DEPARTMENT OF EDUCATION

GRADE 12

INFORMATION COMMUNICATION TECHNOLOGY

MODULE 1 – INFORMATION AND COMMUNICATION SYSTEMS

FODE DISTANCE LEARNING

PUBLISHED BY FLEXIBLE OPEN AND DISTANCE EDUCATION
FOR THE DEPARTMENT OF EDUCATION
PAPUA NEW GUINEA

Writers and Editors

Mary Ruanne Junsay

Writer

Dr. Janet S. Marcelo

Cleofe Dagale

Diana Akis

Judy Mirou

Martha Pitpit

Editors

GRADE 12

INFORMATION COMMUNICATION TECHNOLOGY

UNIT MODULE 1

INFORMATION AND COMMUNICATION SYSTEMS

TOPIC 1: INFORMATION SYSTEM

TOPIC 2: NETWORKING SYSTEMS

TOPIC 3: NETWORK BASICS

TOPIC 4: NETWORK SOFTWARE

Acknowledgements

We acknowledge the contribution of all Secondary and Upper Primary teachers who in one way or another helped to develop this Course.

Our profound gratitude goes to the former Principal of FODE, Mr. Demas Tongogo for leading FODE team towards this great achievement. Special thanks are given to the staff of the Information Communication Technology Department-FODE who played an active role in coordinating writing workshops, outsourcing of lesson writing and editing processes involving selected teachers in NCD.

We also acknowledge the professional guidance and services provided through-out the processes of writing by the members of:

Information Communication Technology Subject Review Committee-FODE
Academic Advisory Committee-FODE
Information Communication Technology Department- CDAD

.
This book was developed with the invaluable support and co-funding of the GO-PNG and World Bank.

DIANA TEIT AKIS
Principal-FODE

Published in 2017

ISBN: 978-9980-89-686-5
National Library Services of Papua New Guinea

Compiled and finalised by: Information Communication Technology Department-FODE

Printed by the Flexible, Open and Distance Education

CONTENTS

12.1.4 : NETWORK SOFTWARE

SECRETARY'S MESSAGE

Achieving a better future by individual students, their families, communities or the nation as a whole, depends on the curriculum and the way it is delivered.

This course is part and parcel of the new reformed curriculum – the Outcome Base Education (OBE). Its learning outcomes are student centred and written in terms that allow them to be demonstrated, assessed and measured.

It maintains the rationale, goals, aims and principles of the National OBE Curriculum and identifies the knowledge, skills, attitudes and values that students should achieve.

This is a provision of Flexible, Open and Distance Education as an alternative pathway of formal education.

The Course promotes Papua New Guinea values and beliefs which are found in our constitution, Government policies and reports. It is developed in line with the National Education Plan (2005 – 2014) and addresses an increase in the number of school leavers which has been coupled with a limited access to secondary and higher educational institutions.

Flexible, Open and Distance Education is guided by the Department of Education's Mission which is fivefold;

- to facilitate and promote integral development of every individual
- to develop and encourage an education system which satisfies the requirements of Papua New Guinea and its people
- to establish, preserve, and improve standards of education throughout Papua New Guinea
- to make the benefits of such education available as widely as possible to all of the people
- to make education accessible to the physically, mentally and socially handicapped as well as to those who are educationally disadvantaged

The College is enhanced to provide alternative and comparable path ways for students and adults to complete their education, through one system, many path ways and same learning outcomes.

It is our vision that Papua New Guineans harness all appropriate and affordable technologies to pursue this program.

I commend all those teachers, curriculum writers and instructional designers, who have contributed so much in developing this course.

UKE KOMBRA, PhD
Secretary for Education

UNIT 1: INFORMATION AND COMMUNICATION SYSTEMS

INTRODUCTION

The field of study called information systems encompasses a variety of topics including systems analysis and design, computer networking, information security, database management and decision support systems.

Information management deals with the practical and theoretical problems of collecting and analysing information in a business function area including business productivity tools, applications programming and implementation, electronic commerce, digital media production, data mining, and decision support. Communications and networking deals with the telecommunication technologies. Information systems (IS) bridges business and computer science using the theoretical foundations of information and computation to study various business models and related algorithmic processes within a computer science discipline. Computer information system(s) (CIS) is a field studying computers and algorithmic processes, including their principles, software and hardware designs, applications, and impact on society, whereas Information System emphasises functionality over design.

Take note that activities are found at the end of every module lesson and summative exercises after every topic. All answers to activities are found after the summative exercises.

The following icons are used in this module:

 Student Aims

 Student Activity

 Time Frame

 Note

 Practical Student Activity

 Answers to Learning Activities

Objectives or aims

On successful completion of this module, students will be able to:

- analyse and describe an information system in terms of the information processes and equipment required
- describe the effects of information systems on the individual, society and the environment
- describe and set up a simple local area network (LAN)

- describe communications hardware, software and methods of connection
- describe suitable data protection and security procedures for a network.

Time Frame

This unit should be completed within 10 weeks.

If you set an average of 3 hours per day, you should be able to complete the unit comfortably by the end of the assigned week.

Try to do all the learning activities and compare your answers with the ones provided at the end of the unit. If you do not get a particular exercise right in the first attempt, you should not get discouraged but instead, go back and attempt it again. If you still do not get it right after several attempts then you should seek help from your friend or even your tutor. Do not pass any question without solving it first.

12.1.1 Information System

12.1.1.1 Information System

Many organisations work with large amounts of data. This situation calls for a need for a system of doing things. A system is often referred to as a set of connected things that form a whole or work together. It is an organised scheme or method. In this context, an information system is necessary for an organised way of working with large amounts of data. Data are basic values or facts and are organised in a database. Many people think of data as synonymous with information; however, information actually consists of data that has been organised to help answer questions and to solve problems. The distinction of data and information has been thoroughly discussed in Grade 9 Design and Technology-Computing Topic 3.

An Information System (IS) is defined as the software that helps organise and analyse data. So, the purpose of an information system is to turn raw data into useful information that can be used for decision making in an organisation.

Moreover, an information system is a system composed of people and computers that processes or interprets information. The term is also sometimes used in more restricted senses to refer to only the software used to run a computerised database or to refer to only a computer system. In a broad scope, the term Information Systems is a scientific field of study that addresses the range of strategic, managerial, and operational activities involved in the gathering, processing, storing, distributing, and use of information and its associated technologies in society and organisations. It is also used to describe an organisational function that applies IS knowledge in industry, government agencies, and not-for-profit organisations. Further, it often refers to the interaction between algorithmic processes and technology. This interaction can occur within or across organisational boundaries. An information system then is the technology an organisation uses and also the way in which the organisations interact with the technology and the way in which the technology works with the organisation's business processes. Information systems are distinct from Information Technology (IT) in that an information system has an information technology component that interacts with the processes' components. In a broad sense, the term is used to refer not only to the information and communication technology (ICT) that an organisation uses, but also to the way in which people interact with this technology in support of business processes.

Looking at it, an Information System makes it possible to answer questions and solve problems relevant to the mission of an organisation. IS is any specific information system which aims to support operations, management and decision making.

To elaborate more, there is a clear distinction between information systems, computer systems, and business processes. Information systems typically include an ICT component but are not purely concerned with ICT, focusing instead on the end use of information technology. Information systems are also different from business processes. Information systems help to control the performance of business processes.

An information system is a work system whose activities are devoted to processing (capturing, transmitting, storing, retrieving, manipulating and displaying) information. This makes IS useful in large data organisation for a distinctive purpose in decision making. The information systems field includes the people in organisations who design and build information systems, the people who use those systems, and the people responsible for managing those systems. The demand for traditional IT staff such as programmers, business analysts, systems analysts, and designer is significant. Many well-paid jobs exist in areas of Information technology.

Further, research in Information System which is divided into two scientific models including behavioural science develops and verifies theories that explain or predict human or organisational behaviour and design science extends the boundaries of human and organisational capabilities by creating new and innovative artifacts.

Clearly, information system is now an indispensable tool in today's modern world of task completion and decision making.

While information systems may differ in how they are used within an organisation, they typically contain the following components:

1. **Hardware**
   The term hardware refers to machinery. This category includes the computer itself, which is often referred to as the central processing unit (CPU), and all of its support equipment. Among the support equipment are input and output devices, storage devices and communications devices. Computer-based information systems use computer hardware, such as processors, monitors, keyboard, and printers.

2. **Software**
   The term software refers to computer programs and the manuals (if any) that support them. Computer programs are machine-readable instructions that direct the circuitry within the hardware parts of the system to function in ways that produce useful information from data. Programs are generally stored on some input / output medium, often a disk or tape. These are the programs used to organise, process and analyse data.

3. **Databases**
   Information systems work with data organised into tables and files. Data are facts that are used by programs to produce useful information. Like programs, data are generally stored in machine-readable form on disk or tape until the computer needs them.

4. **Network**
   Different elements need to be connected to each other, especially if many different people in an organisation use the same information system.

5. **Procedures**
   Procedures are the policies that govern the operation of a computer system. "Procedures are to people what software is to hardware" is a common analogy that is

used to illustrate the role of procedures in a system. These describe how specific data are processed and analysed in order to get the answers for which the information system is designed.

6. **People**
Every system needs people if it is to be useful. Often the most over-looked element of the system is the people, probably the component that most influence the success or failure of information systems.

The first four components are part of the general Information Technology (IT) of an organisation. The procedures are very specific to the information needed to answer a specific question.

Student Activity 12.1.1.1

Answer the following.

1. Write down three (3) definitions of an Information System.

a. _____
_____
_____
_____
_____

b. _____
_____
_____
_____
_____

c. _____
_____
_____
_____
_____

2. Give two (2) importance of an Information System.

a. _____

_____

_____

_____

_____

b. _____

_____

_____

_____

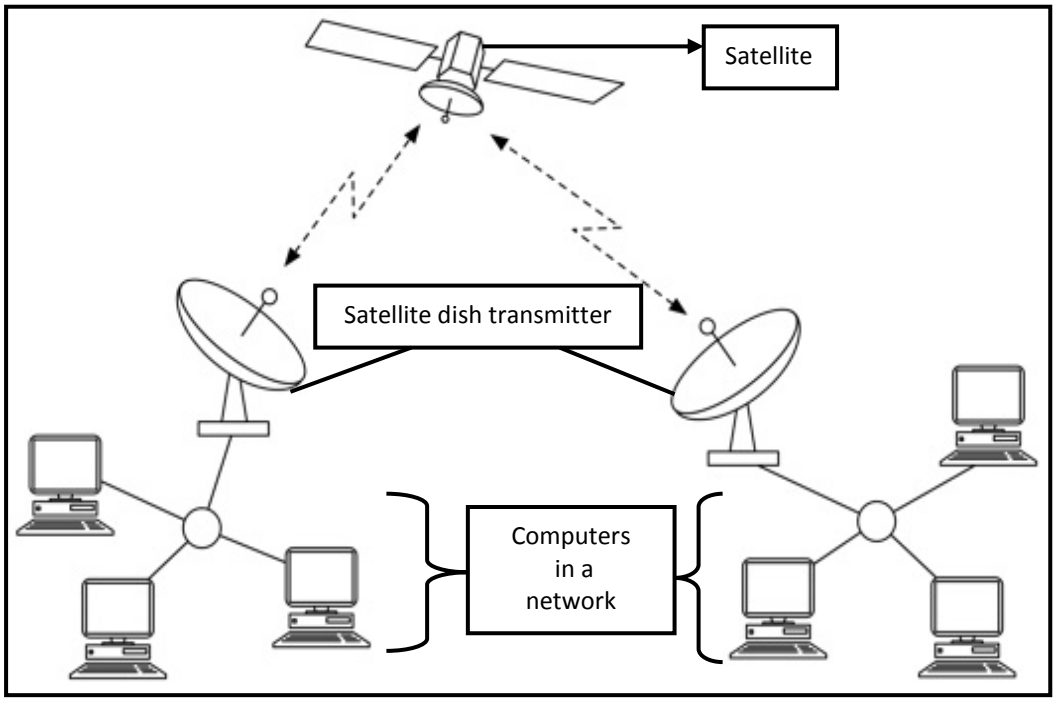
_____

_____

12.1.1.2 The Role of a Network in an Information System

Management of Information and communication are two of the most important things for the success of every organisation. Even though today nearly every organisation uses a substantial number of computers and communication tools (telephones, fax, and personal handheld devices), they are often still isolated. The needed sharing of relevant information for effective communication is not achieved by the people in the organisation in this isolation.

To overcome this obstacle for an effective usage of information technology, computer networks are necessary. 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. Since a network is described as two or more computers, or other electronic devices which are connected together, it then allows the exchange of data. For example, a network allows computers to share files, users to message each other, a whole room of computers to share a single printer and others. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.



A representation of a Network connection.

They are a new kind of organisation of computer systems produced for the need to merge computers and communications. At the same time they are the means to unite the two areas of computers and communication. The unnecessary distinction between tools to process and store information and tools to collect and transport information can disappear. Computer networks can manage to put down the barriers between information held on several (not only computer) systems. Only with the help of computer networks can a borderless communication and information environment be built.

In addition, computer networks allow the user to access remote programs and remote databases either of the same organisation or from other enterprises or public sources.

Computer networks provide communication possibilities faster than other facilities. Because of these optimal information and communication possibilities, computer networks may increase the organisational learning rate, which many authors declare as the only fundamental advantage in competition.

Besides this major reason why any organisation should not fail to have a computer network, there are other organisational reasons as well:

a. cost reduction by sharing hard- and software resources

b. high reliability by having multiple sources of supply

c. cost reduction by downsizing to microcomputer-based networks instead of using mainframes

d. greater flexibility because of possibility to connect devices

In brief therefore, using a computer connected to a network allows us to:

- Easily share files and data
- Share resources such as printers and Internet connections
- Communicate with other network users (e-mail, instant messaging, video-conferencing, etc.)
- Store data centrally (using a file server) for ease of access and back-up
- Keep all of our settings centrally so we can use any workstation

In particular, if we use a computer connected to the Internet, we can:

- Make use of on-line services such as shopping (e-commerce) or banking
- Gain access to a huge range of information for research
- Access different forms of entertainment (games, video, etc.)
- Join on-line communities (e.g. MySpace, Facebook, etc.)

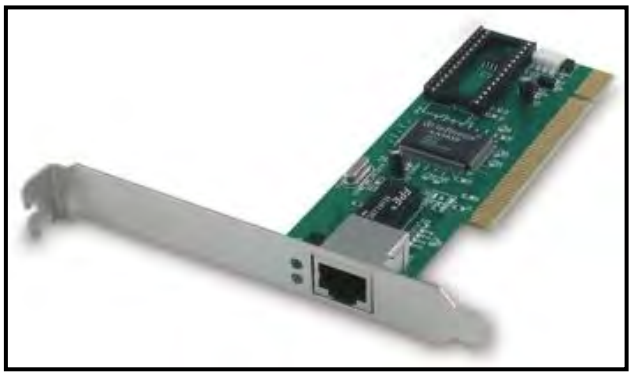
Because of the importance of this technology, decisions about purchase, structure, and operation of computer networks cannot be left to the technical staff. Effective management requires the top management people as well to understanding the technology of computer networks.

A network functions with both the hardware and software parts. The hardware is presented below while the software (network operating software or NOS) will be discussed as we move along in our topic module discussions.

Let us now study the hardware part of how a network functions.

1. **Network Interface Card (NIC)**

Any computer that is to be connected to a network needs to have a network interface card (NIC). The common names of NIC would be Local Area Network Card or Network Card. Most modern computers have these devices built into the motherboard, but in some computers you have to add an extra expansion card (small circuit board)



Network interface card

Remember that some computers, such as laptops, have two NICs; one for wired connections, and the other for wireless connections (which uses radio signals instead of wires)

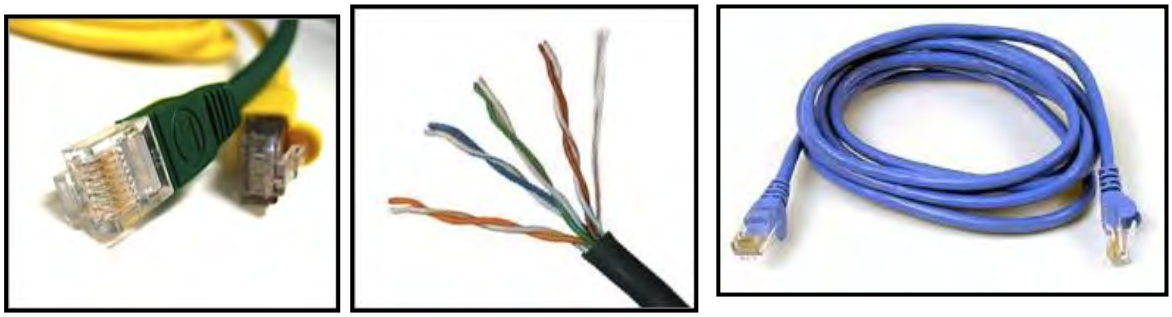
Laptop wireless card

Wireless network card

Take note that in a laptop; the wireless radio antenna is usually built in to the side of the screen. Hence, there is no need to have a long piece of plastic sticking out the side of the computer.

2. **Network Cable**

Cables are needed to connect the different devices to set up a network. Cables are still used in most networks, rather than using only wireless, because they can carry more data per second, and are more secure (less open to hacking).

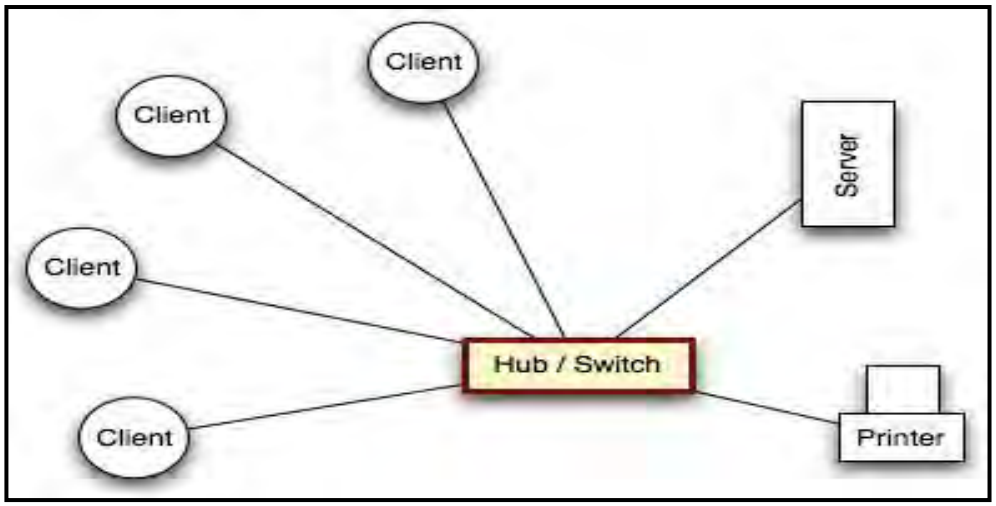


Network Cables

The most common type of network cable in use today, looks like the one shown above, with plastic plugs on the ends that snap into sockets on the network devices. Inside the cable are several copper wires (some used for sending data in one direction, and some for the other direction). A detailed discussion of cable wires will be discussed on Topic 12.1.2.5.

3. **Hub**

A hub is a device that connects a number of computers together to make a LAN. The typical use of a hub is at the center of a common network.



A representation on how a hub connects computers to make a local area

A hub is a 'dumb' device: if it receives a message, it sends it to every computer on the network. This means that hub-based networks are not very secure - everyone can listen in to communications.

A hub

Hubs are pretty much obsolete now that you cannot buy them anymore. It has been out dated by cheap switches.

4. **Switch**

A switch, like a hub, is a device that connects a number of computers together to make a LAN. The typical use of a switch is at the center of a common network or as part of a hybrid network where the switch has cables plugged into it from each computer.

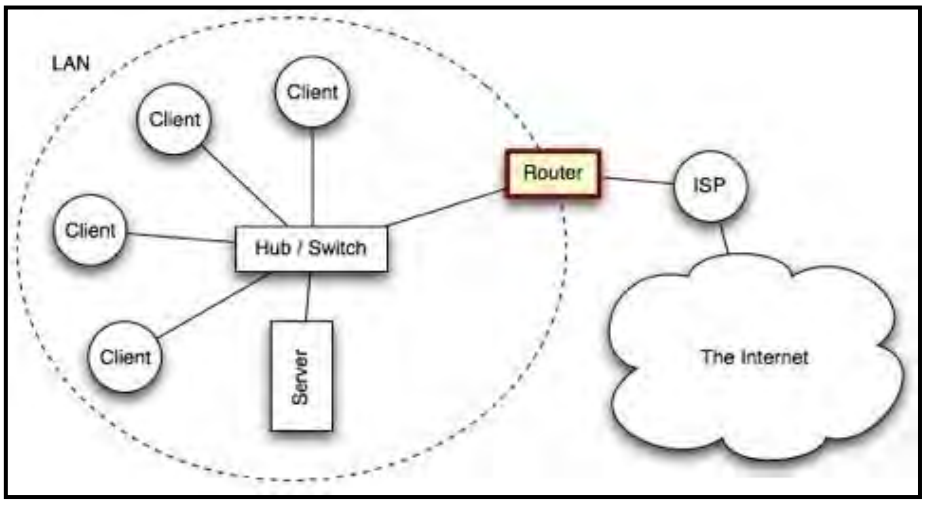
A switch is a more 'intelligent' device than a hub: if it receives a message, it checks who it is addressed to, and only sends it to that specific computer. Because of this, networks that use switches are more secure than those that use hubs, but a little more expensive.

A switch

5. **Router**

A router is a network device that connects together two or more networks. A common use of a router is to join a home or business network (LAN) to the Internet (WAN).

The router will normally have the Internet cable plugged into it, as well as a cable, or cables to computers on the LAN.



A representation on how a router connects two or more networks

Alternatively, the LAN connection might be wireless (Wi-Fi), making the device a wireless router. A wireless router is actually a router and wireless switch combined.

Routers are the devices that join together the various different networks that together make up the Internet.

These routers are much more complex than the one you might have in your home.

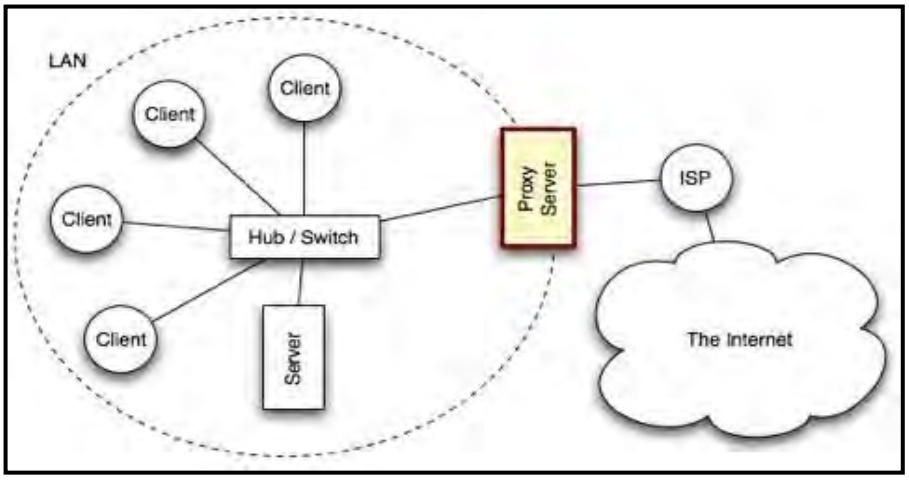
Sample routers

6. **Proxy Server**

A proxy server is a computer setup to share a resource, usually an Internet connection.

Other computers can request a web page via the proxy server. The proxy server will then get the page using its Internet connection, and pass it back to the computer who requested for it.

