DESIGN OF AN INFRASTRUCTURE-BASED WIRELESS LOCAL AREA NETWORK (WLAN) IN THE DEPARTMENT OF ELECTRICAL/COMPUTER ENGINEERING, FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, NIGER STATE

BY

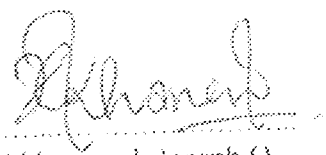
AKHANEMEH JOSEPH O.

(99/8072EE)

A THESIS SUBMITTED TO THE DEPARTMENT OF ELECTRICAL/COMPUTER ENGINEERING IN PARTIAL FULFILMENT OF THE AWARD OF BACHELORS OF ENGINEERING (B.ENG HONS) DEGREE IN THE DEPARTMENT OF ELECTRICAL/COMPUTER ENGINEERING, SCHOOL OF ENGINEERING AND ENGINEERING TECHNOLOGY, FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

ATTESTATION

I, AKHANEMEH JOSEPH O. (99/8072EE) hereby declare that this project titled, "Design of an Infrastructure-Based Wireless Local Area Network (WLAN) in the Department of Electrical/Computer Engineering, Federal University of Technology, Minna, Niger State" was carried out by me in the Department of Electrical/Computer Engineering under the supervision of Mr. J.G. Kolo. All information utilized and their sources have been duly acknowledged.



Akhanemeh Joseph O.

05/12/05

Date

CERTIFICATION

I hereby certify that this work has been read, supervised and meets part of the requirement for the Award of a Bachelors of Engineering (B.Eng) Degree in the Department of Electrical/Computer Engineering, Federal University of Technology, Minna, Niger State.

.....
Mr. J.G. Kolo
Project Supervisor

06-12-05
.....
Date

.....
Engr. M.D. Abdullahi
Head of Department

29/12/05
.....
Date

.....
External Examiner

.....
Date

DEDICATION

This work is dedicated to my parents, Mr. and Mrs. J.A Itsibor (KSM) and to my brothers and sisters.

ACKNOWLEDGEMENT

My foremost gratitude goes to God Almighty for His guidance and protection through all these years, especially during the course of my studies.

My special thanks goes to my parents, Mr. and Mrs. J.A. Itsibor (KSM) for their love and support. Also to my brothers and sisters I say a big "thank you" for their love and support.

Many thanks to my project supervisor, Mr. J.G. Kolo for his guidance and extensive briefing during the course of my project work.

I also want to use this opportunity to appreciate my friends and colleagues who have all contributed through sharing of their ideas with me to make this project work a success.

ABSTRACT

The implementation of the infrastructure-based Wireless Local Area Network (WLAN) is not a replacement for the already existing guided Local Area Network also known as the wired LAN, but to increase flexibility and ensure easy access (by authorized persons) to information from virtually every point spanned by the wireless radio signal.

Wireless LANs provide network access in places where installation of cables is difficult or impossible to implement.

Security is also a major concern, hence certain security measures are taken to ward off uninvited guests and hackers into the wireless network. Such measures include the use of MAC filtering, WEP and SSID.

In this project, the infrastructure-based Local Area Network was implemented using the IEEE 802.11b standard.

TABLE OF CONTENTS

CHAPTER ONE

.0 GENERAL INTRODUCTION

.1 INTRODUCTION

Resource sharing and data exchange is a key feature of any organization. Data in the past had been exchanged by the use of office messengers (within the office complex) or the post office (for places far from the organization). This method of data transfer was slow, unreliable and insecure. Data lost could not easily be retrieved and resending time was longer leading to loss of productive man hours.

The advent of computers and temporary storage devices such as floppy disks greatly improved the convenience of transferring information and reduced the time lost in resending missing information. Although the method of data transfer still remained by hand, 'sneakernet'.

As early as the 1950s, researchers worked on ways in which data could be exchanged between two or more computers. This is known as a computer network.

A network consists of two or more computers that can communicate and share resources with each other. Resources may include printers and modems.

Networks could be 'peer-to-peer', consisting of a few computers or 'server-client' connected via point-to-point links. These lines include a variety of fiber coaxial cables, twisted pair cables and wireless connections.

1.2 TYPES OF NETWORKS

Networks are basically classified on the basis of their geographical scope. These networks interconnect a number of devices and provide a means for transmitting data from one attached device to another within the specified geographical location.

1.2.1 LOCAL AREA NETWORKS (LAN)

These are small in scale and size. A LAN can consist of all the computers in a single room, floors or a building, the main identifying feature of a LAN is that no long distance or Wide Area Network technology must be used to facilitate communication.

1.2.2 WIDE AREA NETWORKS

These are large scale networks that at the very least span more than one building and can span a city, state, country or ocean. WANs use long distance connectivity techniques to link physically distant networks. If a telephone line is used to transmit data between two locations, it encompasses a WAN.

To increase flexibility, physical cabling is often replaced or combined with wireless components when deploying a network. This is particularly of tremendous advantage where physical cabling is rather too expensive or very inconvenient to install. The inclusion of wireless components to a cabled LAN is known as a Wireless Local Area Network (Infrastructure Based WLAN).

1.3 WIRELESS LOCAL AREA NETWORKS (WLAN)

A Wireless Area Network (WLAN or WiFi) is a data transmission system designed to provide location independent access between computing devices by using radio waves rather than a cable infrastructure.

In the corporate enterprise, wireless LANs are usually implemented as the final link between the existing wired network and a group of client computers and services of the corporate network across a building or campus setting.

The widespread acceptance of WLANs depends on industry standardization to ensure product compatibility and reliability among the various manufacturers.

The major motivation and benefit from wireless LANS is increased mobility, unfettered from conventional network connections, networks users can move about almost without restrictions and access LANS from nearly everywhere. The other advantages of WLANs include cost-effective network setup for hard –to-wire location such as older buildings and solid wall structures and reduced cost of ownership- particularly in dynamic environments requiring frequent modifications. WLANS liberate users from dependence on hard-wired access to the network access. This freedom to roam offers numerous user benefits on a variety of work environments such as:

i. Immediate bedside access to patient information for doctors and hospital staff.
ii. Real-time access to study group meetings and research links for students.
iii. Easy, real-time network access for consultants or auditors.
iv. Simplified network configuration with minimal (MIS) involvement for temporary setups such as trade shows or conference rooms.
v. Improved database access for roving supervisors such as production line managers, warehouse auditors or construction engineers.
vi. Faster access to customers' information for service vendors and retailers, resulting in better improved customer satisfaction.
vii. Location independent access for network administrators, for easier on-site trouble shooting and support.

1.4 PURPOSE OF STUDY

The objective of this project is to present Wireless Local Area Network (WLAN) as an enhancement to the guided or Wired LANs rather than as a total alternative.

It also seeks to show the flexibility of the WLAN and its importance to an academic community.

This study also addresses issues such as security management in a Wireless Local Area Network.

1.5 SCOPE OF STUDY

The scope of this project is limited to the implementation of the Wireless Local Area Network in the department of Electrical/Computer Engineering, Federal University of Technology, Minna, Niger State.

of years later, CODEX, Motorola attempted to implement a WLAN at 1.73GHz, that particular project was also abandoned after negotiations with the FCC failed.

Although all pioneering WLAN projects were abandoned, WLANs continued to attract attention and negotiations continued with the FCC to secure frequency bands for this purpose. These projects revealed several important challenges facing the WLAN industry, some of which remain till today.

2.2 NETWORK ARCHITECTURES

Network architectures provide different ways to solve a common problem – moving data quickly and efficiently in the network medium. The particular network architecture used defines the topology and access modes of the nodes on the network.

