

# **DESIGN AND IMPLEMENTATION OF A LOCAL AREA NETWORK**

(A CASE STUDY OF ELECTRICAL DEPARTMENT)

**BY**

**OLUSHOLA E. AKINTOLA**

99/8074EE

**DEPARTMENT OF ELECTRICAL AND  
COMPUTER ENGINEERING,  
SCHOOL OF ENGINEERING AND  
ENGINEERING TECHNOLOGY  
FEDERAL UNIVERSITY OF TECHNOLOGY,  
MINNA, NIGERIA.**

**NOVEMBER, 2005**

**DESIGN AND IMPLEMENTATION OF A  
LOCAL AREA NETWORK  
(A CASE STUDY OF ELECTRICAL DEPARTMENT)**

**BY**

**OLUSHOLA E. AKINTOLA**  
99/8074EE

**A PROJECT SUBMITTED TO THE DEPARTMENT  
OF ELECTRICAL AND COMPUTER  
ENGINEERING  
IN FULFILMENT OF THE REQUIREMENT FOR  
AWARD OF BACHELOR OF ENGINEERING  
(B.Eng) DEGREE IN ELECTRICAL AND  
COMPUTER ENGINEERING  
SCHOOL OF ENGINEERING AND ENGINEERING  
TECHNOLOGY,  
FEDERAL UNIVERSITY OF TECHNOLOGY,  
MINNA.**

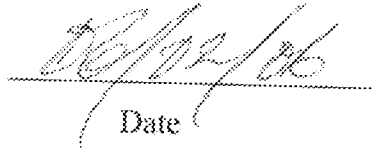
**NOVEMBER 2005.**

## ATTESTATION

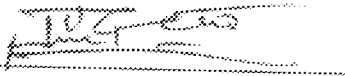
This is to certify that Olushola E. Akintola 99/8074EE carried out the project work presented in this report under my supervision.



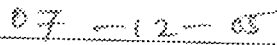
Engr. M.D. Abdullahi  
Head of Department



Date



Engr. J.G. Kolo  
Project Supervisor



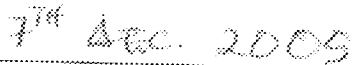
Date

External Examiner

Date



Olushola E. Akintola  
Student



Date

## ACKNOWLEDGEMENT

I really acknowledge the awesome power and favor of God Almighty upon my life throughout this project. He is the one that has predestined my life unto good works here on earth. The Lord whose name my faith is anchored as I move ahead in the fulfillment of His plan for my life.

I equally want to acknowledge and thank the members of staff of this great department for granting me opportunity to learn from their wealth of knowledge and experience. Especially my supervisor Engr.J.G.Kolo, Engr.M.D.Abdullahi, Engr.Abraham, Engr.Ajiboye Engr.David O. Omata, Engr.Salawu, Late Engr. T Asula, Engr.Shehu, Engr.Umar, Dr Onwuka, Associate professor Y.A Adediran, this acknowledgement will not be complete without acknowledging the following people: Prof. J.O Adeniyi, Prof. E.A. Salako, Dr. W.P. Akanmu and his wife, Mrs. T.Baba. My special thanks goes to Obakore for her loving and caring words during writing and typing this project, you have proved the stuff that you are made of to me, to all of you I say 'big thank you' and I LOVE YOU ALL.

## DEDICATION

I dedicate this project first of all to Lord God Almighty, whose mighty hand and strength saw me through this programme.

Also to my very mother who in her own little way frantically sought for me the wherewithal so that I can be educated, I will always pray and praise God for your life.

## ABSTRACT

This project is focused on the design and implementation of local area network together with site and cabling layout on which the computers are networked.

With the site and cabling layout, computers are physically and logically installed. The server being the brain of the network was configured logically to provide and share resources with the clients' computers, and they are also configured too in order to communicate with the server. Hardware and software that are compatible were installed for better performance

After all the computers have been networked, the computer that was made the proxy server was connected to the school of Engineering and Engineering Technology's radio room which made it possible for the department to be connected to the World Wide Web. The process of networking computers is very simple and interesting when the protocols are followed. So this project provides a simple and straight forward way of achieving this end.

# TABLE OF CONTENTS

COVER PAGE.....	i
TITLE PAGE.....	ii
ATTESTATION.....	iii
ACKNOWLEDGEMENT.....	iv
DEDICATION.....	v
ABSTRACT.....	vi
TABLE OF CONTENTS.....	vii
CHAPTER ONE.....	1
INTRODUCTION.....	1
CHAPTER TWO.....	6
LITERATURE REVIEW.....	6
THE WORLD OF COMPUTER NETWORKING.....	6
THE BASIC OF LOCAL AREA NETWORK.....	6
THE BASIC LAN BUS NETWORK.....	7
ETHERNET.....	9
ETHERNET MEDIA AND TOPOLOGIES.....	10
A BASIC STAR TOPOLOGY LAN.....	10
FAST ETHERNET.....	12
TOKEN RING LANS.....	12
BASIC RING TOPOLOGY LAN.....	13
FDDI.....	13
STANDARDS AND PROTOCOLS.....	14
NETWORK OPERATING SYSTEMS.....	15
NETWORKING TODAY.....	15

<b>CHAPTER THREE</b> .....	17
DESCRIPTION OF THE COMPONENTS.....	17
INTRODUCTION.....	17
THE CABLE.....	17
CABLE TYPES.....	17
CABLE CHARACTERISTICS.....	18
THE TWISTED PAIR CABLE .....	21
UNSHIELDED TWISTED PAIR CABLE.....	22
SHIELDED TWISTED PAIR CABLE.....	24
NETWORK INTERFACE CARD.....	25
THE PARALLEL TO SERIAL AND SERIAL TO PARALLEL DATA TRANSMISSION.....	25
PRINCIPLE OF NIC CONFIGURATION .....	29
SETTING INTERRUPT REQUESTS.....	31
BASE I/O PORTS.....	33
COMMON PC IRQS.....	33
BASE MEMORY ADDRESS .....	35
MAKING THE NETWORK ATTACHMENT.....	36
CHOOSING NETWORK ADAPTERS FOR BEST PERFORMANCE.....	37
THE SWITCH.....	40
<b>CHAPTER FOUR</b> .....	42
DESIGN AND IMPLEMENTATION OF A LOCAL AREA NETWORK .....	42
CONFIGURING THE NETWORK SERVER.....	42
CONFIGURING THE NETWORK INTERFACE CARD.....	43
CONFIGURING THE CLIENTS.....	43
NETWORK CLIENTS AND NETWORK SERVICES SOFTWARE.....	44
ADMINISTERING THE NETWORK.....	45
THE DESIGN OF THE NETWORK.....	46-47



CHAPTER FIVE.....	48
RECOMMENDATION AND CONCLUSION .....	48
RECOMMENDATION.....	48
CONCLUSION.....	49
REFERENCES.....	50

## CHAPTER ONE

### 1.0 INTRODUCTION

Networking involves connecting computers together for the Purpose of sharing information and resources. Even though the concept is basic, a great deal of technology is required to permit one computer to connect and communicate with another. The most elementary of all networks consist of two computers that are connected to each other so that no matter how many computers and which ever connection you used, they are all networking derives from the basic description above.

The motivation for networking arises from a need for individuals to Share data quickly and efficiently and to share other peripheral devices such as printers, scanners, fax machine and the like. The interesting thing about networking and some of the benefit therein are:

Data sharing permits groups of users to exchange information routinely and to route data from one individual to another as workflow demands. Data sharing also means that master copies of data files reside somewhere special on another computer on the network and that user can access the master copies in order to do their work, and some other are read only, which implies that it is restricted to one user to modify and effect change, that is an aspect of internet security.

Because data sharing is permitted among user, it also means that it improves human communication substantially. Peripheral device sharing allows groups of users to take advantage of peripheral such as printers, scanner, fax machines and other devices attached directly to a network or a computer that is always available attached to the network. So this reduces a firm or company cost of spending money in buying more peripherals.

