WIRELESS LOCAL AREA NETWORKING:

THEORY, DESIGN AND IMPLEMENTATION IN ELECTRICAL COMPLEX, GIDAN KWANO.

AYUBA, ANCHE JR

2004/18798EE

A Thesis Submitted To The Department Of Electrical and Computer Engineering,

Federal University of Technology, Minna.

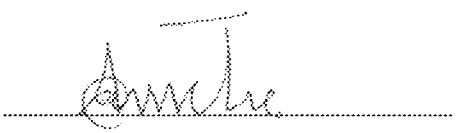
2ND DECEMBER, 2009.

DEDICATION

I dedicate this work to Almighty God for guiding me throughout my academic pursuit and for the strength and provision he has blessed me with so far. I also want dedicate this work to my family, for without them I would not be where I am today and this work would not have been possible.

DECLARATION

I (AYUBA, ANCHE JR) with Matriculation Number 2004/18798EE hereby declare that this work was done by me and it has never before been presented elsewhere for the award of a degree. I hereby relinquish the right to the Federal University of Technology, Minna, Niger State.



01/02/2010

AYUBA, ANCHE JR

2004/18798EE

Date

CERTIFICATION

This is to certify that this project titled "Wireless Local Area Network: Theory, Design and Implementation" meets the regulations governing the award of Bachelor of Engineering degree in Electrical /Computer Engineering Department of Federal University of Technology, Minna, Niger state.

02/02/2010

Engr (Mrs) C.O Alenoghena
(Project Supervisor)

Date

May 6, 2010

Engr Dr Y. A Adediran
(Head of Department)

Date

09/03/10

External Supervisor

Date

ACKNOWLEDGEMENT

I will like to first and foremost thank Almighty God for the gift of Life, Good Health and Strength. I also want to thank him for the resources and everything he has blessed me with to make this work a success through the numerous ways he has made possible.

I also want to thank my dear father for his wise words, advices, coaching and occasional scolding. All this have combined to make me a better person. God bless you Sir, you are a mentor. I also want to thank my mother for always being there, and for being a source of inspiration to me with her wise words. My two elder sisters, who have always encouraged me and supported me in ways I can't even begin to mention, my elder brother, who is pushing me the limits to bring out the best in me, my immediate elder sister who has always challenged me to do better, and finally, my niece who is giving me a reason to want to succeed.

My profound gratitude also goes my supervisor, Engr (Mrs) C. O. Alenoghena and Mallam Yahaya, my assistant project supervisor /technical supervisor. My HOD Electrical /Computer Engineering, Engr Dr Y.A. Adediran, and all my lecturers who have assisted me directly or indirectly to make sure this work is a success.

My very special thank goes to Quanteq Technology Services who helped me greatly to improve my knowledge in computing in general and networking in particular. Very special thank also goes to all the staffs who have helped me and contributed to the success of this project.

I also want to appreciate all my friends. You all have been of great help to me. I cannot even begin to mention areas where you guys have contributed to my life. Thank you all.

ABSTRACT

Local area networking grew out of the need to connect computers and rely on some kind of physical transmission medium like the twisted pair cable, coaxial cable or optic fibre cables to transfer data between connected devices.

During the course of this research, I investigated technologies that make wireless LAN work, capabilities and limitation, security of a wireless network, design and implementation of a wireless LAN, wireless LAN components and infrastructures. This work also takes a look at typical wireless LAN consideration factors and implementation of a fictional wireless LAN connection of the electrical complex in the school's permanent site.

The approach taken by this work is from the basic networking through the OSI layers 1 & 2 and then specific issues that relate to enterprise applications.

The major limitation of today's wireless LAN is basically that of incompatibility. Then again, for unlicensed operation, the ISM band is being used, which brings about interference issues. Most of the limitations of wireless LANs today are transitional in nature and will be solved by additional standards or global business politics.

TABLE OF CONTENTS

Dedication i

Declaration ii

Certification iii

Acknowledgement iv

Abstract iv

CHAPTER 1: INTRODUCTION

1.2 Objectives

1.3 Methodology

1.4 Organization of Thesis

CHAPTER 2: LITERATURE REVIEW

2.1 Theoretical Background

2.2 The OSI Model and Wireless LAN Overview

2.3 Anatomy of a Wireless Device

2.4 Wireless LAN Transmission Technology

2.4.1 Infrared

2.4.2 Narrow-Band Single Frequency Radio LAN Technology

2.4.3 Multi-Path Distortion in RF Channel

2.4.4 Spread Spectrum

2.5 Wireless LAN Standard

2.5.1 Home RF

2.5.2 The IEEE 802.11 Family of Standards

2.5.3 Hiperlan /2

2.6 Wireless Network Topologies

2.6.1 Basic Service Set Network

2.6.2 Independent Basic Service Set Network

2.6.3 Extended Service set Network

2.7 Switched Wireless LAN

2.7.1 Advantages of Switched Wireless LAN

2.7.2 Disadvantages of Switched Wireless LAN

CHAPTER 3: DESIGN AND IMPLEMENTATION OF A WIRELESS LAN

3.1 Defining the Requirement for the Wireless Network

3.2 Some General Wireless Design Consideration

3.2.1 Understanding Wireless Performance Consideration

3.2.2 Factoring In Attenuation

3.2.3 Factoring In Multi- Path Distortion

3.2.4 Factoring In The Earth's Bulge- The Fresnel Zone And Antenna Height

3.2.5 What Wi-Fi Means

3.3 Consideration For The Frequency Band And The Number Of Channels

3.4 Design Consideration For Mobility

3.5 Design Consideration for High Performance

3.6 Designing External Point-to-Point to Multi-Point Links

3.7 Comparing Different Technologies With Respect to Design Consideraiton

3.8 Site Survey for A Wireless LAN Implementation

3.9 Implementing A Wireless Network

3.9.1 The Components of A Wireless LAN

3.9.1.1 Wireless NICs'

3.9.1.2 Access Points

3.9.1.3 Wireless LAN Switch

3.9.1.4 Amplifiers

3.9.1.5 Antenna

3.9.1.6 Distribution System

3.9.2 Calculating the Number of Access Points Required

3.9.3 Comparing 802.11 Performance in Different Configuration

3.9.4 Operating System Support for Wireless LANs'

3.9.4.1 Microsoft Windows

3.9.4.2 GNU Linux

3.10 Securing the Wireless Network

3.11 Putting the Network Togeiher

CHAPTER 4: DESIGN SIMULATION

4.1 Block Diagram of the Connection of the Wired to the Wireless Aspect of the Network.

4.2 Electrical Bill of Quantity of the Design.

CHAPTER 5: CONCLUSION.

5.1 Conclusion

5.2 Recommendation.

CHAPTER 1:

1.1 INTRODUCTION

Wireless communications are part of our everyday life and are shaping our everyday life as well beyond cell phones and text messaging. Access to data is paramount for all business in today's digital world and wireless data communications are revolutionizing the way we interact with business information, providing a more reliable and consistent access to it.

While everything else seems to become wireless today technologies are many and it may not always be easy to have a clear picture of what may work for our specific needs. This project will try to clarify the options available on the market for the need of small businesses and identify the four main standards used today to exchange data wirelessly, each one created with a specific target use in mind:

- Bluetooth: For short range connection of interactive devices
- Wireless USB: For plug-and-play ultra fast computer peripherals connectivity.
- Wi-Fi (802.11): For local area Networking
- Wi MAX: For wide area internet access at high speed.

BLUETOOTH: A very intelligent wireless protocol. Bluetooth networking transmits data via low power radio waves. It communicates on a frequency of 2.45GHz (actually between 2.402 and 2.480 GHz). This frequency has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM). One of the ways by which Bluetooth avoids interference with other devices is by sending

out very weak signals of about 1 milliwatts. This low power limits the range of the Bluetooth device to about 10 meters. Bluetooth can connect up to eight (8) devices simultaneously with each of these devices in the same 10 meters range. It uses a technique called **spread-spectrum frequency hopping** which makes it rare for more than one device to be transmitting at the frequency at the same time.

WIRELESS USB: This is a brand new standard for closer-range cable replacement that promises the same plug-and-play advantage normal USB offers for all devices without the hassle of cable. It is extremely fast at 480Mbps within 10ft and 110Mbps at up to 30ft. It is poised to become a very common way to connect devices such as printer, external DVD players and hard disk drives to computers. Because it is recently introduced, only a few devices are compatible but there is a wide roster of options expected to reach the market.

802.11 (Wi-Fi):

Wi-Fi is a technology designed to link computers into a local area network (LAN) replacing the traditional Ethernet cables. It can operate in a peer-to-peer mode, but it is most commonly utilized with a central access point that connects all users and bridges them with other resources on the network including internet access where applicable.

The most recent of 802.11 versions is the "802.11n Draft 2.0". It provides great performance and security improvements over the previous ones, i.e. 802.11b, 802.11a and 802.11q affording up to 270Mbps (with about 100mbps average) data transfer rates and range of up to 300ft enough to connect to demanding resources such as database

server or to flawlessly stream multimedia contents across the network. This new standard is backward compatible with "B" and "G" devices.

Wi MAX:

Wi MAX stands for Worldwide Interoperability for Microwave Access. This technology offers transmission of wireless data via a number of transmission methods; such as portable or fully mobile internet access via point- to- multipoint links. The Wi MAX technology offers about 72 Mega bits per seconds speed without any need for cable. Wi MAX is based on a standard that is **IEEE 802.16**. It is usually called Broadband Wireless Access. The backhaul of the Wi MAX is based on the typical connection to the public wireless networks using optical fibre, microwave links, cable or any other high speed connectivity. In few cases such as mesh networks point-to-multipoint connectivity is also used as a backhaul. Ideally Wi MAX use point-to-point antenna as a backhaul to join subscriber sites to each other and to base stations across long distances.

1.2 OBJECTIVES OF WIRELESS LAN:

As a result of the great demand for mobility this days even at work, I have decided to carry this project to implement a wireless network in the electrical complex of the school's permanent site to provide the staffs, students and any body within the access points` area of coverage connectivity to the internet and other vital information even outsides offices and classrooms.

Implementing this project will also provide an extension to the already existing wired LAN and will also provide better and faster internet connection as implementing this will reduce the congestion on the wired LAN thereby resulting to greater throughput.

This design will also reduce the mess created by cables around the building, as cables will only be limited to office desk areas and other strategic areas of the buildings. The wireless network will cover the laboratories, stair ways, corridors and other difficult to wire areas of the buildings.

1.3 METHODOLOGY:

The approach to investigating WLANs taken here is a path through the basic networking, the relevant technologies upon which WLANs are based, looking at WLANs from the perspective of the bottom two layers of the OSI model with necessary parallels to wired networks. What the prevailing standards define is also looked at, as well as issues that have arisen from present implementations and interim solutions proffered as well as what the ultimate WLANs as a means of pervasive computing and how it can be planned and implemented with a fictional setup. The implementation first involves taking a physical inspection of the entire building, taking into consideration the offices, stair ways, corridors, etc and then mapping out access points locations to offer full coverage of the entire building and finally configuration of every device to provide internet connection to the entire building and also interconnectivity between different users. A comparative approach is given to competing standards/technologies as well as actual product performance.

1.4 ORGANIZATION OF THESIS:

Chapter two handles the literature review, theoretical background of wireless LANs, beginning with a very basic introduction of the two components of any computer network. How wireless LAN fits into the OSI model, transmission technologies and standards, the anatomies of wireless LAN components as well as performance and implementation issues like security, mobility and interference.

Chapter three looks at what it takes to design a wireless LAN beginning with the need for wireless LANs, technical and non-technical design.

It also looks at implementation consideration and how they affect the key issues in wireless LAN-mobility and capacity.

A comparison of different technologies/standards is done to see how they fit or don't fit design requirements / considerations. The different physical wireless LAN components are then introduced and how they practically relate to what aspects of the design. Also their current limitations and configuration parameters as well as any special practical issues relating to them. This chapter concludes by looking at a security implementation from the perspective of four logical layers as well as the types of attacks and proposed security against these attacks on the design.

Chapter four comprises the implementation of this design in the Electrical complex of the schools permanent site which puts into consideration high performance, security, and mobility. It also gives the cost analysis of implementing such a design.

Chapter five looks at difficulties encountered during the course of this design and the limitations of the design. What standard based methods are considered to address these limitations?

CHAPTER 2:

2.1: LITERATURE REVIEW

Wireless LAN is a growing technology which could be a potential replacement for the wired connections, as a result of their hitherto niche application. There are however a few books that have cone into the market with the boom of the wireless LAN technology to provide an up-to-date information on this new technology, but the most recent information is found on the IEEE standard's manufacturers' technical publication and a little hand-on experience.

The 1995 New Riders, Wireless Networking Handbook by Geiger. J. is one of the earliest and most extensive books on this topic that I have come across. The work gives a history of wireless networks, wireless networks architecture, both physical and logical with close correlation to the OSI model, extensive treatment of network analysis, design installations and support. Like in almost any other work, the benefits of wireless network are treated. There is also a thorough treatment of the wireless network market as well as concerns such as interference, inter-operability, power management, security and health issues. Not only does the book treat modulation and medium access schemes for both RF and Optical transmission, but it takes a brief look at proprietary pre-IEEE wireless networks, which are the LAN and Range Link, lucent's WaveLAN and Windata's Freeport, So-leteck's Airlan etc. A fairly detailed treatment of packet radio WANs, analog cellular WANs, cellular Digital Packet Data (CDPD) WANs as well as satellite communications.

