STRUCTURAL CABLING AND SYSTEM INTEGRATION OF ELECTRICAL LAB.

BY

SANGODERE MATTHEW OLUWAFEMI

97/6161EE

A PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF ENGINEERING DEGREE (B. ENG) IN THE DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING,
SCHOOL OF ENGINEERING AND ENGINEERING TECHNOLOGY, FEDERAL UNIVERSITY OF TECHNOLOGY MINNA,
NIGER STATE.

SEPTEMBER 2003.

CERTIFICATION

THIS IS TO CERTIFY THAT THIS PROJECT HAS BEEN EXAMINED AND APPROVED HAVING MET THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF ENGINEERING (B.ENG) DEGREE IN ELECTRICAL AND COMPUTER ENGINEERING DEPARTMENT, FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA NIGER STATE.

....

DR. Y. A. ADEDIRAN
PROJECT SUPERVISOR

DATE

..... 7/4/09

ENGR. NWOHU
Ag. HOD ELECT/COMP. ENGR.

DATE

....

EXTERNAL EXAMINAL

DATE

DECLARATION

I HEREBY DECLARE THAT THIS PROJECT WAS AS A RESULT OF PERSONAL EFFORTS AND EXPERIENCE UNDER THE SUPERVISION OF DR. Y. A. ADEDIRAN, ELECTRICAL AND COMPUTER ENGINEERING DEPARTMENT, FEDERAL UNIVERSITY OF TECHNOLOGY MINNA, DURING THE 2001/2002 ACADEMIC SESSION.

SANGODERE MATTHEW OLUWAFEMI

16/07/03

DATE

DEDICATION

This Project is dedicated to the **ALMIGHTY GOD** my Creator and Saviour whose role in my life is ***Indispensable*** and ***Totally without Substitute*** in all aspect.

GOD TO YOU BE ALL GLORY HONOUR AND PRAISES.

I also dedicate this to the memory of my late father **Mr. MOSES ADEBAYO SANGODERE** for his will to give me the best of education. And it is this will and the grace of God that keeps the family going.

ACKNOWLEDGEMENT

The success of a man is not strictly as a result of self-effort but of the help of God and those who care. Therefore, I am most grateful to the ALMIGHTY GOD for the protection, provision and guidance throughout the period of my studies in Fut. Minna.

All human beings have only acted in the capacity of mere instruments or vessels as God directed them. Therefore, with all joy, I deemed it fit and good to thank all the people who allowed them to be used by God for the success of my program.

The help of my parents Mr. and Mrs. SANGODERE is therefore gratefully acknowledge, especially my wonderful and caring mother, for her untiring care, love, support and consistent prayers.

I cannot but be grateful to my project supervisor ASSO. PROF. ADEDIRAN YINUSA, the HOD of Electrical and Computer Department, FUT, Minna. Who also doubied as my project Supervisor for the great role he played to make this project a success, for his support during this training.

It will be crime against humanity not to sincerely and wholeheartedly appreciate the good effort of a my brother EBENEZER SANGODERE and sisters, BOSE, TEMITOPE AND ADETOUN for their assistance, help, love and understanding. Of a truth, blood is thicker than water.

To the following, I say a big thank you for their love and moral support; MR. AND MRS. KOLA OLAGUNJU, TUNDE RICHARDS, SEGUN OJO, STEPHEN, GBOLAHAN SALISU, Mr. And Mrs. BABATUNDE SALISU, MR. AJIBADE, all staffers of Datasoft Computers Ltd, Others are MR. AND MRS. OGUNMEKAN, MR. AND MRS. MOSADOMI, MR NIYI OLAGUNJU, GBENGA ALOBALORUN and the ADEPOJUS.

My specially appreciation goes to **TEMITOPE BENJAMIN**, and All members of C&S CHURCH MOVEMENT, MINNA.

My profound thanks go to AMOO TOSIN HAFIZ my project partner, thanks for understanding and cooperation. To the following I say thanks for always being there, C&S unification, ADE AJIBOLA JOHNSON, RAFIU, TUNDE, IDRISU (NFA Chairman), BIMBO AYODELE.

My acknowledgement is not complete if I fail to appreciate the. I am also greatly indebted to MR. JOSHUA NWABINELI the HOD ENGINEERING DEPT. COSTECH LTD IKJ. Who has wonderfully affected my life with the level of training impacted in me.

To many more who I have not mentioned I am indeed very grateful.

"The Horse may be ready for the day of battle but victory rest with the Lord"

Thank you ALMIGHTY GOD for directing my path and seeing me through these years.

ABSTRACT

Modern living would have been a mere dream without an efficient and easy communication system. Because of the relevance of information dissemination in modern society, communication system and information technology become imperative.

Networking has gone from being an experimental technology to become a key business tool used by companies and individuals worldwide.

This project is aimed at interconnecting the systems in the Electrical and Computer Engineering Department for easy sharing of files, resources and folders.

TABLE OF CONTENT

CHAPTER ONE

INTRODUCTION AND LITERATURE REVIEW

1.1 INTRODUCTION

A Computer network is a collection of hardware and software that enables a group of computers to communicate and provide users with the access to shared resources. These shared resources can include data, such as files or messages; applications and other software; and hardware, such as printers or modems. This ability to share resources is one of the primary reasons why organizations implement networks.

At the most basic level, a computer network consists of at least two computers connected by a communication link, such as a physical cable.

Typically, one of the computers acts as a server, making its hardware and software resources available for use by other computers on the network. A computer that uses the resources of *server* is called a *client.*

1.1.1 TYPES OF NETWORK.

Networks come in many shapes and sizes. However, in most cases one can categorize them based on their geographical reach. One will likely see four terms describing the general size of networks. Local Area Network (LAN), which is our primary area of discussion, Metropolitan Area Network (MAN), campus area network(CAN), and Wide Area Network (WAN).

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 workgroup, department or a single floor a multistory building, several LANs can also be interconnected within a building or campus of buildings to extend connectivity.

1.1.2 BASICS OF LOCAL AREA NETWORK.

Today Local Area Networking is a shared access technology. This means that all of the devices attached to the LAN share a single communication medium, usually a Coaxial, Twisted Pair, and or Fiber Optic Cable. The physical connection to the network is made by putting a Network Interface Card (NIC) inside the computer and connecting it to the network cable. The physical connection is in place, it is up to the network software to manage communications between stations on the network.

1.1.3 LAN NETWORKING MODELS

Computers can be connected by following one of two models; Peer-To-Peer and Server-Based. A third possibility is simply a combination of those two models.

In a Peer-To-Peer Network, each workstation acts as both a server and a client by sharing its resources with other computers and accessing others shared resources.

In a server-based network, dedicated servers share resources. In this model, dedicated servers function only as server - they are not used as clients. Typically, dedicated servers are optimized to quickly process requests from clients; they also ensure the security of data.

Many businesses combine the server-based and peer-to-peer network types to create a combination network. In these types of environment, dedicated servers and workstations co-exist with computers that function as both server and client. This structure can be advantageous when an area or business unit needs to share data or resources, but cannot afford the costs associated with implementing a dedicated server.

1.2 LITERATURE REVIEW

Computer networking is the act of linking a group of computers with the aim of making them communicate with each other and share available resources among themselves. However, computer networking came into existence from system engineer`s bid to improve communication standard of a computer.