This project is all about the LAN (local area network) which is a high-speed fault tolerant data networks that covers relatively small geographical area. It typically connects workstations, personal computers, printers and other devices. LAN offers computer user many advantages, including shared access to devices and application, file exchange between connected users, and communication between users via electronic mail and other applications; another very important application of this is the ability to use it to communicate with voice e.g. voice over internet protocol (VOIP), intercom, although all these require interfacing with some hardware and some application software. This project was carried out in the department of Electrical with computer engineering of the Federal University of Technology Minna. The project was carried out first by laying the CAT 5 cables running through the electrical laboratory and some of the electrical department offices.

The cables are laid in such away that they will not break or get injured. The distance covered by the cable to avoid slowness of the network. Ideally there is a standard for which a length of cable must run through a computer to another computer, but in this case it is not an ideal. The RJ 45 was crimped using the crimping tools and the standard IEE (Institute Electrical Engineers) color coding was followed. The color are listed below

- |    |              |   |
|----|--------------|---|
| 1. | Light yellow | 1 |
| 2. | Yellow       | 2 |
| 3. | Light green  | 3 |
| 4. | Blue         | 4 |
| 5. | Light blue   | 5 |
| 6. | Green        | 6 |

7. Light brown 7
8. Brown 8

The next thing that was done was that the operating system windows 2000 SERVER was installed on the computer which is the server, and an extra NIC (Network Interface Card) was installed on it so as to tap from it to expand the network. The other client computers in which their operating system needs to be re-installed or upgraded, the re - installation and upgrading was done in order to get a desirable network environment.

Some of the constraint we may have later is when the new offices are created and new staffs are employed and the need to expand the network arises, the network will become more slower, because the little bandwidth is being shared among the five departments in the school of engineering and engineering technology in which only four (4) ports from the switch was allocated to electrical department through which we expanded the network whereby about ten (10) computers are connected. Another constrains we might encounter is that the Radio room has no standby generator, which mean that the school of engineering server will be down if there is power failure. it doesn't matter if other department have another means of power supply, provided the server is down no one connected to that server through the main switch can access the internet.

The involvement of other departments is due to the internetworking. Internetworking refers to linking individual LANs from different department together to form a single internetworking.

This internetwork is sometimes called an enterprise network because it interconnects the entire computer network throughout various departments in the school

of engineering. Internetworking also allows separate buildings on campuses or businesses to be linked together so that all of the computing systems at that site are interconnected. Geographically distant in the enterprise wild internetwork.

An individual LAN is subject to limits on such things as how far it can extend, how many stations can be connected to it, how fast data can be transmitted between stations, and how much traffic it can support. If a company wants to go beyond those limits – link more stations than that LAN can support, for example – it must install another LAN and connect the two together in an internetwork.

There are two main reason for implementing multiple LANs and internetworking them. One is to extend the geographic coverage of the network beyond what a single LAN can support from multiple floors in a building, to nearby buildings, and to remote sites. The other key reason for creating internetwork is to share traffic loads between more than one LAN. A single LAN can only support so much traffic if the load increases beyond its carrying capacity, users will suffer reduced throughput and much of the productivity achieved by installing the LAN in the first place will be lost. One way to handle heavy network traffic is to divide it between multiple internetworked LANs.

There are three major types of devices used for internetworking: **bridge**, **routers** and **switch**. Today the most commonly used internetworking devices are high - speed routers, especially in wide area internetworks linking geographically remote sites. But routers are also heavily used in building and campus internetworks. Bridges have also been popular, even though they offer less functionality than routers, because they are less expensive to purchase, implement, and maintain.

LAN switches are new class of internetworking devices, and many people believe that switched networks will become the most common design for linking building and campus LANs in the future. Today's LAN switches and switching hubs are the first steps on a migration path to something called **asynchronous transfer mode (ATM)** switch, an emerging technology that will be widely implemented in both LANs and wide area networks in the coming years.

## CHAPTER TWO

### 2.0 LITERATURE REVIEW

#### 2.1 THE WORLD OF COMPUTER NETWORKING.

In the last 15 years, LANs have gone from being experimental technology to becoming a key business tool used by companies' world wide. A LAN is a high speed communications system designed to link computers and other data processing devices together within a small geographical area such as a workgroup, department or a single floor of a multistory building.

##### 2.1.1 THE BASIC OF LOCAL AREA NETWORK

Today, the local area networking is a shared access technology. This means that the entire device attached to the local area networking share a single communication media, usually a coaxial, twisted pair, or optic fibre cable. The figure below illustrates this concept.



**FIGURE 1      A BASIC LAN BUS NETWORK**

Several computers are connected to a single cable that serves as a medium for communication for all of them. The physical connection of the network is made by putting a network interface card (NIC) inside the computer and connecting it to the network cable. Once the physical connection is in place, it is up to the

communication software to manage the communication between the stations on the network.

### 2.1.2 THE BASIC LAN BUS NETWORK

From the figure 1 shown above which is an example of LAN Bus network, when station 2 sends a packet to another station on the LAN, it passes by all the stations connected to that LAN. On the bus network illustrated here, the electrical signal representing the packet travels away from the sending station in both directions on the shared cable. All the stations will see the packet, but only the station it is addressed to will pay attention to it.

In a shared media network, when one station wishes to send a message to another station, it uses the software in the workstation to put the message in an "envelope". This envelope is called a packet, this consist of a message data surrounded by a *header* and a *trailer* that carry special information used by the network software to the destination station. One of the pieces of information placed in the packet header is the address of the destination station.

The NIC then transmit the packet onto the LAN. The packet is transmitted as a stream of data bit represented by changes in electrical signals. As it travel along the shared cable, all of the station attached to it sees the packet. As it goes by the NIC in each station, the NIC checks the destination address in the packet header to determine if the passes the station it is addressed to, the NIC at that station copies the packet and then takes the data out of the envelope and gives it to the computer. The diagram in figure 1 shows one source station sending a single message to one destination station. If the message of the source station wants to send is too big to fit into one packet, it will send the



message in series of packets. On a shared LAN, all stations share the same cable. Since each individual packet is small, it takes very little time to travel to the end of the cable where the electrical signal dissipates. So after a packet carrying a message between one pair of stations passes along the cable, another station can transmit a packet to whatever station it needs to send a message. In this way, many devices can share the same LAN medium connected to that LAN. On the bus network illustrated here, the electrical signal representing the packet travels way from the sending station in both directions on the shared cable. All stations will see the packet, but only the station it is addressed to will pay attention to it.

In a shared media network, when one station wishes to send a message to another station it uses the software in the workstation to put the message in an "envelope". This envelope, called a packet, consists of message data surrounded by a header and trailer that carry special information used by the network software to the destination station. One of the pieces of information placed in the packet header is the address of the destination station.

The NIC then transmits the packet onto the LAN. The packet is transmitted as a stream of data bits represented by changes in electrical signal. As it travels along the shared cable, all of the stations will see the packet. As it goes by the NIC in each station, the NIC checks the destination address in the packet header to determine if the packet is addressed to it. When the packet passes the station it is addressed to, the NIC at that station copies the packet and then takes the data out of the envelope and gives it to the computer.

Figure 1 shows one source station sending a single message packet to one destination station. If the message the source station wants to send is too big

to fit into one packet, it will send the message in a series of packet. On a shared access LAN, however, many stations all share the same cable. Since each individual packet is small, it takes very little time to travel to the ends of the cable were the electrical signal dissipates. So after a packet carrying a message between one pair of stations passes along the cable, another station can transmit a packet to whatever station it needs to send a message. In this way, many devices can share the same LAN medium.

### **2.1.3 ETHERNET**

The most widely used LAN technology in use today is Ethernet. It strikes a good balance between speed, price, ease of installation, and supportability. Approximately 80 percent of all LAN connections installed use Ethernet.

The Ethernet standard is defined by the institute of Electrical and Electronics Engineering (IEEE) in a specification commonly known as IEEE 802.3. The 802.3 specification covers rules for configuring Ethernet LANs, the types of media that can be used, and how the elements of the network should interact. The Ethernet protocol provides the services called for in the Physical and Data Link Layer of the OSI reference model.

One element of the 802.3 (or 802.3u) specification states that Ethernet Networks run at a data rate of 10 million bits per second (10 Mbps) or 100 million bit per second (100 Mbps) in the case of fast Ethernet. This means that when a station transmits a packet onto the Ethernet medium it travels along that medium at 10 Mbps.

