexpensive components also enabled a wide variety of other 900 MHz products like cordless telephones. Consequently, the band quickly became crowded with a variety of unlicensed products. Building upon technology originally developed for military applications, spread spectrum techniques were employed to minimize sensitivity to interference. This approach allowed the design and manufacture of 900 MHz WLAN products having nominal data rates of 500 kilobits per second. Ultimately, the growing popularity of the band for a large range of unlicensed products, aggravated by the limited bandwidth caused users of WLAN to look to a different frequency band for growth in performance. The second generation of WLAN products evolved in the 2.40-2.483 GHz ISM band. Again enabled by semiconductor advances, this time from the PCS market, products were developed by a number of manufacturers for this band, again generally for

specialized vertical markets. Because a major user of the 2.4 GHz ISM band is microwave ovens, a transmission scheme less sensitive to this type of noise source needs to be used. Extending the experience from the crowded 900 MHz band, spread spectrum techniques combined with more available bandwidth and more complex modulation schemes allowed second generation 2.4 GHz band products to operate at data rates of up to 2.0 megabits per second. Third generation WLAN products are evolving to more complex modulation formats in the 2.4 GHz band to allow nominal 11 megabit per second raw data rate and about 7 megabit per second throughput even as the decreasing cost of 2.4 GHz semiconductor technology allows for ever more use of this band. In the third and fourth quarters of 1998, the first 2.4 GHz cordless telephones became available as did several new consumer electronic PC interconnection products. The history of the 900 MHz band WLAN seems poised to repeat itself as the 2.4 GHz band becomes a victim of its own success. The fourth generation of WLAN technology, offering users data rates of 10 megabits per second and up, is beginning. Again evolving from advances in semiconductor technology, fourth generation devices are operating at a new, higher frequency at 5 GHz band. The first of these fourth generation products has been available from RadioLAN Inc since late 1996. The initial products operate in the 5.775-5.850 GHz ISM band, and additional bandwidth around 5.2 GHz has also been made available. Unlike the lower frequency bands used in prior generations of WLAN products, the 5 GHz bands do not have a large indigenous population of potential interferers like microwave ovens or industrial heating systems as was true at 900 Mhz and 2.4 GHz. In addition there is a much more bandwidth available at 5 GHz, 350 Mhz compared with 83 Mhz at 2.4 GHz and 26 Mhz at 900 MHz. This combination of greater available bandwidth and reduced sources of interference make the 5 GHz bands an ideal region in which WLAN products having performance comparable to that achieved by wired networks are being created. A Wireless LAN can enhance the value of installed wired networks in large corporations by offering untethered mobility and reduce the total costs of network ownership in small companies by easy reconfiguration with growth and change. In the sections below, a brief review of data networks will be presented. This will be followed by a section on the various technology issues surrounding WLAN and finally by a discussion of the different standards relating to WLAN.

STANDARDS

Symbol has been a leader in establishing wireless standards—for interoperability, Multimedia transmission, and international connectivity. Our engineers sit on the committees of a number of trade organizations dedicated to creating and implementing these standards. Following are the key wireless technology standards in use today. Check the Glossary for full explanations of each standard:

- . IEEE 802.11 interoperability standard

- . IEEE 802.11a 5.4 GHz standard

 - Data rate is up to 54 Mbps (IEEE 802.11a)

