Chalimbana University

DIRECTORATE OF DISTANCE EDUCATION

PMI 2101: MANAGEMENT OF INFORMATION SYSTEM

FIRST EDITION 2019

Author
Sikalumbi A. Dewin, PhD

Chalimbana University
School of Humanities & Social Sciences
Department of Humanities

Chalimbana University © 2019

Copyright

© 2019 Chalimbana University

First Edition

All rights reserved

No part of this publication may be reproduced, stored in a retrievable system, or transmitted in any form or by any means, electronic, mechanical, photocopying or recording or otherwise without prior written permission of the copyright owner, Chalimbana University.

Chalimbana University
School of Humanities and
Social Sciences
Department of Humanities
Private Bag E1
Chongwe
Zambia
Cell: 0977485465
Website: www.chau.ac.zm

Acknowledgements

Chalimbana University, wishes to thank **Dr. Sikalumbi A. Dewin** for producing this module: Management of Information System.

Table of Contents

MODULE OVERVIEW

Pre-requisite: None

Introduction

Welcome to Management of Information System module. This module aims at equipping you with knowledge and skills in management of information system. The knowledge acquired from this module can be applied in given organisations to enhance the timely flow of information for informed decision making. You are therefore, required to study with an open mind and read other related materials. All the best.

Aim

The aim of the course is to equip students with an understanding of information systems, their management and utilisation in organisations.

Learning Outcomes

By the end of this course, learners should be able to:

1. evaluate the role of information systems in today's competitive business environment.
2. describe important features of organizations in order to build and use information systems successfully.
3. demonstrate systems analysis, design and decision making in a business setting.
4. describe the fundamentals of hardware, software, database management, data communications and systems related to the management activities of an organization.
5. assess how information systems support the activities of managers and end-users in organizations.

6. identify the principal management challenges posed by the ethical and social impact of information systems and management solutions.

Rationale

There is no gainsaying the fact that numerous technologies have taken over the day-to-day office work. This has landed us into information age as everybody knows today. The world is a global village which is a product of information technologies. The introduction of a new information system involves much more than new hardware and software. Information technology can promote various degrees of organizational change, ranging from incremental to far-reaching. Building a new information system is one key step in gain a competitive advantage to many organisations. Therefore, this course brings out concepts and strategies on how information systems should be management for maximum performance.

 Summary

The module looks at the management of information system and its impact on the performance of an organisation.

 **Prescribed Reading:**

Laudon C. K. and Laudon P. J. (2014). Management Information Systems: Managing the Digital Firm, 13th Edition: Prentice Hall, Cloth.

French C. S. (2003). Computer Science. 5th Edition. Continuum International Publishing Group: London

Oliver E. C. and Chapman R. J. (1990). *Data Processing and Information Technology*. 8th Edition. Letts Educational: London.

Phiri, W. (2016). *Research Based ICT Education*. Lusaka; MP Publishers

Laudon Kenneth C. and Laudon Jane P. (2013). *Management Information Systems: Managing the Digital Firm.* Twelfth edition. Pearson Education, Inc.

O'Brien J. A. (1999). *Management Information System: Managing Information Technology in the Networked Enterprise*. Tata-McGraw-Hill.

Recommended Reading:

1. Agbasi K.C. (1993): Computer Appreciation; An Individual Computer to Systems, ACENA Publishers, Enugu.
2. Ahituv, N., Neumann, S., & Riley, H. N. (1994). Principles of information systems for management (4th ed.). Dubuque, IA: Wm. C. Brown Communications.
3. Alo, U.R., Ugah J.O., & Igwe J.S. (2009): Computer Application & Information Technology; WilyRose and Appleseed Publishing Coy, Abakaliki, Ebonyi State, Nigeria, 42p, 135p -137p.
4. Ashwin D. (2008): Characteristics of Management Information Services; Online @ http://www.blog.maia_intelligence.com, visited on 24th September, 2010.
5. Awad, E. M., & Gotterer, M. H. (1992). *Database management.* Danvers, MA: Boyd & Fraser.
6. Banerjee, U. K., & Sachdeva, R. K. (1995). *Management information system: A new frame work.* New Delhi: Vikas Publishing House.

Study Skills

As an adult l-earner, your approach to learning will be different to that of your school days: you will choose when you want to study, you will have professional and/or personal motivation for doing so and you will most likely be fitting your study activities around other professional or domestic responsibilities.

Essentially you will be taking control of your learning environment. As a consequence, you will need to consider performance issues related to time management, goal setting, stress management, etc. Perhaps you will also need to acquaint yourself with areas such as essay planning, searching for information, writing, coping with examinations and using the internet as a learning resource. Your most significant considerations will be *time* and *space* i.e. the time you dedicate to your learning and the environment in which you engage in that learning.

It is recommended that you take time now —before starting your self-study— to familiarise yourself with these issues. There are a number of excellent resources on the web. A few suggested links are:

http://www.how-to-study.com/

The "How to study" website is dedicated to study skills resources. You will find links to study preparation (a list of nine essentials for a good study place), taking notes, strategies for reading text books, using reference sources, test anxiety.

http://www.ucc.vt.edu/stdysk/stdyhlp.html

This is the website of the Virginia Tech, Division of Student Affairs. You will find links to time scheduling (including a "where does time go?" link), a study skill checklist, basic concentration techniques, control of the study environment, note taking, how to read essays for analysis, memory skills ("remembering").

Timeframe

You are expected to spend at least 36 hours of study time on this module. In addition, there shall be arranged contact sessions with lecturers from the University during residential possibly in April, August and December. You are requested to spend your time judiciously so that you reap maximum benefit from the course.

Need Help?

In case you have difficulties during the duration of the course, please get in touch with your lecturer for routine enquiries during working days **(Monday-Friday)** from 08:00 to 17:00 hours on Cell: +260963804004**; E-mail: adsikalumbi@gmail.com; website: www.chau.ac.zm.** You can also see your lecturer at the office during working hours as stated above.

You are free to utilise the services of the University Library which opens from 07:00 hours to 20:00 hours every working day.

It will be important for you to carry your student identity card for you to access the library and let alone borrow books.

List of equipment

In this module you will need a computer.

Assessment

In this course you will be assessed on the basis of your performance as follows:

Continuous Assessment		**50%**
Assignment	10%	
Project	15%	
2 Tests of equal weight	25%	
Final Examination		**50%**
Total		**100%**

How to get the most out of this course

In distance learning, the study units replace the university lecturer. This is one of the huge advantages of distance learning mode; you can read and work through specially designed study materials at your own pace and at a time and place that is most convenient. Think of it as reading from the teacher, the study guide indicates what you ought to study, how to study it and the relevant texts to consult. You are provided with exercises at appropriate points, just as a lecturer might give you an in-class exercise.

Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit and how a particular unit is integrated with the other units and the course as a whole. Next to this is a set of learning objectives. These learning objectives are meant to guide your studies. The moment a unit is finished, you must go back and check whether you have achieved the objectives. If this is made a habit, then you will increase your chances of passing the course. The main body of the units also guides you through the required readings from other sources. This will usually be either from a set book or from other sources. Self-assessment exercises are provided throughout the unit, to aid personal studies and answers are provided at the end of the unit. Working through these self-tests will help you to achieve the

objectives of the unit and also prepare you for tutor marked assignments and examinations. You should attempt each self-test as you encounter them in the units.

The following are practical strategies for working through this course

1. Read the course guide thoroughly

2. Organize a study schedule. Refer to the course overview for more details. Note the time you are expected to spend on each unit and how the assignment relates to the units. Important details, e.g. details of your tutorials and the date of the first day of the semester are available. You need to gather together all these information in one place such as a diary, a wall chart calendar or an organizer. Whatever method you choose, you should decide on and write in your own dates for working on each unit.

3. Once you have created your own study schedule, do everything you can to stick to it. The major reason that students fail is that they get behind with their course works. If you get into difficulties with your schedule, please let your tutor know before it is too late for help.

4. Turn to Unit 1 and read the introduction and the objectives for the unit.

5. Assemble the study materials. Information about what you need for a unit is given in the table of content at the beginning of each unit. You will almost
always need both the study unit you are working on and one of the materials recommended for further readings, on your desk at the same time.

6. Work through the unit, the content of the unit itself has been arranged to provide a sequence for you to follow. As you work through the unit, you will be encouraged to read from your set books.

7. Keep in mind that you will learn a lot by doing all your assignments carefully. They have been designed to help you meet the objectives of the course and will help you pass the examination.

8. Review the objectives of each study unit to confirm that you have achieved them. If you are not certain about any of the objectives, review the study material and consult your tutor.
9. When you are confident that you have achieved a unit's objectives, you can start on the next unit. Proceed unit by unit through the course and try to pace your study so that you can keep yourself on schedule.

10. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned, pay particular attention to your tutor's comments, both on the tutor marked assignment form and also written on the assignment.
    Consult you tutor as soon as possible if you have any questions or problems.

11. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in this course guide).

You should endeavour to attend the tutorials. This is the only opportunity to have face-to-face contact with your tutor and ask questions which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefit from the course tutorials, have some questions handy before attending them. You will learn a lot from participating actively in discussions.
GOODLUCK!

UNIT 1

INTRODUCTION TO MANAGEMENT OF INFORMATION

1.1 Introduction

As level of information needed for day to day activities increases, more data are being stored and linked; man began to analyse this information bringing further detail, creating entire management reports from the raw, stored data.

This unit present the meaning of MIS, its goal, characteristics, advantages and general concepts one need to know about MIS. Because the constituents of MIS are common terms used on daily bases in industries, offices, understanding of every concept is as easy as the terms themselves.

1.2 Objectives

At the end of this unit, you should be able to:

- Explain the concept of MIS.
- State the goals of MIS.
- Enumerate the characteristics of MIS.
- State the advantages and disadvantages of MIS.
- Describe the meaning of some parameters associated with MIS.

1.3 The concept of MIS

Student, how would you define MIS?

Well, to managers, Management Information System is an implementation of the organizational systems and procedures. To a programmer it is nothing but file structures and file processing. However, it involves much more complexity.

The three components of MIS as you can see in the title provide a more complete and focused definition, where System suggests integration and holistic view, Information stands for processed data, and Management is the ultimate user, the decision makers.

Management information system can thus be analysed as follows −

Management

Management covers the planning, control, and administration of the operations of a concern. The top management handles planning; the middle management concentrates on controlling; and the lower management is concerned with actual administration.

Information

Information, in MIS, means the processed data that helps the management in planning, controlling and operations. Data means all the facts arising out of the operations of the concern. Data is processed i.e. recorded, summarized, compared and finally presented to the management in the form of MIS report.

System

Data is processed into information with the help of a system. A system is made up of inputs, processing, output and feedback or control.

Thus MIS means a system for processing data in order to give proper information to the management for performing its functions.

Definition of MIS

Management Information System or 'MIS' is a planned system of collecting, storing, and disseminating data in the form of information needed to carry out the functions of management.

MIS may be defined as the use of information technology, people, and business processes to record, store and process data to produce information that decision makers can use to make day to day decisions.

MIS is the acronym for Management Information Systems. In a nutshell, MIS is a collection of systems, hardware, procedures and people that all work together to process, store, and produce information that is useful to the organization.

1.3.1 The need for MIS

The following are some of the justifications for having an MIS system.

Decision makers need information to make effective decisions. Management Information Systems (MIS) make this possible.

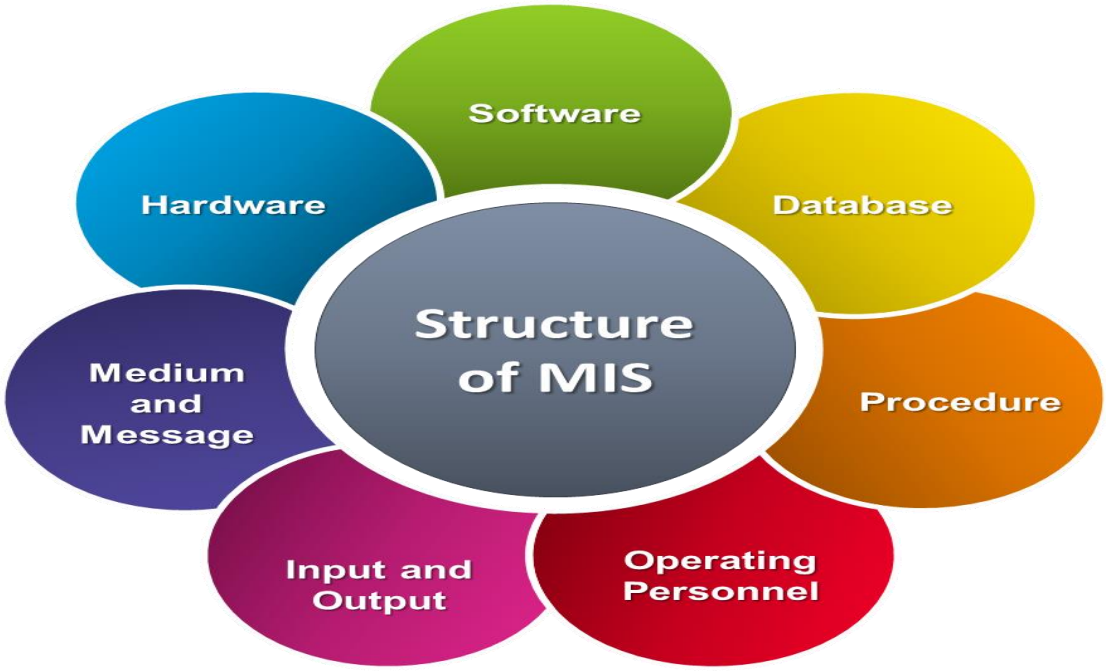
- MIS systems facilitate communication within and outside the organization – employees within the organization are able to easily access the required information for the day to day operations. Facilitates such as Short Message Service (SMS) & Email make it possible to communicate with customers and suppliers from within the MIS system that an organization is using.
- Record keeping – management information systems record all business transactions of an organization and provide a reference point for the transactions.

1.4 Components of MIS

The major components of a typical management information system are;

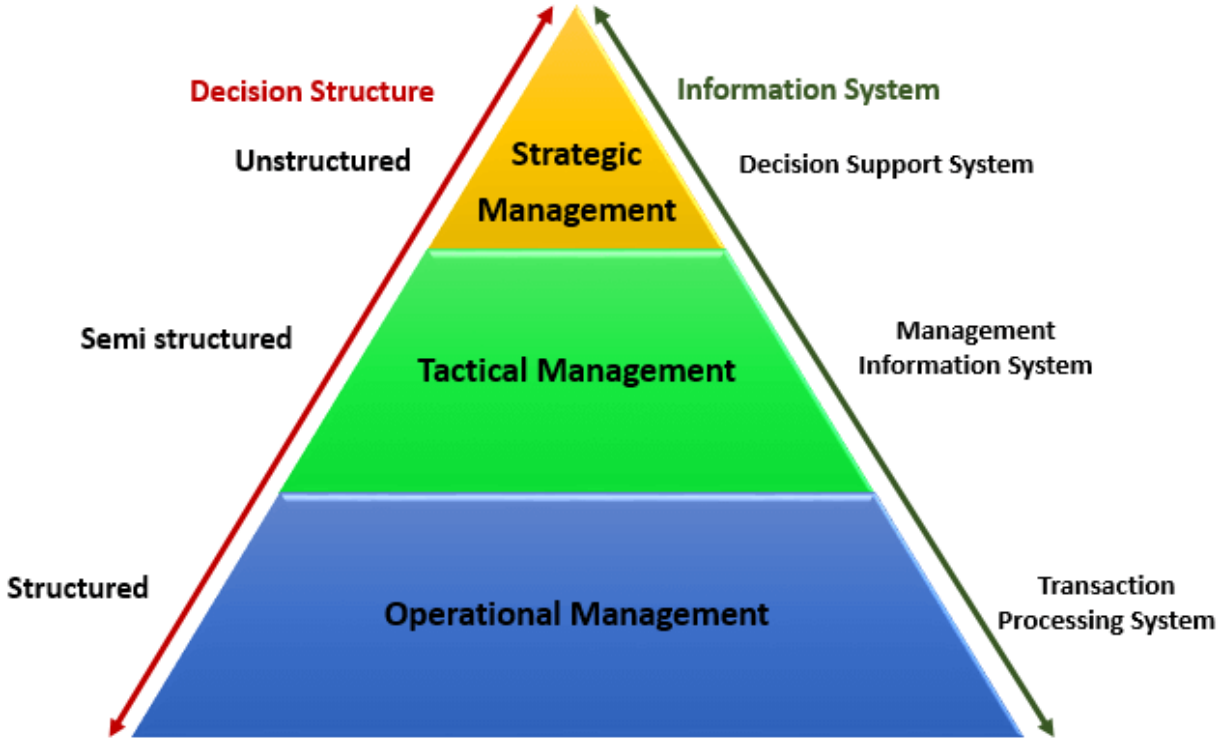
- **People –** people who use the information system
- **Data –** the data that the information system records
- **Business Procedures –** procedures put in place on how to record, store and analyze data
- **Hardware –** these include servers, workstations, networking equipment, printers, etc.
- **Software –** these are programs used to handle the data. These include programs such as spreadsheet programs, database software, etc.