In the mid 1960`s the most commonly reported experiment was conducted by Marill and Roberts (1966), which later formed the basis of computer networks. In their work, they connected TX – 2 computers at Lincoln Laboratories and q – 32 computers at the system Development Corporation such that the user of one computer could access the others.

Subsequent advancement led to the establishment of a WAN – Wide Area Network, by USA defense department in the late 1960's. The WAN was named **Advanced Research Projects Agency Network** (ARPANET), which is a network of military sites situated in the US and Mexico. Later the network went into connecting Universities and Research Organizations in the US, UK, Mexico and Norway.

In 1983, ARPANET was divided into two. ARPANET carries out civil tasks and researches while MILNET carries out military tasks. With both networks, interconnected LANs later joined with others like BITNET, CSNET this forming INTERNET- coined from **International Networks**. Recently, however, the internet has emerged as the largest WAN in the world.

New techniques were also established, such as network topologies namely BUS, STAR, RING, MESH topologies, bridges, repeaters, routers, protocols, packet switching etc.

Packet switching is a form communication that works on the principle of splitting data into small units called packets before transmitting and later re-assembles them at the destination.

Much effort has been made in exploiting the interconnectivity of computers, but due to problems arising from different manufacturing companies and different communication conventions, the Open System Interconnection (OSI) model was developed by the International Organization for Standardization (ISO), which provides a means of describing the data flow in a network and how it could be generally managed.

The aim of this project is design, analysis and implementation of a LAN using a client- server model and implementation carried out with Star Topology architecture.

1.3 SCOPE OF THE PROJECT

1.3.0 PROJECT DISCUSSION

The design and implementation of a Local Area Network (LAN) using a client – server model and implementation done with the Star Topology architecture. The network design covers the Electrical and Computer Engineering Department of Federal University of Technology, Minna.
The functionality of the Computers in the Electrical Laboratory is also of paramount importance to the success of the Network implementation. Therefore the computers were upgraded and made functional.

1.3.1 OBJECTIVE OF COMPUTER NETWORKS

Computer networks satisfy a broad range of purposes and meet various requirements. Some of the common objectives set to be achieved by the design of this computer network are mentioned below.

1. To enable and encourage the sharing of resources amongst users.
2. To establish a communication link between computers located at various places using a star topology.
3. To provide an efficient means of transporting large volumes of data among remote locations.
4. Most importantly, to allow for interpersonal communication by programs such as Netmeeting, chatting, Electronic mail (E-Mail) and bulletin boards. In addition, to permit users to share information by accessing a file that is stored on the file server within the Intranet.
5. To enable users share application software. This offers a cost advantage and makes supporting and maintaining the software much easier. When the school or department adopts a new version of software, it consumes less time updating on a centrally shared hard disk than updating on each stand-alone personal computer.
6. To provide compatibility of dissimilar equipment and software. Hence, there is a growing trend towards compatibility through standardization, for all types of communication hardware and software.
7. To provide network users with maximum performance at minimum cost.
8. To provide centralized management and allocation of network resources such as host processors associated databases, transmission devices and the files.

1.4 NETWORK ARCHITECTURES

Network Architecture is the combination of standards, topologies and protocols that create a working network. Four of the major architectures are the Ethernet, Token Ring, Apple Talk and ARCnet.

Ethernet is the most widely used LAN technology. It strikes a good balance between speed, price, ease of installation, and supportability. Approximately 80 percent of all LAN connections installed use Ethernet, for the Basis of this project, the Ethernet architecture will be preferred and used.

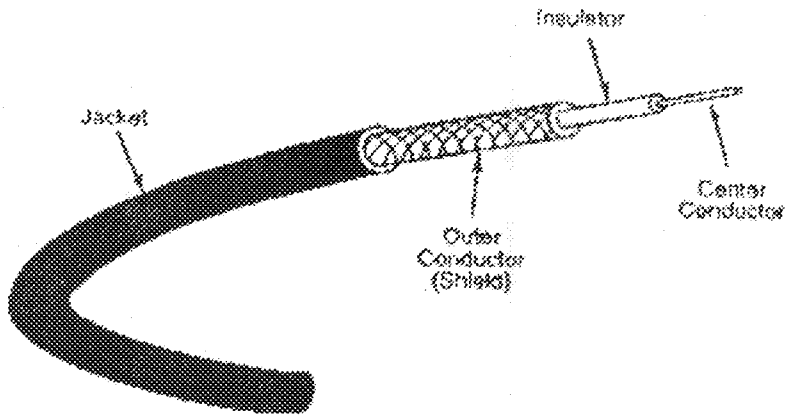
The Institution of Electrical and Electronic Engineers (IEEE) define the Ethernet standard in a specification commonly known as IEEE 802.3. The 802.3 specification covers rules for configuring Ethernet LANs, the types of media that can be used and how the elements of the network should interact. The Ethernet protocol provides the services called for in the physical and data link layers of the 802.3 (or 802.3u) specification states that the Ethernet networks run at a data rate of 10 million bits per second (10 Mbps) or 100 million bits 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.
The access method to be used by the stations connected to an Ethernet LAN is called CARRIER SENSE MULTIPLE ACCESS with COLLISION DETECTION (CSMA/CD).

In this method, each station contends for access to shared medium. It is possible for two stations to try sending packets at the same time, which results in 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.

1.4.1 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 the three diffe nt media.

Figure 1.1 A Coaxial Cable



Coaxial cable was the original LAN medium and it is used in what is called a BUS Topology. In this configuration, the coaxial cable forms 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 in Bus LAN unless it is very small.

1.4.2 A BASIC BUS TOPOLOGY LAN

The Bus topology is often used when a network installation is small, simple or temporary. On a typical bus network, the cable is just one or more wires with no active electronics in form of hub to amplify the signal or pass it along from computer to another computer. It is basically a passive topology. When ever message(s) is/are sent, all the computers receives it but only the one that has the encoded address accepts the message or information, the rest neglect or discard the message(s).

Only one computer can send a message at a time, when a number of computers are connected, it can affect the speed of the network; hence, one must wait until traffic is free before it can send.

Since electrical signals (messages) are sent throughout the length of the entire cable, it is necessary to terminate the ends of the cables to avoid a phenomenon none known as **RINGING**. It occurs when signal gets

to the ends of the cable and bounces back through out the length of the cable in a continuous process. The terminator must have a resistance value equal to the resistance value of the cable used. It is of paramount importance that a bus topology be terminated to avoid continuous reflection of signals.