 - Transmission frequency is between 5.725 - 5.850 Ghz

- . IEEE 802.11b high rate standard

 - Data rate is Up to 11 Mbps

 - Transmission frequency is between 2.4 - 2.484 Ghz

- . H.323 multimedia standard

- . Wi-Fi™

- . GSM

- . CDMA and TDMA

IEEE 802.11 ARCHITECTURE

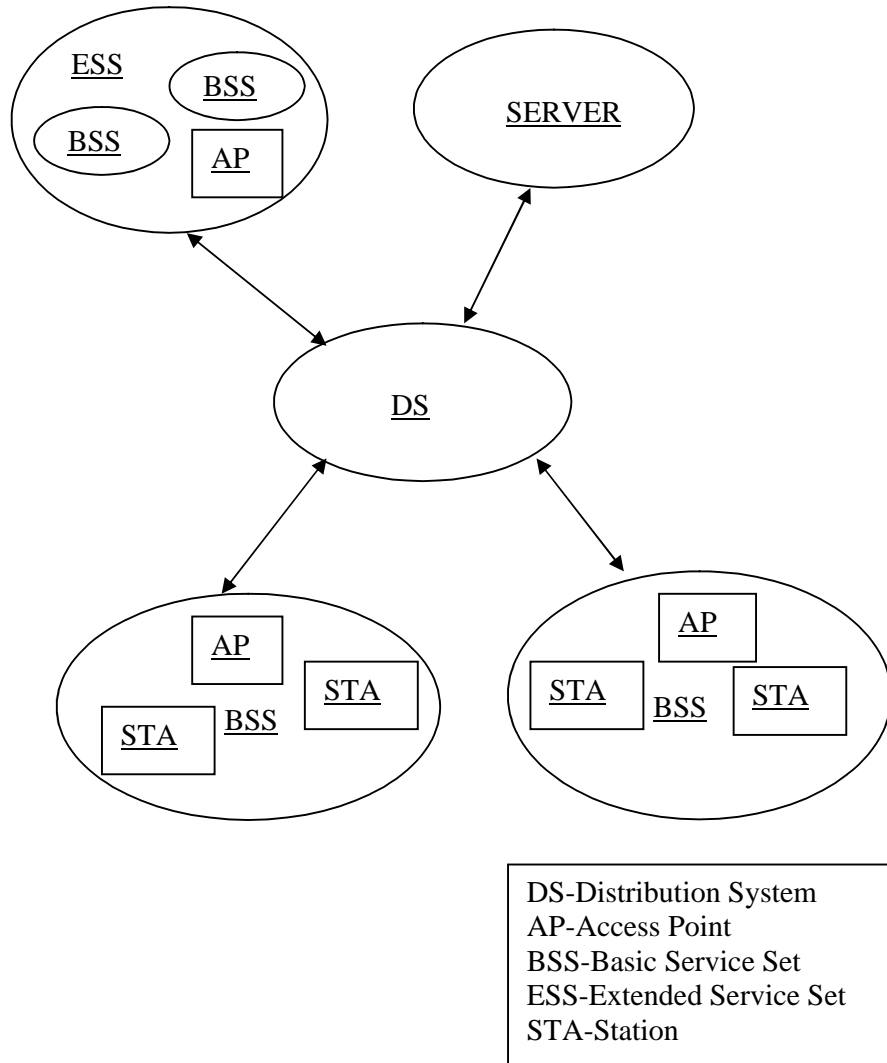


Figure 1

The figure indicates the model developed by the 802.11-working group. The smallest building block of wireless LAN is a Basic Service Set (BSS), which consist of some number stations executing the same MAC protocol and competing for accessing the same-shared medium.

A BSS may be isolated or it may connect to a backbone-distributed system through an Access point. The Access Point functions as bridge. The MAC protocol

may be fully distributed or controlled by a central coordination function housed in the access point.

An Extended Service Set (ESS) consists of two or more BSS interconnected by a distribution system. Typically, the distributed system is a wired backbone LAN.

The standard also defines three types of stations based on mobility.

1. No transmission:

A station in this will be either stationary or moves only within the direct

Communication range of the communicating stations of a single BSS.

2. BSS transmission:

This is defined as a station movement from one BSS to another BSS within the same ESS.

2. ESS transmission:

This defined as a station movement from a BSS in one ESS to a BSS within another ESS.

NETWORK

IEEE 802.11 Architectures

In IEEE's proposed standard for wireless LANs (IEEE 802.11), there are two different ways to configure a network: ad-hoc and infrastructure.