Proxy servers are often since additional software can be easily installed on the computer such as anti-virus, web filtering and others. It should be seen that proxy servers and routers serve at different protocol levels. Proxy servers basically deal with data content while Router deals with TCIP data packets routing them to their respective IP addresses. **Transmission Control Protocol/Internet Protocol** (**TCP/IP**) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

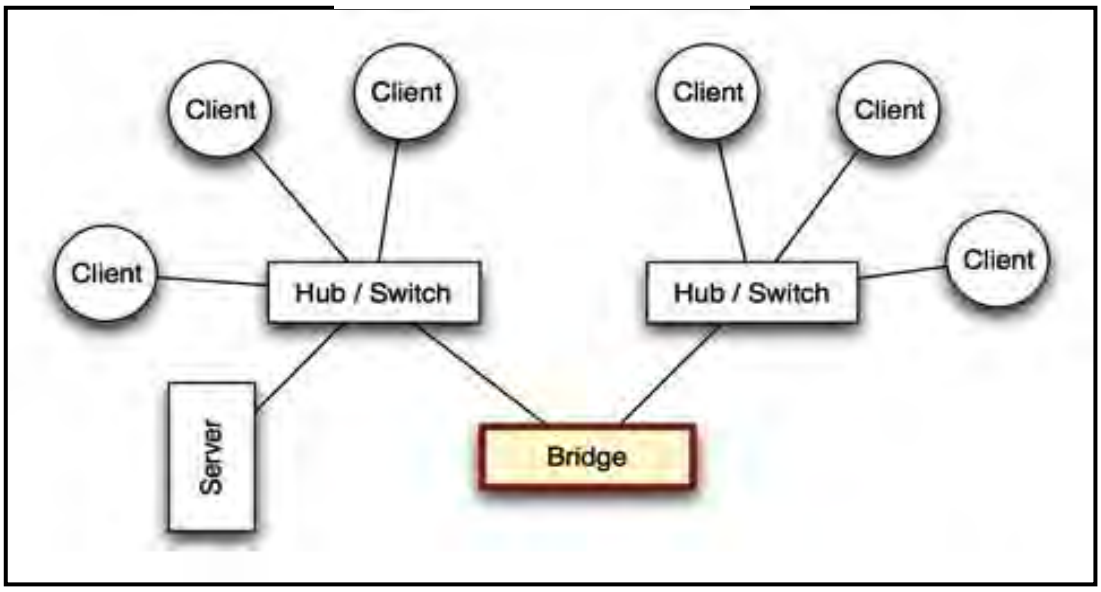


A representation of how proxy server works

7. **Bridge**

A bridge is a network device that typically links two different parts of a LAN, whereas a router is usually used to link a LAN to a WAN (such as the Internet), a bridge links independent parts of a LAN so that they act as a single LAN.

A bridge

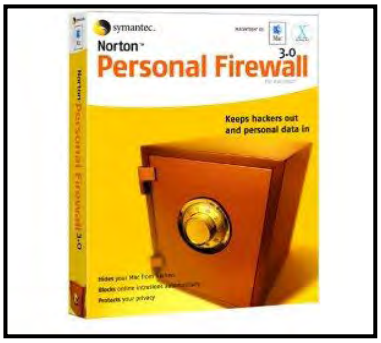


A representation on how a bridge links two different parts of a local area network

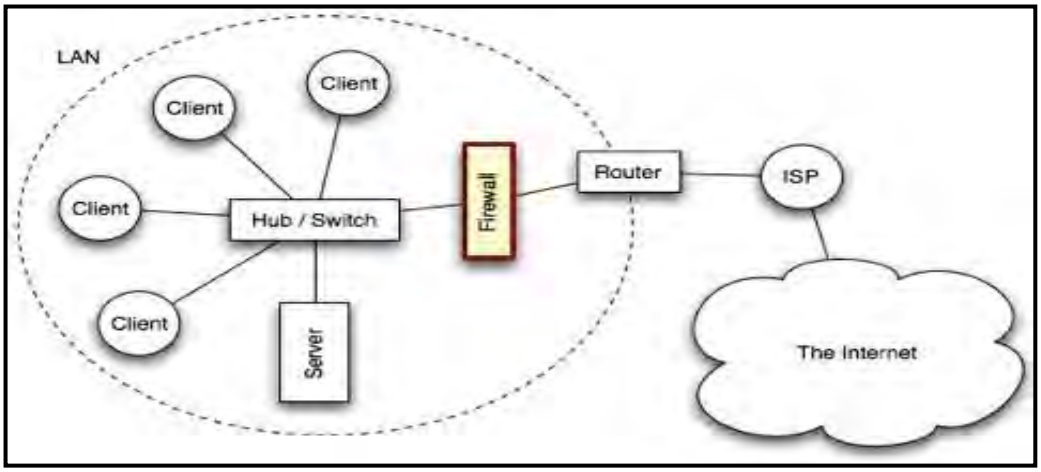
8. **Firewall**

A firewall is a device, or a piece of software that is placed between a computer and the rest of the network. To protect your whole LAN from hackers out on the Internet, one can place a firewall between the LAN and the Internet connection.

Firewall as a Hardware

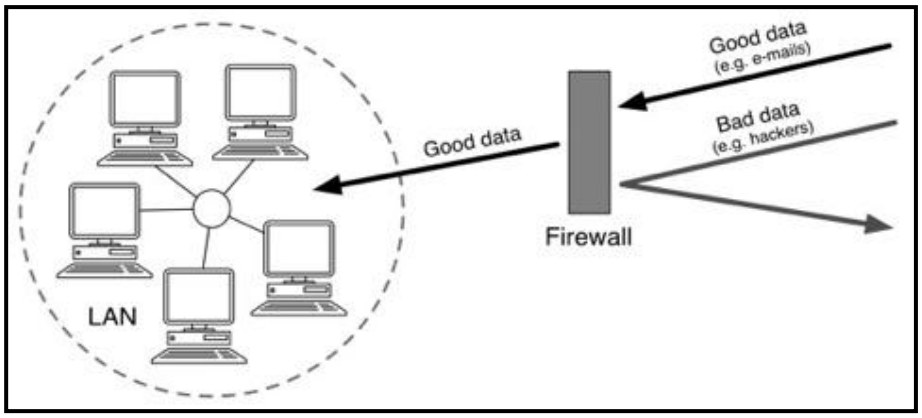


Firewall as a Software



A representation on how firewall is placed between a computer and the network

A firewall blocks unauthorised connections being made to your computer or LAN. Normal data is allowed through the firewall (e.g. e-mails or web pages) but all other data is blocked.



A representation on how a firewall blocks unauthorised connections

In addition to physical devices, firewalls can also be software. In fact most computer operating systems have a software firewall built in (e.g. Windows, Linux and Mac OS)

9. **Modem (Mo**dulate **Dem**odulate**)**

Before the days of broadband Internet connections, most computers connected to the Internet via telephone lines or dial-up connections.

The problem with using telephone lines is, they are designed to carry voices, which are analogue signals. They are not designed for digital data.

An illustration of analogue signal used by telephones

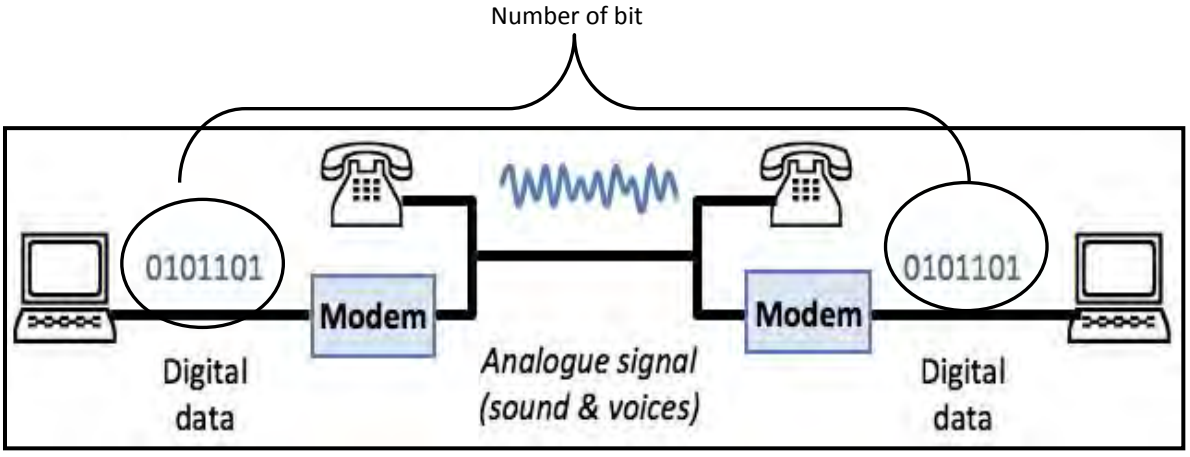
The solution was to use a special device to join the digital computer to the analogue telephone line. This device is known as a modem.

A modem contains a Digital to Analog Converter (DAC) and an Analog to Digital Converter (ADC.) The DAC in the modem is required so that the digital computer can send data down the analogue telephone line where it converts digital data into noises which is exactly what the telephone line is designed to carry.

The ADC in the modem is required so that the analogue signals (noises) that arrive via the telephone line can be converted back into digital data.

The reason telephone lines were used is that almost all buildings in the world are joined to each other via the telephone system. Using the telephone system for connecting computers meant that people did not have to install new wires to their houses and offices just for computer use.

In the last few years however, this is exactly what people did. Special cables have been installed just for Internet access. These special cables are designed to carry digital data, so no modem is required. The word modem is an abbreviation of **MO**dulator **DEM**odulator. A modulator acts as a DAC, and a demodulator acts as an ADC.



A representation on how a modem is used

Therefore, a modem is required because computers are digital devices and the telephone system is analogue. The modem converts from digital to analogue and from analogue to digital.

Network connections between computers are typically created using cables (wires). However, connections can be created using radio signals (wireless or Wi-Fi), telephone lines (and modems) or even, for very long distances, via satellite links. Two very common types of networks include are the Local Area Network (LAN) and the Wide Area Network (WAN). These will be further discussed in the coming topics.

Student Activity 12.1.1.2

Answer the following.

1. Describe a network.

_____

_____

_____

_____

2. How does a network help in an efficient Information System (IS)?

_____

_____

_____

_____

_____

_____

_____

3. List down at least three (3) importance of a network in an information system.

a. _____

_____

b. _____

_____

c. _____

_____

12.1.1.3 Characteristics of Information Systems

The use of information systems to facilitate works is crucial to improve productivity. People have to access, manage, input, and manipulate data in a system to track and handle all daily routines like inventory, cash flow, invoicing, sales, and many more. Thus, IT division in an organisation has an important role and responsibility to create reliable and powerful applications to enable other divisions to run the system very well. Here are the main characteristics of a good information system:

1. **Accessible**
   Accessibility is the main requirement of information system because all authorised users have to access the system first to do their works. The system must be designed accessibly so the employees can do the jobs through desktop/gadget, software, and internet network easily.

2. **Accurate**
   An information system must be accurate in calculating and showing the information because an organisation may even make a loss if there is any inaccurate data or calculation. Wrong data or information in an information system will impact the result and even become worse because managers surely tend to make wrong decision.

3. **Simple**
   The use of an information system is intended to simplify day to day routines. Thus, it must be designed and created simply to allow all authorised users to access the system and to manipulate data easily as they may not be able to do their tasks if they use a complex system.

4. **Flexible**
   It is essential to have a flexible information system that can be used by all divisions in a company to see valuable and important information. For example, people in the production division need to see outgoing products in sales database so they can keep producing on time and estimate the amount of the products to be produced.

5. **Secure**
   Only authorised users are able to input and manipulate data so there must be username and password required for them to access the information. Information system that has good security will keep all data including customers' data, cash flow, and others.

Lastly, apart from creating good information systems based on some characteristics above, IT specialists are also highly responsible for monitoring how the clients use the systems. The following are some questions that need to be answered by a good information system:

a. Does it work very well?

b. Can all users access the system?

c. Is it able to be accessed 24/7?

It is a must for IT specialists to monitor because it must work very well to allow certain employees to access the application anytime and anywhere virtually. Thus, IT division that creates good applications and keeps monitoring the system's performance will be able to lead an organisation to success.

A good MIS provides information that is relevant and accurate for its purpose, provides information that is sufficiently complete and reliable to instil confidence in the user, communicates the information to the right user in time for its purpose and targets its detail appropriately for the use to which it may be put, communicates the information to the user in such a way that it is understandable.

Student Activity 12.1.1.3

What makes a good information system? Describe in your own words.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

12.1.1.4 Types and Purposes of Information System

Information systems are used to collect data and process it according to the needs of the organisation. For example, businesses operate more efficiently by using varied information systems to interact with customers and partners, curtail costs and generate revenues.

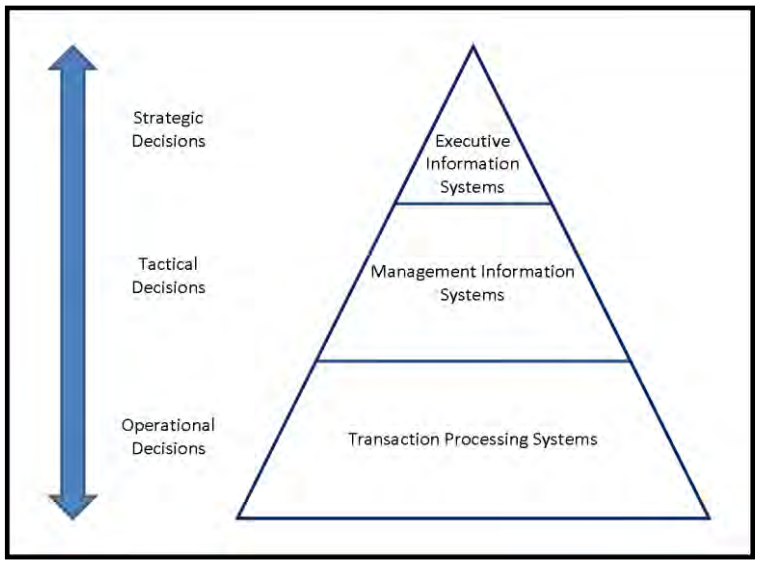
As discussed earlier, an information system is a collection of hardware, software, data, network, people and procedures that are designed to generate information that supports the day-to-day, short-range, and long-range activities of users in an organisation.

The different types of information system that can be found are identified through a process of classification. Classification is simply a method by which things can be categorised or classified together so that they can be treated as if they were a single unit.

The classification of information systems into different types is a useful technique for designing systems and discussing their application. It is not however, a fixed definition governed by some natural law. A 'type' or category of information system is simply a concept, an abstraction, which has been created as a way to simplify a complex problem through identifying areas of commonality between different things. One of the oldest and most widely used systems for classifying information systems is known as the pyramid model. This is further described below.

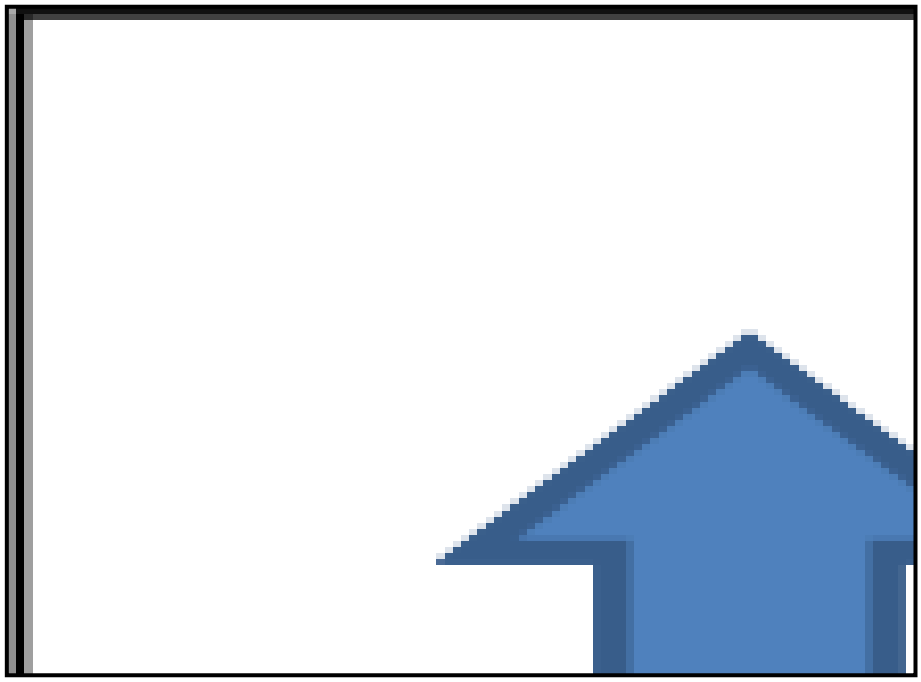
Most attempts to classify Information systems into different types rely on the way in which task and responsibilities are divided within an organisation. As most organisations are hierarchical, the way in which the different classes of information systems are categorised tends to follow the hierarchy. This is often described as "the pyramid model" because the way in which the systems are arranged mirrors the nature of the tasks found at different levels in an organisation.

For example, this is a three level pyramid model based on the type of decisions taken at different levels in the organisation.

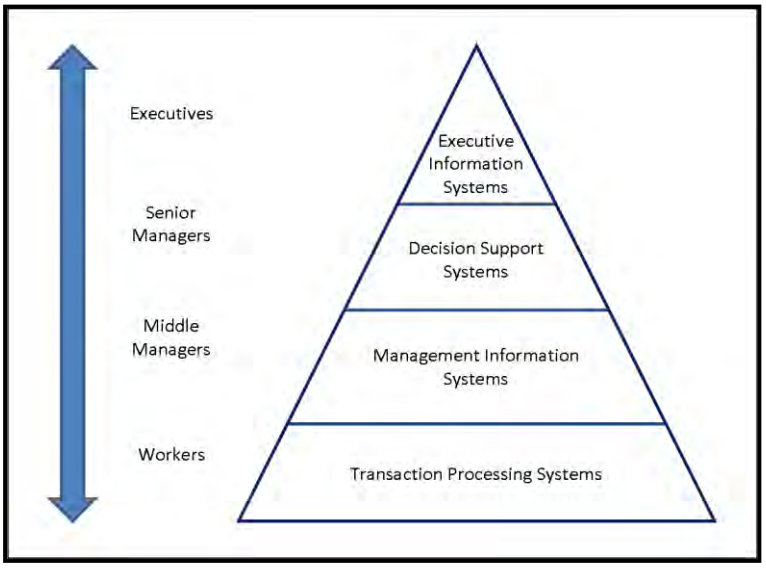


Three level pyramid model based on the type of decisions taken at different levels in an organisation

Similarly, by changing our criteria to the different types of date / information / knowledge that are processed at different levels in an organisation, we can create a five level model.



Five level pyramid model based on the processing requirement of different levels in an organisation



Four level pyramid model based on the different levels of hierarchy in an organisation

While there are several different versions of the pyramid model, the most common is probably a four level model based on the people who use the systems. Basing the classification on the people who use the information system means that many of the other characteristics such as the nature of the task and informational requirements are taken into account more or less automatically.

Using the four level pyramid models above, we can now compare how the information systems in our model differ from each other.

1. **Transaction Processing Systems (TPS)**

Transaction Processing System is operational-level systems at the bottom of the pyramid. They are usually operated directly by shop floor workers or front line staff, which provide the key data required to support the management of operations. This data is usually obtained through the automated or semi-automated tracking of low-level activities and basic transactions.

Functions of a Transaction Processing Systems (TPS)

TPS are ultimately little more than simple data processing systems.

Functions of a TPS in terms of data processing requirements		
Inputs	Processing	Outputs
Transactions Events	Validation Sorting Listing Merging Updating Calculation	Lists Detail reports Action reports Summary reports

Some examples of Transaction Processing Systems (TPS) are:

- Payroll systems
- Order processing systems
- Reservation systems
- Stock control systems
- Systems for payments and funds transfers

Below are the roles of Transaction Processing Systems (TPS)

- Produce information for other systems
- Cross boundaries (internal and external)
- Used by operational personnel + supervisory levels
- Efficiency oriented

2. **Management Information Systems (MIS)**

For historical reasons, many of the different types of Information Systems found in commercial organisations are referred to as "Management Information Systems". However, within our pyramid model, Management Information Systems are management-level systems that are used by middle managers to help ensure the smooth running of an organisation in the short to medium term. The highly

structured information provided by these systems allows managers to evaluate an organisation's performance by comparing current with previous outputs.

Functions of Management Information Systems (MIS)
MIS are built on the data provided by the TPS

Functions of a MIS in terms of data processing requirements		
Inputs	Processing	Outputs
Internal Transactions Internal Files Structured data	Sorting Merging Summarising	Summary reports Action reports Detailed reports

Some examples of Management Information Systems (MIS) are:

- Sales management systems
- Inventory control systems
- Budgeting systems
- Management Reporting Systems (MRS)
- Personnel (HRM) systems

Below are the roles of Management Information Systems (MIS)

- Based on internal information flows
- Support relatively structured decisions
- Inflexible and have little analytical capacity
- Used by lower and middle managerial levels
- Deals with the past and present rather than the future
- Efficiency oriented

3. **Decision Support Systems (DSS)**
A Decision Support System can be seen as knowledge based system, used by senior managers, which facilitates the creation of knowledge and allow its integration into the organisation. These systems are often used to analyse existing structured information and allow managers to project the potential effects of their decisions into the future. Such systems are usually interactive and are used to solve ill structured problems. They offer access to databases, analytical tools, allow "what if" simulations, and may support the exchange of information within the organisation.

Functions of Decision Support Systems (DSS)
DSS manipulate and build upon the information from a MIS and/or TPS to generate insights and new information.

Functions of a DSS in terms of data processing requirements		
Inputs	Processing	Outputs
Internal Transactions Internal Files External Information	Modeling Simulation Analysis Summarising	Summary reports Forecasts Graphs / Plots

Some examples of Decision Support Systems (DSS) are:

- Group Decision Support Systems (GDSS)
- Computer Supported Co-operative work (CSCW)
- Logistics systems
- Financial Planning systems
- Spreadsheet Models

Below are the roles of Decision Support Systems (DSS)

- Support ill- structured or semi-structured decisions
- Have analytical and/or modeling capacity
- Used by more senior managerial levels
- Are concerned with predicting the future
- Are effectiveness oriented

4. **Executive Information Systems (EIS)**
Executive Information Systems are strategic-level information systems that are found at the top of the Pyramid. They help executives and senior managers analyse the environment in which the organisation operates, to identify long-term trends, and to plan appropriate courses of action. The information in such systems is often weakly structured and comes from both internal and external sources. Executive Information System are designed to be operated directly by executives without the need for intermediaries and easily tailored to the preferences of the individual using them.

Functions of Executive Information Systems (EIS)
EIS organises and presents data and information from both external data sources and internal MIS or TPS in order to support and extend the inherent capabilities of senior executives.

Functions of a EIS in terms of data processing requirements		
Inputs	Processing	Outputs
External Data Internal Files Pre-defined models	Summarising Simulation "Drilling Down"	Summary reports Forecasts Graphs / Plots

Some examples of Executive Information Systems (EIS)
Executive Information Systems tend to be highly individualised and are often custom made for a particular client group; however, a number of off-the-shelf EIS packages do exist and many enterprise level systems offer a customisable EIS module.

Below are the roles of Executive Information Systems (EIS)

- Are concerned with ease of use
- Are concerned with predicting the future
- Are effectiveness oriented
- Are highly flexible
- Support unstructured decisions
- Use internal and external data sources
- Used only at the most senior management levels

The many different types of information systems are divided into categories based on where they are used in the hierarchy of an organisation.

Student Activity 12.1.1.4

Answer the following.

1. Based on the discussions, what are the three categories that Information Systems can be classified into?

   a. _____

   b. _____

   c. _____

2. Fill up the table below with needed information for the four level pyramid models.

Type of Information System	Description of the Information System	Function of the Information System	Example of the Information System
1.			
2.			
3.			
4.			