The diagram below illustrates with an inclusion of medium and input and output processes.



1.5 Types of Information Systems

The type of information system that a user uses depends on their level in an organization. The following diagram shows the three major levels of users in an organization and the type of information system that they use.



Transaction Processing Systems (TPS)

This type of information system is used to record the day to day transactions of a business. An example of a Transaction Processing System is a Point of Sale (POS) system. A POS system is used to record the daily sales.

Management Information Systems (MIS)

Management Information Systems are used to guide tactic managers to make semi-structured decisions. The output from the transaction processing system is used as input to the MIS system.

Decision Support Systems (DSS)

Decision support systems are used by top level managers to make semi-structured decisions. The output from the Management Information System is used as input to the decision support system. DSS systems also get data input from external sources such as current market forces, competition, etc.

1.6 Manual VS Computerized Information Systems (MIS)

Data is the bloodstream of any business entity. Everyone in an organization needs information to make decisions. An information system is an organized way of recording, storing data, and retrieving information. In this section, we will look at manual information systems vs. computerized information systems.

1.6.1 Manual Information System

A manual information system does not use any computerized devices. The recording, storing and retrieving of data is done manually by the people, who are responsible for the information system. The following are the major components of a manual information system

- People –people are the recipients of information system
- Business Procedures –these are measures put in place that define the rules for processing data, storing it, analyzing it and producing information
- Data –these are the recorded day to day transactions
- Filing system – this is an organized way of storing information
- Reports –the reports are generated after manually analysing the data from the filing system and compiling it.

The following diagram illustrates how a typical manual information system works

Source: GURU99, retrieved on 22/11/19.

Advantages of a manual information system

The following are the advantages of manual information systems

- Cost effective – it is cheaper compared to a computerized system because there is no need to purchase expensive equipment such as servers, workstations, printers, etc.
- Flexible –evolving business requirements can easily be implemented into the business procedures and implemented immediately

Disadvantages:

The following are some of the disadvantages of a manual information system.

- Time consuming –all data entries need to be verified before filing, this is a time consuming task when done by humans. Retrieving data from the filing system also takes a considerable amount of time
- Prone to error – the accuracy of the data when verified and validated by human beings is more prone to errors compared to verification and validation done by computerized systems.
- Lack of security – the security of manual systems is implemented by restricting access to the file room. Experience shows unauthorized people can easily gain access to the filing room
- Duplication of data –most departments in an organization need to have access to the same data. In a manual system, it is common to duplicate this data to make it easy to accessible to all authorized users. The challenge comes in when the same data needs to be updated
- Data inconsistency – due to the duplication of data, it is very common to update data in one file and not update the other files. This leads to data inconsistency
- Lack of backups – if the file get lost or mishandled, the chances of recovering the data are almost zero.

1.6.2 Computerized information system

Computerized systems were developed to address the challenges of manual information systems. The major difference between a manual and computerized information system is a computerized system uses a combination of software and hardware to record, store, analyse and retrieve information.

Advantages of a computerized information system (MIS)

The following are some of the disadvantages of a computerized information system.

The following are the advantages of computerized information systems

- Fast data processing and information retrieval – this is one of the biggest advantages of a computerized information system. It processes data and retrieves information at a faster rate. This leads to improved client/customer service
- Improved data accuracy – easy to implement data validation and verification checks in a computerized system compared to a manual system.
- Improved security – in addition to restricting access to the database server, the computerized information system can implement other security controls such as user's authentication, biometric authentication systems, access rights control, etc.
- Reduced data duplication – database systems are designed in such a way that minimized duplication of data. This means updating data in one department automatically makes it available to the other departments
- Improved backup systems – with modern day technology, backups can be stored in the cloud which makes it easy to recover the data if something happened to the hardware and software used to store the data
- Easy access to information – most business executives need to travel and still be able to make a decision based on the information. The web and Mobile technologies make accessing data from anywhere possible.

Disadvantages

- It is expensive to set up and configure – the organization has to buy hardware and the required software to run the information system. In addition to that, business procedures will need to be revised, and the staff will need to be trained on how to use the computerized information system.
- Heavy reliance on technology – if something happens to the hardware or software that makes it stop functioning, then the information cannot be accessed until the required hardware or software has been replaced.
- Risk of fraud – if proper controls and checks are not in place, an intruder can post unauthorized transactions such as an invoice for goods that were never delivered, etc.

1.7 Characteristics of high quality information

Provided below are the five characteristics of high quality information which are accuracy, completeness, consistency, uniqueness, and timeliness.

Accuracy: The information that is input into a data base is presumed to be perfect as well as accurate. The information that is accessed is deemed reliable. Flaws do arise with database design but do not let something in your control, accurate and reliable data, be one of them. A database design that is accurate and reliable will help achieve the development of new business ideas as well as promoting the organizational goals.

Completeness is another attribute of high quality information. Partial information may as well be incomplete information because it is only a small part of the picture. Completeness is as necessary as accuracy when inputting data into a database.

Consistency is key when entering information into a database. For example, with a column for a phone number entry 10 digits is the expected length of the field. Once the fields have been set in the database, a number more or less than 10 digits will not be accepted. The same applies for any field, whether it is an entry that requires a number, a series of numbers, an address, or a name, etc. If the fields are not set to a specific limit for information then consistency is even more important.

Uniqueness is the fourth component of high quality information. In order to add value to any organization, information must be unique and distinctive. Information is a very essential part of any organization and if used properly can make a company competitive or can keep a company competitive.

A fifth important aspect of information is **timeliness**. New and current data is more valuable to organizations than old outdated information. Especially now, in this era of high technological advances, out-of-date information can keep a company from achieving their goals or from surviving in a competitive arena. The information does not necessarily need to be out of date to have effect, it just needs to not be the most current. Real-time information is an element of timeliness.

1.8 Summary

Student, you have to the end of unit one. In this unit, you have covered the following;

- MIS is the acronym for Management Information System. It is a collection of people, procedures, data, and information technology that aids managers to make informed decisions.
- Computerized information systems are more efficient compared to manual information systems. Manual information systems are cheaper compared to computerized information systems.
- Transaction processing systems (TPS) are by operational staff to record day to day business transactions, and they are used to make structured decisions
- Management Information Systems (MIS) are used by middle-level managers to make semi-structured decisions
- Decision Support Systems are used by top level managers, and they help top level managers to make unstructured decisions

1.8 Revision Questions

1. Analyse the relationship among these three terms: data, information and instruction.
2. Enumerates the bottlenecks associated with MIS.
3. What is the difference between database and decision support systems as components of MIS?
4. State the overall aims of MIS.

   Bring out questions and activities that directly reflect what they experience and do at their place of work. This will help them relate the content learnt to what is in practice.

Make your work as interactive as possible for the distance learner.

UNIT 2: LEVELS OF MANAGEMENT IN ORGANISATIONS

2.0 Introduction

Welcome to unit 2. In this unit, I am going to discuss the various levels management system that exit. Also necessary is the communication channels existing among the established levels of management.

2.1 Objectives

After completing this unit, you should be able to:

- Discuss different levels of management.
- Analyse how the various levels of management interact.
- State how management information system is developed.

2.2 Levels of Management

There are three levels of management that could be identified in most organizations. These are: top management cadre (strategic level), middle management cadre (tactical level), and operational group cadre (operational level).

2.3.1 Top Strategic /Management Level

This level of management coordinates the activities of the whole organization and has a strategic view of the organization. This level is concerned with establishing (estimating) the overall objectives of the organization and in devising appropriate policies so that the objectives may be achieved.

Typical of the functions of top management are:

(i) Long term planning

(ii) Capital investment decisions

(iii) Organizational restructuring

(iv) Middle management appointment

(v) Acquisitions and mergers

The top management level is the overall policy making section of the management and as such will be actively involved in corporate planning process of an organization.

2.3.2 Middle Management Level

This may be termed the tactical level of management whose overall function is to implement top management policy. This level of management does set objectives but these objectives are more limited in scope and are subordinate to the objectives set by the top management level. Examples of the functions of the middle management are:

a. Purchasing
b. Product planning
c. Sales promotion
d. Discount and credit policy
e. Staff appointment
f. Implementation of marketing and advertising policies of the organization.

2.3.3 Operational Level of Management

This level of management is concerned with the day-to-day process of supervision i.e. direction associated with the normal activities of the organization.

Functions of the operational level are:

a. Production
b. Dispatching
c. Sales
d. Accounting.

Often this level of management may not be called managers but they have titles, such as, heads of …, supervisors, chief clerical, foremen, etc. Even though the work this group does involves management, it is of different categories.

2.4 Communication among Levels of Management

It is important that these groups of management levels will be able to communicate effectively for the purpose of achieving effective goals of an organization. It has been observed that this group of management levels has been able to pass all necessary information in the form of communication within the different groups. It is important also that information from the top management level be passed down through the usual procedure. Normally, information from top management level will not go to the operational level first before the middle management level for adequate flow of information within an organization. It is a bad system of information flow and it encourages misinformation and confusion in an organization. Therefore,

information has to be communicated from the top management level to the operational level through the middle management level; and vice versa.

2.5 Management Structure and MIS

A broad structure of information supplied by MIS is divided into planning and controlling. This division is of great importance not only because of the intrinsic nature of these two types of information management but also because of the destruction within the management structure. Figure below illustrates the broad relationship between the proportion of planning and controlling information received and management place in hierarchy.

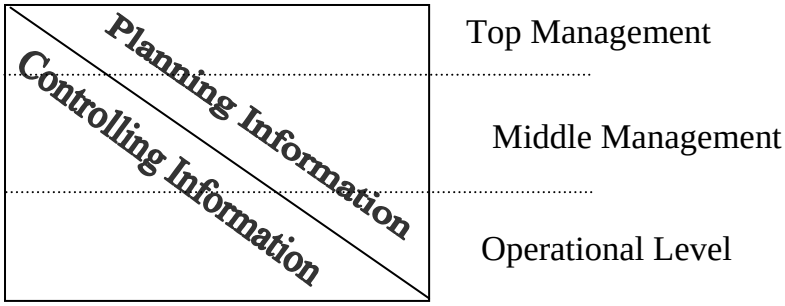


Fig 2: Relation between planning and control at different management levels.

Top management level deals with more planning of information than controlling of information. This level has little of control of information as fig. 2 shows but at the middle management level, the planning and controlling of information are proportionate (about equal). The operational level has very little to do of planning but controls what is going on and implement the plans of top and middle management levels.

2.6 Development of Management Information System

All levels of management need information on which to base decisions, to plan, to organize and to control. People organize information directly by way of observing and experiencing events. But as an organization becomes larger and more complex, it becomes impossible for management, particularly the middle and top management levels to observe and experience all operations. In some form of decentralized organizations, management virtually never saw the actual events and has to rely almost entirely on information provided through the formal and informal channels. Although much viable information is passed through decisions, meetings and casual conversations, such methods do not generally give a complete picture nor do they provide information in the correct form of intended use.

So, as an organization grows, there is a shift from informal to more formal methods of disseminating information. More formal information systems are observed through reports, operating system, special analysis, various returns, balance sheet returns, etc. These have the advantages of comprehensiveness, consistency, and reasonable accuracy but may suffer from the disadvantages of not meeting the exact requirements of the problem at hand, the lack of flexibility, time lag of events or operations to reports and costs. In spite of these possible disadvantages, the development of MIS is virtually necessary in most organizations today.

2.7 Summary

Different levels of management exist in organization ranging from top level management to middle to operational level. And these levels of management need information on which to base decisions for proper planning, organization and control. This unit tried also to analyse the communication channels existing among these levels.

2.8 Revision questions

1. Mention and explain any three levels of management in an organization.
2. How is communication channelled among the levels of management?
3. Discuss management structure in relation to MIS.
4. Bring out activities depicting real life situations and work place experiences and how they are able to deal with them.

   Make your work as interactive as possible.

3.0 Introduction

Welcome to unit 3 of this module. Communication is key in directing the organisation towards achieving the organisational goals. Web-based communication is defined as the sharing of information, words or ideas over a network of computers known as the Internet. Email is an example of web-based communication. Online webinars are an example of web-based communication. Therefore, in this unit, we are going to discuss the web-based communication and types.

3.1 Objectives

At the end of this unit, you should be able to;

- describe the concept of web-based communication.
- explain the mode of web-based communication.
- demonstrate usage of web-based communication.

3.2 Electronic Mail

Electronic mail is a method of transmitting data, text files, digital photos, or audio and video files from one computer to another over an intranet or the Internet. Email is a method of exchanging digital messages across the internet or other computer network. Originally, email was transmitted directly from one user to another computer. This required both computers to be online at the same time. It enables computer users to send messages and data quickly through a local area network or beyond through the Internet. E-mail widespread has become a major development in business and personal communications for recent years. The e-mail is a store and forward technology.

E-mail users create and send messages from individual computers using commercial e-mail programs or mail-user agents (MUAs). Most of these programs have a text editor for composing messages. The user sends a message to one or more recipients by specifying destination addresses. An email message consists of two components, the message header, and the message body, which is the email's content. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually additional information is added, such as a subject header field. Originally a

text-only communications medium, email was extended to carry multi-media content attachments.

The address of an e-mail message includes the source and destination of the message. Different addressing conventions are used depending upon the e-mail destination. An interoffice message distributed over an intranet, or internal computer network, may have a simple scheme, such as the employee's name, for the e-mail address. E-mail messages sent outside of an intranet are addressed according to the following convention: The first part of the address contains the user's name, followed by the symbol @, the domain name, the institution's or organization's name, and finally the country name.

A typical e-mail address might be *igwejoe@ebsu.edu*. In this example *igwejoe* is the user's name; ebsu is the domain name—the specific company, organization, or institution that the e-mail message is sent to or from; and the suffix *edu* indicates the type of organization that *ebsu* belongs to - *com* for commercial, *org* for organization, *edu* for educational, *mil* for military, and *gov* for governmental. An e-mail message that originates outside the United States or is sent from the United States to other countries has a supplementary suffix that indicates the country of origin or destination. Examples include *uk* for the United Kingdom, ng for Nigeria, *fr* for France, and *au* for Australia.

E-mail data travels from the sender's computer to a network tool called a message transfer agent (MTA) that, depending on the address, either delivers the message within that network of computers or sends it to another MTA for distribution over the Internet. The data file is eventually delivered to the private mailbox of the recipient, who retrieves and reads it using an e-mail program or MUA. The recipient may delete the message, store it, reply to it, or forward it to others.

Email messages are not secure if email encryption is not used correctly.
Many MTAs used to accept messages for any recipient on the Internet and do their best to deliver them. Such MTAs are called open mail relay. This was very important in the early days of the Internet when network connections were unreliable. If an MTA couldn't reach the destination, it could at least deliver it to a relay closer to the destination. The relay stood a better chance of delivering the message at a later time. However, this mechanism proved to be exploitable by people sending unsolicited large email and as a consequence very few modern

MTAs are open mail relays, and many MTAs don't accept messages from open mail relays because such messages are very likely to be spam.

3.3 Teletext/Viewdata

Teletext is written information on television. It is also a term used to refer a system of broadcasting news and other information in written form that can be viewed on specially equipped television sets, superimposed on, or in place of, the picture. It is a system for transmitting commercial and other information through existing television networks. TELETEXT is a one-way, or non-interactive, system for transmission of text and graphics via broadcasting or cable for display on a television set. A decoder or microchip resident in the TV set is needed to extract the teletext information. Teletext can be transmitted over one-way cable or over-the-air broadcasting via radio or television. In the case of TV, it can occupy a full channel or be encoded in the vertical blanking interval, or VBI.

Viewdata is a videotex implementation. It is a type of information retrieval service in which a subscriber can access a remote database via a common carrier channel, request data and receive requested data on a video display over a separate channel. Viewdata is an interactive information system in which text and graphic data stored in a central computer are transmitted over telephone lines to be displayed on a modified television receiver. Viewdata is different from teletext in some ways. For instance, users can interrogate the data held in the system and also supply information to it.

And also the viewdata system uses a combination of telephones, computers, television, and communication networks. Viewdata is still in use today in the United Kingdom, mainly by the travel industry. Travel agents use it to look up the price and availability of package holidays and flights.

3.4 Fax

Facsimile transmission is a technology that allows an exact copy of an original document including diagrams, pictures and text to be electronically in digitized form over telephone lines and reproduces in its original form at the receiving end. It performs similar function as photocopying machine with the difference of using a telephone to cover a long distance. The most recent and improved fax machine can interactively be used to transmit both voice and data simultaneously.