Owing to the fast development of wireless technologies, the technology aspect of the book is obsolete by all standards. However, procedures for design, business cases and support still remain excellent and can be applied even to today's modern wireless LAN.

In designing a wireless Network (2001, Syngress) Wheat et al try to trace the emergence of wireless communication from traditional means of communication. The work explores present application for wireless networks in both horizontal and vertical markets. A basic treatment of electromagnetic transmission, propagation and such factors as attenuation, and refraction that affect propagation is given, and based on the knowledge built, it goes ahead to show the place and relevance of wireless elements like antennas access points, and the need for regulatory bodies. The OSI model, its relevance to networking and its correlation to TCP/IP is given as a basis for understanding how computer network functions. This book goes on to introduce fixed wireless technologies like wireless loop, LMDS and treat IEEE 802.11 wireless LANs in fair detail. Mobile and optical wireless technologies are also briefly treated. The high point of the book is in its detailed and thorough methodology for design and implementation of wireless LANs based on Lucent's NEMA methodology which is only applicable for medium to large scale implementation. This design methodology is backed up with design case studies that cover all three possible wireless LAN implementations – SOHO, medium and campus/ enterprise.

Ouellet et al in 'Building a Cisco Wireless LAN' (2002, Syngress) is a good resource for wireless LANs, treating relevant technology but then focuses on implementation using Cisco equipment. Detailed configuration of Cisco devices as complementary Cisco accessories. Thorough consideration is given to security-vulnerability, standards-based

and proprietary ways of handling and improving security. Newer technologies like 802.11q, cross vendor roaming and wireless switches are not discussed probably because they are developments of mid 2003, after the book has be published.

In building wireless community networks (2002, O'Reilly), Flickenger focuses on how to build wireless networks of community use with IEEE 802.11b technology, primarily to extent internet access. As such, great details are given to outdoor site survey especially the use of topographical mapping. Network components are introduced and a do-it-yourself approach is employed to increase understanding of such components as antennas and access points.

2.2: THEORETICAL BACKGROUND

COMPUTER NETWORKING BASICS

This is a brief overview of what it takes to get two or more computers to communicate together. Before two computers can communicate to each other, there must be a middle ground between the devices which possibly have a different operating systems, different hardware architecture and are not connected in any way. The main component of a computer networks are:

i. **Network Medium:** This provides a means of transferring signals from one computer to another possibly over large distances. Computers must share a common communication medium before they can communicate. Examples of Network media include twisted pair cabling, coaxial cable, fibre-optic cable and the atmosphere for wireless connection. The network medium defines the limit to the number and type of devices that can be connected to the network, the type of connectors to be used and the maximum span.

ii. **Network Interface:** The computer connects to the network through some kind of interface that is standard for all computers connecting to a medium. Implemented as Network Interface Card (NIC) or Network adapters, most adapters are made for the PCI bus and are usually plug-and-play under most recent operating systems, PCMCIA rules for portable computers while card bus and USB based interface are growing in popularity. Network cards implement the protocols for the Data link layer and the physical layer of the OSI model.

iii. **Network Protocols:** These are common set of agreed upon by which all devices on the network use for communication. Protocols govern such issues like signal interpretation, unique node identification, how to initiate and end communications, etc. The most common network protocol stack is the TCP/IP stack (used on the internet). Other protocols include the IPX/SPX and NetBill which are less popular alternatives.

iv. **Network Software**: The most important software is the Network Operating System (NOS) in which most protocols (typically from the layer three of the OSI model and above) are implemented through software protocols like DNS, DHCP, RADIUS, etc. There must also be software that enables us to use the network; examples are Web Browsers, chat clients and newsreaders. On a windows XP or Linux computer for instance, these software channel their information through the operating system. The different software implements different protocols.

2.3: THE OSI MODEL AND WIRELESS LANS OVERVIEW

The Open System Interconnect (OSI) model is a reference model that was developed by ISO in the early 1980's for communication between computers. It defines a set of open

protocols that facilitates high level, high function networking services among dissimilar computers on a global scale. Originally, it was intended to be the standard international protocol stack for networking; it was unable to unseat the TCP/IP and is now only a reference model for other protocols specification.

The OSI model consists of seven layers that can be sub-divided into two sets: The application set, and the Data Transport set. Wireless LAN standards only specify the physical and medium access control sub-layer of the Data Link layer of the OSI model. All other protocols above the MAC sub-layer apply both for wired and wireless applications.

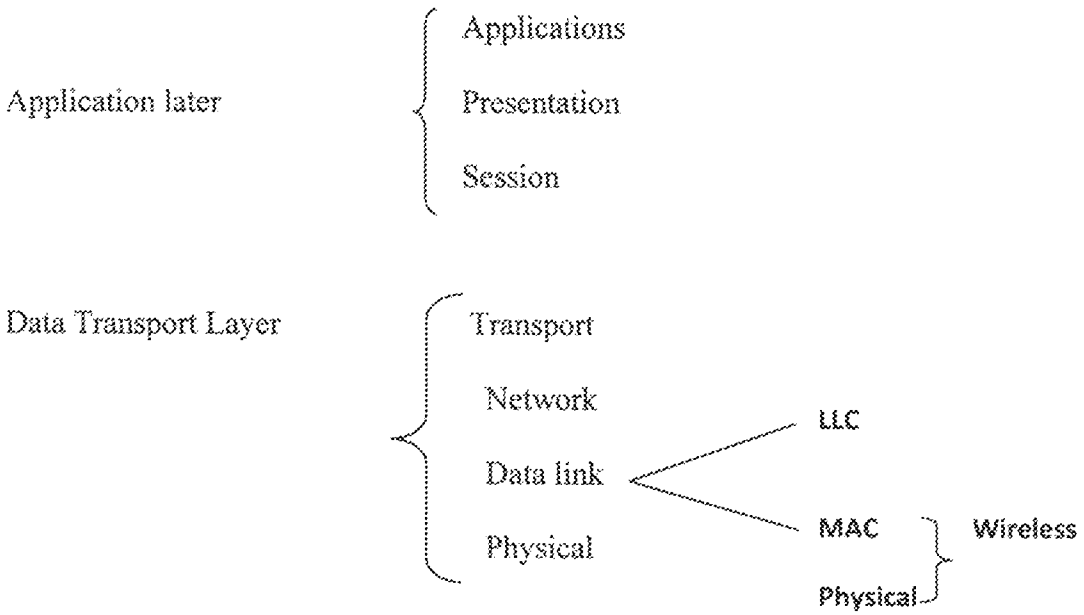


Fig 2.1: LAYERS OF THE OSI MODEL, IN RELATION TO WIRELESS STANDARDS

The table below briefly describes each layer of the OSI model, its function and some protocols in each layer:

TABLE 1: THE OSI MODEL, ITS FUNCTIONS AND PROTOCOLS.

Layer	Layer Name	Functional Description	Protocols
7	Application	Provides a set of interfaces for application to access networks services, handle general network access and error recovery for application. Application talks directly to TCP or UDP	Web browser telnet. HTTP FTP, NFS, DNS. IM, SMTP
6	Presentation	Provides data translation, defines data formats such as ASCII, PNG and GIF, provides syntax and also handles encryption and decryption	JPEG, GIF,PNG, MPEG, ASF, Encryption
5	Session	This defines how to start, control, and end a session. Controls and manages multiple bi-directional messages thus allowing the presentation layer to have a seamless view of an incoming data steam.	RPC, SQL NFS, Net-Bios names Apple talk ASP, DEC net SCP
4	Transport	Multiplexing of incoming data from different flows to application on the same host. Depending on application, transport layer protocols do or do not provide error recovery.	TCP, UDP, SPX
3	Network	Defines end to end delivery of packets by defining logical addresses that enable nodes to be uniquely identified. Routing is defined here. Packet fragmentation done here.	IP, IPX, Apple Talk ICMP

2	Datalink	Define delivery across an individual link thus the protocols are connected with the type of media involved. IEEE standard divides this layer into LLC (Logical Link Control) and MAC (Media Access Control)	IEEE 802.3/802.2 IEEE 802.11 ATM, PPP.
1	Physical	This layer deals with physical characteristics of the transmission medium such as connectors, pins, electrical current voltages, encoding & light	EIA/TIA -232 RJ45, V.24 V.35. IEEE 802.3 IEEE 802.11

2.4: ANATOMY OF A WIRELESS DEVICE

The figure below shows a functional diagram of a wireless device which shows the players involved from the air interface to an application the user is using. The host interface is the card interface to the computing device through one of its bases- typically the PCMCIA but could be PCI, card bus or rarely ISA. This interface allows the driver to communicate with the MAC controller and is characterized by speed (I/O, shared memory or DMA) and the ability to process request in parallel.

With all modern Operating System, the end application does not access directly the hardware; it uses a standard Application Programming Interface (API). The operating system needs a driver to interface the hardware to the network stack (TCP/IP, NetBEUI,

IPX/SPX, etc.). The main function of the driver is to manage the hardware and to answer its request, i.e. service interrupts.

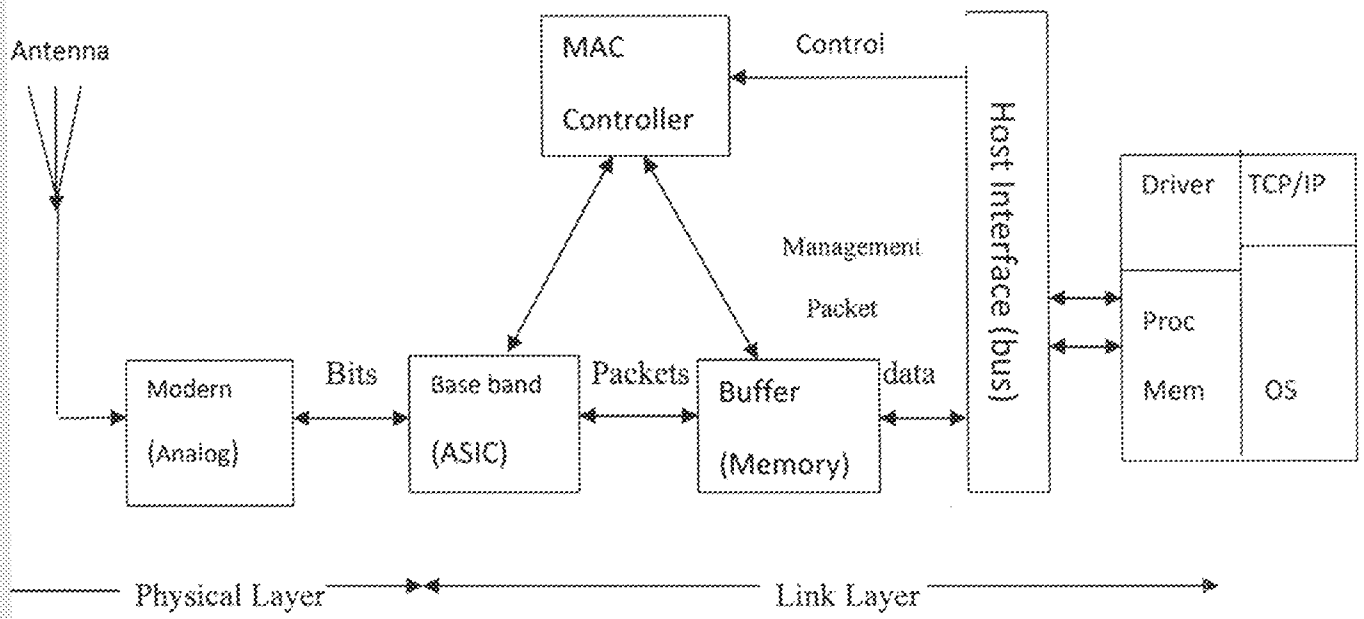


Fig 2.2: FUNCTIONAL DIAGRAM OF A WIRELESS DEVICE FROM AN OSI PERSPECTIVE

2.5: WIRELESS LAN TRANSMISSION TECHNOLOGIES:

2.5.1: INFRARED: This technology use IR beams to send signal between devices, because strong ambient illumination is a source of interference. The device must generate reasonably strong signals for communication to be effective in an office environment or outdoors. As a WLAN solution, infrared is pretty much dead but it finds applications in wireless printing and small short range ad-hoc networks. In fact most notebooks made within 1998-2000 and using windows operating system have infrared capabilities built in that enable them seek other infra-red devices nearby and communicate with them at transmission rates of up to 10Mbps at practical distance of 30.48 (100') maximum.

2.5.2: NARROW-BAND SINGLE FREQUENCY RADIO LAN TECHNOLOGY

This technology use low powered two-way radios in which receivers and transmitters are tuned to the same frequency. They don't require LOS so long as the devices stay within max range of 70m. The table below gives the characteristics of this frequency.

TABLE 2.2:

CHARACTERISTICS	VALUE
Frequency Range	Unregulated: 902-928MHz, 2.4GHz 5.72-5.85 GHz
Max Distance	50-70m
Bandwidth	1-10Mbps
Interference	Highly susceptible
Security	Highly susceptible to eavesdropping

2.5.3: MULTI-PATH DISTORTION IN RF CHANNELS:

Multi-path is the composition of a primary signal plus duplicates or echoed images caused by reflections of signals off objects between the transmitter and receiver. Multiple path distortions occur because there are multiple paths for a wave to travel from transmitter to receivers. When a wave radiated from the antenna of an access point for example, that signal could get reflected off different surfaces in different path and reaches the receiver a bit later and out-of-phase with the original signal. These multiple versions of signal interfere with each other, a phenomenon called Inter Symbol Interference (ISI). In real life, the signal is called delay spread, which can be as high as 4 micro-seconds (4 μsecs).