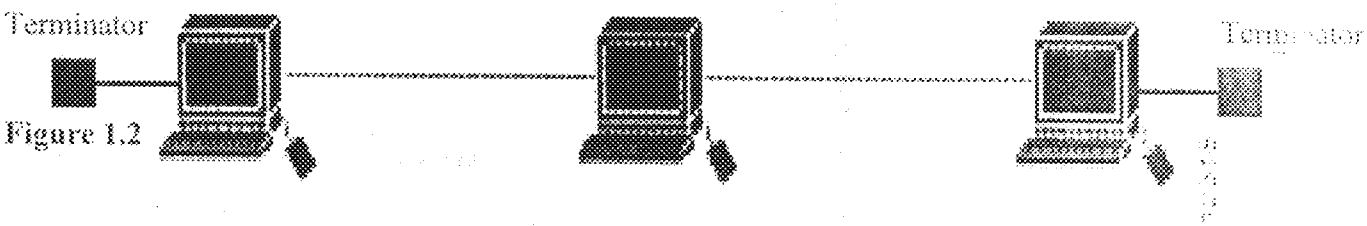


Figure 1.2

ADVANTAGES AND DISADVANTAGES

- The bus is simple, reliable in very small networks easy to use and understand but limit ones network.
- Least amount of cable is required but cable breaks can disable the network.
- A repeater can be used easily to enhance the connectivity of the network because it boost signal and allows it to travel longer distance.
- Heavy networks can slow a bus considerably.
- Interference and conflict is prevalent here.
- Troubleshooting is extremely difficult with bus.

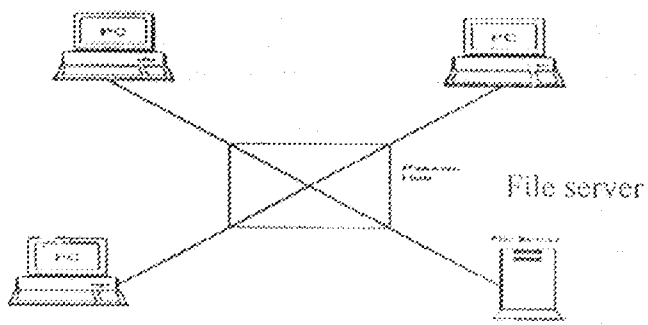
1.4.3 A BASIC STAR TOPOLOGY LAN

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 parts 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 of figure 1.3 illustrates a Star Topology LAN, - which is more robust topology than the Bus topology. In a Star topology, each station connected to a central wiring concentrator or hub, by an individual length of twisted pair cable.

The cable is connected to the station NIC (Network Interface Card) at one end to a port on the hub at the other. The hubs are placed in wiring closets centrally located in a building.

Figure 1.3



1.4.4 CABLES OR MEDIA IN ETHERNET

thernet networks can be built using three different types of media: ***shielded and unshielded twisted pair, oaxial and fiber optic cable.*** By far the most common is the twisted pair because it is associated with the ore popular star topology. It is inexpensive, and very easy to install, troubleshoot and repair.

Twisted pair cable comes both Unshielded Twisted Pair (UTP) cable used for LAN is similar to telephone able but has somewhat more stringent specifications regarding its susceptibility to outside electromagnetic nterference (EMI) than common telephone wire.

hielded Twisted Pair (STP) as its name implies comes with a shielding around cable to provide more rotection against EMI. Of the two types of twisted pair cable, UTP is by far the most commonly used. The pecification for the running Ethernet on UTP is called 10 Base T. This stands for 10 Mbps, Base band ignaling method used by Ethernet networks) over twisted pair cable. Other Ethernet cable specifications shall e explained in details in the subsequent chapters.

tar topology provides architectural flexibility and allows use of several types of cable to implement a etwork. Expansion can be effected in a star network by placing another star hub where a computer might otherwise be called "SACKING THE NETWORK" thus this allows several more computers or hubs to be onnected.

DVANTAGES AND DISADVANTAGES.

- It is easy to modify and add new computers to a star network without disturbing the entire network, though larger network tend to affect speed of data transmission.
- Easy diagnosis of network fault, intelligent Hubs tend to act as repeater it tries to make the signal receive ok before retransmitting
- Centralized monitoring and management of network.
- Allows different cables to the hub, failure of hub leads to failure of network.
- Simple computer breakdown does not disable the whole network, and allows for easy expansion.
- Hubs could be expensive though important.

1.4.5 RING TOPOLOGY LAN

Ring almost the same as the bus but with little modification. The cables are made to form a closed loop; the underlying term here is *CLOSED LOOP.*

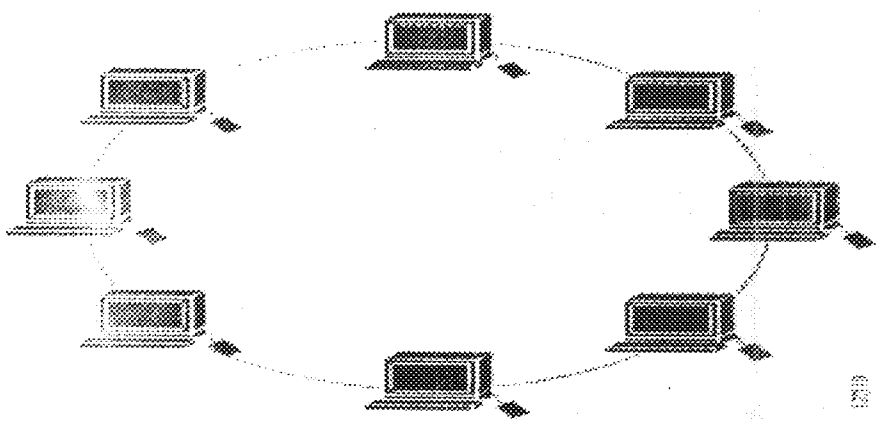


Figure 1.4 Bus Connection

Here each computer is a repeater, each configured to act as a repeater. The repeater works by accepting the signal and rebroadcast it to other computers on the network. This is done to avoid attenuation i.e. lost of signals.

Different types of NIC will be used, not as in bus topology; this is because NIC need be configured to route i.e. to repeat signals.

Another thing that is of importance in ring is the use of Token. Tokens are authorization packet that allows a computer to accept and transmit signals received. Token allows the transmission of messages in a Ring topology.

ADVANTAGES AND DISADVANTAGES

- Each node is consequently a repeater and as such duplicates data signal resulting in very little or no degradation of signals or attenuation.
- Equal access to the network by all systems, though failure of one system on the network renders the network dead and invalid.
- Capacity is hardly exceeded though may be slower with more systems.
- Addition or removal of systems disrupts normal operation of network.
- Difficulty in troubleshooting and tends to be expensive hence the use of repeater NIC.

1.4.6 MESH TOPOLOGY LAN

Mesh Topology LAN is generally divided into two types.

a. Fully connected network where all systems are connected to one another.
b. Randomly connected network, all the systems does not necessarily connect together but most of the systems are connected haphazardly to one another.