Another important element defined by the 802.3 specification is the access method to be used by stations connection to an Ethernet LAN, called

carrier sense multiple access with collision detection (CSMA/CD). In this method, each station contends for access to the shared medium. It is possible for two stations to try sending at the same time, which results in a collision on the LAN. In Ethernet networks, collisions are considered normal events and the CSMA/CD access method is designed to quickly restore the network to normal activity after a collision occurs.

#### **2.1.4 ETHERNET MEDIA AND TOPOLOGIES**

An important part of designing and installing a LAN is selecting the appropriate medium and topology for the environment. Ethernet networks can be configured in either a star or bus topology and installed using any of these different media. Coaxial cable was the original LAN medium it is used in what is called a bus topology in this configuration; the coaxial cable forms a single bus to which all stations are attached. This topology is rarely used in new LAN installations today because it is relatively difficult to accommodate adding new users or moving existing users from one location to another. It is also difficult to troubleshoot problems on a bus LAN unless it is very small.

#### **2.1.5 A BASIC STAR TOPOLOGY LAN**

In a star topology all stations are wired to a central wiring concentrator called a hub. Similar to a bus topology, packets sent from one station to another are repeated to all ports on the hub. This allows all stations to see each packet sent on the network, but only the station a packet is addressed to pays attention to it.

The diagram illustrates a star topology LAN --- which is a more robust topology than the bus topology. In a star topology, each station is connected to a

central wiring concentrator, or hub, by an individual length of twisted pair cable. The cable is connected to the station's NIC at one end and to a port on the hub at the other. The hubs are placed in wiring closet centrally located in a building.

Ethernet networks can be built using three different types of media: shielded and unshielded twisted pair, coaxial, and fiber optic cables. By far the most common is twisted pair because it is associated with the more popular star topology. It is inexpensive, and very easy to install, troubleshoot, and repair. Twisted pair cable comes both unshielded and shielded. **Unshielded twisted pair (UTP)** cable used for LANs is similar to telephone cable but has somewhat more stringent specification regarding its susceptibility to outside **electromagnetic interference (EMI)** than common telephone wire. **Shielded twisted pair (STP)**, as its name implies, comes with a shielding around the cable to provide more protection against EMI.

Of the two types of twisted pair cable, UTP is by far the most commonly used. The specification for running Ethernet on UTP is called **10Base-T**. This stands for 10 Mbps, base band signaling (the signaling method used by Ethernet networks), over twisted pair cable. Other Ethernet specifications include **10Base5**, which uses a thick coaxial cable, and **10Base2**, which uses a thin coaxial cable media. Today, 10Base5 is seldom installed in new Ethernet networks, and 10Base2 is used only in very small office networks or networks in high EMI areas. An additional standard, **10Base-FL**, allows Ethernet to run on fiber optic link

## 2.1.6 FAST ETHERNET

An extension of the popular 10Base – T Ethernet standard, **Fast Ethernet** transports data at 100 Mbps. With rules defined by the IEEE 802.3u standard, Fast Ethernet leverages the familiar Ethernet technology and retains the CSMA/CA protocol of 10 Mbps Ethernet. Three types of Fast Ethernet are available: 100Base – TX, which runs over Category 5 UTP; 100Base – T4 which runs existing Category 3 UTP; and 100 Base – FX, which operates over multi mode fiber optic cabling.

## 2.1.7 TOKEN RING LANs

Another major LAN technology in use today is **Token Ring**. Token Ring rules are defined in the IEEE 802.5 specification. Like Ethernet, the Token Ring protocol provides services at the physical and Data link layers of the OSI model. Token Ring networks can be run at two different data rates, 4 Mbps or 16 Mbps.

The access method used on Token Ring networks is called **token passing**. Token passing is deterministic access method in which collisions are prevented by assuring that only one station can transmit at any given time. This is accomplished by passing a special packet called a **token** from one station to another around a ring. A station can only send a packet when it gets the free token. When a station gets a free token and transmits a packet, it travels in one direction around the ring, passing all of the other stations along the way. As with Ethernet, the packet is usually addressed to single stations and when it passes by that station the packet is copied. The packet continues to travel around the ring until it returns to the sending station, which removes it and sends a free token to the next station around the ring.

## 2.1.8 BASIC RING TOPOLOGY LAN.

The ring topology used Token Ring networks is a collapsed ring that looks like a physical star. Each station is connected to a Token Ring wiring connector by single twisted pair cable with two wire pairs. One pair serves as the "inbound" portion of the ring (also known as the receive pair) and the other pair serves as the "outbound" or transmit pair.

In Token Ring LANs, each station is connected to a Token Ring wiring concentrator, called a **multistation access unit (MAU)**, using an individual run of twisted pair cable. Like Ethernet hubs, MAUs are located in wiring closets.

## 2.1.9 FDDI

**Fiber Distributed Data Interface**, commonly known as FDDI, provides data transport at 100 Mbps, a much higher data rate than Ethernet or Token Ring. Originally, FDDI networks required fiber optic cable, but today they can be run on UTP as well. Fiber is still preferred in many FDDI networks because it can be used over much greater distance than UTP cable. Like Token Ring, FDDI uses a token passing media access method. It is also used usually configured in a collapsed ring, or physical star, topology. FDDI is used primarily as a backbone, a segment of network that links several individual workgroup or department LANs together in a single building. It is also used to link several building LANs together in campus environment.

## 2.2 STANDARDS AND PROTOCOLS

LANs are complex systems that implement many different services in order to provide communication between all of the types of devices that can be connected to them. A communications model called the **Open System Interconnects (OSI)** reference model was developed by the International Standards Organization (ISO) to define all of the services a LAN should provide. This model defines seven layers, each of which provides a subset of all of the LAN services. This layered approach allows small groups of related services to be implemented in a modular fashion that makes designing network software much more flexible. A network software module that implements services at the Network and Transport Layers of the model can be paired up with other modules to meet the requirements of the user's application.

But the OSI model doesn't say how these Services should actually be implemented in LAN equipment. The "how to" part has been defined in a number of different **protocols** that have been developed by international standards bodies, individual LAN equipment vendors, and ad hoc groups of interested parties. These protocols typically define how to implement a group of services in one or two layers of the OSI model. For examples, Ethernet and Token Ring are both protocols that define different ways to provide the services called for in the physical and Data Link Layers of the OSI model. They have both been approved by the Institute of Electrical and Electronics Engineers (IEEE), an international communications standards body.

The International Standards Organization (ISO), the primary standard-setting body in the data communications industry, developed the framework for

LAN standards called the Open Systems Interconnect reference model. This reference model represents a standard approach to communicate information throughout networks so that a variety of independently development computer and communications devices can interoperate

## **2.3 NETWORK OPERATING SYSTEMS**

Ethernet and Token Ring technologies are just one part of a complete LAN. They provide the services specified in the Physical and Data Link Layers of the OSI model, but several other services must be added on top of the connectivity of Ethernet or Token Ring. Network operating systems (NOSs) are most often used to provide the additional communication services.

A Network operating system (NOS) defines clients and server systems. Clients are individual user workstations attached to the network where application program are run and data is generated. Serves are shared network resources that provide hard disk space for users to store files, printers' services, and a number of other network services. The network operating system provides a set of protocols in software that run on both serves and clients systems and allow then to communicate with each other, share files, printers, and other network resources.

## **2.4 NETWORKING TODAY**

LAN technology is evolving. In the early 1080s LANs were strictly local Area networks, linking small group of computers in company departments. As workgroup LANs, proliferated over the past 10 years, users began connecting them to form internetworking, first with bridges and later with routers. Today's



networks typically comprise a combination of workgroup and campus hubs, bridges, and routers. Switches are also beginning to become more prevalent.

The next few years will see networks evolve to include more sophisticated LAN switches and switching hubs. They will be designed using several different types of components, both old and new. Ethernet and Token Ring LANs will be built with stackable workgroup hubs, which in turn, will be interconnected by large modular hubs that may incorporate LAN switching functionality. Large networks will include another layer of consolidation with **network center** hubs linking workgroup hubs and switches. Routers will continue to be used as gateways to the wide area network linking other buildings and remote sites.

For networks to deliver the performance today's users require, their many components must work together to deliver seamless connectivity between all of the users and computing systems throughout the enterprise. Flexibility to grow, power to support applications, and seamless connectivity are what users expect in the products they choose to build LANs and enterprise networks.