2.2.1 ETHERNET (IEEE 802.3)

Ethernet is the most commonly deployed network architecture in the world. Ethernet provides access to the network using CSMA/CD (Carrier Sense Multiple Access With Collision Detection). This strategy means that the nodes on the network listen to (sense) the network and wait until the line is clear. The computer then sends its packets out into the line. If there is more than one computer transmitting, collisions result. On sensing the collisions, the computer stops transmitting and waits until the line is free. One of the computers will then transmit, gaining control of the line and completing the transmission of packets.

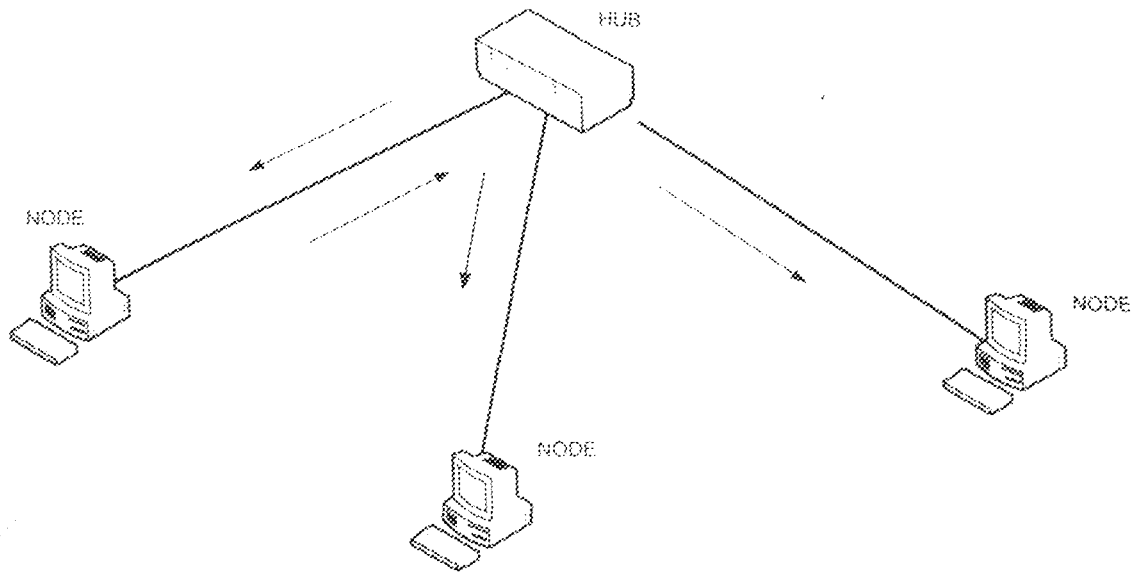


Fig 1: Operation of a Star-Wired CSMA/CD

Table 1: Ethernet Implementations

Ethernet Designation	Cable type	Maximum cable length	Connector Types
10BaseT	Cat. 5 UTP	100 meters	Hub
10Base2	Thinnet	185 meters	T-Connectors, Barrel connectors, Terminators
10Base5	Thicknet	500 meters	Vampire taps, transceivers, drop cables, terminators
10BaseFL	Fibre-Optic	2000 meters	Repeaters, terminators

The various Ethernet frame types are as follows:

- Ethernet 802.3 – Although this frame has the appropriate IEEE number, it is actually not completely in compliance with the specifications for Ethernet. This frame type is used by Novell Netware 2.2 and 3.1 networks.

- Ethernet 802.2 – This is the frame type that is in full compliance with the IEEE specifications. It is used by later versions of Novell Netware, including Netware 3.12, 4.x and 5.x.
- Ethernet SNAP – This Ethernet frame type is used in AppleTalk networks.
- Ethernet II – Networks running multiple protocols such as the internet generate Ethernet II frames.

A major disadvantage of the Ethernet is the number of collisions of the network.

2.2.2 IBM TOKEN RING (IEEE 802.5)

IBM Token Ring is characterized as a fast and reliable network that uses token passing as its media access strategy. Token Ring networks are wired in a star configuration with a Multistation Access Unit (MAU) providing the central connection for the nodes. The actual ring on which the token is circulated (the token moves in one direction as characterized by the ring topology) is a logical ring inside the MAU.

The token is passed around the ring until a computer wanting to send information out into the network takes possession of the token. A computer that passes the token to the next computer on the logical ring is called the Nearest Active Upstream Neighbor (NAUN). The computer to which the token is passed is the Nearest Active Downstream Neighbor (NADN).

After a computer takes possession of the token and transmits data, it then passes a new token to its NADN and the token makes its way around the ring until a node on the network takes possession to transmit.

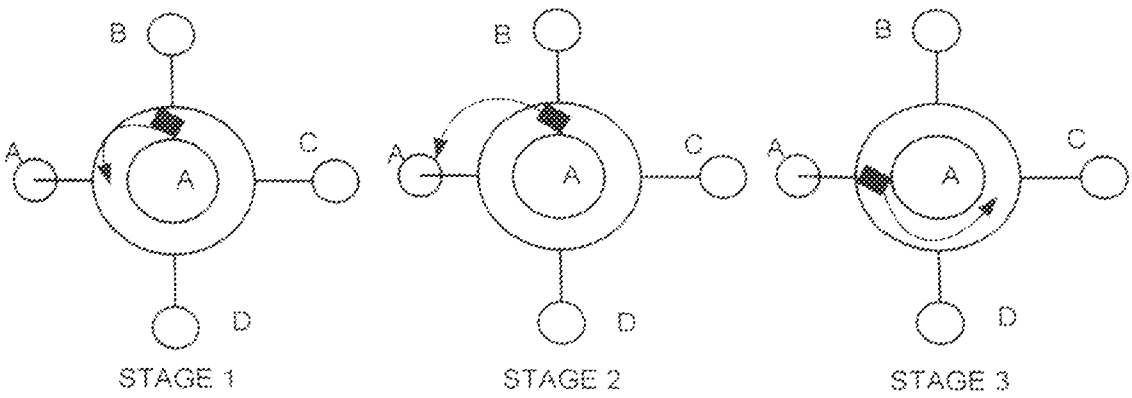


Fig 2: Token-Ring Operation

2.2.3 FIBRE DISTRIBUTED DATA INTERFACE (FDDI)

The FDDI is an architecture that provides high-speed network backbones that can be used to connect a number of different network types. FDDI uses fiber-optic cable and a wired-in-a-ring topology. FDDI uses token passing as its media access method and can operate at high speeds (Most implementations operate at 100Mbps but faster data transfer rates are possible).

Because FDDI uses a token passing media access strategy, it is reliable and provides equal access to all the nodes on the network. With FDDI, priority levels can be set. However, servers on the network could be allowed to send more data frames onto the network than client computers.

Because FDDI uses a true ring topology, breaks in the cable system can be a problem. To build fault tolerance into the FDDI network, a secondary ring is used. When a computer cannot communicate with its downstream neighbor, it sends data to the second ring (which circulates the data in the opposite direction from the one the primary ring uses).

2.2.4 APPLETALK

AppleTalk is the networking architecture used by Apple Macintosh computers. The networking hardware required is already built into each Macintosh or gotten from a Mac Ethernet NIC (Network Interface Card). The cabling system used to connect Macintosh computers is called Local Talk and uses shielded twisted-pair cables with a special Macintosh adapter.

AppleTalk uses a special dynamic addressing system to determine the address of the nodes on the network. When a Macintosh is powered up on the network, the computer generates a random address and broadcasts it out onto the network. This random address becomes its network address.

AppleTalk is similar to Ethernet in that it is passive network architecture. AppleTalk uses Carrier Sense Multiple Access with Collision Avoidance CSMA/CA. Basically the computers sit on the network and listen to determine that the wire is clear. After making sure the network is clear, the computer will send a packet onto the network letting all the other computers know that it intends to transmit data. The computer then sends out its data.