Although businesses usually maintain some kind of fax capability, the technology has faced increasing competition from internet-based alternatives. However, fax machines still retain some advantages, particularly in the transmission of sensitive material which, if sent over the Internet unencrypted, may be vulnerable to interception. In some countries, because electronic signatures on contracts are not recognized by law while faxed contracts with copies of signatures are recognized, fax machines enjoy continuing support in business.

In many corporate environments, standalone fax machines have been replaced by "fax server" and other computerized systems capable of receiving and storing incoming faxes electronically, and then routing them to users on paper or via an email (which may be secured). Such systems have the advantage of reducing costs by eliminating unnecessary printouts and reducing the number of inbound analog phone lines needed by an office.

3.5 Bulletin Board System

This is an online forum used to exchange emails, chat, and access software. Bulletin Board System is a computer or an application dedicated to the sharing or exchange of messages or other files on a network. Originally an electronic version of the type of bulletin board found on the wall in many work places, the BBS was used to post simple messages between users. The BBS became the primary kind of online community through the 1980s and early 1990s, before the World Wide Web arrived.

Most BBSes are devoted to a particular subject, although some are more general in nature. Among special interests represented on BBSes are dentistry, law, guns, multiplayer games, Druidic practices, and information for the disabled. A significant number of BBS sites offer "adult-oriented" chat and images that can be downloaded. The BBS is often free, although some charge a membership or use fee. Many BBSes have Web sites, and many Internet access providers have bulletin board systems from which new Internet users can download the necessary software to get connected. The BBS has its own culture and jargon. For example, a sysop is the person who runs the site. Online chat became widely popular through the BBS and many chat acronyms originated there.

3.6 Voice-Mail

Voicemail (also known as voice-mail Systems (VMS) or message bank) is a centralized system of stored telephone messages that can be retrieved later. The term is also used more broadly to denote any system of conveying a stored telecommunications voice message, including using an answering machine. It is electronic communication system that stored digitized recording of telephone messages for later playback.

Voicemail systems are designed to convey a recorded audio message to a recipient. To do so they contain a user interface to select, play, and manage messages; a delivery method to either play or otherwise deliver the message; and a notification ability to inform the user of a waiting message. Most systems use phone-networks, either cellular or land-line based, as the conduit for all of these functions. Some systems may use multiple telecommunications methods, permitting recipients and callers to retrieve or leave messages through multiple methods.

Simple voicemail functions as a remote answering machine using a touch-tone as the user interface. More complicated systems may use other input devices such as voice or a computer interface. Simpler voicemail systems may play the audio message through the phone, while more advanced systems may have alternative delivery methods, including email or text message delivery, message transfer and forwarding options, and multiple mailboxes.
Notification methods also vary based on the voicemail system. Simple systems may not provide active notification at all, instead requiring the recipient to check with the system, while others may provide an indication that messages are waiting.

Almost all modern voicemail systems use digital storage and are typically stored on computer storage devices.

3.7 Telnet

This is an internet service that makes a user's computer a terminal to other computers on the internet. It presents a user to appear to be physically using another computer which is away from his own computer. Individual on his own can run programs, delete files, view content files, modify, save, lock files in another or remote computer.

To cut short, telnet is a terminal emulation program that allows computer users to connect interactively to a server and access remote sites. It was the first packet-switched network service

that was available to the general public. Various commercial and government interests paid monthly fees for dedicated lines connecting their computers and local networks to this backbone network. Free public dialup access to Telnet, for those who wished to access these systems, was provided in hundreds of cities throughout the United States.

3.8 Network

A computer network, often simply referred to as a network, is a group of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources. It is a system of two or more computers, terminals, and communications devices linked by wires, cables, or a telecommunications system in order to exchange data.

The network may be limited to a group of users in a local area network, or be global in scope, as the Internet is. Network users are able to share files, printers, and other resources; send electronic messages; and run programs on other computers. A computer network allows sharing of resources and information among interconnected devices.

In the 1960s, the Advanced Research Projects Agency (ARPA) started funding the design of the Advanced Research Projects Agency Network (ARPANET) for the United States Department of Defence. It was the first computer network in the world. Development of the network began in 1969, based on designs developed during the 1960s.

A network has three layers of components: application software, network software, and network hardware. Application software consists of computer programs that interface with network users and permit the sharing of information, such as files, graphics, and video, and resources, such as printers and disks. One type of application software is called client-server. Client computers send requests for information or requests to use resources to other computers, called servers that control data and applications. Another type of application software is called peer-to-peer. In a peer-to-peer network, computers send messages and requests directly to one another without a server intermediary.

Network software consists of computer programs that establish protocols, or rules, for computers to talk to one another. These protocols are carried out by sending and receiving formatted instructions of data called packets. Protocols make logical connections between

network applications, direct the movement of packets through the physical network, and minimize the possibility of collisions between packets sent at the same time.

Network hardware is made up of the physical components that connect computers.
Two important components are the transmission media that carry the computer's signals, typically on wires or fibre-optic cables, and the network adapter, which accesses the physical media that link computers, receives packets from network software, and transmits instructions and requests to other computers. Transmitted information is in the form of binary digits, or bits (1s and 0s), which the computer's electronic circuitry can process.

A network has two types of connections: physical connections that let computers directly transmit and receive signals and logical, or virtual, connections that allow computer applications, such as e-mail programs and the browsers used to explore the World Wide Web, to exchange information. Physical connections are defined by the medium used to carry the signal, the geometric arrangement of the computers (topology), and the method used to share information. Logical connections are created by network protocols and allow data sharing between applications on different types of computers, such as an Apple Macintosh or a personal computer (PC) running the Microsoft Corporation Windows operating system, in a network. Some logical connections use client-server application software and are primarily for file and printer sharing. The Transmission Control Protocol/Internet Protocol (TCP/IP) suite, originally developed by the United States Department of Defense, is the set of logical connections used by the Internet, the worldwide consortium of computer networks. TCP/IP, based on peer-to-peer application software, creates a connection between any two computers.

3.9 Teleconferencing and Videoconferencing

Tele-conference is an offshoot of one-to-one telephone conversation. It allows many people to be simultaneously connected so that discussion can take place even when they reside in different places at the time. The impact it creates facilitate speedy gathering and assessing of information in an organisation. Teleconferencing has only one short coming, which is its inability to identify or authenticate the speakers during meeting.

Video-conferencing is the technology where participants in different places connected by both audio and video links hold meetings. Though videoconferencing is far more expensive than teleconferencing, it solves the problem of user identification. An example is MTN e-Presence.

3.10 Summary

Congratulations for reading the whole unit successfully. You have realised that there is no gainsaying the fact that numerous technologies have taken over the day-to-day office work. This has landed us into information age as everybody knows today. That the world is a global village is a product of information technologies described above.

This unit itemised one after the other eight information technologies employed today in office, which include: electronic mail, telex, voicemail, computer network, teleconference and video conference, fax, Bulletin Board Service and telnet.

3.11 Revision Questions

1. Demarcate between teleconference and videoconference.
2. View data is an example of information technology. True or false?
3. MUA stands for …….
4. Use diagram to demonstrate star topology arrangement.
5. Write brief notes on the following: voice mail, email, teletext and networking.
6. Describe skype and clearly indicate its benefits and weaknesses.

Bring out a practical activity relating to a real-life situation

Attend to the module's interactivity

UNIT 4: INTERNET, NETWORKING AND TELECOMMUNICATIONS

4.0 Introduction

Calling the world a global village is another way of appreciating the role the internet has played in the development of both the world economy and the societal lives of its inhabitants. Internet is the master disseminator of information around the globe. In this unit, you are going to learning about internet, networking and telecommunications. Enjoy the unit.

4.1 Objectives

At the end of this unit, you should be able to:

- explain the meaning of internet and its origin.
- state the requirement for connecting to internet.
- state the different formats for displaying information.
- demonstrate knowledge and skills in using the internet.
- list the limitations of the internet

4.2 The concept of internet

The Internet is a vast connectivity of global network linking several other networks and electronically associating millions of people and computer users around the world. The networks makes it possible for information stored in the major computers connected to it known as hosts, to be accessible by other users irrespective of the distances separating them. The Internet is the base of global communication and information sharing.

The internet is hosted by several computers networked together as shown in the figure below.

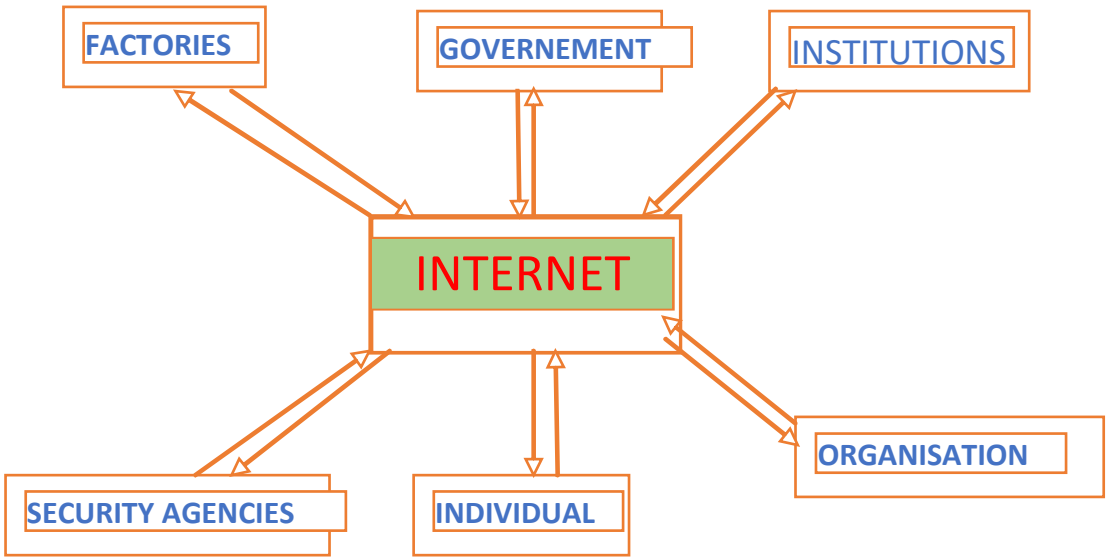


FIG. 4: Dissemination of Information to and fro the Internet

4.2.1 Origin of the Internet

History had it that in the 1950s and early 1960s, prior to the widespread internetworking that led to the Internet, most communication networks were limited in that they only allowed communications between the stations on the network. Some networks had gateways or bridges between them, but these bridges were often limited or built specifically for a single use. One prevalent computer networking method was based on the central mainframe method, simply allowing its terminals to be connected via long leased lines. This method was used in the 1950s by Project RAND to support researchers such as Herbert Simon, in Pittsburgh, Pennsylvania, when collaborating across the continent with researchers in Sullivan, Illinois, on automated theorem proving and artificial intelligence. The research led to the development of several packet-switched networking solutions in the late 1960s and 1970s, including ARPANET and the X.25 protocols. The ARPANET involved several experts from the government, military, universities and the public to decentralise the network for other users apart from the United States Defense.

Additionally, public access and hobbyist networking systems grew in popularity, including unix-to-unix copy (UUCP) and FidoNet. They were however still disjointed separate networks, served only by limited gateways between networks. This led to the application of packet switching to develop a protocol for inter-networking, where multiple different networks could be joined together into a super-framework of networks.

It was until 1989 when the National Science Foundation (NSF) took over from ARPANET to form the NSFNET that the Internet as we have it today evolved. Several supercomputers were provided to serve as a hosts or main servers, and involved private companies and other business networks to serve as links for smaller users.

By defining a simple common network system, the Internet protocol suite, the concept of the network could be separated from its physical implementation. This spread of inter-network began to form into the idea of a global inter-network that would be called 'The Internet', and this began to quickly spread as existing networks were converted to become compatible with this. This spread quickly across the advanced telecommunication networks of the western world, and then began to penetrate into the rest of the world as it became the de-facto international standard and global network. However, the disparity of growth led to a digital divide that is still a concern today.

The use of the World Wide Web, which was developed in the late 80s to allow for graphics and multimedia, and the integration of several aspects of the Internet, was introduced in the early 90s.

4.2.3 Requirement for Internet Connectivity

For anyone to connect to the Internet, he/she will need certain components. The basic requirements for one to connect to the internet include the following:

Computer System: You can use PC or any type of computer such as IBM-compatible or Macintosh computer to connect to the Internet. It is advisable to use a system with at least 128 MB of RAM, 10 gigabytes of hard disk and above, Windows NT, 95 or higher versions of windows operating system e.t.c

Modem (Modulator-Demodulator): A modem is a device that lets computers communicate through telephone lines. Modems provide easy way to access information on the Internet. There are also other high speed connections such as an integrated services Digital Network (ISDN), Digital subscriber Line (DSL), radon technology etc.

Phone Line: You use the same phone line for telephone and modem calls.

ISP: ISP stands for Internet service provider. An ISP is a company that gives you access to the Internet for a fee.

Cables and phone sockets: You need cables to connect your modem to the phone socket and the computer. The computer needs to connect to the modem which in turn dials up the ISP using the phone socket.

Browser: Browsers are software programs that allow you surf or browse the Internet. A typical example of a browser is the Internet explorer, Mozilla Fireworks, and the Netscape navigator.

4.2.4 Information Format on the Internet

Information is stored on the Internet in different formats. The most common and most popular are discussed below:

- **Web pages:** A web page is made up of text, pictures, animations and hyperlinks (a hyper link or simply link is the underline word, or phrase on a web page which when clicked on will take you to another section of the page or to another page(s) entirely) .A collection of related web pages is called a web site and collection of web sites on the Internet is called the World Wide Web (www).
- **File transfer protocol (FTP):** FTP allows you to download a file to your personal computer.
- **Email:** This format allows you to send and receive messages to specific people of interest.
- **Newsgroups:** The groups let you exchange information among the entire group of people sharing the same interest. It is been used widely by Newspaper publishers over the internet.

4.2.5 Internet Usage

The first time you connect to the Internet, you need to enter your username and your password and the number to dial if you are using dial-up connection. All these information can be found from the letter from your ISP. Your computer can then save these items so that you don't have to type in them every time you want to connect to the Internet. If you are on a cyber café, all you need to do every time is to type in your username and password to gain access to the Internet. The essence of this process is to either authenticate the user's permission to use the internet through the local network or through the ISP, or to estimate the period when the Internet is in use.

You start accessing the internet as soon as you start your browser either by double clicking it on the desk top or lunching it through the task bar or start menu. The common operations involved in surfing the Internet include:

Browsing the Web Site; Browsing is an event in which internet users navigate through web pages for information. To visit a web site, you must know the web site's name you want to visit. To visit a web site, just type the name of the web site in the address field and click go or press "Enter" key on the keyboard. The home page of the web site is displayed, from where you can view or link other pages of the site.

Search the Web; To search the web means to look for information on the Internet. With the help of Internet Search Engines, one can easily get at particular information on the web. An Internet Search Engine is an Internet site designed to help user find information on a given subject, usually by locating several sites or web pages that have the required information.

There are many Search Engines existing today. They include:

- google.com,
- yahoo.com,
- altavista.com,
- 37.com,
- ask.com,
- USA.com,
- infoseek.com,
- lycos.com,
- 87.com,
- metacrawler.com,
- webcrawler.com, and
- excite.com.

The Google site is essentially a search engine that does not provide many other public websites services. It has one of the largest database coverage, searching more than 3 billion web pages to provide matches for queries.

When you type in the keywords into the search box and click **Google Search,** it then queries for the information across millions of web pages and in seconds presents you with several options.

Downloading a File; to download a file means to copy a file from the Internet to your computer. Actually to download implies to move data from a larger computer folder to a smaller one. Most downloadable programs in the internet provide for a link to be clicked on by those who want to download, and information, such as: click here to download, is given to notify the user.

4.2.6 Limitations of the Internet

There are quite a few limitations of the Internet or disadvantages, which include that Internet:

- is time consuming
- is sometimes costly
- can have corrupting influence
- degrades morals
- causes anxiety
- causes stereotyping
- can be a tool for dissemination of heresy
- has privacy infiltration risks

Attraction of people to your web site is a very **slow, tedious process** - search engines can take up to 3 to 6 months to start reporting your site.

UNIT 5: NETWORKING AND INTERNET PROTOCOLS

5.0 Introduction

Welcome to unit 5. This unit discusses the concept of networking, types of networking, networking topologies and protocols. It is envisaged that you will appreciate the content of this unit and think of its application.

5.1 Objectives

At the end of this unit, you shall be able to;

- define networking.
- describe the types of networks.
- diagrammatize the network topologies.