## CHAPTER THREE

### 3.0 DESCRIPTION OF THE COMPONENTS

#### 3.1 INTRODUCTION.

In this chapter, the design and the implementation of local area network, a case study of the electrical department Federal university of technology Minna, is explained from the description of each of the component used, the diagram of the component and equipment, their usefulness and limitation. The design procedures from the beginning to the end of the design, all the steps taken and why those steps were taken are all the explained in this chapter.

#### 3.2 THE CABLE

Regardless of the kind of media in use, data must enter and leave the computer at some point to allowed networked communication to occur. When data is passing through the OSI model (Open System Interconnection) and reaches the physical layer, it must find its way into a medium that is useful to physical transfer data from computer, this medium is called cable. Cabling communication are therefore the heart of networked communication. It is the network interface card's role to prepare the data for transmission, but it is the cables role to properly move the data to its intended. destination

##### 3.2.1 CABLE TYPES

Fundamentally, all forms of cabling are similar, in that they provide a medium across which network information can travel in the form of a physical signal, whether it is a type of electrical transmission or some sequence of light pulse. Given the many types of cable available in today's market place, it should come

as a relief for us to investigate and understand only three types, which represent the vast majority of cabling types used to interconnect networks :

1. coaxial cable

2. twisted pair ( TP )

- Unshielded twisted pair ( U T P )

-Shielded twisted pair ( S T P )

3. Fibre optics

Each of this cabling comes in a variety of forms, each with its own unique design and usage characteristics, with associated cost, performance and installation criteria. For this project we will discuss the general characteristics of cables, and give some salient characteristics of the three types of cable mention above.

### 3.2.2 CABLE CHARACTERISTICS

All cables shares certain fundamental characteristics; studying them will facilitate our understanding of their function and appropriate use. The following characteristics apply to equally to both types of cabling:

- **Bandwidth rating:** Each type of cable can transport only so much data over a given period of time; this is measured in terms of bandwidth, which describes how many bits or bytes of information a cable can carry over a limit time. Typically, this is measured in some number of bits per second e.g megabits per second or Mbps.
- **Maximum segment length:** Each type of segment can transport data only so far before its signal begins to weaken beyond the point where it can still be read

accurately; this is what we called attenuation. When rating maximum cable segment length, the maximum segment length value falls within a range where signal can be regenerated correctly and retransmitted accurately. So, an internet work can be constructed of several such cable segments, provided the hardware interconnecting them can capture and regenerate the incoming signal at full strength.

- **Maximum Number of segment per internet work:** Each cable is also subject to a measure called latency, which measure the amount of time a signal takes to travel from one end of the cable to the other. Most networks are subject to some kind of maximum tolerable delay, after which its assumed signal can no longer arrive. A network of network is therefore subject to maximum number of interconnected segments, simply because of the latency when signal level from one physical end of the network to another. By arranging cable segments in hierarchy, the span of a network can be quite large, even within these limitations, because the limitation applies to the maximum number of segments between any two particular network segments.
- **Maximum number of devices per segment:** Each time a network device is attached to a cable, a phenomenon called **insertion loss** occur, that is, each physical connection adds to the attenuation of the signals on a cable segment, making it necessary to restrict the maximum number of devices to keep the signals that traverse it clean and strong enough to remain intelligible to all devices. When calculating maximum legal segment length, the real formula for distance equals the rated maximum minus the sum of the insertion losses for all the devices attached to that segment.

Mathematically

$$K = y - x$$

Where k = The true maximum

Y = Rated maximum

X = Insertion losses

- Interference Susceptibility : Each type of cable is more or less susceptible to other signals that may be present in the environment, where such interference may be electromagnetic that is electromagnetic interference, EMI or may result from other broadcast signals called RFI, for radio frequency interference. Motors, Transformers, and other sources of intense electrical activity can emit both EMI and RFI, but RFI problems are also associated with the proximity of strong broadcast sources in an environment such as nearby radio or television station.

- Connection hardware: Each type of cable has connector associated with it, that influences the type of hardware it can connect to, as well as the costs of the resulting network.

- Cable grade: Both building and fire codes include specific cabling requirements; usually aimed at the combustibility of the sheath material and insulation that covers most cable. The polyvinyl chloride (PVC) covers the cheapest and most common cables.

- Bend radius: Although some types of cabling are less prone to damage from bending many types beyond a provided bend radius damages or destroys them. This is mostly particularly true of the most expensive types of cable; For networks,

this means primarily that fibre Optics and heavy duty coaxial cables must be treated with care.

Most of the more sensitive cable types cannot be bent more than 60 degrees in one foot span without sustaining some damages. The most important thing is to understand the limitations of the cabling itself and not to bend it past its limits. For the purpose of this work, we shall only place our emphasis on out of the three types of cable mentioned above.

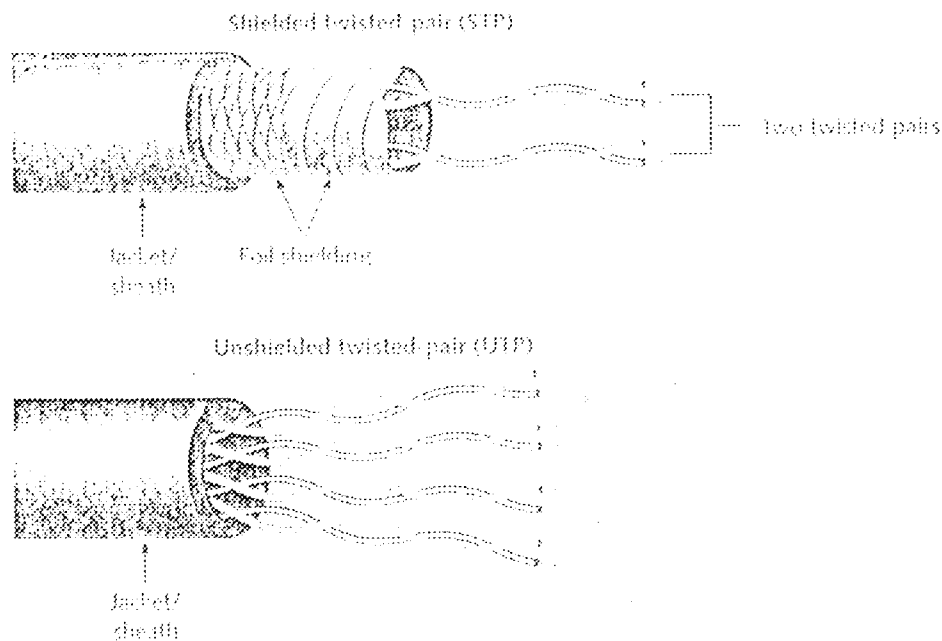
### **3.3 THE TWISTED PAIR CABLE**

The most basic form of twisted (TP) wiring consists of one or more pairs of insulated strands of copper wire twisted around one another. This twist are important because they cause the magnetic fields that form around a conducting wire to wrap around one another to improve twisted pairs resistance to interference, while also limiting the influence of the signals traveling on one wire over another which is called cross talk. In fact, the more twists per unit length, the better these characteristic become. It's safe to say that more expensive twisted pair wire is usually twisted than the less expensive types.

There are basically two types of twisted pair cables, namely

1. The unshielded twisted pair (UTP)
2. Shielded twisted pair. (STP)

The unshielded twisted pair, which simply contains one or more pairs of insulated wires within an enclosing insulating sheath, and the shielded twisted pair, which simply enclose each pairs of wire within a foil shield as well as within an enclosing insulating sheath. The UTP and STP is depicted in the figure below.



### 3.3.1 UNSHIELDED TWISTED- PAIR (UTP)

Another version of the IEEE Ethernet specification is called 10Base T; here T stands for UTP and represents another type of Ethernet cabling. In fact, 10 Base T is now the most popular form of LAN; a 10Base T segment is 100 metres, or 328 feet.

The UTP cable used for networking usually includes one or more pairs of insulated wire. UTP specification govern the number of twist per foot (or per metre), depending on the cable's intended use. The type of cable used for telephone system, UTP is therefore common in most office buildings and other work environments.