The fact that a computer that intends to send data onto the network notifies the other network nodes as its intentions greatly reduces the number of collisions on a CSMA/CA network.

However, these announcement packets do have a tendency to slow down the network and Macintosh networks only have a transmission speed of 230.4kbps.

2.2.5 IEEE 802.11

The IEEE 802.11 is the first WLAN standard and so far, the only one that has secured a market. The IEEE 802.11 standardization activity originally started in 1987 as part of the IEEE 802.4 token bus standard under the group number IEEE 802.4L. in 1990, the 80.4L was renamed as 802.11, an independent 802 standard, to define the Physical and MAC layers for WLANs. The first IEEE 802.11 standard for 1 and 2 Mbps, completed in 1997, supported DSSS, FHSS and diffused infrared (DFIr).

2.2.6 BLUETOOTH

Bluetooth is an open specification for short range wireless voice and data communications that was originally developed for cable replacement in Personal Area Networking (PANs) to operate all over the world. Its specification is the IEEE 802.15 WPAN (Wireless Personal Area Network) standard for 1 Mbps networks.

The topology of Bluetooth is referred to as scattered ad hoc topology. The network should be self-configurable, providing an easy mechanism to form a new small network and a procedure for participation in an existing one.

2.2.7 INFRA RED WIRELESS NETWORK

The infrared Physical Layer IEEE 802.11IR defines 1Mbps and 2Mbps operations by bouncing light off ceilings and walls to provide connectivity within a room or small office. Infrared systems use frequencies in the Terahertz range. This places infrared signals in the light region, invisible to the human eye and beyond the control of the FCC. Because of the extremely high frequency, infrared light is highly reflective, which makes it behave like an incandescent light bulb. Each client station is equipped with an infrared

transducer that can both transmit and receive light signals. The transducer diffuses the light, which makes the signal available from anywhere within a typical room.

Infrared light have the advantage of higher security, less radio interference but with the disadvantage of limited range, inability to penetrate obstacles and incompatibility of access points and transducers.

2.3 THE OSI LAYERS (OPEN SYSTEM INTERCONNECT)

The layers of the OSI model explain the process of moving data on a network. The OSI model provides the mechanisms and rules that make the handling of data possible. The chart below shows the OSI layers.

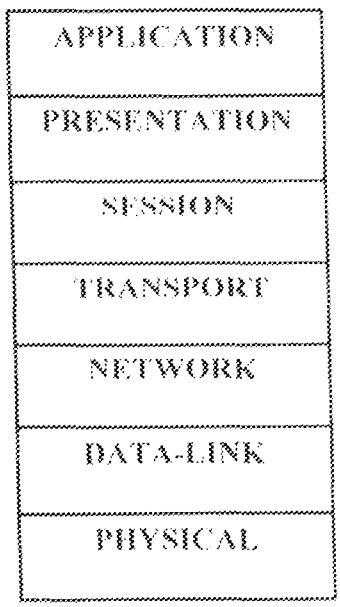


Fig. 3: OSI Model showing the OSI layers

2.3.1 APPLICATION LAYER

The Application Layer provides the interface and services that support user applications. It is also responsible for general access to the network.

2.3.2 PRESENTATION LAYER

The Presentation Layer can be considered the translator of the OSI model. This layer takes the packets from the application layer and converts it into a generic format that can be read by all computers.

2.3.3 THE SESSION LAYER

The Session Layer is responsible for setting-up the communication link or session between the sending and receiving computers. This layer also manages the session that is set up between theses nodes. It also places check points in the data stream.

2.3.4 TRANSPORT LAYER

The Transport Layer is responsible for the flow control of data between communicating nodes. Data must not only be delivered error-free but also in the proper sequence. The transport layer is also responsible for sizing the packets so that they are in a size required by the lower layers of the protocol stack. This packet size is dictated by network architecture.

2.3.5 NETWORK LAYER

The Network Layer addresses packets for delivery and is also responsible for their delivery. Route determination takes place at this layer, as does the actual switching of packets onto that route. Layer 3 is where logical addresses (such as IP addresses) are translated to physical addresses (hardware address of the NIC).

Routers operate at the network layer and use Layer 3 routing protocols to determine the path for data packets.

2.3.6 DATA – LINK LAYER

The Data-link layer is responsible for data movement across the actual physical link to the receiving node and so uniquely identifies each computer on the network based on its hardware address that is encoded into the Network Interface card (NIC).

2.3.6 THE PHYSICAL LAYER

At the Physical Layer, the frames passed down from the data-link layer are converted into a single bit stream that can be sent out onto the network media. The Physical Layer also defines the actual physical aspects of how the cabling is hooked to the computer's NIC. On a computer receiving data, the Physical Layer receives the bit stream.

2.4 WIRELESS STANDARDS

The most critical issue affecting WLAN demand has been limited throughput. The data rates supported by the original 802.11 standards are too slow to support most general business requirements and slowed the adoption of WLANs.

Recognizing the critical need to support higher data transmission rates, the IEEE ratified the 802.11b standard (also known as 802.11 high rate) for transmission of up to 11Mbps. After 802.11b, two standards 802.11a in January 2002 and 802.11g in 2003.

2.4.1 IEEE 802.11b

With 802.11b WLANs, mobile users can get Ethernet levels of performance, throughput and availability. The basic architecture, features, and services of 802.11b are defined by the original 802.11 standard. The 802.11b specification affects only the physical layer, adding higher data rates and more robust connectivity.

The key contribution of the 802.11b addition to the wireless standard was to standardize the Physical Layer support of two new speeds: 5.5Mbps and 11Mbps.

To accomplish this, Direct Sequence Spread spectrum(DSSS) had to be selected as the sole physical layer technique for the standard since, as frequency hopping cannot support the higher speeds without violating current FCC regulations, the implication is that 802.11b systems will interoperate with 1Mbps and 2Mbps 802.11 DSSS systems, but will not work with 1Mbps and 2Mbps 802.11 Frequency Hopping Spread Spectrum (FHSS) systems.

The original 802.11 DSSS standard specifies an 11-bit chipping called a Barker sequence to encode all data sent over the air. Each 11-chip sequence represents a single data bit (1 or 0), and is converted to a waveform, called a symbol, that can be sent over the air.

These symbols are transmitted at 1MSPS (1 million symbols per second) symbol rate using a technique called Binary Phase Shift Keying (BPSK). In the case of 2Mbps, a more sophisticated implementation called Quadrature Phase Shift Keying (QPSK) is

used. It doubles the data rates available in BPSK via improved efficiency in the use of the radio bandwidth. To increase the data rate in 802.11 b standard, advanced coding techniques are also employed.

For higher data rates, the 802.11b employs QPSK as the modulation technique and signals at 1.375MSPS. When devices move beyond the optimal range for 11Mbps operation, devices will transmit at lower speeds, falling back to 5.5, 2 and 1Mbps. Likewise, if the device moves back within the range of a higher speed transmission, the connection will automatically speed up again. Rate shifting is a physical layer mechanism transparent to the user and the upper layers of the protocol stack.

One of the most significant disadvantages of 802.11b is that the frequency band is crowded and subject to interference from other networking technologies, microwave ovens, 2.4GHz cordless phones and Bluetooth devices. There are drawbacks to 802.11b, including lack of interoperability with voice devices and no QoS (Quality of Service) provisions for multimedia content. Interference and other limitations aside, 802.11b is the clear leader in business and institutional wireless networking and is gaining a fair share of home applications as well.

2.4.2 IEEE 802.11a

802.11a is much faster than 802.11b, with a 54Mbps maximum data rate, operates in the 5GHz frequency range and allows eight simultaneous channels. 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM), a new encoding scheme that offers benefits over spread spectrum in channel availability and data rates

Channel availability is significant because the more independent channels are available, the more scalable the wireless network becomes. 802.11a uses OFDM to define a total of non-overlapping 20MHz channels across the two lower bands. By comparison, 802.11b uses 3 non-overlapping channels.