5.2 The concept of networking

Networking is defined as the act of interlinking multiple computers and computer devices, making contact and exchanging information with other people, groups and institutions to develop mutually beneficial relationships, or to access and share information between computers. A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. Two very common types of networks include: Local Area Network (LAN) Wide Area Network (WAN). You may also see references to a Metropolitan Area Networks (MAN), a Wireless LAN (WLAN), or a Wireless WAN (WWAN).

5.3 Types of networks

Basically, there are four types of networks according size. These are discussed below.

Personal Area Network

The Personal Area Network (PAN), is a computer network organized around an individual person within a building. This could be inside an office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles and other personal entertainment devices connected together.

If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network, or HAN. In a very typical setup, a residence will have a single wired Internet connection connected to a modem. This modem then provides both wired

and wireless connections for multiple devices. The network is typically managed from a single computer but can be accessed from any device.

This type of network provides great flexibility. For example, it allows you to:

- Receive and send a document to the printer in another office while you are sitting in your office with your laptop.
- Upload a photo from your cell phone to your desktop computer.
- Watch movies from an online streaming service to your TV.

If this sounds familiar to you, you likely have a PAN in your house without having called it by its name.

Local Area Network

A Local Area Network (LAN) is a network that is confined to a relatively small geographic area such as a writing lab, school, or building.

Computers connected to a network are broadly categorized as servers or workstations. Servers are generally not used by humans directly, but rather run continuously to provide "services" to the other computers (and their human users) on the network. Services provided can include printing and faxing, software hosting, file storage and sharing, messaging, data storage and retrieval, complete access control (security) for the network's resources, and many others.

Workstations are called such because they typically do have a human user which interacts with the network through them. Workstations were traditionally considered a desktop, consisting of a computer, keyboard, display, and mouse, or a laptop, with integrated keyboard, display, and touchpad. With the advent of the tablet computer, and the touch screen devices such as iPad and iPhone, our definition of workstation is quickly evolving to include those devices, because of their ability to interact with the network and utilize network services.

Servers tend to be more powerful than workstations, although configurations are guided by needs. For example, a group of servers might be located in a secure area, away from humans, and only accessed through the network. In such cases, it would be common for the servers to operate without a dedicated display or keyboard. However, the size and speed of the server's processor(s), hard drive, and main memory might add dramatically to the cost of the system. On the other hand, a workstation might not need as much storage or working memory, but

might require an expensive display to accommodate the needs of its user. Every computer on a network should be appropriately configured for its use.

On a single LAN, computers and servers may be connected by cables or wirelessly. Wireless access to a wired network is made possible by wireless access points (WAPs). These WAP devices provide a bridge between computers and networks. A typical WAP might have the theoretical capacity to connect hundreds or even thousands of wireless users to a network, although practical capacity might be far less (Router-switch.com, 2019).

Metropolitan Area Network

A metropolitan area network, or MAN, consists of a computer network across an entire city, college campus or small region. A MAN is larger than a LAN, which is typically limited to a single building or site. Depending on the configuration, this type of network can cover an area from several miles to tens of miles. A MAN is often used to connect several LANs together to form a bigger network. When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN.

Wide Area Network

Wide Area Networks (WANs) connect networks in larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of global network. Using a WAN, universities in Zambia can communicate with places like Tokyo in a matter of seconds, without paying enormous phone bills. Two users a half-world apart with workstations equipped with microphones and a webcams might teleconference in real time. A WAN is complicated. It uses multiplexers, bridges, and routers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN (BELDEN, 2019).

5.4 Advantages and disadvantages of installing a network

Advantages of installing a Network

User access control: Modern networks almost always have one or more servers which allows centralized management for users and for network resources to which they have access. User credentials on a privately-owned and operated network may be as simple as a user name and

password, but with ever-increasing attention to computing security issues, these servers are critical to ensuring that sensitive information is only available to authorized users.

Information storing and sharing: Computers allow users to create and manipulate information. The network provides both a place to store the information and mechanisms to share that information with other network users.

Connections: Administrators, employees, suppliers, customers, instructors and even students and guests can be connected using the campus network.

Services: The institution can provide services, such as registration, school directories, course schedules, access to research, and email accounts, and many others. (Remember, network services are generally provided by servers).

Internet: The institution can provide network users with access to the internet, via an internet gateway.

Computing resources: The institution can provide access to special purpose computing devices which individual users would not normally own. For example, a school network might have high-speed, high quality printers strategically located around a campus for instructor or student use.

Flexible Access: School networks allow students to access their information from connected devices throughout the school. Students can begin an assignment in their classroom, save part of it on a public access area of the network, then go to the media center after school to finish their work. Students can also work cooperatively through the network.

Workgroup Computing: Collaborative software allows many users to work on a document or project concurrently. For example, educators located at various schools within a county could simultaneously contribute their ideas about new curriculum standards to the same document, spreadsheets, or website.

Disadvantages of installing a Network

Expensive to Install: Large campus networks can carry hefty price tags. Cabling, network cards, routers, bridges, firewalls, wireless access points, and software can get expensive, and the installation would certainly require the services of technicians. But, with the ease of setup of home networks, a simple network with internet access can be setup for a small campus in an afternoon.

Requires Administrative Time: Proper maintenance of a network requires considerable time and expertise. Many schools have installed a network, only to find that they did not budget for the necessary administrative support.

Servers Fail: Although a network server is no more susceptible to failure than any other computer, when the files server "goes down" the entire network may come to a halt. Good network design practices say that critical network services (provided by servers) should be redundant on the network whenever possible.

Cables May Break: The Topology chapter presents information about the various configurations of cables. Some of the configurations are designed to minimize the inconvenience of a broken cable; with other configurations, one broken cable can stop the entire network.

Security and compliance: Network security is expensive. It is also very important. A school network would possibly be subject to more stringent security requirements than a similarly-sized corporate network, because of its likelihood of storing personal and confidential information of network users, the danger of which can be compounded if any network users are minors. A great deal of attention must be paid to network services to ensure all network content is appropriate for the network community it serves.

5.5 Network topologies

Network topology refers to how computers, printers and other devices are connected, and describes the layout of wires; devices and routing path on a network. When referring to topology through the lens of the "Internet of Things," it is how sensors, actuators and gateways communicate with one another. To decide which network is best for your organisation; you need to know the advantages and disadvantages of each. There are number of common topologies; point to point, bus, ring, star and mesh. I will be discussing them one by one. Below is diagram showing how computers and computer devices can be networked.

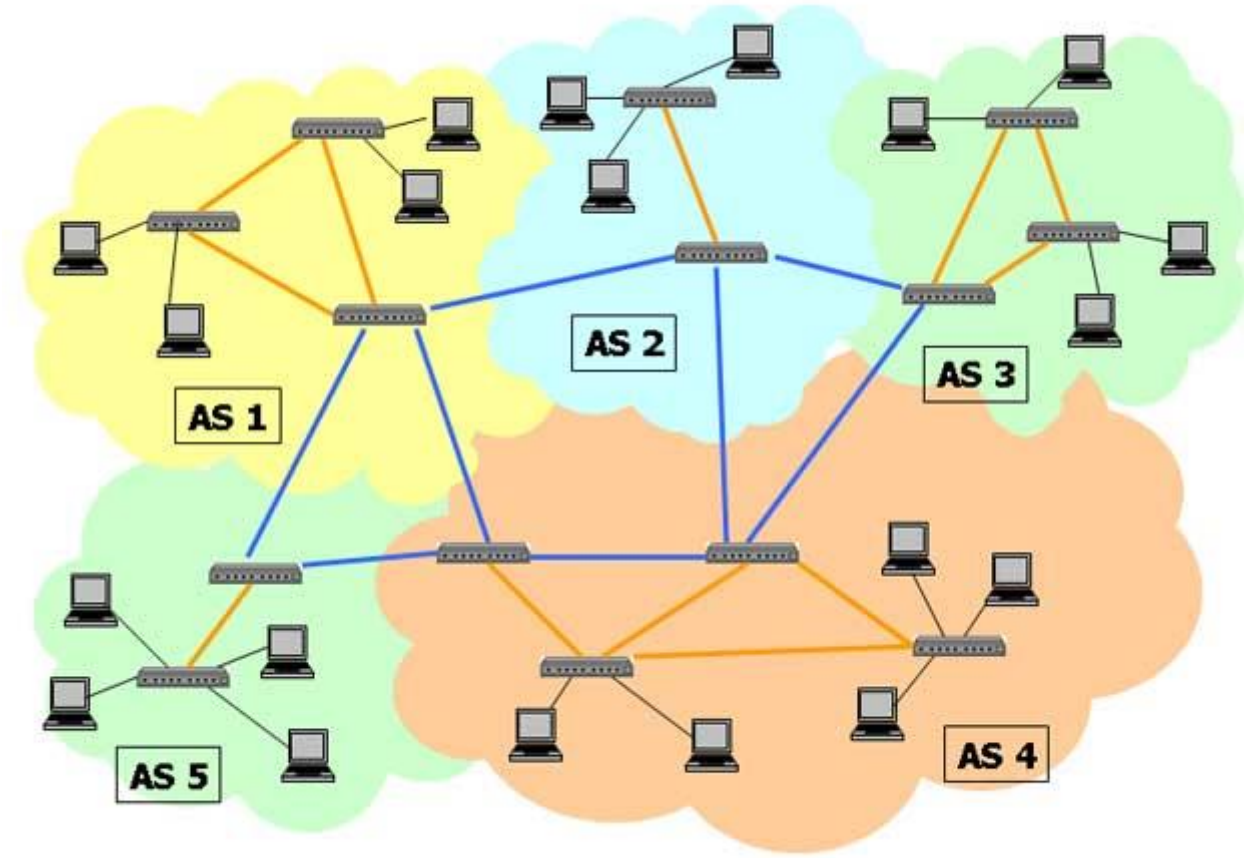


Fig 5: Networking computer and computer devices

The diagram above shows how PAN or LAN can be networked/linked to another e.g. AS1 with AS2, AS3, AS4 and/or AS5 and so forth.

5.6 Types of network topologies

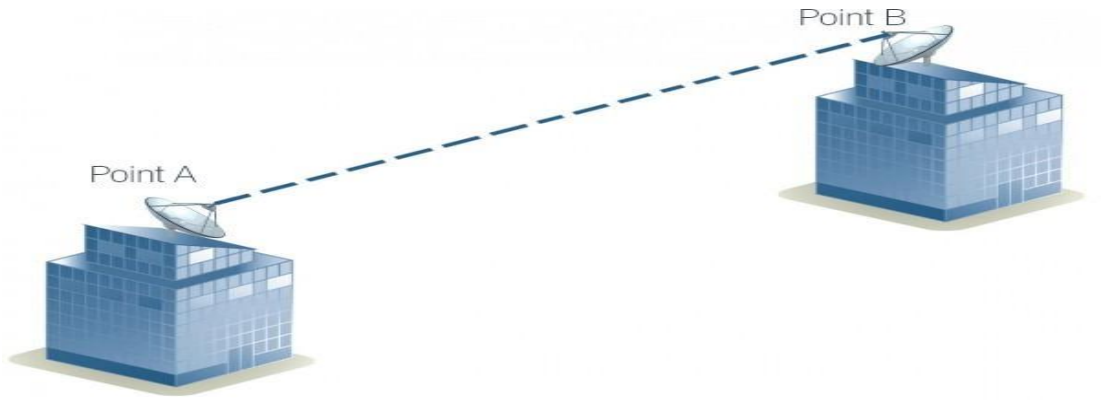
There are different types of network topologies. These are discussed below.

1. **Point to Point Topology**

A point-to-point network establishes a direct connection between two network nodes. Communication can take place only between these two nodes, or devices. An example of this type of network is a Bluetooth link between a cell-phone and an ear piece. The advantages of point-to-point networking are its simplicity and low cost. The primary limitations spring from the one-to-one relationship that exists between two devices; the network cannot scale beyond these two nodes, therefore it is not a widely used topology for organisations.

The advantage of point-to-point network topology is that it is much simpler than any other topology because the topology simply tunnels a flow of data either unidirectional or bidirectional between two points**.**

The disadvantage is that point-to-point networks are not very useful in organisations. However, they are still used in some SCADA systems, traffic data systems, or in point-to-point broadcast systems (like police or fire radios), but it rarely makes sense in organisations to have a receiver talk to a single node instead of multiple nodes. The diagram below shows point to point topology.



2. Star topology

In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection, with every computer indirectly connected to every other node with the help of the hub. The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network; but all of the nodes on the network must be connected to one central device. All traffic that traverses the network passes through the central hub as shown in the diagram below.

Source: Computernetworktopology.com, 2019

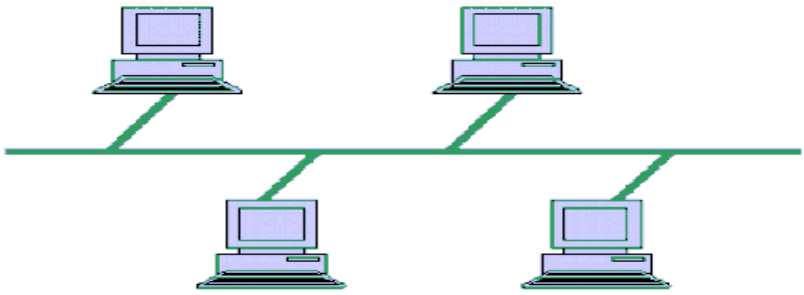
From the explanation above, the advantage of star topology is that all the complexity in the network is driven to a central node, so all the other nodes only need to communicate in their time or frequency slot. How they communicate depends on whether wireless multiplexing is

done through frequency-division multiple access (FDMA), time-division multiple access (TMA), or code-division multiple access (CDMA).

However, the primary disadvantage of star topology is that the radio link between; the gateway and the end node or terminal can be very long, which means the further a node is away from the gateway, the more energy it has to expend relaying a message. But unlike a mesh node that has to be constantly "awake, star nodes are able to rest between message transmissions, helping conserve the total amount of energy expended by each node.

3. Bus

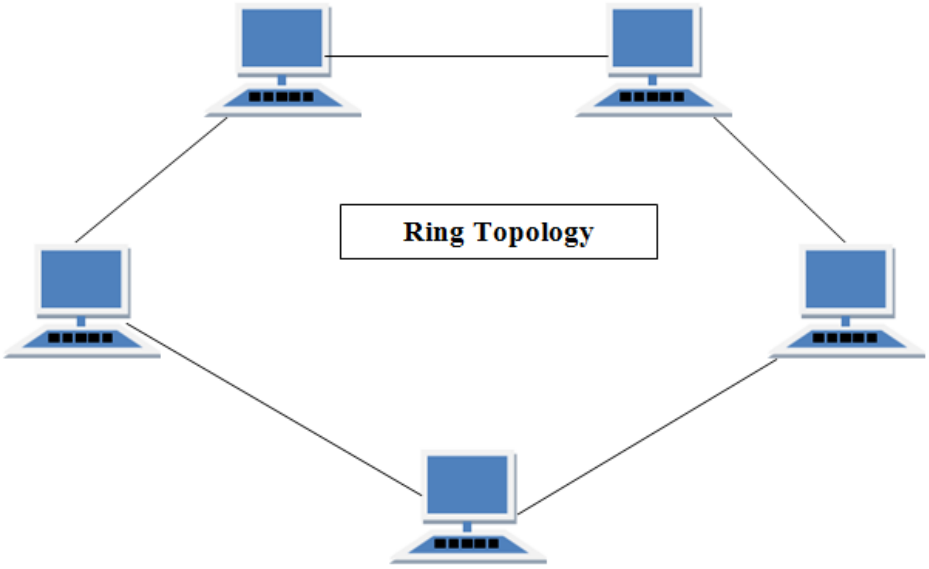
In local area networks where bus topology is used, each node is connected to a single cable with the help of interface connectors. This central cable is the backbone of the network and is known as the bus. A signal from the source travels in both directions to all machines; connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Because the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. The diagram below shows the bus topology.



4. Ring Topology

In the ring topology, the nodes are connected in the form of a ring with the help of twisted pair cable. Each node is connected directly to the other two nodes in the network. The node, which wants to send a message, first passes the message to its consecutive node in the network. Data is transmitted in the clockwise direction from one node to another.

Figure 4 shows the arrangement of computers in the ring topology. Each node incorporates a repeater, which passes the message to next node when the message is intended for another node.



Advantages of ring topology are:

- Each node has an equal access to other nodes in the network.
- Addition of new nodes does not degrade the performance of the network.
- Ring topology is easy to configure and install.

The following are the disadvantages of ring topology:

- It is relatively expensive to construct the ring topology.
- The failure of one node in the ring topology affects the other nodes in the ring.