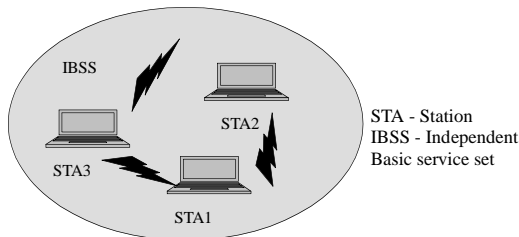
AD-HOC Network

In the ad-hoc network, computers are brought together to form a network "on the fly." As shown in Figure 1, there is no structure to the network; there are no fixed points; and usually every node is able to communicate with every other node. A smallest Wireless LAN may consist of computers each equipped with wireless n/w interface card. This mode of operation is possible when stations are able to

communicate directly and the network does not have an AP. This type of network is often formed when a station is not able to locate an AP and starts communicating with the peer stations directly. It can share printer, but cannot share resource of wired LAN unless one of the computer act as bridge to the wired LAN using special s/w (bridge)

A good example of this is the aforementioned meeting where employees bring laptop computers together to communicate and share design or financial information. Although it seems that order would be difficult to maintain in this type of network, algorithms such as the spokesman election algorithm (SEA) have been

Figure 2

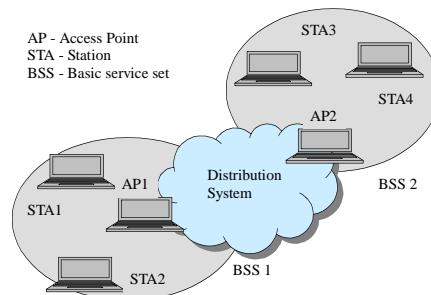


designed to "elect" one machine as the base station (master) of the network with the others being slaves. Another algorithm in ad-hoc network architectures uses a broadcast and flooding method to all other nodes to establish who's who.

Infrastructure Network

As shown in Figure 3, the second type of network structure used in wireless LANs is the infrastructure.

Figure 3



This architecture uses fixed network access points with which mobile nodes can communicate. If station wants to send data to another station then it has to send only through AP. Before transmitting, station has to become a member of infrastructure BSS. If a station moves out of its BSS, it can no longer communicate with other members of the same BSS and AP. AP act as providing connectivity for wireless computer. These network access points are sometime connected to landlines to widen the LAN's capability by bridging wireless nodes to other wired nodes. If service areas overlap, handoffs can occur. It can connect WLAN to wired LAN and can its resources. In this topology 15-50 clients can be connected. This structure is very similar to the present day cellular networks around the world.

PROTOCOL ARCHITECTURE

To provide a basis for the further discussions of the technology and standards issues related to WLAN, a brief review of network structures is in order. The first concept to keep in mind is that networks represent an interactive collection of often-powerful computers. The complexities of the interactions among these members of the network are many. To provide a common framework for describing and understanding, the International Standards Organization approved a standard called ISO-7498 that defines a seven-layered model to describe the interconnection processes between various members of a network. This model, which is officially known as the Open System Interconnect model, is the basis for most discussions of network function. The seven layers are shown in Figure 1. WLAN products, in common with other networking products, typically work at the two bottom most layers of the 7-layered model. The Physical Layer (usually referred to as simply PHY) is the actual physical method by which data is passed from one member of the network to another. For a WLAN its description includes such things as frequency of operation, data rate, modulation method, etc. In addition to the PHY, the lower half of the Data Link layer, usually known as the Media Access Control (or MAC) layer is defined by the WLAN product. The MAC layer is conventionally defined as the protocol by which data is transferred between network members. In Figure 1, the shaded areas represent the PHY and MAC layers. These layers and their important

features will be discussed in the Technology section that follows. Wireless networks are implemented with two basic types of components: a Network Adapter which is the electronic interface between the client computer (these days often a notebook PC) and the wireless network and an Access Point which provides the bridge between the wireless network and a wired network. A wireless network can consist solely of Network Adapters connecting members of a completely wireless network, or a combined network in which wired and wireless connectivity is employed. Because a client, wireless-networked computer could appear as a member of any number of potential networks due only to the clients own mobility, the topology of the network in which the new client appeared is altered by the additional member as is the network geometry.