12.1.1.5 Design and Plan an Information System

It has been mentioned that an Information System (IS) helps organise and analyse data with a purpose of turning raw data into useful information that can be used for decision making in an organisation. As such, it is made of vital components of hardware, software, databases, network, procedures and people. The complexity of the information resources environment suggests that planning is vital to success.

The plan describes the structure and content of the information system and how it is to be developed. The organisation's strategic plan should be the basis for the Management Information System (MIS) strategic plan. The overall responsibility of IS planning is the responsibility of Chief Information Officer (CIO).

A quality Information Systems Plan (ISP) must exhibit five distinct characteristics before it is useful. These five are presented in the table that follows.

Characteristic	Description
Timely	The ISP must be timely. An ISP that is created long after it is needed is useless. In almost all cases, it makes no sense to take longer to plan work than to perform the work planned.
Useable	The ISP must be useable. It must be so for all the projects as well as for each project. The ISP should exist in sections that once adopted, can be parceled out to project managers and immediately start.
Maintainable	The ISP must be maintainable. New business opportunities, new computers, business mergers, etc. all affect the ISP. The ISP must support quick changes to the estimates; technologies employed, and even possibly to the fundamental project sequences. Once these changes are accomplished, the new ISP should just be a few computer program executions away.
Quality	While the ISP must be a quality product, no ISP is ever perfect on the first try. As the ISP is executed, the metrics employed to derive the individual project estimates become refined as a consequence of new hardware technologies, code generators, techniques, or faster working staff. As these changes occur, their effects should be installable into the data that supports ISP computation. In short, the ISP is a living document. It should be updated on quarterly bases with every technology event.
Reproducible	The ISP must be reproducible. That is, when its development activities are performed by any other staff, the ISP produced should essentially be the same. The ISP should not vary significantly by staff assigned.

Whenever a proposal for the development of an ISP is created it must be assessed against these five characteristics. If any fail or not addressed in an optimum way, the entire set of funds for the development of an ISP is risked.

The following are the approaches in organising and supervising the information system planning effort:

1. Planning staff within information systems functions (planning specialists)
2. Ad hoc planning groups within information systems
3. Planning group with representatives from various functions

Whichever is chosen as an approach to organise and supervise an information system, the following are the activities needed to be undertaken:

a. Master plan is reviewed by the steering committee which comprises of executives from major functional areas.

b. The committee also periodically reviews progress against the plan.

c. The master plan is integrated in the organisational plan by top management after review and approval.

d. Information system policies and procedures are defined.

Now let us study the content of Master Development plan also known as the Information System plan or the Information Resource plan.

The master plan has two components: a long-range plan and a short-range plan. The long-range plan provides general guidelines for direction and the short-range plan provides a basis for specific accountability as to operational and financial performance. It consists of the following subheadings:

a. Information system goals, objectives, and architecture which must contain the following information:

- Organisational goals, objectives, and strategies
- External environment (it can be other originations or industry, government regulations, customers or stakeholders and suppliers)
- Internal organisational restrictions such as management philosophy
- Assumptions about risks and potential consequences
- Overall goals, objectives, and strategy for the information system

- Architecture or planned design of the information system

b. Inventory of current capabilities is divided into two: first, the actual inventory of the hardware, software (System software, Database management System (DBMS) and others) and the application systems (classified on the basis of functional systems, organisational strategy, maintenance need). Second, the analysis of expense, hardware utilisation, software utilisation, personnel utilisation (further classification such as job, skill, functional area), status of projects in progress and the assessment of strengths and weaknesses important aspects that affect the planned design of the information system.

c. Forecast of developments against the plan includes the following:

- Hardware and software technological availabilities should be forecasted with expected impact on existing IS
- Methodology changes should be forecasted
- Environmental developments such as government regulations, tax laws and competitors affecting IS should be stated

d. The specific plan must consists of the following:

- Hardware acquisition schedule
- Purchased software schedule which includes both the systems software and the applications software
- Application development schedule
- Software maintenance and conversion schedule
- Personnel resources required and schedule of hiring and training
- Financial resources required by object of expenditure

The maintenance of master plan involves a requirement of an update of the Information System (IS) plan on the following:

- Changing organisational setup
- Changes in technology
- Changing needs of system
- Internal events
- Progress of new systems

- External events

Therefore, planning and designing an Information System must meet all the organisation's needs and priorities at the end. The designed plan must be feasible to cater for the organisation's expected cost savings, increased revenue, increased profits, and reductions in required investment. Such now spells the efficient information systems plan for an effective organisational management.

Student Activity 12.1.1.5

The following are the activities necessary to be undertaken in planning and designing an information system. Write a brief explanation of the importance of each in your own words.

a. Master plan is reviewed by the steering committee which comprises of executives from major functional areas.

_____

_____

_____

b. The committee also periodically reviews progress against the plan.

_____

_____

_____

_____

c. The master plan is integrated in the organisational plan by top management after review and approval.

_____

_____

_____

d. Information system policies and procedures are defined.

_____

_____

_____

_____

12.1.1.6 Issues related to Information Systems

New computer technologies for gathering, storing, manipulating, and communicating data are revolutionising the use and spread of information. Along the way, they are also creating ethical dilemmas. Issues have sprouted from this ethical dilemmas brought about by technology.

The speed and efficiency of electronic information systems, which include local and global networks, databases, and programs for processing information, force people to confront entirely new rights and responsibilities in their use of information and to reconsider standards of conduct shaped before the advent of computers.

Information is a source of power and, increasingly, the key to prosperity among those with access to it. Consequently, developments in information systems also involve social and political relationships-- and so make ethical considerations in how information is used all the more important. Electronic systems now reach into all levels of government, into the workplace, and into private lives to such an extent that even people without access to these systems are affected in significant ways by them. New ethical and legal decisions are necessary to balance the needs and rights of everyone.

The following are some of the issues related to the use of information systems:

1. Ethical issues: intellectual property rights, electronic monitoring of employees, data utilisation, and morality in information systems usage;

2. Cultural issues: assimilation of emerging technologies, developing trust, power asymmetry, policy implementation, and social environments;

3. Human interaction issues: recruitment and retaining of technical personnel, motivation, leadership, social presence, and organisational champions of information systems;

4. Relationship issues: development partnerships, virtual teams, group cohesiveness, collaboration, group facilitation, networking, and buyer-supplier linkages;

5. Security issues: misuse of data, virus/worm creation, Intranet abuse, data protection, fraud with systems use, and standards and regulations.

Generally speaking, ethics include moral choices made by individuals in relation to the rest of the community, standards of acceptable behaviour, and rules governing members of a profession. The broad issues relating to electronic information systems include control of and access to information, privacy and misuse of data, and international considerations.

1. **Control and access to information**
   It has been discussed that a network is any set of computers able to communicate with one another. Some networks are contained within institutions or companies, enabling people within a single organisation to communicate electronically. Many of

these small systems are also hooked into other organisations' computers. Thousands of such networks collectively form the Internet.

Control and access to information now becomes a problem as the fluidity of information on the networks has caused some confusion about how copyrights and intellectual property rights apply to electronic files. In the relatively small world of the original network users, an emphasis on free exchange of information and a common understanding of intellectual property allayed most potential conflicts over use of information.

Now, as the networks grow larger and attract a broader range of people, some clarification of how electronic files may be used is becoming necessary. The ease with which electronic files can be distributed and the nature of some electronic information create problems within existing copyright law: either the law does not address the uniqueness of electronic information or the law is too easily undermined by the ease with which files can be copied and transferred. Similar problems have arisen with photocopy machines, VCRs, and tape recorders. To make matters more complex, other countries may have different copyright laws, so information made available globally through a network may not have the same protections in other places.

One of the major issues in electronic networks is the question of access: who will have access to the networks, and what kinds of information will be accessible. These questions are important because networks offer tremendous economic, political, and even social advantages to people who have access to them. As the networks become a larger present in the society, conflicts may arise between information "haves" and "have-nots." Conceivably, network communication could create greater equality by offering common access to all resources for all citizens. Already, in a few places scattered around the country, experiments with "freenets," network connections established through local libraries or other municipal or local organisations specifically for people who otherwise would have no way to use the networks, have shown that those people will, for instance, participate more in local government issues. They, therefore, have a greater voice in whatever happens with the local government. Conversely, if access is not evenly distributed, it threatens to perpetuate or deepen existing divides between the poor, who cannot afford expensive computer systems, and the better-off.

2. **Privacy and misuse of data**

Countering questions of rights to access are questions of privacy. The degree of control that people have over what other people can find out and distribute about them has dropped markedly with the growth of electronic databases and network communications. The amount and kinds of personal information available as a result of both technologies is startling: financial, medical, educational and employment histories; driving records, insurance records, buying habits, hobbies, pets, family and associates, travels, phone usage(where and when), income, marital status, criminal records, address changes, and so on, can all be accessed through electronic networks.

Two kinds of individuals have access to personal information that might be kept in a networked computer. **Hackers** are those with no right to a system on which personal files might be held, and **system operators**, who have rights to be on a system but not necessarily to read personal files. System operators have access to root directories and can, for instance, read everything on private e-mail accounts. They might also hold backup tapes of entire root directories containing personal files that were thought to be safely deleted. Hackers and system operators do not necessarily pose a threat to privacy rights that is any greater than risks run with a curious postman or telephone operator. However, they can gain access to personal information with a much smaller risk of detection, which makes the enforcement of privacy rights much more difficult.

Issues about the use of Information System have brought about a change in culture. Cultural norms and values shape a society's definition of acceptable behaviour. On-line standards of conduct are founded on the norms of the society in which a network is set, but these broader norms and values are often challenged by the character of human interaction in electronic networks. Networks stretch across societies that have different values and traditions. The computers that form them have capacities that allow people to do things they could not do before and to do so with anonymity.

Lastly, the networks, new as they are, have their own social history, in which somewhat different norms have been formed. The people who have so far populated the virtual community have tend to value individuality, free expression, and free exchange of information, anarchy and nonconformity more than other groups. Acceptable behaviour on the networks, therefore, has slightly different standards. These may change as many more people join the networks. But, so far, the less conventional on-line standards of conduct have been jealously guarded by long-time network users. These users generally are people who have strong feelings about the shape of life on their various networks and about what shape it will take in the future. New users of the Internet and of various smaller networks should be aware that they are entering an unconventional social community.

3. **International considerations**

In the international arena, issues of community standards will remain sensitive. The problem may, in some countries, be a prime consideration in how the Internet is allowed to grow. Some nations have far different attitudes towards political debate and the expression of political dissent. Among world religions, tremendous differences exist in attitudes toward blasphemy, heresy, and family values.

Finally, no international consensus exists on issues of human sexuality, obscenity, reproduction, and personal values. The free expression so valued by long-term network users thus conflicts directly with another valued feature of the Internet with its international reach and potential for rich cross-cultural exchanges. How the issue will be resolved will affect the fundamental nature of the Internet in the future.

Despite efforts to settle issues brought about by the use of information systems, legal decisions lag behind technical developments. Ethics fill the gap as people negotiate how the use of electronic information should proceed.

Solutions to these issues brought about by the use of information systems can be seen in the different government laws and controls on data and hardware security, the use of Netiquette and acceptable user policies which have all been discussed in the Grade 11 Information and Communication Technology module.

In addition to the discussions on Netiquette provided in Grade 11, it is worthwhile to include these guidelines when on-line.

Some simple guidelines to on-line civil behaviour are:

- In general, do not waste other people's time, be disruptive, or threaten.
- Do not take up network storage space with large, unnecessary files; these should be downloaded.
- Do not look at other people's files or use other systems without permission.
- When joining a bulletin board or discussion group, check the FAQ (frequently asked questions) file before asking questions.
- Remember that on-line communications lack the nuances of tone, facial expression, and body language. Write clearly and try to spell correctly and use good grammar.
- Add emoticons, or Smileys --expressive symbols--to clarify meaning.
- Do not SHOUT needlessly. Capital letters are the on-line equivalent of shouting.
- Use asterisks to give emphasis, but do so *sparingly*.
- Sign messages, and include an e-mail address when writing to strangers, just in case a message's header is lost.
- Personal attacks or complaints are called flaming. Be discriminate: flaming can turn into flame wars and disrupt discussion groups.
- People who become too unbearable can be banned from a system or simply ignored.

Student Activity 12.1.1.6

Quote one issue from a newspaper article about the use of information system and give a brief reaction to it.

Summative Exercise 12.1.1

Answer the following questions.

1. Explain the difference between each pair of words or terms.

   a. Local Area Network and Wide Area Network

   _____

   _____

   _____

   _____

   b. Information System and Network

   _____

   _____

   _____

   _____

   c. Hardware and Software

   _____

   _____

   _____

   _____

   d. Databases and Procedures

   _____

   _____

   _____

   _____

   e. Transaction Processing System and Management Information System

   _____

   _____

   _____

   _____

f. Decision Support System and Executive Information System

_____

_____

_____

_____

2. Explain the importance of the following in an Information System.

a. Network

_____

_____

_____

_____

_____

b. Hardware

_____

_____

_____

_____

c. Software

_____

_____

_____

_____

d. People

_____

_____

_____

_____

_____

e. Information System Plan

_____

_____

_____

_____

f. Government control and laws

_____

_____

_____

_____

_____

g. Netiquette

_____

_____

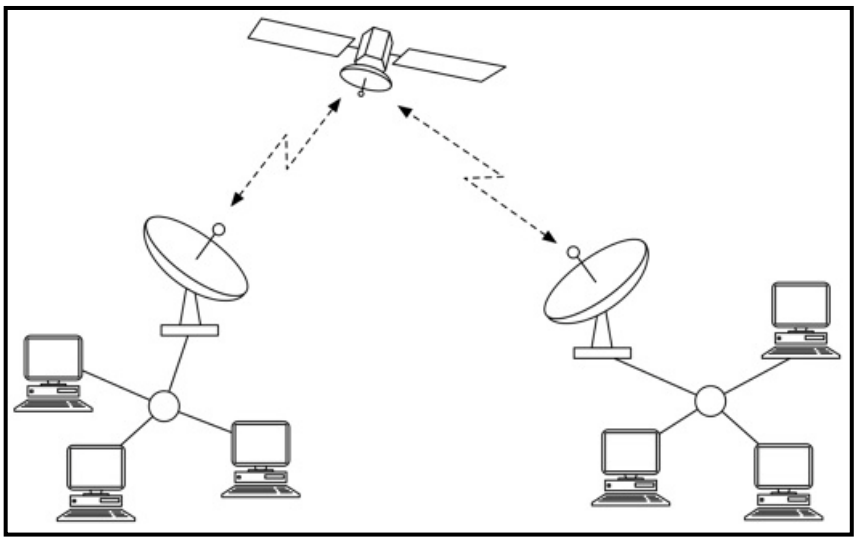
_____

_____

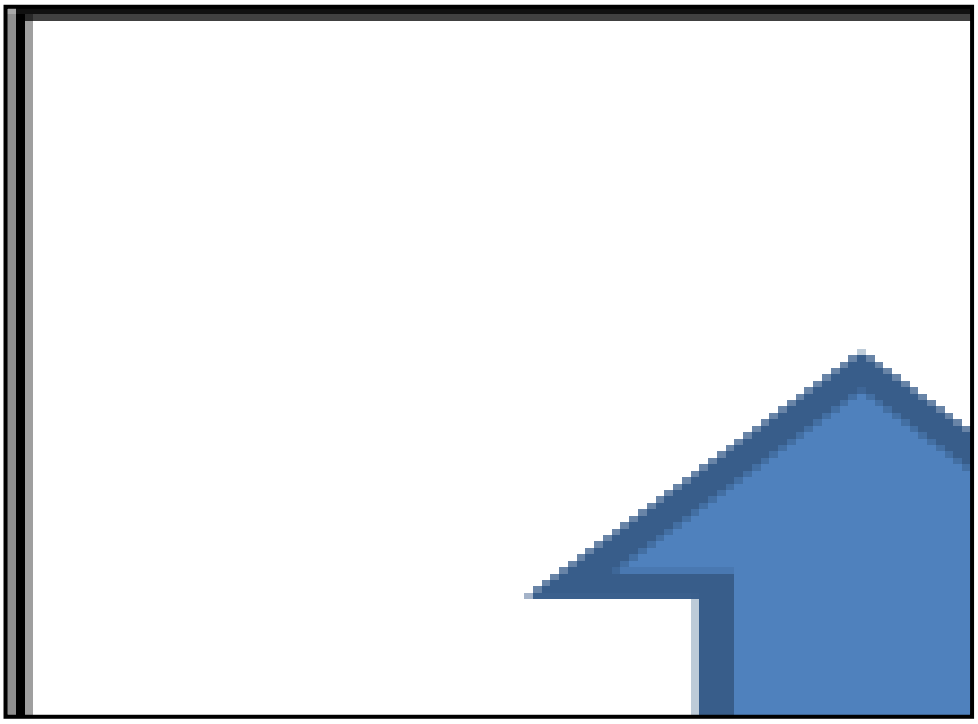
_____

3. Explain or describe the following figures and diagrams.

a.



b.



_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Answers to Activity 12.1.1

Student Activity 12.1.1.1

1. Any three of the following can be the answers.

    a. An Information System (IS) is defined as the software that helps organise and analyse data.

    b. An information system is a system composed of people and computers that processes or interprets information.

    c. Information Systems is a scientific field of study that addresses the range of strategic, managerial, and operational activities involved in the gathering, processing, storing, distributing, and use of information and its associated technologies in society and organisations.

    d. An organisational function that applies IS knowledge in industry, government agencies, and not-for-profit organisations.

    e. The interaction between algorithmic processes and technology.

    f. The technology an organisation uses and also the way in which the organisations interact with the technology and the way in which the technology works with the organisation's business processes.

    g. Any specific information system which aims to support operations, management and decision making.

h. An information system is a work system whose activities are devoted to processing (capturing, transmitting, storing, retrieving, manipulating and displaying) information.

2. Any two from these can be the answers.

   a. useful in large data organisation for a distinctive purpose in a decision making.

   b. Information System makes it possible to answer questions and solve problems relevant to the mission of an organisation.

   c. Turn raw data into useful information that can be used for decision making in an organisation.

   d. To turn raw data into useful information that can be used for decision making in an organisation.

Student Activity 12.1.1.2

1. 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.

2. Network allows then the exchange data. a network allows computers to share files, users to message each other, a whole room of computers to share a single printer and others. Computer networks allow the user to access remote programs and remote databases either of the same organisation or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities.

3. Any three from the following can be the answers

   - cost reduction by sharing hard- and software resources
   - high reliability by having multiple sources of supply
   - cost reduction by downsizing to microcomputer-based networks instead of using mainframes
   - greater flexibility because of possibility to connect devices
   - Easily share files and data
   - Share resources such as printers and Internet connections
   - Communicate with other network users (e-mail, instant messaging, video-conferencing, etc.)
   - Store data centrally (using a file server) for ease of access and back-up

- Keep all of our settings centrally so we can use any workstation
- Make use of on-line services such as shopping (e-commerce) or banking
- Get access to a huge range of information for research
- Access different forms of entertainment (games, video, etc.)
- Join on-line communities (e.g. MySpace, Facebook, etc.)

Student Activity 12.1.1.3

The answer can be similar to this one below.

A good information system must have the capability to facilitate works to improve productivity. It must enble the people to have access, manage, input, and manipulate data in a system to track and handle all daily routines like inventory, cash flow, invoicing, sales, and many more. It must be accessible, accurate, simple, flexible, and secured.

Student Activity 12.1.1.4

1.

a. based on the type of decisions taken at different levels in the organisation

b. based on the processing requirement of different levels in the organisation

c. based on the different levels of hierarchy in the organisation

2. The answers may be similar to these ones below.

Type of Information System	Description of the Information System	Function of the Information System	Example of the Information System
1. Transaction Processing Systems (TPS)	Transaction Processing System is operational-level systems at the bottom of the pyramid.	They are usually operated directly by shop floor workers or front line staff, which provide the key data required to support the management of operations.	• Payroll systems • Order processing systems • Reservation systems • Stock control systems • Systems for payments and funds transfers

2. Management Information Systems (MIS)	Management Information Systems are management-level systems that are used by middle managers to help ensure the smooth running of the organisation in the short to medium term.	The highly structured information provided by these systems allows managers to evaluate an organisation's performance by comparing current with previous outputs.	• Sales management systems • Inventory control systems • Budgeting systems • Management Reporting Systems (MRS) • Personnel (HRM) systems
3. Decision Support Systems (DSS)	A Decision Support System can be seen as knowledge based system, used by senior managers, which facilitates the creation of knowledge and allow its integration into the organisation.	These systems are often used to analyze existing structured information and allow managers to project the potential effects of their decisions into the future. Such systems are usually interactive and are used to solve ill structured problems. They offer access to databases, analytical tools, allow "what if" simulations, and may support the exchange of information within the organisation.	• Group Decision Support Systems (GDSS) • Computer Supported Co-operative work (CSCW) • Logistics systems • Financial Planning systems • Spreadsheet Models
4. Executive Information Systems (EIS)	Executive Information Systems are strategic-level information systems that are found at the top of the Pyramid.	They help executives and senior managers analyze the environment in which the organisation operates, to identify long-term trends, and to plan appropriate courses of action.	Executive Information Systems tend to be highly individualised and are often custom made for a particular client group; however, a number of off-the-shelf EIS packages do exist and many enterprise level systems offer a customizable EIS module.

Student Activity 12.1.1.5

The answers may be similar to these ones below.

a. The importance of this is for the administration to review well the master plan if all items are in line with the organisation's aims and policies as well as to review any possible existence of errors and loop holes in the plan.

b. The committee must review the plan periodically to ensure proper implementation done. This will monitor the progress of the implementation and can immediately resolve ant issue that might arise.

c. The master plan must be integrated in the organisational plan to avoid any conflict of interest in the implementation of the master plan vis-à-vis with the existing organisational plan.

d. This defined system policies will ensure clear implementation guidelines for the master plan which will further ensure less problems and hiccups along the way.

Student Activity 12.1.1.6

The sample on the next page shows an article or a study dealing with how ICT impacts society. Any article with sufficient reaction may be the valid answer for this item.

The impact of Information and Communication Technology (ict) on News Processing, Reporting and Dissemination on Broadcast stations in Lagos, Nigeria.

ifeanyi adigwe MR, *Afica Regional Centre for Information Science (ARCIS), University of Ibadan, Nigeria*

Follow

Date of this Version

2012

Citation

Adigwe.,I (2012) The impact of Information and Communication Technology (ict) on News Processing, Reporting and Dissemination on Broadcast stations in Lagos, Nigeria. *Library Philosophy and Practice*

Abstract

Information and Communication technology is perceived to be a force to be reckoned with in the 21st century because it has caused and continues to cause major changes in the way we live. In the electronic media, ICT has ignited and provoked radical and drastic changes that has affected and revolutionized the broadcast industry, most especially in immediacy and timeliness of news. With Information and Communication Technology information spread, infinitely becomes faster and cheaper and readily available. This study attempts to investigate the impact of information and communication technology in news processing and reporting on some selected broadcast stations in Nigeria. The Research Design employed is the descriptive survey design. Three research questions were formulated for the study. The population for the study consisted of 90 respondents sampled in the selected broadcast stations in Lagos, Nigeria. Questionnaire was used as the instrument for gathering data for the study. Data collected were analyzed using frequency tables and simple percentage. This study uncovered some of the numerous benefits and challenges associated with the use of ICT in news processing in broadcast industry. This study concludes that ICT has created opportunities for widespread electronic and timely delivery of news. Furthermore, not only are there technology barriers that news organizations need to overcome to deliver news electronically, but there are also problems of employee attitudes toward new technologies and resistance to change. The implication of the use ICTs to broadcast stations might lead to an overall shrink in the need for human correspondents.

ICT in any area would surely have a great impact to it. This study confirms that the use of ICT in broadcasting will have its upsides and downsides.