The figure 2.3 below illustrate multi-path for an indoor scenario:

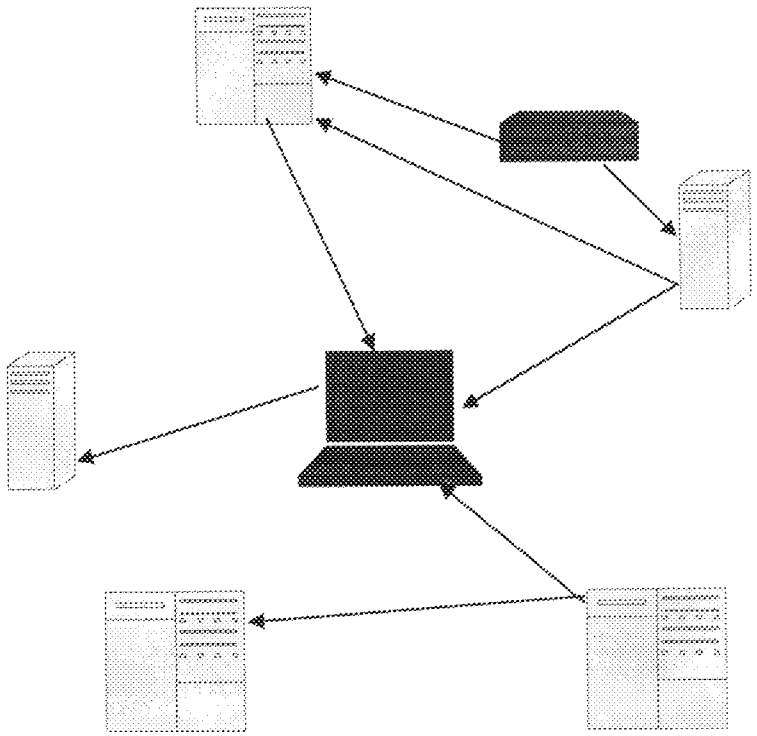


Fig 2.3: Multi Path Phenomenon in A Typical Office Setting.

The channel impulse response (CIR) is a common representation of a Multi-path channel and is the signal at the receiver if a single pulse is transmitted. A critical measure concerning the multi-path channel is the delay. Tmax of the longest path with respect to the earliest path. T. A received symbol can be theoretically influenced by Tmax/T

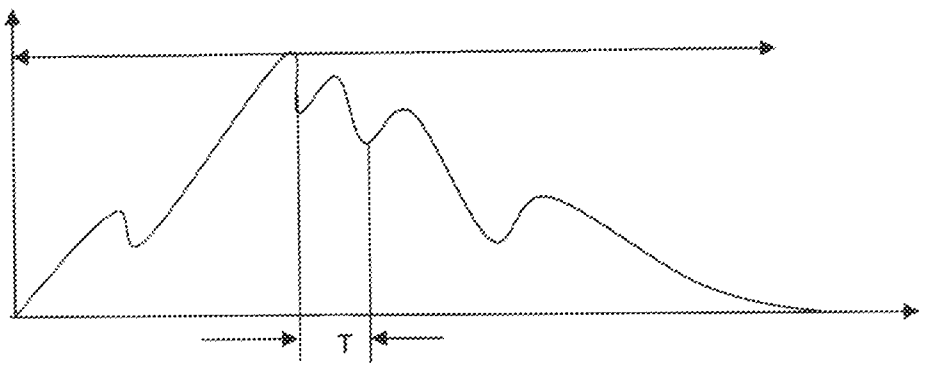


FIG 2.3: THE CIR REPRESENTAITON OF MULTI-PATH RF CHANNEL.

.5.4: SPREAD-SPECTRUM

Spread – spectrum is an RF transmission technique in which the baseband is intentionally spread over a larger bandwidth by injecting a higher – frequency signal (pseudo random noise code) which is the modulation waveform. As a direct consequence, energy used in transmitting the signal is spread over a wider bandwidth and appears as noise. The ratio (in dB) between the spread baseband and the original signal is called processing gain.

Typical spread- spectrum processing gains run from 10dB to 60dB. Different spread – spectrum techniques are available but they all have one idea in common; the Pseudo-random noise code or key attached to the communication channel. The manner of inserting this code precisely defines the spread-spectrum techniques in question.

The figure below shows the generalized paradigm of spread spectrum communication.

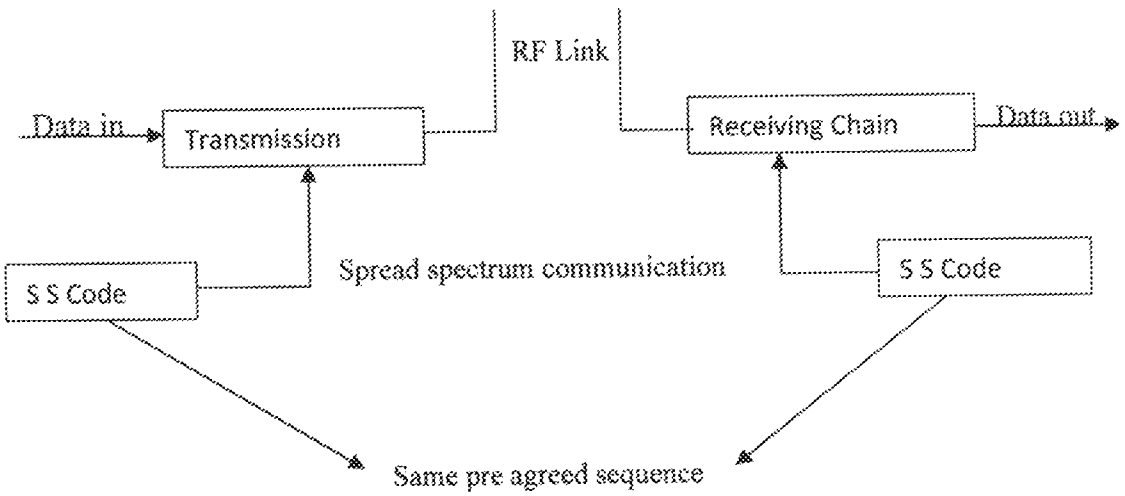


FIG 2.4: GENERALIZED PARADIGM OF SPREAD SPECTRUM COMMUNICATION

THE EFFECT OF SPREADING / DESPREADING ON THE BANDWIDTH:

More bandwidth is used but it is not wasted because multiple users can share the bandwidth. Spread-spectrum modulation is applied to signals that are already modulated by some digital modulation scheme, usually BPSK.

An important point to note is that any signal not receiving the spread-spectrum code (SS), like noise or signal from other transmitter will remain un-spread and during the de-spreading operation, it will be spread, thus making the system less susceptible to noise and jamming.

2.6: WIRELESS LAN STANDARD:

2.6.1: HOME RF:

This is a non-IEEE wireless LAN standard that operates at 2.4GHz with current bit rates of up to 22Mbps and is primarily geared toward the home. It has a relative range of 45.72m (150ft) and it uses Frequency Hopping Spread Spectrum (FHSS) as the physical layer transmission mechanism. It has the same architecture as Bluetooth; i.e. clients can connect to ad-hoc or link to a central connecting point. The inclusion of standard Wireless Access Protocol (SWAP) gives Home RF the capability to handle multimedia applications more effectively than older versions of 802.11 technologies. SWAP 2.0 extended the bit rate to 10Mbps and provided roaming while increasing security from 40 to 128 bit encryption. A SWAP can consist of three types of devices; a control point, synchronous voice device and an asynchronous data device which is a typical mix for the home environment. The incorporation of DECT technology in the Home RF protocol stack gives it some voice/phone-centric capabilities like caller ID.

The Home RF operates in two layers as relate to the OSI model, that is Mac sub layer and the physical layer.

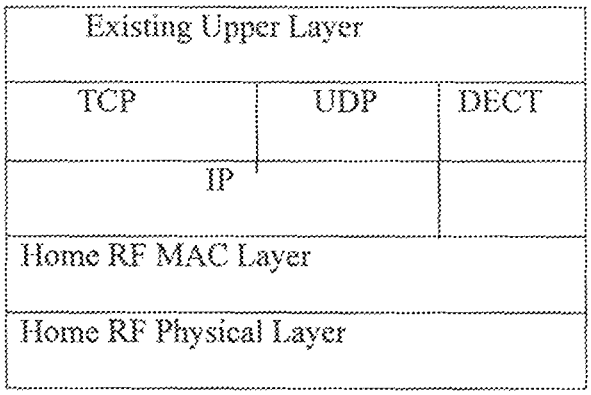


Fig 2.5: HOME RF RELATIONSHIP TO THE OSI MODEL

2.6.2: THE IEEE 802.11 FAMILY OF STANDARDS

This is a wireless networking standard that is defined by the institution of Electrical and Electronics Engineering (IEEE) committee 802.11. This standard is only concerned with the physical layer and MAC sub-layer of the datalink layer. The standard defines the network topologies, air as the transmission medium, medium access methods to which manufacturers must conform to for their devices to be inter-operable. The standard ensures that all stations both radio-based network interface cards (NIC) and access points implement access methods for sharing the air medium. The three physical layer options for 802.11 are infra-red (IR), baseband PHY and two RF PHY's. Due to line-of-sight limitations, very little development has occurred with infra-red 2.4GHz bandwidth with OFDM implemented for later development. These different physical layer implementations have different data rates and ranges: IEEE 802.11b uses DSSS and

another method called complementary code keying (CCK). IEEE 802.11a uses OFDM while 802.11g uses DSSS/CCK and OFDM. All wireless LAN uses the same LLC sub layer implementation as both Ethernet and token ring.

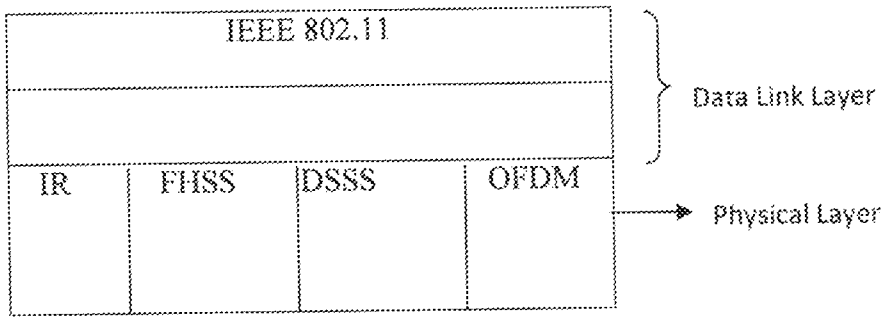


Table 2.2: IEEE 802.11 FAMILY STANDARDS.

IEEE STANDARD FOR WIRELESS LAN WITH RESPECT TO OSI MODEL

Nine services implemented in software and hardware work behind the scene to support the 802.11 architecture, four of these services are station services while the remaining five distribution services.

2.6.3: HYPERLAN /2

This is a wireless LAN standard developed by the European Telecommunication Standard Institute (ETSI) under its broadband Radio Access Network (BRAN) program. It is similar to the IEEE 802.11a in the physical layer. Hiperlan/2 operates in the 5GHz frequency band using orthogonal frequency division multiplexing (OFDM) and offers data rates of up to 54MBps.

However, these similarities stop at MAC layer. While 802.11a uses carrier sense multiple Access with collision avoidance (CSMA/ CA) to transmit packets, Hiperlan/2 uses Time Division Multiple Access (TDMA).

Unlike CSMA/CA where stations have to wait for an indefinite period of time before they can send packets, TDMA allocates time slots for each station based on the station's need for throughput. The stations then transmits at regular intervals according to their respective time slots making more efficient use of the medium and improving support for voice and video applications.

Hiperlan/2 has a number of attractive features, amongst which is higher throughput. Both 802.11a and Hiperlan/2 boasts maximum throughput of 54MBps, however, the actual throughput of Hiperlan/2 is 42MBps while for 802.11a is 18MBps. Hiperlan/2 also implements quality of service (QoS) protocols for different sorts of connections. Hiperlan/2 is presumably more cost effective that 802.11a. While the initial Hiperlan/2 products will cost more than its 802.11a counterparts, the better throughput outweighs the slight price difference. Another unique feature of the Hiperlan/2 is its ability to interface with other high speed networks including 3G cellular, Asynchronous Transfer Mode (ATM), etc.

2.6 WIRELESS NETWORK TOPOLOGIES

In traditional wired networking, the topology is the specific physical (real or logical i.e. virtual) arrangement of elements on a network. It is also referred to as network architecture. It refers to how various network equipment and nodes may be

interconnected to function properly. Wireless networks can operate in one of three topologies:

- Basic service set
- Independent Basic Service Set and
- Extended service set.

2.6.1 BASIC SERVICE SET (BSS) NETWORK

A BSS is a set of stations controlled by a single co-ordination function. A co-ordination function is a logical function that determines when a station can transmit or receive. A basic service set consist of at least one base-station (access point) connected to a wired network and a set of wireless clients associated to it. All communication between wireless clients must pass through the base station which acts like a server for the cell or channel.