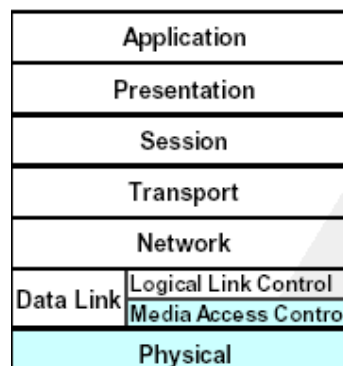


Figure: 4 Open System Interconnect Model

PHYSICAL LAYER

The PHY layer, which actually handles the transmission of data between nodes, can use either direct sequence spread spectrum, frequency hopping spread spectrum, or infrared (IR) pulse position modulation. IEEE 802.11 makes provisions for data rates of either 1 Mbps or 2 Mbps, and calls for operation in the 2.4 - 2.4835 GHz frequency band (in the case of spread-spectrum transmission), which is an unlicensed band for industrial, scientific, and medical (ISM) applications, and 300 - 428,000 GHz for IR transmission.

Infrared (IR)

Infrared is generally considered to be more secure to eavesdropping, because IR transmissions require absolute line-of-sight links (no transmission is possible outside any simply connected space or around corners), as opposed to radio frequency transmissions, which can penetrate walls and be intercepted by third parties unknowingly. Infrared transmissions can be adversely Provide data rate between 1Mbs and 2Mbps at a wavelength between 850nm and 950 nm. It is immune to electrical interface. However, infrared transmissions can be adversely affected by sunlight [5], and the spread-spectrum protocol of 802.11 does provide some rudimentary security for typical data transfers.

Spread Spectrum Radio

Spread-spectrum protocol of 802.11 does provide some rudimentary security for typical data transfers. It's data rate is 2Mbps. It is easy to generate and can travel long distance. It can also penetrate through wall.

Two types this technology

Frequency Hopping Spread Spectrum (FHSS)

Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS)

In a Frequency Hopping Spread Spectrum (FHSS) system, the data is modulated on to the carrier in a manner identical to that employed for standard narrow band communications. Most frequency hopping systems employ Gaussian Frequency Shift Keyed modulation, either two or four level. The carrier frequency is then changed (hopped) to a new frequency in accordance with a pre-determined

hopping sequence. If the receiver frequency is then hopped in synchronism with the transmitter, data is transferred in the same manner as if the transmitter and receiver were each tuned to a single fixed frequency. If different transmitter-receiver pairs hop throughout the same band of frequencies, but using different hopping sequences, then multiple users can share the same frequency band on a non-interfering basis. The operation of a pair of frequency hopping transmitter-receiver pairs is shown schematically in Figure 2. The obvious question arises: why not just assign a fixed frequency to each user and share the bandwidth in that manner? The answer lies in how a FHSS responds to interferers.

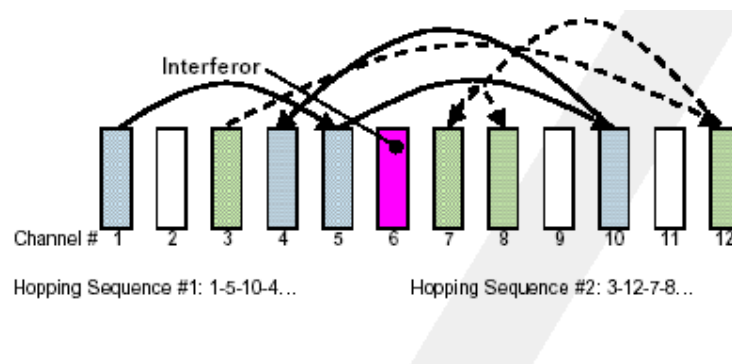


Figure 5

If a particular hop channel is noisy due to a fixed frequency source (e.g. a microwave oven), then information transferred in that particular channel can be lost. The system then hops to the next frequency, which is hopefully not occupied by an interferer, and information transfer continues. As will be discussed below, the communication protocol employed in the design of the system can offer means of further reducing the impact of a noisy channel. In the 2.4 GHz band, there are 79 1.0 MHz wide channels assigned, and a total of 78 different hopping sequences. In theory, all 78 hop sequences could be shared on a non-interfering basis, but statistically only about 15-20 (depending on individual user data traffic patterns) can be used. Thus a network manager could assign 15 different hopping sequences in the same physical area with minimal interference. This has the effect of multiplying the total available bandwidth by 15 times although each individual user would only experience a 2 Megabit per second maximum data rate.