As information can be available anytime, broadcasting it in real time is a demand that through ICT it can be achieved efficiently. However, the need for people in this area will likely be diminished as machines now can efficiently and accurately do what a human person can.

Whatever the situation be, it is important to take note that both humans and machines need to work in a complementary manner as one cannot do what one can perhaps in its own unique way. ICT can make things easier and faster but still manpower is still relevant amidst the existence of ICT.

Answers to Summative Activity 12.1.1

1. Answers may be similar to these ones below.

   a. Local Area Network and Wide Area Network
   A local area network, or LAN, consists of a computer network at a single site, typically an individual office building while a wide area network, or WAN, occupies a very large area, such as an entire country or the entire world.

   b. Information System and Network
   An Information System (IS) is defined as the software that helps organise and analyse data while the 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.

   c. Hardware and Software
   Hardware consists of tangible machines and equipment necessary to put up and maintain a network while the software is the NOS or the network operating system which compliments with the network in putting up and maintaining a functional network.

   d. Databases and Procedures
   Databases consist of all the stored information arranged in a particular way to answer the daily operational needs of an organisation while the Procedures speak of the policies on how the database and the network or the information system plan must be implemented, monitored and evaluated.

   e. Transaction Processing System and Management Information System
   Transaction Processing System is operational-level systems at the bottom of the pyramid. They are usually operated directly by shop floor workers or front line staff, which provide the key data required to support the management of operations while Management Information Systems are management-level systems that are used by middle managers to help ensure the smooth running of the organisation in the short to medium term.

   f. Decision Support System and Executive Information System
   A Decision Support System can be seen as knowledge based system, used by senior managers, which facilitates the creation of knowledge and allow its integration into the organisation while Executive Information Systems are strategic-level information systems that are found at the top of the Pyramid. They help executives and senior managers analyse the environment in which the organisation operates, to identify long-term trends, and to plan appropriate courses of action.

2. Answers may be similar to these ones below.

a. Network
It allows then the exchange data. For example a network allows computers to share files, users to message each other, a whole room of computers to share a single printer and others.

b. Hardware
It provides the platform necessary for network to exist and function. This includes the machine, the cables, the cards, the modems and all other tangible equipment and machine necessary to put up a network.

The term hardware refers to machinery. This category includes the computer itself, which is often referred to as the central processing unit (CPU), and all of its support equipment. Among the support equipment are input and output devices, storage devices and communications devices. Computer-based information systems use computer hardware, such as processors, monitors, keyboard, and printers.

c. Software
The software is the network operating software or NOS which provides all the necessary programs for a network to function.

The term software refers to computer programs and the manuals (if any) that support them. Computer programs are machine-readable instructions that direct the circuitry within the hardware parts of the system to function in ways that produce useful information from data. Programs are generally stored on some input / output medium, often a disk or tape. These are the programs used to organise, process and analyze data.

d. People
This includes all users in the network and all those who put up and maintain the operation of a network. These are people making use, maintaining and monitoring the network.

Every system needs people if it is to be useful. Often the most over-looked element of the system is the people, probably the component that most influence the success or failure of information systems.

e. Information System Plan
The plan describes the structure and content of the information system and how it is to be developed. The organisation's strategic plan should be the basis for the Management Information System (MIS) strategic plan.

f. Government control and laws
These are all the controls and laws regarding proper use of computer machine with all its data and information and Internet. The Child Protection Act,

Designs, Patent and Privacy Laws and Data Protection Act are among others which ensure proper use of computer data and information.

g. Netiquette
This provides the common ways on how to properly behave in the information technology world especially when connected to the Internet.

3.

a. Network connections is shown here where the computers are logged into a network where one way of connection would either be wired using cables or wireless using the satellite to transmit the signals.

b. Four level pyramid model based on the different levels of hierarchy in the organisation which compare how the information systems in our model differ from each other.

It consists of the Transaction Processing System is operational-level systems at the bottom of the pyramid. They are usually operated directly by shop floor workers or front line staff, which provide the key data required to support the management of operations.

Next, Management Information Systems are management-level systems that are used by middle managers to help ensure the smooth running of the organisation in the short to medium term. The highly structured information provided by these systems allows managers to evaluate an organisation's performance by comparing current with previous outputs.

Then the Decision Support System can be seen as knowledge based system, used by senior managers, which facilitates the creation of knowledge and allow its integration into the organisation. These systems are often used to analyze existing structured information and allow managers to project the potential effects of their decisions into the future.

Lastly, the Executive Information Systems are strategic-level information systems that are found at the top of the Pyramid. They help executives and senior managers analyze the environment in which the organisation operates, to identify long-term trends, and to plan appropriate courses of action.

12.1.2 Networking Systems

12.1.2.1 Definition, Benefits and Threats of Networking Systems

It has been previously discussed that a network consists of two or more computers or other electronic devices connected to each so they can exchange data. A system speaks of an organised method of doing things. Putting these two words together, one will come up with what is known as a networking system which consists of a computer network or data network. A computer network or data network is a telecommunications network that allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections. Data is transferred in the form of packets. A packet consists of two kinds of data: control information and user data where the control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information.

A representation of a computer networking system

The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the Internet. Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the physical media used to transmit their signals, the communications protocols to organize network traffic, the network's size, topology and organisational intent. In most cases, communications protocols are layered on (i.e. work

using) other more specific or more general communications protocols, except for the physical layer that directly deals with the physical media.

Networking protocols and transmission modes will be further elaborated as we will continue discussing the networking systems.

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.

Today, computer networks are the core of modern communication. The scope of communication has increased significantly in the past decade. This boom in communications would not have been possible without the progressively advancing computer network. Computer networks, and the technologies that make communication between networked computers possible, continue to drive computer hardware, software, and peripherals industries. The expansion of related industries is mirrored by growth in the numbers and types of people using networks, from the researcher to the home user.

The benefits networking offers to its users can be separated into two main groups:

- Connectivity
- Sharing

Networks make computers and their users capable of being connected together. This facilitates sharing of resources and information between the users. The modern businesses are expanded all over the world. So, uses and significance of networking has gained momentum during the past years.

The many benefits that networking offers to us are:

1. **Helps to enhance connectivity.**
   Networks connect and link unlimited number of computers. This in turn connects the people using those computers. Individuals within a work group are connected through local area networks. Many LANs in distant locations are interconnected through larger wide area networks (WANs). These connections ease the communication between people using technologies like e-mail. Today, e-mail has become the easiest and cheapest mode of transformation of information between the users.

2. **Networking helps in sharing of hardware.**
   Networks help in sharing of different kinds of hardware devices. For example, sharing of a single printer in an office of twenty people is done through networking of wires. This saves lot of cost that could otherwise have incurred if twenty different printers were provided for each computer in use.

3. **Eases out management of data.**
   Networking provides the advantage of centralisation of data from all the user systems to one system where it can be managed in an easy and better way. Administrators can thus manage all this data efficiently and in the best interest of the company. Even the access of this data becomes easy for the users.

4. **Internet**
   The most beautiful gift of networking is internet that is massively used by people all over the world. Whenever you are accessing internet, you are making use of a network.

5. **Data Sharing**
   Sharing of data through the use of networks helps save a lot of time and energy. It also facilitates the use of applications like databases that are based on ability of many individuals to access and to share exactly the same data.

6. **Networking has promoted gaming.**
   Many internet games are being played by players all over the world using common servers. These give fun and enjoyment to people and also improve their skills.

   Such are the varied benefits of networking to the people all over the world. The success of networking in providing benefits to people depends upon the frequency of its use. So, make the maximum out of this wonderful gift of technology to man.

More specifically, networking systems offers the following key benefits:

1. **Strengthening Relationships**
   Networking is about sharing, not taking. It is about forming trust and helping one another toward goals. Regularly engaging with your contacts and finding opportunities to assist them helps to strengthen the relationship. By doing this, you sow the seeds for reciprocal assistance when you need help to achieve your goals.

2. **Fresh Ideas**
   Your network can be an excellent source of new perspectives and ideas to help you in your role. Exchanging information on challenges, experiences and goals is a key benefit of networking because it allows you to gain new insights that you may not have otherwise thought of. Similarly, offering helpful ideas to a contact is an excellent way to build your reputation as an innovative thinker.

3. **Raised Profile**
   Being visible and getting noticed is a benefit of networking that is essential in career building. Regularly attending professional and social events will help you gain recognition. You can then help to build your reputation as knowledgeable, reliable and supportive by offering useful information or tips to people who need it.

4. **Access To Opportunities**
   Expanding your contacts can open doors to new opportunities for business, career advancement, personal growth, or simply new knowledge. Active networking helps

to keep you top of mind when opportunities such as job openings arise and increases your chances of being exposed to potentially relevant people or even a referral.

5. **New Information**
Networking is a great opportunity to exchange best practice knowledge, learn about the business techniques of your peers and stay abreast of the latest industry developments. A wide network of informed, interconnected contacts means broader access to new and valuable information.

6. **Advice and Support**
Gaining the advice of experienced peers is an important benefit of networking. Discussing common challenges and opportunities opens the door to valuable suggestions and guidance. Offering genuine assistance to your contacts also sets a strong foundation for receiving support in return when you need it.

Despite these benefits, there will always be the other side of the coin, the threats. With an increasing amount of people getting connected to networks, the security threats that cause massive harm are also increasing.

Network security is a major part of a network that needs to be maintained because information is being passed between computers and other electronic devices. This is very vulnerable to attack. Over the past five years people who manage network security have seen a massive increase in the number of hackers and criminals creating malicious threats that have been pumped into networks across the world.

Data and computer security had been discussed in the Grade 11 Information and Communication Technology Module One. Going more specifically in our discussion, the following are the common networking threats that would offer significant disadvantages to both the user and the computer. Along with the discussion of the threats, solutions will be discussed as well.

1. **Viruses and Worms**
A Virus is a “program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes”. Viruses can cause a huge amount of damage to computers. An example of a virus would be if you opened an email and a malicious piece of code was downloaded onto your computer causing your computer to freeze.

In relation to a network, if a virus is downloaded then all the computers in the network would be affected because the virus would make copies of itself and spread itself across the networks. A worm is similar to a virus but a worm can run itself whereas a virus needs a host program to run.

Solution: Install a security suite that protects the computer against threats such as viruses and worms.

2. **Trojan Horses**

A Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.

In a network, if a Trojan Horse is installed on a computer and tampers with the file allocation table it could cause a massive amount of damage to all computers of that network.

Solution: Security suites, such as Norton Internet Security, will prevent you from downloading Trojan Horses.

3. **SPAM**

SPAM is "flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it". It is believed that SPAM would not be the biggest risk to a network because even though it may get annoying and plentiful it still does not destroy any physical elements of the network.

Solution: SPAM filters are an effective way to stop SPAM. These filters come with most of the e-mail providers online. Also you can buy a variety of SPAM filters that work effectively.

4. **Phishing**

Phishing is "an e-mail fraud method in which the perpetrator sends out legitimate-looking emails in an attempt to gather personal and financial information from recipients." It is believed that phishing is one of the worst security threats over a network because a lot of people who use computers linked up to a network are amateurs and would be very vulnerable to giving out information that could cause situations such as theft of money or identity theft.

Solution: Similar to SPAM use Phishing filters to filter out this unwanted mail and to prevent threat.

5. **Packet Sniffers**

"A packet sniffer is a device or program that allows eavesdropping on traffic travelling between networked computers. The packet sniffer will capture data that is addressed to other machines, saving it for later analysis."

In a network a packet sniffer can filter out personal information and this can lead to areas such as identity theft so this is a major security threat to a network.

Solution: "When strong encryption is used, all packets are unreadable to any but the destination address, making packet sniffers useless." A solution then, is to obtain strong encryption.

6. **Maliciously Coded Websites**
Some websites across the net contain code that is malicious. Malicious code is "Programming code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computer system."
Solution: Using a security suite, such as AVG, can detect infected sites and try to prevent the user from entering the site.

7. **Password Attacks**
Password attacks are attacks by hackers who are able to determine passwords or find passwords to different protected electronic areas.

Many systems on a network are password protected and hence it would be easy for a hacker to hack into the systems and steal data. This may be the easiest way to obtain private information because you are able to get software online that obtains the password for you.

Solution: At present there is no software that prevents password attacks.

8. **Hardware Loss and Residual Data Fragments**
Hardware loss and residual data fragments are a growing worry for companies, governments and others.

An example of this is, if a number of laptops are stolen from a bank that has client details on them, this would enable the thieves to get personal information from clients and maybe steal the client's identities.

This is a growing concern and as of present the only solution is to keep data and hardware under strict surveillance.

9. **Shared Computers**
Shared computers involve sharing a computer with one or more people. The following are a series of tips to follow when sharing computers:

- Do not check the "Remember my ID on this computer" box
- Never leave a computer unattended while signed-in
- Always sign out completely
- Clear the browsers cache
- Avoid confidential transactions
- Be wary of spyware
- Never save passwords
- Change your password often

10. **Zombie Computers and Botnets**

A zombie computer or "drone" is a computer that has been secretly compromised by hacking tools which allow a third party to control the computer and its resources remotely. A hacker could hack into a computer and control the computer and obtain data.

Solution: Antivirus software can help prevent zombie computers.

A botnet "is a number of Internet computers that have been set up to forward transmissions (including spam or viruses) to other computers on the internet, although their owners are unaware of it."

This is a major security threat on a network because the network which is unknown to anyone, could be acting as a hub that forwards malicious files to other computers.

Solution: Network Intrusion Prevention (NIP) systems can help prevent botnets.

With all of these threats, network security must be a priority which must consists of provisions and policies adopted by the network administrator to prevent and monitor unauthorised access, misuse, modification, or denial of the computer network and its network-accessible resources.

Moreover, with network security there is the authorisation of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. This method of enforcing an efficient network security will lessen much of the threats any networking systems might have.

Student Activity 12.1.2.1

Answer the following.

1. Define a networking system.

_____

_____

_____

_____

_____

2. Give two (2) benefits of a networking system.

a. _____

_____

b. _____

_____

3. Give three (3) threats of a networking system and provide a solution for each given threat.

a.

Threat: _____

Solution:_____

_____

_____

b.

Threat: _____

Solution:_____

_____

_____

c.

Threat: _____

Solution:_____

_____

_____

12.1.2.2 Protocols of Networking Systems

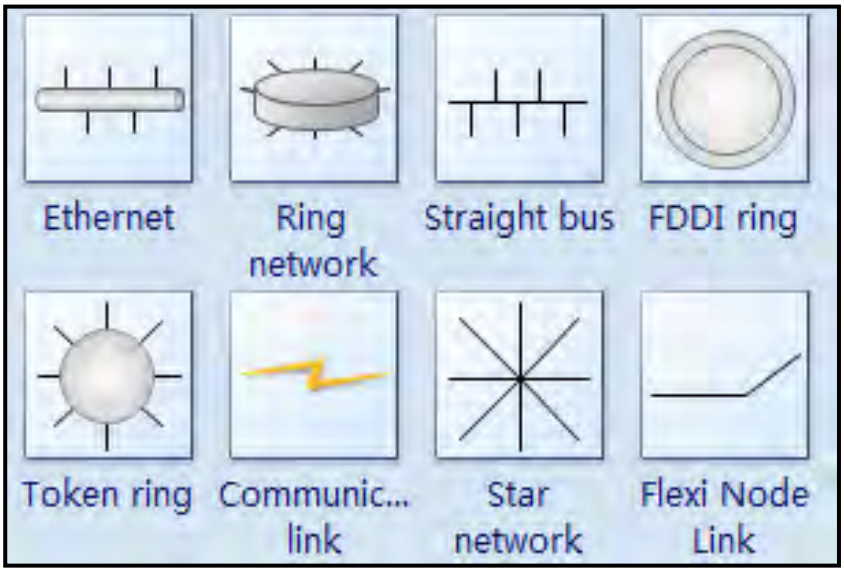
Network Protocol is a set of rules that governs the communication between computers on a network. Rules of network protocol include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer. Access method, topologies, types of network connection or cabling and speed of data transfer will be discussed as we move through our study. Let us study first, what a protocol is.

Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication. Hundreds of different computer network protocols have been developed. Each designed for specific purposes and environments.

The most common network protocols are:

1. Ethernet
2. Local Talk
5. ATM
3. Token Ring
4. FDDI

The following are some commonly used network symbols to represent different kinds of network protocols.



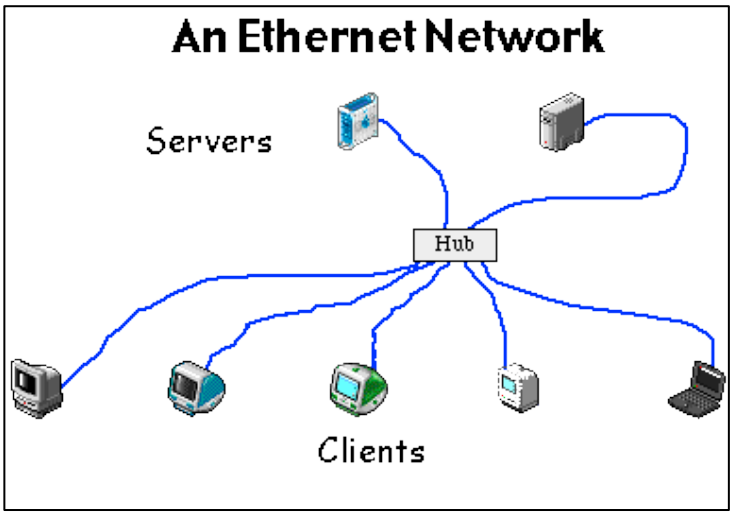
Commonly used network symbols

Let us discuss them one at a time.

1. **Ethernet** protocol is by far the most widely used one. 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 nodes

have already transmitted 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. A collision occurs when this happens. 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 affect the speed of transmission on the network.

The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.

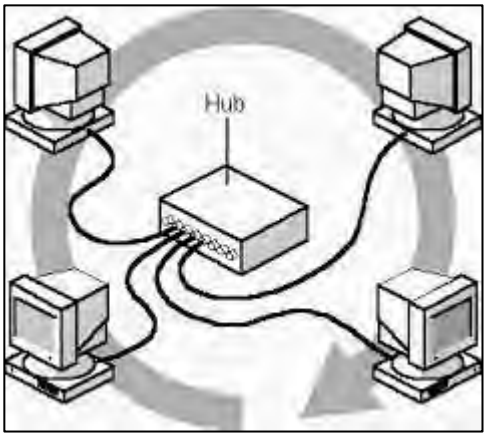


2. **Fast Ethernet** allows for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the application of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary. Fast Ethernet is becoming common in schools that have been recently wired.

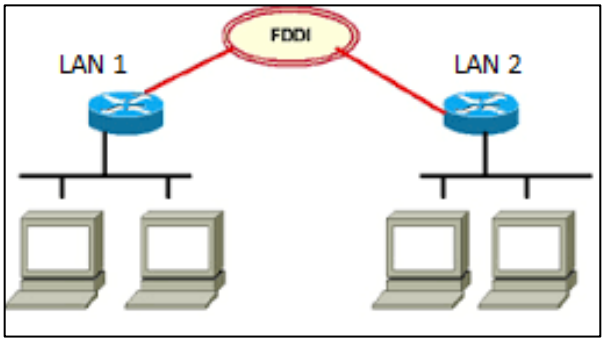
3. **Local Talk** is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by Local Talk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. Local Talk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established.

   The Local Talk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of Local Talk is low speed. Its speed of transmission is only 230 Kbps.

4. **Token Ring** protocol was developed by International Business Machines (IBM) in the mid-1980s. The access method used involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring in school environments has decreased.

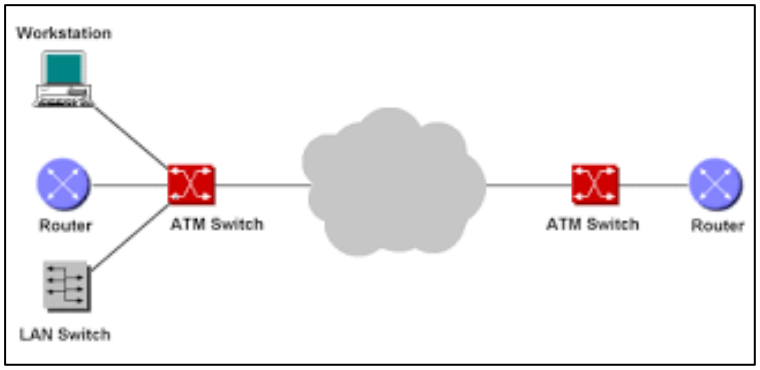


5. **Fiber Distributed Data Interface (FDDI)** is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new and complete ring. A major advantage of FDDI is high speed. It operates over fiber optic cable at 100 Mbps.



6. **Asynchronous Transfer Mode (ATM)** is a network protocol that transmits data at a speed of 155 Mbps and higher. ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.

ATM is most often used to interconnect two or more local area networks. It is also frequently used by Internet Service Providers to utilise high-speed access to the Internet for their clients. As ATM technology becomes more cost-effective, it will provide another solution for constructing faster local area networks.



7. **Gigabit Ethernet** protocol is the latest development in the Ethernet standard that has a transmission speed of 1 Gbps. Gigabit Ethernet is primarily used for backbones on a network at this time. It will probably also be used for workstation and server connections in the future. It can be used with both fiber optic cabling and copper. The 1000BaseTX, the copper cable used for Gigabit Ethernet, became the formal standard in 1999.

In a nutshell, the table below displays a comparison of all the network protocols that we have discussed.

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

It is worthy to take note that different protocols are used for different purposes on the network. The list provided in this discussion is some of the commonly used network protocols. A group of network protocols that work together at higher and lower levels are often called a protocol family. Modern operating systems like Microsoft Windows contain built-in daemons or services that implement support for some network protocols. Applications like Web browsers contain software libraries that support the high level protocols necessary for that application to function.

Student Activity 12.1.2.2

Answer the following.

1. What is a protocol?

_____

_____

_____

_____

_____

2. What is the importance of a network protocol?

_____

_____

_____

_____

_____

3. Name three (3) commonly used network protocols which are similar to each other, when it comes to cable. Contrast them when it comes to speed and topology.

_____

_____

_____

_____

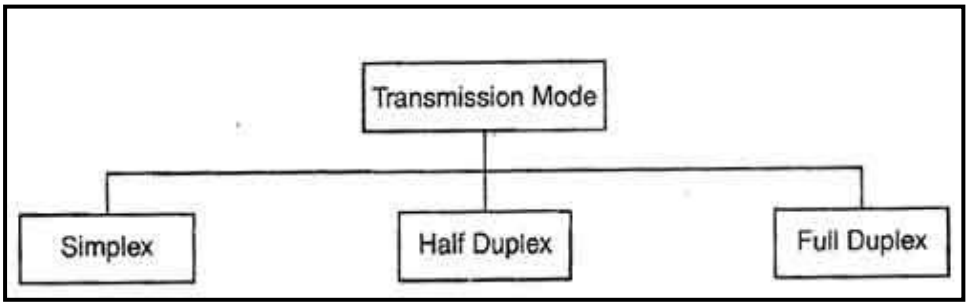
_____

12.1.2.3 Data Transmission Modes of Networking Systems

The way in which data is transmitted from one place to another is called data transmission mode. It is also called the data communication mode. It indicates the direction of flow of information. Sometimes, data transmission modes are also called directional modes.

Transmission mode defines the direction of the flow of information between two communication devices. That is, it tells the direction of signal flow between the two devices.

There are three ways or modes of data transmission. These are the Simplex, the Half-duplex (HDX) and the Full duplex (FDX)



An illustration of the three modes of data transmission

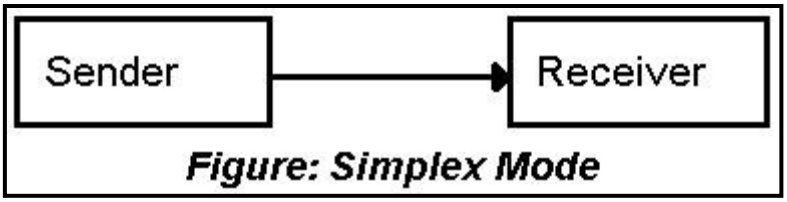
Let us discuss them one at a time.

