

DESIGN AND IMPLEMENTATION OF COMPUTER NETWORKING

(LOCAL AREA NETWORK)

(A CASE STUDY OF MATH/COMPUTER SCIENCE DEPARTMENT FUT MINNA)

BY

ISELEWA VICTOR OLAREWAJU

PGD/MCS/2007/1222

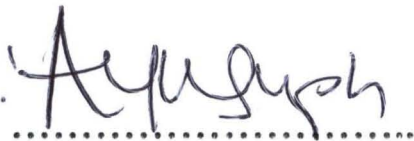
**A PROJECT SUBMITTED TO THE DEPARTMENT OF
MATHEMATICS/COMPUTER SCIENCE,
SCHOOL OF SCIENCE AND SCIENCE EDUCATION,
FEDERAL UNIVERSITY OF TECHNOLOGY,
MINNA, NIGER STATE**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE
AWARD OF POST GRADUATE DIPLOMA (PGD)
IN COMPUTER SCIENCE**

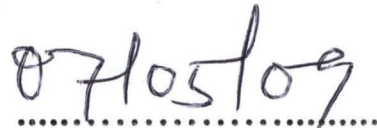
APRIL 2009

CERTIFICATION

This is to certify that this project work “**Design and implementation of Computer Networking (Local Area Network)**” (a case study of Mathematics/Computer Science Department, Federal University of Technology, Minna, Niger State) was carried out by **Iselewa Victor Olarewaju** with Registration Number **PGD/MCS/2007/1222** in the Department of Mathematics/Computer Science, School of Science and Science Education, Federal University of Technology, Minna, Niger State.



.....
Dr. Y.A. Yahaya
Project Supervisor



.....
Date

.....
Dr. N.I. Akinwande
Head of Department

.....
Date

.....
External Examiner

.....
Date

DEDICATION

This Project work is dedicated to the Almighty God, the I AM that I AM, the ruler of the universe, the custodian of great wisdom and the giver of knowledge, who has filled my heart with joy and mouth with praise. To HIM who stoops down to make me great and loves me above all else. I say be thy glory, honor, power, and praises.

Also to my parent Mr. P.F. Iselewa and Mrs. M.T. Iselewa, thanks for given me an inexhaustible gift (education).

ACKNOWLEDGEMENT

To God be the glory, great things He has done. I shall again praise Him, my helper and my lord for sparing my life up to this moment.

Naturally, a work can not be successfully accomplished without the assistance/support of others. Therefore, I wish to express my sincere gratitude to all those that made me what I am today.

I acknowledge the efforts of my honorable and ever dynamic supervisor, Dr. Y.A. Yahaya for his guidance, patience and assistance through the period of this project. I also thank the Head of Department and his co-lecturer.

My up most appreciation goes to my parents, Hon. P.F. Iselewa and Mrs. M.T. Iselewa, for given me immeasurable gift of life “education” and for their support, care, love, prayer and advice.

My profound gratitude goes to my friends, Mr. Fidelis Ogbonna, David Omagu and others. Thanks for always being there for me.

I am equally grateful for the support of my uncle and cousin Nathaniel Obafemi. I pray the good God will reward you abundantly.

My sincere thanks go to my loving brother, Olatunji A. Iselewa, late Abolarinwa T. Iselewa (R.I.P) and my sister, Funmilayo Peace Iselewa. The Iselewa, I love you all.

Victor.

ABSTRACT

Globally, most business ideas and operations are facilitated by uninterrupted flow of information. Businesses have grown to the extent of using the latest up-to-date information available and shared between computers facilities inform of electronic information transfer. This project work is concerned with the design and implementation of computer networking (Local Area Network), to share information, pass data, and transfer, for the improvement on the service of system infrastructure in the computer laboratory, Department of Math/Computer Science, Federal University of Technology, Minna. In order to produce high throughput.

TABLE OF CONTENTS

<u>CONTENTS</u>	<u>PAGES</u>
COVER PAGE	
TITLE PAGE	i
CERTIFICATION.....	ii
DEDICATION.....	iii
ACKNOWLEDGEMENT.....	iv
ABSTRACT	v
TABLE OF CONTENT	vi-vii
 <u>CHAPTER ONE</u>	
1.0 INTRODUCTION.....	1
1.1 An Overview of the Study	1
1.2 Statement of Problem	2
1.3 Aims and Objectives of the Proposed System.....	2 - 3
1.4 Scope and Limitations.....	3 - 4
1.5 Definition of Terms	4 - 6
 <u>CHAPTER TWO</u>	
2.0 LITERATURE REVIEW.....	7 - 9
2.1 The Computer Network System.....	9
2.2 Network Component.....	10
2.3 Network Model.....	10 - 13
2.4 Classification of Network.....	13 - 16

2.5	Networking Operating System (N.O.S)	17 - 22
2.6	Open System Interconnection (O.S.I)	
	Reference Model.....	22 - 26
2.7	Network (Transmission) Media.....	27 - 47
2.8	Network Topologies.....	48 - 53
2.9	Network Protocol.....	54 - 55
2.10	Popular Protocol Suites.....	56 - 68
2.11	Types of Network.....	68
2.11.1	ARCNET (Attached Resources Computer).....	68 - 69
2.11.2	Ethernet.....	70 - 73
2.11.3	Token Ring.....	74 - 75
2.11.4	F.D.D.I (Fiber Distribution Data Interface).....	75 - 76

CHAPTER THREE

3.0	NETWORK DESIGN AND CONFIGURATION	77
3.1	System Analysis and Design.....	77
3.2	Analysis of the Existing System.....	78
3.3	Problem of the Existing System.....	79 - 80
3.4	Introduction of LAN.....	81 - 82
3.5	LAN Architecture.....	82
3.6	Network Hardware/LAN devices.....	83 - 86
3.7	Hardware Requirement.....	87
3.7.1	Server Specification.....	87
3.7.2	Client Specification.....	87 - 88

3.8 LAN Configuration.....88 - 89

CHAPTER FOUR

4.0 NETWORK IMPLEMENTATION: Network Service,
Network Administration, Network Management,
and Network Troubleshooting.....90

4.1 Network Service.....90 - 94

4.2 Network Administration.....94

4.3 Network Management.....94 - 98

4.4 Network Troubleshooting.....98 - 101

CHAPTER FIVE

5.0 SUMMARY, CONCLUSION, AND RECOMMENDATION...102

5.1 Summary.....102 - 103

5.2 Conclusion.....103

5.3 Recommendation.....103 - 104

REFERENCE.....105

CHAPTER ONE

1.0 INTRODUCTION

1.1 An Overview of the Study

The importance of electronic information transfer and proper information management can not be overemphasized in our modern day. Many Organizations Companies and industries have grown and their appetite for timely information is inexhaustible. Their businesses have grown to the extent of using up-to-date information for running high business deals and improving productivity. Every Organization, Company or Industries focuses on how to have fast access to information and optimized earning.

Decision and policy making in such organizations depends solely on good database, information accessing protocols, sharing of available resources, flexibility of the system (Hardware and Software), cost effectiveness and system reliability. In view of the importance of electronic information transfer and change in the environment location of the computer laboratory, Department of math/computer science, federal university of technology, minna, there is a need for the improvement on the network arrangement in the computer laboratory to improve resource sharing, faster throughput information access. This therefore necessitated this project **“Design and Implementation of computer networking (Local Area Network)”**.

1.2 Statement of Problems

Before the introduction of computer networking, the existing system poses the following problems;

- No sharing of computer resources among users.
- Operational cost is very high.
- The existing system does not aid research for lecturer/software development.
- Maintenance is expensive and difficult.
- The existing system is prone to error and errors without standard error correction techniques.

1.3 Aims And Objectives Of The Proposed System

Communication of data through computer networks is being used for numerous services, suitable for exploitation by any organization or group of computer users. The main objective of this project is aimed at linking the computers in an organization or institution together with a careful consideration for expansion, to enable data transfer, resources sharing, security of data (e.g. student's results) and increase awareness in networking.

The ease and innumerable advantage of being on a network was observed when computers on a LAN easily shared expensive peripheral devices. Human traffic between offices is thus cut down due to the ability to send and receive messages. All this in the long run minimizes the cost to the organization, by maximizing performance of the system.

The project is about the design and implementation of Local Area Network. The network is expected to serve the department by producing services in:

- a. Computer laboratory for students
- b. Research for lecturer/software development
- c. Internet center/business center

The objective of the project is as follows:

- To enable sharing of available resources among the “networked computer”.
- To provide high performance in cyber café’ and business center.
- To ensure the security of important data.
- To allow for interpersonal communication by some message programs.
- To enable the users share application software.
- To increase the departments administrative and organizational benefits.

1.4 Scope and Limitations

Nowadays, there are various types of computer networks with various network media and network topologies. It is the ambitious purpose of this project to provide an informative and unified view into broad field of computer networks.

This project is limited to implementing a Local Area Network (LAN) within the department of an institution or organization.

The LAN is the network that covers a relatively small geographical area ranging from a few feet or a kilometer. And are typically used in offices, building or across university campuses.

1.5 Definitions of some Terms in the project

Computer: A high speed electronic machine that performs tasks, such as calculations or electronic communication automatically, under the control of a set of instructions called a program.

Network: two or more computers connected to exchange data or share resources such as printers, files and storage space.

Network Protocol: this is a written rules used for communication. They are languages the computer uses to talk to each other over a network.

Network Protocol Driver: the software that is installed on every computer within a computer network that allows computer to 'talk the same language' across a computer network.

Network Interface Card: the hardware required to allow computer to transmit messages using a specific type of network protocol.

Ethernet: a network protocol defined by a set of international standard. Normally used for computers located within a 100m radius, but can be used over longer distance.

Transmission Control Protocol (TCP): defines how data are transferred across the internet to their destination.

Internet Protocol (IP): defines how data are divided into chunks, called packets, for transmission; it also determines the path each packet takes between computers.

Internet: a global computer network using the TCP/IP protocol.

TCP/IP or Transmission Control Protocol/ Internet Protocol: Set of rules that enable different types of computers and networks on the internet to communicate with one another.

Internet Service Provider (ISP): It provides internet services to various people.

Bridge: this is a device that allows the segmentation of a large network into two smaller, more efficient networks. It monitors information traffic on both sides of the network so that it can pass packet of information to the correct location.

Media: this is a physical connection between the devices on the network.

MODEM (this is also known as modulator/demodulator): This is a device that converts digital information to analog information and vice versa.

Software: instructions or programs that describe the tasks to be carried out by the computer.

NOS (this is Network Operating System): It coordinates the activities of multiple computers across a network. The NOS act as a director to keep the network running smoothly.

Server: this is a powerful computer that provides service to the other computer on the network.

Client: this is a computer that uses the services that a server provides. The client is usually less powerful than the server.

Peer: this is a computer that acts as both client and server.

LAN (this is also known as local area network): This type of network consist of a set of nodes that are interconnected by a set of link covering a relatively small geographical area ranging from a few feet to a kilometer.

MAN (this is metropolitan area network): It is a group of LANS located in a city.

WAN: computer networks that cover a wide geographical area.

Stand-alone computer: computer that is not networked or linked.

Resources: these are anything that is available to a client on a network. Examples of such are printer, data, fax devices, information etc..

User: this is any person that uses a client to access resources on the network.

CHAPTER TWO

2.0 LITERATURE REVIEW

Computer networks started in the early 60's. The major event viewed as the beginning of the technology and the reason for networking was the necessity to share expensive resources more effectively. The early system (RTDS for IBM 360 GECOS iii for the Honeywell 600, demand for the Univac 1108 and tss18 for the PDP 8) provided the means by which user could simultaneously (from user's perspective) share and use the expensive central processing unit (CPU) and associated resources (John Mark In 1960). The early development made computer more accessible to a wider number of individuals.

The second event in the timeline to networking was the development and introduction of communication oriented software and hardware component such as asynchronous line protocols (SDLC, Bisync), intelligent terminals and line concentrators. These developments led to the development of large disjointed system such as airline reservation system, banking information system, credit reporting and information system and remote booking and point of sales keeping. These still were not network but disjoint system that communicated sporadically using leased lines or telephone circuits to transfer information.

A feature, which ultimately provided the economic reason to interconnect computers to fixed networks, was the drastic drop in computer equipment cost and the improvement in performance. When

taken together, the factors resulted in the inception of the early network. The goal of network was to provide more effective use of the various computer resources via resources sharing and to provide for effective dissemination of information and more computing power to users.

[See Afolayan (1998): computer networking as an effective tool in information technology, oxford publisher, Lagos. Pages 1-7]

Thus the first operational network was Arpanet (advance research project agency network), which was constructed by bolt, beranet, and Newman of Cambridge, Massachusetts, under the contact of arpa and came on-line in 1969 using packet communication. [See "ARPANET" (Microsoft student) Redmond, WA: Microsoft Corporation, 2006.] This and the early network provide the vehicle to research many of the issues in inter-computer communications and to set the groundwork to provide the stimulus to researcher to refine technologies seen in this network.

In 1980, due to the advent of relatively cheap PCs, there is a provision for stand-alone computer, mainly IBM. Compatible machine running Microsoft's operating system and apple Macs. They were single-user systems that excited a wide range of application. The PCs were initially isolated, with data and applications being transferred and loaded on disks. However, increasingly they become connected to work group local area network (LAN). A server on the LAN provided centralized file and print facilities. In this LAN-based mode of operation, the client machines sore and run application locally but use the server to store common data and provide print facilities.

In today network, the user's machine access both application and data on networked servers. The network is very reliable and it can be LAN, MAN or WAN. User on network can access all the servers and all users' machine. Server can also access other servers, enabling one server to draw on applications or services they provide.

X2.1 The Computer Network System

A network is simply defined as the linkage of items together such that they can communicate with each other. However, a computer network can be said to be a method in which a number of computers can be linked together such that they can effectively share data, information and any available resources.

Computers that are not linked or networked are called stand alone computers and can not efficiently share peripheral devices. For instance, a small office with ten stand alone computers and one printer allows only the user connected to the printer to utilize it, other users will have to copy their data onto a floppy diskette, and transfer to the system in question. It will be cheaper in the long run for the organization to link the computers together in a network to enable them share the use of printer, from individual locations rather than trying to purchase a printer for each system.

No matter how far apart computers are from each other, they can always be linked together in a network, which vary in connection modes based on the distances apart, or the application user intends to run.