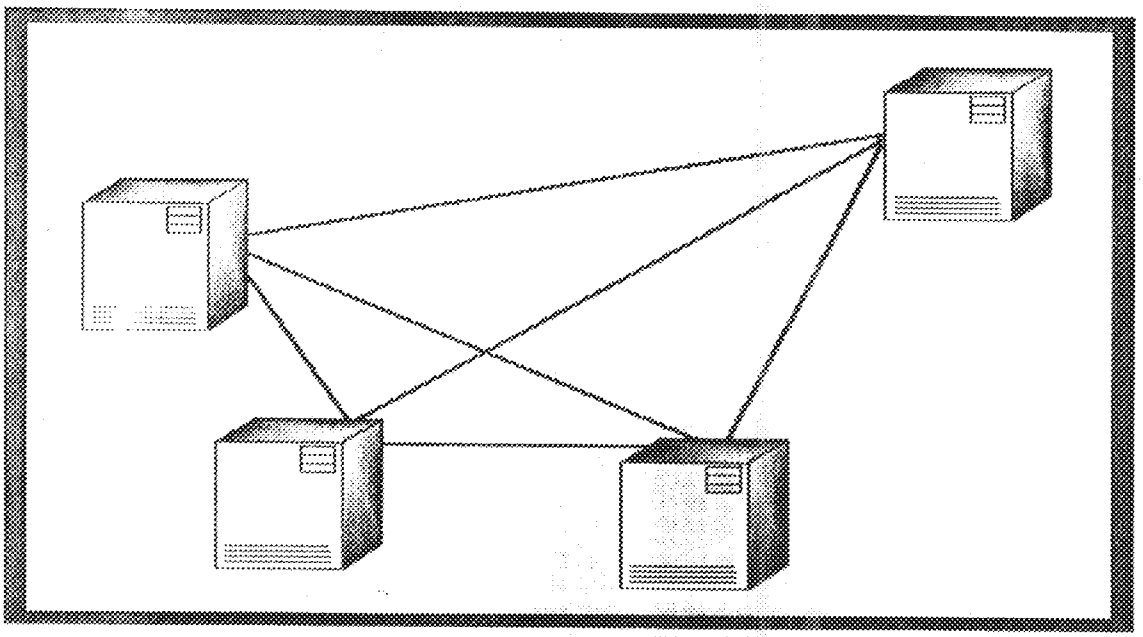


Figure 1.5 A Mesh Connection

A mesh configuration consist of a network in which each device has a point to point connection to every other devices on the network. The complexity and cost make this configuration impracticable for networks; also, much of the bandwidth available in mesh configurations is wasted. Number of cable used here can be designated by the formula

$$\text{Equation} = \frac{n\,(n+1)}{2}$$

n is number of nodes, when n = 4; the no. of cables equal 10. It is not practicable for large networks.

ADVANTAGES AND DISADVANTAGES OF MESH TOPOLOGY LAN

- Troubleshooting is easy; isolation of network failure is easy.
- Fault tolerance is maximized by rerouting traffic around failed link.
- It is difficult to install, configuration and reconfigurations tends to be increasingly difficult.
- It is expensive because of redundant connections and wasted bandwidth.

CHAPTER TWO

2.1 DATA TRANSMISSION

There are three processes or means in which network resources are shared and transmitted.

- Client: These computers use network resources but do not provide other resources.
- Peer: These are computers that use and provide network resources.
- Services: These are computers, which only provide network resources.

The type of Operating System the computer uses determines each of these computer roles. Servers run network operating systems such as Windows NT Server, Novell Netware e.t.c Clients run Client Operating systems, such as MS-DOS, OS/2, Windows 9X e.t.c. Peers run Peer Network Operating Systems such as windows 9X, Macintosh
Operating system.

Each of this operating system is optimized to provide services for the role it plays. Based on these roles the computers on network are divided into three environment types.

2.1.1 Peer-To-Peer Network Architecture- It works with machine or computers of compatible length without server. It uses the network to share resources among independent peers. It is easy to install and use where no ambition for expansion is paramount.

Advantages of Peer Network

- No extra investment in server hardware or software is required.
- Easy to install or setup.
- Lower cost for small network.
- No reliance on other computers for their operation.
- Ability of users to control resources sharing.
- Extra cost of server hardware or software is eliminated.

Disadvantages of Peer Networks

- Added responsibility on individual computers.
- Lack of central organization, which can lead to data mismanagement
- No central point of storage, for file archiving.
- Each computer must posses all hardware requirements.
- Weak and intrusive security.

2.1.2 Client – Server Network Architecture: - This network is usually called multi-user network, it comes in effect when a network needs to be enlarge. It consists of a computer (called server) to which all other computers (client or workstations) are connected.

The server provides security and administration of the network. It is usually more powerful than the clients in terms of speed, memory and the hard disk capacity.

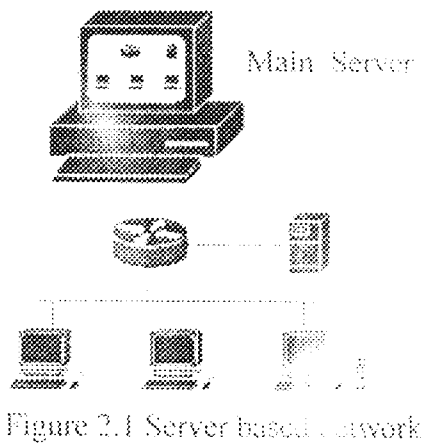


Figure 2.1 Server based network

Advantages of Server-Based Network

- Strong central organization and security.
- Provide access to and from central files/data storage.
- Less intrusive security and faster network.
- Easy manageability of a large number of users and of backup files.
- Ability to share expensive equipment such as printer, modem e.t.c
- Ability of serers to pool available hardwae and software lowering the overall costs.

Disadvantages of Server-Based Networks.

- Expensive network operating system software required.
- Dedicated hardware required.
- A dedicated network administrator is usually required.

2.1.3 Hybrid Networks:-Hybrid networks have all three types of computers on it and generally have active domains and workgroups. This means that while most shared resources are located on server network users still have access to any resources being shared by peers in the workgroup.

The network users do not have to log on to the domain controller of server to access workgroup resources being shared by peers.

Advantages of Hybrid Computing

- Combines the advantages of server-based and peer networking.
- Ability of users and network administrators to control security based on the importance of the shared resources

Disadvantages of Hybrid Computing

- Disadvantages of server based networking.

2.2 DATA TRANSMISSION MODES

This is the way i.e. direction in which computers or communication devices sends information.
Three basic modes are identified.

1. **SIMPLEX MODE**: Data can flow only in one direction alone. It uses a two-wire facility such as telephone cable.

2. **HALF-DUPLEX MODE**: Data can flow in either direction but not as the same time, here, data are sent or received based on time and access. In this transmission mode, we have *Transmit And Receive Mode* when it sends, it is called a transit mode and the time taken or time at which a transmit mode turn to a receive mode and vise versa is termed **TURN AROUND TIME** (TRT)

   A four-wire facility of the half-duplex mode does not need modem turn around time for the four-wire half-duplex mode. In this process, two wires are used to send and two are used to receive and it can be at the same time.

3. **FULL DUPLEX MODE**: Maximum utility of the modem is achieved here it can send and receive all at the same time in an easy and efficient means. It works with the four wire facility and it is also possible to use the two (2) wire facility but four wire facility is the Standard.

   It works by means of frequency distribution by use of two frequency range bandwidth one can use the two (2) wire facility but they work best on aliasing effects when appropriate signal is allocated and there is no interference.

2.3 NETWORK DESIGN

This focuses on protocol (command) on which network functions. It further reveals the network architectures and components for LAN expansion.

Protocols define a common method of communication between computers. Generally, a network protocol defines how communication should begin and end properly, and the sequence of events that should occur during data transmission.

At the computer transmitting data (source computer), the protocol defines how data is broken down into packets. Packets are small division of the data.

2.3.1 Protocol Suites

A set of protocol that are typically used together is called a protocol suite. Many network operating system vendors such as Microsoft and Novell, provide their own protocol suites, but enable you to use other protocol as well. The Microsoft Windows NT provides the NetBEUI (Network Bios Extended User Interface), IPX/SPX, and TCP/IP protocol suites with the Network Operating System software. Some Networks enable you to run multiple protocol suites others support only one.