1. **Simplex Mode**

   In simplex mode, data can flow in only one direction. In this type of transmission mode data can be sent only through one direction that is, communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems.

   Examples of simplex mode are loudspeaker, radio or television broadcasting, television and remote, keyboard and monitor etc. In this mode, a sender can only send data and cannot receive it. Similarly, a receiver can only receive data but cannot send it. Data sent from computer to printer is an example of simplex mode.

   In simplex mode, it is not possible to confirm successful transmission of data. It is also not possible to request the sender to re-transmit information. This mode is not widely used. However, this mode is used in business field at certain point-of-sale terminals. The other examples of simplex communication modes are Radio and T.V transmissions.



A representation of sender and receiver data transmission in a simplex mode

   In communication networks, communication can take place in one direction connected to such a circuit are either a send only or receive only device. There is no mechanism

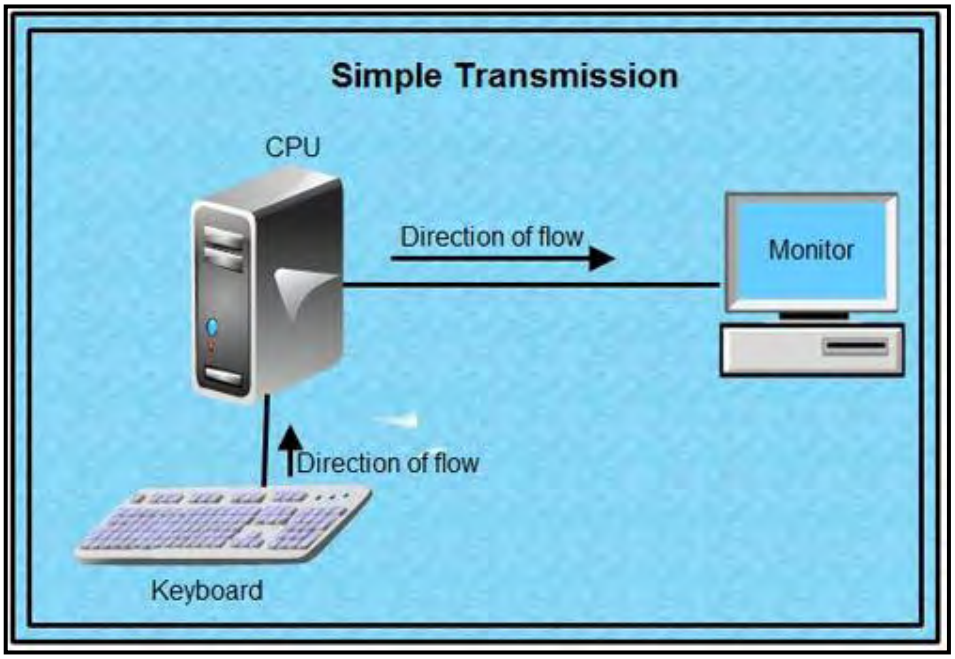
for information to be transmitted back to the sender. Communication is unidirectional and TV broadcasting is an example. Simplex transmission generally involves dedicated circuits. Simplex circuits are analogous to escalators, doorbells, fire alarms and security systems:

Examples of Simplex mode are:

1. A communication between a computer and a keyboard involves simplex duplex transmission. A television broadcast is an example of simplex duplex transmission.

2. Another example of simplex transmission is the loudspeaker system. An announcer speaks into a microphone and his/her voice is sent through an amplifier and then to all the speakers.

3. Many fire alarm systems work the same way.

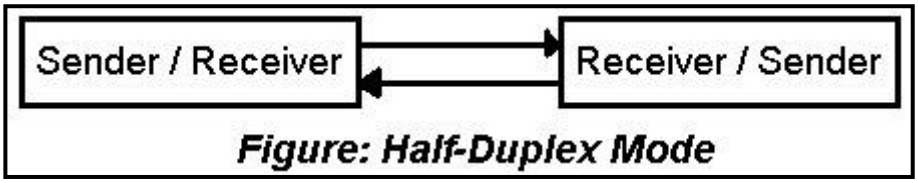


A representation of how a simplex transmission works

2. **Half-Duplex Mode**

In half-duplex mode, data can flow in both directions but only in one direction at a time. We can send data in both directions but it is done one at a time that is when the sender is sending the data then at that time we cannot send the sender our message. The data is sent in one direction. In this mode, data is sent and received alternatively. It is like a one-lane bridge where two-way traffic must give way in order to cross the other.

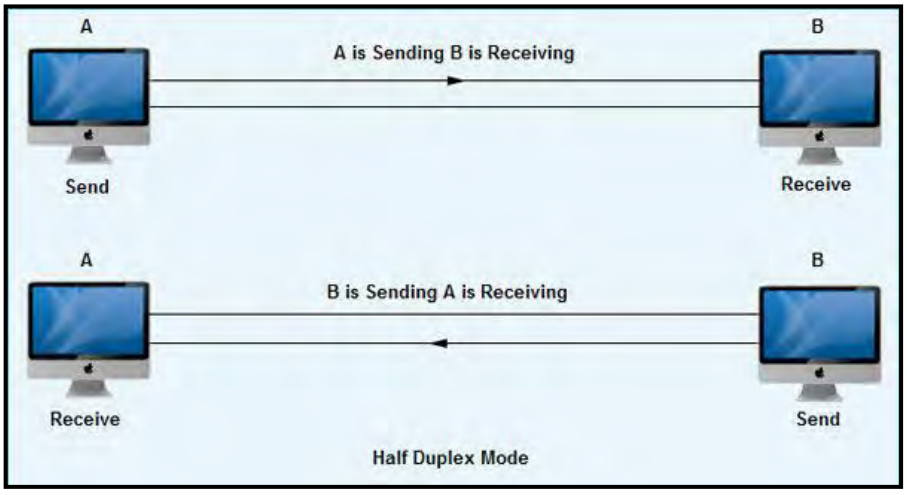
The Internet browsing is an example of half duplex mode. The user sends a request to a Web server for a web page. It means that information flows from user's computer to the web server. Web server receives the request and sends data of the requested page. The data flows to the Web server to the user's computer. At a time a user can a request or receive the data of web page.



A representation of sender and receiver data transmission in a half-duplex mode

A half-duplex system can transmit data in both directions, but only in one direction at a time which means half duplex modes support two-way traffic but in only one direction at a time. The interactive transmission of data within a time sharing system may be best suited to half-duplex lines. Both the connected devices can transmit and receive but not simultaneously. When one device is sending the other can only receive and vice-versa. Data is transmitted in one direction at a time, for example: a walkie-talkie.

This is generally used for relatively low-speed transmission, usually involving two-wire, analog circuits. Due to switching of communication direction, data transmission in this mode requires more time and processes than under full duplex mode. Examples of half duplex application include line printers, polling of buffers, and modem communications (many modems can also support full duplex).



A representation of how a half-duplex mode transmission works

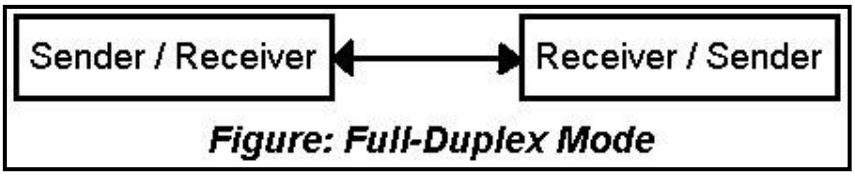
An example of half-duplex mode is a walkie-talkie. It can only send or receive a transmission at any given time. It cannot do both at the same time.

As shown in the figure, computer A sends information to computer B. At the end of transmission, computer B sends information to computer A. Computer A cannot send any information to computer B, while computer B is transmitting data.

3. **Full-Duplex Mode**

In full duplex-mode, data can flow in both directions at the same time. In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data.

Example of Full Duplex is a telephone network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time. It is the fastest directional mode of data communication. The telephone communication system is an example of full-duplex communication mode. Two persons can talk at the same time. Another example of fully-duplex mode in daily life is automobile traffic on a two-lane road. The traffic can move in both directions at the same time.



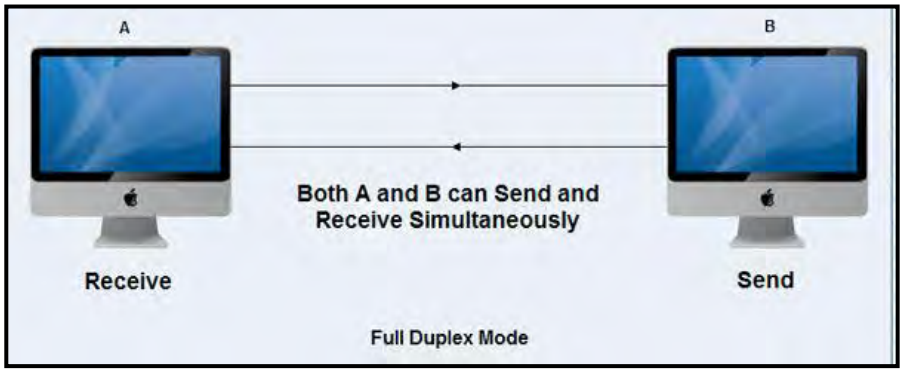
A representation of sender and receiver data transmission in a full-duplex mode

A full duplex system can transmit data simultaneously in both directions on transmission path. Full-duplex method is used to transmit the data over a serial communication link. Two wires needed to send data over a serial communication link layer. In full-duplex transmission, the channel capacity is shared by both communicating devices at all times.

Both the connected devices can transmit and receive at the same time. Therefore it represents truly bi-directional system. The link may contain two separate transmission paths one for sending and another for receiving.

Example of Full duplex mode:

Telephone networks operate in full duplex mode when two persons talk on telephone line; both can listen and speak simultaneously.



A representation of how a full-duplex mode transmission works

After studying the different transmission modes, it is worthy to look into the types of data transmission. There are two types of data transmission; these are the parallel transmission and the serial transmission. Topic 3 Lesson 17 of Grade 9 Design and Technology-Computing gave an introductory and basic discussion on this topic.

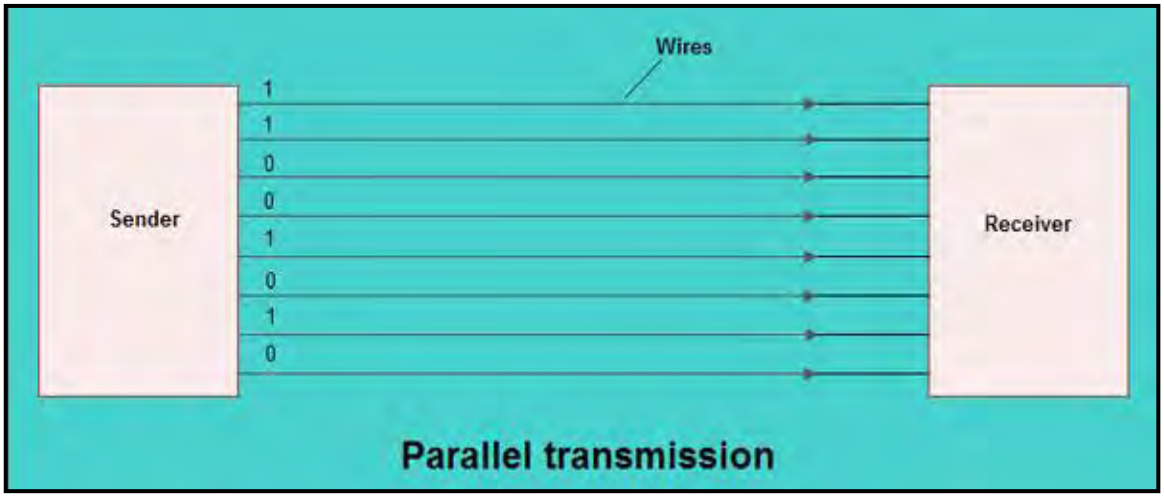
Now, let us discuss further.

1. **Parallel transmission**

Within a computing or communication device, the distances between different subunits are too short. Thus, it is normal practice to transfer data between subunits using a separate wire to carry each bit of data. There are multiple wires connecting each sub-unit and data is exchanged using a parallel transfer mode. This mode of operation results in minimal delays in transferring each word.

Parallel transmission is characterised by the following:

- Transmission is faster.
- In parallel transmission, all the bits of data are transmitted simultaneously on separate communication lines.
- In order to transmit n bits, n wires or lines are used. Thus each bit has its own line.
- All n bits of one group are transmitted with each clock pulse from one device to another i.e. multiple bits are sent with each clock pulse.
- Parallel transmission is used for short distance communication.
- As shown in the figure below, eight separate wires are used to transmit 8 bit data from sender to receiver.



A representation of how parallel transmission works

The advantage of parallel transmission is that it is fast way of transmitting data as multiple bits is transmitted simultaneously with a single clock pulse. However, its disadvantage is that it is a costly method of data transmission as it requires lines to transmit bits at the same time.

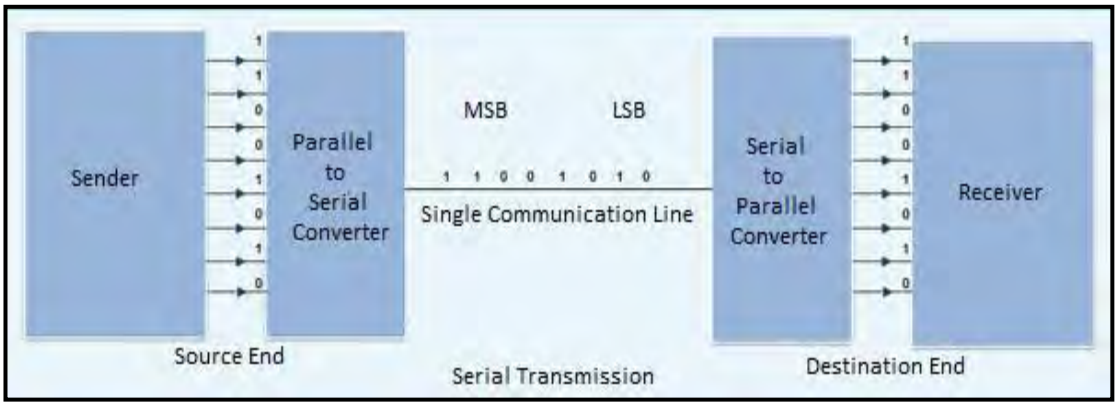
2. **Serial Transmission**

When transferring data between two physically separate devices, especially if the separation is more than a few kilometres, for reasons of cost, it is more economical

to use a single pair of lines. Data is transmitted as a single bit at a time using a fixed time interval for each bit. This mode of transmission is known as bit-serial transmission.

Serial Transmission is characterised by the following:

- In serial transmission, the various bits of data are transmitted serially one after the other.
- It requires only one communication line rather than n lines to transmit data from sender to receiver.
- Thus all the bits of data are transmitted on single line in serial fashion.
- In serial transmission, only single bit is sent with each clock pulse.
- As shown in the figure below, suppose an 8-bit data 11001010 is to be sent from source to destination. The Least Significant Bit (LSB) like 0 will be transmitted first followed by other bits. The Most Significant bit (MSB) like 1 will be transmitted in the end via single communication line.



A representation of how serial transmission works

- The internal circuitry of computer transmits data in parallel fashion. So in order to change this parallel data into serial data, conversion devices are used.
- These conversion devices convert the parallel data into serial data at the sender side so that it can be transmitted over single line.
- On the receiver side, serial data received is again converted to parallel form so that the interval circuitry of computer can accept it.
- Serial transmission is used for long distance communication.

The advantage of serial transmission is the use of single communication line reduces the transmission line cost by the factor of n as compared to parallel transmission.

However, the following are its disadvantages: the use of conversion devices at source and destination end may lead to increase in overall transmission cost and this method is slower as compared to parallel transmission as bits are transmitted serially one after the other.

Furthermore, there are two types of serial transmission. These are the synchronous and asynchronous. Both these transmissions use 'Bit synchronisation'. Bit Synchronisation is a function that is required to determine when the beginning and end of the data transmission occurs. Bit synchronisation helps the receiving computer to know when data begin and end during a transmission. Therefore, bit synchronisation provides timing control.

Let us discuss the two types of serial transmission.

A. Asynchronous transmission

Asynchronous transmission can be characterised by the following:

- Asynchronous transmission sends only one character at a time where a character is either a letter of the alphabet or number or control character i.e.; it sends one byte of data at a time.
- Bit synchronisation between two devices is made possible using start bit and stop bit.
- Start bit indicates the beginning of data i.e. alerts the receiver to the arrival of new group of bits. A start bit usually 0 is added to the beginning of each byte.
- Stop bit indicates the end of data i.e. to let the receiver know that byte is finished, one or more additional bits are appended to the end of the byte. These bits, usually 1s are called stop bits.

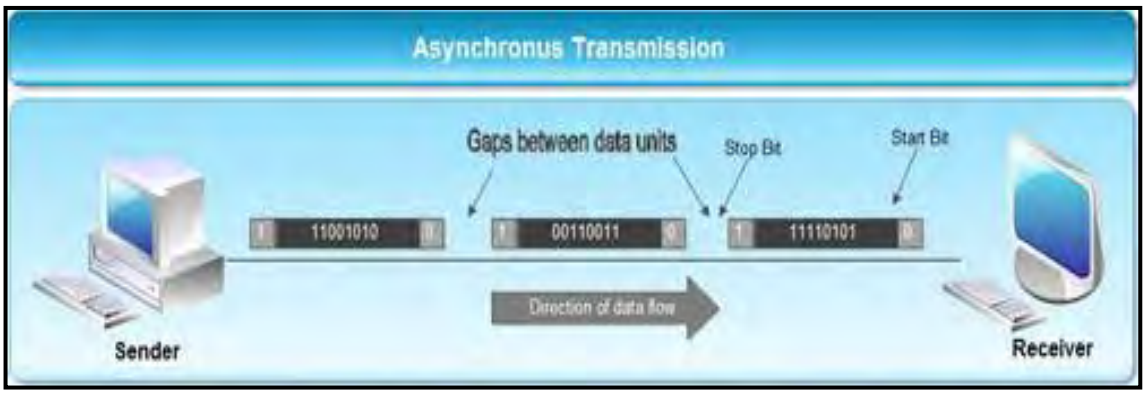
A representation of Start and stop bit

- Addition of start and stop increase the number of data bits. Hence more bandwidth is consumed in asynchronous transmission.
- There is idle time between the transmissions of different data bytes. This idle time is also known as Gap.

- The gap or idle time can be of varying intervals. This mechanism is called Asynchronous, because at byte level sender and receiver need not to be synchronised. But, within each byte, receiver must be synchronized with the incoming bit stream.

Asynchronous Transmission can be applied in the following situations:

- Asynchronous transmission is well suited for keyboard type-terminals and paper tape devices. The advantage of this method is that it does not require any local storage at the terminal or the computer as transmission takes place character by character.



A representation of sender and receiver data transmission in Asynchronous Transmission

- Asynchronous transmission is best suited to Internet traffic in which information is transmitted in short bursts. This type of transmission is used by modems.

The following are the advantages of Asynchronous transmission:

- This method of data transmission is cheaper in cost as compared to synchronous. For example, if lines are short, asynchronous transmission is better, because line cost would be low and idle time will not be expensive.

- In this approach each individual character is complete in itself; therefore if character is corrupted during transmission, its successor and predecessor character will not be affected.

- It is possible to transmit signals from sources having different bit rates.

- The transmission can start as soon as data byte to be transmitted becomes available.

- Moreover, this mode of data transmission is easy to implement.

However, the disadvantages of asynchronous transmission are as follows:

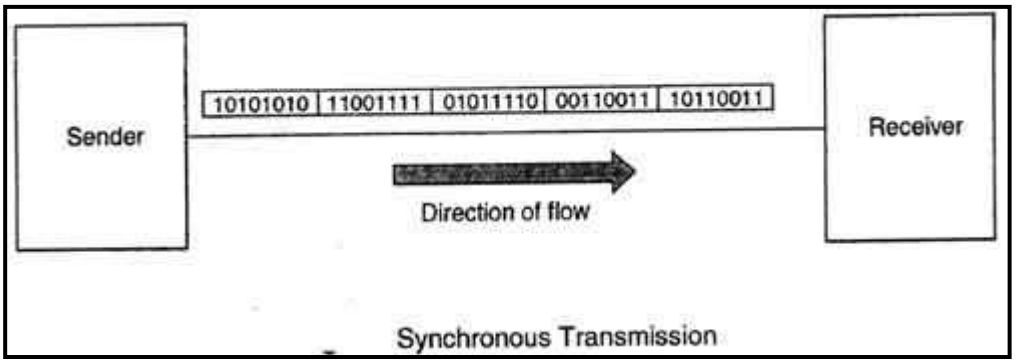
- This method is less efficient and slower than synchronous transmission due to the overhead of extra bits and insertion of gaps into bit stream.

- Successful transmission inevitably depends on the recognition of the start bits. These bits can be missed or corrupted.

B. Synchronous Transmission

Synchronous Transmission can be characterised by the following:

- Synchronous transmission does not use start and stop bits.
- In this method bit stream is combined into longer frames that may contain multiple bytes.
- There is no gap between the various bytes in the data stream.



A representation of how synchronous transmission works

- In the absence of start and stop bits, bit synchronisation is established between sender and receiver by 'timing' the transmission of each bit.
- Since the various bytes are placed on the link without any gap, it is the responsibility of the receiver to separate the bit stream into bytes so as to reconstruct the original information.
- In order to receive the data error free, the receiver and sender operates at the same clock frequency.

Synchronous transmission is used and applied for high speed communication between computers.

The advantage of Synchronous transmission is that this method is faster as compared to asynchronous as there are no extra bits (start bit & stop bit) and also there is no gap between the individual data bytes. However, its disadvantages are: firstly, it is costly as compared to asynchronous method. It requires local buffer storage at the two ends of line to assemble blocks and it also requires accurately synchronised clocks at both ends. This leads to increase in the cost and secondly, the sender and receiver have to operate at the same clock frequency. This requires proper synchronisation which makes the system complicated.

After discussing the two types of transmission, let us put our comparison in a table. Study the table on the below.

No.	Factor	Serial	Parallel
1.	Number of bits transmitted at one clock pulse	One bit	*n* bits
2.	No. of lines required to transmit *n* bits	One line	*n* lines
3.	Speed of data transfer	Slow	Fast
4.	Cost of transmission	Low as one line is required	Higher as *n* lines are required.
5.	Application	Long distance communication between two computers	Short distance communication. like computer to printer.

Comparison table for serial and parallel transmissions

Lastly, let us study the table below which summarises the comparison between the types of serial transmission.

No.	Factor	Asynchronous	Synchronus
1.	Data send at one time	Usually 1 byte	Multiple bytes
2.	Start and Stop bit	Used	Not used
3.	Gap between Data units	Present	Not present
4.	Data transmission speed	Slow	Fast
5.	Cost	Low	High

Comparison table for asynchronous and synchronous transmissions

Student Activity 12.1.2.3

Answer the following.

1. Describe data transmission mode.

_____

_____

_____

_____

_____

_____

_____

_____

_____

2. Fill in the missing information in the table below.

Data transmission mode	Description	Example
Simple		
Half-duplex		
Full-duplex		

3. Differentiate between the two kinds of transmission.

_____

_____

_____

_____

_____

4. What is the function and importance of data transmission modes?

_____

_____

_____

_____

_____

_____

_____

_____

12.1.2.4 Data Transmission Rates of Networking Systems

We have discussed that a network protocol is a set of rules that governs the communications between computers on a network while data transmission mode speaks of the direction of the flow of information or signal flow between two communication devices.