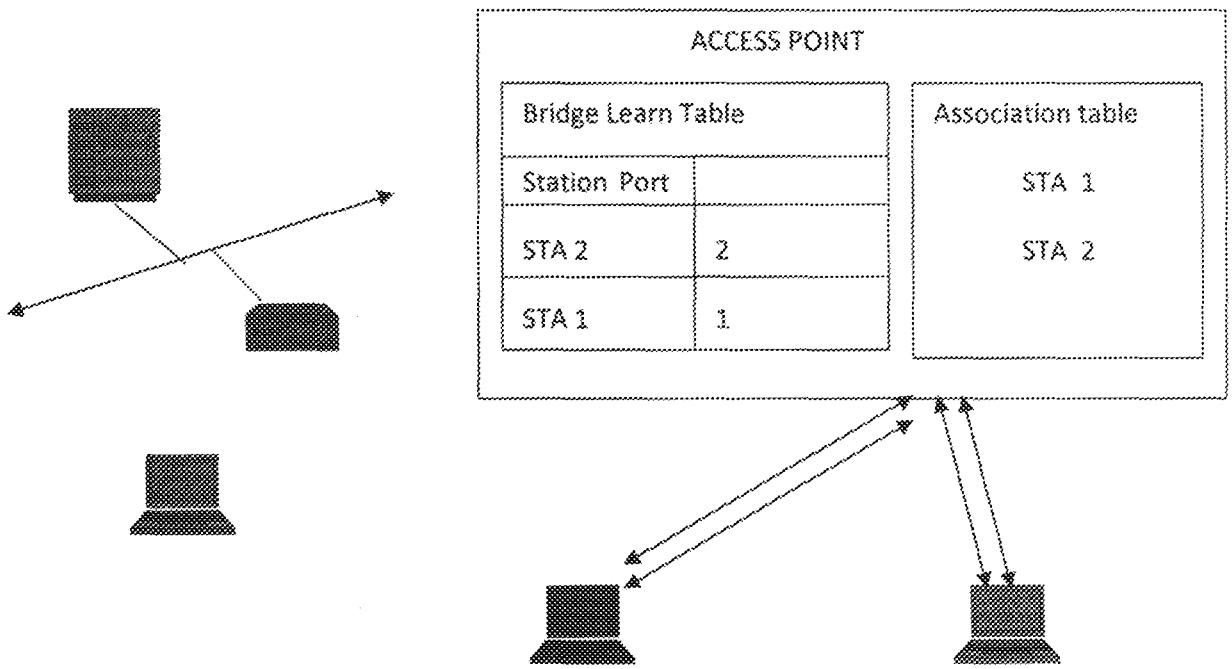


FIG 2.6: BASIC SERVICE SET NETWORK

.6.2 INDEPENDENT BASIC SERVICE SET (IBSS) NETWORK

This is also called the ad-hoc network. This architecture is the equivalent of a peer-to-peer wired network. An IBSS is a basic service set which forms a self-contained network in which there is no access to wired LAN. Wireless client in this topology can communicate directly with one another. No access point or connection to a wired network is required. One of the stations is configured to initiate the network and assumes the co-ordination function periodically broadcasts beacons to offer connection parameter to potential clients. When a device is configured for ad-hoc, if it doesn't see a beacon with a matching network name, the device itself will start issuing beacons. All stations in an IBSS network participate in sending beacons. This is done by initiating a random timer prior to the point in time when the next beacon should be sent. The firs station whose timer expires sends the beacon.

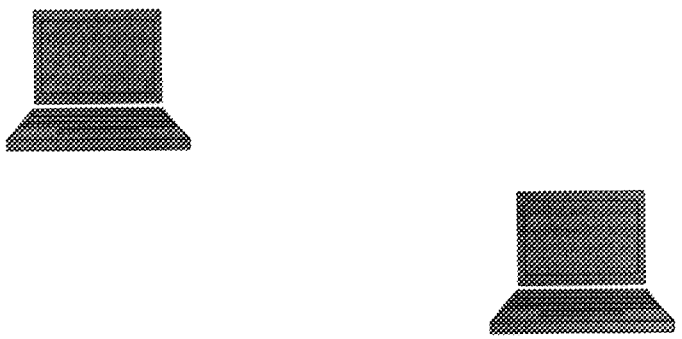


FIG 2.7: INDEPENDENT BASIC SERVICE SET NETWORK.

2.6.3 EXTENDED SERVICE SET (ESS) NETWORK

An ESS network consists of a series of overlapping BSS network in which the respective base stations are interconnected by a distribution system (DS)-typically an Ethernet LAN.

Wireless clients communicate with each other through the access points and can roam between them seamlessly if the footprints of the access points overlap and if configuration remains consistent. Each of the stations must be operating on a separate wireless channel to avoid any interference.

For wireless distribution system, the access point will typically have two wireless PC cards, one that serves as the distribution system port and the other which interfaces with clients collating wireless cards like this raises issues with frequency channel allocation so that no interference occurs locally. The configuration must also ensure that clients don't associate with the card that serves the distribution system. This can be accomplished by setting the relevant SSID ad security options to not match what the clients have.

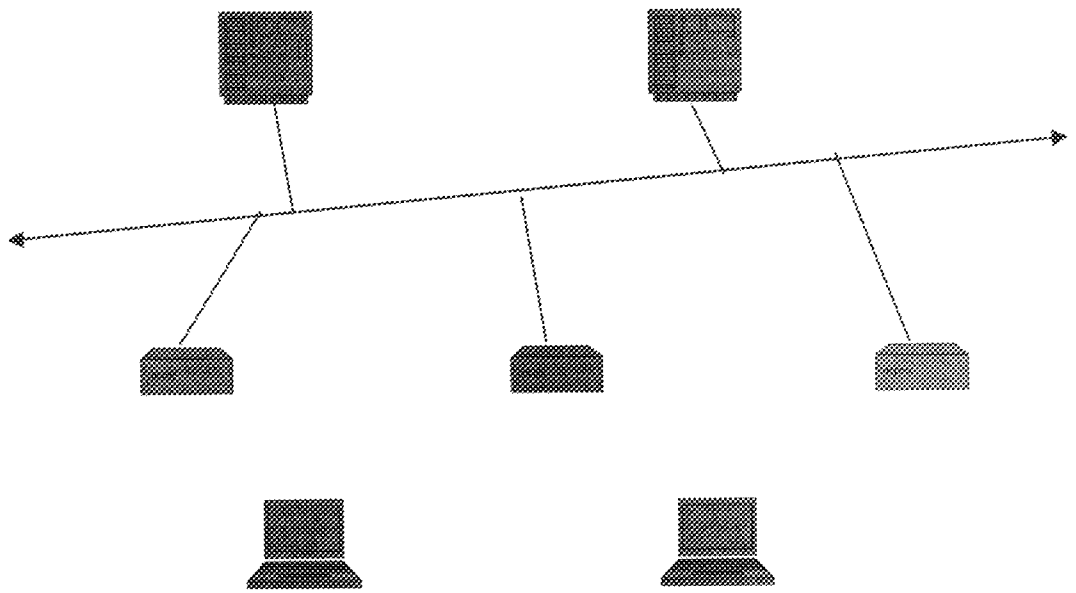


FIG 2.8: EXTENDED SERVICE SET NETWORK

.7 SWITCHED WIRELESS LANs

Traditional access points offer a shared medium, wherein clients take turn transmitting data. Collision occurs if two nodes try to transmit at the same time, necessitating a re-transmission of the packet. This increases the amount of time it takes to send a packet which reduces overall throughput of the wireless LAN. Switched wireless LANs enable multiple wireless clients to communicate with the same access point simultaneously and it eliminates collisions between packets resulting in better range and throughput.

One approach to wireless LAN switching is to have a single access point switch that takes the place of multiple access points. The switch uses planar phased array antennas to support simultaneous traffic for a given number of users, 1, 150 for the vivato wireless LAN switch). The access point switch covers its footprints using highly directive narrow bends that automatically points to specific clients roaming through the facility instead of transmitting RF signals in every direction like traditional access points, the device uses proprietary technology to concentrate power into a single directional beam, very much like a movable high-gain directional antenna. Since the switches use phased – array antennas, they can send different signals in different directions at the same time. This enables simultaneous collision free transmission among clients associated with the same access point.

Another approach is to have a single Ethernet – based switch that interconnects many 'thin' or 'lite' access points mounted throughout a facility. This switch runs the control and management functions for the wireless network. All of the intelligence and features found in normal access points go into the switch. The lite access points are relatively simple and simply download a configuration from the wireless switch.

.7.1 ADVANTAGES OF SWITCHED WIRELESS LANS

Increased capacity and range: Results from multiple simultaneous directed RF beams from intelligent antenna array to each client. Directivity increases range while multiple simultaneously beams increase capacity. Potential savings in cost for large implementations can be made from these increases.

Simpler installation: Due to user separation by switching mechanism rather than RF channels, the usual hassles of RF channel planning practically disappear.

Centralization of network management in the switches makes configuration and troubleshooting a lot easier. Because there are generally fewer components, there is a much lower chance of something going wrong.

Improved security: it is possible to implement tighter security measures, mainly because centralization limits the number of devices that hackers can exploit.

2.7.2 DISADVANTAGES OF SWITCHED WIRELESS LAN

* High initial cost: Vivato's wireless LAN switches cost from $8,995 to $13,995 as at January 2004.
* No ratified standards for wireless LAN switches
* If lite / thin access points are not directly connected to the wireless LAN switch, then it could leave wireless users data unprotected on the wired segment.
* If the wireless LAN switch is placed in the data room with many intermediate LAN switches / routers between it and the lite access points, then there may be an additional propagation delay as all packets must make a round trip for access

point to switch and back. This significantly increases the load on the enterprise wired LAN.

CHAPTER 3: DESIGN OF A WIRELESS NETWORK

3.1 DEFINING REQUIREMENT FOR THE WIRELESS NETWORK

Knowing the requirements of the intended network enables better information gathering, therefore better planning. This information can be gathered via questionnaires, interviews with employees and other future users of the WLAN and also consultation with the organization's IT department.

The most common requirements are:

i. **User profile and Interface requirements:**

This identifies the attributes of each person who will be utilizing the system, providing human factors that designers can use for better select or develop applications. In additions, the profile assists the installation team when assigning user names. The user profile should identify the person's names, job title and description, level of networking experience and knowledge of application. Users will require some form of interface to the system's databases and other resources. Most interfaces today are graphical – client – server – based applications.

ii. **Functional requirements**

Functional requirements describe what the users and the organization expect the system to do. Therefore, functional requirements run parallel to the tasks and actions users anywhere on a network perform. For example, the need to access the internet or the local email or database server from anywhere on a campus is a functional requirement. In most cases, application software's implements functional requirements.

iii. **Application requirements**

Applications requirements specify that the wireless LAN and utilize specific applications. For instance, the use of Microsoft office as the standard for office automation is an application requirement and it helps in determining how much bandwidth each user will need, thus defining the user experience as well as the number of access points required. A good rule of thumb for an 802.11a network is to allow for 2Mbps downstream and upstream (4Mbps total) per user, which delivers about the same user experience as being on a shared wireless LAN. For an 802.11b network, a rule of thumb is to allow for 500kbps each way (1Mbps total) which delivers a good user experience for a very fast internet connection.

iv. **Information flow requirements**

Business processes within companies depend heavily on communications. For this requirement, specify the information path flow between people and systems, types and formats of information sent, frequency of information transaction and maximum allowable error rates. These requirements will provide a basis for the selection of network components as well as determine roaming pattern and security profiles.

v. **Mobility requirements**

These describe the movement of the users when performing their tasks. They should distinguish whether the degree of movement is continuous or periodic. When the user or network component must have the capability to utilize network resources while physically moving, they are said to be in continuous movement. example: Users of VOIP phones and handhelds and healthcare professions. These requirements will distinguish between seamless and nomadic roaming.

3.2: SOME GENERAL WIRELESS DESIGN CONSIDERATION

3.2.1 UNDERSTANDING WIRELESS PERFORMANCE PARAMETERS

This is especially important in order to set expectations for the end users as well as plan a particular implementation based on products with a given specification. Performance parameters include: Data rate, throughput, response time, power consumption and capacity.

i. **DATA RATE:** Most product data sheet gives the data (or bit) rate which is speed of all data transfer in Mbps. Example, 11Mbps max for 802.11b and 54Mbps for 802.11a. The data here involves management and protocol control frames which do not directly give value to the user. Bit rate depends on the kind of digital modulation used, error correction and protocol overhead and usually automatically drops with distance between transmitter and receiver in predetermined steps as defined by the associated standards. Data rate fails as range increases and the range is directly proportional to the access points transmitting power. It is often necessary to lower transmit power in order to limit range and thus increase associated data rate.

ii. **THROUGHPUT:** Expressed in kilobytes per second, this is a performance parameter that the user actually faces. It reflects when a user transfer files, streams media or some other operation that moves data over the wireless LAN. Throughput is always lower than the bit rate due to overheads in implementing the MAC and PHY, interference or operating systems efficiency in implementing protocols stacks – In OFDM based systems, only 48 of the 52 sub-carriers are used to carry data, the other four are used for protocol overhead and signal protection. Throughput as perceived by users depends on:

- Topology (IBSS, BSS or ESS) being used
- Protocol stacks being used (TCP/IP, NETBEUL, IPX/SPX) – The OS comes in here.
- Number of stations in the cell
- Path between station and access point (distance and destructions may cause lots of retransmissions)
- File size being transferred.

Data throughput is affected by interference which can cause collisions. When collisions occur, the packets involved must be retransmitted entirely. Some access points handle this issue by fragmenting packets so that smaller frames are sent.