2.2 Network Component

The under listed items are the components of network:

- i. Server
- ii. Client
- iii. Peer
- iv. Media
- v. Resources
- vi. User
- vii. Protocol

2.3 Networking Model

Network model describe how information is process by the computers on the network. Data can be processed by client, central server, or everyone. The best server model for your needs is generally determined by the application you need to run.

The three basic models of network are:

- a. Centralized
- b. Collaborated
- c. Distributed

A. Centralized Network

This type of network keeps all data in a location assuring everyone is working with the same information. These networks give the ability to access the mainframe from a remote location.

Characteristic of Centralized Network

- i. All data are stored in a location

- ii. It is easy to backup data
- iii. Terminal do not require a floppy drive
- iv. All informations are kept in the server.
- v. The chance of network being infected with a virus is low.
- vi. The server needs to be powerful system with a lot of storage space.
- vii. Termination does not require real processing or storage capacity of it own.

Advantages of Centralized Network

- i. Easy backup
- ii. Security is guarantee
- iii. Low cost of implementation

Disadvantages of Centralized Network

- i. Slow network access
- ii. If the users have a variety of needs, meeting these needs in a centralized computing network is difficult because user's application and resources have to be set up separately.

B. Collaborated Network

This allows computers to share processing power across a network. Application can be written to use the processing on other complete jobs more quickly. These types of network can be faster, users are not limited to the processing power of one system to complete tasks.

Characteristics of Collaborated Network

- i. Users are not limited to the processing power of one system to complete tasks, i.e. it has the ability to process tasks on multiple systems.
- ii. It allows users to share data, resources and services between themselves.

Disadvantages of Collaborated Network

- i. Susceptible to viruses
- ii. Difficult to backup
- iii. File synchronization

C. Distributed Network

This is type of network where all work is done on the server, data storage and processing is done on the local workstation.

This allows for faster access to data. This type of network accommodate user with a variety of needs, yet it allows them to share data, resources and services. Computers in distributed network are capable of working as a stand-alone system but are networked together for increased functionality.

Characteristics of Distributed Network

- i. Server does not need to be as powerful and expensive
- ii. Its accommodate user with a variety of need
- iii. Computers involved are capable of working as a stand-alone

Advantages of Distributed Network

- i. Quick access: - each computer can store and process its own data.
Moving this task from the server to the workstation allows for
Quicker access to data
- ii. Multiple user: - with each workstation handling its own processing
of data, user can be doing many types of work simultaneously.

Disadvantages of Distributed Network

- i. Virus susceptibility:-any user can introduce an infected file, which
may quickly spread throughout the network.
- ii. Backup difficulty:-if data is spread throughout the network, it can
be difficult to backup all needed files.
- iii. File synchronization:-when files are stored in several locations,
making sure users are working the same version can be difficult.

2.4 Classification of Network

A network is no longer just a group of computers in one office or even one large building. Networks are constantly being connected to each other to form larger inter-nets. An internet is a large network made up of connected smaller networks.

The sizes of networks are generally classified into three different groups namely:

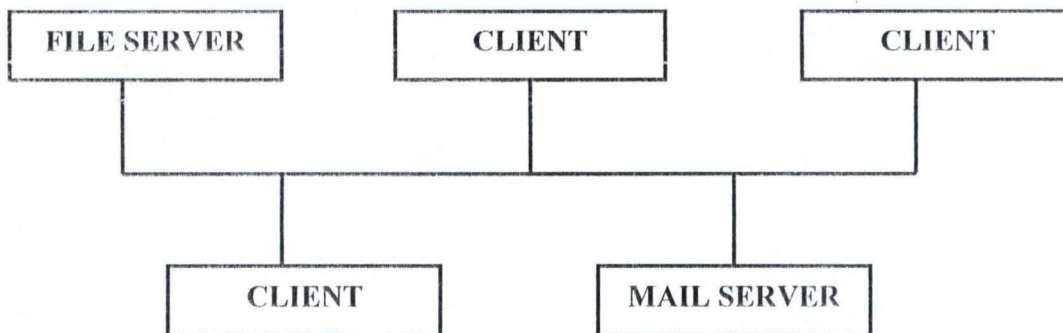
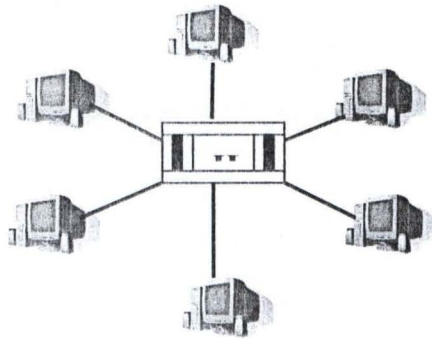
- a. Local Area Network (LAN)
- b. Metropolitan Area Network (MAN)
- c. Wide Area Network (WAN)

A. Local Area Network (LAN)

This is a type of network that consists of set nodes that are interconnected by a set links covering a relatively small geographical area ranging from a few feet or a kilometer usually 50km apart.

Characteristics of Local Area Network

- i. Small areas, usually in one office or building
- ii. High speed
- iii. Most inexpensive equipment
- iv. Low error rates



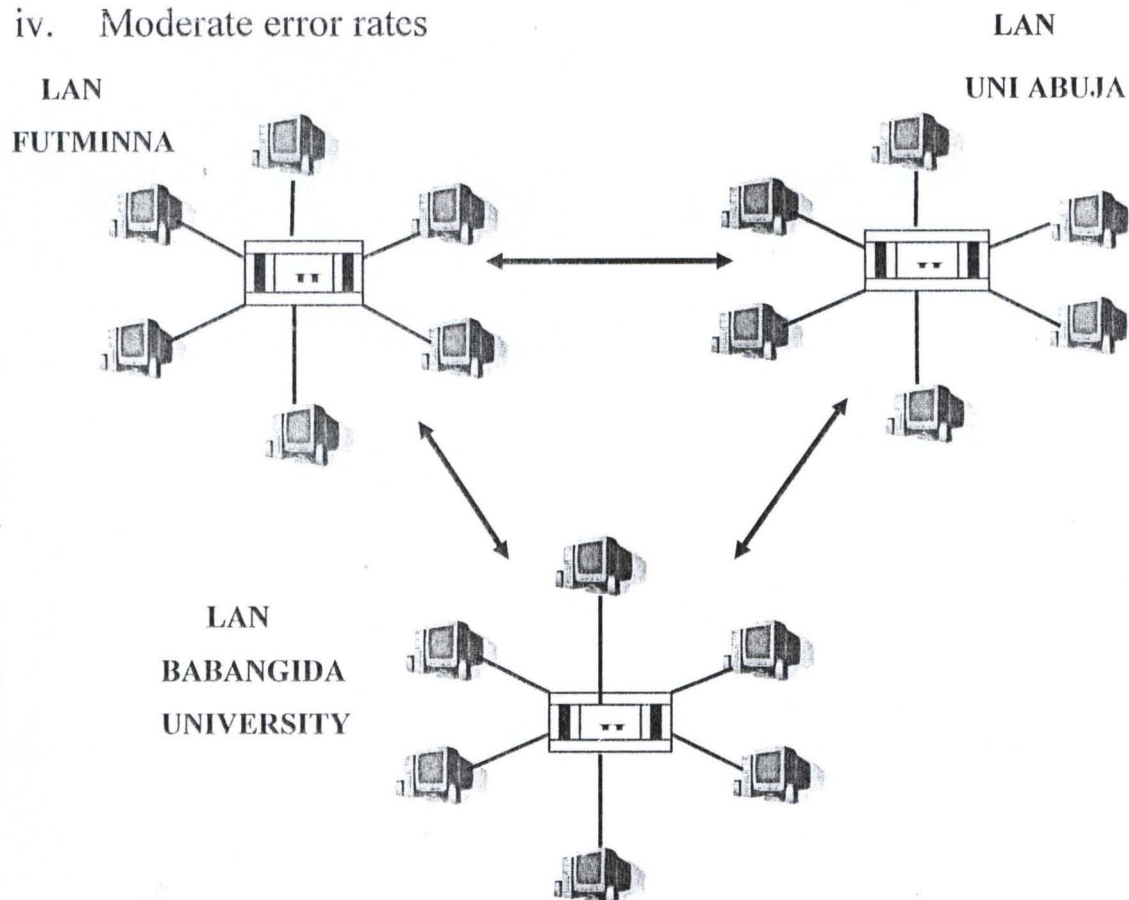
LAN

B. Metropolitan Area Network (MAN)

This is a group of local area network located in a city. It is basically a longer version of the LANs and uses a similar technology. It is optimized for a larger geographical area than LANs, ranging from several blocks of building to a whole town. They can also depend on communication channels of moderate to high data rate.

Characteristics of MAN

- i. Large area than a LAN:-usually a large campus or organization spread over a city –size
- ii. Slower than a LAN, but faster than a wan
- iii. Expensive equipment
- iv. Moderate error rates



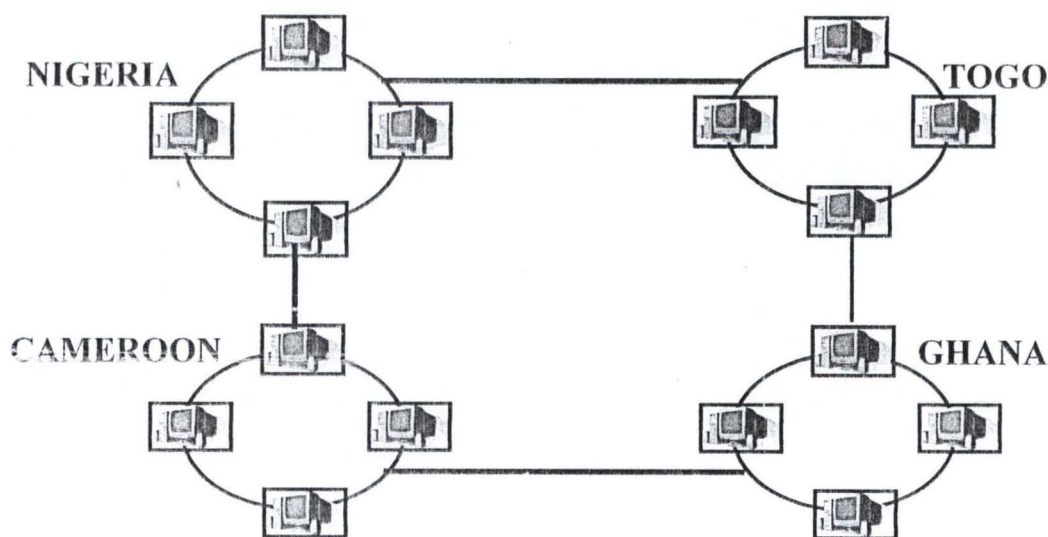
C. Wide Area Network (WAN)

This is a type of network that connects nodes in a large geographical area, usually on hundreds of kilometers such across a country or continent. It span is normally based on conventional telecommunication techniques. WANs spanning consideration distance may use microwave transmission or even communications satellites as routing stations. Such systems are extremely fast.

A microwave network sends voice or data traffic by radio waves between relay towers. Each tower in the chain receives, amplifies and retransmits signals. Cable TV network also provide potentials for data communications.

Characteristics of WAN

- i. It can be as large as worldwide
- ii. Usually much slower than LAN speed
- iii. Highest possible error rate of all types
- iv. Expensive equipment



2.5 Network Operating System (NOS)

This coordinates the activities of multiple computers across a network.

The NOS acts as a director that keeps the network running smoothly.

It provides the control and management of all the components connected to the network only (send-receive). At the upper level, it manages input/output devices, storage devices, computers and the associate software processes operation on the system.

The network operating system (NOS) allows users to request for services while being oblivious to whether it is local or remote request. For tight control of devices dispersed over a wide range, an integrated distribution operation system with services for synchronizing processes and distributed control is necessary.

Function of Network Operating System

The NOS provide the following function:

- i. Processor and memory management
- ii. Input and output devices management
- iii. Network management
- iv. File management

Types of Network Operating System

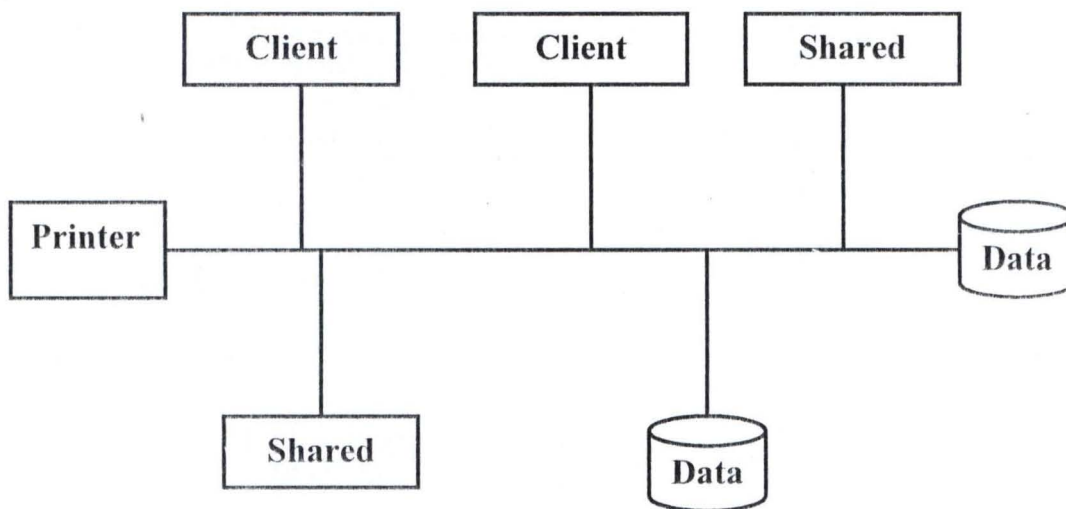
There are two major types of network operation system namely:

- i. Peer-to-peer network operating system
- ii. Client/server network operating system

(I) Peer-To-Peer Network Operating System

In this type of NOS, each workstation acts as both a client and a server. This is no central repository for information and no central server to maintain. Data and resources are distributed throughout the network and each user is responsible for sharing data and resources connected to their system.

Peer-To-Peer Network with Shared Resources



The following operating system associated with peer-to-peer networking:

- a. Windows 95
- b. Windows for workgroups
- c. Windows NT workstation
- d. Os/2
- e. Netware Lite

Characteristics of Peer-To-Peer NOS

- i. It is meant for small office
- ii. User can keep their date own local workstation
- iii. It allows them to handle their own security and by-pass the need for a large and expensive server.