There must now be an understanding that the network is directed by a set of rules that govern how it communicates and signal flows from one direction to another differently.

With these, it is now worthy to take note that there are also varying speed rates of how these signals are transferred from communicating devices in a network. This difference in speed is called the Data Transfer Rate (DTR).

A data transfer rate (DTR) also known as throughput refers to the speed at which a device or network component can send and receive data. Data transfer is often measured in megabytes per second, although other measurements can also be used. It is the speed with which data can be transmitted from one device to another. Data rates are often measured in megabits (million bits) or megabytes (million bytes) per second. These are usually abbreviated as Mbps and MBps, respectively.

The data transfer rate is commonly used to measure how fast data is transferred from one location to another. For example, a hard drive may have a maximum data transfer rate of 480 Mbps, while your internet service provider (ISP) may offer an Internet connection with a maximum data transfer rate of only 1.5 Mbps.

Data rate as mentioned earlier is the number of bits transmitted per unit of time through the physical medium. From the table, the transmission system reflects how the signal is carried through by varying physical medium. These will be further discussed in wired and wireless transmission.

Now, let us look at some examples of data rates:

Transmission System	Data Rate	Comment
Telephone twisted pair	33.6kbps	4Khz telephone channel
Cable modem	500Kbps up to 4Mbps	CATV cable - shared
ADSL-Twisted pair	64-640Kbps out 1.536-6.144Mbps in	coexists with phone
Radio LAN in 2.4Ghz band	2Mbps	wireless LAN
Ethernet-twisted pair	10Mbps	Few hundred feet
Fast Ethernet-twisted pair	100Mbps	same
Optical fiber	2.4Gpbs-9.6Gpbs < 10Tbps	Using single wavelength Using multiple wavelengths DWDM = Dense Wavelength Division Multiplexing)

Notice that from the table, the data rate is faster as go down the table. Fiber optics seems to offer the fastest data rate. These physical media used to transfer signal will be discussed as we move along in our discussions.

DTR is important in assessing various devices and technologies. In general, the data transfer rate reflects changes and improvements in digital technologies, where newer systems like solid-state electronics have resulted in much higher data transfer rates within only a few decades.

Student Activity 12.1.2.4

Answer the following.

1. Differentiate between the following terms.

   a. Network protocol and data transmission mode

   _____

   _____

   _____

   b. Data transmission mode and data transmission rate

   _____

   _____

   _____

   _____

   c. Megabits and megabytes

   _____

   _____

   _____

   _____

2. What is the importance of data transmission rate?

   _____

   _____

   _____

   _____

12.1.2.5 Data Transmission- wire of Networking Systems

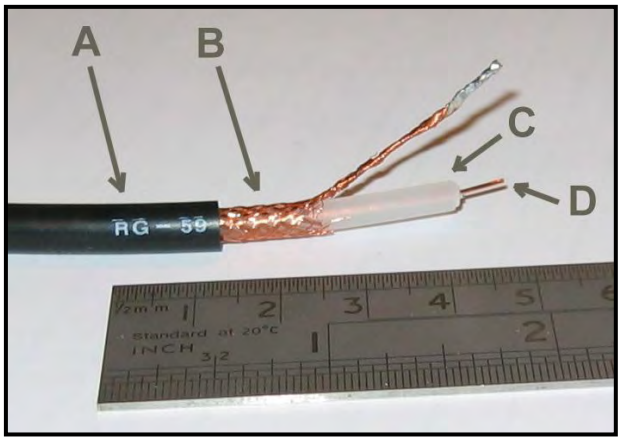
Wired communication is a type of LAN technology which is based on a special type of cable which is used to transfer data. The maximum data transfer rate of this technology is 10Mbps. The cables used to configure the network are special. Examples are Ethernet and wired LAN.

These are the commonly used cabling for wired technology:

1. **Coaxial cables**

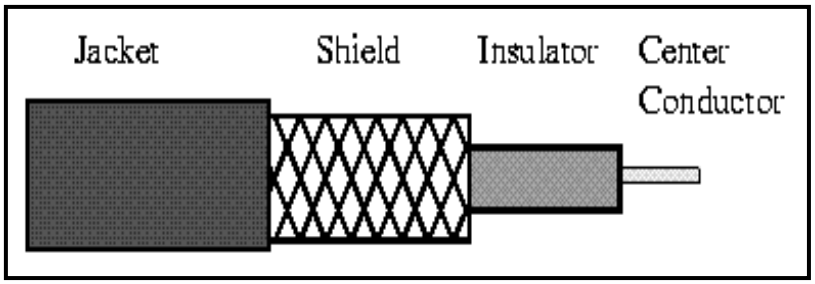
It is an armored cable with sheathed plastic that contains two concentric conductors or wires. It is used primarily for TV standard-definition connection. It is used to implement computer networks like Ethernet. It is also used to connect radio networks.

Coaxial Cable consists of 2 conductors. The inner conductor is held inside an insulator with the other conductor woven around it providing a shield. An insulating protective coating called a jacket covers the outer conductor.



A: Plastic outer insulation
B: Copper-clad aluminium braid shield conductor
C: Dielectric insulator
D: Central Conductor (copper-clad steel)

Coax Cable



The inner and outer shields of a coaxial cable

The outer shield protects the inner conductor from outside electrical signals. The distance between the outer conductor (shield) and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties or impedance. Typical impedances for coaxial cables are 75 ohms for Cable TV, 50 ohms for Ethernet Thinnet and Thicknet. The excellent control of the impedance

characteristics of the cable allow higher data rates to be transferred than Twisted Pair cable.

The use of coaxial cables has the following advantages:

- It has sufficient frequency to support multiple channels
- Each of the multiple channels offers substantial capacity
- Inner conductor is in a Faraday shield, therefore noise immunity is reduced

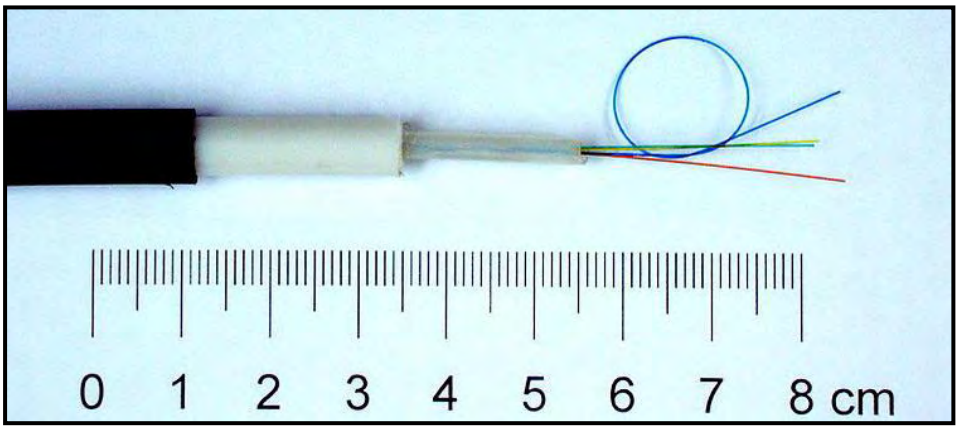
However, it has its disadvantages like:

- Signal leakage causing slower transmission
- Imperfect shield of coaxial cable can causes visible or audible interference
- External current sources like switched-mode power supplies create a voltage across the inductance
- Common mode current occurs when stray currents in the shield flow in the same direction as the current

2. **Fiber optic cables**

The fiber optical consists of several thin fibers of glass or plastic of 50 to 125 micrometers of diameter. They are used in fiber optic communications which permit transmission over longer distances and at higher bandwidths.

The wire is a 10–100 micrometre (µm) strand of glass, silicon, or plastic. Fiber optic signals are light pulses which are lasers or light-emitting diodes (LED) converted from electricity to light. The fiber transmits light, and then a photo diode light detector converts from light to electricity.



Fiber optic cable

The fibre optic cable has the following advantages:

- Fiber optic cables are not susceptible to Radio Frequency (RF) interference

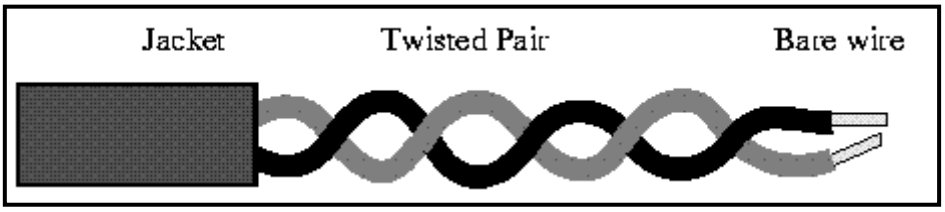
- Fiber optic cables can transmit data over exceptionally long distances with or without much data loss
- Wiretapping is more difficult compared to electrical connections.
- High data rates (Gbit/sec) over long distances (km) with low error rates.
- Hard to snoop signals, tapping difficult.
- Lighter and thinner than metallic wires; much greater cost/benefit ratio.
- Immune to electric interference or corrosion (rust).
- Less support electronics needed less frequently.

However, the fibre optic cabling has also its disadvantages, like:

- it can cost more than double what a typical broadband connection costs.
- its connections are not available in many areas.
- it is hard to tap and splice
- it is restricted optical end-to-end network topologies
- it is subject to physical trauma (kinking, crushing)
- it is a simplex channel
- it is a dual-core fiber

3. **Twisted pair cables**

Twisted pair cabling is a type of wiring in which two conductors (the forward and return conductors of a single) are twisted together to cancel electromagnetic interference. Unshielded twisted pairs (UTPs) are mainly used in Ethernet and telephone systems. They are also used for indoor applications. Twisted pair is the cheapest, oldest, most common wired media.

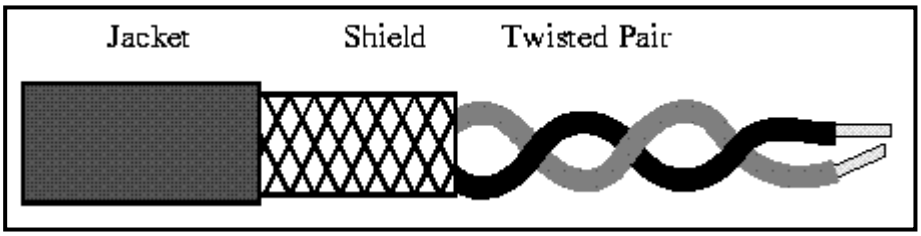


An illustration of the wires in a twisted pair cable

The wires in Twisted Pair cabling are twisted together in pairs. Each pair would consist of a wire used for the +ve data signal and a wire used for the -ve data signal. Any noise that appears on either of the wires would occur on the other wire. Since

the wires have opposite polarities, they are 180 degrees out of phase (180 degrees - phasor definition of opposite polarity). Therefore, when the noise appears on both wires, it cancels or nulls itself out at the receiving end.

The degree of reduction in noise interference is determined specifically by the number of turns per foot. Increasing the number of turns per foot reduces the noise interference. To further improve noise rejection, a foil or wire braid shield is woven around the twisted pairs. This "shield" can be woven around individual pair or around a multi-pair conductor (several pairs).



An illustration of shielded twisted pair cable

Cables with a shield are called Shielded Twisted Pair and commonly abbreviated STP. Cables without a shield are called Unshielded Twisted Pair or UTP. Twisting the wires together can result in characteristic impedance for the cable. Typical impedance for UTP is 100 ohm for Ethernet 10BaseT cable.

Unshielded Twisted Pair (UTP) cable is used on Ethernet 10BaseT and can also be used with Token Ring. It uses the RJ line of connectors (RJ45, RJ11, and others).

Shielded Twisted Pair (STP) is used with the traditional Token Ring cabling or ICS - IBM Cabling System. It requires a custom connector. IBM STP (Shielded Twisted Pair) has a characteristic impedance of 150 ohms.

The use of twisted pair has the following advantages:

- It is a thin, flexible cable that is easy to string between walls.
- More wires can be run through the same wiring ducts.
- UTP costs less per meter/foot than any other type of LAN cable.

However, it has the following disadvantages:

- UTPs susceptibility to electromagnetic interference greatly depends on the pair twisting schemes.
- In video applications that send information across multiple parallel signal wires, twisted pair cabling can introduce signalling delays known as skew which results in colour defects and ghosting.

When it comes to choosing a backbone to carry a facility's building-automation information, wired bus systems have become the norm. However, wireless systems have been growing in

popularity since the arrival of energy-autonomous and service-free wireless components. The next topic will focus more on wireless communication. Study the table below. It displays a comparison between the wired and wireless data transmission.

Feature	Wired	Wireless
Range	Better	Bad
Installation effort and flexibility	Worse	Better
Data volume	Better	Worse
Availability of information in room	Bad	Better
Reliability	Better	Good
Cost	Good	Better

Features of wired and wireless transmission of data

Going through and making an assessment of major criteria from the table above indicates that neither of the two transmission media (wired or wireless) comes out alone on top in a building-automation scenario. An optimal solution requires both; each implemented where it works better than the other.

In summary, wired media constrains transmission in certain directions where the transmission rates are inversely proportional to distance. This means that the error rates are proportional to distance. Though, highly efficient in signal transmission, fibre optic costs double compared to a typical broadband, hence the future approaches with cheaper optical electronics.

Student Activity 12.1.2.5

Answer the following.

1. Describe wired data transmission.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

2. Fill-up the table below.

Type of wired data transmission	Description	Describe one advantage	Describe one disadvantage
1. Coaxial cables			
2. Fibre optic cables			
3. Twisted pair cables			

3. Cite an importance of wired data transmission.

_____

_____

_____

_____

_____

_____

12.1.2.6 Data Transmission-wireless of Networking Systems

We have finished the discussion on wired communication which uses a special kind of cable for data transfer. Unlike, communications using wired transmission media such as twisted-pair, coaxial, fiber-optic cables, wireless media do not use solid substances to transmit data. Rather, wireless media send data through air or space using infrared, radio, or microwave signals. Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices which can communicate wirelessly. Wireless signals are spread in the air and are received and interpreted by appropriate antennas.

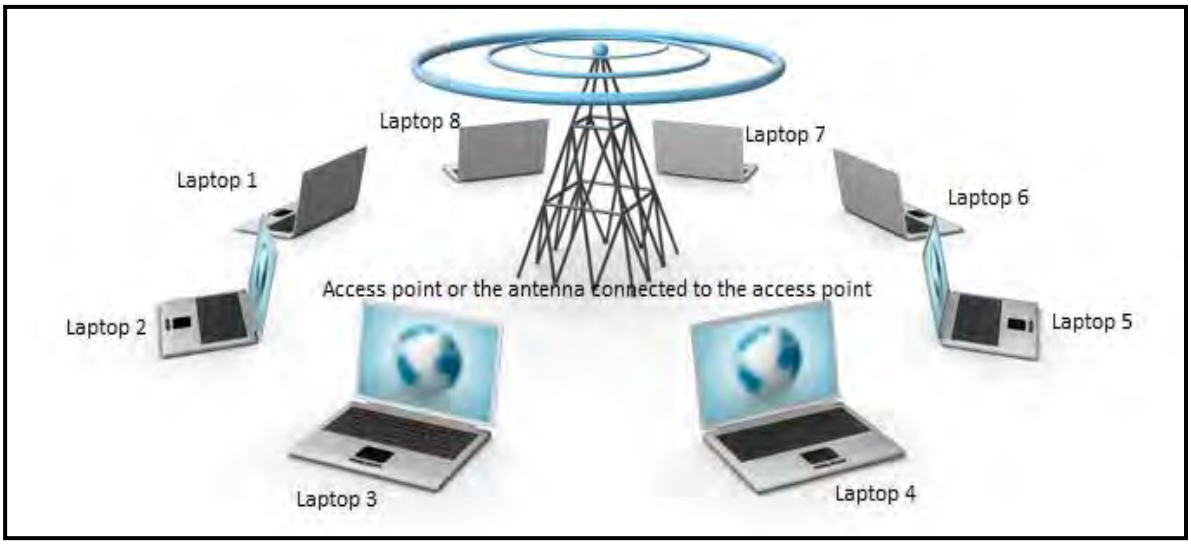
A representation of how devices are linked through wireless communication

Wireless communication uses radio frequencies (RF) or infrared (IR) waves to transmit data between devices on LAN. Key components are a wireless hub, or access point used for signal distribution. Wireless signals are electromagnetic waves that can travel through a vacuum of outer space.

Communication methods such as cell phones, the radio and the Internet all use technological advancements in wireless data transmission systems which carry invisible electromagnetic waves to transmit data over long distances within a short amount of time. There are multiple types of wireless data transmission systems which enable information signals to be quickly sent and received by other units.

Wireless networks (WLAN, Wi-Fi) gained popularity in many applications, especially in the areas of production and storage. Users in those segments of the market gain on performance, through the use of mobile terminals and computers. These devices allow a constant data transmission to the central processing systems. Construction of the wired network (LAN) is usually very difficult, sometimes even impossible for technical reasons. In those enterprises where technical capabilities do not allow for the construction of a cable network, Wi-Fi is the ideal solution.

Structure of wireless networks uses electromagnetic waves (radio frequency) from one point to another without cables. Access point, (or the antenna connected to the access point) is usually mounted high, but may also be installed anywhere to achieve required range.



A representation of how wireless network uses radio frequency

Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. It is commonly used in the telecommunications industry to refer to telecommunications systems (e.g. radio transmitters and receivers, remote controls etc.) which use some form of energy (e.g. radio waves, acoustic energy, etc.) to transfer information without the use of wires. Information is transferred in this manner over both short and long distances.

The most common wireless technologies use radio. With radio waves distances can be short, such as a few meters for television or as far as thousands or even millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking.

Somewhat less common methods of achieving wireless communications include the use of other electromagnetic wireless technologies, such as light, magnetic, or electric fields or the use of sound.

The biggest advantage of a wireless data transfer is that wireless operations permit services, such as long-range communications, that are impossible or impractical to implement with the use of wires.

The following are more common examples of wireless equipment include:

- Telemetry control and traffic control systems
- Infrared and ultrasonic remote control devices
- Professional Land Mobile Radio (LMR) and Specialised Mobile Radio (SMR) typically used by business, industrial and Public Safety entities.
- Consumer Two way radio including Family Radio Service (FRS), General Mobile Radio Service (GMRS) and Citizens band ("CB") radios.

- The Amateur Radio Service (Ham radio).
- Consumer and professional Marine VHF radios.
- Airband and radio navigation equipment used by aviators and air traffic control
- Cellular telephones and pagers: provide connectivity for portable and mobile applications, both personal and business. Cellular data service offers coverage within a range of 10-15 miles from the nearest cell site. Speeds have increased as technologies have evolved, from earlier technologies such as GSM, CDMA and GPRS, to 3G networks
- Global Positioning System (GPS): allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.
- Cordless computer peripherals: the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless using technology such as Wireless USB or Bluetooth
- Cordless telephone sets: these are limited-range devices, not to be confused with cell phones.
- Satellite television: Is broadcast from satellites in geostationary orbit. Typical services use direct broadcast satellite to provide multiple television channels to viewers.
- Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in large rural areas or remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use.
- Wireless Sensor Networks are responsible for sensing noise, interference, and activity in data collection networks. This allows us to detect relevant quantities, monitor and collect data, formulate meaningful user displays, and to perform decision-making functions.
- Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet.
- New technologies such as Mobile Body Area networks (MBAN) the capability to monitor blood pressure, heart rate, and oxygen level and body temperature, all with wireless technologies. The MBAN works by sending low powered wireless signals to receivers that feed into nursing stations or monitoring sites. This technology helps with the intentional and unintentional risk of infection or disconnection that arise from wired connections

Wireless networking is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice

to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

These are the different wireless data transmission methods that exist.

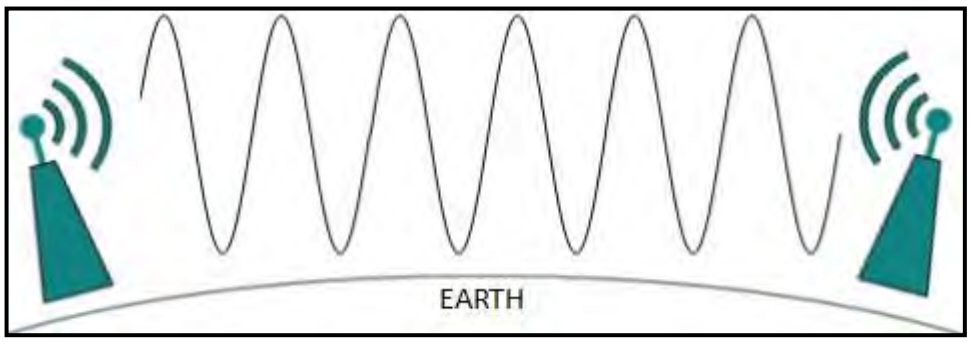
1. **Radio**

A radio is a wireless media that transfers data by carrying electromagnetic waves with low frequencies to distant locations through an electrical conductor and an antenna. Sometimes, the electromagnetic waves experience interference from large obstructions such as mountains or by the receiving location being too far from the radio signal, thus inhibiting the frequency in these circumstances.

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and similar structures. Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency).

Radio waves at lower frequencies can travel through walls whereas higher RF travels in straight line and bounces back. The power of low frequency waves decreases sharply as it covers longer distance. High frequency radio waves have more power.

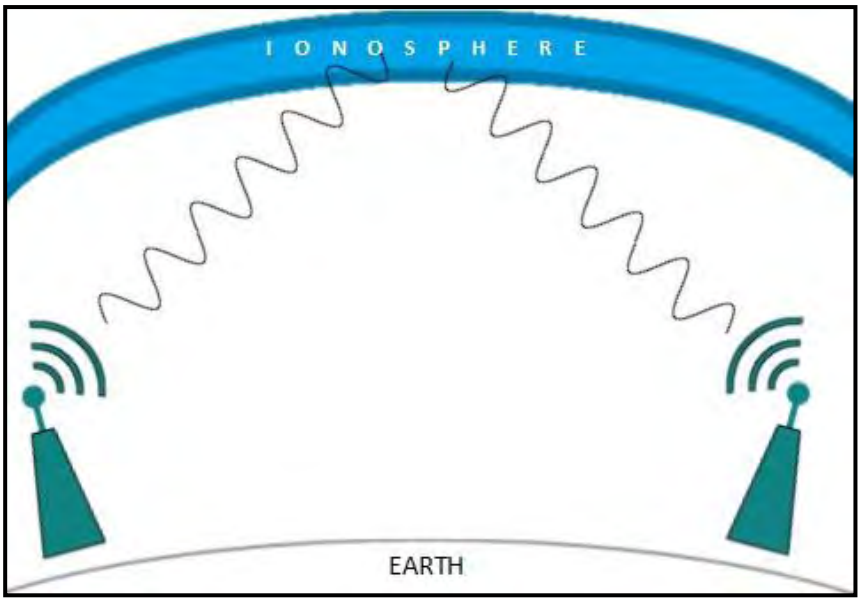
Lower frequencies like (VLF, LF, MF bands) can travel on the ground up to 1000 kilometers, over the earth's surface.



A representation of radio wave frequency travelling on the ground

Radio waves on high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves

such as HF and VHF bands are spread upwards. When it reaches Ionosphere it is refracted back to the earth.