5. Mesh Topology

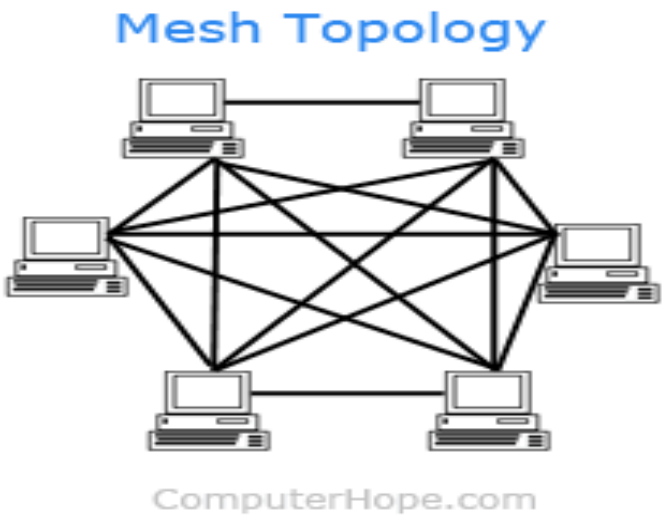
In Mesh Topology, all the computers are inter-connected to each other in a network. Each computer not only sends its own signals but also relays data from other computers. This type of topology is very expensive as it is very difficult to establish the connections of the mesh topology. In a Mesh topology every node has a point-to-point connection to the other node. The connections in the mesh topology can be wired or wireless.

Mesh Topology can be divided into two types:

1) Fully Connected Mesh Topology: has all the computers connected to every other computer.

2) Partial Connected Mesh Topology**:** all the nodes are not necessary to be connected with each other in a network. This partial mesh topology is less costly compared to full mesh topology.

Below is an example of mesh topology.



Advantages of Mesh Topology:

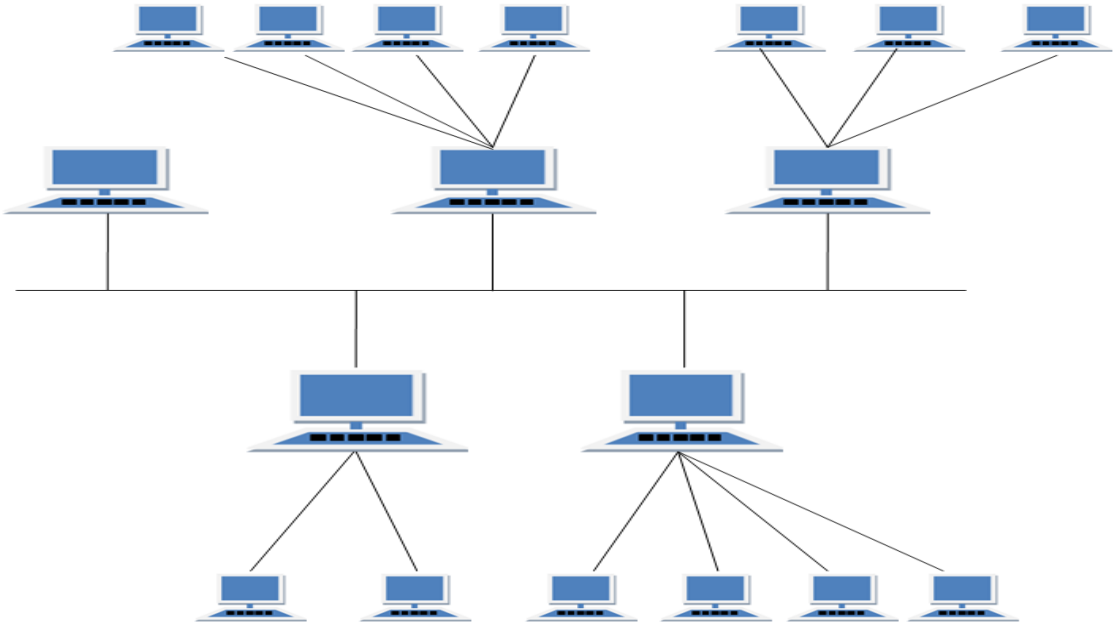
1. There is no traffic problem as there are dedicated point to point links for each computer.
2. It has multiple links, so if one route is blocked then other can be accessed for data communication.
3. It provides high privacy and security.
4. Fault identification is easy because of point-to-point connection.

Disadvantages of Mesh Topology:

1. Mesh topology requires high NO: of cables and I/O ports for the communication.
2. Installation is very difficult in mesh topology, as each node is connected to every node.
3. Mesh topology is costly compared to the other network topologies i.e. star, bus, point to point topology.

6. Hybrid Topology

The hybrid topology is the combination of multiple topologies, used for constructing a single large topology. The hybrid topology is created when two different network topologies are interconnected. If two ring topologies are connected, then the resultant topology is not the hybrid topology. On the other hand, if the ring topology is connected to the bus topology then the resulting topology is called the hybrid topology. This topology generally combines the features of the two or more topologies and is therefore, more effective and efficient than the individual topologies. Figure 6 shows a typical arrangement of computers in hybrid topology.



Source: Include Help.com, 2019

Advantages of hybrid topology are:

- The hybrid topology is more effective as it uses multiple topologies.
- The hybrid topology contains the best and efficient features of the combined topologies from which it is constructed.

The following are the disadvantages of hybrid topology:

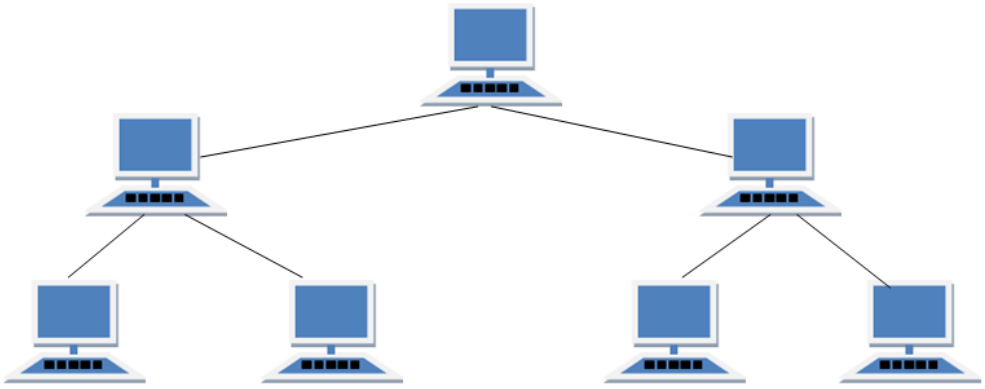
- The hybrid topology is relatively more complex than the other topologies.
- The hybrid topology is difficult to install and configure.

7. Hierarchical (Tree) Topology

The hierarchical topology is also known as tree topology, which is divided into different levels connected with the help of twisted pair, coaxial cable or fiber optics. This type of topology is arranged in the form of a tree structure in which top level contains parent node (root node), which is connected with the child nodes in the second level of hierarchy with point-to-point link. The second level nodes are connected to the third level nodes, which in turn are connected to the fourth level nodes and so on. Except the top-level nodes, each level node has a parent node.

The number of point-to-point links in the hierarchical type of topology is generally one less than the total number of nodes in the structure. The hierarchical topology is symmetrical, having a fixed branching factor, f, associated with each node. The branching factor is the number of point-to-point links between the levels of hierarchy.

Figure 8 below shows the arrangement of computers in hierarchical topology.



Advantages of hierarchical topology are:

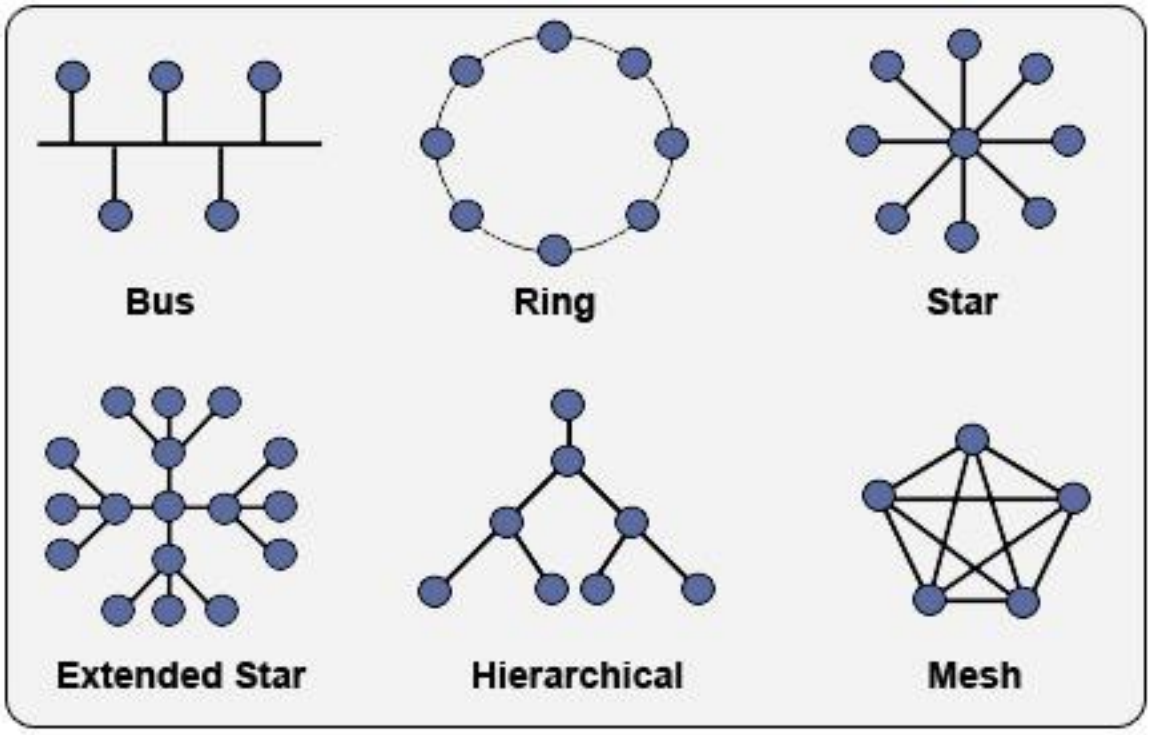
- The hierarchical topology is generally supported by most hardware and software.
- In the hierarchical topology, data is received by all the nodes efficiently because of point-to-point link.

The following are the disadvantages of hierarchical topology:

- In the hierarchical topology, when the root node fails, the whole network crashes.
- The hierarchical topology is difficult to configure.

ACTIVITY

Write brief notes on each of the following diagrams below.



5.7 Internet protocols

5.7.1 The concept of internet protocols

A protocol is a set of rules that governs the communications between computers on a network. In order for two computers to talk to each other, they must be speaking the same language. Many different types of network protocols and standards are required to ensure that your computer (no matter which operating system, network card, or application you are using) can communicate with another computer located on the next desk or half-way around the world. The OSI (Open Systems Interconnection) Reference Model defines seven layers of networking protocols. The complexity of these layers is beyond the scope of this tutorial; however, they can be simplified into four layers to help identify some of the protocols with which you should be familiar (see fig below).

OSI Layer	Name	Common Protocols
7	Application	HTTP | FTP | SMTP | DNS | Telnet
6	Presentation	
5	Session	
4	Transport	TCP | SPX
3	Network	IP | IPX
2	Data Link	Ethernet
1	Physical	

Fig 1. OSI model related to common network protocols

Figure 1 illustrates how some of the major protocols would correlate to the OSI model in order to communicate via the Internet. In this model, there are four layers, including:

- Ethernet (Physical/Data Link Layers)
- IP/IPX (Network Layer)
- TCP/SPX (Transport Layer)
- HTTP, FTP, Telnet, SMTP, and DNS(combined Session/Presentation/Application Layers)

Assuming you want to send an e-mail message to someone in Italy, we will examine the layers "from the bottom up" -- beginning with Ethernet (physical/data link layers).

5.7.2 Ethernet (Physical/Data Link Layers)

The physical layer of the network focuses on hardware elements, such as cables, repeaters, and network interface cards. By far the most common protocol used at the physical layer is Ethernet. For example, an Ethernet network (such as 10BaseT or 100BaseTX) specifies the type of cables that can be used, the optimal topology (star vs. bus, etc.), the maximum length of cables, etc. (See the Cabling section for more information on Ethernet standards related to the physical layer).

The data link layer of the network addresses the way that data packets are sent from one node to another. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple

Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

Ethernet

The original Ethernet standard was developed in 1983 and had a maximum speed of 10 Mbps (phenomenal at the time) over coaxial cable. The Ethernet protocol allows for bus, star, or tree topologies, depending on the type of cables used and other factors. This heavy coaxial cabling was expensive to purchase, install, and maintain, and very difficult to retrofit into existing facilities.

The current standards are now built around the use of twisted pair wire. Common twisted pair standards are 10BaseT, 100BaseT, and 1000BaseT. The number (10, 100, 1000) ands for the speed of transmission (10/100/1000 megabits per second); the "Base" stands for "baseband" meaning it has full control of the wire on a single frequency; and the "T" stands for "twisted pair" cable. Fiber cable can also be used at this level in 10BaseFL.

Fast Ethernet

The Fast Ethernet protocol supports transmission up to 100 Mbps. Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary. Fast Ethernet standards include:

- 100BaseT - 100 Mbps over 2-pair category 5 or better UTP cable.
- 100BaseFX - 100 Mbps over fiber cable.
- 100BaseSX -100 Mbps over multimode fiber cable.
- 100BaseBX - 100 Mbps over single mode fiber cable.

Gigabit Ethernet

Gigabit Ethernet standard is a protocol that has a transmission speed of 1 Gbps (1000 Mbps). It can be used with both fiber optic cabling and copper. (see the Cabling section for more information).

- 1000BaseT - 1000 Mbps over 2-pair category 5 or better UTP cable.
- 1000BaseTX - 1000 Mbps over 2-pair category 6 or better UTP cable.
- 1000BaseFX - 1000 Mbps over fiber cable.
- 1000BaseSX -1000 Mbps over multimode fiber cable.
- 1000BaseBX - 1000 Mbps over single mode fiber cable.

The Ethernet standards continue to evolve. with 10 Gigabit Ethernet (10,000 Mbps) and 100 Gigabit Ethernet (100,000 Mbps),

Ethernet Protocol Summary

Protocol	Cable	Speed
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps
Fast Ethernet	Twisted Pair, Fiber	100 Mbps
Gigabit Ethernet	Twisted Pair, Fiber	1000 Mbps

Older Network Protocols

Several very popular network protocols, commonly used in the 90's and early 21st century have now largely fallen into disuse. While you may hear terms from time to time, such as "Localtalk" (Apple) or "Token Ring" (IBM), you will rarely find these systems still in operation. Although they played an important role in the evolution of networking, their performance and capacity limitations have relegated them to the past, in the wake of the standardization of Ethernet driven by the success of the Internet.

5.7.3 IP and IPX (Network Layer)

The network layer is in charge of routing network messages (data) from one computer to another. The common protocols at this layer are IP (which is paired with TCP at the transport layer for Internet network) and IPX (which is paired with SPX at the transport layer for some older Macintosh, Linus, UNIX, Novell and Windows networks). Because of the growth in Internet-based networks, IP/TCP are becoming the leading protocols for most networks.

Every network device (such as network interface cards and printers) have a physical address called a MAC (Media Access Control) address. When you purchase a network card, the MAC address is fixed and cannot be changed. Networks using the IP and IPX protocols assign logical addresses (which are made up of the MAC address and the network address) to the devices on the network, This can all become quite complex -- suffice it to say that the network layer takes care of assigning the correct addresses (via IP or IPX) and then uses routers to send the data packets to other networks.

5.7.4 TCP and SPX (Transport Layer)

The transport layer is concerned with efficient and reliable transportation of the data packets from one network to another. In most cases, a document, e-mail message or other piece of information is not sent as one unit. Instead, it is broken into small data packets, each with header information that identifies its correct sequence and document.

When the data packets are sent over a network, they may or may not take the same route -- it doesn't matter. At the receiving end, the data packets are re-assembled into the proper order. After all packets are received, a message goes back to the originating network. If a packet does not arrive, a message to "re-send" is sent back to the originating network.

TCP, paired with IP, is by far the most popular protocol at the transport level. If the IPX protocol is used at the network layer (on networks such as Novell or Microsoft), then it is paired with SPX at the transport layer.

5.7.5 HTTP, FTP, SMTP and DNS (Session/Presentation/Application Layers)

Several protocols overlap the session, presentation, and application layers of networks. There protocols listed below are a few of the more well-known:

- DNS - Domain Name System - translates network address (such as IP addresses) into terms understood by humans (such as Domain Names) and vice-versa
- DHCP - Dynamic Host Configuration Protocol - can automatically assign Internet addresses to computers and users
- FTP - File Transfer Protocol - a protocol that is used to transfer and manipulate files on the Internet
- HTTP - HyperText Transfer Protocol - An Internet-based protocol for sending and receiving webpages

- IMAP - Internet Message Access Protocol - A protocol for e-mail messages on the Internet
- IRC - Internet Relay Chat - a protocol used for Internet chat and other communications
- POP3 - Post Office protocol Version 3 - a protocol used by e-mail clients to retrieve messages from remote servers
- SMTP - Simple Mail Transfer Protocol - A protocol for e-mail messages on the Internet

5.8 Summary

Much as you know, Internet today means the world business either in items of buying and selling of goods and services or transacting, negotiating and reaching agreement with other firms on the net. So much varying services it provides that maximize the essence of information technology. Based on personal value, little mention bottlenecks exist as enumerated above. However, this unit discussed the concept of internet; its emphasis much on its origin, the requirement for its connectivity, the information format, its usage and the limitation for the usage. It further discussed the types of network topologies that exist.