Advantages of Peer-To-Peer NOS

- i. Inexpensive
- ii. Easy setup
- iii. Easy maintenance

Disadvantages of Peer-To-Peer NOS

- i. No central administration
- ii. Scattered data
- iii. Difficult-to-locate resources
- iv. Weak security
- v. Dependent on user training

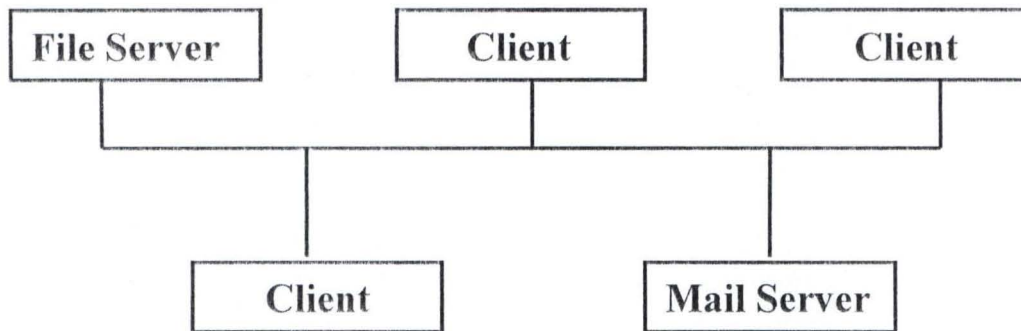
(II) Client/Server Network Operating System

In this type of network operating system, there is one computer (usually larger than the client), which is dedicated to handling our files and/or information for the client. The server controls the data as well as printer and other resources that the client need to access. It is very fast with a better processor. It requires much storage space to contain all the data that needs to be shared to the client. Server allows the client to be less functional because they only request resources.

They are known as **intelligent computer**.

Characteristics of Client/Server NOS

- i. It provide service to other computer
- ii. Security is easily maintained
- iii. Ease of accessing and backing up data



Client/Server Network

Server can be either dedicated server or specialized service server

(A). Dedicated server can be divided into:

- i. File and print server
- ii. Application server

(I) File and Print Server

These servers are optimized to hand out files to client and to handle printing requests. They are mainly used to store data application. When a client runs on an application from a file and print server, it copies the needed files down locally and runs the application. No application processing is done on server everything is done on the client.

(II) Application Server

Application server applications are almost opposite of file servers. The application runs and is stored on the client. Requests are then sent to the server to be processed and the processed information i.e. sent back to the client.

This way, the client processes little information, and everything is done by the server. A good example of this is a database application with a front-end on the client. A front-end is a small application that runs on a client, which sends and receives information to and from the server. The front-end acts mainly as an interface to the database stored on the server. When a user at the client end needs information from the database, an instruction is sent from the client to server telling the server to search for that information. The server then sorts through the database, locates the information that was requested, and sends the answer back to the client.

(B) Specialized Server

This is the server that has a single specialized purpose. The types of such servers are:

- i. Mail server
- ii. Communication server

(I) Mail Server: this is a server specifically set up to handle client e-mail needs.

(II) Communications Server: communication server is set up to handle remote user dialing into your network. The communication server applications are normally put on a separate server for security.

The operating system that client-server supports are window NT, Novell's Netware etc

Advantages of Client-Server Network Operating System

- i. Centralized security
- ii. Dedicated server
- iii. Easy accessibility
- iv. Easy backup
- v. Synchronized files

Disadvantage of Client-Server Network Operating System

- i. Dependent an administration
- ✗ii. Expensive server

2.6 Open System Interconnection Model

Open System: This is a model that allows any two different computer to communicate regardless of their under lying architecture.

Open System Interconnection: This comprises a set of recommendation for conceptual protocol layer necessary in every open communication network. OSI suggest a way of organizing network protocols and looking at various levels of their functionality.

Open System Interconnection Model

This is a layered framework for the design of network system that allows for communication across all types of computers. It consists seven separate but related layers, each of which defines a segment of the process of moving information across a network. Layer one; two and three are the support layer. It deals with the physical aspects of moving data from one device to another. Layer four, five, six and seven are referred to as user support layer. They allow interoperability among unrelated software layer.

Purpose of OSI Model

OSI model offers the following function:

- i. Network hardware and software designers can allocate tasks more effectively among network resources.
- ii. A network layer can be replaced easily by a layer from another network vendor.
- iii. Processes from mainframe can be off-loaded into feds or another network control devices.
- iv. Network can be upgraded easier by replacing individual layer instead of the entire software system.

Advantage of Layering

The following are the advantages of layering:

- i. Standard interface between layers allow internal development within a particular layer to evolve.

- ii. Alternative services may be offered at a given layer by having different options or routes through the layer
- iii. Internal mechanisms of each layer are invisible to the other layers.
- iv. Layer may be completely removed if not required, or a simplified version can be used as substitute where appropriate.

OSI model

Layer 7	Application Layer
Layer 6	Presentation Layer
Layer 5	Session Layer
Layer 4	Transport Layer
Layer 3	Network Layer
Layer 2	Data Link Layer
Layer 1	Physical Layer

Open System Interconnection Layer

OSI layer comprises of the following:

- i. Physical
- ii. Data link
- iii. Network
- iv. Transport
- v. Session
- vi. Presentation
- vii. Application

Physical Layer (Layer 1)

This is the bottom most layer which transmits the instructed raw bits stream over a physical medium, the layer relates the electrical, optical, mechanical and functional interface to the cable.

It is also responsible for transmitting bit from one computer to another. It defines the data encoding and bit synchronization to ensure that when a transmitting host sends I bit, it is received as I bit.

Data Link (Layer 2)

This is the layer that next to physical layer. It sends data from the network layer to the physical layer. On the receiving end, it package raw bits from the physical layer into data frames (a data frame is an organized logical structure in which data can be placed).

Network Layer (Layer 3)

This layer is responsible for addressing message and names to physical addresses. It determines the route from source to the destination computer. It determines which path the data should take based on network condition priority of service and other factors. It also manages traffic problems on the network such as pack of switching routing and controlling the congestion of data.

Transport Layer (Layer 4)

It provides an additional connection level between the session layers. It ensures that packets are delivered error-free in sequence with no losses or duplication.

This layer repackages message dividing long message into several packets and collecting small packets together to be transmitted efficiently over the network. At the receiving end, the transport layer impacts the messages the message reassemble the original message and typical send and acknowledgement of receipt.

Session Layer (Layer 5)

This allows the application on different computer to establish use and end connection called a session. It performs name recognition and function such as security needed to allow two applications to communicate over the network.

Presentation Layer (Layer 6)

This layer determines the format use to exchange data among network computer. At the sending computer, the layer translates data from a format sent down from the application layer into commonly organized intermediary format. At the receiving computer, it translates the intermediary format into a final format.

Application Layer (Layer 7)

This is the topmost layer of OSI model. It represents the services that directly support user application such as software for the transfers, for database access and for e-mail, the layer handle general network access flow control and error recovery.

2.7 Network Media

2.7.1 Network Adapter

This is commonly known as network interface cards (NICs) or network card. It is responsible for moving data from the computer to the transmission media. The network adapter transforms data into signals that are carried across the transmission media to its destination. Once the signal reaches the destination devices, the NICs translate the signal back into information the computer can process. The circuitry on the card that does the conversion of the signal is known as a **TRANSCIEVER**. Ethernet can run over a few different cable types but the main circuitry on all the Ethernet cards should be the same, only the transceiver should be different.

The following are the type of Network Adapter:

- i. **ISA:** Industry Standard Architecture
- ii. **MCA:** Micro Channel Architecture
- iii. **EISA:** Extended Industry Standard Architecture
- iv. **VESA:** Video Electronic Standard Association
- v. **PCI:** Peripheral Component Interface
- vi. **PCMCIA:** Personal Computer Memory Card International Association

Network Adapter Port

This is a port that allow adapter card to connect to the network media. The type of connector you can use may depend on the brand of network adapter you chose or the type of network to which it is connecting.

Type of Connector

BNC connector

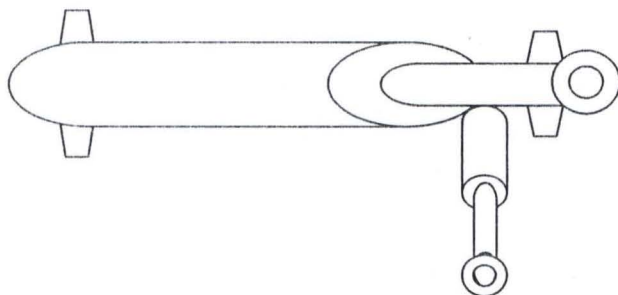
RJ-45 connector

DIX connector

AUI connector

BNC Connector

This is used in attached resource computer network (ARCNET) and in thin Ethernet (10 base-2). The connector is a small, round cylinder with two small prongs on the outside that allows a connector to attach to it. BNC looks like T connector. It is used to connect the network adapter to the two pieces of coaxial cable.



RJ-45 Connector

The RJ-45 connector looks much like a normal telephone cable connector, but larger. It uses twisted pair cabling with four pairs of wires. A normal telephone jack uses an RJ-11 connector, which is a twisted pair with two pairs of wires.

DIX Connector

These connectors are not used often anymore but were widely used when thick Ethernet was popular. DIX is a 15-pin connector with two rows of pins. A cable was attached to the NIC through this port and was attached to the thick Ethernet cable by use of a “vampire tap” the tap had to be drilled into the cable and tightened down. Dix stands for three companies that invented it: digital, Intel, and Xerox.

AUI Connector

This is also known as attachment unit interface. It is a renamed DIX connector. It is mainly used today for external transceiver.

2.7.2 Bounded Media / Transmission Media

Bounded media are also known as wire or network cable. They are referred to as bounded media because the signal travels through a physical media shield on the outside (bounded) by some material. Bounded media are made up of a central conductor (usually copper) surrounded by a jacket material. Bounded media are great for LANs because they offer high speed, good security and low cost.

The following are the characteristics to look for in selecting or choosing a cable:

- i. Cost: cost can be an important consideration when deciding on a network cable.
- ii. Capacity: this is a characteristic to be considered when choosing a cable. “How fast will it go” matters most.

Cable speed is referred to as bandwidth and is an important

characteristic of a media type.

- iii. Attenuation (Maximum Distance): depending on what you need to network together, the maximum cable distance may also be considered.

Type of Bounded Media

Three common types of bounded media are

- a. Coaxial
- b. Twisted pair
- c. Fiber optic

2.7.2.1 Coaxial Cable

Coaxial cable gets its name because it contains two conductors that are parallel to each other, or on the same axis. The center conductor in the cable is usually copper. The copper can be either a solid wire or a standard material. Outside this central conductor is a non-conductive material. It is usually white, plastic like material, used to separate the inner conductor from the outer conductor. The outer conductor is a fine mesh made from copper.

The actual network data travels through the center conductor in the cable should be grounded at one end to dissipate this electrical interface.

The most common coaxial standards are:

- 50-ohm RG-7 OR RG 11: used with thick Ethernet
- 50-ohm RG-58: used with thick Ethernet
- 75-ohm RGG-59: used with cable television

- 93-ohm RGG-62: used with ARCNET

Characteristics of Coaxial Cable

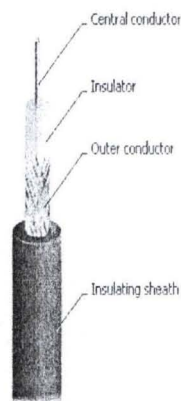
- Low cost
- Easy to install
- Up to 10mps capacity
- Medium attenuation
- Medium immunity from EMI

Advantages of Coaxial Cable

- Inexpensive
- Easy to wire
- Easy to expand
- Moderate level of EMI immunity

Disadvantage of Coaxial Cable

- Signal cable failure can take down an entire network.



Coaxial Cable

2.7.2.2 Twisted Cable

Twisted-pair cable is made up of pairs of solid or standard copper twisted around each other. The twists are done to reduce the vulnerability to EMI and cross talk. The number of pairs in the cable depends on the type. The copper core of the cable is usually 22-awg or 24-awg, as measured on the American wire gauge standard.

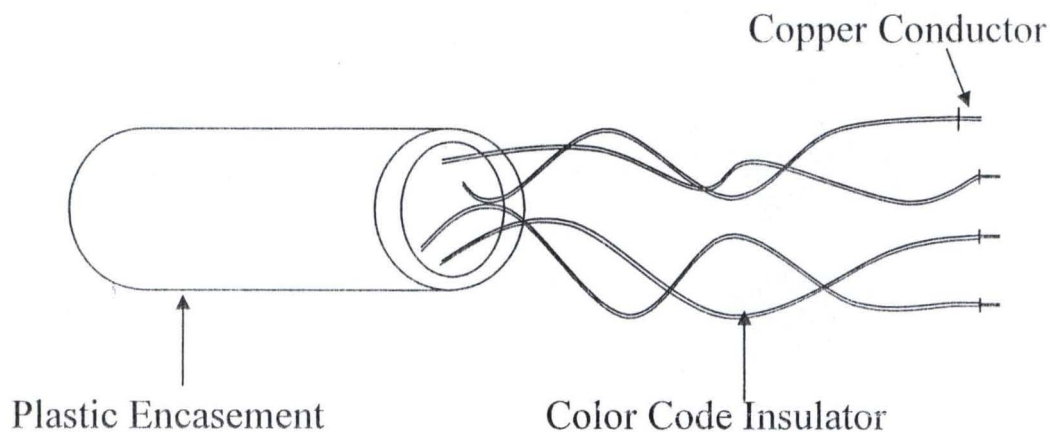
It is lightweight, easy to install, inexpensive, and support many different types of networks. It can also support speed of up to 100mbps.

There are two varieties of twisted pair cable namely:

- a. Unshielded twisted pair (UTP)
- b. Shielded twisted pair (STP)

Unshielded Twisted Pair (UTP)

UTP data cables consist of two or four pairs of twisted cables. Cable with two pair use RJ-11 connectors, and four-pair cables use RJ-45 connectors. It can be either grade or data grade, depending on the application. UTP cable normally has an impedance of 100 ohms. UTP costs less than shielded twisted pair.