Direct Sequence Spread Spectrum (DSSS)

The second type of spread spectrum is known as Direct Sequence Spread Spectrum (DSSS). In this system, the data stream is multiplied by a pseudo-random spreading code to artificially increase the bandwidth over which the data is transmitted. This is shown in Figure 3. The resulting data stream is then modulated onto the carrier using either Differential Binary Phase Shift Keying or Differential Quadrature Phase Shift Keying. By spreading the data bandwidth over a much wider frequency band, the power spectral density of the signal is reduced by the ratio of the data bandwidth to the total spread bandwidth. In a DSSS receiver the incoming spread spectrum data is fed to a correlator where it is correlated with a copy of the pseudo-random spreading code used at the transmitter. Since noise and interference are by definition de-correlated from the desired signal, the desired signal is then extracted from a noisy channel. While the block diagram of a DSSS WLAN product is somewhat simpler than a FHSS product, there are some very subtle difficulties that come into play in the presence of strong interfering signals. The basis of the noise immunity of a DSSS system is the fact that the desired signal and interference or noise is uncorrelated.

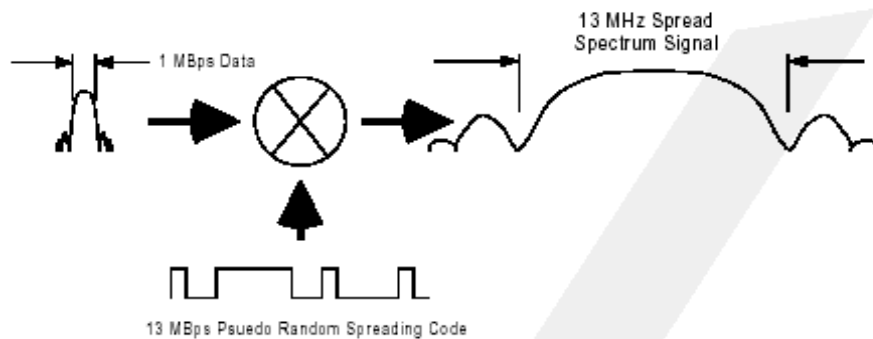


Figure 6

In complex interference environments which are becoming more common as usage increases, particularly ones in which very strong signals maybe present, non-linearities in the receiver generate intermodulation distortion products between the desired signal and the interfering signals. These IM products are now correlated with the desired signal thus reducing the resulting signal to noise ratio when processed in the receiver. The usual implementation of DSSS in the 2.4 GHz band employs a 13 MHz wide channel to carry a 1 MHz signal. Channels are centered at 5 MHz spacing, giving significant overlap. Within the designated 2.400 to 2.483 GHz band there are eleven available channels for users in the US. In a practical network, there are typically three non-overlapping channels that can be utilized in deploying a network. In an analogous manner to that described for FHSS, the total bandwidth in a physical region could effectively be multiplied by a factor of three for DSSS networks, although each user would again only experience 2 Megabit per second throughput.

MAC LAYER

The MAC layer is a set of protocols, which is responsible for maintaining order in the use of a shared medium. The primary function of the MAC Layer is to provide medium access control to application that contend for medium in such a way as to maximize the utilization of the channel.

Specifies two access protocol

Distributed access protocol

Centralized access protocol

Distributed access protocol uses CSMA/CA algorithm, which distribute the decision to transmit all the nodes using carrier sense mechanism. It defines the Distributed Coordination Function.

Centralized access protocol regulates the transmission by centralized decision maker. it defines the Point Coordination Function.