2.3.2 Transmission Control Protocol/ Internet Protocol:

This is the most widely used protocol on the internet. This protocol was originally Developed by the Department of Defense of the U.S.A. primarily to connect dissimilar networks or computers on different platforms in different military installations. But it was later developed for civilian use and has since become an industry standard. Other reasons for its popularity are:

i) It is the most widely used protocol and is supported by almost all network operating systems. It is the required protocol for internet access.

ii) TCP/IP is scalable for use in small and large networks. TCP/IP provides routing services.

iii) TCP/IP is designed to be fault tolerant and is able to dynamically reroute packets if networks links become unavailable (assuming alternate path exists).

iv) Protocol companions like Dynamic Host Configuration Protocol(DHCP) and Domain Name Systems (DNS) offer advanced functionality.

2.2.3 Configuring TCP/IP:

TCP/IP requires an IP address and a subnet mask. There are other optional parameters such as DNS and WINS settings which are discussed later in this chapter. Depending on the network setup TCP/IP configuration is done either manually or dynamically.

IP Address:

The IP address uniquely identifies a specific computer on the network. The IP address is four fields,32-bit address, separated by periods. Parts of the address are used to identify the network address and the other part of the address is used to identify the host (or local) computer address.

Depending on the size and configuration of the unique, the IP address format must be suitable for the desired network. There are three main types of IP address formats (IP class assignments).

IP CLASS ASSIGNMENT

Network Class	Address Range of First Field	Number of Networks Available	Number of Nodes Supported	Default Subnet Mask
A	1-126	126	16,777,214	255.0.0.0
B	128-191	16,384	65,534	255.255.0.0
C	192-223	2,097,152	254	255.255.255.0

Subnet Mask: The subnet mask is used to specify which part of the IP address is the network address and which part of the address is the host address. By default the following subnet mask are applied;

Class A 255.0.0.0

Class B 255.255.0.0

Class C 255.255.255.0

By using 255, i.e an octet is used to identify the network address. For example in the class A IP address of 10.0.0.1 the default subnet mask is 255.0.0.0,it means that 10.0.0.0 is the network address and 0.0.0.1 is the host address.

Class A

Class B

Class C

Domain Name System (DNS): This is the TCP/IP network service that translates fully qualified domain names into IP addresses.

Dynamic Host Configuration Protocol: This is a TCP/IP network service that automatically assigns IP addresses to client computer on a network.

Windows Internet Naming Service: This is another TCP/IP network service that is used to resolve NetBIOS names into IP addresses.

2.4 NETWORK ARCHITECTURES.

Network architecture is the combination of standards, topologies and protocols that create a working network, four of the major architectures are - Ethernet, token Ring, Apple Talk and ARCnet.

For the purpose of this design, Ethernet architecture will be used. It is the most commonly used networking scheme. Xerox Corporations originally developed it in the 1970s. Ethernet offers an economical price respectable bandwidth, and compatibility with other network products.

The Ethernet specification was extended and formalized by the institute of Electrical and Electronics Engineers (IEEE) in the 802.3 specification. IEEE 802.3 includes modifications to classic Ethernet data packet structure among other minor changes. Although IEEE 802.3 is not the same as Ethernet, it is often called **Ethernet instead of IEEE 802.3.**

Some of the basis for the Ethernet and Cabling standards are

- 10Base2 (called thinnet or cheapernet)
- 10BaseT (802,3 over twisted pair-cabling)
- 10Base5 (thicknet)
- 100BaseT (the megabit form of 802.3; runs over twisted pair of fiber Optic).
- 100BaseVG (special form of 802.3; runs over twisted pair)
- 1Base5 (starLAN)
- 10Broad36 (a Broad band form of 802.3)

The names of the configurations indicate three characteristics about them:

- The data rate measured in megabits per second, is indicated by the first number in the configuration name. for example, the 10 in 10Base2 indicates that the rate is 10Mbps.
- The type of signaling, either broadband or baseband is indicated in the middle portion of the name. for example, the Base in 10Base2 indicates the type of signaling is baseband.
- The maximum segment length, rounded to the nearest 100 meters, is indicated by the last number in the name for example, the 2 in 10base2 indicates the maximum segment length is 200 meters (actually, the maximum segment length of 10Base2 is 185 meters, which rounded up the "200").
- T indicates that the configuration uses twisted pair cable.

2.5 INTERNETWORKING DEVICES.

These are devices that are used to interconnect systems for efficiency and better usage. They include Hub, Repeater, Bridge, Router, Brouter, Gateway and Switches.

Hubs: used to connect systems these are the active and the passive hub based on the effect of transmission on the data.

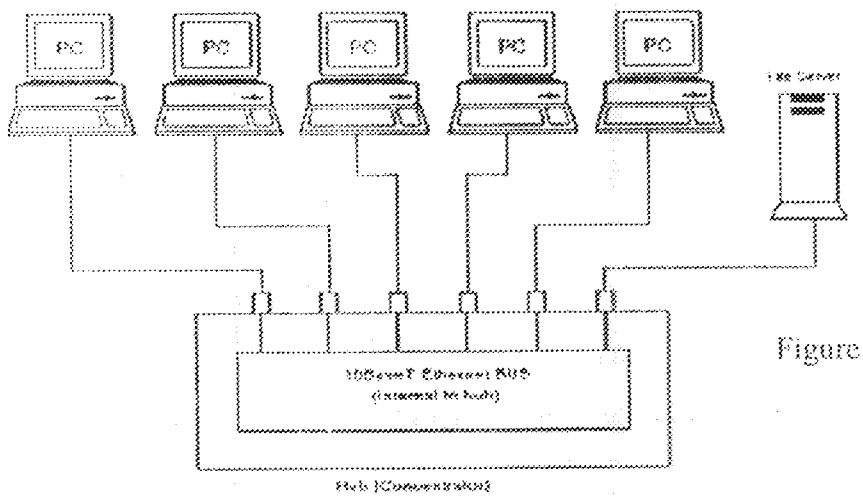


Figure 2.1 Hub Connection

Repeater: - Simplex internetworking device, it can only connect two LANs together and they must be similar. It can connect only two similar networks. It takes messages, amplify it and send it to the next LAN. At the OSI-RM it connects only at the Physical Layer.