Throughput from LAN products based on chipset that support frames bursting is better. Frame busting is an implementation of the IEEE 802.11e draft specification that cuts on traffic overhead, thus leaving more bandwidth available for data.

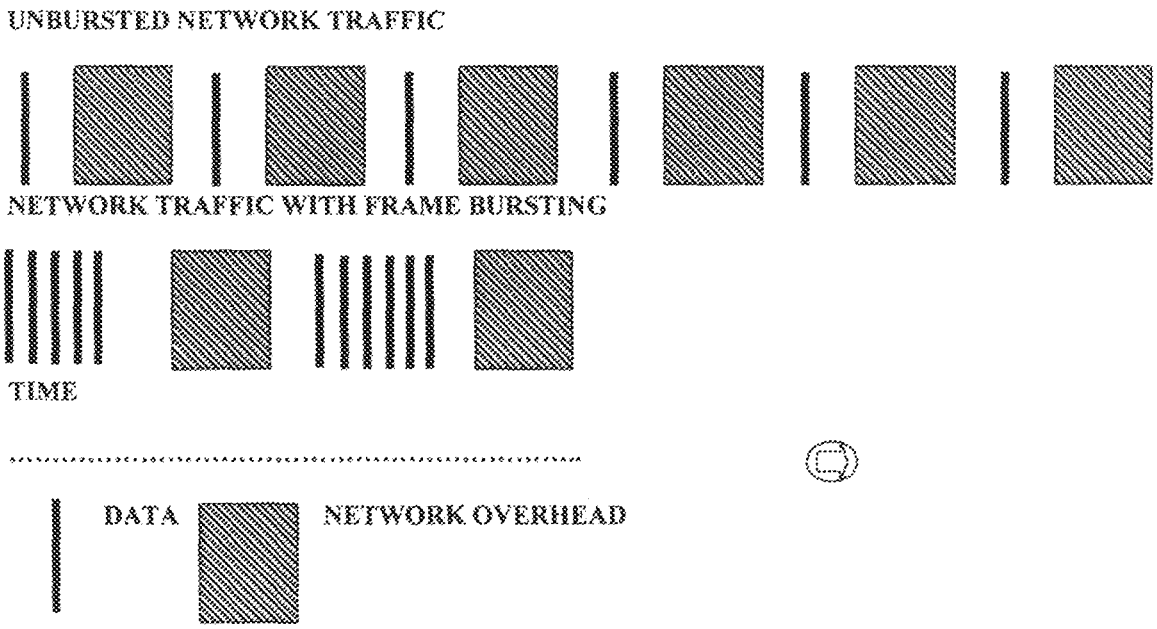


FIG 3.1: INCREASING THROUGHPUT WITH FRAME BURSTING

iii. **CAPACITY:** This refers to the number of stations that can exist in a single cell. Cell capacity is determined by:

- **Application bandwidth requirements:** Office automation requires more bandwidth than simple internet access for example while CADD and photo editing require more bandwidth than word processing.
- **Cell dimension:** Since data rate falls with increased range, the smaller the cell, the higher the bit rate, throughput and capacity.
- **Available** bandwidth per cell (directly proportional) to throughput)
- **Number of collocated cells:** Can potentially double or triple cell capacity. The number of collocate – able cells depends on the number of non-overlapping channels available for use. In real life, the total throughput from N collocated cells is always slightly less than N times the typical throughput per channel.

3.2.2 FACTORING IN ATTENUATION:

For a network to perform well, one must anticipate sources of attenuation and factor them in the design so as to set user expectations realistically. RF is subject to the inverse square law of electromagnetic radiation – in practical terms this means that the further you go away from an antenna, the weaker the signal becomes. WLANs fall in the category of UHF (>300MHz) wave propagation which is line of sight (LOS) dependent. Thus any solid obstacles in the path of the wave will further attenuate it, these includes, walls, doors, windowing, filling cabinets, shelves and other buildings.

Because the components and processes upon which a wireless system is based are far from perfect, their use also introduces some attenuation especially in cabling. Cables that

bear RF waves have when installing access points and antennas. Cable attenuation is best handled using the shortest possible very high quality low – loss cabling between the access point and antenna or amplifier. It is better to run long Ethernet cabling than long RF cabling.

Weather conditions such as rain, fog, harmattan dust and mist and snows (in areas where applicable) only have effects on higher frequencies (>20GHz) where associated wavelengths becomes comparable to the physical sizes of rain drops etc. Natural atmospheric absorption has a very small effect on WLANs operating in the 2.4GHz range (1dB per 100 miles).

Attenuation from solid objects must be handled by a higher access point density using antennas with higher gain and greater directivity as required. For long point to point or point to multipoint links, the free space path loss (Lo) is:

$$Lo = 20 \log (d) + 20 \text{ Log } (f) + 36.6 \text{ (dB)}$$

Where (d) = Link distances in mile

(f) = Central frequency in MHz or RF channel being used.

3.2.3: FACTORING IN MULTI-PATH DISTORTION

Although the medium access /channel coding schemes used in wireless LANs have inbuilt capabilities to handle multi-path distortion. It can be further reduced based on an understanding of the RF properties of an antenna. Practically, especially for point – to – point links, two things can be done:

- Using antennas with high directivity: as such, reflected signals in the 'dead zone' will have no effect on performance. Fig. 3.2.3 illustrates these using two yagi antennas.

- Using antenna diversity: An antenna splitter is used to connect two antennas to the same radio on the access point. The access point then dynamically selects which antenna to use depending on the signal quality factor of that antenna. The access point can switch between the antennas and work with different clients from different antennas. In these modes only one of the antennas is used at any given moment.

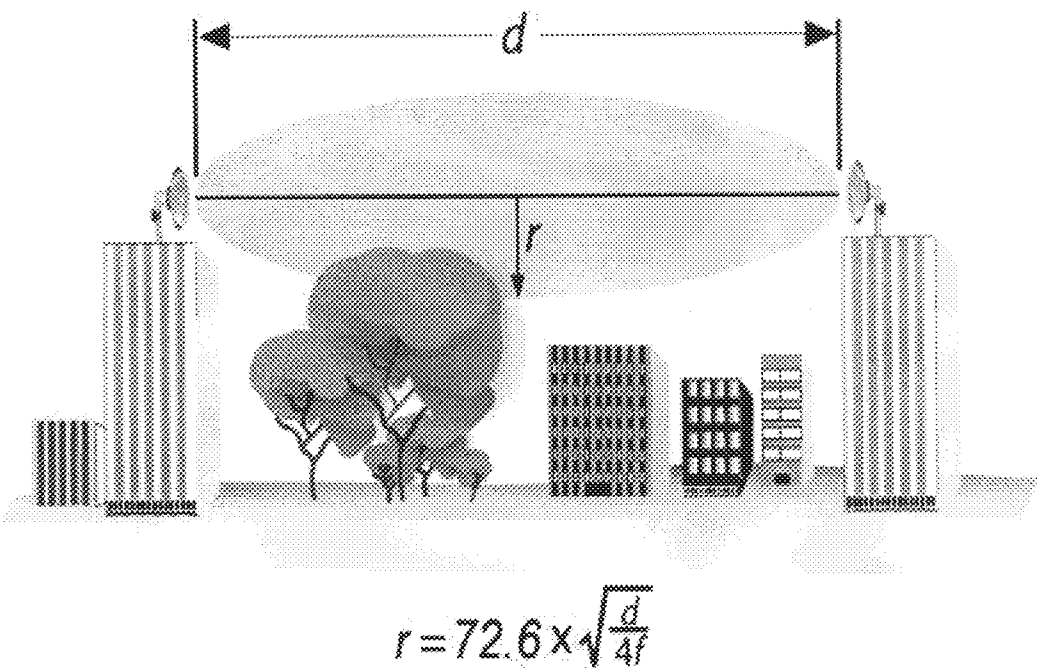


FIG 3.2:TWO ANTENNAS EXPLAINING THE FRESNEL ZONE.

3.2.4: FACTORING IN EARTH'S BULGE – THE FRESNEL ZONE AND ANTENNA HEIGHTS

A pair of antennas define a three dimensional elliptical RF propagation path which is divided into several zones called Fresnel zones based on the phase and speed of the propagating waves. Fig. 3.2.2 illustrates a typical long RF path between two antennas.

This brings up an important issue in point – to- point to multipoint links: Radio line-of-sight is not the same as visual line-of-sight. Radio line-of-sight is not a straight line between the antennas; it is more of an ellipse. In a good point –to-point link design the Fresnel zone must be clear of obstacles and any reflective surfaces (that create multi-path) to provide a good signal. The radius of the midpoint radius of Fresnel zone is given by:

$$R = 72.1 \sqrt{\frac{d_1 d_2}{F\,(d_1+d_2)}} = 72.1 \sqrt{\frac{d}{4f\,(\text{miles})}}$$

Where:

d = distance between the transmitter and the receiver (feet d_1 and d_2 are distances from each point of the path F = frequency (GHz)

The antenna must be high enough to clear the Fresnel zone at the midpoint radius. To get good link quality, the industry standard is to jeep at least 60% of the Fresnel zone radius clear of obstacles. Any object that extends up to 40% into the Fresnel zone radius at its widest zone will adversely affect link quality. For links that span more than 11;265km (7 miles), an additional antenna height must be included to cater for the earth's curvature. This additional antenna height is given by:

$$\Delta h = d2\ /8\ (\text{miles}).$$

Thus, for a 60% clearance of the midpoint radius of the Fresnel zone for a link that is longer than 7 miles, the antenna height is:

$$h = 0.6 \times 72.1 \sqrt{\frac{d_1 + d_2}{4F \quad 8}} = 43.26 \sqrt{\frac{d + d2}{4f \quad 8}}$$

3.2.5: WHAT WI-FI MEANS

Wireless fidelity (Wi-Fi) is a logo carried by wireless LAN equipment to show that it has passed the Wi-Fi alliance tests to ensure that it works according to specification and is inter-operable with all certified equipment. During implementation, especially if using equipments from different vendors, it is wise to ensure that all wireless LAN components are Wi-Fi certified so that interoperability between interoperable devices will not be an issue. However, with the vagaries of wireless LAN technology reaching a pitch, it is a lot safer to stick with equipments from the same vendor.

3.3: CONSIDERATIONS FOR THE FREQUENCY BAND AND THE NUMBER OF CHANNELS

The higher the frequency of operation, the shorter the range of the signal and the higher the free space path loss. To increase the capacity and or coverage calls for frequency or channel reuse and with out proper planning. Co-channel interference can severely hamper operation. There are only 3 non-overlapping channels in the 2.4GHz band while there are at least 8 or more in the 5GHz band. The four colour theorem in mathematics implies that the minimum number of overlapping channels required so that no adjacent cells use the same channel if our thus there is no configuration of channel in the 2.4GHz (802.11b/g) in which no two adjacent channels overlap. This imposes severe limitations for deploying high capacity (channel co-location) or seamless roaming applications in a large area for 802.11b/g. innovation in wireless LAN switching which employ dynamic frequency selection (DFS) mean that frequency planning is no longer a big design issue because the switch and / or associated smart antenna system handles it automatically.

3.4: DESIGN CONSIDERATION FOR MOBILITY

When users roam, if they associate with an access point that is attached to a different port on a different switch and router subnet, any current IP sessions may be compromised as in effect the session will loose layer 3 connectively. On a wireless LAN, network permissions now need to follow users as the roam. A mobility requirement imposes a persistent IP configuration on a client so that sessions are not lost during new associations or during handoffs. Also the path through which the use is expected to move must have RF coverage all the way, preferably of the same uniform capacity.

3.5: DESIGN CONSIDERATION FOR HIGH PERFORMANCE

By high performance, I mean data throughput of more than 20Mbps as may be required if a wireless LAN is being implemented in lieu of a wired LAN. Since present standards limit maximum data rate of 54Mbps at typical throughputs of about 25Mbps that will be maximum per cell. However, using proprietary methods, some systems are capable of data rates of 72Mbps. The most capacity can be obtained when channels are collocated thus making the maximum throughput theoretically equal to the number of non-overlapping channels times the maximum throughput for the topology, (see table in section 3.9.1. and 3.9.2) this comes to more 300Mbps.

3.6: DESIGNING EXTERNAL POINT TO POINT TO MULITPOINT LINKS

The longer distance between transmitter and receiver, the more difficult it becomes to obtain visual line of sight, ensure 60% clearance of obstacles in the Fresnel zone as well as compensate for the earth's curvature. Whether point to point or point to multipoint,

high gain directional antennas must be used at the receiving end with same for transmitter if it is a point to point link and an Omni or point to multipoint links.

An important analysis that must be done for such links is the system operating Margin (SOM) or Edge Margin which is the difference (dB) between the nominal signal level received at one end of radio link and the signal level required by that radio to assure that a packet of data is decoded with input error,. The higher the SOM, the better the quality of the link. The effective isotropic radiated power (EIRP) is the actual power (dBm) as measured in the main lobe (or focal point) of an antenna.

$EIRP = P_t - L_{ct} + G_t$ (dBm)

G_t = Transmitter antenna gain in dBi

Pt = Power of transmitter radio in dBm

L_{ct} = Less in coaxial cable connecting transmitting radio to

Antenna measured in dB.

The received signal power is then calculated as:

$Pr = EIRP - Lo + Gr - L_{CR}$ (dBm)

Pr = Receiver radio power in dBm

Gr = Receiver transmitter antenna gain in dBi

Lo = Free space loss

Lcr = Loss in coaxial cable connecting receiver radio to antenna

SOM = Pr – Sr (dBm)

Sr = Receiver radio sensitivity in dBm

Ultimately, the measure of good link quality is the signal to noise ratio (SNR) and by using careful RF planning to avoid interference as well as directional antennas to compensate for multi-path, on acceptable SNR could be obtained.