5.9 Revision Questions

1. What is Internet?
2. Enumerate the limitations of Internet.
3. Write short notes on any three Internet usages.
4. Give brief history of the Internet.

Add activity depicting real life situation

6.0 Introduction

Welcome to this unit. Having learnt internet and networking, you can now look at networking hardware. Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network. Hope you will enjoy the unit.

6.1 Objectives

At the end of the unit, you should be able to;

- describe the various components of the networking hardware.
- recommend the suitable networking hardware to the organisation.

6.2 Networking hardware

There are various networking hardware. However, selection is dependent on the size of the organisation, affordability and functionalities. Common networking hardware are discussed below.

File/Network Servers

One or more network servers is a part of nearly every local area network. These are very fast computers with a large amount of RAM and storage space, along with a one or more fast network interface card(s). The network operating system provides tools to share server resources and information with network users. A sophisticated permissions-handling system is included, so that access to sensitive information can be carefully tailored to the needs of the users. For small networks, a single network server may provide access control, file sharing, printer sharing, email, database, and other services.

The network server may be responding to requests from many network users simultaneously. For example, it may be asked to load a word processor program to one workstation, receive a database file from another workstation, and store an e-mail message during the same time period. This requires a computer that can store and quickly share large amounts of information. When configuring such a server, budget is usually the controlling factor. The following guidelines should be followed:

- Fastest processor(s)

- Large amount of RAM
- multiple large, fast hard drives
- Extra expansion slots
- Fast network interface card(s)

Optionally (if no other such devices are available on the network):

- A RAID (Redundant Array of Inexpensive Disks) to preserve large amounts of data(even after a disk failure)
- A back-up unit (i.e. DAT tape drive, removable hard drives, or CD/DVD/BluRay burner)

Workstations

Computers that humans use are broadly categorized as workstations. A typical workstation is a computer that is configured with a network interface card, networking software, and the appropriate cables. Workstations do not necessarily need large storage hard drives, because files can be saved on the file server. Almost any computer can serve as a network workstation.

Laptops/Mobile Devices

Laptops and other mobile devices are becoming more and more common. These devices typically have modest internal storage, but enough power to serve as a workstation for users on the go. These machines nearly always have a wireless adapter to allow quick network connections without cumbersome cabling. In a school environment with good wireless coverage, a mobile device user can move about the campus freely, and remain continuously connected to the network.

Network Interface Cards

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, and they are included in the purchase of most computers. Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using. The most common network interface connections are Ethernet cards and wireless adapters.

Ethernet Cards

Ethernet cards are usually included with a computer, although additional ethernet cards can be purchased and installed on most computers, Ethernet cards can contain connections for either coaxial or twisted pair cables (or both) (See fig. 1). If it is designed for coaxial cable, the connection will be

BNC. If it is designed for twisted pair, it will have a RJ-45 connection. Some Ethernet cards also contain an AUI connector. This can be used to attach coaxial, twisted pair, or fiber optics cable to an Ethernet card. When this method is used there is always an external transceiver attached to the workstation.

Wireless Adapters

Wireless adapters are found in most portable devices, such as laptops, smart phones, and tablet devices. External wireless adapters can be purchased and installed on most computers having an open USB (Universal Serial Bus) port, or unused expansion slot.

Switches

An ethernet switch is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central switch/hub. Most switches are active, that is they electrically amplify the signal as it moves from one device to another. The predecessor of the switch was the hub, which broadcasted all inbound packets out all ports of the device, creating huge amounts of unnecessary network traffic. Modern switches build a port map of all IP address which respond on each port, and only broadcasts on all ports when it doesn't have a packet's target IP address already in its port map. Switches are:

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or tree topology
- Available as "managed" or "unmanaged", with the later less expensive, but adequate for smaller networks
- direct replacements for hubs, immediately reducing network traffic in most networks
- Usually installed in a standardized metal rack that also may store network servers, bridges, or routers

Repeaters

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters.

The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

Bridges

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two. A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. You might say that the bridge is like a traffic cop at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling, or physical topologies. They must, however, be used between networks with the same protocol.

Routers

Routers are the traffic directors of the global internet. All routers maintain complex routing tables which allow them to determine appropriate paths for packets destined for any address. Routers communicate with each other, and forward network packets out of or into a network. Here's an example:

You want to search for something on the internet using a search engine. You open a browser on your workstation. The browser opens to a blank page (not usually the default, but appropriate for this example). You type "http://www.google.com" into the URL (Universal Resource Locator) address line of the browser. The browser software packages up the URL you typed, and sends it with a request for an IP address to the DNS (Domain Name Server) that has been set in your network adapter's configuration. The domain server returns an IP, such as 74.125.67.103 (actual address returned by DNS for google.com on June 7th, 2011). The browser ships the request for that IP address off to the network card, which bundles the request into an ethernet packet, destined for 74.125.67.103. The network card sends the packet to the gateway of your network, which opens the header of the packet, and makes a determination that the packet is traveling out of your network, in search of 74.125.67.103. Your network's router has routing tables which it has been building from communicating with other routers, and potentially augmented with "static routes", which are specific

paths added by your network's administrators to make the task of accessing certain networks easier, or faster, or in some cases, not possible. In this case, I find that my router knows about another router at my ISP(Internet Service Provider), which in turn has several more routers that are all on networks of which I am just a small node, much like finding an atom of a molecule of a piece of dust on a rock on a moon of a planet of a sun of a galaxy of the universe. In any case, the packet gets passed from router to router, each time moving out of the subnets of the packet sender, towards a router that will know where the desired server is. The packet finally reaches the router of the network at 74.125.67.103, which dutifully delivers the packet to the server at that IP address. The server carefully crafts a response, and sends a reply back, which follows the same process to get the response "Yes. Go ahead" back to the requester. Whew. And that's just the initial request.

While bridges know the addresses of all computers on each side of the network, routers know the addresses other routers which in turn know about their own networks. Routers can even "listen" to entire networks to determine which sections are busiest -- they can then redirect data around those sections until traffic congestion clears.

So, routers are network gateways. They move network packets from one network to another, and many can convert from one network protocol to another as necessary. Routers select the best path to route a message, based on the destination address of the packet. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.
If you have a organisation LAN that you want to connect to the Internet, you will need to purchase a router. In this case, the router serves as the forwarder between the information on your LAN and the Internet. It also determines the best route to send the data over the Internet.

Firewalls

A firewall is a networking device that is installed at the entrance to a LAN when connecting a networks together, particularly when connecting a private network to a public network, such as the internet. The firewall uses rules to filter traffic into and out of the private network, to protect the private network users and data from malevolent hackers. Firewalls are either hardware or software, depending on their intended use. A firewall used to protect a network is a hardware device that should be installed in the network between the router and the network. Almost all hardware firewalls will have at least two ports, labelled "Trusted" and "Untrusted". These terms imply the true nature

of the firewall's responsibility to the private network. The public network is connected to the untrusted network port, and the private network is connected to the trusted port.

Firewall rules are usually simple, consisting of a verb, either allow or deny, the direction of the traffic, either inbound or outbound, and an address or other network traffic identifier. Firewall rules are cumulative, so general rules may be specified, and exceptions added as necessary. Some examples are:

- Allow outbound all (all private network users can do anything on the public network)
- Deny inbound all (default setting to prevent all traffic from the public or untrusted port, to the private port)
- Allow inbound port 80 (allow internet web traffic to come into network to find web servers)
- Allow inbound port 80 destined to 170.200.201.25 (allow inbound web traffic to a specific web server on your private network)
- Deny inbound from 201.202.1.1/24 (deny all inbound traffic from a specific IP address or range of addresses)

Software firewalls are commonly included in modern workstation and server operating systems. They operate in a similar way as hardware firewalls, except that they filter traffic in and out of the machine itself. These software firewalls are typically unnoticed by machine users, and only need attention occasionally when an internet-connected application don't work as expected. The software firewall should always be considered a "suspect" in such cases. The problem is easily resolved, by setting an exception rule in the firewall for the software that is attempting to communicate.

6.3 Summary

Student, you have successfully finished unit 6 on networking hardware. You have learnt the various types of networking hardware and how they are used. Hope you can recommend the right networking hard to your organisation of your choice.

6.4 Revision Questions

1. Discuss the various existing networking hardware.
2. Which ones would you recommendation to the institution of your choice?
3. Defend your answer in 2.

UNIT 7: MODES OF INFORMATION COMMUNICATION AND COMPUTER OPERATION

7.0 Introduction

Student, it is always said that communication is the brain behind information. An obvious fact is that without communication there is no information flow. Where there is no information flow, decisions made are not informed. Discussed in this unit are the modes of communication and their implication.

7.1 Objectives

At the end of this unit, you should be to;

- describe the different ways information can be communicated.
- explain the modes of computer operation.

7.2 Types of modes

There are different types of information modes. These are;

7.2.1 Simplex Mode

In this mode of information communication, information flow takes place only in one direction. That is, information can be either transmitted or received but not both. A system can only receive information and will never transmit information or transmit only but cannot receive information. A commercial radio station transmission is an example of simplex mode of communication.

7.2.2 Duplex Mode

In this mode of information communication, information flow both directions. A mode of where the information flow in both direction, but not at the same time is referred to as half-duplex mode of communication. But a full-duplex mode allows communication in both direction and the same time as well. An example of half – duplex mode system is a two-way radio set popularly known as walkie-talkie that allows one user listens while the other talks as the circuitry of the receiver is automatically turn off during transmission mode. A good example of full duplex mode is the handsets invoke everywhere today.

7.2.3 Network System Mode

Computer network system is a communication system whereby many computer systems are linked together for the purpose of sharing information as well time among the computer users. Distribution of computations among computers, coordination among processes running on different computers, remote input/output device accesses, remote data and file accesses, personal communications, internet, world wide web are possible through computer network system.

7.2.4 Computer Operation Modes

Modes of computer operation refer to various ways computer can be operated upon with regard to other computer or components. We are going to discuss three modes of operation: stand alone, batch processing and time-sharing modes.

7.2.4 Stand -Alone Mode

In this mode of operation, it is only one user that is permitted a time to use the computer. This implies that a current user must quit and give way before another user can operate the system. This mode is rampantly used especially with personal computers as laptops, desktops or notebooks.

7.2.5 Batch Processing Mode

This is a mode of operation whereby tasks belonging to different computer users are stored in the computer memory in queues and the jobs are then executed one after the other according to order they were served. Because jobs can be prioritized, jobs with less priority can over stay without being executed.

7.2.6 Time – Sharing Mode

This is the mode of computer operations whereby a user is allocated a given time slice, typically some seconds, during which the user can do whatever he wants. Time sharing mode is a special multiprogramming mode which involves the sharing of time among all the users of a given computer. The computers are often located far away from the various users and the interconnected to them through telecom or data communication network. It is worthy of note that time sharing is an internal activity within the system unit.

7.3 Terminal

A terminal is an input/output that uses a keyboard for input and a monitor for output. The most common type of terminal is dumb. This terminal can only be used to receive information from a computer. An example of a dumb terminal is airline clerks at airport ticket and check – in counter. Another type of terminal is intelligent terminal where information can be processed using an inbuilt processor. Examples include Automated Teller machine and Point of Scale.

7.4 Teleprocessing

It is process whereby computer are connected to the central processor by telecommunication network by special dedicated satellite links or microwave using a terminal located on a remote stations. Data and instructions inputs from each remote station are transmitted to the central processor and the result of the processing is transmitted back almost immediately.

7.5 Summary

The flow of information within an organization is the strong force that draws the major economic stream of business. The configuration of computer determines the mode which it operates. The direction which information flows is the subject to communication mode. I have been able to put you through the modes of computer operations like stand alone, batch processing and time sharing modes. Also, the different information communication modes such as simplex, half duplex and full duplex modes.

7.6 Revision Questions

1. Explain the modes of computer operations.
2. What is teleprocessing?
3. Analyse the modes of information flows.

UNIT 8: INFORMATION SECURITY

1.0 Introduction

The organizational information contained in computer files and disks need to be protected against malicious damages and attacks from unscrupulous intruders. This is because information is a strategic resource which is exclusively used by staff and management of that organization. This attacks which can be perpetuated through the environment, hardware or software disclose organizational information to unauthorized users hence exposing them to a lot of dangers. Computers and the information they contain are often considered confidential because they are restricted from a number of users. Discussed in this unit is the concept of information security and its implication on an organisation.

8.1 Objectives

At the end of this unit, you should be able to:

- explain the concept of information security.
- discuss the threats to computer security
- describe the different security measures

8.2 Meaning of Computer Security

Computer security is a branch of technology known as information security. The objective of computer security includes protection of information and property from theft, corruption, modification or natural disaster while allowing the information to remain accessible and productive to its intended users. In other words, computer security is a technique developed to safeguard information and information processing tools in a computer from malicious users. Computers and the information they contain are often considered as confidential systems because their uses are typically restricted to a limited number of users. This confidentiality can be compromised in a variety of ways hence introducing threats to the computer. People who intentionally break through ones confidentiality are computer experts who are knowledgeable enough in information processing techniques and software programming. With the ever increasing use of computers in diverse application areas of human endeavours therefore has made computer security a global issue.

8.3 Threats to a Computer

With their increasing power and versatility, computers simplify day-to-day activities of life. Unfortunately, as computer use becomes more widespread, so do the opportunities for misuse. Computer hackers (people who illegally gain access to other people's computer systems often violating privacy and tampering with, modifying or destroying records. Programs called viruses or worms can replicate and spread from computer to computer, erasing information or causing system malfunctions. The various threats to a computer include the following:

8.3.1 Computer Virus

Computer viruses have been a problem for years and are still prevalent today. The common blunder people make when the topic of computer virus arises is to refer to a worm or Trojan horse as a virus. These words which are normally used interchangeably do not exactly have the same meaning. Yet they are all malicious programs that can cause CITage to your computer.
A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner. It attaches itself to a program or file enabling it to spread from one computer to another and leaving infections as it travels. A true virus can only spread from one computer to another when its host is taken to the target computer. For instance, if a user sent a virus over a network or carried it in a removable storage medium (floppy disk, compact disk (CD), digital video disk (DVD), or Universal Serial Bus (USB) drive (Flash)), it increases the chances of spreading to other computers by infecting files. Like a human virus, a computer, a computer virus may exist on your computer but it actually would not infect your computer unless you run or open the malicious program. At this point, it is important to note that a virus cannot be spread without a human action such as running an infected program or file to keep it going. People unknowingly continue the spread of computer virus by sharing infected files, removable storage devices and network resources.

In order to replicate itself, a virus must be permitted to execute codes and write to memory. For this reason, many viruses attach themselves to executable files that may be part of the legitimate programs. If the user attempts to run an infected program, the virus code may be executed simultaneously. Viruses can be divided into two types based on their behaviour when they are executed.
They are:-

(a) **Non Resident Viruses:** These are viruses that immediately search for the hosts that can be infected, infects them and finally transfers control to the application program

they infected. Hence they can be thought to have a finder module and a replication module. The finder module is responsible for finding new files to infect. Foe each executable file the finder module encounters, it calls the replication module to infect that file with a copy of itself.

(b) **Resident Viruses:** These are viruses that do not search for hosts when they are started. Instead, a resident virus loads itself into the memory on execution and transfers control to the host program. The virus stays active in the background and infects new host when those files are accessed by other programs or the operating system itself. Resident viruses therefore contain a replication module similar to the one that is employed by non-resident viruses. This module is not called by a finder module. The virus loads the replicating module into the memory when is executed instead and ensures that this module is executed each time the operating system is called to perform a certain operation. The replication module can be called for example each time the operating system executes a file. In this case, the virus infects every suitable program that is executed on the computer.

8.3.2 Computer worms

A worm is similar to a virus by design. Worms are self-replicating computer programs that use networks to send copies of it to other nodes (computers on networks) and may do so without intervention. Worms spread from computer to computer but unlike the virus, it has the capability to travel without any human action. A worm takes advantage of a file or information transport features on your system which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system. So, rather than your computer searching out a single worm, it would send out hundreds or thousands of copies of itself creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then the worm replicates and sends itself out to every address listed in each of the receivers address book and the manifest continues. Due to the copying nature of worms and its capability to travel across networks, the end result in most cases is that the worm consumes too much system memory or network bandwidth causing network servers and individual computers to stop responding. In recent worm attacks such as the much dreaded Blaster worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer from remote ends.