There are five levels of data grade cabling namely:

- i. **Category 1:** this category is intended for use in telephone lines and low speed data cable.
- ii. **Category 2:** category 2 includes cabling for lower speed network. These can support up to 4 mbps implementations.
- iii. **Category 3:** this is a popular category for standard Ethernet network. These cable support up to 16mbps but are most often used in 10 Ethernet situations.
- iv. **Category 4:** this is used for longer distance and higher speeds than category 3 cable. It can support up to 220 mbps.
- v. **Category 5:** this cable is intended for higher performance data communications. This is the highest rating for UTP cable and can support up to 1000 mbps.

Characteristic of UTP

- i. Low cost (but slightly higher than coaxial!)
- ii. Easy to install
- iii. High-speed capacity
- iv. High attenuation
- v. Susceptible to EMI
- vi. 100-meter limit

Advantages of UTP

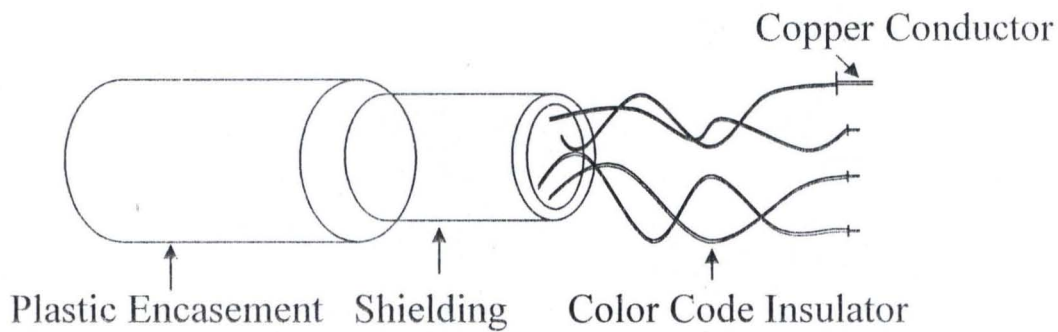
- i. Easy installation
- ii. Capable of high speed for LANS
- iii. Low cost

Disadvantage of UTP

- i. Short distance due to attenuation

Shielded Twisted Pair (STP)

STP is similar to UTP but has a mesh shielding that protects it EMI, which allows for higher transmission rates and longer distances without errors. STP is usually used in **token ring**.



STP has different levels and they are describing below:

Type 1: Type 1 STP feature two pairs of 22-AWG, with each pair foil wrapped inside another foil sheath that has a braid ground.

Type 2: This type includes type 1 with four telephone pairs sheathed to the outside to allow one cable to an office for both voice and data.

Type 6: This type feature two pairs of stranded, shielded 26-AWG to be used for patch cable.

Type 7: This type of STP consist of stranded, 26-AWG wire

Type 9: Two pairs of shielded 26-AWG, used for data, comprise this type of cable.

Characteristics of STP

- i. Medium cost
- ii. Easy of installation is medium due to grounding and connectors.
- iii. Higher attenuation, but the same as UTP
- iv. Medium immunity from EMI
- v. 100-meter limit

Advantage of STP

- i. Shielded
- ii. Faster speed than UTP and coaxial

Disadvantage of STP

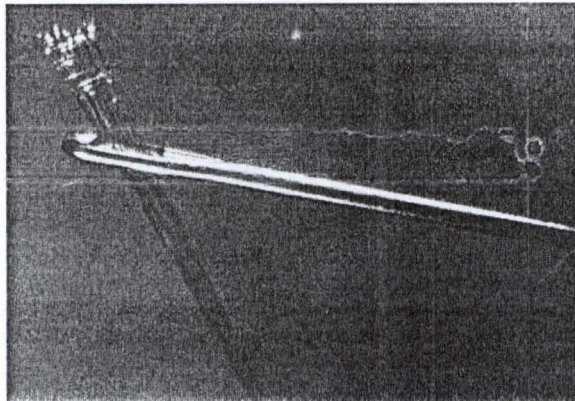
- i. More expensive than UTP and coaxial
- ii. More difficult installation
- iii. High attenuation rate.

2.7.2.3 Fiber-Optic Cable

Fiber optic cable makes use of light to transmit data. In a fiber cable, light only moves in one direction. For two communication to take place, a second connection must be made between the two devices, which why you examine fiber cable you notice it is actually two strands of cable each strand is responsible for one direction of communication.

A laser at one device sends pulse of light through this cable to the other device. These pulses are translated into O's and 1's at the other end. In the center of the fiber cable is a glass strand, or core. The light from the laser travels through this glass to the other device.

Around the internet core is a reflective material known as cladding. No light escapes the glass core because of this reflective cladding. Fiber optic cable has a bandwidth of more than 2 Gbps.



Fiber-Optic Cable

Characteristics of Fiber-Optic Cable

- i. Expensive
- ii. Very hard to install
- iii. Capable of extremely high speed
- iv. No EMI problems

Disadvantages of Fiber-Optic Media

- i. Hard to install
- ii. Expensive

Electrical Properties of Bound Media

Resistance: when electricity moves through a media, it meets resistance. When moves resistance is met, more electricity is lost during transmission. The resistance causes the energy to be covered to heat. Cable with small diameters has more resistance than cable with large diameter.

Impedance: the loss of energy from an alternating current (AC) is impedance. It is measure in ohms. DC travels through the core of the wire while AC travels on the surface.

Noise: noise is a serious problem for cabling and some times hard to pinpoint. Noise can be caused by radio interference (RFT) or electromagnetic interface (EMI). Some common causes are fluorescent light, transformation, Power Company on a bad day, and nearly anything else that creates an electrical field. Noise can be easy to avoid if you plan your cable installation well.

Attenuation: this is the fading of the electrical signal over a distance.

Cross Talk: this is when the signal from one cable is leaked to another by an electrical field. An electrical field is created whenever an electrical signal is sent through a wire. If two wires are close enough and do not have enough EMI protection, the signal may leak and cause noise on the other wire.

2.7.3 Unbounded Media

Unbounded media is also known as wireless media. This media does not use any physical connector between the two devices communication. The transmission is sent through the atmosphere, but sometimes it can be just across a room. Wireless media is used when a physical obstruction or distance block the use of cable media.

Types of Unbounded Media

The three main types of wireless media are:

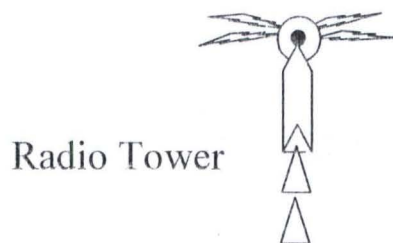
- a. Radio wave
- b. Microwave
- c. Infrared

2.7.3.1 Radio Wave

Radio wave has frequencies between 10 KHz and 1GHz.

Radio wave includes the following type:

- i. Short-wave (SW)
- ii. Very-high frequency (VHF) television and radio
- iii. Ultra-high frequency (UHF) television and radio.



Radio wave transmission can be into the three categories:

- i. Low power, single frequency
- ii. High power, single frequency
- iii. Spread spectrum

(I) Lower Power, Single Frequency

This type transmits on one frequency and has low power output. The normal operating range on these types of devices is 20-25 meters. The speed of this system varies from 1mbps to 10mbps. Attenuation is a problem with these devices due to the low power output that is allowed.

Characteristics of Low Power Single Frequency

- i. Low cost wireless media
- ii. Simple installation with reconfiguration equipment
- iii. 1mbps to 10mbps
- iv. high attenuation, which can limit range to 25 meters
- v. low immunity to EMI

(II) High Power, Single Frequency

This system is similar to low power, single frequency but the only different is that the device can communicate over greater distances.

Transmission can be line of sight or bounced off the atmosphere for longer distance.

Characteristics of High Power, Single Frequency

- i. Moderate cost for wireless media
- ii. Easier installation than low-power solution
- iii. 1mbps to 10mbps capacity
- iv. Low attenuation for long distances
- v. Low immunity to EMI

(III) Spread Spectrum

This system uses several frequencies at once provide reliable transmission that are resistance to resistance. Spread spectrum communicate makes use of the following method transmit information.

- i. Direct-sequence modulation and
- ii. Frequency hoping

(i) Direct-Sequence Modulation:-This break data chips and transmit the chips across several frequencies. The receivers know which data to collect on different frequency and assemble them accordingly.

(ii) Frequency-Hopping:-This system strict timing to switch frequency. Both the sender and the receiver are sets to change frequency at specific time. Burst of data are sent on one frequency, and then the machine switch to another frequency for the next data bust.

Characteristics of Spread Spectrum

- i. Moderate cost
- ii. Simple to moderate installation
- iii. 1-6Mbps capacity
- iv. High attenuation
- v. Moderate immunity to EMI

2.7.3.2 Micro Waves

Microwave travel at higher frequency than radio wave and provide better throughput as a wireless network media. Microwave transmission requires the sender to be within sunlight of the receiver.

Communication system can be:

- a. Terrestrial microwave and
- b. Satellite microwave

(a) Terrestrial Microwave

Terrestrial microwave transmission is used to transmit wireless signals across a few miles. The system is often used to across roads or other barriers that cable connections difficult.

This system requires that direct parabolic antennas be point at each other.

Relay towers can be used as a repeater to extend the distance of the transmission. Terrestrial microwave operate in the low Giga-hertz range.

Characteristics of Terrestrial Microwave

- i. Moderate to high cost
- ii. Moderately difficult installation
- iii. 1-10mbps capacity
- iv. Variable attenuation
- v. Low immunity to EMI

(b) Satellite Microwave

Satellite microwave transmission is used to transmit signal throughout the world. These systems use satellite in orbit 50,000km above the earth. Satellite dishes are used to send the signal to the satellite where it is then sent back down to the receiver satellite.

This transmission use directional parabolic antennas within line of site. The large distance the signal can cause propagation delays. These system can provide average bandwidth but if lack advance security and protection from interference.

Characteristics of Satellite Microwave

- i. High cost
- ii. Extremely difficult and complex installation
- iii. 1-10mbps capacity
- iv. Variable attenuation
- v. Low immunity to EMI

2.7.3.3 Infrared

The technology of infrared is similar to the use of a remote control for a television. It frequency is below visible light. Because of it high frequency, it allows high-speed data transmission. Objective obstructing the sender or receiver and any interference from light source can affect infrared transmission. These systems are electromagnetic interference and can be used successfully where certain type of cable media fail.

This type of transmission falls into the following two categories:

- a. Point-to-point
- b. Broadcast

(a) Point-To-Point

This transmission utilizes high beams to transfer signal directly between two systems. Point-to-point requires direct alignment between devices. This system is susceptible to interference from anything that can block the part beam. It provides high level of security. Many laptop and PDA (personal data assistance) use point-to-point transmission.

Characteristics of Point-To-Point

- i. Wide range of cost
- ii. Moderate easy installation
- iii. 100kbps-16mbps capacity
- iv. Variable attenuation
- v. High immunity to EMI

(b) Broadcast

Broadcast infrared transmission use a spread signal, one broadcast in all directions, instead of direct beams. This help to reduce the problem of alignment and obstruction. It allows multiple receivers of signal. Broadcast infrared operate in the same frequency as point-to-point infrared and is susceptible to interference from light sources.

Characteristics of Broadcast Infrared

- i. Inexpensive
- ii. Simple installation
- iii. 1mbps capacity
- iv. Variable attenuation
- v. Moderate immunity to EMI

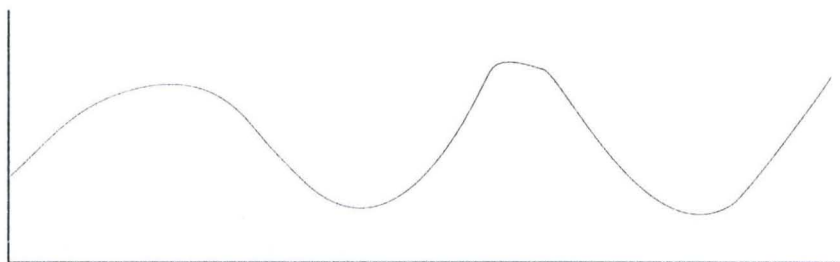
2.7.4 Data Transmission

Data transmission is the way in which data is being transferred in the network. Data transmission across the network can occur in two forms namely:

- Analog
- Digital

• Analog Signaling

An analog signal takes form of a wave, which smoothly curves from one value to the next. The analog wave starts at zero, increases to its high peak, recedes past zero to its low peak. And then rises to zero. This change in the wave is known as the wave cycle.

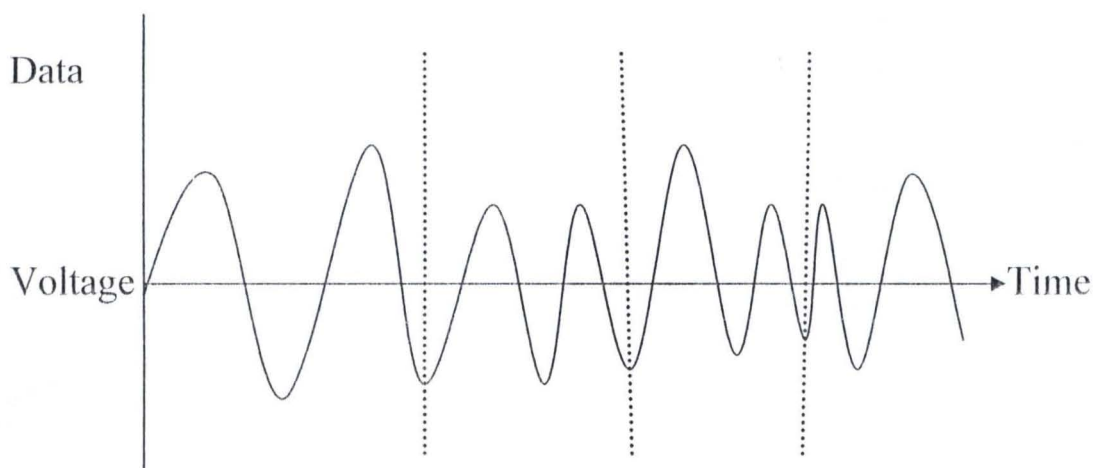


ANALOG SIGNAL

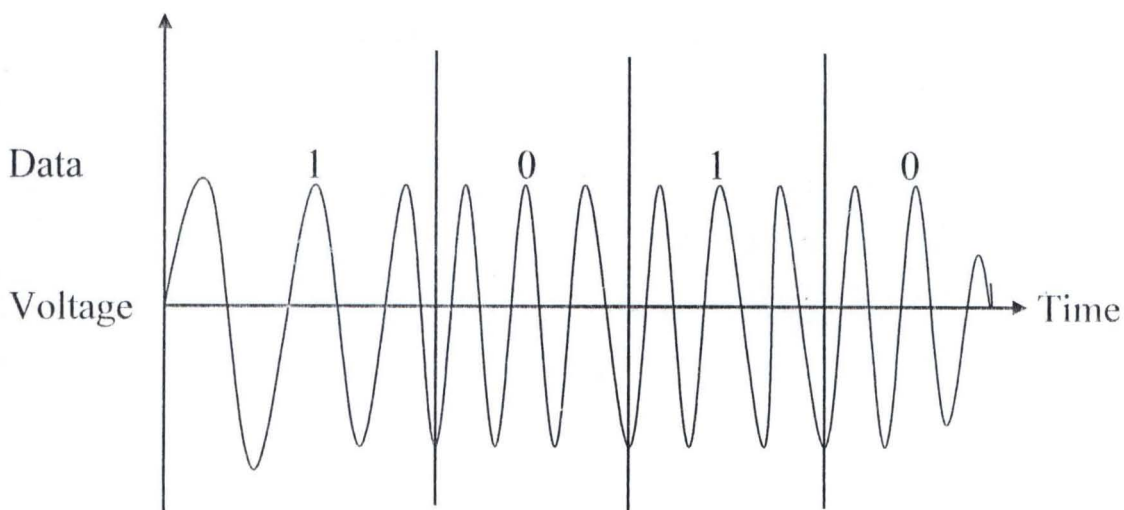
Characteristics of Analog Signal

The following are the Characteristics of analog signal:

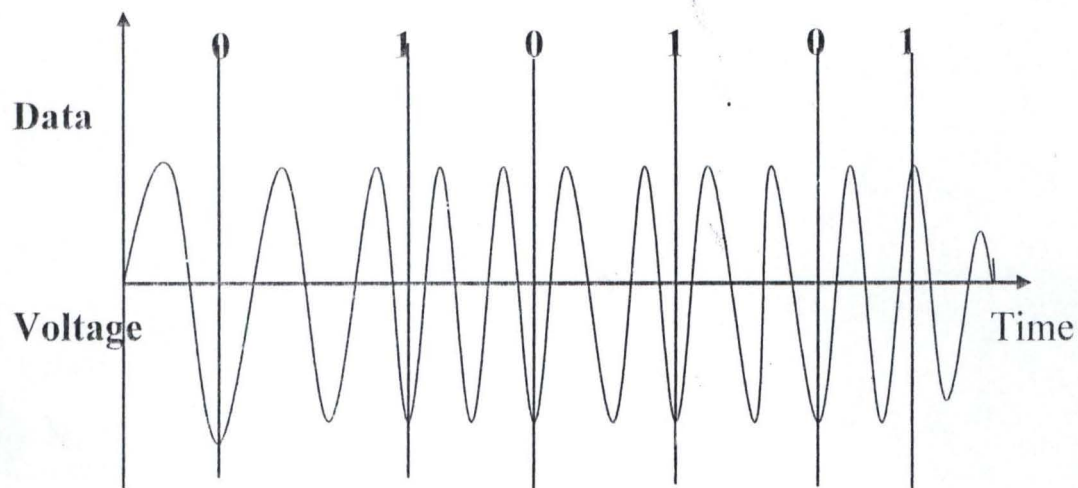
Amplitude: this is the signal strength and is measured as the distance from the zero baselines to the high peak. The method use to encode data using amplitude is called **amplitude shift keying (ASF)**



Frequency: this is the time it makes signal to complete its cycle. Frequency is measured in hertz. The method use to encode data value using frequency is called **Frequency Shift Keying (ASK)**



Phase: this is determined by comparing the cycle of two signal of the same frequency. Phase is measured in degree. The method use to code data value using phase is called **Phase Shift Keying (PSK)**



Advantages of Analog Signaling

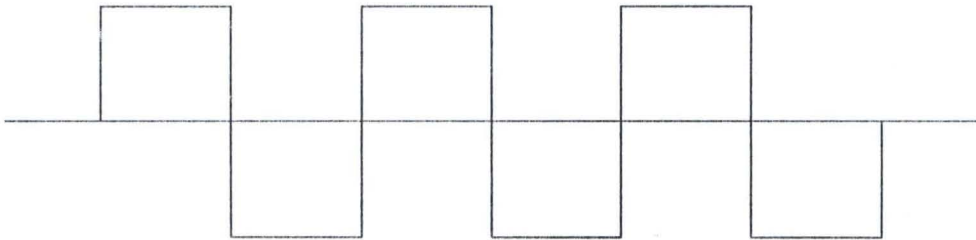
- i. Allows multiple transmission across the cable
- ii. Suffer less from attenuation.

Disadvantages of Analog Signaling

- i. Suffer from EMI and noise
- ii. Can only be transmitted in one direction without sophisticated equipment

- **Digital Signaling**

This is the kind of signal that changes from 0 to 1 instead of smooth curve in analog signaling, digital jump directly to the next value. Digital signal are synchronized in bits this can be clocked by either sending a separate clocking scheme across the network with the bits, or by using a guaranteed state change clocking scheme.



DIGITAL SIGNAL

Advantages of Digital Signaling

- i. Equipment is cheaper and simpler than analog equipment
- ii. Signal can be transmitted on a cable bi-directionally.
- iii. Digital signal suffer less noise and interference

Disadvantages of Digital Signaling

- i. Only one signal can be sent at a time
- ii. Digital signal suffer from attenuation

2.8 Network Topology

Topology can be defined as the interconnection of network nodes. The topology of a network is simply the way in which the cable connections are made, it specifically refers to the physical layout of the network, especially the computers and how the cable is run between them. It is vital to select the right topology and how the network would be used because each has its own weaknesses and strengths, determined by speed, distance cost, reliability and load requirement.

This can be classified into the following:

- a. Physical topology
- b. Logical topology

(a) Physical Topology: - This refers to the way in which the end point of computers is connected electronically. It involves how cable and computer are connected together.

(b) Logical Topology: - This is the method in which the information is passing between the workstation and main server.

Types of Topology

The following are the types of topology

- i. Point-to-Point topology
- ii. Ring topology
- iii. Bus topology
- iv. Star topology
- v. Mesh topology

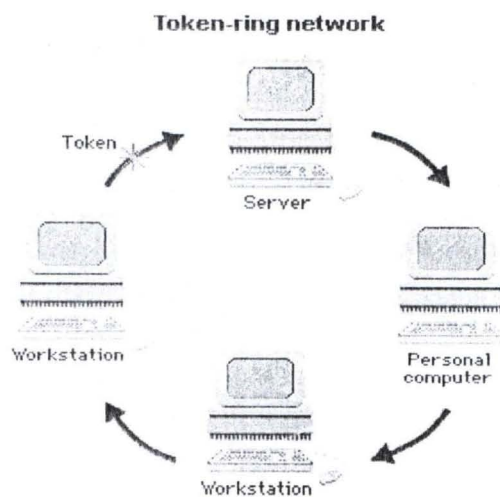
Point-To-Point Topology

This is the simplest, consisting of two connected computers.

LANs commonly use **ring**, **bus** or **star topologies**. WANs, which connect distant equipment across the country or internationally, often use special leased telephone lines as point-to-point links.

Ring Topology

In a Ring Network, devices (nodes) are connected in a closed loop, or ring. Messages in a ring network pass in one direction, from node to node. As a message travels around the ring, each node examines the destination address attached to the message. If the address is the same as the address assigned to the node, the node accepts the message; otherwise, it regenerates the signal and passes the message along to the next node in the circle. Such regeneration allows a ring network to cover larger distances than in other network configurations. It can also be designed to bypass any malfunctioning or failed node. Because of the closed loop, however, new nodes can be difficult to add.



Ring topology connects all the terminals or microcomputers with one continuous loop. Within this loop, data travels in one direction only making a complete circle around the loop.

Advantages of Ring Topology

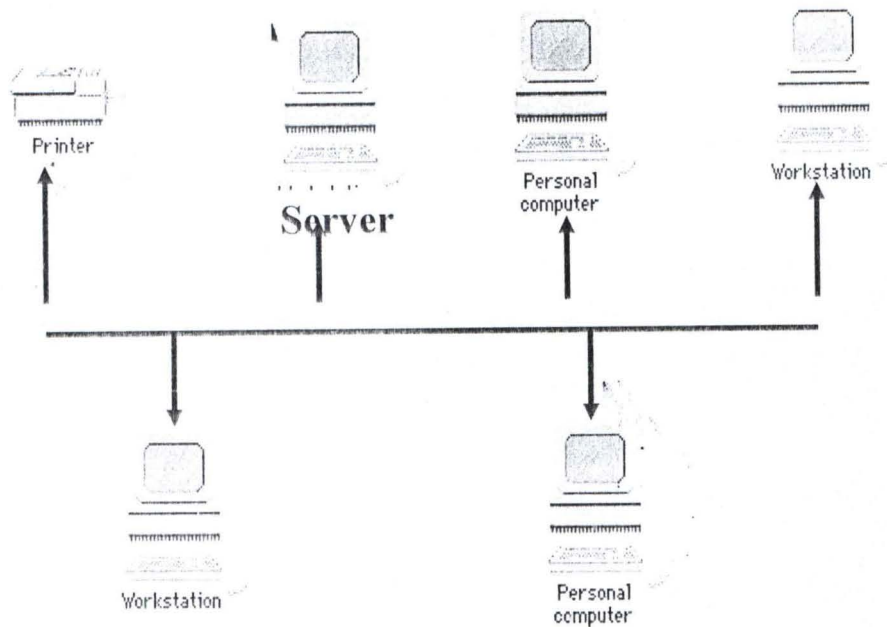
- i. It provide an orderly network in which every device has access to the token and can transmit
- ii. It perform well under heavy load

Disadvantages of Ring Topology

- i. Malfunctioning workstation and cable create problems for the entire network
- ii. Changes made when adding or removing a device affect the entire network

Bus Topology

A topology (configuration) for a Local Area Network in which all nodes are connected to a main communications line (bus). On a bus network, each node monitors activity on the line. Messages are detected by all nodes but are accepted only by the node(s) to which they are addressed. Because a bus network relies on a common data “highway,” a malfunctioning node simply cease to communicate; it doesn’t disrupt operation as it might on a ring network, in which messages are passed from one to the next. To avoid collisions that occur when two or more nodes try to use the line at the same time, bus network commonly rely on collision detection or token passing to regulate traffic



In this type of topology, each of the terminals or microcomputers is connected to a signal cable that runs the entire length of the network. Messages travel directly to or from the intended terminal or microcomputer.

Advantages of Bus Topology

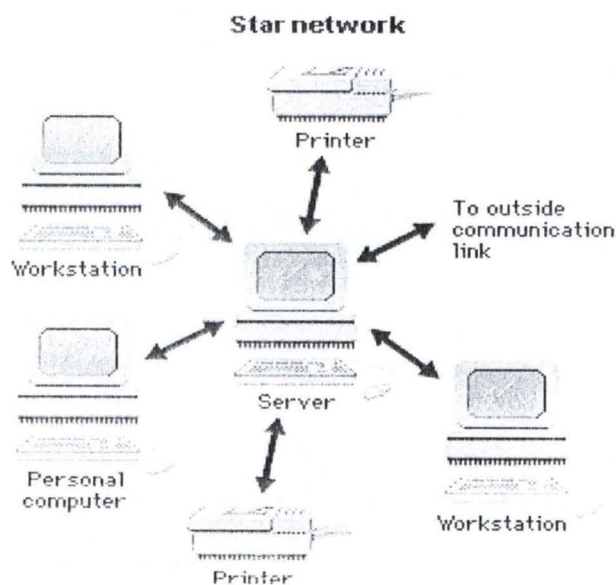
- i. Easy to install and configure
- ii. Inexpensive
- iii. Easily extended

Disadvantages of Bus Topology

- i. Performance degrades
- ii. Barrel connector used to extend the cable lengths can weaken the signal
- iii. Troubleshooting a bus can be quite difficult

Star Topology

This is a local area network in which each device (node) is connected to a central computer in a star-shaped configuration (topology); commonly, a network consisting of a central computer (the hub) surrounded by terminals. In a star network, messages pass directly from a node to the central computer, which handles any further routing (as to another node) that might be necessary. A star network is reliable in the sense that a node can fail without affecting any other node on the network. Its weakness, however, is that failure of the central computer results in a shutdown of the entire network. And because each node is individual wired to the hub, cabling costs can be high.



Star topology uses a separate cable for each workstation. This cable connects the workstation to a central device, typically a hub. This configuration provides a more reliable network that is easily expanded.

Advantages of Star Topology

- i. Easily expanded
- ii. Easier to troubleshoot
- iii. Multiple cable types supported by hubs

Disadvantages of Star Topology

- i. The hub can be a single point failure
- ii. Requires more cable than most other topologies
- iii. May require a device to rebroadcast signals across network

Mesh Topology

Here each computer is connected to all the others at once, this becomes quite difficult to install as the number of computers increases. For example to connect seven (6) computers together, it will require 15 links $[\{(n-1) n\}/2, n=6]$ and so on. However, they are easy to troubleshoot, and are fault tolerant, which is a major advantage. Its major disadvantage is the difficulty installation and reconfiguration.

2.9 Network Protocols

Protocol is a set of rule and convention used to impose standardize structure language for the communication between multiple parties.

For example, a protocol might define the order in which information is exchange between two parties. Protocols are set of rules that specify precisely how different parts of the network interact to allow devices to communicate with one another. They describe what routing information is included with the transmitted data to ensure that the correct device receives it properly.

To perform the full range of network functionally, several protocols are typically active simultaneously in any given network. The multiple protocols that exist in a network environment are related to one another as member of a “**protocol suite**”.

They must be able to evaluate the performance of the network, identify and correct error, okay transfer of data, facilitate physical connections and enables projected expandability.

The two internationally recognized, vendor-independent standard protocol suites are the **Transmission Control Protocol/Internet Protocol (TCP/IP) suite** and the **Open System Interconnection (OSI) suite**. They are both open standards, which mean they are not proprietary. Protocol software resides in the computer memory or in the memory of the **Network Interface Card (NIC)**. When data are ready for transmission, this protocol software is executed.

Protocol Suite: - This is a collection of protocols that work together to form a single system to handle networking devices. It can be defined as a set of many layers, and is usually part of the operating system kernel on machines connected to the internet.