But voice telephony is much less demanding than networking in terms of bandwidth and signal quality. This, even though it may be tempting to try to turn unused telephone wiring in to network connection, it's worth attempting this unless a cable technician tests those lines and pronounces them fit for network use.

UTP cabling is rated according to a number of categories devised by the electronic industries Alliance (EIA) and the telecommunication industries Association (TIA); since 1991, the American National standards Institute (ANSI) has also endorse these standards. A document known as the ANSI/EIA/TIA 568,

The ANSI/EIA/TIA 568 standard generally includes five categories for unshielded twisted pair wiring, as follow:

- **Category 1:** Applies to traditional UTP telephone cabling, which is designed to carry voice but not data.
- **Category 2:** Certifies UTP cabling for bandwidth up to 4Mbps and consist of four pairs of wire. Since 4Mbps is blower them most networking technologies in use today (except for original token ring installation and ARC net), category 2 is rarely encountered in networking environments.
- **Category 3:** certifies UTP\_cabling for band width up to 10Mbps, with signaling rates up to 16MHz. This include most conventional networking technologies, such as 10 base T Ethernet, 4Mbps token ring, ARC net, and more. Category 3 consists of four pairs, each pair having a minimum of three twists per foot (10 twists per meter). 100VG-Any -LAN is also rated to work on category 3 cable, but testing recommended for older installations.



- **Category 4:** certifies UTP cabling for bandwidth up to 16Mbps with signaling rates up to 20MHz. This includes primarily 10Base T Ethernet and 16Mbps token ring. This is the first ANSI/EIA/TIA designation that labels the cables as data grade rather than voice grade. Category four consists of four pairs.
- **Category 5:** certifies UTP cabling for bandwidth up to 100Mbps, with signaling rates up to 100MHz. This includes 100Base x, Asynchronous transfer mode (ATM) networking technologies at 25 and 155Mbps, plus FDDI at 100M bps, as governed by the twisted pair, physical media Dependent (TP-PMD) specification. Some experiment implementations of Gigabit Ethernet use category 5 cable, but standards are yet undefined for this technology. Category 5 also uses four cables.

### **3.3.3 SHIELDED TWISTED – PAIR (STP)**

As its name implies, shielded twisted pair (STP) includes shielding to reduce cross talk as well as limit the effects of external interference. For most STP cables, this means that the wiring includes a wire braid inside the cladding or sheath material, as well as a foil wrap around each individual wire pair. This shielding improves cables transmission and interference characteristics, which in turn support higher bandwidth over longer distances than unshielded twisted pair (UTP). Unfortunately no set of standard for UTP, and it is not unusual to find STP cables rated according to those standards.

### 3.4 NETWORK INTERFACE CARD (NIC)

For any computer to be used on the network, the network interface card (NIC) performs two crucial tasks:

1. It translates digital computer data into signals (appropriate for networking medium) for outgoing messages, and translates signals into digital computer data for incoming messages.
2. It establishes and manages the computer's network connection.

In other words, the NIC establishes link between a computer and a network and then manages that link on the computer's behalf.

### 3.5 THE PARALLEL TO SERIAL AND SERIAL TO PARALLEL DATA TRANSMISSION

Because of the nature of the connection between most NIC's and the computers to which they are attached, network adapter also manage transformations in the form that network data takes. Most computer use a serial of parallel data lines, called a computer bus (or bus for short) to send data between the CPU and the adapter card, including the network adapter. This allows the computer and adapter to exchange data in chunks equal to the number of lines that extend between them. Because data travels along multiple lines at the same time, and those line run both metaphorically and physically parallel, this type data transmission is called **parallel transmission**. However, for nearly all forms of networking media, the signals that traverse the media consist of a linear sequence of information that corresponds to a linear sequence of bits of data (or their analog equivalent for non digital media). Because these bit of data follow

one another in a straight line, or a series, this type of transmission is called serial transmission. Thus, one of the most important jobs a network adapter performs is to grab outgoing transmission from the CPU in parallel form and recast them into their serial equivalents. For incoming messages, the process reverses: the network adapter must grab on incoming series of signal translate them into bits, and distribute those bit across the parallel lines used to communicate with the CPU

An analogy may help to clarify the difference between the parallel and serial forms of data. A parallel transmission works like a multi-lane highway, in which each lane carries part stream of traffic information between sender and receiver at the same time. The larger the number of lanes, the more traffic or information, the highway can carry at any given moment.

Using the same analogy serial transmission resembles a one lane road. Obviously, serial line is inherently slower than a parallel line, because the speed of the line alone limits the amount of data a serial line can transmit, for a parallel set of lines; both the number of lines and their speeds play a role in how fast data can travel. Consequently one of the most important components on a network adapter is memory, which acts as a holding tank, or **buffer**. The data going out in large parallel chunks must be serialized for output; incoming data arrives one bit at a time and must be distributed across all the parallel lines before a single set of these bits can be delivered to the CPU

The connection of parallel lines that links elements inside a computer is called a bus. When data moves from one component to another, it moves along the bus. Earliest generation of PCs used 18-bit buses, which means they used eight lines

for data in parallel and could move 8 bits worth of data in a single bus transfer. The number of parallel lines that make up a particular kind of computer bus is called its **bus width**. For example, ISA supports 8- and 16- bits bus widths. EISA and MCA support 16- and 32- bit bus widths and PCI support 32- and 64- bit bus widths.

To transmit data across the network medium, a network adapter must include or access a device called a **receiver** that is design for the specific medium in use. For common networking technologies such as Ethernet that work over a variety of media, it's not uncommon to find multi way NICs that can be configured to use one of several media to attachments built into the card.

The figure below shows an Ethernet NIC that include the female BNC connector where the base of the T-connector attaches to a thinnet network, along with an AUI for thinnet and an RJ-45 for 10base T. with the appropriate setting choosing, the card can be told which attachment to use and brings the appropriate circuitry to bear for both thinnet and 10baseT. Such NICs include a built in, on-board Transreceiver; for thinnet and external Transreceiver must be connected to the card through the AUI port at the back.

Network adapters that use more exotic media-for example, some wireless technology or fiber optic cable usually support only that one medium. In that case, it's necessary to make the right connections to the card to establish a network connection, whether wired or wireless.

Network adapters also handle important data packaging functions as they serialize outgoing parallel data streams from the CPU and translate incoming serial data streams from the network medium into parallel data. The NIC

packages all the bits into orderly collections called **packets** and then transmits individual packets serially onto the network medium. For incoming messages, the NIC creates packets of data from incoming signals and then extracts the content of each packet of parallel translation and delivery to the CPU. Packets are the fundamental unit of data for network transmission and reception. Much of the important processing that network adapters performs not only involves creating, sending, and receiving packets, but also dealing with packet-level errors and incomplete or unintelligible packet structure.)

Other important roles a NIC plays are packing and preparing data for transmission across the medium and managing access to the medium to know when to send data. Network adapters examine incoming network packets and check to find any addressed to the computer where the adapter resides. The NIC acts as a kind of gatekeeper and permits

Inbound communication aimed only at its computer to pass through the interface and on to the CPU. Some NICs have the ability to operate in what, called "promiscuous mode"-this essentially turns off the gatekeeper functions and enables the NIC to forward any packets it sees to the computer. This kind of functionality is important function when it interacts with network scanning or sniffing software that analyzes overall traffic flow or permits detailed inspection of individual packets. For ordinary users, though, such functionality is usually unnecessary.

The NIC's role as gate keeper points to another important function network adapter provider namely, determining whether the computer is the appropriate recipient of data sent across the wire. Each card has a unique identifier, called a

network address that takes the form of data programmed onto Read - Only Memory (ROM) on the interface. The IEEE sponsors a manufacturer's committee that designed an addressing scheme for network adapter and assigns unique blocks of addresses to NIC manufacturers. Each new NIC built has a unique, identifiable address encoded onto it, guaranteeing each computer its own network address. The gate keeper function simply looks for an address bit string in the decoded packet that matches its own address or that corresponds to a valid "general delivery" address by now. It should be clear that the NIC is intimately involved in managing and controlling network access, and its roles goes beyond creating a physical link between a computer and a network medium. The NIC also handles data transfers to and from the network and CPU and translates which forms such data can take between parallel and serial representations. In addition, the NIC interacts with the medium to determine when data the data transmission is permissible.