3.7: COMPARING DIFFERENT TECHNOLOGIES WITH RESPECT TO DESIGN REQUIREMENTS

TABLE 3:

PARAMETER	IEEE 802.11B	IEEE 802.11a	IEEE 802.11a
TECHNOLOGY	DSSS	OFDM	DSS(CCK)/OFDM
Frequency range	2.4 – 2.4835 GHz	5.15 – 5.35GHz 5.725 – 5.825GHz	2.4 – 2.4835 GHz
Typical indoor range	30m at 11Mbps	23m at 36Mbps	23m at 36Mpbs
Data Rate (Mbps)	1,2, 5.5, 11	6,9,12,18,24.36,48,54	1,2,5.5,6,9,11,12,18,24,36,48,54
Typical maximum throughput	7Mbps	25Mbps	8Mbps in mixed mode = 25Mbps in pure mode
Non-overlapping channels	3 (1,6 and 11)	12	3 (1, 6 and 11) 8 x 3 = 24Mbps
Maximum capacity with channel co-location	7 x 3 = 21Mbps	25 x 12 = 300Mbps	25 x3 = 75 Mbps

User Per AP Cost	Low cheapest	Higher than 11b expensive: shorter ranger implies more access point for larger	Higher than 11b more expensive than .11b but cheaper to implement than .11a
Compatibility	With 802.11g only	With 802.11g only	With 802.11b and a
Susceptibility to interference	From Bluetooth, cordless phones and microwaves oven	None	Same as .11b.

3.8: SITE SURVEY FOR A WIRELESS LAN IMPLEMENTATION

With wireless systems, it is very difficult to predict the propagation of radio waves and detect the presence of interfering signals without the use of test equipment. Even when using Omni directional antennas, radio waves do not travel the same distance in all directions because, walls, doors, furniture, people and other obstacles offer varying degrees of attenuation which cause the RF propagation pattern to be irregular and unpredictable.

STEPS TAKEN TO CARRY OUT SITE SURVEY:

- **OBTAIN A FLOOR PLAN:** I could not get the blue print of the complex, so I made a sketch of the floor plan of the building taking into consideration the windows, doors, stairways, corridors, offices, lecture halls, laboratory, etc on AutoCAD.

  A copy of the floor plan is attached in the appendix.

- **VISUALLY INSPECT THE FACILITY:** This is just to make sure the diagram I have reflects the existing structure. This is a good time to note any potential barriers that may affect the propagation of RF signals, such as metal racks and partitions.
- **IDENTIFY USER AREAS:** On the facility diagram, I marked out the areas of fixed and mobile users. In addition to illustrating where mobile users may roam, indicate where they will not go. Marking out the roaming area is just to minimize the use excess access points.
- **DETERMINE PRELIMINARY ACCESS POINT LOCATION:** By considering the location of wireless users and range estimations of the wireless LAN products we are using, we should approximate the location of access points that will provide adequate coverage throughout the user areas. For roaming, plan for overlap with the consequent requirement that adjacent channels be non-overlapping. An access point signal may reach floors above and below the one on which it is installed.
- **DETERMINE ANY EXISTING RF ACTIVITY:** Prior to placing your own access points, it is nice to get a good knowledge of RF activity in the facility. This involves but is not limited to other access points being run by neighbors, as well as other devices that operate in the unlicensed frequencies. A spectrum analyzer is ideal for this purpose or other specialized devices like fluke Network's wave – Runner which locates devices and the channels in which they operate. But for this design, I could not get hold of any of these equipments, so considering that the entire school building is new, I assumed that no other RF activity is in existence in or around the complex. So it will be safe to install our access points without interference.

- **DOCUMENT FINDINGS:** After indicating access point location and carrying out the design, it is also important to provide a log of signal readings and supported data rates near the outer propagation boundary of each access point as a basis for future redesign efforts. Typical information to be documented includes:
- Access points MAC and IP addresses
- Switch ports that feed access points
- Vlans identify if you are using VLAN to segment traffic
- Information about access point that you don't own/control
- A listings of access points configurations: firmware and hardware revisions
- The powering method for each access point either POE, power injector or mains
- For lite access points, any redundancy connection mode
- Which access points are fat and which are lite fat access points contains sensitive security data and so cannot be placed just anywhere.

3.9: THE COMPONENTS OF A WIRELESS LAN

3.9.1.1: WIRELESS NICS:

Every station that needs wireless access must have a wireless network card installed. Typically, a PCMCIA card though USB and PCI versions are also very common. Most wireless NICs are made in the PCMCIA form factor probably because they target notebook computers more. Most of the NICs have some kind of connector to which an external antenna can be connected apart from the built-in antenna. Installing the drivers or a particular OS and then configuring network parameters such as channel SSID and other securing settings.

3.9.1.2: ACCESS POINTS

An access point is the core component of a traditional wireless LAN where it not only connects wireless clients to a wired network, but also controls access to and from both networks. An access point typically has two interfaces:

- A wireless interface which is either an onboard radio or embedded PCMCIA wireless NIC.
- A wired interface which is typically 10/100 Base T/TX Ethernet, but could be a dial-up or another wireless adapter.

The 802.11 standard does not explicitly define how clients seek and associate to access points, thus several vendors implemented it differently.

Most access points can be operated either as bridges or routers and different access point models differ on the basis of the following feature:

- Whether it is 'fat' or 'thin' or 'lite'
- NAT/DHCP/VPN etc capabilities
- Multiple radios (Thus more users can be supported or usage as repeaters)
- Radio output power
- External antenna connectors.

3.9.1.3: THE WIRELESS LAN SWITCH

These are devices which centralize control and management functions for the wireless network intelligence that was previously in the access points which now resides in the wireless switch with a corresponding improvement in flexibility and functionality. Some switches incorporate intrusion detection technology – combined with the fact that there are less attack points improves security.

3.9.1.4: AMPLIFIERS

The transmit power of most wireless NICs and access points ranges from about +15dBm (32mW) to +20dBm (100mW). Long range links (miles) require higher transmit power and for high gain outdoor antennas. Amplifiers compensate for coaxial cable losses allow for maximum / authorized transmit power and typically increase the radio receiver sensitivity by a few dB. For best performance, the amplifier should be located as close as possible to the antenna. Amplifiers used in wireless LAN applications must be bi-directional. It is normally in the receive mode and is amplifying all the incoming signals.

3.9.1.5: ANTENNA

Antenna enable us extend range of coverage. Some of the most important practical design characteristics of antenna are:

- POLARIZATION
- DIRECTIVITY
- FEQUENCY BANDWIDTH
- EFFECTIVE GAIN

3.9.1.6: DISTRIBUTION SYSTEM (DS)

The DS typically is the wired network that is used to connect a set of BSS cells. In effect, it is the backbone of the wireless LAN. Obviously, if all the required network services and application reside directly on accessible wireless systems as in the case of an IBSS network, there will be no need for a DS. A network distribution system is absolutely necessary if such things as database, application and print services reside on

servers located on the wired network which is the typical case in enterprise implementations.

3.9.2 CALCULATING THE NUMBER OF ACCESS POINTS REQUIRED

Once you know the expected total bandwidth (from analyzing application and user requirements), you need to define a minimum over-the-air rate at which the system should function. For high capacity deployments, a good rule of thumb is to set baseline association rates at 11Mbps for 802.11b and 36Mbps for 802.11a&g. Then compute the number of access points required for a given service area:

$$\text{Number of APs} = \frac{\text{Bandwidth x No. of users x \% Activity rate per user}}{\text{\% Efficiency x Baseline Association rate per AP.}}$$

Bandwidth = Total bandwidth for bidirectional data

Percentage efficiency = Overall overhead efficiency factor, including MAC inefficiency and error correction overhead.

3.9.3: COMPARING 802.11 PERFORMANCE IN DIFFERENT CONFIGURATIONS

TABLE 3.2: COMPARING 802.11 PERFORMANCES IN DIFFERENT CONFIGURATIONS.

WIRELESS ACCESS POINTS	WIRELESS CLIENTS	THROUGHPUT (Mbps)	REMARK
Linksys BEFW11S4	Linksys WPC 11	4.125	This is a pure 802.11b network since both access point and client use 802.11b
Linksys BEFW11S4	D-Link DWL – 650 + Airplus	4.266	A normal Linksys access point is being used with the D-Link Airplus 802.11b card. The throughput is comparable to the previous one
D-Link DI – 714P + Airplus	D-Link DWL – 650 + Airplus	5.695	The Linksys wireless access points is connected to the D-Link multimode access point which supports 802.11a and 802.11b. However the NIC is still 802.11b. The improved performance is due to Airplus features.
Linksys BEFW11S4 connects to Linksys WAP51AB	D-Link DWL – AB520 Airpro	8.88 – 23.12	Linksys wireless access point is connected to the Linksys WAPSIAB, which supports both 802.11a and 802.11b. On the client side, the D-Link PCI wireless point which also supports both 802.11a and b. throughput obtained ranges from 1.11Mbps to 2.80Mbps.

Linksys BEFW11S4 connects to Linksys WAP S1AB	Linksys WPC S1 AB	8.88 – 25.12	The Linksys wireless access point connects to the Linksys WAPS1AB which supports both 802.11a and 802.11b. Linksys NIC is used on client side, which supports only 802.11a. Throughput obtained ranges from 1.11Mbps to 2.88Mbps.

3.9.4: OPERATING SYSTEM SUPPORT FOR WIRELESS LANS

Microsoft windows in its various flavors rule the desktop world which represents the market and points. Linux is growing in popularity everyday although it is strong in the server mode. Lots of IT enthusiasts are taking a liking to it for desktop usage also. Also, out of strong convictions that Linux should be the desktop OS of choice for engineering students, I have picked these two operating system to investigate what features they contain that specifically addresses usage in wireless LANs.

3.9.4.1: MICROSOFT WINDOWS

While windows XP had built in support for auto-configuration and security of wireless LANs. The release of windows server 2005 family has brought several features and enhancements to the above experience in deploying wireless LAN. These enhancements include:

- Enhanced wireless security (IEEE 802.1x support):
- Wireless zero configurations:
- Wireless roaming support:
- Password based authentication for secure wireless connections

3.9.4.2: GNU – LINUX

Right out of the box, the Linux kernel 2.4.20 supports about 25 IEEE 802.11b devices for PCI, ISA and PCMCIA and about five enhanced 802.11b, 802.11a&g cards.

The wireless extension for Linux kernel is a wireless LAN API for Linux systems which has been available since the 2.0.30 release of the Linux kernel. Wireless extensions

enable the user to manipulate the parameters of all wireless devices in a standard and uniform way as well as provide statistics for a wireless connection.

3.10: SECURING THE WIRELESS NETWORK:

The security of this network is the most paramount aspect of this design. Therefore the security techniques I propose to completely eliminate hackers and other attackers from stealing very vital information of the network include:

- First we need to disable any feature on the access point that broadcasts the SSID of the access point to put off casual attackers.
- We also need to implement border lockdown. This allows only known packets gain access into the network. This can also be controlled by setting up Access Control Lists.
- WLAN access control. This selects which station can access the network. It does so primary by the means of MAC address filtering
- Data sent over the network should be strongly encrypted. This can be done by deploying WPA in which a re-authentication is required at time intervals.
- We can also secure this network by implementing Network Monitoring. This allows the network administrator to be able detect rogue access points and intruders. It also ensures that users do not break laid down network policies.
- We can also deploy wireless sniffers and scanners which can capture and analyze packets from other access points and clients within the network.

3.11: PUTTING THE NETWORK TOGETHER

Some strategic steps are to be followed in putting a wireless network together. For this design, the following steps are to be taken to put the network together:

* Mount the antennas and connect them to access points to cover relevant areas
* Configure settings on the access points or wireless switches: The relevance or number of settings will depend on whether fat or lite access points are being used. For fat access points; SSID and broadcast options, WEP or WPA settings, MAC address, IP address and other options must be set. Thin and lite access points will download a configuration from the central switch.
* Connect the access point to the LAN switch. If fat access points are being used, multiple MAC address must be enabled on the LAN switch so it doesn't see the seemingly suspicious activity of multiple devices at the same port. If wireless switches are used to perform the relevant configuration using the supplied configuration tools examples; Trapeze mobility system software (MSS) if a Trapeze mobility system is being implemented.