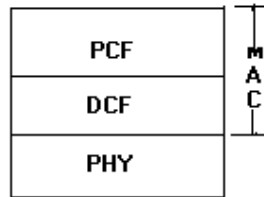


Figure 7

Distributed Coordination Function

Distributed Coordination Function specifies a carrier sense multiple accesses with collision avoidance (CSMA/CA) protocol. In this protocol, when a node receives a packet to be transmitted, it first listens to ensure no other node is transmitting. If the channel is clear, it then transmits the packet. Otherwise, it chooses a random "backoff factor" which determines the amount of time the node must wait until it is allowed to transmit its packet. During periods in which the channel is clear, the transmitting node decrements its backoff counter. (When the channel is busy it does not decrement its backoff counter.) When the backoff counter reaches zero, the node transmits the packet. Since the probability that two nodes will choose the same backoff factor is small, collisions between packets are minimized. Collision detection, as is employed in Ethernet, cannot be used for the radio frequency transmissions of IEEE 802.11. The reason for this is that when a node is transmitting it cannot hear any other node in the system which may be transmitting, since its own signal will drown out any others arriving at the node.

Whenever a packet is to be transmitted, the transmitting node first sends out a short ready-to-send (RTS) packet containing information on the length of the packet. If the receiving node hears the RTS, it responds with a short clear-to-send (CTS) packet. After this exchange, the transmitting node sends its packet. When the packet is received successfully, as determined by a cyclic redundancy check (CRC), the receiving node transmits an acknowledgment (ACK) packet. This back-and-forth exchange is necessary to avoid the "hidden node" problem, illustrated in Figure 3. As shown, node A can communicate with node B, and node B can communicate with node C. However, node A cannot communicate node C. Thus, for instance, although

node A may sense the channel to be clear, node C may in fact be transmitting to node B. The protocol described above alerts node A that node B is busy, and hence it must wait before transmitting its packet.

Point Coordination Function

PCF is an alternative access method implemented on top of DCF .Optional access method that works like polling by centralized polling master (point coordinator)

PCF is applicable only for infrastructure networks.

MAC Layer Frames

There are three types of frames.

Data Frames

It consists of user information.

Control Frames

It consists of control information. They are

RTS (Ready To Send), CTS (Clear To send), ACK

Management Frames

It consists of management information. They are

Authentication and Responded-Authentication

Association/Re-Association and Response, Disassociation

Beacon and Probe frames

MAC Frame Format

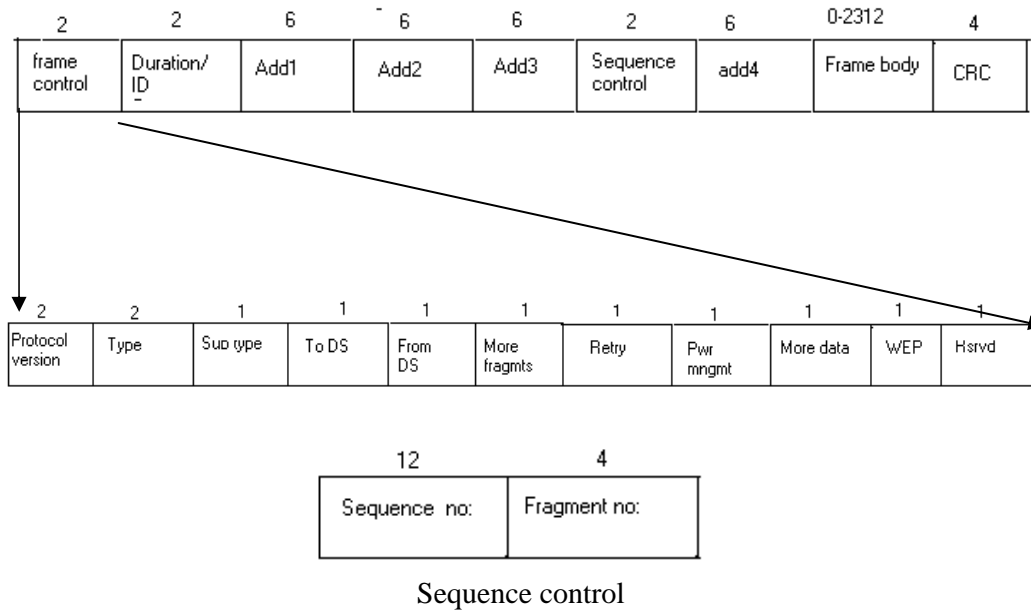


Figure 7

Frame Format

Frame Control

Duration ID

Duration Information - for accessing Network Accessing Vector (NAV)
short ID or Association ID(AID)- to allow A station to retrieve frame buffered at the AP used only in power- save-poll frame