### **3.6 PRINCIPLES OF NIC CONFIGURATION**

Once you match a network adapter to a slot in a PC, or plug it into a serial bus, the next step is to configure it to work with your computer. In a perfect world, this might mean opening the PC, seating (positioning) the network adapter in a bus slot, closing the PC box, and turning on the system. Alternatively, it might only require plugging an external network interface into a serial bus port (very handy for laptops). As soon as the computer boots up, the network would be available. Unfortunately, it isn't usually this easy.

In an attempt to fight this approach this level of perfection, Microsoft introduced its plug and play architecture with the Windows 95 operating system. Plug and

plug and play attempts to define a set of configuration protocols so a computer can communicate with its peripherals during the **POST (power-on self-test)** sequence and negotiate a working configuration without requiring human intervention. If the motherboard, operating system, and all adapter support plug and play, this works well. But if some devices do not support plug and play, or if any device fails to conform precisely to plug and play requirements, manual (human) intervention is required. Today, manual intervention remains the rule on PC's, not the exception. Apple Computer has done a much better job of automating device installation on the Macintosh, to the point where many such devices run immediately when the computer is powered on after adding a device.

For computer systems that do not fit the plug and play model completely, or for PC's that run operating systems other than Windows 95, 98, or 2000, manual configuration is essential to make any NIC work properly.

Typically, NIC configuration involves working with three types of PC settings:

- Interrupt request line (IRQ)
- Base I/O port
- Base Memory Address

Each of these settings is described next.

On some NICs, settings are software configurable; on others, it's necessary to physically manipulate jumper blocks or DIP switches. Working with software configuration requires a bootable computer, so it's important to be able to start the machine with the NIC's defaults. Cause conflicts with other adapters, removing those adapters may be necessary to bring the PC up to run the NIC's

configuration utility for the first time. For that reason, software configured NIC's are always the unmitigated boon that some think they are.

Hardware configured NIC's impose a different set of problems namely, most require that you remove the card to make configuration changes. It is wise to test your configurations (at least the first time) without completely reassembling the PC's case. That way you can change the settings more quickly as you make your way to a working NIC's configuration.

Two ways of setting hardware configurations are with jumper blocks of DIP (dual inline package) switched as depicted in fig. 4-4. A **jumper** is a small plastic cased connector that bridges two pins. By extension, a **jumper blocks** is a collection of jumpers pins placed in a line. A **DIP switch** is a small electronic part with one or more single throw switches set in line. You can use a paper clip or a small screwdriver to change DIP switch settings.

### 3.7 SETTING INTERRUPT REQUESTS (IRQ'S)

Most computers have only one CPU (or at most a handful) but many adapters. An average PC whether a server or a desktop machine -- has one or more disc controllers, a floppy controller, a graphics card, one or more serial controllers, one or more network cards, a sound card, and perhaps more adapters plugged into its bus connections. With so many devices competing for the CPU's attention, some method of peripherals to signal a request for its services is imperative.

Such request for the CPU's are called **interrupts** (or more formally **interrupt requests**). Each PC uses a number of dedicated lines, called **interrupt request lines (IRQs)**, which gives peripherals a way to send a signal at any time to the



CPU that they need service. In fact, each PC peripheral must have its own IRQ line to the CPU so each one can signal the CPU independently. IRQs are identified by a number, which corresponds to the "address" for a line reserved exclusively for one peripheral to signal the CPU.

To prevent this problem, before you try to install any adapter card in a CP, construct a map of IRQs already in use on the machine. The only way to be sure which IRQs are available is to run **diagnostic software** that generates a report. For PCs running DOS, windows 3.x, or Windows 95, use the DOS **MSD.EXE** program to determine which IRQs are taken (and which are available). For windows 98, use the Device Manager (Start, Settings, Control panel, System applet, Device Manager tab, then click the properties button to get IRQ, I/O, DMA, and Memory mapping information). Or use the Add New Hardware Wizard to attempt to resolve hardware conflicts. For PCs running Windows NT, use the Windows NT Diagnostic Tool, which appears in the administrative Tools (common) entry. You can also access it by clicking start, Run on the task bar, and entering **WINMSD.EXE**. For windows 2000, use the Device Manager utility (start, settings, control panel, system, hardware tab, Device Manager Button, and then pick Resources by type from the view menu to see DMA, I/O, IRQ, and memory resources)

Interrupt-driven device handling is a hallmark of PCs, dating back to their earliest incarnations. many IRQs assigned for specific uses are unavailable for use in most cases anyway; other are sometimes available, depending on how the particular machine is configured. Table 4-1 (see next page) lists the 16 most common PC IRQs and indicates those most commonly available.

### 3.7.1 BASE I/Q PORTS

Once the CPU acknowledges an interrupt from a device, the device needs to send data to explain what it wants. The CPU usually needs to send data back to the device in response to its request. The **base input/output (I/Q) port** assigned to a device defines an area of memory the CPU and the device can use to move messages between them. This area of memory acts like a mail box, where the CPU can leave a message for the device and vice versa. Like an IRQ, a base I/Q port for any device must be unique.

Base I/Q ports are identified by three digit **hexadecimal** (a mathematical notation for representing numbers in base 16 form) numbers often expressed as a 16-bit range of number: so, port 200 corresponds to the address range 200-20F. By default, most NICs assign a base I/Q port of 300, where the address usually appears as 300h (to indicate a hexadecimal number) or 0x300 (which also indicates hex notation). Other common base I/Q ports for NICs include 280h and 310h. If none of these values is available, consult Table 1 a value that's not usually assigned for other purposes.

**TABLE 1 COMMON PC IRQS**

IRQ	TYPICAL ASSIGNMENT
0	PC System timer.
1	Keyboard
2	Cascading IRQ controller or video adapter
3	Unassigned (used for COM2/COM4 or bus mouse)

4	COM1/COM2
5	Unassigned (used for LPT2, often for sound card)
6	Floppy disc controller
7	Parallel port LPT1
8	Real-time clock
9	Cascading IRQ controller, sometimes sound card
10	Unassigned (used for primary SCSI controller)
11	Unassigned (used for secondary SCSI controller)
12	PS/2 mouse (if none present, unassigned)
13	Math co-processor (if none present, unassigned)
14	Primary hard drive controller, usually IDE (if no IDE drives, unassigned)
15	Secondary hard drive controller, usually IDE (if absent, unassigned)

Port	Device	Port	Device
200	Game port	300	NIC
210	Unassigned	310	NIC
220	Unassigned	320	Unassigned
230	Bus mouse	330	Unassigned
240	Unassigned	340	Unassigned
250	Unassigned	350	Unassigned
260	V	360	Unassigned
270	LPT3	370	LPT2
280	NIC	380	Unassigned

290	Unassigned	390	Unassigned
2A0	Unassigned	3A0	Unassigned
2B0	Unassigned	3B0	LPT1
2C0	Unassigned	3C0	EGA/VGA Video
2D0	Unassigned	3D0	CGA Video
2E0	Unassigned	3E0	Unassigned
2F0	COM2	3F0	COM1, floppy disk controller

### 3.7.2 BASE MEMORY ADDRESS (MEMBASE)

To do their jobs, peripheral devices and the CPU must do much more than signal interrupt and pass messages back and forth they must move large volumes of data. Where NICs are concerned, memory space is essential for buffering input and output, to allow the creation of packets for large amount of data in serial form and to unpack incoming packets and translate them into to parallel transmission for delivery to the CPU.

To that end, the NIC establishes a buffer area in memory to store incoming and outgoing data temporarily before transferring it else where for transmission over the network or delivering it to some application. The starting address for the NICs buffer space is called the **base memory address**, or **membase**. That address, plus the buffer having a fixed maximum size (called an **extent**), carefully circumscribes the region of memory available for data transfers to and from the NIC. For historical reason, such buffers are usually allocated in address range between 640KB and 1MB (A0000 to FFFFF in hex notation) called the upper memory area, or **high memory area (HMA)**. Most NICs use a default

member of D8000, which seldom needs adjustment unless the HMA on the PC where the NIC is installed is crowded.