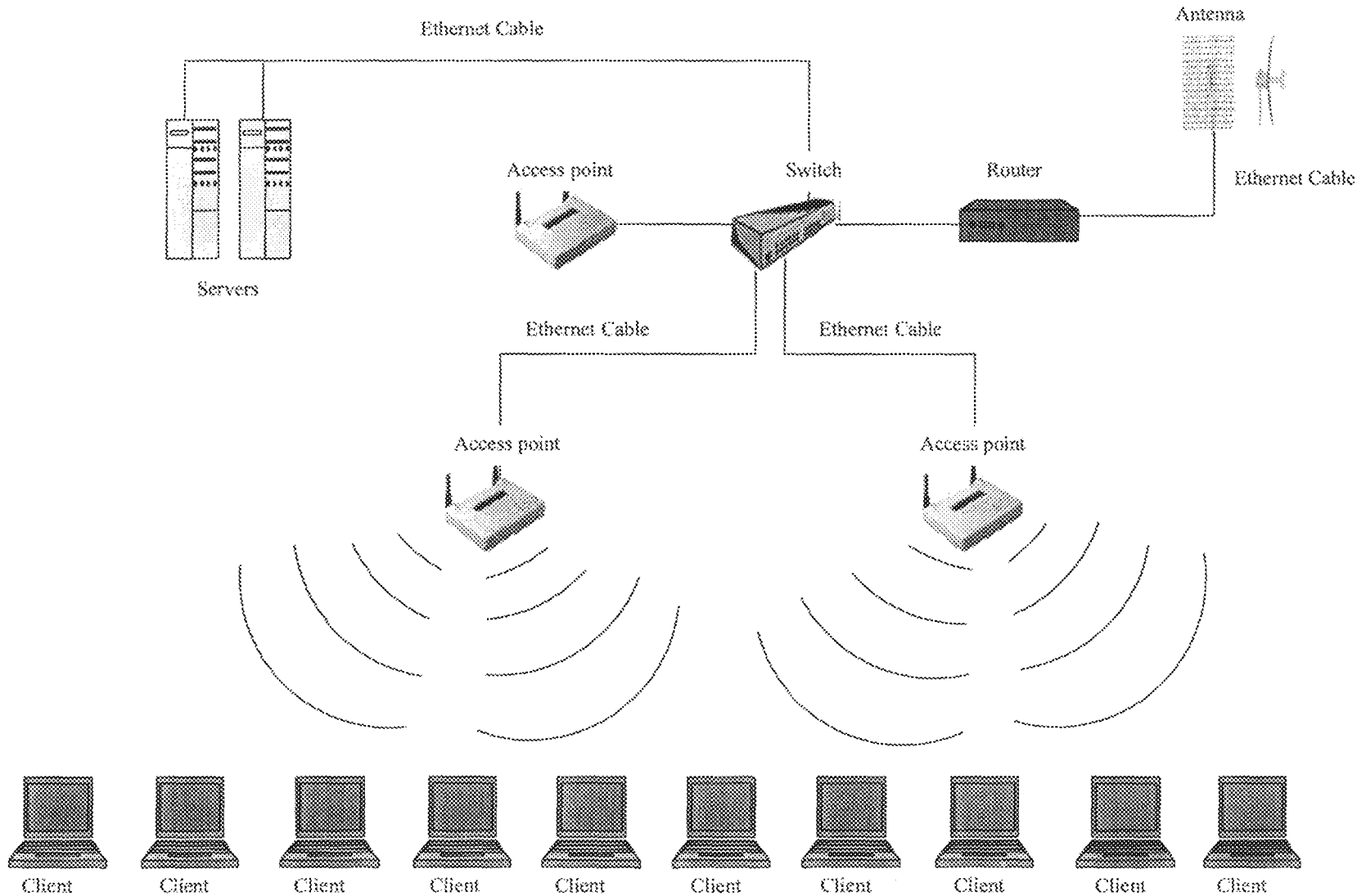
CHAPTER FOUR:

4.1: IMPLEMENTATION OF THE DESIGN:

The implementation of this design is simulated on AutoCAD as shown below:

For this design a total of three access points were used, with one of them configured as the root access point, which co-ordinates all the activities of the other access points and relates them to the server. The server and root access point are both stored in a private room in which case, for this design, they will be located in the HOD's office. The other two access point will be configured and located on the 1st floor of the complex strategically placed to ensure complete coverage of the entire complex.

The figure below shows a complete diagrammatic representation of the connection between the wired aspects of the network to the wireless aspect of the network:



FIGS 4.1 BLOCK DIAGRAM SHOWING THE CONNECTION BETWEEN THE WIRED TO THE WIRELESS ASPECT OF THE NETWORK

This next plate shows the access points location on the first floor of the complex:

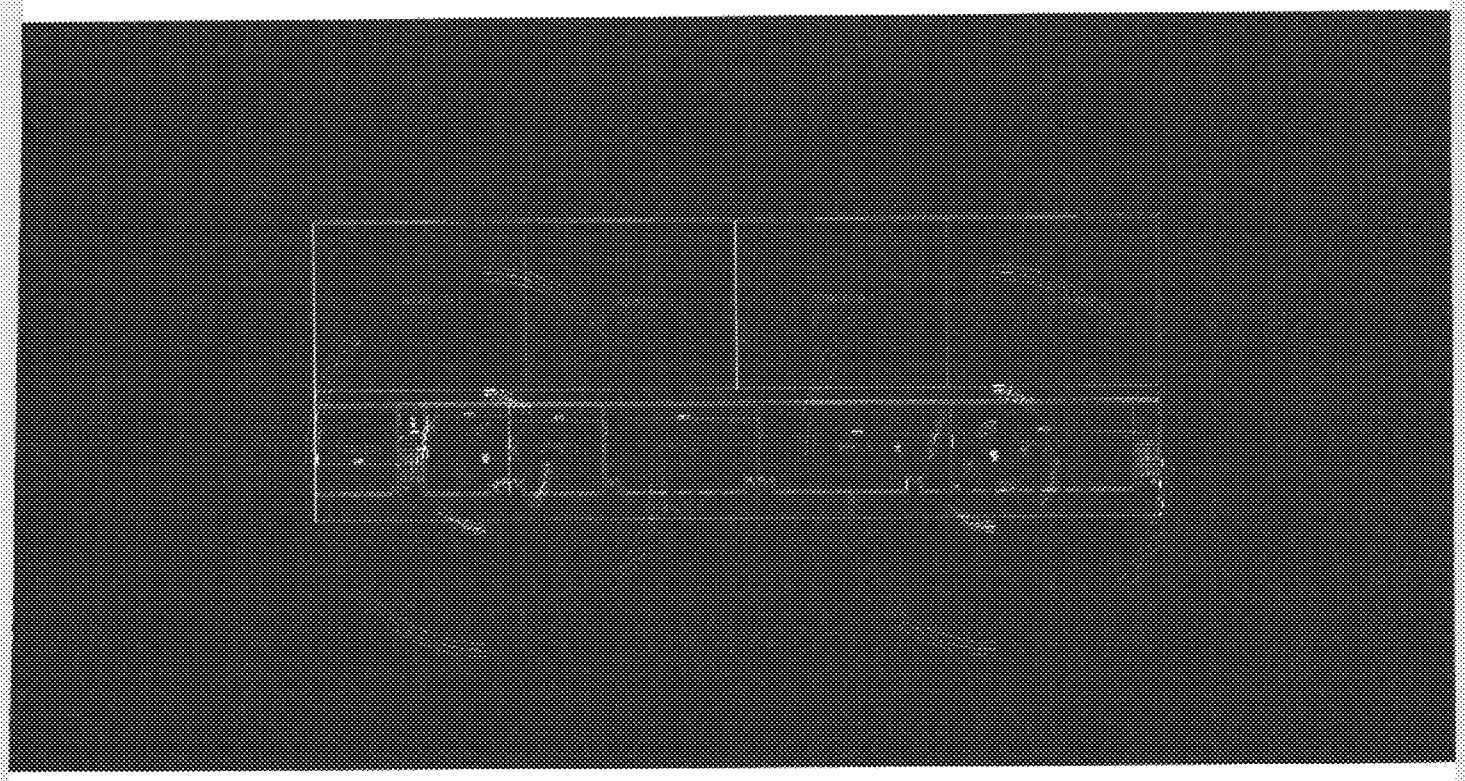
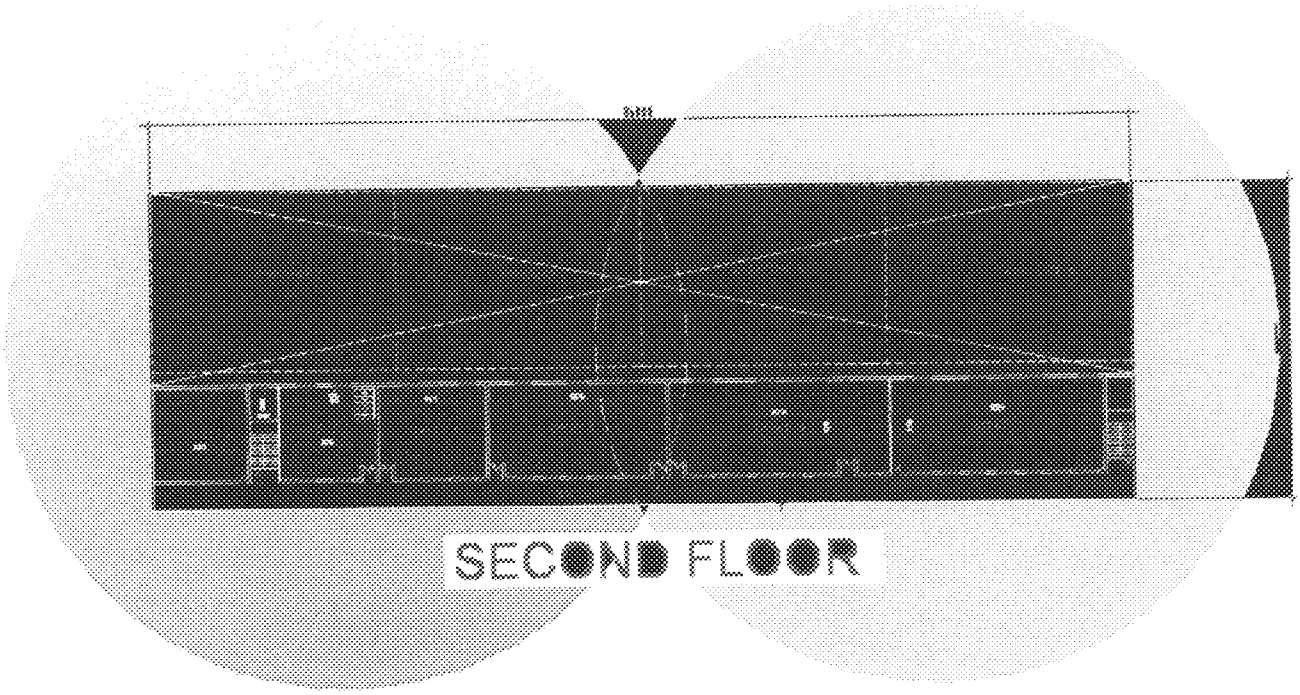
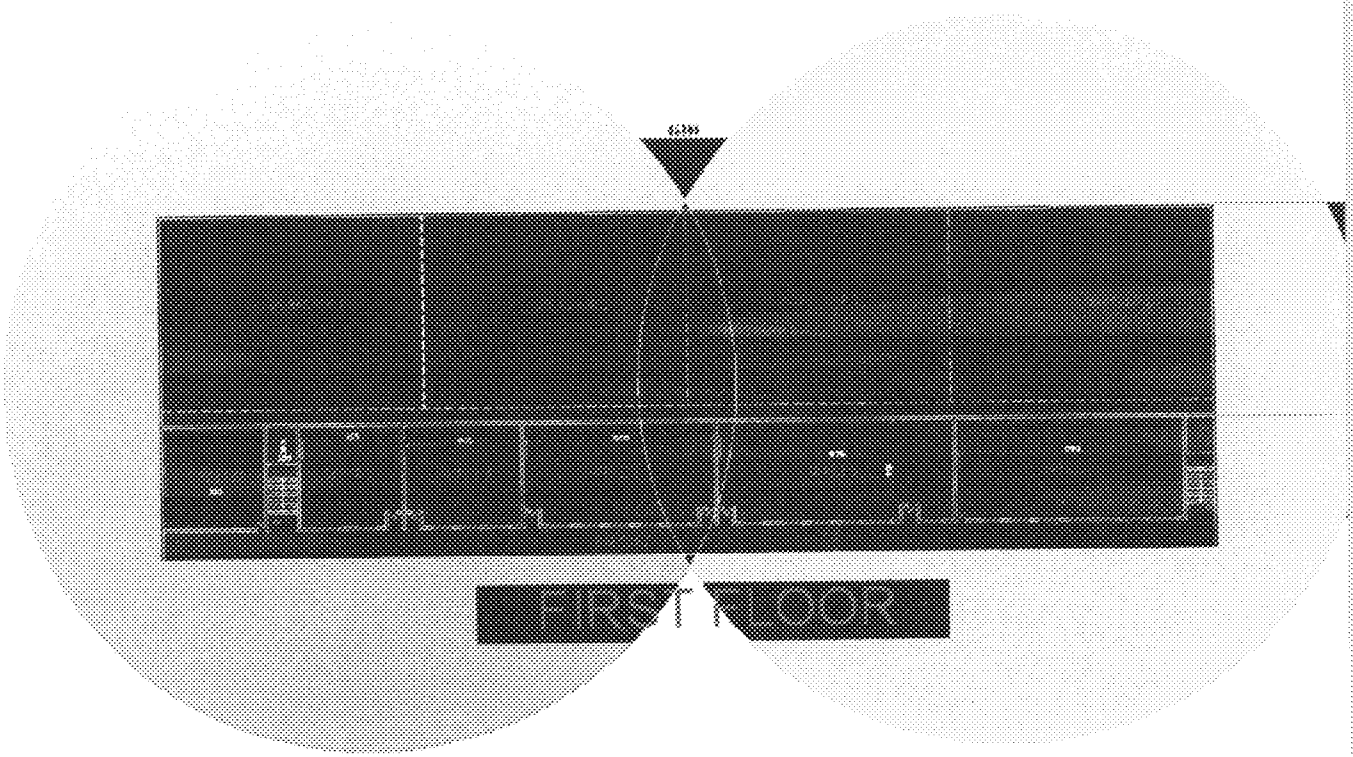
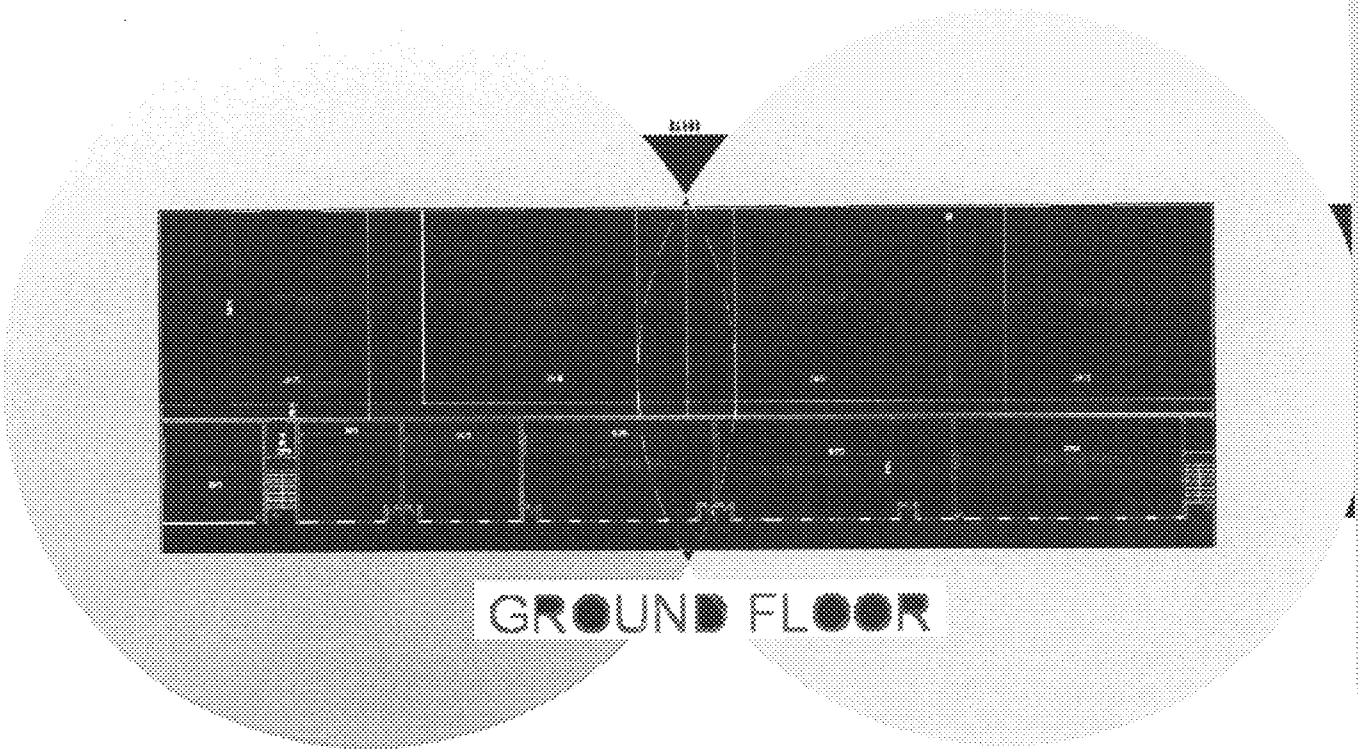