All wireless LANs use unlicensed spectrum, therefore they are prone to interference and transmission errors. To reduce errors, both types of 802.11 automatically reduce the Physical Layer data rates. IEEE 802.11b has three lower data rates (5.5, 2, and 1Mbps.), and 802.11a has seven (48, 36, 24, 18, 12, 9, and 6 Mbps). 802.11a also uses a higher frequency band, 5GHz which is both wide and less crowded than the 2.4GHz band that 802.11b shares with cordless phones, microwave ovens and Bluetooth devices.

The wider band means that more radio channels can co-exist without interference. Each radio channel corresponds to a separate network, or a switched segment on the same network. One big disadvantage is that it is not directly compatible with 802.11b and requires new bridging products that can support both types of networks.

2.4.3 IEEE 802.11g

Though 5GHz has many advantages, it also has problems. The most important of these is compatibility. The different frequencies mean that 802.11a products are not interoperable with 802.11b base. To get around this, the IEEE developed 802.11g which should extend the speed and range so that it is fully compatible with the older systems.

The standard operates entirely in the 2.4GHz frequency but uses a minimum of two modes (both mandatory) with two optional modes. The mandatory modulation/access modes are the same CCK (Complementary Code Keying) mode used by 802.11b and the

OFDM (Orthogonal Frequency Division Multiplexing) mode used by 802.11a (but in this case, in the 2.4GHz frequency band). The mandatory CCK mode supports 11Mbps and the OFDM mode has a maximum of 54Mbps. There are also two modes that use different methods to attain a 22Mbps data rate:- PBCC – 22 (Packet Binary Convolution Coding, rated for 6 to 54Mbps) and CCK – OFDM mode (with a rated max of 33Mbps).

The obvious advantage of 802.11g is that it maintains compatibility with 802.11b and also offers faster data rates comparable with 802.11a. the number of channels available however, is not increased, since channels are a function of bandwidth, not radio signal modulation – and on that score, 802.11a wins with its eight channels, compared to the three channels available with either 802.11b or 802.11g. another disadvantage of 802.11g is that it works in the 2.4GHz band and so due to interference, will never be as fast as 802.11a.

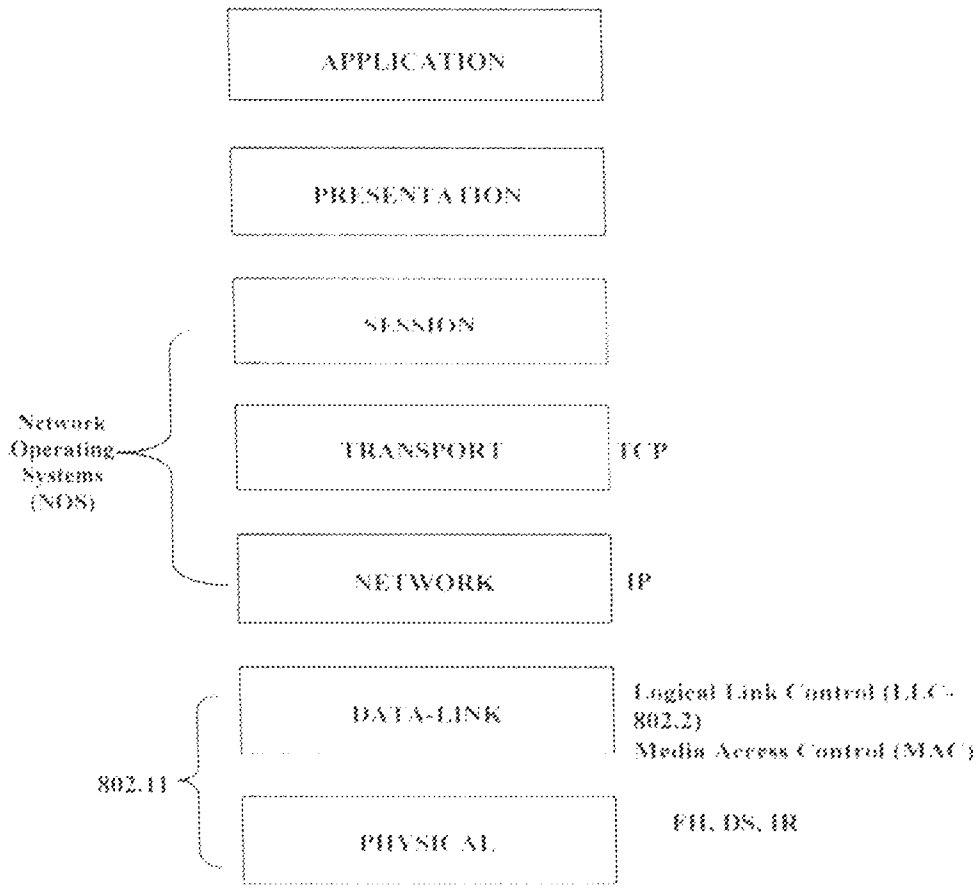


Fig.4: IEEE 802.11 and the OSI Model

2.5 ACCESS METHODS FOR WLANs

2.5.1 CSMA/CA

The protocol known as Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) is adopted by the IEEE 802.11 wireless LAN standard. The elements of CSMA/CA used in the IEEE 802.11 are Inter frame Spacing (IFS), contention window (CW), and a Back-off counter. The CW intervals are used for contention and transmission of the packet frames. The IFS is used as an interval between two CW intervals. The back-off counter is used to organize the back-off procedure for transmission of packets.

Consider three workstations: A, B and C. Station A has a frame in the air when Station B and sense the channel to find it busy. Each of the stations will run its random number generator to get a back-off counter by random. All two terminals persist on sensing the channel and deferring their transmission until the transmission of the frame from terminal A is completed. After completion, the two remaining terminals wait for the IFS period and start their counters immediately. As soon as the first terminal, station C for example finishes counting its waiting time, it starts transmission of its frame. The other two terminals freeze their counters and wait while sensing the channel. After C has completed its transmission, the other terminals wait for the IFS, resume counting and the first workstation to complete its count begins transmission.

Table 2: Brief History of Data –Oriented Networks.

DATE	EVENT
1979	Diffused Infrared. (IBM Rueschlikon Labs, Switzerland)
1980	Spread spectrum using SAW devices (HP Labs., California)
Early 1980s	Wireless Modem (Data Radio)
1983	ARDIS (Motorola/IBM)
1985	SM Bands for commercial spread spectrum applications
1986	Mobitex (Swedish Telcom and Ericsson)
1990	IEEE 802.11 for wireless standards
1990	Announcement of wireless LAN products
1991	RAM mobile (Mobitex)
1992	Formation of WINFORUM
1992	ETSI and HIPERLAN in Europe
1993	Release of 2.4, 5.2 and 17.1-17.3GHz bands in EU
1993	CDPD (IBM and 9 operating companies)
1994	PCS licensed and unlicensed bands for PCS
1996	Wireless ATM Forum started
1997	U-NII bands released, IEEE 802.11 completed, GPRS started
1998	IEEE 802.11b and Bluetooth announcement
1999	IEEE 802.11a/HIPERLAN-2 started

CHAPTER THREE

3.1 NETWORK PLANNING

In order to modify the traditional fixed network infrastructure to support wireless connections, a new wireless infrastructure is needed as an interface between the backbone wired network infrastructure and the mobile communication terminals. A good plan would ensure a smooth running wireless network. The major aspect of wireless network planning apart from the physical location of the node is the network topology.