### 3.7.3 MAKING THE NETWORK ATTACHMENT

Network adapters perform several vital roles to coordinate communications between a computer and a network, including:

- Establishing a physical link to the networking medium
- Generating signal that transverse the networking medium and receiving incoming signals
- Implementing control for when to transmit signals to or receive signals from the network medium

Because the network medium attaches directly to the network adapter, or through a transceiver attached to the adapter, it's important to match the adapter you choose with the medium to which it must attach. Every networking medium has its own physical characteristics that the adapter must accommodate. That is why NIC's are built to accept certain kinds of connectors that match the media involved.

For common networking technology for example, Ethernet is unusual for a network adapter to be able to accommodate two or three media types (usually two or more of thinnet, thinnet, and 10 Base T, as figure 4-2 indicates) but when a network adapter support more than one media type, selecting the one to use becomes another configuration option. Normally, selecting the media type on switch cards involves changing DIP switches or shifting a jumper block (illustrated earlier in figure 4-4), if the card isn't software configurable.

Whenever you encounter such a card, read the manual to get the information you need to configure the card correctly.

### 3.8 CHOOSING NETWORK ADAPTERS FOR BEST PERFORMANCE

As the focus of the network traffic on work stations, and of large volume of traffic on network servers (even those with more than one network interface), NICs can exert significant influence on network performance. If a NIC is slow, it can limit network performance. Particularly on network with shared media, slow NIC's anywhere on the network can decrease performance for all users.

When selecting a network adapter, you must first identify the physical characteristics the card must match. This includes the type of network technology in use and the kind of connector or physical attachment the adapter must accommodate. Once you determine these basic characteristics, it's equally important to consider other options available for purchase that can seriously affect a cards speed and data handling capabilities. Some of these options suit server better, whereas others work equally well for servers and clients: all help improve overall network performance. These hardware enhancement options include

- **Direct Memory Access (DMA)** allows an adapter to transfer data directly from its on-board buffers into the computer's memory, without requiring the CPU to coordinate memory access.
- **Shared Adapter Memory** means the adapters buffer map directly into RAM on the computer. When the computer thinks its writing to its own memory its

writing to the buffers on the NIC. In this instance, the computer treats adapter RAM as its own.

- **Shared System Memory** means a NIC's on-board processor select a region of RAM on the computer and write to it as if it were buffer space on the adapter. In this instance, the adapter treats computer RAM as its own.
- **Bus Mastering** permits a network adapter to take control of the computer's bus to initiate and manage data transfers to and from the computer's memory, independent of the CPU. This lets the CPU concentrate on other tasks and can improve network performance 20% to 70%. Such cards are more expensive than other NIC's, but are worth the price, especially for servers.
- **RAM Buffering** means a NIC includes additional memory to provide additional memory to provide temporary storage for incoming and outgoing data that arrives at the NIC faster than it can be shipped out. This speed overall performance because it lets the NIC process data as quickly as it can, without having to pause occasionally to grab (or send) more data.
- **On board co-processors** included on some NIC's permit the card to process data (such as packetizing outgoing data or depacketizing incoming data) without requiring service from the CPU. Today, most NIC's include such processors to speed network operations.
- **Security features** may be available on some high end NIC's. These permit the card to handle all kinds of protocol functions, including IPsec and other encryption services related to authentication and payload protection. (IPsec

is a secure transport mechanism that's gaining broad acceptance as a way to protect network traffic from unwanted snooping)

- **Traffic management or grooming** may also be available on some high-end NICs. These services include improved abilities to guarantee levels of access to the network (called **QoS**, or **Quality of Service**, when applied to streaming video or multimedia or other applications that require bandwidth guarantees) to support remote management software and services, and more.
- **Improved fault tolerance**, in the form of redundant NICs with failover capabilities, may be available in some high-end NICs. By installing a second such NIC in a PC, failure of the primary NIC shifts network traffic to the second NIC, rather than cutting off the PC from the network.

Selecting the number of such options on any network interface means weighing carefully how much network traffic the adapter must handle and how important its continued functioning is. The more traffic, the bigger the payback speed-up options can provide. For servers, this means buying the fastest network interface you can find (or afford as the case may be); usually, this means 32-bit, bus-mastering NICs with shared memory and substantial on-board buffer space. For workstation, slower card may be acceptable on machine that use the network lightly, but any machine that access the network heavily for demanding applications. Such as data base management systems (DBMSs) or CAD, benefits from any speed-up options a quality network adapter can provide. Increased availability, and manageability, reliability, and manageability have obvious pay-offs for servers that may not apply to workstation.



### 3.9 THE SWITCH

Switches are another type of device used to link several separate LANs and provide packet of filtering between them. A LAN switch is a device with multiple ports, each of which can support a single end station or an entire Ethernet or Token Ring LAN with a different LAN connected to each of the switch's ports, it can switch packets between LANs as needed. In effect, it acts like very fast multiports are filtered by the switch based on the destination address.

Switches are used to increase performance on an organization's network by segmenting large networks into many smaller, less congested LANs, while still providing necessary interconnectivity between them. Switches improve network performance by providing each network with dedicated bandwidth, without requiring using to change any existing equipment, such as NICs, hubs, wiring, or any routers or bridges that are currently in place. Switches can also support numerous transmissions simultaneously.

Deploying technology called **dedicated LANs** is another advantage of using switches. Each port on an Fast Ethernet switch supports a dedicated 100 Mbps Ethernet LAN. Usually, these LANs comprise multiple stations linked to a 100 BASE-TX hub, but it is also possible to connect a single high performance station, such as a server, to a switch port. Using LAN switches allows a network designer to create several small network segments. These smaller segments mean that fewer stations are competing for bandwidth, thereby diminishing network congestion.

In this case, that one station has an uncontested 100Mbps Fast Ethernet LAN all to it self. Packets forwarded it over it from other ports on the switch will never produce any collisions because there are no other stations on the LAN at that port.

As was noted earlier, LAN switching is a relatively new technology. Today's switching devices switch relatively large, variable length LAN packets between different local area networks. ATM is another switching technology that switches small, fixed-length cells containing data. ATM network can be run at much higher data rates than today's LANs. Eventfully, they will be used to carry voice, video and multimedia traffic, as well as computer-generated data over both short and long distances. ATM will be one of the dominant enterprise network technologies of the future, and many companies are beginning to develop strategies to incorporate ATM in their existing LANs and LAN internetworks.

## CHAPTER FOUR

### 4.0 DESIGN AND IMPLEMENTATION OF LOCAL AREA NETWORK

This chapter focuses on how the design and implementation was carried out. Designing a network does not have to be difficult. The most important point to consider are the number of users, where they are located the type of software, special requirements such as security and electromagnetic interference. All impact how a network is designed.

#### 4.1 CONFIGURING THE NETWORK SERVER

Since the design is in starlan, server would be used, in order for the other client computers to interact smoothly with it.

The server is a computer like any other. It has a hard disc on which it stores data, a CPU to compute, and a network interface adapter to connect it to the rest of the network. It also has an operating system to control the hardware and to provide the network services that makes a server the heart of networking activity. This hardware's must be chosen properly to enhance the speed, scalability usability and ease of administration of your network. The server must be more powerful than any other computer in terms of speed. The operating system include window NT. The operating system must be compatible before installing it on the system. Before you install the network operating system, you may wish to partition the computer's hard disk.

Partitioning is the process of dividing the space on the hard disks for the operating system, user files, shared files, programs and other purposes.

## **4.2 CONFIGURING THE NETWORK INTERFACE CARD**

Servers communicate on network through their network adapter cards. When you install the operating system, you tell it which type of network adapter card you have and you need to provide a driver for the card, although some operating systems detect and install automatically.

Depending on the type of card you use, the interrupt request must be provided and port settings for the card. Your adapter card manual will tell whether or not this information's are needed. The protocol to be used must also be determined, for instance Windows NT gives three choices:

- Transmission control protocol (TCP/IP)
- Internet work packet exchange (IPX)
- Network Basic input/output system extended user interface (NetBEUI)

In this design transmission control protocol is used because it is good for small non-routed networks or workshops. It is fastest and to setup of all the transport protocols.

## **4.3 CONFIGURING THE CLIENTS.**

The client on network must be configured so that application software such as word processors and spreadsheet could be run on them. Configuration of server and client are almost the same process, but the only difference is that, the server, being the brain of the network, must be powerful in server than clients.