Address 1,2,3,4

Typical 48-bit IEEE 802 address format

Different possible interpretation depending on frame type and all four may not always present

Source Address (SA)-Identifies original source of the frame

Destination Address (DA)- Identifies the final identification of the frame

Transmitter Address (TA)- identifies station that transmitted the frame on to the wireless medium. It may not equal to the SA due to indirection

Receiver Address (RA)- Identifies the station that is to receive the frame. It may not equal DA due to indirection

BSSID-Identifies the BSS

Sequence Control

Used to identifies the sequence of frame

Contain sequence no: assigned to MAC Service Data unit

Fragment Number-MSDU may be fragmented across multiple MAC Protocol Data Unit(MPDU)

Frame Body

Maximum length 2312 Bytes

Frame Check Sequence

It is used to detect the error in each frame.

Control Frame

Protocol Version

Version of IEEE 802.11 in use at the frame

Type

Indicate the type of the frame: data, control, and management

Subtype

- It give subtype for a given type

Management example

- 0000 → association request
- 0001 → Association response

Control Examples

- 1011 → RTS
- 1101 → CTS
- Data Examples
- 0000 → data

“To DS “and “From DS”

- To DS set for data frame from station to AP
- From DS set for data from AP to station

More Frags

- 1 → One or more fragments follow
- 0 == this is the last or only frame

Retry

- 0 → This is the first transmission attempt
- 1 → This is a retransmission attempt

Power Management

- 0 → Station will remain active after this exchange
- 1 → Station will enter in a power management mode after this full exchange is complete

More Data

- 0 → AP has no more data available for station
- 1 → AP has more data available for station

WEP(Wired Equivalent Protection)

- 0 → Frame body is not encrypted
- 1 → Frame body is encrypted

Order

0 → Ordered service not requested

1 → Higher layer requested ordered service

MAC Functionalities

The primary function of the MAC Layer is to provide medium access control to application that contend for medium in such a way as to maximize the utilization of the channel

- The MAC layer will also provide the Power Management and Synchronization.
- The MAC handles three types of messages: Data, Control, Management.
- Authentication/Deauthentication based on Wired Equivalent Privacy
- Association/Resuscitation
 - Associating station to station by sending request. Once associated AP is responsible for delivering frames to and from the station
- MSDU delivery
- Scanning
 - Station scan to find BSS to join
- Joining station to BSS
 - After scanning station will join to a BSS
- Address Filtering

It is complex than traditional LAN, since a station may receive frame from multiple BSS and contain multiple target address-SA, DA, RA, TA, BSSID. It accept frames from the BSS with which it is associated.

BENEFITS

The widespread strategic reliance on networking among competitive businesses and the meteoric growth of the Internet and online services are strong testimonies to the benefits of instantaneous data capture, wireless voice, and shared resources. With wireless technology, users can immediately and continuously access shared information, while IT managers can set up or augment networks (such as temporary conference or work spaces) and devices (such as wireless cash registers, kiosks, and displays) without installing or moving wires. Just some of the benefits that wireless LANs offer include:

Mobility That Improves Productivity and Service

Wireless LAN systems can provide users with access to real-time information anywhere in their organization. This supports better productivity and service opportunities not possible with wired networks, leading to faster decision-making and lowered costs.

Installation Speed and Simplicity

Installing a wireless LAN system is faster and easier than a wired implementation, as it eliminates the need for complex cabling and construction tasks. Installation can even take place without taking your current wired system off-line, allowing work to continue as usual.

Installation Flexibility

Wireless technologies can go into spaces where wired systems cannot, such as historic sites or sites where new wiring cannot be undertaken for structural reasons.

Reduced Cost-of-Ownership

While there is an initial investment required for wireless hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, adds and changes.

Scalability

Wireless LAN systems can be configured and reconfigured in a variety of topologies to meet the needs of specific applications and installations. Symbol networks are also designed to adapt easily for corporate expansion—simply add more access points to grow your network.