The entire communication network consists of two types of elements: the communicating devices and the network infrastructure. The communicating devices provide an interface between the user application and the network infrastructure. Theses devices are usually referred to as communication systems, terminals or hosts. The network infrastructure is a collection of point-to-point wired or wireless lines and a number of switches or routers interconnecting several of these communication terminals in geographically separated locations. Traditional communication devices are connected to the communications network through a fixed connection point. The geographical location of the infrastructure remains fixed.

The mobile communication terminals need to be equipped with wireless front-ends to communicate with the wired backbone through the new wireless infrastructure. In addition to switches, routers and point-to-point links (air in this case), the wireless network infrastructure also needs wireless transceivers to communicate with the wireless communication terminals and act as a point of access to the fixed part of the wireless network infrastructure. Theses transducers are referred to as Access Points.

3.2 WIRELESS NETWORK TOPOLOGIES

Wireless network topology is a configuration in which a mobile terminal communicates with another. There are two fundamental topologies used in wireless networks. they are Infrastructure or Centralized topology or Ad hoc or Distributed topology.

3.2.1 INFRASTRUCTURE NETWORK TOPOLOGY

In Infrastructure topology, there is a fixed (wired) infrastructure that supports communication between mobile terminals and fixed terminals. The infrastructure networks are often designed for large coverage areas and multiple base stations or access point operations. The base stations or access points (AP) serve as the hub of the network and the mobile terminals are located at the end of the spokes. Any communication that is between peers has to be sent through the base station/access point. The hub station usually controls the mobile stations and monitors what each station is transmitting. Thus, the hub station is involved in managing user access to the network.

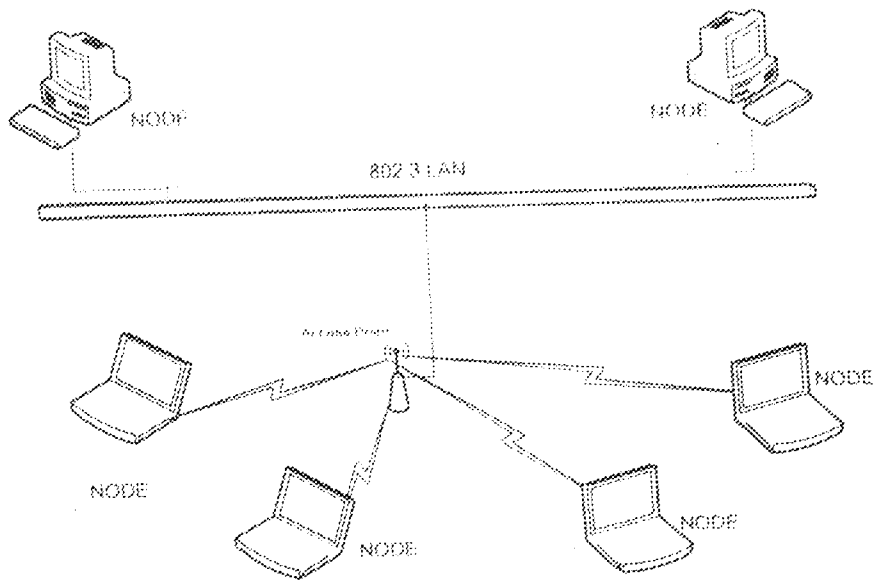


Fig. 6: AN INFRASTRUCTURE-BASED NETWORK

3.2.2 AD HOC NETWORK TOPOLOGY

Ad hoc or distributed network topology applies reconfigurable networks that can operate without the need for a fixed infrastructure. These networks are primarily used by the military and also in a few commercial applications for voice and data transmission. Such a topology is suitable for rapid deployment of a wireless network in a mobile or fixed environment.

There are two types of ad hoc topologies, namely:

i. Single-hop ad hoc network topology

ii. Multi-hop ad hoc network topology

In single-hop network topology, every user terminal has the functional capability of communicating directly with any of the other user terminals.

In multi-hop network topology, a given user may be able to reach only a portion of the other users in the network due to transmitted signal power limitations. In this situation, user terminals will have to co-operate in carrying messages across the network between widely separated stations.

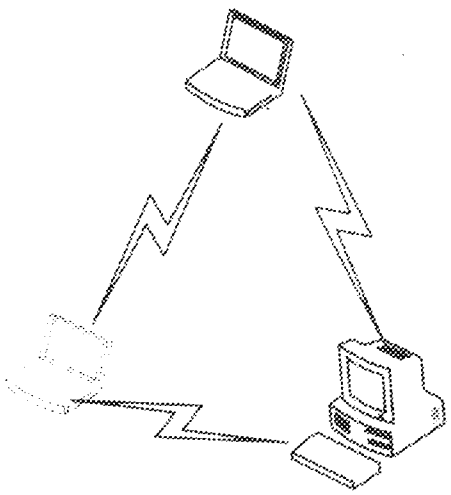


Fig. 7: AD HOC WIRELESS NETWORK

3.3 WI-FI ANTENNAS

To extend the range of the WLAN, an external antenna with good gain and directional or omni-directional capabilities is installed. These antennas include the following.

3.3.1 DIRECTIONAL ANTENNAS

Directional antennas are used for point-to-point or sometimes, for multi-point systems depending on the setup in moving from one location to another. These antennas include:

i. Yagi Antennas: These antennas are typically very directional and are used for point-to-point or to extend the range of a point-to-multipoint system. Radiolabs 14 or 16 elements weather proof antennas are used for outdoor installations. They have excellent signal strength and in the right circumstances can communicate for miles.

ii. Backfire Antennas: The backfire is a small directional antenna with excellent gain. They look similar to a parabolic dish, but the gain is not as high. They are used for point-to-point or point-to-multipoint systems because of the excellent gain and the good noise figures.

iii. Parabolic or Dish Antennas: Parabolic dish antennas put out tremendous gain but are a little hard to point and make a connection with. As the gain of an antenna increases, the antenna's radiation pattern decreases until a very little window to point or aim the dish correctly is left.

Dish antennas are used for a point –to-point system for long haul systems. The parabolic dish antennas work by focusing the power to a central point and beaming the radio's signal to a specific area. They are highly focused and are perfect tools for sending signals for very long distances.