Routable Protocol: - this is the ability of a protocol to communicate across the router. This type of protocol needs extra layers to handle the routing feature.

Non Routable Protocol: - This is the type of protocol that cannot be routed and are limited to smaller LANS. These are as large as they are today. Non-routable protocols are usually faster and provide better transfer speeds due to fewer overheads.

Connectionless Protocol: - This is a type of protocol that sent out data across the network with no feedback as to whether it arrived at the destination device or not. This type of protocol is mainly used when there is a need to send data to multiple computers at once or where high speed is needed.

Connection-Oriented Protocol: - this is a type of protocol employ when you need to ensure that certain data arrives at its destination. Protocols send acknowledgement to show that data was received successfully.

2.10 Popular Protocol Suites

The following are some popular protocol suites

- i. TCP/IP
- ii. IPX/SPX

TCP/IP Protocol Suites

Transmission Control Protocol / Internet Protocol (TCP/IP)

This protocol suite is also known as internet protocol. This is a suite of industry-standard and protocol. The TCP/IP suite is made up of many protocols. It has a broad feature set due to its large number of open standard protocols.

Internet Protocol

IP is the standard that defines the manner in which the network layers of two hosts interact. These hosts may be on the same network or reside on physically distinct heterogeneous networks. IP provides a connectionless, unreliable, best-effort packet delivery service.

TCP/IP and the OSI Model

This original design for TCP/IP was started long before the OSI model was developed. Instead of OSI seven layer model, TCP/IP was based on DOD (department of defense) model with four layers. The four layers can be loosely method to the OSI model in the following ways:

Network Access Layer

This layer corresponds to the physical and data link layer of the OSI model. When TCP/IP was developed, it was made to use existing standards for these two layers so it could work with such protocols as Ethernet and token ring.

Internet Layer

This layer of the DOD model roughly matches up with the network layer of the OSI model. Both of these layers are responsible for moving data to other devices on the network. Internet protocol (IP) is mainly responsible for the job.

Host-To-Host Layer

This one is similar to the transport layer OSI model. The job of both of those layers is to communicate between peers on the network. As a result of this, almost all devices on a TCP/IP network are considered hosts, whether they are workstation, server, or network-attached printer.

Process/Application Layer

This fourth layer does the same job as the top three of the OSI model, which is to provide network services.

TCP/IP Protocols and how they correspond to the OSI Model.

TCP/IP Address

This is an address that is usually set by the administrator, though it is sometimes automatically set by the network protocol suite used, which allow two computers on a network to communicate.

This address is unique 4-byte address is dotted notation for example 56.88.1.231. IP addresses are handed out by a single organization called interNIC, so each computer has its own unique address. IP addresses are divided into classes. IP addresses classes are used to segment the pool of addresses into size corresponding to various organization sizes.

Classes of IP Address

Class A: Class A address have one byte for the network and three byte for the host. For example, the address 56.88.1.231 has a network number of 56, and the remaining number signify the host. The first class of class a network addresses is always between 1 and 127.

Class B: Class B address have 2 bytes for the network address and the remaining two for the host address. With this arrangement each class b network can have to 65,000 hosts. The first byte of class b addresses is always between 128 and 191.

Class C: class c address is the most common. They use the first 3 bytes of the address for the network portion and the final byte for the host. This allows for a great number of networks given out with more than 250 hosts. Class c address always has the first byte between 192 and 223.

Subnet Mask

Subnet mask is responsible for separating the IP address into the host portion and the network portion. It completes computer's address on a TCP/IP network. For example, class A has one byte for the network and three byte for the host. It has the subnet mask of 255.0.0.0. The 255 in the first byte signify the network address.

Standard Suite Protocols

Subnet Mask	Network Class
255.0.0.0	Class A
255.255.0.0	Class B
255.255.255.0	Class C

TCP/IP Suite Protocols

Below are some of the protocol contain in TCP/IP

Internet Protocol

The internet protocol (IP) is a connectionless that sits in the network layer of OSI model. An IP header is attached to each packet (data gram) and includes the source address, destination address, and other information used by them receiving host.

Function of IP

- i. It addresses and route packet according through the network
- ii. It fragment and reassemble packets that were slit in transmit

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) Provides error reporting for IP. IP can not detect error when an error occurs on the network. ICMP is up to report errors back to the host that sent IP packet. If a device cannot forward in IP packet on the next network in this journey, than it will send back a message to the source of that packet using ICMP to explain the error. Some of common types of errors that ICMP can report are:

- i. Destination unreachable
- ii. Congestion
- iii. Echo request
- iv. Echo reply

Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) are two routing protocols in the internet protocols suite. RIP use the number of routers (hops) between the originating computer and the destination to decide the best way to route a packet. OSPE is configured to figure in the hop count, the speed the connection between the hops and the loading balancing to calculate the best way to route packet.

Transmission Control Protocol

This is a connection-oriented protocol that corresponds to the transport layer of OSI model. TCP opens and maintains a connection between two communication hosts on a network.

When an IP packet is sent between them, a TCP header that contains flow control, sequencing, and error checking is added to the packet.

Each virtual connection to a host is given a port number so data grams being sent to the host go to the correct virtual connection. For example, an internet web server uses 80, while mail server usually post 25.

User Datagram Protocol

This is the connectionless transport protocol and is used when the overhead of TCP is not needed. UDP is responsible for transporting data gram. UDP uses port number (53) similar to TCP, except that do not correspond to a virtual connection, but to a process on the other host.

Address Resolution Protocol

This is the protocol that handles the conversion of the address by sending out a discovery packet. This protocol allows computers to communicate with another on a network. The discovery packet is sent out to the broadcast MAC address so every device on the network receives it. The packet contains the request for the owner of the IP address. When the receiving computer with the IP gets the discovery packet, it replies to the originator to let the originator know that it owns that IP. ARP maintains a list of IP and MAC address so as discovery packet is not needed every times communication takes place.

Domain Name System (DNS)

This is the system that converts user-friendly name such as <http://www.ebeconsult.com> to the correct IP address. DNS is a distribution database hierarchy maintained by different organization. There are a number of maintain DNS servers that point clients to the more specific server at each company.

File Transfer Protocol

This is the file-sharing protocol most commonly used in a TCP/IP environment. This protocol allows user remotely log on to other computer on a network and browse, download and upload file. One of the main reasons FTP is still very popular is that it is platform independent.

Simple Mail Transfer Protocol (SMTP)

SMTP is responsible for making sure that called e-mail is delivered. SMTP only handles the delivery of mail server and between servers.

Dynamic Host Conglutination Protocol (DHCP)

DHCP is responsible for automatic IP addressing. Instead of configuration each device on the network manually, the administration does it once for the entire network on the DHCP server. DHCP server is given a range of IP address to hand out to network device. When a computer comes online to the network, it sends out a DHCP request. The nearest DHCP server responds with all the information to set up TCP/IP on the new client.

TELNET

TELNET allows a user to remotely log to another computer and run application

Network File System

This is an advance way to share file and disk that FTP and telnet require you to use a separate client, NFS allows user to connect to notebook drive and use them as if they were local hard drives.

IPX/SP Protocol

Internet work packet exchange/sequence packet exchange protocol suite was developed and maintained by novel, inc. IPX/SP protocol suite everything from file and disk sharing to message and application services. IPX/SP functionality is aimed toward requesting and receiving services from large server.

IPX/SP network makes use of the server-centric NetWare operating system. The IPX/SP protocol and network application are written so the network environment is comfortable for users. IPX/SP suite is very functional because it is modular. That is, piece can be removed and replace by protocols fro other suite. For example you could remove the main IPX/SP protocol and replace them with other user datagram protocol (UDP) and TCP. Because it is design in modular form, it allows the protocol suite to be very adaptable to other need and permit IPX/SP to use other types of network.

One of the features of the IPX/SP protocol is its ease of use and administration. IPX/SP need no manual addressing for workstation to function. The only real addressing needs is on the NetWare server, and is just to pick a network address not found on any other connected network. This information is automatically passed on to the network client.

IPX/SP protocol can be divided into

- i. Lower-layer protocol
- ii. Middle IPX/SP and
- iii. Upper layer IPX/SP

(i) Lower-Layer Protocol

In the IPX/SP suite correspond to the link layer of the OSI model. There are no protocols in the physical layer of the IPX/SP suite because it can utilize any popular physical network types, such as Ethernet, token ring, or FDDI.

The protocols that work at the data link layer are responsible for media access and interfacing to the network card. There are two protocols in this layer namely:

- a. Multiple link interface driver protocol
- b. Link support layer protocol

(a) Multiple Link Interface Driver Protocol

These protocols concerned with media access. MLID is piece of software that makes the network card in the computer work that is a network interface board specification this driver is written to a certain specification called open data link interface IDO specification.

(b) Link Support Layer Protocol

This layer is responsible for making sure data goes to the correct upper-layer protocol. It also makes sure that multiple protocol stacks is load. It serves as an interface between mild and the upper-layer protocol.

(ii) Middle IPX/SP Suite Protocol

This middle protocol is the IPX/SP suite map to the network and transport layers of the OSI model. There are responsible for transferring data between devices on the network, as well as carrying some routing functionality. The protocol that is in middle IPX/SP suite protocol is:

- a. IPX
- b. SPX
- c. NLSP
- d. RIP

(a) Internet Work Packet Exchange

This protocol corresponds to the network layer of the OSI model (IPX) protocol corresponds for connectionless data service. It handles the routing of data cross an internet work, as well as the handle network addressing.

In a NetWare most data transfer between client and server are handling IPX protocol. An IPX address is a combination of the physical MAC address on the network card and a logically assigned network address. Example of such is 123456789ABCD. Socket number in IPX/SP is equivalent of TCP/IP port number. IPX decide the best to a remote device by using one of the built in routing protocols.

(b) Sequenced Packet Exchange (SPX)

SPX is a connection oriented with sequencing and error control. SPX makes up for the inherent unreliability of IPX and because of this reason; SPX rides on tops of IPX to this extra functionality in a similar way that TCP rides on top of IP in the TCP/IP suite. SPX is mainly used when a connection is made across an internet work device such as a router, or to a print server to service a printing request. SPX uses acknowledgment to ensure delivery. SPX also establishes virtual circuit called connections, between devices. Each connection has its on connection id to distinguish it. Connection ids can be tied to upper-layer process.

(c) Network Link Services Protocol (NLSP)

This protocol uses a link state mechanism to choose the best. NLSP broadcast routing information when a change occurs, not at preset interval. NLSP uses far less bandwidth

(d) Routing Information Protocol (RIP)

This is a protocol that is used by IPX to decide the best route through an internet work. It uses the distance vector method to calculate hops count (i.e. it counts number of times a piece of data crosses a route before reaching its destination) and then crosses the route with the number of hops.

(iii) Upper-Layer IPX/SP Protocol

The upper-layer protocol in IPX/SP comprises of:

- i. Network core protocol
- ii. Service access protocol

Network core protocol corresponds to the transport, session, presentation and application layers in ISO model while service access protocol corresponds to session layer in ISO model.

(i) Network Core Protocol

This is the “**language**” spoken between a NetWare client and a server.

This protocol handles most NetWare services such as file services, printing; file locking, resource access and synchronization. NCP functions as the following four layers of the OSI model:

- i. Transport layer –it connects services with segment sequencing, error control and flow control.
- ii. Session layer-it controls the movement of data from transport layer to presentation layer.
- iii. Presentation layer-it translates character.

- iv. Application layer –it serves as application and service interface to the end-user application.

(ii) Service Access Protocol

This protocol allows each computer sharing a resource on the network to send out sap packet containing information about the resource and where it is located.

2.11 Network Type

Network type combine physical layer with the physical topology to form the basic network. The different types of network are

ARCNET

Ethernet

Token Ring

FDDI

Characteristics of Network Types

- a. Maximum number of clients
- b. Speed
- c. Distance
- d. Media access type

Types of Network

2.11.1 ARCNET

ARCNET (Attached Resource Computer Network): it is the oldest network types. Data point corporation created it in 1977.

ARCNET uses passing in combination with a star/bus topology to transmit data at 2.5mbps. ARCNET was designed to be a simple, inexpensive, and reliable topology. ARCNET utilizes UTP or coaxial cable hubs as many 225 computers.

Characteristics of ARCNET

- i. Topology- star to bus
- ii. Transmission speed: 2.5mbps or 20 225
- iii. Maximum number of network nodes:225
- iv. Cable types:rg-62, 90 ohm or coaxial, UTP, and optic
- v. Maximum network length: 20,000 feet
- vi. Maximum segment length
- vii. Coaxial cable 400 feet
- viii. UTP cable:400 feet
- ix. Fiber optic cable: 11,500 feet

Advantages of ARCNET

- i. Reliable, mature technology
- ii. Uses simple technology that is easily installed
- iii. Operates over several cable types

Disadvantages of ARCNET

- i. Limited to 255 devices
- ii. Operate at low speed of 2.5mbps

2.11.2 Ethernet

Ethernet is a network standard developed by Intel, digital and Xerox. It offers for a variety protocols and computer platform. Ethernet is available in three main standards namely:

- i. 10 Base-5
- ii. 10 Base-2
- iii. 10 Base-T

10 Base-5: 10 Base-5 is also thick Ethernet. It makes use of RG-8 cable which uses external transceiver and a vampire clamp that fastens directly into the cable, which is wired in a linear bus. 10 base-5 can have five segments with four repeaters, and only three segments can have workstation.

Characteristics of 10 Base-5 Networks

- i. Topology: bus
- ii. Media access method: CSMA/CD
- iii. Cable type: 50 ohm thickness coax cable
- iv. Transmission speed 10 mbps
- v. Maximum number of network nodes: 300
- vi. Maximum number of nodes per segment: 100
- vii. Maximum network of segment: 5:3 of which have connected nodes.
- viii. Maximum network length 2,500 meters
- ix. Maximum segment length: 500 meters

10 Base-2:- This was developed as one of the alternatives to 10 Base-5 because the rg-8 cable used in 10 Base-5 is rigid and difficult to work with 10 base-2 uses RG-58 cable along with T segment supporting as many as 30 devices, which must be 1.5 feet apart.

Characteristics of 10 Base-2 Networks

- i. Topology- bus
- ii. Media access method: CSMA/CD
- iii. Cable type: 50 ohm, rg-58 coax cable
- iv. Transmission speed: 10 mbps
- v. Maximum number of network nodes: 90
- vi. Maximum number of nodes per segment: 30
- vii. Maximum number of segment: 5:3 of which have connected nodes.
- viii. Maximum network length: 925 meters
- ix. Maximum segment length: 185 meters

10 Base-T: - This standard utilizes 22 AWG UTP cables with RJ-45 jacks arrange in a star configuration. This configuration eliminates the single point of failure problem associated with the bus configuration. Each device has a separate UTP cable connection it to the hub.