WLAN CARD AND AP VENDORS

- Intel
- D-Link
- Compaq
- Sony

MAJOR CHIPSETS VENDORS

- Atheros
- Intersil

CONCLUSIONS

IEEE 802.11 is still in the process of being adopted as a standard by the IEEE standards body. Although 802.11 provides a reliable means of wireless data transfer, some improvements to it have been proposed. For example, at Virginia Tech, research is being performed into ways in which the 802.11 network parameters can be dynamically adjusted to improve throughput. The use of wireless LANs is expected to increase dramatically in the future as businesses discover the enhanced productivity and the increased mobility that wireless communications can provide in a society that is moving towards more connectionless connections.

ABSTRACT

A wireless local area network is a flexible data communication system implemented as an extension to, or an alternative for, a wired LAN within a building or campus. Wireless LAN no longer constitutes a niche market, used primarily by business unable to conveniently link devices with conventional cable. As WLAN have become more popular IEEE 802.11 technologies designed to provide an Ethernet like wireless networking environment, have become dominant approach.

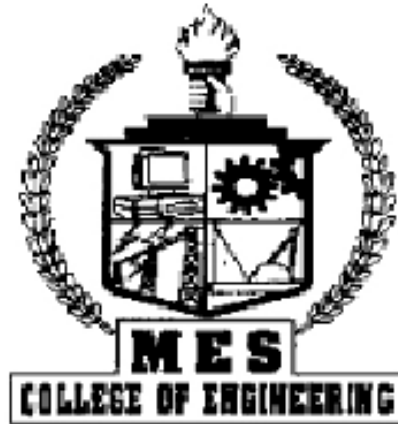
IEEE 802.11b, currently the most popular version operates in 2.4GHz frequency band. The actual data rate in typical office environment is 2-4Mbps. IEEE 802.11g and 802.11a uses more efficient data encoding to increase 802.11b's transmission rate up to 54 Mbps and 5GHz of frequency band.

Although the Radio based technology's Wired Equivalent Privacy (WEP) security protocol is relatively weak, 802.11 is the most popular in WLAN approaches. IEEE 802.11 is the most popular in WLAN approaches. IEEE 802.11 is faster and more range than HomeRF (Home Radio Frequency) As a result there has been a boom in the market for IEEE 802.11 chipset, which are used in NIC, laptops and PDA's to implement WLAN. This covers an introduction, standards's architecture, protocol architecture and its benefits.

CONTENTS

- Introduction
- Standards
- 802.11 Architecture
- Networks
- Protocol Architecture
- Physical Layer
- MAC Layer
- Benefits
- Products
- Chipsets

MES COLLEGE OF ENGINEERING
KUTTIPPURAM



SEMINAR REPORT

ON

Wireless LAN-IEEE 802.11

Presented by

Shanish Mon K.P

DEPARTMENT OF INFORMATION TECHNOLOGY

2002-2003

**MES COLLEGE OF ENGINEERING
KUTTIPPURAM**

DEPARTMENT OF INFORMATION TECHNOLOGY

CERTIFICATE

This is to certify that the Seminar titled *Wireless LAN - IEEE 802.11* was prepared and presented by *Shanish Mon K.P* of the final semester of the Department of Information Technology, in partial fulfillment of the requirement for the award of Bachelor of Technology Degree of Information Technology under the University of Calicut during the academic year 2002 - 2003.

Staff in Charge

Head of the Department

Kuttippuram

Date:

ACKNOWLEDGEMENT

I thank God Almighty for the successful completion of my seminar. Sincere feelings of gratitude for Dr.Agnisharman Namboothiri, Head of the Department, Information Technology. I express my heartfelt gratitude to Staff-in-charge, Miss. Sangeetha Jose and Mr. Biju, for their valuable advice and guidance. I would also like to express my gratitude to all other members of the faculty of Information Technology department for their cooperation.

I would like to thank my dear friends, for their kind-hearted cooperation and encouragement.

REFERENCES

Data and computer communication(6th edition)

By William Stallings

Sites visited:

www.itpapers.com

www.google.com