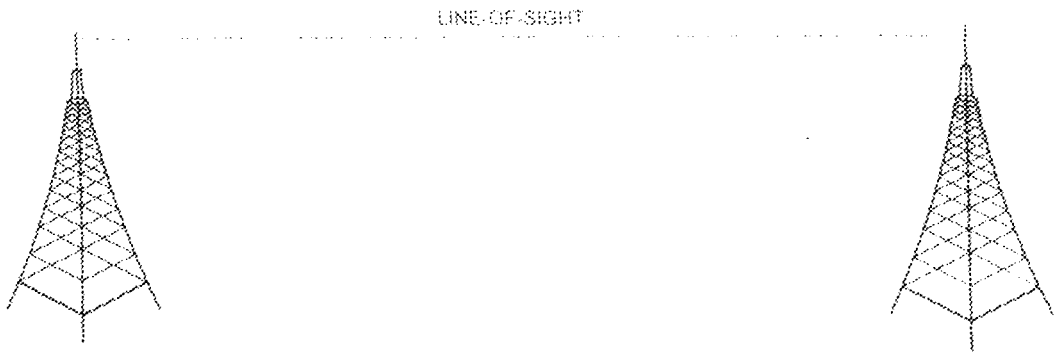


Fig. 8: POINT-TO-POINT WI-FI SYSTEM

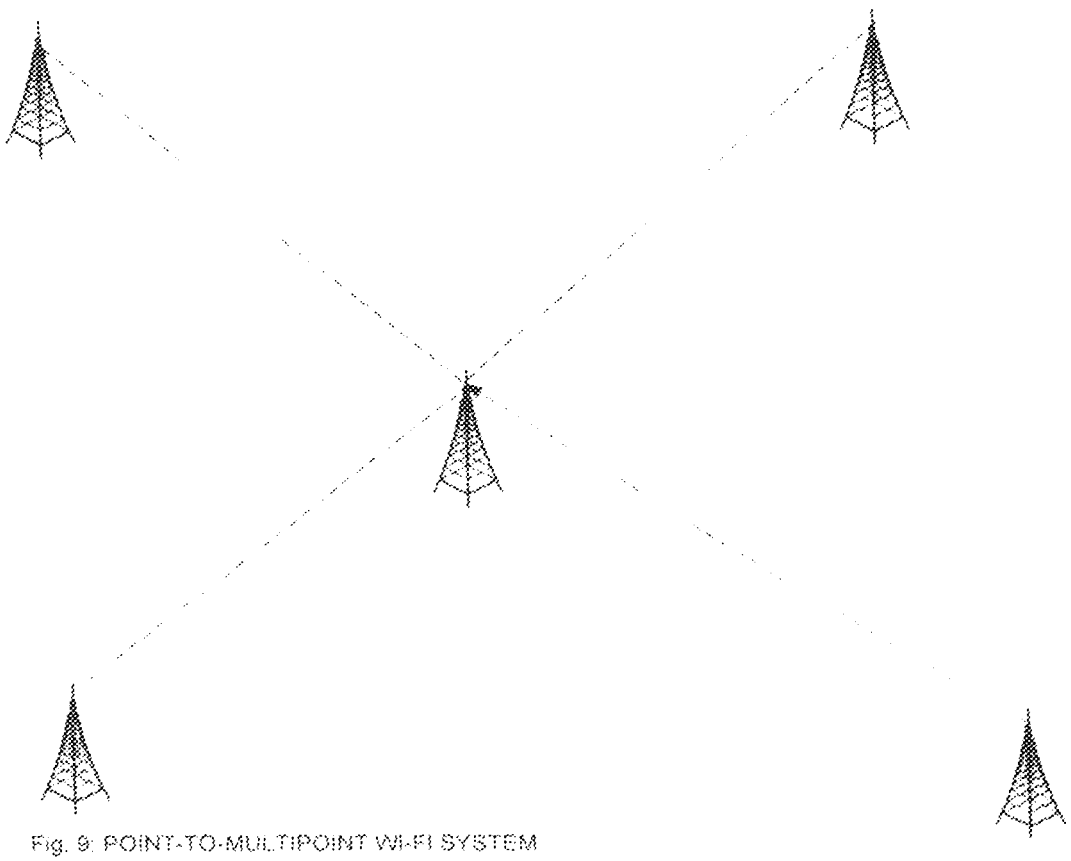


Fig. 9: POINT-TO-MULTIPOINT WI-FI SYSTEM

3.3.2 OMNI-DIRECTIONAL ANTENNAS

This is the common antenna used for point-to-multipoint systems. They distribute signals in all directions. These antennas include vertical omnis, ceiling domes, rubber ducks, small desktops, and mobile vertical antennas.

3.4 WIRELESS ROUTERS

A router is a general purpose device that can be used to connect dissimilar networks that operates at layer 3 of the OSI model. The router should be able to cope with a variety of differences among networks. A wireless router is one that accesses nodes in the network via an unguided channel.

3.5 WLAN SECURITY

The broadcast nature of wireless communication renders it very susceptible to malicious interception and wanton or unintentional interference. At least minimal security features are essential to prevent casual 'hacking' into wireless networks. Since the advent of analogue telephony, wireless service providers have suffered several billion dollars worth of losses due to fraud. A few WLAN security mechanisms are treated below

3.5.1 SERVICE SET IDENTIFIER

A service set identifier (SSID) is a code attached to all packets on a wireless network to identify each packet as part of that network. The code consists of a maximum of 32 alphanumeric characters. All wireless devices attempting to communicate with each other

must share the same SSID. Apart from identifying each packet, SSID also serves to uniquely identify a group of wireless network devices used in a given "service set".

There are two major variants of the SSID

i. Ad hoc wireless networks use the IBSS ID (Independent Basic Service Set Identifier)

ii. Infrastructure networks use the BSS ID or ESSID (Basic Service Set Identifier and Extended Service Set Identifier)

3.5.2 MAC FILTERING

MAC filtering is the process of configuring an access point with a list of MAC addresses that will either be allowed or not allowed to gain access to the rest of the network via the wireless access point. The most common configuration has a list of allowed addresses that are supposed to be on the wireless LAN.

To be associated with a WAP implies that a client is fully connected to the WAP and is now allowed to pass traffic through the A P. Therefore, the client has complete access to the rest of the network, both wireless and wired. MAC filters set to keep unauthorized clients from becoming associated with the WAP

3.5.3 WEP (WIRED EQUIVALENT PRIVACY)

This is a security protocol for wireless LANs defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicality of their structure, having some or all parts of the network inside a building

that can be protected from unauthorized access. WLANs which are over radio waves, do not have the same physical structure, and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one point to another.

3.6 PROTOCOL TYPES

In a network, a protocol defines how communication will occur between computers. Protocols can be divided into two (2) major groups, namely:

a) Connectionless protocols

b) Connection-oriented protocols

3.6.1 CONNECTIONLESS PROTOCOLS

Connectionless protocols send and receive data without checking for proper transmission sequence or errors. Therefore, this type of protocol is fast but unreliable. Also, it is possible for the data sent later to arrive before the one sent previously. That is why it is best suited for the LAN environment.

This protocol can be used in situations such as a single message with high probability, but no guarantee of arrival.

Examples of this protocol type are User Datagram Protocol (UDP/IP), Internet Packet Exchange (IPX), and Asynchronous Transfer Mode (ATM).

3.6.2 CONNECTION-ORIENTED PROTOCOLS

This is a protocol type that is best suited for WAN environments because it ensures that all transmitted data reaches its destination. This protocol ensures the reliable delivery of data because it controls the amount of data transmitted, detects transmission errors and manages requests for transmission.

Examples of connection-oriented protocols are File Transfer Protocols (FTP) and Transmission Control Protocol (TCP/IP).

There are basically six (6) protocol suites that are involved in the networking environment.

1. TCP/IP – Transmission Control Protocol/Internet Protocol
2. SLIP – Serial Line Internet Protocol
3. PPP – Point-to-point protocol
4. NETBEUI – NetBIOS Extended User Interface
5. IPX/SPX – Internet Packet Exchange/Sequence Packet Exchange
6. AppleTalk

RANGE OF 802.11b/g (2.4 GHz - 2.484 GHz)

Channel 1 – 2.412 GHz

Channel 2 – 2.417 GHz

Channel 3 – 2.422GHz

Channel 4 – 2.427GHz

Channel 5 – 2.432GHz

Channel 6 – 2.437GHz

Channel 7 – 2.442GHz

Channel 8 – 2.447GHz

Channel 9 – 2.452GHz

Channel 10 – 2.457GHz

Channel 11 – 2.462GHz

Each channel is 5MHz wide.

3.7 TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL

TCP/IP is an industrial standard suite of protocols designed for Wide Area Networks (WANs). TCP/IP is one of the most popular protocols in the Windows environment today because it offers a method of gaining access to the internet.

Aside this, one of the major advantages is that traffic congestion on the network could be minimized. This is possible because TCP/IP is routable and an acknowledgement is not required for every packet sent.