The configuration of these computers is mainly on the physical arrangement of hardware and logical installation of the softwares. After the physical arrangement of the system, the necessary hardware such as network adapter is

configured by double – clicking network icon on the status menu, which display network connection dialog box. From this select the add button to add a networking component and select adapter to add an adapter. Find the network interface card installed in the computer. If your adapter is not included in the list, select Hard disk and select adapter from the floppy disk provided by the manufacturer.

#### **4.4 NETWORK CLIENTS AND NETWORK SERVICES SOFTWARE**

The final links to connecting the client computer to the network are the network client and the network services software.

These packages log you into the network and redirect file accesses and print request for the file print servers. Some packages that come with Window 95, which is used in this design, include:

- Client for Microsoft networks
- Client for Netware networks
- File and printer sharing for Microsoft networks
- File and printer sharing for Netware networks

To use network services, you must first log into the network and to do that you need the network client package for that network, which is installed from the network dialog box in the control panel. You need to configure the client attach it to network. For Microsoft work group (peer) networks, you select the identification tab in the network dialog-box. There, computer's name is entered

and the name of the work groups. The network domain's name must be specified in the properties section of the client for Microsoft network software package.

#### 4.4 ADMINISTERING THE NETWORK

After the installation and configuration of the network, the network must also be administered in order to be able to manage the running network. The network administrator is concern with proper operation of the network, the duty of a network administrator includes:

- Creating a useful network environment
- Managing the network environment
- Protecting the network

Creating a network environment covers the planning of overall nature of the network, the creation of users and groups the implementation of network policies and the documentation of the network once it is installed. In creating of user's environment, each person is given a username and a password. The person uses that to establish a personal – computing environment including such things as the background pattern on the screen and the location of personal files. While group help you to organize user accounts by needs, functions and attributes. Permission could also be assigned to groups so that individuals within a group can share resources, such as a common directory or printer.

Protecting the network environment covers such activities as implementing fault-tolerant systems, scanning for viruses, and installing uninterrupted power supplies.

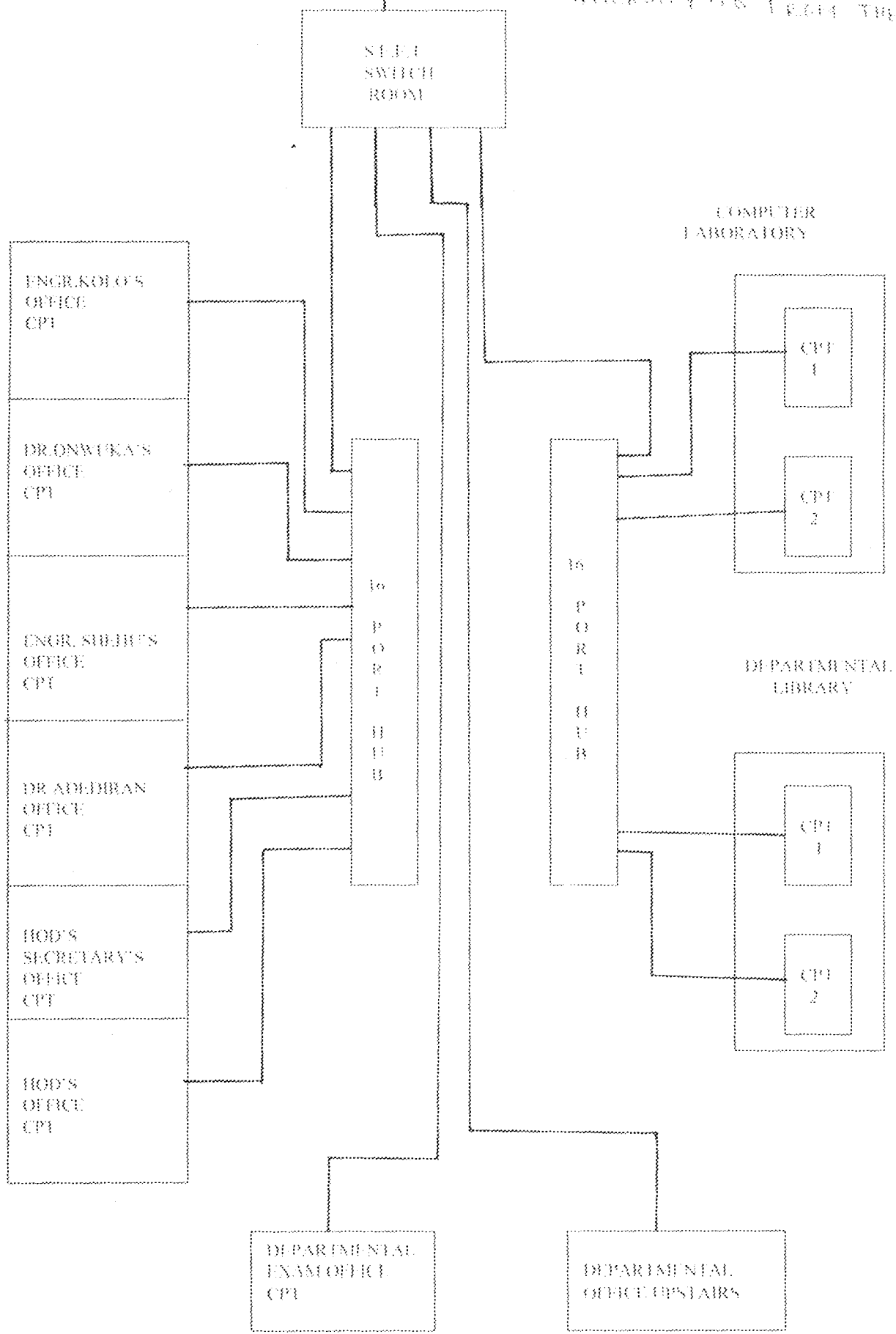
Managing a network environment covers the periodic tasks of managing user account, upgrading servers, monitoring network performance, and backing up the network.

#### **4.5 THE DESIGN OF THE NETWORK**

The following diagrams and figures illustrate how the design was done. They also show the arrangement of the server and the clients.

A hub of sixteen ports was used to connect the server and clients. Cables are run from each client and server to the hub. The cabling layout is also illustrated there too. The entire installation took place at the electrical department as shown on the site layout.

TO MAIN ANTENNA TERMINAL  
FROM THE UNIVERSITY TO THE VENT





## CHAPTER FIVE

### 5.0 CONCLUSION AND RECOMMENDATION

#### 5.1 RECOMMENDATION

I recommend that computer networking should be implemented in electrical/computer engineering department because this enables easy transferring and sharing of resources within the department, school of engineering and even outside the school of engineering

I also recommend that the computer laboratory in the department should be equipped with more computers and possibly an internet cafe for researching; although that will mean the department will have to get its own wireless equipments, but its worth going for because of the benefit that will be derived from it.

## 5.2 CONCLUSION

The various steps involved in the design and implementation of local area network together with the site and cabling layout have so far been highlighted in this report.

The major hardware components utilized in the design of the network are network interface card (NIC), which combines with the compatible software and cables to produce the network.

The proper configuration of the proper and logical operation of the systems was employed. The compatibility of the components with the software was employed, which enable easy installation and configuration of the systems.

The network was carried out in order to provide easy way of implementing it.

## REFERENCES

1. Ed Tittel and David Johnson, Guide to networking Essentials, second edition, Kristen Duert, Canada, 2001, pp. 80-130.
2. John Wiley and Sons Inc, Computer mediated Communication, 1991, pp.32
3. AT and T. Star LAN, Network Technical Reference Manual Publication, 1986, pp.2200-2208.
4. James Chellis, MSCE Networking Essential Study Guide, Second Edition, 2004.
5. John Wiley and Sons Inc. The New technology of financial Management, pp.47
6. Charles J. Brooks and Marcraft International Corporation, A+ Certification Guide, 2004
7. Basic Reference Model, International Organization Standardization ISO 7494, 1984
8. [HTTP// WWW.LAN\\_TUTOR.COM](http://www.lan-tutor.com) -CIS Exploring Access Method
9. [HTTP//WWW.LAN-TUTOR.COM](http://www.lan-tutor.com) -CIS Exploring Network Topologies
10. [HTTP//WWW.BEST\\_TUTORIALS.COM](http://www.best-tutorials.com)