The workstation must be at least 2 feet apart and no more than 328 feet from the hub. It follows five segments with u to 512 device standard. Network can be segment in order to provide network expansion i.e smaller network are connected using bridges or routers, gives larger network.

Characteristics of 10 Base-T

- i. Topology-star
- ii. Media access method-CSMA/CD
- iii. Cable types categories 3-5 UTP
- iv. Transmission speed: 10 MBPS
- v. Minimum number of network nodes: 1,024
- vi. Minimum number of node per segment: 1
- vii. Minimum number of segment 1,042
- viii. Minimum distance between nodes: 2.5 minimum lengths
- ix. Minimum segment length: 100 meters

10 Base-100:- 10 base-100 is also known as fast Ethernet, which can transmit at either 10mbps or 100mbps. Fast Ethernet can transmit across UTP or fiber optic. 10 base-100 has three standards, which were developed based on the type of cable used. These standards are:

- i. 10 Base-100: TX using two pair categories 5 UTP and STP cable.
- ii. 10 Base-100:- T4 is using for pair categories 3 through 5 UTP cable.
- iii. 10 Base-100:- T uses fiber cable.

This standard allows for several options with base 100. For 100mbps 10 Base 100, the adapter and hub must be capable of 100mbps transfer rate. Fiber optic provide for greater cable lengths at 100mbps than UTP cable. UTP, you limited to two hubs between workstations, and the hub A must be connected using a 5-meter cable. Fiber optic allows a distance of 400 meter between hubs.

Characteristics of 10 Base-100

- i. Topology-star
- ii. Media access method: CSMA.CD
- iii. Cable types:
 - 10 base-100:-TX: categories 5 UTP
 - 10 base-100:-T4: categories 3-5 UTP
 - 10 base-100:-FX: categories optic
- iv. Transmission speed: 10 mbps
- v. Minimum number of nodes per segment
- vi. Minimum number of network nodes 1,042
- vii. Minimum number of segment 1,042
- viii. Minimum distance between nodes: 2.5 meter
- ix. Minimum segment length: 100 meter
 - 100 Base-TX: 100 meters
 - 100 Base-TX: 100 meters
 - 100 Base-TX: 2 meters

Advantages of Ethernet

- i. Flexible standards allowing a variety of equipment
- ii. Inexpensive network option
- iii. High-speed network that can operate at 10 or 100 mbps
- iv. Easily expanded

Disadvantage of Ethernet

- i. Performance degradation under network load

2.11.3 Token Ring

This type of network token passing in a physical star configuration connected in a ring hub. It allows devices to have varying priority in accessing the network media.

Characteristics of Token Ring

- ii. Topology: physical star, logical ring
- iii. Media access method token passing
- iv. Cable types: SIP, UTP, and fiber optic
- v. Transmission speed 4 or 16Mbps
- vi. Minimum number of network nodes: UTP: 72 and STP: 260
- vii. Maximum number of nodes segment: varies according to the hub
- viii. Maximum number of segment: 33
- ix. Maximum distance between nodes: 2.5 meter
- x. Maximum network length: no maximum length
- xi. Maximum segment length
 - UTP: 45 meters
 - STP: 101 meters
 - Frame size
 - Mbps 4k
 - 16 mbps: 6k

Advantages of Token Ring

- i. Performance under heavy load
- ii. Uses intelligent
- iii. High-speed network capable of 4 or 6 Mbps.

Disadvantage of Token Ring

- i. Expensive
- ii. Difficult to troubleshoot

2.11.4 Fiber Distribution Data Interface (FDDI)

FDDI is a token-passing ring network similar to token ring out running over a fiber-optic cable. FDDI uses concentrators to connect devices. Because it utilizes fiber-optic cable, it is capable of transmitting at the rate of 100 mbps. FDDI is a token-passing network over the ring, but the method used in FDDI is much different from token –ring. FDDI allows many frames to be transmitted simultaneously. This is possible because the station that control the token can send several frames without waiting for the previous frame to complete it journey around the ring. The following terms are common to FDDI and they are help in increasing the speed of the network.

- i. Synchronous frame
- ii. Multi frame dialog
- iii. Wrapping

(i) Synchronous Frame: - this is a process of assigning transmission times to certain devices.

(ii) Multi Frame Dialog:-this is a process of two devices to transmit to one another without interference.

(iii) Wrapping: - this is the connection made between two rings before and after the break of cable

Characteristics of FDDI

- i. Topology-ring
- ii. Media access method: token passing
- iii. Cable type
- iv. Transmission speed: 100mbps
- v. Maximum of network nodes: 500
- vi. Maximum number of nodes per segment: no maximum number of node per segment
- vii. Maximum number of segment- node
- viii. Maximum network length: 100 kilometers
- ix. Maximum segment length: no maximum segment length

Advantages of FDDI

- i. FDDI is the fastest network and is capable of 100mbps transfers
- ii. Fiber-optic cable allows signal travel great distance, up to 200 kilometers.
- iii. Dual rings provide a higher level of fault tolerance.

Disadvantages of FDDI

- i. Expensive cable and equipment is required
- ii. Workstation can be single point of failure for both rings
- iii. FDDI requires a high level of expertise to install, troubleshoot, and maintain.

X CHAPTER THREE

3.0 NETWORK DESIGN AND CONFIGURATION

3.1 Systems Analysis and Design

The semester report of the Math/Computer department is usually done by computer; this is to say that student's data are input into the computer system to form a master record of all students' results, which is then printed out as hard copy.

The introduction of the computer networking will automatically present not only students result, but also give the lecturer the ease to know the exact students in the department, from any of the computers: which is the basis of the analysis i.e. concerned with the study and gathering of data about the existing systems for improvement, the identification of problems and difficulties encountered by the member of staff responsible for the production of the semester results and accessibility to the results.

The systems analysis in this regard is concerned with producing a more flexible, users friendly and accurate package in place of the existing system.

3.2 Analysis of the Existing System

Before designing a new or enhanced information system, sufficient and proper grasp of the existing system and information flow should be made; this is done by conducting interview with students and staff of the institution or organization.

The interview and observation gathered from the case study were:

In the department, there are only twenty-five (23) computers;

- One computer in the H.O.D's office.
- One computer in the secretary's office.
- One computer in the examiner's office
- Twenty computers in the computer room.

It was interesting to find out that of all these computers, none was connected to the other. After a test or exam in the department, lecturers mark the scripts, record the results onto a paper and then input the student's names and corresponding results into the computer system (optional). The lecturer now sends a copy of these result sheets to the examination officer. The examination officer now copies out these results onto his records i.e. paper or computer system.

3.3 Problem of the Existing System

Before any problem can be solved, there must be a clear definition of such problem, else the wrong solution will be applied and the whole objective will be defeated. However, the following questions may help in defining the problem:

1. What is the problem?
2. Detail of the problem?
3. How significant is the problem?
4. What are the feasible solutions to the problem?

What is the Problem?

In the department of math/computer, the problems is the non-networking of computers, to ease the execution of jobs by the lecturers and staff of the department in the process of trying to organize lectures for the students and other related school work.

Detail of the Problem

Using this scenario to explain, a student goes to the exam officer to check for her results for the year, the lecturer now discovers that there are some missing results, rather than use the computer in his office to check for the missing results, the student is been asked to write an application letter requesting for the results from the lecturer involved. In the case where the lecturer is not available, that student can not get access to his/her results, thereby delaying the progress of the student.

How Significant is the Problem?

The significant of the problem can be outlined as:

- Rushing from one computer to another in your office; attending to several different jobs at various locations.
- Moving files that needs printing from one pc that you happen to be working on, to the pc that is connected to the printer.
- A student having to wait for the exams officer before getting access to his or her result.
- A lecturer with his system can not get the names of the entire student in the department, unless he goes to the secretary office.
- The H.O.D not having access to all the names of lecturers and staff in his department until he calls the secretary.

The Feasible Solution

The only possible solution in the case of non-interaction between different computers in an institution like a university department or an organization would be a computer networking (LAN), where one would be in his office and get access to any kind of information relating to the department, as and when required.

3.4 Introduction of Local Area Network (LAN)

Successful implementation of a LAN requires careful planning. The primary networking rule is that “the network will always outgrow initial expectation”. Network are modular, once a network is built on a solid base, additional network needs can be easily added.

The following procedures are carried out in the implementation of the LAN. These are to ensure that the network meets standards set by the international standard organization (ISO), the open systems interconnection (OSI) seven layer reference model.

- Determination of topology.
- Determination of network cabling.
- Installation of network interface card.
- Location and connection of hub.
- Loading and configuration of server/workstation operating system.
- Creation of user environment and implementation of security.

Choice of Cables

The first step taken in the determination of the choice of cables (otherwise called topology), involved a careful assessment and measurement of the site.

Next, a cabling scheme should be analyzed, and because future expansion is important in any network design, a topology that would ease this problem was chosen, so the STAR topology was decided upon, this enable ease of expansion and troubleshooting.

There are two main factors that determine ones choice of cables:

- ✓ Size of wire.
- ✓ Speed of transmission.

The use of UTP, category 5 cables was decided upon; this supports the star topology and upgrading.

3.5 LAN Architecture

In any LAN, there are three roles the computer plays:

CLIENTS: Computer which use but do not provide network resources.

PEERS: Computer which uses and also provides network resources.

SERVERS: Computer which only provide network resources.

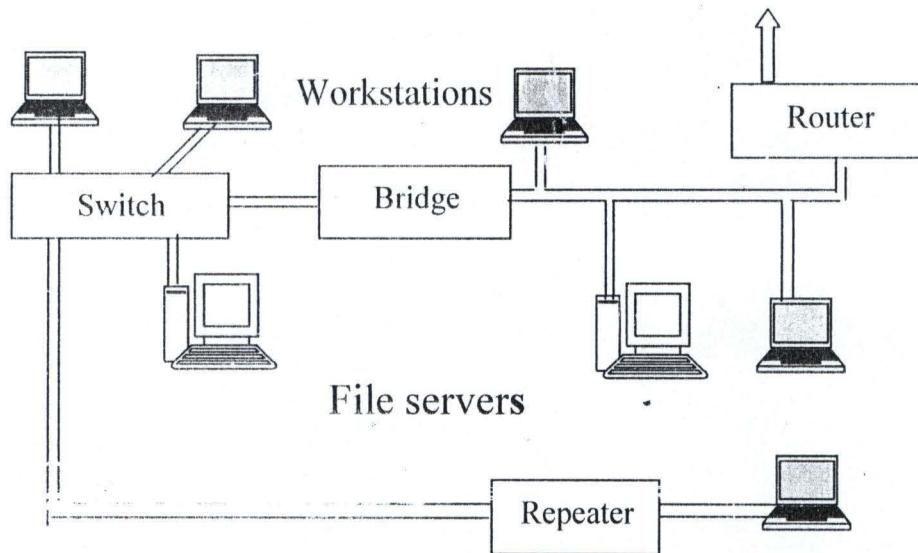
Client-Server Network Architecture

Otherwise called the multi-user network emerged as the need to connect more systems together. Consists of a central computer (called the server) to which all other computers (clients or workstations) are connected.

Servers provide security and administration of the network; they are usually more powerful than the clients in terms of speed, memory and hard disk capacity. Allow for centralization of service and maintains a strong control over the network environment, are good for e-mail, data organization and internet access.

3.6 Networking Hardware

Networking Hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communication within the network.



LAN Devices

Local area network devices are:

File Server

Network Interface Card

Repeater

Bridges

Ethernet hubs

Switches

Modem

Routers

Gateways

Multiplexers

Workstation

Repeater: - Repeater is a device used to boost a network signal as it passes through. Repeaters are normally two-port boxes that connect two segments. It works at the physical layer to generate the electrical signal on the network media.

Advantage of Repeater

- i. Repeater easily extend length of a network
- ii. They require no processing overhead, so very. If nay, performance degradation occurs.
- iii. You can connect segment from the same network type that use different types of cable.

Disadvantages of Repeaters

- i. Repeater can not be used to connect segment of different network types.
- ii. They can not to segment traffic on a network to reduce congestion.
- iii. Many types of network have limits on the number of repeaters that used at once.

Bridges: - this is a device that allows the segmentation of a large network into two smaller, more efficient networks. It monitors information traffic on both sides of the network so that it can pass packet of information to the correct location.

Advantages of Bridges

- i. Bridge extend network segment by connecting them together to makes one logical network
- ii. They segment traffic between networks by filtering data it does not need to pass.
- iii. Special translation bridges can connect different network type together

Modem: - This is converting digital information from the sender end to analog information and vice-versa

Router: - This is a device that translates information from one network to another. It selects the best path to router a message based on the destination address and original.

Gateways: - The computer hardware and software that connect networks that use different protocols (rules hardware and software use to communicate), or that transfer data between two incompatible application on a network. The gateway reformats data so that it is acceptable to the receiving network or application.

Hub: A hardware devices that contains multiple independent but connected modules of network and internetwork equipment.

Switch: A concentrator is a device that provides a central connection point for cable from workstations, servers and peripherals. Most concentrators contain the ability to amplify the electrical signal they receive.

File Server: A computer connected to the network that contain primary/application and shares them as requested with the other computers on the network.

Workstation: A computer connected to a network at which uses interact with software stored on the network.

Workgroup: A collection of workstations and servers on a LAN that are configured to communicate and exchange data with one another.

Multiplexers: A device that allows multiple logical signals to be transmitted simultaneously across a single physical channel.

3.7 Hardware Requirement

These are the hardware require in order to implement the network.