The main difference therefore between a computer virus and computer worm is that a virus is a set of computer programs that attaches itself to programs or files in other computers. The viruses are often parts of documents that are transmitted as attachments. On the other hand, a worm is similar to a virus but is a self-contained program that replicates and transports itself from one computer to another.

8.3.3 Trojan Horse

A Trojan horse is as much trickish as the mythological Trojan horse it was named after. The Trojan horse is a destructive program disguised as a utility or application program. At first glance, it will appear to be useful software but will actually do something devious to the computer once installed or run on the computer. Those on the receiving end of a Trojan horse are usually tricked into opening them because they appear to be receiving legitimate software files from legitimate sources. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious like changing your desktop, adding silly active desktop icons or they can cause serious CITage by deleting files and destroying information on your system. Trojans are also known to create backdoor on your computer that gives malicious users access to your system possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

8.3.4 Logic Bombs

This infects computers memory but unlike a virus, it does not replicate itself. A logic bomb delivers its instructions when triggered by specific conditions such as when a particular date or time is reached or when a combination of letters is typed on a keyboard. A logic bomb has the ability to erase a hard disk drive or delete certain files.

8.3.5 Computer Hackers

These are people who illegally gain access to computer systems and often violating privacy and tampering with or destroying records. Unfortunately computer hackers are experts that are totally engrossed in computer technologies. In 1980s, with the advent of personal computers and dial up computer networks, hackers acquired a pejorative connotation often referring to someone who secretively invades other people's computers, inspecting and tampering with the programs or data stored on them.

Furthermore, malicious hackers are increasingly developing powerful software, crime tools such as virus generators, Internet eavesdropping sniffers, password guessers, vulnerability testers and computer service saturators. For example, an Internet eavesdropping sniffers intercepts Internet messages sent to other computers. A password guesser tries millions of combination of characters in an effort to guess a computers password. Vulnerability testers look for software weaknesses. These crime tools are also valuable security tools for testing the security of computers and networks. Some hackers go beyond mere programming and takes apart operating systems and programs to see what makes them tick.

8.3.6 Blended Threats

A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious program codes into one single threat. Blended threats can use server and Internet vulnerabilities (weaknesses) to initiate then transmit and also spread an attack. Characteristics of blended threats are

- They cause harm to the infected system or network
- They propagate using multiple methods
- Their attack could come from multiple points
- They exploit vulnerabilities

To be considered a blended threat, the attack would normally serve to transport multiple attacks in one payload. For example, it wouldn't just launch a denial of –service (DoS) attack; it would also for example install a backdoor and may even CITage a local system in one shot. DoS is an illegal attempt to put a computer out of action by overloading it with data from many sources simultaneously. Additional blended threats are designed to use multiple modes of transport. So while a worm may travel through e-mails easily, a single blended threat could use multiple routes including e-mail, file sharing network, etc

Lastly, rather than a specific attack on a predetermined **.**exe file, a blended threat could do multiple malicious acts like modifying your files, Hypertext Mark-up Language (HTML) files and registry keys at the same time. This means that it can basically cause CITage within several areas of your network at the same time. Blended threats therefore are considered to be the worst risk to security. Most blended threats also require no human intervention to propagate.

6.3.7 Hardware Failure/ Malicious CITage

Computer components (hardware) are subject to failure just as any other machine. The computer contains vital information that ought to be preserved. To ensure the sustenance of the

component parts and the information they contain, one should be aware of the causes of hardware failure which could come from power supply, destruction of computer hardware (fire, flood, theft, etc), malicious CITage, etc. Malicious CITage of some component parts can be done by criminals who though are computer staff but intend to defraud the organization poses a major security threat. To overcome this, appropriate authorization, environmental security and backups would aid in reducing this threat.

8.4 Information Security Measures

Computers and the information they contain are often considered confidential systems because of its sensitivity. This confidentiality which can be compromised in a variety of ways can be curbed using a variety of security techniques. They include

8.4.1 Backup

Storing backup copies of software and data and having backup computer and communication capabilities are important basic safeguards because the data can then be restored if it was altered or destroyed by a computer crime or accident. This back up can equally be done on removable storage devices like floppy disks, compact disks (CD), digital convergence disk (DVD), USB flash, hard disks, etc. Computer data should be backed up frequently and should be stored nearby in secure locations in case of CITage at the primary site. Transporting sensitive data to storage locations should also be done securely.

8.4.2 Encryption

Another technique to protect confidential information is encryption. Encryption is a process of converting messages or data into a form that cannot be read without decrypting or deciphering it. The root of the word encryption— *crypt*—comes from the Greek word *kryptos*, meaning “hidden” or “secret.” The study and practice of encryption and decryption is called the science of cryptography. Scientists who study different ways to protect and ensure the confidentiality, integrity, and authenticity of information are called cryptologists. Cryptologists also engage in cryptanalysis to find ways to break encryption methods.

Encryption uses a step-by-step procedure called an algorithm to convert data or the text of an original message, known as plaintext, into cipher text, that is its encrypted form. Cryptographic algorithms normally require a string of characters called a key to encrypt or decrypt data. Those who possess the key and the algorithm can encrypt the plaintext into cipher text and then

decrypt the cipher text back into plaintext. Computer users can scramble information to prevent unauthorized users from accessing it. Authorized users can unscramble the information when needed by using a secret code called a key. Without the key the scrambled information would be impossible or very difficult to unscramble. A more complex form of encryption uses two keys, called the public key and the private key, and a system of double encryption. Each participant possesses a secret, private key and a public key that is known to potential recipients. Both keys are used to encrypt, and matching keys are used to decrypt the message. However, the advantage over the single-key method lies with the private keys, which are never shared and so cannot be intercepted. The public key verifies that the sender is the one who transmitted it. The keys are modified periodically, further hampering unauthorized unscrambling and making the encrypted information more difficult to decipher.

Cryptologists engage in an unending competition to create stronger cryptographic techniques and to break them. Many recent cryptography techniques are nearly unbreakable even with the most powerful computers. These systems produce cipher text that appears to be random characters. These systems resist most existing methods for deciphering back into plaintext. The many different types of new cryptosystems use highly complex mathematical language and resist breaking even though cryptologists may know the techniques used in creating them. Three of the most popular cryptography systems used are the Data Encryption Standard (DES), Pretty Good Privacy (PGP), and the Rivest, Shamir, Adleman (RSA) system. DES uses a single key for both encrypting and decrypting. It was developed by International Business Machines Corporation (IBM) and approved by the United States National.

Institute of Standards and Technology in 1976. The Rivest, Shamir, Adleman (RSA) algorithm is a popular encryption method that uses two keys. It was developed for general use in 1977 and was named for the three computer scientists—Ronald L. Rivest, Adi Shamir, and Leonard Adleman—who originated it. The RSA Data Security Company has been highly successful in licensing its algorithm for others to use. PGP is an encryption system that also uses two keys. It is based on the RSA algorithm. PGP was invented by software developer Philip Zimmerman and is one of the most common cryptosystems used on the Internet because it is effective, free, and simple to use. PGP is such an effective encryption tool that the United States government sued Zimmerman for releasing it to the public, alleging that making PGP available to enemies of the United States would endanger national security. The lawsuit was dropped, but it is still illegal in some countries to use PGP to communicate with people in other countries.

8.4.3 Approved Users

Another technique to help prevent abuse and misuse of computer data is to limit the use of computers and data files to approved persons. Security software can verify the identity of computer users and limit their privileges to use, view, and alter files. The software also securely records their actions to establish accountability. Military organizations give access rights to classified, confidential, secret, or top-secret information according to the corresponding security clearance level of the user. Other types of organizations also classify information and specify different degrees of protection.

8.4.4 Passwords

These are confidential sequences of characters that allow approved persons to make use of specified computers, software, or information. To be effective, passwords must be difficult to guess and should not be found in dictionaries. Effective passwords contain a variety of characters and symbols that are not part of the alphabet. To thwart impostors, computer systems usually limit the number of attempts and restrict the time it takes to enter the correct password. A more secure method is to require possession and use of tamper-resistant plastic cards with microprocessor chips, known as “smart cards,” which contain a stored password that automatically changes after each use. When a user logs on, the computer reads the card's password, as well as another password entered by the user, and matches these two respectively to an identical card password generated by the computer and the user's password stored in the computer in encrypted form. Use of passwords and 'smart cards' is beginning to be reinforced by biometrics, identification methods that use unique personal characteristics, such as fingerprints, retinal patterns, facial characteristics, or voice recordings.

8.4.5 Firewalls

A firewall is a system that prevents unauthorized use and access to your computer. A firewall can be either hardware or software. Hardware firewalls provide a strong degree of protection from most forms of attack coming from the outside world and can be purchased as a stand-alone product or in broadband routers. Unfortunately, when battling viruses, worms and Trojans, a hardware firewall may be less effective than a software firewall, as it could possibly ignore embedded worms in outgoing e-mails and see this as regular network traffic.

For individual home users, the most popular firewall choice is a software firewall. A good software firewall will protect your computer from outside attempts to control or gain access your computer, and usually provides additional protection against the most common Trojan programs or e-mail worms. The downside to software firewalls is that they will only protect the computer they are installed on, not a network. It is important to remember that on its own a firewall is not going to rid you of your computer virus problems, but when used in conjunction with regular operating system updates and a good anti-virus scanning software, it will add some extra security and protection for your computer or network. Computers connected to communication networks, such as the Internet, are particularly vulnerable to electronic attack because so many people have access to them. These computers can be protected by using firewall computers or software placed between the networked computers and the network. The firewall examines, filters, and reports on all information passing through the network to ensure its appropriateness. These functions help prevent saturation of input capabilities that otherwise might deny usage to legitimate users, and they ensure that information received from an outside source is expected and does not contain computer viruses.

8.4.6 Intrusion Detection Systems

Security software called intrusion detection systems may be used in computers to detect unusual and suspicious activity and, in some cases, stop a variety of harmful actions by authorized or unauthorized persons. Abuse and misuse of sensitive system and application programs and data such as password, inventory, financial, engineering, and personnel files can be detected by these systems.

8.4.7 Application Safeguards

The most serious threats to the integrity and authenticity of computer information come from those who have been entrusted with usage privileges and yet commit computer fraud. For example, authorized persons may secretly transfer money in financial networks, alter credit histories, sabotage information, or commit bill payment or payroll fraud. Modifying, removing, or misrepresenting existing data threatens the integrity and authenticity of computer information. For example, omitting sections of a bad credit history so that only the good credit history remains violates the integrity of the document. Entering false data to complete a fraudulent transfer or withdrawal of money violates the authenticity of banking information. These crimes can be prevented by using a variety of techniques. One such technique is *checksumming*. Checksumming sums the numerically coded word contents of a file before and

after it is used. If the sums are different, then the file has been altered. Other techniques include digital signatures, cyclic redundancy checks, authenticating the sources of messages, confirming transactions with those who initiate them, segregating and limiting job assignments to make it necessary for more than one person to be involved in committing a crime, and limiting the amount of money that can be transferred through a computer.

8.4.8 Disaster Recovery

Organizations and businesses that rely on computers need to institute disaster recovery plans that are periodically tested and upgraded. This is because computers and storage components such as diskettes or hard disks are easy to CITage. A computer's memory can be erased or flooded with irrelevant information, fire, or other forms of destruction can CITage the computer's hardware. Computers data and components should be installed in safe and locked facilities.

8.5 Summary

Well done. You have come to the end of the unit. You have learnt that computer security is an important concept considered in the usage of any computer system either as a stand-alone computer or in a network. It is critical in almost all technology driven industry which operates on computer systems. The topics covered in this unit ranges from the rudimentary understanding of what computer and information security is all about to those factors that constitutes a threats to computer and information stored in it. We also discussed in detail the measures to combat these threats.

8.6 Revision Questions

1. What is computer security and why are portions of organizational budgets spent on managing information.
2. The use of removable storage media in various computers and networks increases the chances of spreading the virus. Discuss.
3. Differentiate between the resident and non-resident viruses.
4. Differentiate between a computer worm and the Trojan horse.
5. What is a blended threat and why is it referred to as the most dangerous?
6. Briefly explain the three most popular cryptographic systems.

9.0 Introduction

Almost every organisation is moving towards globalisation and choosing the best system for information management is key to gain a competitive advantage. Discussed in this unit are the phases in system development and data base management.

9.1 Objectives

At the end of this unit, you should be able to;

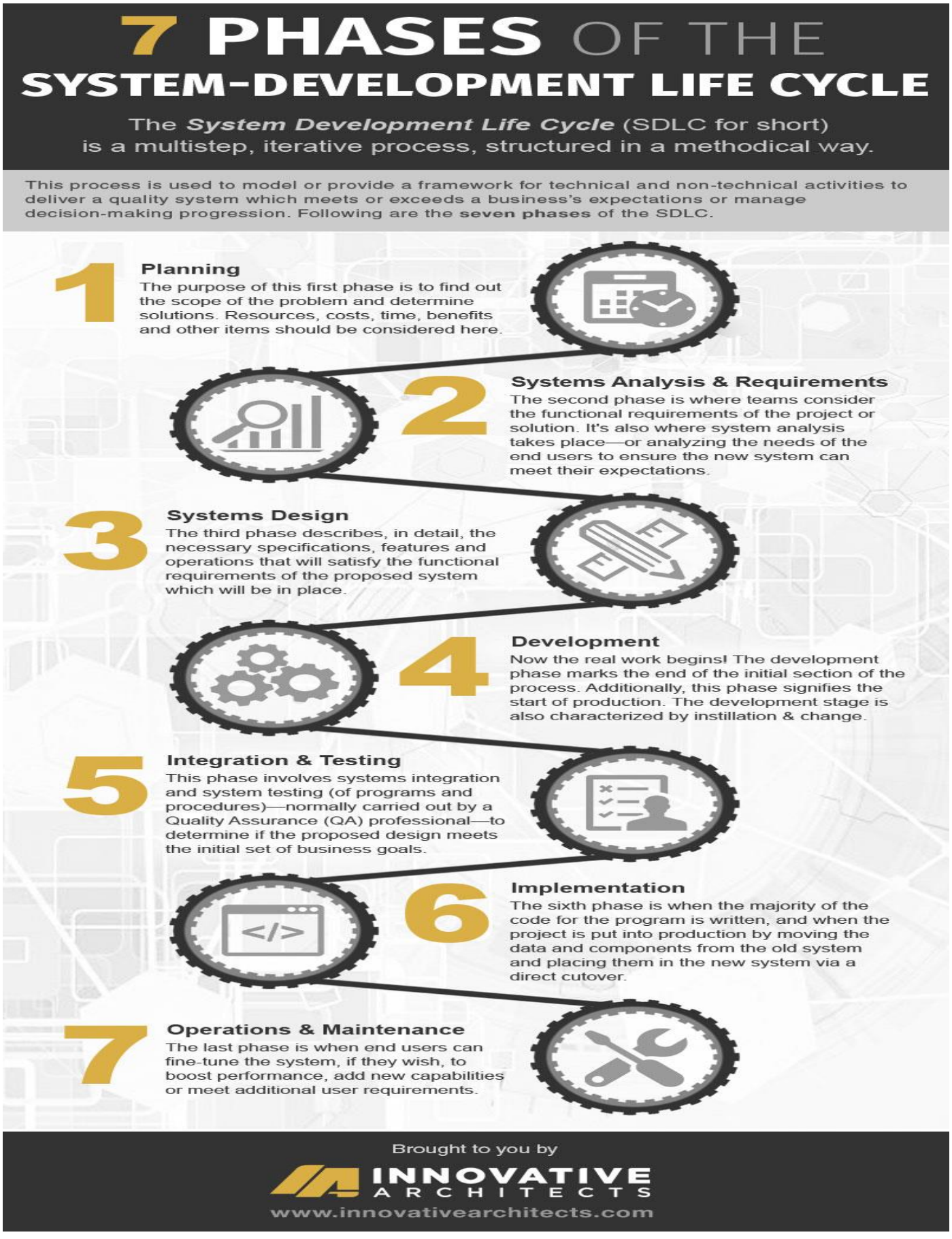
- Describe the phases in system development.
- Discuss data base management and its implication in the organisation.

9.2 Phases in System Development Life Cycle

The system-development life cycle enables users to transform a newly-developed project into an operational one. The System Development Life Cycle (SDLC) is a multistep, iterative process, structured in a methodical way. This process is used to model or provide a framework for technical and non-technical activities to deliver a quality system which meets or exceeds a business's expectations or manage decision-making progression.

Traditionally, the systems-development life cycle consisted of five stages. That has now increased to seven phases. Increasing the number of steps helped systems analysts to define clearer actions to achieve specific goals.