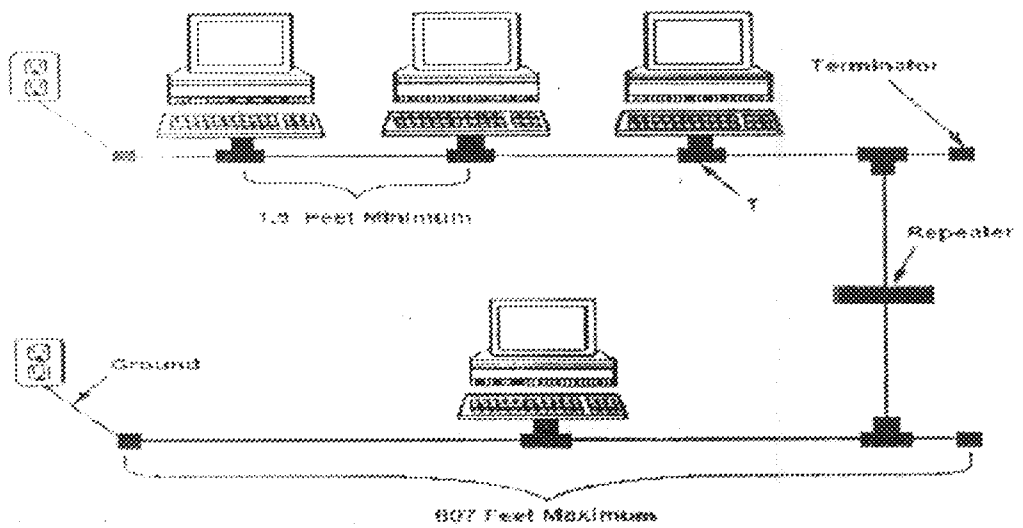


Figure 2.2 A repeater Network

Bridge: it can connect only two networks, i.e. LANs but here they can be dissimilar and it interconnects at the data link layer. Bridges works with Data format conversion, the bridge also do the error correction. It cannot amplify signal to a very high level.

Router: most intelligent internetworking device. It is of high efficiency, they may be computers configured to work as a router. They have their own processor, RAM, Random Access Memory, and ROM Read Only Memory. Etc. it connects at the Network layer and can connect as many network as possible. It has non-volatile ROM. It works with IOS (Internetworking Operating System). It is this Operating System that actually controls the system. It is a CISCO Trademark.

Gateway: it interconnects at any of the four upper layer of the OSI; transport, session, physical and application. It is an automatic device, you don't tell it to do it, it just do all it knows it ought to do. It does all the functions of a router and others.

Switches (ATM) Asyuchronous Transfer Mode. Most switches are now working with ATM. Switches are used to segment LAN such as to reduce congestion. They localize the flow of information and avoid or prevent interference basically used for LAN segmentation.

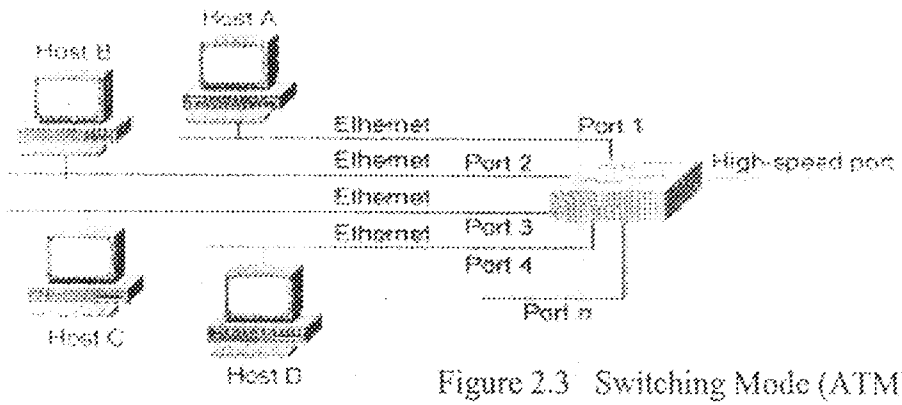


Figure 2.3 Switching Mode (ATM)

2.6 NETWORKING OPERATING SYSTEM.

A network Operating System (NOS) is very similar to a regular client Operating System such as Windows or OS/2 only that it controls the basic functions of the computer in the network. Unlike regular Operating system provides network services such as files and print sharing and user account management.

As reliance of many computers on the services of a server increase, good network operating systems are implemented with features such as preemptive multi-tasking, which prevent poorly written server component software from crashing the server and strong security, and also manage the accessibility of the different resources provided by the server.

Technically, the only different between a server and a client computer is the software each runs. A complete network requires two types of network software namely

- The network Operating system, which runs on the server and allows the share of server resources such as hard disk, printers and CD-Rom.
- Client Networks access software, which runs on the client and provides access to the resources shared by the server.

CHAPTER THREE

3.0 NETWORK PROTOCOL AND STANDARDS.

Protocol is a network standard, instruction, or rules that govern communication or network procedure. In 1977, the International Organization for Standardization (ISO) approved Open System Interconnection (OSI) reference model that was adopted in 1983. The term "OPEN" denotes the ability of any two computer systems conforming to the reference model and the associated standards to connect (i.e. systems capable of interconnection by virtue of each system having implemented the common set of protocols) or better still compatibility for communication.

In order for computers to communicate, there must be accepted rules of communication. For communication to take place effectively on a network composed of a variety of network devices, these rules must be clearly defined. The OSI model is simply a conceptual framework that can be used to better understand the complex interactions taking place among the various devices on a network. It (OSI) simply defines which tasks to be done and which protocols will handle those tasks at each of the seven layers of the model, which is downward compatible.

The layers are as follows:

Level 1	Physical layer
Level 2	Data link layer
Level 3	Network layer
Level 4	Transport layer
Level 5	Session layer
Level 6	Presentation layer
Level 7	Application layer

Each layer is independently defined though they work with them selves. Brief explanations on roles each of the layer perform are as follows:

3.0.1 PHYSICAL LAYER: - This is the lowest layer of the OSI-RM and deal with the mechanical, electrical, functional and procedural means required for the transmission of data. It also deals with physical characteristics of the physical medium. Specifications under the physical layer include details such as connectors, pins, electrical currents, encoding, media types and characteristics, transmission methods and topology.

3.0.2 **DATA LINK LAYER**: - These specifications are concerned with getting data across one link or medium, and it is concerned with the type of media in question. It provides for control of the physical layer. It detects and possibly corrects errors that can occur during the transmission. The data link layer is usually concerned with signal interference on the physical transmission media.

3.0.3 **NETWORK LAYER**:- this layer is responsible for data routing in a multiple segment network, end – to – end delivery of packets. It functions are:

--- Translates addresses: - logical addresses such as machine names, that had passed down from upper layers are transmitted into physical addresses that the data link layer can use.

--- Determines best routing: - it determines the best for the data packet to ensure timely delivery.

--- Manages network traffic: - this layer manages problems like packet congestion.

3.0.4 **TRANSPORT LAYER**: - this layer ensures that data moves e.g from point A to point B, in order without errors. This layer provides

- --- Repackaging of large data blocks into smaller packets.
- --- Flow control, packets, sequencing, and sequence checking.
- --- Resynchronization with time out and retransmission.
- --- Error detection and recovery, transport connection multiplexing.

3.0.5 **SESSION LAYER**: - It allows an application to know how the transmission and reception of data are progressing. In simple terms, the session can be thought of as the TIMING and FLOW CONTROL layer.

- flow control is the process of controlling the rate at which computer sends data. Flow control is needed because any computer sends data faster than it can receive data. Methods of implementing flow control includes

1. Buffering 2. Congestion Avoidance 3. Windowing.

3.0.6 **PRESENTATION LAYER**: - The function of this layer is defining data formats. It converts the data from the application into a common format. The layer also defines protocol for Encryption of data. It also does compression / expansion of data in line with decryption.

3.0.7 **APPLICATION LAYER**: - This layer is the ultimate source and sink of data exchange. The application layer is the end-user interface. It is where the applications, such as electronic mails, database display modules etc. reside. The application layer task is to display received information and send the users new data to the lower layers.