3.7.1 ADVANTAGES OF TCP/IP

Reliability is TCP/IP's strong suit. It is highly appropriate for mission-critical communication. But there are many other ways in which TCP/IP out does the competition and justifies the extra effort required to implement it.

i. Compatibility: TCP/IP could almost be considered the universal protocol. It is supported by most operating systems and platforms and highly diverse systems such as Macintosh workstations, UNIX servers and Windows computers to

communicate with one another. Connection to the Internet requires the TCP/IP protocol.

ii. Scalability: more than any set of protocols can scale from the smallest home network to the largest network of all – internet. Because of its unique addressing system scheme, TCP/IP is especially suitable for large internetworks (networks that are interconnected with other networks).

iii. Routability: Closely related to scalability is the protocol stack's capability of spanning subnets. Unlike unroutable protocols such as NETBEUI, its data packets can cross from one network, or subnet to another by traveling through devices called routers. Internet communication often involves journeying through many different networks before the data finally gets to its destination.

CHAPTER FOUR

4.0 IMPLEMENTING THE WIRELESS LOCAL AREA NETWORK

In deploying a WLAN, certain steps should be taken. These include the following:

4.1 SITE SURVEY

This is the first step taken when implementing a Wireless Local Area Network. To avoid undue interference, the site for the WLAN must be devoid of devices that may transmit radio "noise" such as microwave ovens and electric blenders.

Also obstacles can also inhibit Wireless communication. These include metal cabinets, refrigerators, large aquariums, washers, and metallic based UV tinted windows. Devices using or operating in the 2.4GHz band should have their channels changed, switched over to another frequency band or removed completely. It is also of great importance to scan for any wireless networks nearby that may conflict with the WLAN about to be deployed. If a wireless network operating on same frequency is found, it is advisable to move as far away from that channel as possible.

4.2 PLACEMENT OF THE WIRELESS ROUTER

After a thorough site survey, the router is placed in a centralized position, as close as possible to the center of the wireless devices.

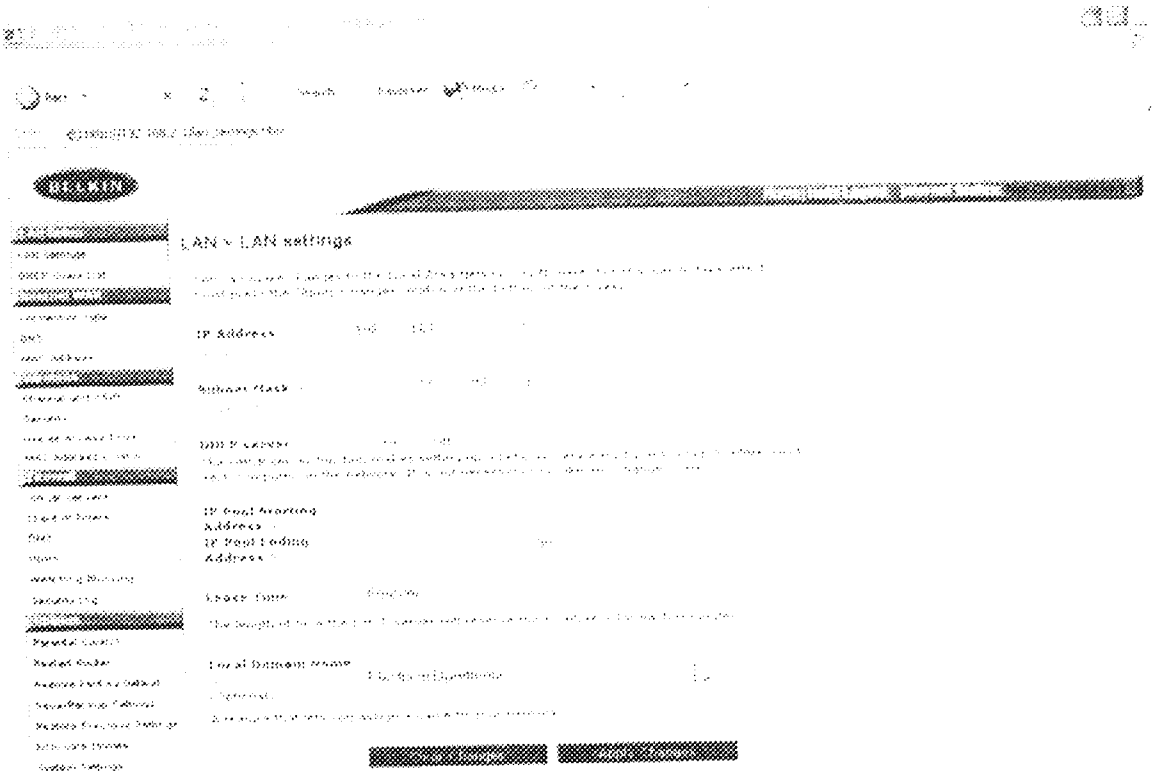
To achieve the best network coverage, the antennas are positioned vertically towards the ceiling. In multi-storey buildings, the wireless router is placed on a floor that is as close to the centre of the building as possible. This may mean placing the router (access point) on an upper floor. Cordless phones operating at 2.4GHz should be religiously avoided.

4.3 CONNECTING AND CONFIGURING THE WIRELESS ROUTER

The router is connected to the power supply and the network cable provided is connected to a port on the switch while the other end is connected to the router.

The router home setup is accessed via internet explorer and the following steps are taken.

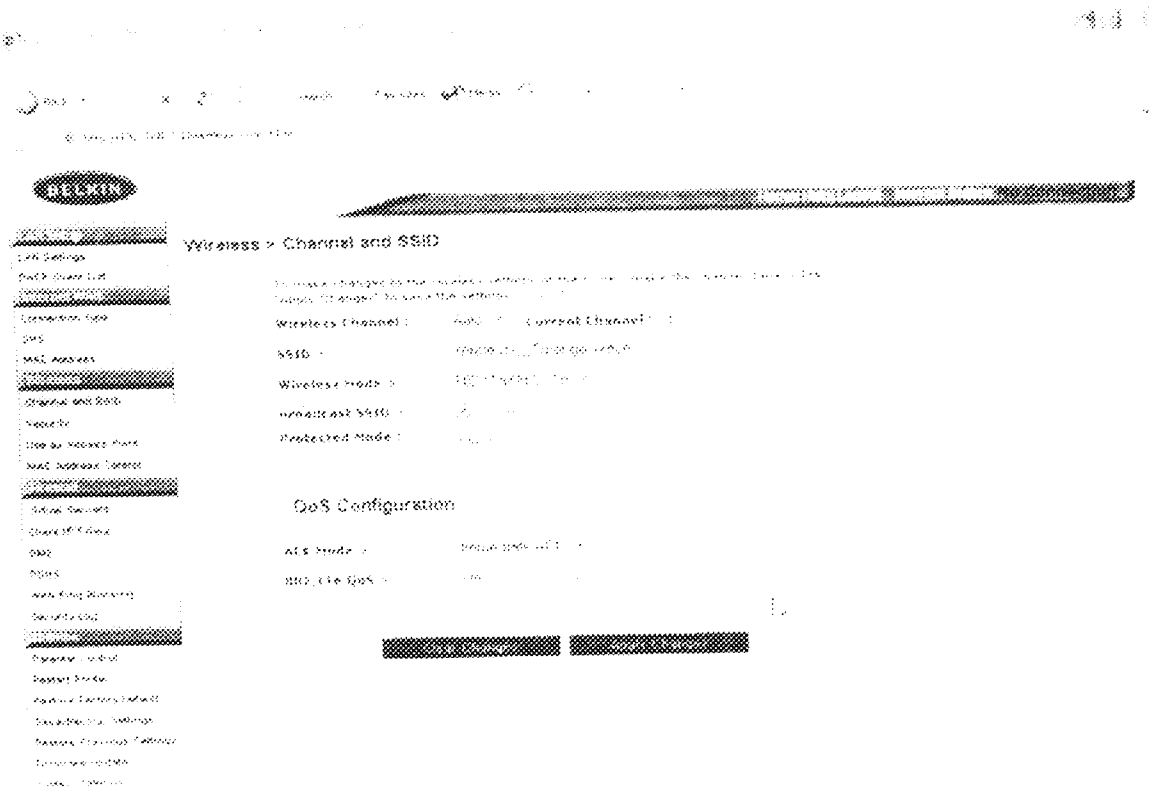
4.3.1 LAN SETINGS



The IP address provided is entered, subnet mask entered and Dynamic Host Configuration Protocol (DHCP) enabled