Similar to a project life cycle (PLC), the SDLC uses a systems approach to describe a process. It is often used and followed when there is an IT or IS project under development. The SDLC highlights different stages (phrases or steps) of the development process. The life cycle approach is used so users can see and understand what activities are involved within a given step. It is also used to let them know that at any time, steps can be repeated or a previous step can be reworked when needing to modify or improve the system. The diagram below summaries the phases in system development life cycle.



Source: Innovate architects, 2019

9.3 Data base management

9.3.1 The concept of data base management

A database management system (DBMS) is a software package designed to define, manipulate, retrieve and manage data in a database. A DBMS generally manipulates the data itself, the data format, field names, record structure and file structure. It also defines rules to validate and manipulate this data.

9.3.2 Database Management System (DBMS)

A database management system (DBMS) is a software package designed to define, manipulate, retrieve and manage data in a database. A DBMS generally manipulates the data itself, the data format, field names, record structure and file structure. It also defines rules to validate and manipulate this data.

A DBMS relieves users of framing programs for data maintenance. Fourth-generation query languages, such as SQL, are used along with the DBMS package to interact with a database.
Some other DBMS examples include:

- MySQL
- SQL Server
- Oracle
- dBASE
- FoxPro

A database management system receives instruction from a database administrator (DBA) and accordingly instructs the system to make the necessary changes. These commands can be to load, retrieve or modify existing data from the system.
A DBMS always provides data independence. Any change in storage mechanism and formats are performed without modifying the entire application.

9.3.3 Types of data base organisations

There are four main types of database organization:

- **Relational Database**: Data is organized as logically independent tables. Relationships among tables are shown through shared data. The data in one table may reference similar data in other tables, which maintains the integrity of the links among them. This feature is referred to as referential integrity – an important concept in a relational database system.

Operations such as "select" and "join" can be performed on these tables. This is the most widely used system of database organization.

- **Flat Database**: Data is organized in a single kind of record with a fixed number of fields. This database type encounters more errors due to the repetitive nature of data.
- **Object-Oriented Database:** Data is organized with similarity to object-oriented programming concepts. An object consists of data and methods, while classes group objects having similar data and methods.
- **Hierarchical Database:** Data is organized with hierarchical relationships. It becomes a complex network if the one-to-many relationship is violated.

9.4 Building the system

Building a new information system is one kind of planned organizational change. The introduction of a new information system involves much more than new hardware and software.

9.4.1 Systems Development and Organizational Change

Information technology can promote various degrees of organizational change, ranging from incremental to far-reaching. There are four kinds of structural organizational change that are enabled by information technology. These are;

1. *Automation* - assist employees with performing their tasks more efficiently and effectively.
2. *Rationalization* - a deeper form of organizational change and one that follows quickly from early automation
3. *Business process redesign* - business processes are analysed, simplified, and redesigned
4. *Paradigm shifts* - involves rethinking the nature of the business and the nature of organization. Each carries different risks and rewards.

9.4.2 Business Process Redesign

Business process management provides a variety of tools and methodologies to analyse existing processes, design new processes, and optimize those processes. It has to go through the following steps:

1. *Identify processes for change*: managers need to determine what business processes are the most important and how improving these processes will help business performance.
2. *Analyze existing processes*: existing business processes should be modelled and documented, noting inputs, outputs, resources, and the sequence of activities.
3. *Design the new process*: once the existing process is mapped and measured in terms of time and cost, the process design team will try to improve the process by designing a new one. A

new streamlined “to-be” process will be documented and modelled for comparison with the old process.

4. *Implement the new process*: new information systems or enhancements to existing systems may have to be implemented to support the redesigned process.
5. *Continuous measurement*: once a process have been implemented and optimized, it needs to be continually measured because they may lose their effectiveness if the business experiences other changes or deteriorate over time as employees fall back on old methods.

9.5 Overview of Systems Development

The activities that go into producing an information system solution to an organizational problem or opportunity are called systems development. Systems development is a structured kind of problem solved with distinct activities such as analysis, systems design, programming, testing, conversion, and production and maintenance.

Systems Analysis – the analysis of a problem that a firm tries to solve with an information system. It also includes a feasibility study to determine whether that solution is feasible or achievable, from a financial, technical, and organizational standpoint.

Establishing Information Requirements – it carefully defines the objectives of the new or modified system and develops a detailed description of the functions that the new system must perform.

Systems Design – shows how the system will fulfil this objective. The design of an information system is the overall plan or model for that system.

The Role of End Users – users must have sufficient control over the design process to ensure that the system reflects their business priorities and information needs, not the biases of the technical staff.

9.6 Completing the Systems Development Process

The remaining steps in the systems development process translate the solution specifications established during system analysis and design into a fully operational information system. They are

- *Programming* – system specifications that were prepared during the design stage are translated into software program code.
- *Testing* – conducted thoroughly to ascertain whether the system produces the right results.
- *Conversion* – the process of changing from the old system to the new system.
- *Production and Maintenance* – after the new system is installed and conversion is complete, the system is said to be in production. Changes in hardware, software,

documentation, or procedures to a production system to correct errors, meet new requirements, or improve processing efficiency are termed maintenance.

9.7 Modelling and Designing Systems:

Structured and Object-Oriented Methodologies

There are alternative methodologies for modelling and designing systems. Structured methodologies and object-oriented development are the most prominent.

Structured Methodologies

Structured methodologies have been used to document, analyse, and design information systems since the 1970s. It refers to the fact that the techniques are step by step, with each step building on the previous one. They are top-down, progressing from the highest, most abstract level to the lowest level of detail – from the general to the specific. **Process specifications** describe the transformation occurring within the lowest level of the data flow diagrams. They express logic for each process. **The structure chart** is a top-down chart, showing each level of design, its relationship to other levels, and its place in the overall design structure.

The methodologies may include;

a. Object-Oriented Development: Object-oriented development addresses these issues. It uses the object as the basic unit of systems analysis and design. An object combines data and the specific processes that operate on those data.

b. Computer-Aided Software Engineering: Computer-aided software engineering (CASE) – sometimes called computer-aided systems engineering, provides software tools to automate the methodologies we have just described to reduce the amount of repetitive work the developer needs to do. CASE tools also facilitate the creation of clear documentation and the coordination of team development efforts.

c. Alternative Systems-Building Approaches

i. Traditional Systems Life Cycle

The systems life cycle is the oldest method for building information systems. The life cycle methodology is a phased approach to building a system, dividing systems development into formal stages. The systems life cycle is still used for building large complex systems that require a rigorous and formal requirements analysis, predefined specifications, and tight controls over the system-building process.

ii. Prototyping

Prototyping consists of building an experimental system rapidly and inexpensively for end users to evaluate. The prototype is a working version of an information system or part of the system, but it is meant to be only a preliminary model.

Steps in Prototyping

Step 1: Identify the user's basic requirements.

Step 2: Develop an initial prototype.

Step 3: Use the prototype.

Step 4: Revise and enhance the prototype.

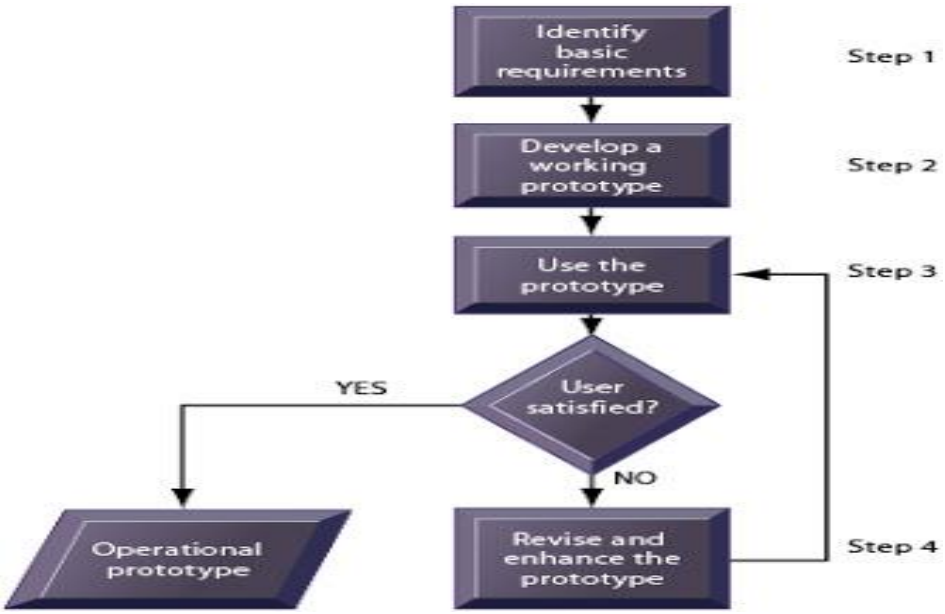


Fig. The Prototyping Process

iii. End-user Development

Some types of information systems can be developed by end users with little or no formal assistance from technical specialists. This phenomenon is called end-user development. A series of software tools categorized as fourth-generation languages makes this possible. Fourth-generation languages are software tools that enable end users to create reports or develop software applications with minimal or no technical assistance. Query languages are software tools that provide immediate online answers to requests for information that are not predefined.

9.8 Application Development for the Digital Firm

In the digital firm environment, organizations need to be able to add, change, and retire their technology capabilities very rapidly to respond to new opportunities. Companies are starting to use shorter, more informal development processes that provide fast solutions.

9.8.1 Rapid Application Development (RAD)

The term **rapid application development (RAD)** is used to describe this process of creating workable systems in a very short period of time. RAD can include the use of visual programming and other tools for building graphical user interfaces, iterative prototyping of key system elements, the automation of program code generation, and close teamwork among end users and information systems specialists. Sometimes a technique called **joint application design (JAD)** is used to accelerate the generation of information requirements and to develop the initial systems design. Properly prepared and facilitated, JAD sessions can significantly speed up the design phase and involve users at an intense level**. Agile development** focuses on rapid delivery of working software by breaking a large project into a series of small subprojects that are completed in short periods of time using iteration and continuous feedback.

9.8.2 Component-based Development and Web Services

To further expedite software creation, groups of objects have been assembled to provide software components for common functions such as a graphical user interface or online ordering capability that can be combined to create large-scale business applications. This approach to software development is called **component-based development**, and it enables to a system to be built by assembling and integrating existing software components**. Web services** can provide significant cost savings in systems building while opening up new opportunities for collaboration with other companies.

9.9 Top 10 considerations when choosing a modern Database Management System (According Tom Eburne, 2014)

When you are confident combining your various data sources and handling all the updates, you may well be looking to source a Database Management and Business Intelligence system. Because selection and implementation of such a system can be a complex process and involve various teams or personnel, we take a look here at the main factors to consider when making your decision, to help you with the whole process.

Ensure that the system has the capacity to grow with your data and your business.

1) Usability

Consider how user-friendly the system will be for all those members of staff required to use it. In some organisations those may include Marketing professionals, the IT department, Database Developers and others. Look at the suitability from everyone's perspective, and consider if you can

set different levels of permission for different teams or personnel. Many systems offer drag-and-drop execution, which makes for an intuitive working methodology. Importantly, however the system works, make sure it is usable for your whole team.

2) Visualisation & Reporting

Review the ease of visually analysing and displaying results for any queries you run on your data, while making selections and deciding segments. Also, check how the software displays campaign results if you feed this information back into the database. You should look for visual displays that will help you show selections and results to colleagues (likely other teams or managers/directors) in a way that they will be able to understand quickly and easily.

3) Security

Security of your data is an essential aspect of any database implementation. Business-sensitive data and any personal information you hold must be stored securely to adhere to regulations and to protect it from loss or theft. It is important to consider both the physical risk to data (e.g. the risk from fire, theft, etc.) and the risks from hacking, or from unintentional corruption of data through human error. Any system you implement must address the issue of keeping your data secure.

4) Functionality

Confirm that the modules available in the data analysis software meet your business requirements. The functionality or modules you should be looking for include:

- Extract and filter data
- Insight and analysis
- Segmentation and modelling
- Automation
- Forecasting strategy
- Results visualisation
- Campaign planning and ROI management.

5) Support and Development

Think about the support service the software company offers for its solution. Is this available during the hours you are likely to need support? Is the support offered by email, phone, other?

Ensure there is a development plan for the selected software so that you can be confident it will grow with emerging technologies. Make sure you will receive upgrades to the most recent version and that you will be supported for as long as you use that software.

6) Integration

Does the system you are considering integrate with your other software systems such as your Email Marketing platform and CRM system? This may be a direct integration to the specific software of there may be an open source code available for integrations.

7) Scalability

Ensure that the system has the capacity to grow with your data and your business. Remember you are likely to be adding to the data all the time, so even though your requirement may not be huge right now, this can grow very quickly if you are gathering and updating your data regularly as planned. Essentially…can it easily manage millions of rows of data?

8) Cost and Suitability

Whilst cost is obviously a factor in any business expenditure, it is wise to ensure that – as far as possible – your decision is based on the software being fit for purpose. It could be a costly mistake to take on a system that you then invest time in building, only to find – too late – that it is not advanced enough for your needs. Equally there is no need to opt for the most expensive software available, if you are unlikely to need much of the functionality it offers.

9) Hosting

Where is your system going to be located (physically)? Will you take the system in-house or engage the services of a company to host the data and the software system for you. This could have implications for support, cost (including any additional hardware you would require), security, and possibly speed.

10) Updates

The two most important factors regarding updates to the database are frequency and automation. Do you need data to be live and constantly in sync with your other systems, or would daily or even weekly updates to the database be sufficient? Consider that in order to automate the update process, you will typically need a consistent data source, i.e. the field types, and the files supplied each time must be the same. You should consider how often source data is likely to change, if you are ever going to import additional data and if so how your chosen software will deal with this.

9.10 Summary

Building a new information system is one kind of planned organizational change. The introduction of a new information system involves much more than new hardware and software. Information technology can promote various degrees of organizational change, ranging from incremental to far-reaching. The core activities in systems development are systems analysis, systems designs, programming, testing, conversion, production, and maintenance. The two principal methodologies for modelling and designing information systems are structured methodologies and object-oriented

development. The oldest method for building systems is the systems life cycle, which requires that information systems be developed in formal stages. The stages must proceed sequentially and have defined outputs; each requires formal approval before the next stage can commence. Companies are turning to rapid application design, joint application design (JAD), agile development, and reusable software components to accelerate the systems development process. Component-based development expedites application development by grouping objects into suites of software components that can be combined to create large-scale business applications. Web services provide a common set of standards that enable organizations to link their systems regardless of their technology platform through standard plug- and –play architecture.

9.11 Revision Questions

1. Describe the Data Base Management System with relevant examples.
2. Explain the ten factors to consider when choosing the information system for the organisation.
3. Explain the methodologies in system development.
4. With examples, discuss the phases in system development.

REFERENCES/FURTHER READINGS

Agbasi K.C. (1993): Computer Appreciation; An Individual Computer to Systems, ACENA Publishers, Enugu.

Nwafor C.E. (2005): Computer and Internet Literacy, Joans Publishers, Enugu.

Nwafor C.E. (2006): Computer and Information Technology Literacy, Dynamic Informer.

Christensen, Clayton M. (1997). *The Innovator's Dilema*. New York, New York: Harper Business. p. 19. ISBN 0-06-662069-4.

Chandler, Doug (September 26, 1988). "Startup Ships 2.5-Inch Hard Disk Aimed for Portables, Laptops". *PC Week*: 6.

Davis, G.B., & Olson, M. H. (1985). *Management information systems: Conceptual foundations, structure, and development.* New York: McGraw-Hill.

Imboden, N. (1980). *Managing information for rural development projects.* Paris: Organization for Economic Co-operation and Development.

Inyiama H.C. (2000): *Understanding Computers; The Dynamic Informer*, 15A Bank Avenue, Aguowa, Trans-Ekulu, Enugu, Nigeria.

Inyiama H.C. (2000): *Computer Applications and Information Technology*, Dynamic Informer, Enugu.

Kotler, Philip; Keller, Kevin Lane (2006). *Marketing Management* (12 ed.). Pearson Education.

Keen, P. G. W., & Morton, M. S. S. (1978). *Decision support systems.* Reading, MA: Addison-Wesley.

Lee, Allen S. (2001). "Editor's Comments". *MIS Quarterly* **25** (1): iii-vii.

Livinus C. N.(2003): *Internet Literacy;* Horizon Publications, Obiagu Road, Ogui New layout Enugu, Nigeria.

Lucas, H. C., Jr. (1990). *Information systems concepts for management.* New York: McGraw-Hill.

Martin, J. (1990). *Telecommunications and the computer* (3rd ed.). Englewood Cliffs, NJ: Prentice-Hall.

Mason, R. D., & Swanson, B. E. (1981). *Measurements for management decision.* Reading, MA: Addison-Wesley.

Mbam B.C.E. (2002): *Information Technology and Management Information System*; Our Saviour Press Ltd, Enugu, Nigeria.