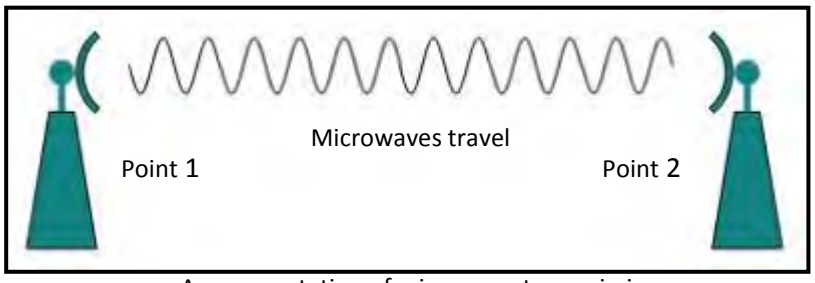
A representation of a radio wave on the Ionosphere

2. **Microwave**

An effective type of wireless data transmission is the microwave, which enables information to travel using two separate methods. One method is the terrestrial method, which uses two microwave towers with a clear line of sight between them and thus no obstacles to disrupt that line of sight. Often used to ensure privacy, the frequency of data transmission for terrestrial systems is typically 4 GHz to 6 GHz or 21 GHz to 23 GHz and the speed is usually 1 megabit per second (Mbps) to 10 Mbps. Another method used to transmit data through the wireless media of a microwave is the satellite method, which transmits information via a satellite that orbits 22,300 miles above the Earth. Stations on the ground send and receive data signals to and from the satellite with a frequency ranging from 11 GHz to 14 GHz and with a transmission speed of 1 Mbps to 10 Mbps.

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.



A representation of microwave transmission

Microwave antennas focus the waves making a beam of it. As shown in the picture above, multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles.

Microwaves transmission depends highly upon the weather conditions and the frequency it is using.

Worldwide Interoperability for Microwave Access is a telecommunications protocol that provides fixed and mobile internet access. It is a standard based technology enabling the delivery of last mile wireless broadband access.

The following are the uses of microwave access:

- It provides portable mobile broadband connectivity across cities and countries.
- It provides a wireless alternative to cable and DSL for last mile broadband access.
- It provides data, telecommunication (VoIP) and IPTV services.
- It provides source internet connectivity as part of a business continuity plan.

The following are its advantages:

- A single station can serve hundreds of users.
- Much faster deployment of new users compared to wired networks.
- Speed of 10Mbps at 10kilometers within line- of-site.
- It is standardised, and the same frequency equipment should work together.

3. **Infrared**

Infrared (IR) is a media transmission system that transmits data signals through light emitting diodes (LEDs, or lasers). However, in an infrared system, the information cannot travel through obstacles and can be inhibited by light. One type of infrared is the point to point system, which entails a transmission between two points limited to a line of sight range. This method is conducive to privacy and preventing eavesdropping. The transmission signal frequency of a point to point system is 100 GHz to 1,000 terahertz (THz) and the speed ranges from 100 Kbps to 16 Mbps. Another type of infrared includes the broadcast system in which a reflective material or a transmission unit amplifies and retransmits a data signal to disperse the signal so several other units may also receive the given signal. With a limited speed of 1 Mbps, the usual frequency of an infrared broadcast system is 100 GHz to 1,000 THz. Infrared waves lay in between visible light spectrum and microwaves. It has wavelength of 700 nm to 1 mm and frequency ranges from 300 GHz to 430 THz.

Infrared waves are used for very short range communication purposes such as television and it is remote. Infrared travels in a straight line so they are directional by nature. Because of high frequency range, Infrared do not cross wall like obstacles.

Infrared Light is electromagnetic radiation with a wavelength between 0.7 and 300 micrometers, which equates to a frequency range between approximately 1 and 430THz. IR wavelengths are longer than that visible light, but shorter than that of terahertz radiation microwaves.

The following are the uses of IR:

- It is employed in short range communication among computer peripherals and personal digital assistants (PDAs).
- It is used for remote controls to command appliances.

IR has the following advantages:

- Low power requirements: therefore ideal for laptops, PDAs and cellphones.
- Low circuitry cost.
- Installation is easy because no proprietary hardware is needed.
- Higher security
- High noise immunity

However, it has the following disadvantages:

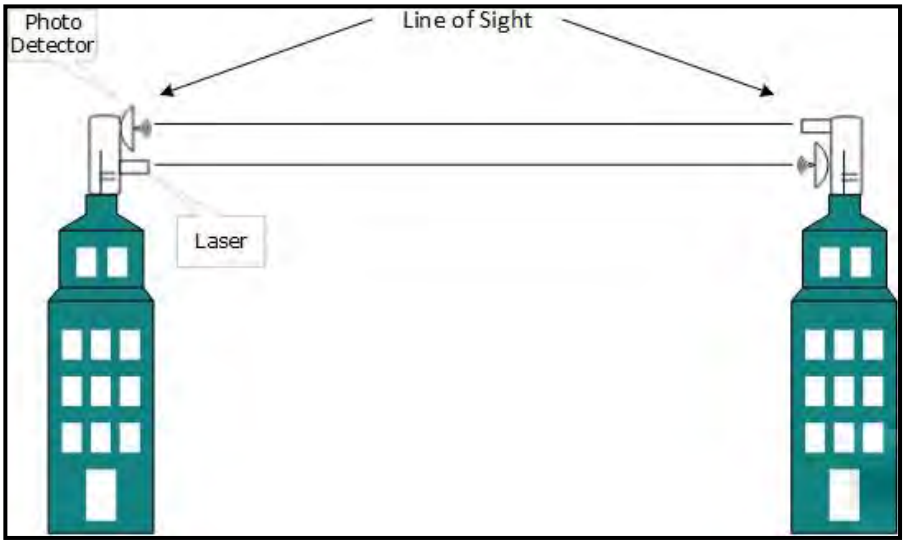
- Performance drops over longer distances.
- It is weather sensitive: data transmission is poor in direct sunlight, rain, fog, dust, and others.
- Data rate transmission is lower than typical wired transmission.
- Data transmission is possible in the line of sight: transmitters and receivers should be aligned.

4. **Light Transmission**

The highest and the most electromagnetic spectrum which can be used for data transmission is light or optical signalling. This is achieved by means of laser.

Because of frequency light uses, it tends to travel strictly in straight line. So the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication laser, photo-detector needs to be

installed. Laser beam is generally 1mm wide so it is a work of precision to align two receptors each pointing to the laser's source.



A representation of light transmission

Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

Lasers cannot penetrate obstacles like walls, rain and thick fog. Additionally, laser beam is distorted by wind and atmospheric temperature or variation in temperature in the path. Lasers are safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.

Wired technology is more secure, reliable, and cheaper and has higher data transmission rates over wireless technology, but one huge advantage that has made wireless technology popular is mobility.

Student Activity 12.1.2.6

Answer the following.

1. Contrast wired with wireless data transfer.

_____

_____

_____

_____

2. Explain how wireless transmission enables devices to "communicate".

_____

_____

_____

_____

_____

3. Give three applications of wireless technology and give its importance.

a. _____

_____

_____

b. _____

_____

c. _____

_____

_____

Summative Activity 12.1.2

Answer the following.

1. Choose from the pool of words below the correct term that matches each of the given description. Write the letter of the correct answer.

   A. Wireless data transmission

   B. Wired data transmission

   C. Transmission rate

   D. Transmission mode

   E. Protocol

   F. Packets

   G. Nodes

   H. Network

   I. Computer network

_____ 1. It is a communication involving no physical link established between two or more devices.

_____ 2. It is a set of rules that governs the communications between computers on a network.

_____3. It is direction of the flow of information or signal flow between two communication devices.

_____ 4. It is a communication between two or more devices.

_____ 5. It is based on a special type of cable which is used to transfer data.

_____ 6. It is a telecommunications network that allows computers to exchange data.

_____ 7. It consists of two kinds of data: control information and user data where the control information provides data the network needs to deliver the user data.

_____ 8. It is the speed at which a device or network component can send and receive data.

_____9. It includes hosts such as personal computers, phones, servers as well as networking hardware.

2. From the list of words given, match with the areas which they relate to. Write the letter of the correct answer.

A. Wired transmission

B. Wireless transmission

C. Transmission mode

D. Network

E. Protocol

_____ 1. Ethernet

_____ 2. Light transmission

_____ 3. Simplex

_____ 4. Coaxial cable

_____ 5. Infrared transmission

_____ 6. Token ring

_____ 7. Half-duplex

_____ 8. Radio transmission

_____ 9. Fast Ethernet

_____ 10. Twisted pair cables

_____ 11. Microwave transmission

_____ 12. Local talk

_____ 13. Full duplex

_____ 14. Fiber optic cable

_____ 15. Asynchronous transfer mode

3. Differentiate between the following pair of words.

a. Simplex and Half-duplex

_____

_____

_____

_____

b. Half-duplex and Full duplex

_____

_____

_____

_____

_____

c. Ethernet and Fast Ethernet

_____

_____

_____

d. Coaxial cable and Fiber optic cable

_____

_____

_____

e. Parallel transmission and Serial transmission

_____

_____

_____

_____

f. Synchronous transmission and Asynchronous transmission

_____

_____

_____

g. Radio transmission and Microwave transmission

_____

_____

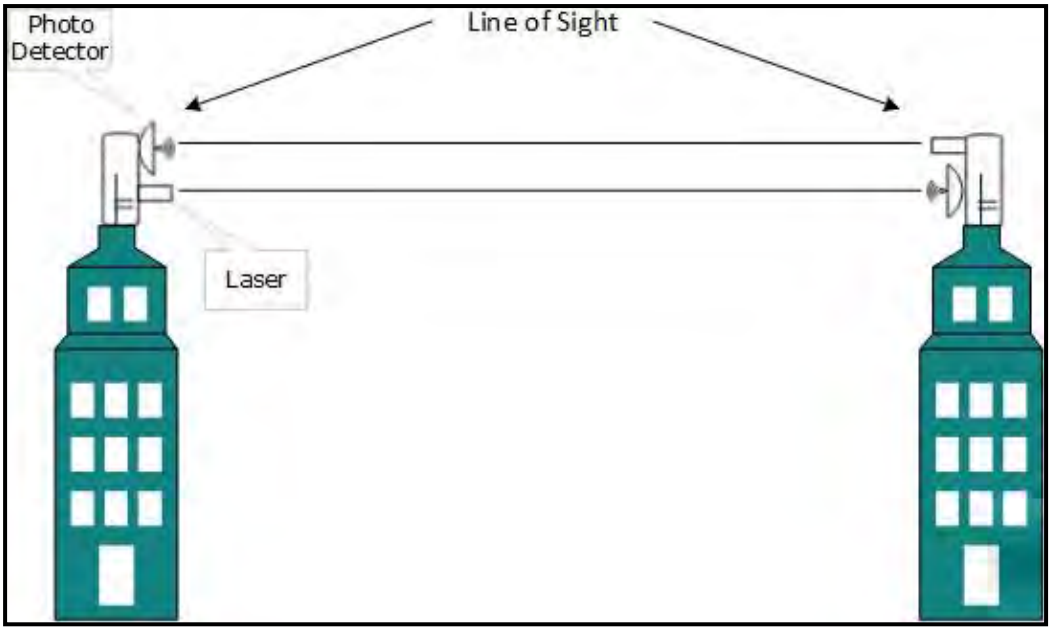
_____

_____

_____

4. Explain or describe the following diagrams.

a.



_____

_____

_____

_____

_____

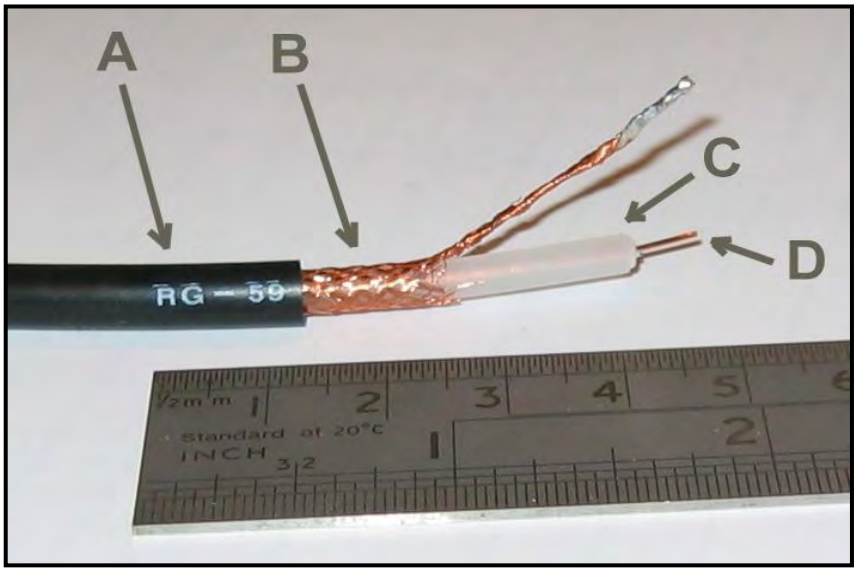
b.

_____

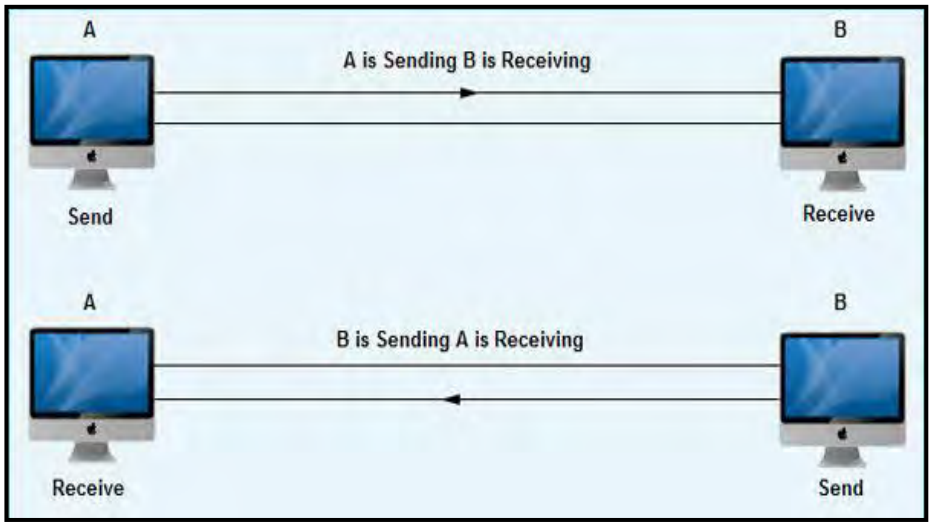
_____

_____

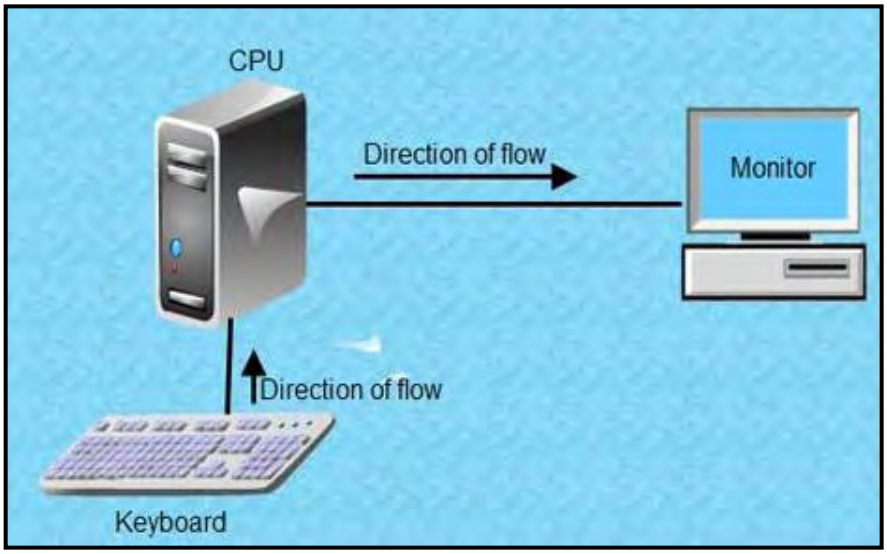
c.


A
B
C
D
RG – 59
Standard at 20°C
INCH

d.


A
B
A is Sending B is Receiving
Send
Receive
A
B
B is Sending A is Receiving
Receive
Send

e.



Answers to Student Activity 12.1.2

Student Activity 12.1.2.1

Answers can be similar to these ones below.

1. Networking system consists of a computer network or data network. A computer network or data network is a telecommunications network that allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections.

2. Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.

   The many benefits that networking offers to us are:

   a. Helps to enhance connectivity.

   b. Networking helps in sharing of hardware:

   c. Eases out management of data.

   d. Internet

   e. Data Sharing

   f. Networking has promoted gaming.

3. Any three of the following can be the answer.

   a. Threat: Viruses and Worms

      Solution: Install a security suite that protects the computer against threats such as viruses and worms.

   b. Threat: Trojan Horses

      Solution: Security suites, such as Norton Internet Security, will prevent you from downloading Trojan Horses.

   c. Threat: SPAM

      Solution: SPAM filters are an effective way to stop SPAM. These filters come with most of the e-mail providers online. Also you can buy a variety of SPAM filters that work effectively.

   d. Threat: Phishing

Solution: Similar to SPAM use Phishing filters to filter out this unwanted mail and to prevent threat.

e. Threat: Packet Sniffers

Solution: “When strong encryption is used, all packets are unreadable to any but the destination address, making packet sniffers useless.” A solution then is to obtain strong encryption.

f. Threat: Maliciously Coded Websites

Solution: Using a security suite, such as AVG, can detect infected sites and try to prevent the user from entering the site.

g. Threat: Password Attacks

Solution: At present there is no software that prevents password attacks.

h. Threat: Hardware Loss and Residual Data Fragments

Solution: Keep data and hardware under strict surveillance.

i. Threat: Shared Computers

Solutions: Do not check the “Remember my ID on this computer” box ; Never leave a computer unattended while signed-in ; Always sign out completely ; Clear the browsers cache ; Avoid confidential transactions ; Be wary of spyware ; Never save passwords ; Change your password often

j. Threat: Zombie Computers and Botnets

Solution: Antivirus software can help prevent zombie computers.

k. Threat: A botnet

Solution: Network Intrusion Prevention (NIP) systems can help prevent botnets.

Student Activity 12.1.2.2

Answers can be similar to these ones below.

1. What is a protocol?

Network Protocol is a set of rules that governs the communications between computers on a network.

2. What is the importance of a network protocol?

Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication.

3. Any three of the following can be the answers.

Ethernet protocol is by far the most widely used one. 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 nodes have already transmitted on the cable, the computer will wait and try again when the line is clear.

The Token Ring protocol uses the access method which involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer.

Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring.

Gigabit Ethernet is primarily used for backbones on a network at this time. In the future, it will probably also be used for workstation and server connections.

Local Talk uses the method CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. Local Talk adapters and special twisted pair cable can be used to connect a series of computers through the serial port.

Student Activity 12.1.2.3

The answers can be similar to these ones below.

1. The way in which data is transmitted from one place to another. Transmission mode defines the direction of the flow of information between two

communication devices. That is, it tells the direction of signal flow between the two devices.

2.

Data transmission mode	Description	Example
Simple	In simplex mode, data can flow in only one direction. In this type of transmission mode data can be sent only through one direction that is, communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems.	• Radio and T.V transmissions • A communication between a computer and a keyboard • Loudspeaker system
Half-duplex	In half-duplex mode, data can flow in both directions but only in one direction at a time. We can send data in both directions but it is done one at a time that is when the sender is sending the data then at that time we cannot send the sender our message. The data is sent in one direction. In this mode, data is sent and received alternatively.	• The Internet browsing • Walkie-talkie
Full-duplex	In full duplex-mode, data can flow in both directions at the same time. In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data.	Telephone network

3. Parallel transmission involves multiple wires connecting each sub-unit and data is exchanged using a parallel transfer mode and within a computing or communication device, the distances between different subunits are too short. Thus, it is normal practice to transfer data between subunits using a separate wire to carry each bit of data while serial transmission is used when transferring data between two physically separate devices, especially if the separation is more than a few kilometres, for reasons of cost, it is more economical to use a single pair of lines.

4. Data transmission modes identifies how data is transmitted from one place to another It indicates the direction of flow of information. Transmission mode defines

the direction of the flow of information between two communication devices. That is, it tells the direction of signal flow between the two devices.

Student Activity 12.1.2.4

Answers may be similar to these ones below.

1. Differentiate the following terms.

    a. Network protocol is a set of rules that governs the communications between computers on a network while data transmission mode speaks of the direction of the flow of information or signal flow between two communication devices. Data transmission mode and data transmission rate

    b. Megabits and megabytes

    Megabits (million bits) or megabytes (million bytes) per second

2. What is the importance of data transmission rate?

    The data transfer rate is commonly used to measure how fast data is transferred from one location to another. DTR is important in assessing various devices and technologies. In general, the data transfer rate reflects changes and improvements in digital technologies, where newer systems like solid-state electronics have resulted in much higher data transfer rates within only a few decades

---

Student Activity 12.1.2.5

Answers may be similar to these ones below.

1. Wired communication is a type of LAN technology which is based on a special type of cable which is used to transfer data. The maximum data transfer rate of this technology is 10Mbps. The cables used to configure the network are special. Examples are Ethernet and wired LAN.

2.

Type of wired data transmission	Description	Describe one advantage	Describe one disadvantage
1. Coaxial cables	It is an armored cable with sheathed plastic	It has sufficient frequency to support multiple channels	Signal leakage causing slower transmission Imperfect shield of

	that contains two concentric conductors or wires.	which means that multiple channels are possible. Each of the multiple channels offers substantial capacity which means that signal is good. Inner conductor is in a Faraday shield, therefore noise immunity is reduced which means that less interference.	coaxial cable can causes visible or audible interference External current sources like switched-mode power supplies create a voltage across the inductance Common mode current occurs when stray currents in the shield flow in the same direction as the current
2. Fibre optic cables	The fiber optical consists of several thin fibers of glass or plastic of 50 to 125 micrometers of diameter. They are used in fiber optic communications which permit transmission over longer distances and at higher bandwidths.	Fiber optic cables are not susceptible to RF (Radio Frequency) interference Fiber optic cables can transmit data over exceptionally long distances with much data loss Wiretapping is more difficult compared to electrical connections. High data rates (Gbit/sec) over long distances (km) with low error rates. Hard to snoop signals, tapping difficult. Lighter and thinner than metallic wires; much greater cost/benefit ratio. Immune to electric interference or corrosion (rust). Less support electronics needed less frequently.	Fiber optic cabling can cost more than double what a typical broadband connection costs. Fiber optic connections are not available in many areas. Hard to tap and splice Restricted optical end-to-end network topologies Subject to physical trauma (kinking, crushing) Simplex channel Dual-core fiber
3. Twisted pair cables	Twisted pair cabling is a type of wiring in which two conductors	It is thin, flexible cable that is easy to string between walls.	UTPs susceptibility to electromagnetic interference greatly depends on the pair

	(the forward and return conductors of a single) are twisted together to cancel electromagnetic interference.	More wires can be run through the same wiring ducts. UTP costs less per meter/foot than any other type of LAN cable.	twisting schemes. In video applications that send information across multiple parallel signal wires, twisted pair cabling can introduce signalling delays known as skew which results in colour defects and ghosting.

3. Wired media constrains transmission in certain directions where the transmission rates are inversely proportional to distance. This means that the error rates are proportional to distance. Though highly efficient in signal transmission, fibre optic costs double than a typical broadband cost, hence the future approaches with cheaper optical electronics.

Student Activity 12.1.2.6

Answers may be similar to these ones below.

1. Wired technology is more secure, reliable, and cheaper and has higher data transmission rates over wireless technology but one huge advantage that has made wireless technology popular is mobility.

2. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas. In wireless data transmission systems which carry invisible electromagnetic waves to transmit data over long distances within a short amount of time.

3. Any three of the following can be the answers.

   a. The use of radio communication. This involves radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking.

   b. Global Positioning System (GPS): allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.

   c. Wireless Sensor Networks are responsible for sensing noise, interference, and activity in data collection networks. This allows us to detect relevant quantities,

monitor and collect data, formulate meaningful user displays, and to perform decision-making functions.

d. Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in largely rural areas or remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use.

e. Satellite television: Is broadcast from satellites in geostationary orbit. Typical services use direct broadcast satellite to provide multiple television channels to viewers.

f. Cordless computer peripherals: the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless using technology such as Wireless USB or Bluetooth

g. Cordless telephone sets: these are limited-range devices, not to be confused with cell phones.

h. Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet.