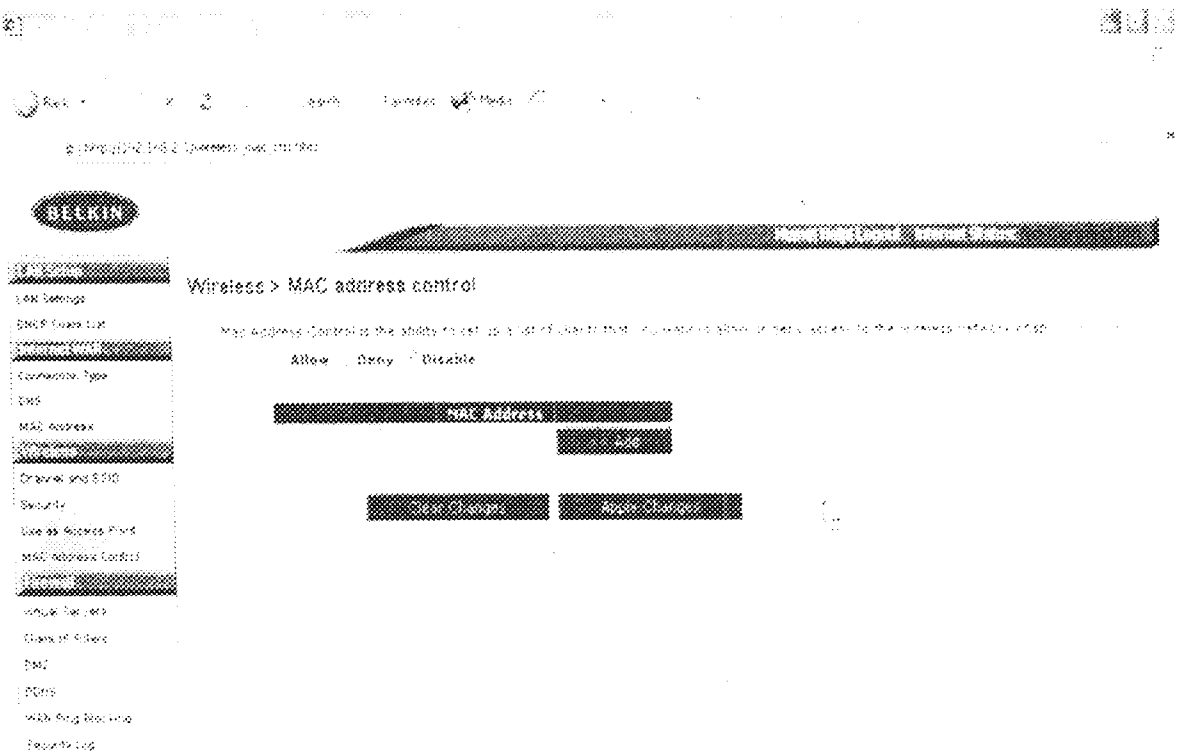
4.3.2 CHANNEL ASSIGNMENT

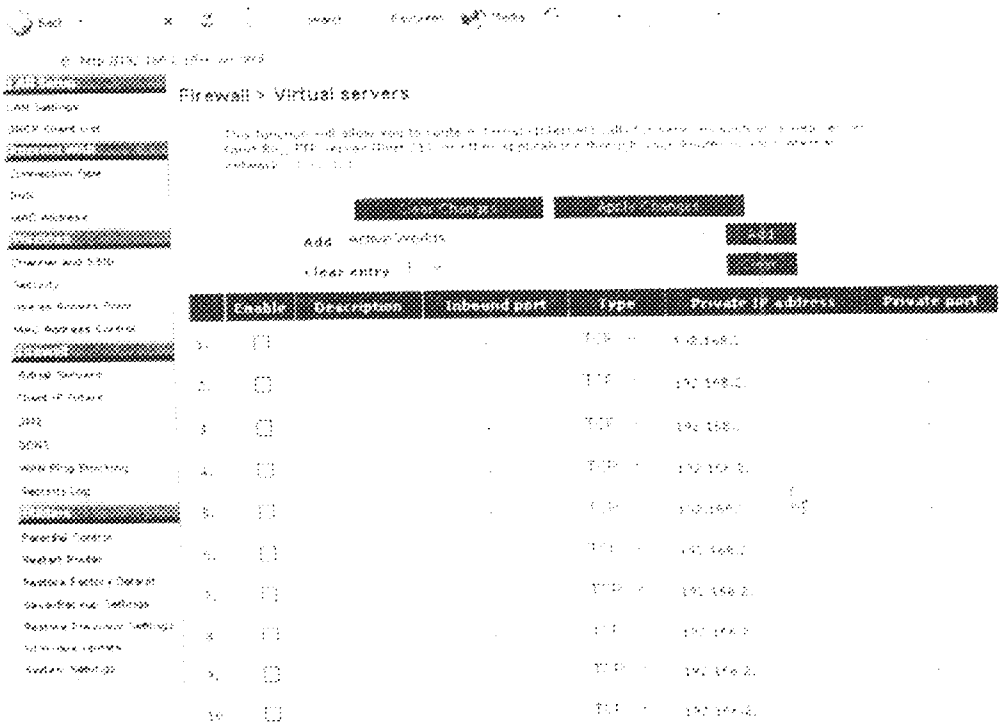
The channel to be used is assigned and Service Set Identifier (SSID) given.



4.3.3 SECURITY

Wired Equivalent Privacy (WEP) is enabled. MAC addresses allowed in the network are entered and the Firewall is setup to enhance network security.





Setting up the firewall

After these configurations are made, the network comes up and authorized wireless nodes are given access into the infrastructure based network.

CHAPTER FIVE

5.0 CONCLUSIONS AND RECOMMENDATIONS

5.1 CONCLUSIONS

From the foregoing, it is seen that a WLAN has a tremendous application to improving flexibility of a local area network in any organization.

In a university community, campus hotspots are a must-have due to the large flow of data exchange. Easy access to such information should be readily available from any point in the institution.

Due to the large population of the university community, deploying cables to provide network access to all and sundry would be rigid, inconvenient and overly expensive. Despite its flexibility, wireless area networks can also be made secure by the use of several security measures which include Wired Equivalent Privacy (WEP), Secure Set Identifier (SSID), and MAC filtering, or a combination of two or more of the above listed.

5.2 RECOMMENDATIONS

Given the benefits of a Wireless Local Area Network (WLAN), the following recommendations are being made:

- Provision of a wireless hotspot cloud over the entire University to enable easy access to information
- Provision of wireless accessories (Wireless routers, access points, wireless NICs) for computers in the various departments

REFERENCES

1. Kaveh Pahvalan and Prashant Krishnamurthy. Principle of Wireless Networks. Pearson Education Incorporated. 2002.pp 11-12.187-190.225-228.420-451.503-505.
2. William Stallings. Local and Metropolitan Area Networks. 5th Edition. Prentice Hall International Inc. 1997.pp 3-5.174-209.
3. N.I.I.T. A+ Hardware. Part-2. Students Guide. GeniPress. LLC. Coronado Phoenix. 2002.pp 393.403.
4. www.iec.org/online/tutorials/win/
5. www.webopedia.com/term/8/802_11.html
6. www.wikipedia.org/wiki/IEEE_802.11