3.1.0 NETWORK STANDARD

Standards are set of rules that allow a common point of reference for discussing network devices and concepts. Standards are required to govern the physical, electrical and procedural characteristics of a network environment and assure that there will be a large market for a particular piece of equipment of software, many network approaches exist by various vendors, each with their own idea on how network should work. Without coordination, there will be failures in the whole network, the only way to resolve this is by setting a standard.

The American institute of Electrical and Electronic Engineers (IEEE) computer society in February 1980 formed its local network standards committee termed Project 802, (after the year and month the project started).

Project 802 defines cabling and data transmission corresponding to the physical and data link layers of the OSI model. Some of the standards that relates to LANs are.

- IEEE 802.1 Internetworking
- IEEE 802.2 Logical Link Control (LLC)
- IEEE 802.3 Carrier Sense Multiple Access with Collision Detection
- IEEE 802.4 Token Bus
- IEEE 802.5 Token Ring
- IEEE 802.6 Metropolitan Area Network (MAN)
- IEEE 802.7 Broadband Technical Advisory Group
- IEEE 802.8 Fiber Optic Technical Advisory Group
- IEEE 802.9 Integrated Voice and Data in LAN
- IEEE 802.10 Standard for Interoperable LAN security
- IEEE 802.11 Wireless Networks
- IEEE 802.12 Demand priority accesses LAN.

3.2.0 NETWORK SECURITY.

Providing security means more than controlling a system to prevent theft. It means controlling the system to prevent exposure, loss, and free will access to network critical data and resources. Accidental loss, especially information systems is quite common. Users sometimes delete file to create space in their hard disks without really knowing what they have deleted. Computers can crash, sometimes losing data in the process. A file can be overwritten with a different document of the same name.

The security measures implemented in networks are designed to prevent both accidental and unintentional loss. All network operating systems require a Lon-On, so that no access to information is given without accountability or authentication. Windows 2000 Server implements resource-level security whereby individual information reserves are secured by type and list of trusted users control access to the resources called Access Control Lists. These measures are quite effective in preventing loss and they form an important part of the total networking process.

When a user or group has an access control entry in an access control list for specific resources that allows access that users has permission to use the resources. The set of access control list is called permissions; the permission is ascertained mostly by entering a password. The network administrator defines and implemented a security policy that protects critical resources without preventing users from performing their work. The balance between protection and usability changes for every organization and it is up to the network administrator to strike the appropriate balance for each individual organization.
Windows 2000 and XP operating system have one of the best network protection or security.

CHAPTER FOUR

4.0 LOCAL AREA NETWORK, DESIGN, IMPLEMENTATION AND TESTING.

4.1.0 INTRODUCTION.

Implementing of local area Network requires careful planning. The common procedure is that the designer should put into consideration the future growth of the initial Networks. Networks are always modular, once a Network is built on a solid base, an additional Network device can easily be added. In order to ensure that the LAN meets standards set by the International Standards Organization (ISO) and the Open System Interconnection (OSI) reference model the following steps were followed.

- Determination of suitable topology
- Determination of Networks cabling
- Installation of Network Interface Cards (NICs)
- Locating and configuration of server and clients operating systems.
- Implementation of security in the Network

4.1.1 LIST OF ITEMS USED. = HARDWARE COMPONENTS

The hardware components employed in the implementation of this project are listed below.

10 BaseT Ethernet hub.

RJ – 45 connectors.

Phase Plates (Wall sockets).

Category 5 UTP cable.(enhanced)

Network Adaptor Card.

Cable clips.

4.1.2 TOOLS USED

The tools used are; Crimping Tool, Set Of Screw Driver, Flushers, Cutter, Tape Rule, Saw Drilling Machine, Hammer, Chisel LAN Tester, Screwdriver, Trucking Pipes, Patch Panel. Etc.

4.2.0 NETWORK TOPOLOGY IMPLEMENTED

Considering the site of implementation i.e. the electrical laboratory, the choice of star network topology was made after careful study of the prevailing factors such as:

1. Future expansion of the network
2. Locations of the computers to be networked.
3. Number of the computers involved.
4. Distance between each computer and accessibility, etc.

4.3.0 CHOICE OF CABLE.

The first step taken in the determination of choice of cables includes, careful assessment and measurement of the site, required speed of the network, required installation properties e. t. c.

4.3.1 INSTALLATION OF UTP CABLES.

On examining the site plan (the Electrical Laboratory), a cabling layout drawing shown in figure 4.1 was produced. It shows connection of cables from the workstations and wall sockets to the hub. Unshielded Twisted Pair (UTP) cable cat 5e (e stands for enhanced) was chosen since it supports Star Network Topology.

The UTP cat 5e contains four twisted pairs of copper wire capable of data transmission of up to 100Mbps. It is connected at both ends with RJ-45 connectors using crimping tool for plugging into the hub and Network Adapter Card respectively.

4.3.2 COLOUR CODE FOR UTP CABLE CATEGORY 5.

WIRE ID	COLOUR CODE	ABBREVIATION
1.	White –Blue	W – BL
2.	Blue	BL
3.	White – Orange	W – O
4.	Orange	O
5.	White –Green	W –G
6.	Green	G
7.	White Brown	W- Br
8	Brown	Br.

The cables were installed from the hub RJ – 45 and NICs via different methods of cabling. These methods are the overhead cabling, surface cabling and truck cabling.

The Electronics Industries Association and the Telecommunications Industries Associations (EIA/TIA) 568 Commercial Building Wiring Standard defines five categories of UTP, Which are described in the table below.

CATEGORY	DESCRIPTIONS
Category 1.	Traditional UTP telephone cable, category 1 can transmit voice signals but not data e.g. Telephone cable.
Category 2.	UTP cable made up of four twisted – pair wires, certified for transmitting data up to 4Mbps (megabits per second)
Category 3.	UTP cable made up of four twisted – pair wires, each twisted three times per foot. Cat 3 is certified to transmit up to 10Mbps
Category 4.	UTP cable made up of four twisted –pair wires. Certified to transmit data up to 16Mbps
Category 5.	UTP cable made up of four twisted – pair wires, certified to transmit data up to 100Mbps

For colour coding, each colour is connected to the same pin number on the two RJ-45 for direct cabling but this is slightly different with cross-cable connection between two systems when on hub is required.

During the installation, consideration was given to cabling path such that effect of nearby source of electromagnetic interference, radio frequency sources is minimized. The maximum length UTP cable can transmit data effectively is 100 meters (328ft).

4.4.0 NETWORK OPERATING SYSTEMS USED IN THE IMPLEMENTATION.

In making a choice of network operating systems, consideration was based on the operating systems with network features. Windows 2000 server was designed with network environments in mind for a server client orientation; hence, this was used in the implementation of this project. Windows 2000 server shares a umber of common features these include.

- Hardware platform support. The designer of network has the choice of selecting the hardware platform that best suite the operational requirements. It supports x86 – based systems.
- Preemptive multi – tasking.
- Security
- Application support
- Network support
- Internet / Intranet support.
- Microsoft exchange
- Net meeting
- Dual booting allowed.

4.5.0 INSTALLATION AND CONFIGURATION OF NETWORK ADAPTER CARDS.

The Network Interface Cards (NICs) were installed by shutting down the computer and putting off the power supply, and then removing the CPU casing. The NICs were secured in the slot by tightening the screw onto metal mount of the systems chassis. The casings were closed, and the RJ-45 connector connected with the UTP cable were plugged into the adapter and the other end of the UTP cable connected to the 10BaseT hub.