This can be classified into two:

- Server computer
- Client computer

3.7.1 Hardware Specification for Server Computer System

Pentium-IV 2.5 GHz with MMX technology

512 SD-RAM

52 x CD ROM drive

3.5 floppy drive

14`` monitor

Network interface card

Modem

Microsoft windows XP

Keyboard

Timer software

Printer

Scanner

40 GB hard disk drives

3.7.2 Hardware Specification for Client Computer System

Pentium III 450 MMX

256 SD-RAM

20GB hard drive

48 x CD ROM drive

3.5 floppy drive

14" monitor

Mouse + pad

Keyboard

Timer software

Microsoft windows XP

3.8 LAN Configuration

- Unplug your computer system
- Put the Ethernet card (network card on any available PCI slot)
- Plug your computer and put it on
- Follow the screen instruction when the computer detect your network and install the card with the appropriate driver.
- Click on start, setting and double click on network. Configure the following:
 - Click on add button
 - Click on the protocol, click on the add button, select TCP/IP protocol, click ok.
 - By doing this, it will allow you to set some properties on your network card.
 - Click on the TCP/IP, and then click on the properties
 - Click IP button
 - On the primary IP, type the IP address e.g. 10.1.1.1 and also type the subnet address e.g. 255.0.0.1 click ok

- Click on file/printer button. This will allow you to share the file and printer.
- Check the facility that will allow sharing file and folder
- Check the facility that will allow share the printer
- Click on the identification tab
- Enter the name of the computer, the work group and the description.
Note the name of the work group must be the same in order to make the system on the same network see one another
- Click ok and reboot your computer system
- When computer system has restarted, computer will recognize your network.

It will allow you to enter password, which will give you access to the network.

On the desktop, double click on the network place icon and you will see the computer icon together with workgroup. If you do not see the computer icon, double on workgroup and it will display the computer icon.

NOTE: To confirm whether the network is well configured, you click on run, type this command ping follow by the IP address then press enter key e.g. ping 10.1.1.1 it will display the configuration of the computer.

CHAPTER FOUR

4.0 NETWORK IMPLEMENTATION

Network Services, Administration, Management and Troubleshooting

4.1 Network Services

Networks are meant to make us more productive by providing services to make us more efficient. Some common services provide by network are:

- i. File servicesp-0;
- ii. Print services
- iii. Message services
- iv. Director services
- v. Application services

(i) File Services

The primary reason for networking computer system is for the files services that a network can provide. Instead of coping file to a floppy disk, user can easily share file.

The following jobs use file services:

- a. File transfer
- b. File storage and migration
- c. File update synchronization
- d. Archiving

(a) File Transfer

Transferring file electronically is the simplest and the most common services on the network. The ability to share file and information across a network allow user to share any information they need and this make them more productive than ever. There are other ways to share file, such as coping files to a removable storage device such as floppy or a zip drive. This method is only possible when all users are allocated in same office. When users are spread through out the country and world, this is not an option. Reliable file transfer across the network then become a more noticeable important services.

(b) File Storage and Migration

Data can be store on many different media, such as hard disk, CD-ROM and magnetic tape. Data is said to be store **on-line**, **off-line** or **near -line** upon the media on which it is stored.

In **on-line storage**, it stores information that's readily available on a server. Central data storage on a server is one of the primary users of a network. User can access this data any time. The devices most commonly used for on-line storage in hard drive.

Off-line storage, data is put on magnetic tape so that it can be loaded back when needed. Off-line storage devices provide provide a low-cost solution to storing data compare to on -line storage. Suppose you need to keep a large amount of data available to user and user can not afford to buy the necessary amount of space on hard disks.

Near-line storage is a way to keep data migration off expensive hard disk but close enough to let user access it. This may be done by using such things as jukeboxes with large numbers of tapes or optical disks. They can automatically put the needed data online. Data is migration when it is moved from one form off storage to another.

(c) File Update Synchronization

This network services keeps track of different versions of the same file. If two clients open a file at the same time and try to save the change that each have made, one file will overwrite the other. File update synchronization tries co-ordinate these change.

(d) Archiving

Archiving is the process of backing up data in case of hard disk failure. Several machine both client and servers can back up using the same hardware and software from one location. Using these software and hardware, the administrator can schedule all computer on the network to be backed up from a location at scheduled interval network will need to be resolved. Old e-mail message will have to be deleted and the space they occupy made available to the system. The type of procedure will have to be performing as user added to or deleted from the network.

(ii) Print Services

Ability to share print devices is another service that network provides. Before the invention of computer network, user had to have a printer attached to their workstation.

This was costly especially if a user needs to print multiple types of form or paper, since they would need a different printer for each.

With network print service companies need only buy small number of printers and share them among all their users.

Other features of print services is queue-based printing and fax services. Queue-based printing allows client's application to spool the print job off to a network server. Therefore the application thinks that the job has been printed and let the user continue to work. While the user continues to work, the network server handles sending the job to the print device.

(iii) Message Services

The network also allows us to send information across many computers. With these facilities, you can send video, sound, document and almost any other type of data.

(iv) Directory Services:

With directory services, it enables the user to maintain information about the entire object in your network. An object is anything you can store information about, such as users, printers, share resources, server etc.

(v) Application Services

Application Services are basically client / server process. The server is providing the application server. With application services, a small application is loaded on the client computer, and the main application and data is loaded on the server. The small application on the client computer is just a front-end to give the user an interface.

It does not process any job of its own. The client application sends queries to the server and let it do the processing. The server then returns the requested information.

4.2 Network Administration

Network administration has to do with Privacy and security. Network security is the term used to prevent unauthorized user to have access to the network and its resources. In network we have two level securities namely:

- i. Share-level security and
- ii. User-level security

(i) Share-level Security: this relies on a single password to access the resource and its workgroup.

(ii) User-Level Security: This requires a user name and password to log on the resources. Users-level security is used domains especially Windows 95 computer in a domain and window NT work stations and server in a workgroup or domain.

4.3 Network Management

Network management is the act of managing the network to be efficient over a period of time. Network management has two goals and these are:

- i. To prevent problem where possible
- ii. To prevent problem that most likely occurs.

Network management has to do with the following:

- i. Monitor and control hard disk space
- ii. Monitor network load and performance
- iii. Add and maintain user login information and workstation information
- iv. Monitor and reset network devices
- v. Perform regular maintenance on software and data store in the servers.
- vi. Make regular back up of data and programs stored.

(i) Managing Hard Disk Space: the server's disk is one of the network's primary commodities. File for network-based program are stored on the disk. Print job that are sent from workstation to network printers are stored on the disk queue before printed. And in some network, users' files and data are stored on the network hard disk. If the disk space has filled up, then print job can't be printed and user cannot save their data files. Data file may also be corrupted since data manipulation can't be accomplished.

If the hard disk space must be available at all time for legitimate users of the network, the hard disk space must be checked everyday.

Growth of user's file should be controlled to ensure that as single user does not monopolize the hard disk. Unwanted file must be deleted and when heavy, disk defragmentation must be used on such hard disk. Files could be back-up and the disk can be reformatted.

(ii) Maintaining User and Workstation Information:

Network user has network identification number that can be used to monitor security and the growth of the network. A network manager must keep a log of information about the network users such as login id, node, address, network address, and some personal information such as phone, name and address.

Also, network cabling, workstation type, configuration, and purpose of use should be kept in record. This information can be stored in a database. It can be used to detect problems with data delivery, make change to user's profiles, workstation profiles, account, and support other tasks.

(iii) Monitoring and resetting network devices:

A network consists not only of server and workstation but also a printer, input devices such as scanners and other machines. Some devices may need to be reset daily (such as gateway), while other devices require periodic maintenance. Some types of electronic mail router need to be monitored hourly to make sure they are working properly. In either case, all devices should be monitored periodically, and a schedule of reset and maintenance should be created to ensure that all network devices work when a user need them.

(iv) Maintaining the software:-Application software, especially database application, needs regular maintenance to rebuild files and space left empty by deleted records.

Space not used must be made available to the system, and in many cases index files will have to be rebuilt.

Additionally, as new software upgrade become available, they need to be placed in the network. After an update is placed in the network, file clean up may have to take place. Also, any inappropriateness between the new software on the hard disk and provide efficient access to data on the server's hard disk. Some networks also make use of software o repack files on the hard disk and eliminate file fragmentation.

(v) Monitoring Server Performance: - The performance of the LAN server will determine how quickly the server can deliver data to the user. The server must be monitored to ensure they are fragmented at their peak.

Factor that Determined the Respond of a Server

- i. The number of user that are attached to the system
- ii. The server's main memory

(i) The number of user that are attached to the system:

Working with more users will slow the response time. If a specific application has a large number of users, the server that contains the application could be dedicated to server only that program.

Other servers could be used to distribute the load of other programs on the system.

(ii) The server's main memory:

The server's main memory should be monitored to make sure that it is used efficiently. Many server uses RAM as disk buffers. These cannot function if there is not sufficiently memory to run the network operating system and the buffers. If a server has to reduce the number of buffers require for I/O, the overall performance of the will suffer.

Most networks provide tools that show statistical data about the use of the network and outline and potential problems. An experienced network administrator uses these statistics to ensure that the network operates at It peak at all time.

4.4 Network Troubleshooting

Network troubleshooting is the act of detecting fault/problem in a computer system, isolating the problem and provides a necessary solution to the problem in order to prevent it from re-occurring again.

The following are the steps in network troubleshooting

- i. Set the problem's priority
- ii. Collect information
- iii. Determine possible causes
- iv. Isolate the cause
- v. Study the result

(i) Set the problem's priority:- priority need to come to pass in network troubleshooting because every one wanted his/her computer fixed right away.

You have to prioritize problems based on things such as the time necessary to fix problem, importance and who has the problem.

(ii) Collect information:-once you have decided which problem to concentrate on, you must then collect information to help to isolate the trouble. Here, users are a good resource of information, since they are using the network all the time. For example, a simple question such as “what problems have you noticed with network?” this may yield all sort of information.

(iii) Determine possible causes: - at this point, you should be starting to determine the source of the problem base on the information you collected. You may not know the exact problem, yet you have a small list of possible causes.

(iv) Isolate the cause:-at this point, try your most likely solution to see if it fixes the problem.

(v) Study the result:-carefully study the results for each fix you try. See if the problem was fixed or change in any way. If the problem was not fixed by your solution, keep trying the ideas on your list until either its fixed or you run out of ideas.

Equipment Used For Network Troubleshooting

The following are the equipment used for networking troubleshooting:

- i. Digital volt meter
- ii. Time-domain reflects meter (TDRS)
- iii. Advance cable testers

- iv. Oscilloscopes
- v. Network monitor
- vi. Protocol analyzers

(I) Digital Volt Meter: - this is a basic electronic measuring device. It is used to check the amount of voltage going through a circuit.

(II) Time-Domain Reflects Meters

DVM can tell you if a break exists in the cable but a time domain electrometer can tell you exactly where the break occurred. The TDR uses sonar-like pulse that is sent down the cable. The signal bounces back from a break in the cable. The TDR calculate the time signal took to go down the cable and back, and compute the distance.

(III) Advance Cable Testers

Advanced cable tester can be used to display information such as:

- i. Frame count
- ii. Congestion errors
- iii. Network utilization
- iv. Late collision
- v. CRC errors
- vi. Network-level statistic
- vii. Protocol statistic
- viii. Information concerning which application is using the network

(IV) Oscilloscopes

Oscilloscope is used to show voltage over time. It can be used to check for:

- i. Shorts
- ii. Crimps in the cable
- iii. Breaks in the cable
- iv. Attenuation

(V) Network Monitors

Are software program that track and show information about a network. They can generate reports showing utilization, errors and overall traffic patterns on your network. By watching the growth, you can predict when problems may rise and take productive steps before they do.

X(VI) Protocol Analyzers

Is a tool used in debugging problem on a network? It is also known as network analyzer or sniffed. Protocol analyzer can be hardware only or a combination of hardware and software. They collect information by examining all data going across the network and decoding the information for display.

CHAPTER FIVE

5.0 SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

The design and implementation of computer networking (Local Area Network) has proved itself superior to the manual method of information transfer in this information age. Computer networking has helped individuals, organization, companies and industries on how to have fast access to information and management of their resources so as to optimize and maximize their profit.

Design and implementation of computer networking helps in solving heterogeneous problem between computers and this allows a user to communicate through his computer and other communication equipment to another user irrespective of geographical location.

When the system was tested, it was evident that the result is realistic because each computer is able to communicate with one another on the network. The design and implementation of computer networking solves the problem of information accessing, processing transferring and allocation of resources.

On the other hand, the timer software solves the problem of congestion in real world especially in computer laboratory. It allows each student to have timely access to computer system services.

Research work is also made easy because all information is on the internet, users can now get information conveniently.

5.2 Conclusion

Computer networking is generally considered an unsuccessful initiative. This is associated with the minds of many with the over hyped network computer that fail to capture significant market share from PCS.

However, computer networking is not dependent on wide-scale network deployment. Infact, one of the key attributes of computer networking is the ability to support services on heterogeneous terminals of varying capabilities-PCS, high end workstations e.t.c

In the nearest future there will be several hundred million connected computing devices of varying degrees of functionally. Services will be adapted to both device capabilities and the characteristics of the network connection.

5.3 Recommendation

The emerging information communication technology revolution in Nigeria and the need to utilize the vast information available on the internet for research, academic pursuit and government in the modern way that is in line with world order calls for the design and implementation of computer networking, in any Computer laboratory. Based on the benefit of computer networking with timer software in the society, I hereby made the following recommendation:

- i. Federal government should make fund available to every institution so that ICT can be established in our higher school of learning.
- ii. Institution of higher learning should see computer networking as a tool that aid learning, research and resource sharing. They should make sure that their ICT center is fully equipped with the necessary equipments such as server, client, and hub e.t.c so that such center will be able to face the challenge of twenty-first century.
- iii. Users of the network should make sure that they use the network and it resource judiciously in order to achieve the aim and object of the innovation.
- iv. Operators should make sure that they are up and doing in order to minimize the risk of networking by putting necessary security measures in places.
- v. Future research on the project work could be on networking security and evaluation.

References:

1. Microsoft Corporation (2007):

Microsoft Student, Microsoft Encarta Encyclopedia.

2. Afolayan (1998): Computer Networking as an effective tool
information technology, oxford publisher, Lagos. (Pages 1-35, 66)

3. Johnston B. (1978): Data Communication and Networking
Fundamental. DTK Publisher, London. (Pages 2-15)

4. MCSE (2002): Networking essential MSCE study guide.(Pages 1-25)

5. Tanenbaum A. S (1996): Computer Networking, New Life Publisher,
USA. (Pages 1-57, 108-112)

6. Hutchison, D. (1989): Local Area Network Architectures
Addison Wesley Publishers, England. (Pages 19-31)

7. Stallings, W. (1992): Data and Computer Communications
Macmillan Publishers, New York. (Pages 33-42)

8. Nussbaumer, H. (1982): Computer Communication Systems
John Wesley & Sons, England. (Pages 11-13, 65)