PLATE 1: ACCESS POINTS ON THE SECOND FLOOR WITH WAVES RADIATING OUT.

The following plates below show the coverage area of the access points on each floor of the complex configured in two different non over-lapping frequencies:


SECOND FLOOR


FIRST FLOOR



GROUND FLOOR

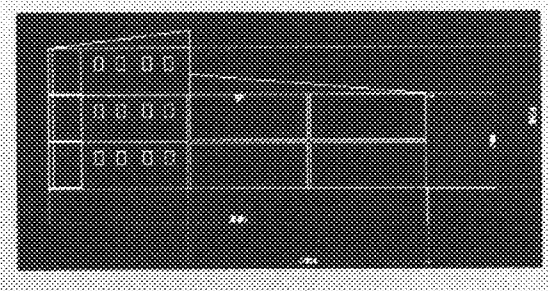
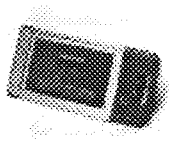
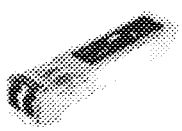


TABLE 4.1 ELECTRICAL BILL OF QUANTITY OF COMPONENTS FOR THE IMPLEMENTATION.

COMPONENT	COMPONENT NAME	PRICE	QUANTITY	COST
	Cisco Aironet 1131AG wireless access point	N75950	3	N227850
	3Com Unified Gigabit Wireless PoE Switch	N248000	1	N248000
	Cisco 802.11B PC CARD	N38750	40	N1550000
	Wireless Network Adapter N	N14880	40	N595200
	Linksys MFEFX1 - Transceiver module	N12245	1	N12245

The total approximate cost of implementing this design according to the market prices I got from the market survey I conducted is N2633295.00

CHAPTER FIVE:

5.1: CONCLUSION:

Wireless networking is without doubt one of the most important technologies of our time that promises to take pervasive computing to a whole new depth. As mobility is the primary attraction of today's global world, this is why I have decided to connect our department to the rest of the world wirelessly. As this will boast the amount of work done in the department as work will not only be carried out in the offices. This implementation will also provide an alternative to the already existing wired network in the department, thereby reducing over crowding of the network, which also leads to greater throughput of data.

However, today's wireless networks still face a lot of issues. Such issues include interference. Wi-Fi transmits at a frequency of 2.4GHz thereby making it susceptible to interference from Bluetooth enabled devices, mobile phones, microwave and other communication devices. Another issue is that Wi-Fi lack high quality media streaming abilities. High quality audio and video can not be viewed flawlessly because of low transfer rate. Another problem is that of security. A wireless network can be easily attacked by hackers to steal private information. Even guests who are not of any potential threat to the network, but utilizing network resources can minimize performance.

5.2: RECOMMENDATION FOR FURTHER WORK;

Wireless network is an ever evolving technology; new technologies are discovered everyday like the evolution of the new 802.11n standard, WiMAX, etc, therefore research on wireless standards will never end.

However, there is always room for improvement on the security. More work can be done to protect a network to put off attackers and ensure maximum protection of data transmitted wirelessly. Also, improvement on ways to reduce interference of a wireless signal is another important aspect to research on. A research on how to improve the quality of streaming audio and video data viewed over the wireless network can also be considered.

REFERENCES

Geiger J. ''Wireless Networking Handbook'' 1995 New Riders

Understanding Wireless LAN Protocols and Components'' by Dell Smith, 08-may-2002

Roger Chung, Infrared wireless protocols development with IBM microelectronics, Toronto

Wendell O. CCNA Exam 640-607 certification guide, Cisco press, ISBN 1-58720-055-4,2002

Geiger J. 802.1b Physical Layer Revealed, June 2003, http://www.802.11planet.com/tutorials/articles.php.21072681

Oullet E., Padjen R., and pfund A., ''Building Cisco Wireless Network'' Syngress, ISBN:1-928994-58-X, 2002, pp70

Wheat J., Hiser R., Tucker J., and Neely A., ''Designing a Wireless Network''. Syngress, ISBN: 1-928994-45-8, 2001, pp133

Cisco Inc, ''Cisco Mobile IP'' November 2003, http//www.cisco.com

Convery S Miller D., ''Cisco SAFE: Wireless LAN Security in Depth'', 2003, http://www.cisco.com

Randy R., ''ABC of Spread Spectrum'' October 2002, http://sss-mag.com/ss.html

CCNP BCMSN Student Guide Version 4.0(2007).pdf

Rune T., ''Wireless Local Area Networks''. March 1998, http://www.netplan.dk/netplan/wireless.html

Dr Mrs E. N. Onwuka, Dept of Elct /Comp Engineering FUT Minna, ''Lecture Material ECE 522''

www.wi-fiplanet.com/tutorials/article.php/2109571)

Sheldon T., Encyclopaedia of ''Telecommunication and Networking''. CD-ROM version

Jerry Char, CBT Nuggets ICND 1 & 2 Video series. Cisco Certification track preparatory video

CWNA - Certified Wireless Network Administrator - Official S.pdf

WiLAN corporation, "Wide band Orthogonal Frequency Division Multiplexing'' 2000, www.wilan.com

Flickenger R., ''Building Wireless Community Networks'', O'Reilly, ISBN: 0-596-00204-1, 2002, pp 65

Microsoft Corp., ''Wireless LAN and Windows XP'' 2002, http://www.microsoft.com

Trapeze Networks Inc., ''Capacity is Critical: Designing Enterprise WLANs for Capacity vs. Coverage''. http://www.trapezenetworks.com

Geiger J., ''Switches Improve Wireless LAN Performance'', July 2003, http://www.wi-fiplanet.com/tutorials/article.php/2231061

www.youtube.com ''ringmaster from trapeze networks /design software for wireless LAN''.

APPENDIX

SWITCH CONFIGURATION:

- From idle mode of the console, type enable
- Config t
- Write erase
- When ask to save, select 'N'
- Type reload
- Hit enter
- When ask do you want to enter initial config, select 'N'

This will erase the initial configuration of the switch.

TO SET SECURITY:

- Type in enable
- Config t
- Enable secret
- Type in your password
- Confirm by disabling then enable.
- Go to global config mode (config t)
- Type line vty 0 4
- Type login
- Type password
- Under global config mode
- Go to line config mode
- Line console 0, to set the console password
- Type in the password
- Exit

SETTING UP IP ADDRESS

- Enable
- Config t
- Type in 'int vlan 1'
- Type in the ip address
- Type 'no shut down'
- Exit

TO SET DEFAULT GATEWAY

- From global config mode
- Type in 'ip default gateway'
- Type in the default gateway address

TO SAVE THE CONFIGURATION

- Type in 'copy running config start up
- Hit enter
- Show run
- Highlight all the config
- 'alt c' to copy configuration
- Paste in another location for reference

ROUTER CONFIGURATION:

- Enable
- Config t
- Type erase to wipe out existing config
- Exit
- When asked to run initial config, select ''N''

TO SET PASSWORD

- Enable
- Config t
- Enable secret
- Type the password

TO SET VTY PASSWORD

- Enable
- Config t
- Line vty 0 4
- Login
- Password: enter paseword
- Exit

TO SET CONSOLE PORT

- Line con 0 from config mode
- Login
- Password: enter password
- Exit

TO ENCRPYT PASSWORD

- From global conf mode
- Service password encrypt
- Exit

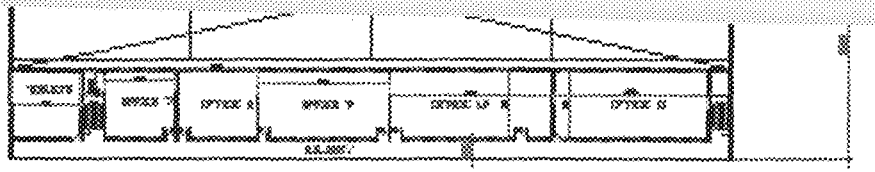
TO SET ROUTER NAME

- Enable
- Config t
- Hostname_ name
- Exit

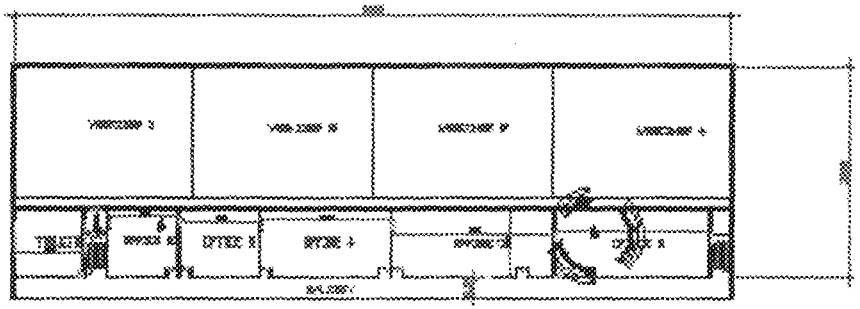
- No IP domain lookup
- No execute time out
- Exit

TO TURN ON RIP ON ROUTER

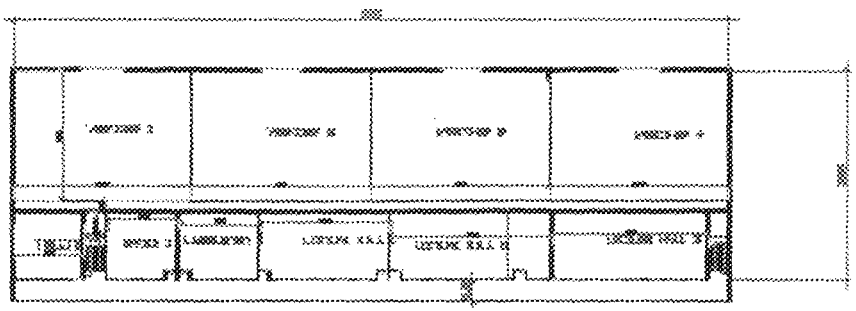
- Enable
- Config t
- Router rip
- Type in the version 1 or 2 (by default, it is 1)
- Network 192.102.1.0 (connected network)
- Exit



SECOND FLOOR



FIRST FLOOR



GROUND FLOOR