After the above process, the computers were booted and the Operating Systems detected the NICs and the best driver for each one was loaded using the manufactures installation disk. After loading the driver the network neighborhood and each system was supplied with the following information:

* The computer name and description.
* The protocol for the network.
* The access control
* The Internet protocol (IP) address and sub – net mask.
* User name and password.

4.6.0 RESOURCE SHARING AND SECURITY TECHNIQUES.

To enable sharing of resources such as the hard disk, CD- Rom drives, printers, files e.t.c. sharing is of high priority. It needs to be configured or enabled for thus sharing access. The start button on the task bar of the windows environment is clicked i. e Star - Program – Administrative tool and the click is made on the resources to be shared. This enables the resources selected for sharing.

4.6.1 NETWORK SECURITY.

Security is an important part of any network, and user definitions are the first line of defense. Network security is generally identified as one of two general security models, via share level and user level the following security measures were implemented from the administrative tool.

- User manager for domains.
- User name and password
- User right policy

4.7.0 TESTS CARRIED OUT

The continuity test was employed to ensure that cables were all in perfect working condition. This test was carried out using a digital multimeter and LAN tester.

4.7.1 CONNECTIVITY AND COMMUNICATION TEST OF THE LAN.

To ensure that there is a communication link between all the computers in the network via the cables and hub, a Dos command or command prompt "Ping" followed by the IP address was applied to each of the system for connectivity.

The system for this command is as follows:

C:/.>.PING.</P address>

1) *I*f address provide logical node identifications. IDs. They are unique addresses assigned by an administrator according to certain guidelines.

They are expressed in four – part dotted .decimal notation, for example, an IP address is 132.454.67.x where x stands for numbers of nodes. It starts from 1 up to n – maximum number of computers on the network. This is done to show communication link between computers in the Local area network. This is done with two basic commands,

i) IPCONFIG: This command displays all your IP configurations.

ii) Ping: This command is used to send an Internet Control Message Protocol (ICMP) echo request and echo reply to verify if the remote computer is available. The PING command has the following syntax:

PING IP address

For example, If your IP address is 10.0.0.1, type the following command:

PING 10.0.0.1

PING is useful for verifying connectivity between two hosts. PINGing an Address successfully confirms that a valid communication path exists.

2) Communication Test: This test is usually carried out to test accessibility and sharing of hard disk, floppy drive, printers, CD-ROM etc.

CHAPTER FIVE

5.0 ANALYSIS AND DISCUSSION OF RESULTS

1.0 DISCUSSION OF RESULTS

he results of the tests carried out in the implementation of the project are discussed as follows

2.0 RESULTS FOR CONTINUITY TEST FOR THE UTP CAT 5e CABLES.

he table below shows the result of the pin-to-pin tests of the UTP cables. Beep indicates that there is ontinuity in the single conductor being tested in each case.

in-to-pin ested	Four pars of conductor in the UTP Cat 5e Cable								Meter Indication	Certified for data transmission
	W-B	B	W-O	O	W-G	G	W-BR	R		
V-B	" "								Beeped	Beeped
		" "							Beeped	Beeped
V-O			" "						Beeped	Beeped
				" "					Beeped	Beeped
V-G					" "				Beeped	Beeped
						" "			Beeped	Beeped
V-BR							" "		Beeped	Beeped
								" "	Beeped	Beeped

able 5.0 CONNECTIVITY TESTS OF UTP CABLES.

2.1 RESULTS OF COMMUNICATION TEST

fter the implementation of the network requirements, the communication test carried out showed that, the bjectives of this project were achieved within the limits of resources available in the network. Hence, the llowing results were obtained:

- The Hard disk were able to be shared within the network
- Sharing the CD ROM drive
- Sharing of application software.
- E-Mail services within the network.
- Sharing of printer.
- Sharing of files and large volumes data transfer process etc.

.3.0 ANALYSIS OF RESULTS OBTAINED.

Results shown in table 5.0, indicates that the cables are continuous, and hence fit for data transmission or receiving processes. The connectivity test results of the computers in the network shows that the systems are actually linked via the UTP cables and the active Hub used.

The destination port and response given back by the receiving computer received the Internet Control Message Protocol (ICMP) echo packets sent by any of the system to another.
The TTL in the response means time-to-leave.

The results obtained from the communication test confirm the success of the implementation in general. Though the speeds of communication were not much, the capabilities were exploited within the hardware factors like the RAM size, environmental factors and other limiting factors.

4 RECOMMENDATION.

In the course of implementing this project, some difficulties were encountered and it is of high necessity to give little ways to get them settled or solved:

The systems were not well maintained as any body just work in and begin to perform all sorts of illegal operation, which helps to grand the computers and made them difficult to revive and operate.

The financial task in carrying out projects that enhance technological advancement is very much. Moreover, it will be in the interest of the school and the Federal Government to finance wholly or in part the cost of these projects implementation. This will raise the enthusiasm of the student to put in the best and achieve greatness for the school, and the country at large.

6.4.1 AREA OF FURTHER STUDIES.

Further studies on this project should be focused on how an expansion component such as repeaters, bridges, routers, brouters and gateways enables Local Area Network (LAN) growth. The whole computers in Federal University of Technology can easily be connected for ease of information sharing and dissemination to yield what is termed Campus Area Network (CAN). To implement this, the following transmission media can be used:

- The Public Switched Telephone Network (PSTN)
- High-speed Fiber Optic Cable.
- Microwave transmission links.
- Wireless radiated media (radio Frequencies).
- Satellite Links.

6.5 SUMMARY.

This project revealed the practically of theoretical Local Area Network model, purpose of the implementing this work. The aim, scope limitation, and assumptions in the project were also outlined.

After the implementation of the network, results showed that the objectives of this project were achieved within the limits of resources available in the site layout.

REFERENCES

CHARLES PERKINS ET .AL "Networking Essentials", Ethernet Networks, Pub. Microsoft press, second edition ISBN 0-7821-1971-9, pp. 154-180

CHARLES PERKINS ET .AL "Networking Essentials", Open system interconnection (OSI) ref. model. Pub. Microsoft press, second edition ISBN 0-7821-1971-9, pp. 154-180

V. AHUJA, Design and Analysis of Computer Communication Networks, McGr -Hill, New York, 1982.

M. DURR, Networking IBM Press 2nd edition, Tech Publications, Singapore, 1987.

R. COOPER, Introduction to Queuing Theory, Macmillan, New York, 1972.

GILBERT. H (1990) "digital Networking and T-Carrier multiplexing", Network Orientation. Pub. Wiley Interscience, New York USA pp. 87-98.

VINCENT, PATRICK. Free Stuff from the World Wide Web (1995, Coriolis Grou).

WRIGHT, GARY R. & STEVENS, W. RICHARD. TCP/IP Illustrated, Volume 2: The Implementa ion (1995, Addison-Wesley).

YGGDRASIL COMPUTING. The Linux Bible: The GNU Testament, 3rd ed. (1995, Yggdrasil).

WEB LINK

http://www.infomagic.com

http://www.frontiertech.com

http://www.spry.com

http://www.netmanage.com