Answers to Summative Activity 12.1.2

1.

1.	A	4.	H	7.	F
2.	E	5.	B	8.	C
3.	D	6.	I	9.	G

2.

1.	E	6.	E	11.	B
2.	B	7.	C	12.	E
3.	C	8.	B	13.	C
4.	A	9.	E	14.	A
5.	B	10.	A	15.	C

3. Contrast the following pair of words.

a. Simplex and Half-duplex
In simplex mode, data can flow in only one direction. In this type of transmission mode data can be sent only through one direction that is,

communication is unidirectional while in half-duplex mode, data can flow in both directions but only in one direction at a time.

b. Half-duplex and Full duplex
In half duplex data is sent in both directions but it is done one at a time that is when the sender is sending the data then at that time we cannot send the sender our message. The data is sent in one direction while in full duplex-mode, data can flow in both directions at the same time. In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data.

c. Ethernet and fast Ethernet
The Ethernet protocol is by far the most widely used one. 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. While fast Ethernet allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps.

d. Coaxial cable and Fiber optic cable
It is an armored cable with sheathed plastic that contains two concentric conductors or wires while the fiber optical consists of several thin fibers of glass or plastic of 50 to 125 micrometers of diameter. They are used in fiber optic communications which permit transmission over longer distances and at higher bandwidths.

e. Parallel transmission and Serial transmission
In parallel transmission, there are multiple wires connecting each sub-unit and data where all the bits of data are transmitted simultaneously on separate communication lines while in serial transmission data is transmitted as a single bit at a time using a fixed time interval for each bit.

f. Synchronous transmission and Asynchronous transmission
Synchronous transmission is used and applied for high speed communication between computers while Asynchronous transmission is well suited for keyboard type-terminals and paper tape devices.

g. Radio transmission and Microwave transmission
A radio is a wireless media that transfers data by carrying electromagnetic waves with low frequencies to distant locations through an electrical conductor and an antenna while microwave transmission enables information to travel using two separate methods which consists of either the terrestrial method or the satellite method.

4. Explain or describe the following diagrams.

a. Light transmission tends to travel strictly in straight line. So the sender and receiver must be in the line-of-sight. Because laser transmission is

unidirectional, at both ends of communication laser and photo-detectors needs to be installed. Laser beam is generally 1mm wide so it is a work of precision to align two far receptors each pointing to lasers source.

b. Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. It is commonly used in the telecommunications industry to refer to telecommunications systems (e.g. radio transmitters and receivers, remote controls etc.) which use some form of energy (e.g. radio waves, acoustic energy, etc.) to transfer information without the use of wires. Information is transferred in this manner over both short and long distances.

c. The coax cable has the following parts: A: plastic outer insulation; B: copper-clad aluminum braid shield conductor; C: dielectric and D: central conductor (copper-clad steel). The outer shield protects the inner conductor from outside electrical signals. The distance between the outer conductor (shield) and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties or impedance.

d. A half-duplex system can transmit data in both directions, but only in one direction at a time that mean half duplex modes support two-way traffic but in only one direction at a time. Computer A sends information to computer B. At the end of transmission, computer B sends information to computer A. Computer A cannot send any information to computer B, while computer B is transmitting data.

e. In simplex mode, data can flow in only one direction. In this type of transmission mode data can be sent only through one direction that is, communication is unidirectional. We cannot send a message back to the sender.

12.1.3 Network Basics

12.1.3.1 Types of Networks

There are several different types of computer networks. Computer networks can be characterised by their size as well as their purpose. One way to categorise the different types of computer network designs is by their scope, scale or geographical spread.

The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

Some of the different networks based on size are:

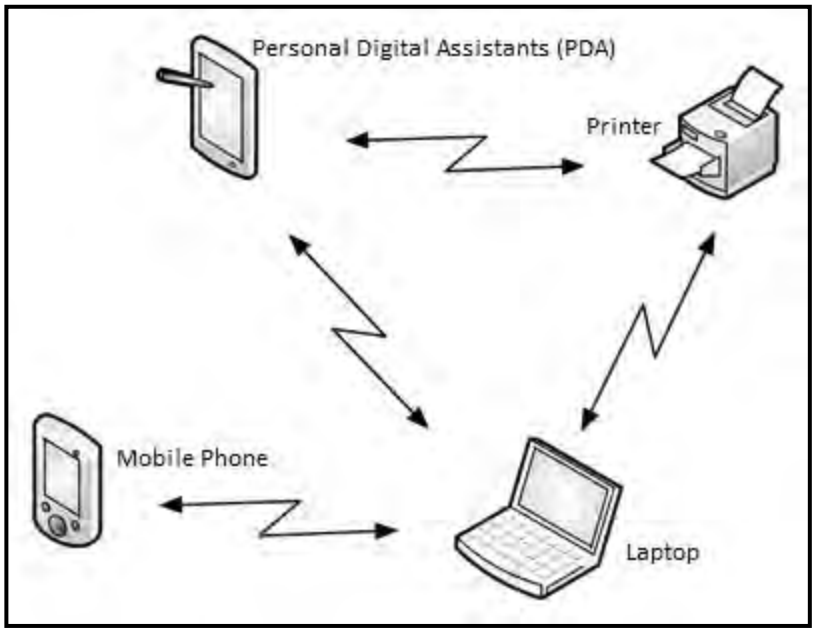
- Personal area network (PAN)
- Local area network (LAN)
- Metropolitan area network (MAN)
- Wide area network (WAN)

In terms of purpose, many networks can be considered general purpose, which means they are used for everything from sending files to a printer to accessing the Internet. Some types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:

- Storage area network (SAN)
- Enterprise private network (EPN)
- Virtual private network (VPN)

Let us study each of these in a bit more detail.

1. **Personal Area Network**
   A Personal Area Network (PAN) is a computer network organised around an individual person within a single building. PAN is also known as Bluetooth. It is a wireless networking technology designed for very short-range connections (typically just a few meters). The idea of Bluetooth is to get rid of the need for all of those cables (e.g. Universal Serial Bus (USB) cables) that connect our computer to peripheral devices such as printers, mice, keyboards and others.



A representation of a personal area network

Bluetooth devices contain small, low-power radio transmitters and receivers. When devices are in range of other Bluetooth devices, they detect each other and can be 'paired' (connected). This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles and other personal entertainment devices.

The following are the typical uses of Bluetooth:

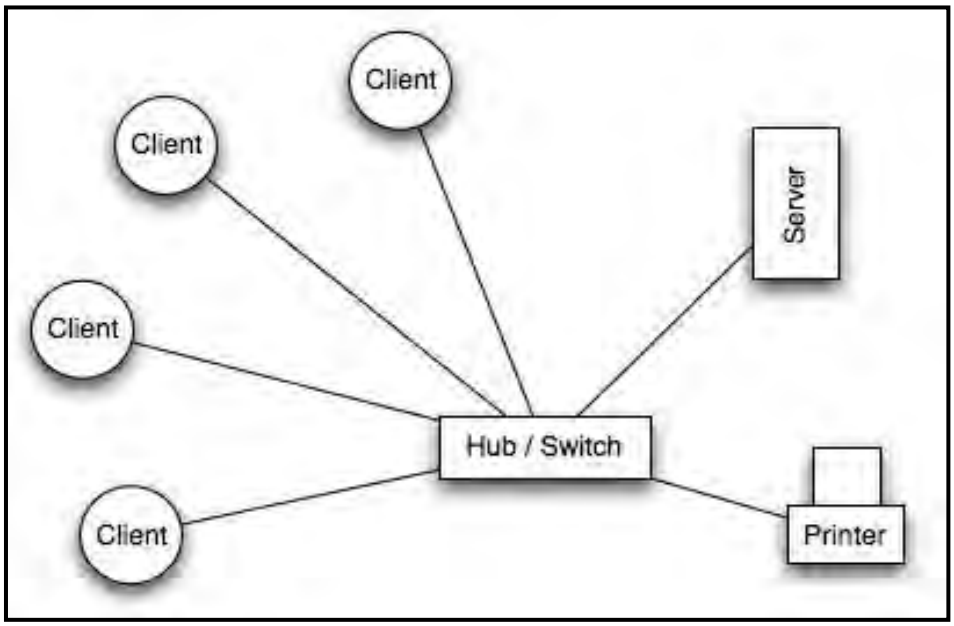
- Connecting a wireless keyboard to a computer
- Connecting a wireless mouse to a computer
- Using a wireless headset with a mobile phone
- Printing wirelessly from a computer or Personal Digital Assistants (PDA)
- Transferring data / music from a computer to an Music Player 3 (MP3) player
- Transferring photos from a phone / camera to another device
- Synchronising calendars on a PDA and a computer

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.

2. **Local Area Network**

A local area network (LAN) consists of a computer network at a single site, typically an individual office building. A LAN is very useful for sharing resources, such as data storage and printers. LANs can be built with relatively inexpensive hardware, such as hubs, network adapters and Ethernet cables.

A Local Area Network is a network confined to one building or site. Often a LAN is a private network belonging to an organisation or business. Because LANs are geographically small, they usually use cables or low-power radio (wireless) for the connections.



A representation of a Local Area Network

The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. High speed and relatively low cost are the defining characteristics of LANs.

LANs are commonly used for single sites where people need to share resources among themselves but not with the rest of the outside world. Think of an office building where everybody should be able to access files on a central server or be able to print a document to one or more central printers. Those tasks should be easy for everybody working in the same office.

If a local area network, or LAN, is entirely wireless, it is referred to as a wireless local area network, or WLAN. Moreover, it is a group of computers which all belong to the same organisation, and which are linked within a small geographic area using a network, and often the same technology (the most widespread being Ethernet).

A local area network is a network in its simplest form. Data transfer speeds over a local area network can reach up to 10 Mbps (such as for an Ethernet network) and 1

Gbps (as with FDDI or Gigabit Ethernet). A local area network can reach as many as 100, or even 1000, users.

By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined:

- In a "peer-to-peer" network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role.
- In a "client/server" environment, in which a central computer provides network services to users.

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings.

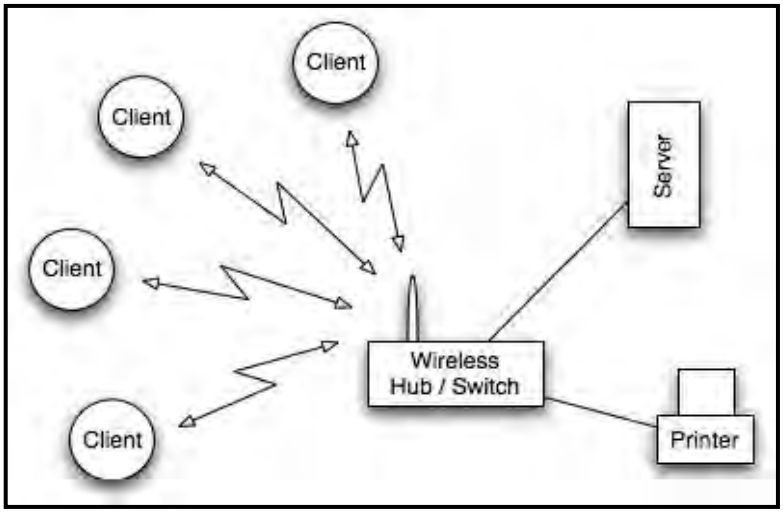
In addition, operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organisation. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

3. **Wireless Local Area Network (WLAN)**

A wireless LAN (WLAN) is a LAN that uses radio signals (Wi-Fi) to connect computers instead of cables.

At the center of the WLAN is a wireless switch or router - a small box with one or two antennas sticking out the back - used for sending and receiving data to the computers. (Most laptops have a wireless antenna built into the case.)

It is much more convenient to use wireless connections instead of running long wires all over a building.



A representation of a wireless LAN

However, WLANs are more difficult to make secure since other people can also try to connect to the wireless network. So, it is very important to have a good, hard-to-guess password for the WLAN connections.

4. **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.

Metropolitan Area Networks (MANs) connect multiple geographically nearby LANs to one another (over an area of up to a few dozen kilometers) at high speeds. Thus, a MAN enables two remote nodes communicate as if they were part of the same local area network. It is a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned and operated by a single entity such as a government body or large corporation.

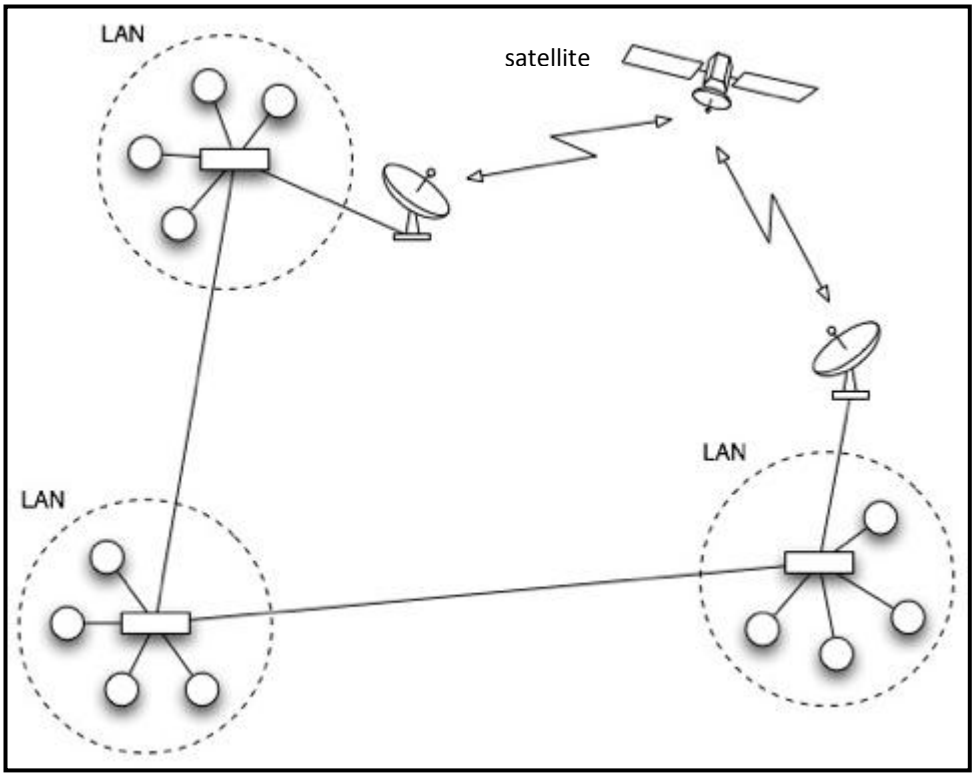
5. **Wide Area Network**

A Wide Area Network or extended network (WAN) connects multiple LANs to one another over great geographic distances. The speed available on a WAN varies depending on the cost of the connections (which increases with distance) and may be low. WANs operate using routers, which can "choose" the most appropriate path for data to take to reach a network node.

A wide area network, or WAN, occupies a very large area, such as an entire country or the entire world. A WAN can contain multiple smaller networks, such as LANs or MANs. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

A Wide Area Network is a network that extends over a large area. A WAN is often created by joining several LANs together, such as when a business that has offices in different countries links the office LANs together. Because WANs are often geographically spread over large areas and links between computers are over long distances, they often use quite exotic technology connections: optical fiber (glass) cables, satellite radio links, microwave radio links, etc.

A Metropolitan Area Network (MAN) is made from switches or routers connected to one another with high-speed links (usually fiber optic cables).



A representation of a Wide Area Network

A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organisation but rather exist under collective or distributed ownership and management. WANs tend to use technology like Automated Teller Machines (ATM) for connectivity over the longer distances. The Internet is the best-known example of a public WAN.

6. **Private Networks**

One of the benefits of networks like PAN and LAN is that they can be kept entirely private by restricting some communications to the connections within the network. This means that those communications never go over the Internet.

For example, using a LAN, an employee is able to establish a fast and secure connection to a company database without encryption since none of the communications between the employee's computer and the database on the server leave the LAN. But, what happens if the same employee wants to use the database from a remote location? What you will need is a private network.

One approach to a private network is to build an enterprise private network, or EPN. An EPN is a computer network that is entirely controlled by one organisation, and it is used to connect multiple locations. Historically, telecommunications companies, like AT&T, operate their own network, separate from the public Internet. EPNs are still fairly common in certain sectors where security is of the highest concern. For example, a number of health facilities may establish their own network between multiple sites to have full control over the confidentiality of patient records.

Different types of networks serve for different purposes based on answering the needs of the user. Each type has its own applications and importance to certain degrees.

Student Activity 12.1.3.1

Answer the following.

1. Compare then contrast the following pairs of types of netwroks.

a. Personal Area Network and Home Area Network

Comparison_____

_____

_____

_____

_____

Contrast_____

_____

_____

_____

_____

_____

_____

b. Local Area Network and Wireless Local Area Network

Comparison_____

_____

_____

_____

_____

Contrast_____

_____

_____

_____

_____

c. Metropolitan Area Network and Campus Area Network

Comparison_____

_____

_____

Contrast_____

_____

_____

_____

d. Wide Area Network and Metropolitan Area Network

Comparison_____

_____

_____

Contrast_____

_____

_____

_____

2. Enumerate three applications which show the importance of use of the different types of network.

a. _____

_____

_____

b. _____

_____

_____

c. _____

_____

_____

12.1.3.2 Components of Networks

The specific discussions we had on data transmission, serial and parallel transmissions, wire and wireless transmissions as well as protocols will be studied in this topic. All these will be put together to create the scenario on how networks are put up.

There are three primary components to understanding networks: physical connections, network operating system and application component. Let us discuss each in detail.

1. **Physical Connections**
   The physical components are the network topology and network connecting devices, which include network interface cards (NIC), cabling, connections, and all other hardware to connect the computers. These hardware parts were all enumerated and discussed in the previous topic on role of network. Let us discuss the items under physical connections.

   a. **Topologies**
      The different methods of connecting computers into a network are called topologies. Each topology has certain advantages and disadvantages that must be considered as one network in an office. These topologies are changing and new hybrid topologies are being developed combining the best of these topologies. We will study the different topologies in our discussions.

   b. **Network Connecting Devices**
      There are a number of physical network components used to network computers. They are network interface cards, cabling, routers, bridges, and hubs. These network connecting devices are considered as the hardware side of networking. Let us briefly discuss them.

      b1. **Network Interface Cards (NIC)**
         Network interface cards are the link between your computer and the cabling to connect your computers to the other computers on the network. There are well over fifty network cards available. When choosing a new card choose the fastest technology and one that is compatible with Windows XP and Vista. Ethernet is a system of protocols for a computer that allows workstations to connect through NICs to other workstations. Ethernet systems are popular because they are relatively inexpensive. The data transmission rate is at 10 MBPS or higher, and uses the bus or star topology.

         Token-Ring, developed by IBM, is more expensive then Ethernet, but transmits data at 16 MBPS or higher. FDDI as we have mentioned in our earlier discussions stands for Fiber Distributed Data Interchange and requires fiber optics cabling to work. Data transmission on FDDI is 100 MBPS and faster. Likewise, ATM which we have studied stands for Asynchronous Transfer Mode and can transfer data from 25 MBPS up to 155 MBPS. It is predicted that the future speeds will be 2

Gigabytes. It appears to be the emerging standard, but still faces inoperability between vendors and backward compatibility issues.

b2. **Cabling (wire and wireless)**

To connect the nodes or workstations of your computer network, you need cabling. Cabling here is referring to both actual physical cabling and the "wireless" variety. In either situation, "cabling" is needed to connect the computers. We have studied wired and wireless connections. Now, let us elaborate more on how these serve as components of a network.

Wire provides the best security and integrity in data transmission at the present time. The two primary types of wire cabling are coaxial and twisted pair. Coaxial cabling is generally less expensive, uses fewer other connector devices, and provides good shielding from outside interference. However, it is more difficult to work with and to install in the walls. Twisted pair cabling has several pairs of wires that are braided within a plastic cover.

Direct cable networking is supported by Windows XP and Vista, and enables two computers to network using either the serial or parallel ports. The parallel ports permit faster transmission but are limited to 50 feet, whereas the serial port cable can extend up to a thousand feet.

Fiber Optic network cable uses light instead of electrical impulses to carry the network signal. Fiber optic is a thin glass filament that connects to optical connectors for each of the computers. Fiber optic's signal strength enables a signal to be run a long distance without any weakening. Because of its signal strength, data speeds can increase from 10 MBPS (10,000,000 bits per second) to over 1G (1,000,000,000 bits per second), which will be sufficient for future network data needs. Fiber optic connectors and cabling are expensive, but may be the choice if electrical interference is present or distance between computers is significant.

Light wave connections use either infrared light beams or lasers to communicate between two computers. Light waves cannot penetrate walls or ceilings, are subject to interference, and network speeds can be quite slow.

Radio wave connections use radio signals to transmit data. They can penetrate walls and ceilings and can transmit from several hundred feet to several miles. Radio-wave connections are typically used when the need to connect mobile laptops in a business is required, such as recording the inventory in nearby warehouses with laptop computers. Radio wave networking can be used to connect buildings and mobile units within a several mile radius. Radio wave

connections are subject to interference of other nearby radio transmissions.

b3. **Gateways**

These are computers that convert one protocol to another protocol. They can convert data from TCP/IP to another protocol or e-mail from one protocol to another. **TCP/IP** (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

b4. **Hubs, Switch, Routers and Bridges**

These are hardware components that connect network segments together to send and receive data between different LANs and WANS. A hub is a connecting device to connect workstations and servers to form a network. They can be used for client/server or peer- to-peer systems.

Switches in networks are devices that filter and forward packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol.

To connect networks together one would use a router or bridge to exchange data information. Routers are generally used to connect and send information from a LAN to the WAN. Bridges are hardware devices that break a large LAN into smaller ones for better management. To connect WANS together; connectors called DSU/CSUs are connected to data transmission lines such as ISDN, and others. A CSU/DSU is a digital-interface device used to connect data terminal equipment (DTE), such as a router, to a digital circuit, such as a Digital Signal 1 (T1) line.

2. **Network Operating System**

In order to communicate on a network, computers must use the appropriate operating protocol selected for the network. This protocol enables the computer to exchange information and ensure correct data transmission. The network operating system (NOS) is the controlling software that enables a server to accommodate multiple clients and provide the communication network between them. The most common network protocols and the products supporting the protocol are: · TCP/IP - Unix, Windows NT™ server, Linux, Internet products. (TCP/IP is the protocol being used on the Internet and for intranets) · IPX/SPX - Novell NetWare™, Windows NT Server™. · NetBIOS - OS/2 WARP Server™, Windows NT Server™.

IPX is a network layer protocol (layer 3 of the OSI Model), while **SPX** is a transport layer protocol (layer 4 of the OSI Model). The **SPX** layer sits on top of the **IPX** layer and provides connection-oriented services between two nodes on

the network. **SPX** is used primarily by client–server applications.

3. **Application Component**
   The value of networking lies in the capability of sharing up-to-date information, software and hardware resources with other users on the system.

   The primary application software networking programs used in the legal profession are word processing, time & billing, calendar/docket/address book, E-mail, document management, conflict management, litigation support, and peripheral sharing such as printers, CD-ROM, PC fax systems, modems and any other hardware.

Hosts, routers & links form the hardware component. Protocols and applications form the software component. Protocols can be viewed as the "glue" that binds everything else together. Network components are vital for the setting up of a network.

Student Activity 12.1.3.2

Answer the following.

1. In your own words explain how physical connection, network operating system and application work as components of a network.

_____

_____

_____

_____

_____

_____

2. Why are the components of a network important?

_____

_____

_____

_____

_____

_____

_____

12.1.3.3 Client Server and Peer-to-Peer Networks

Computers connected together to create a network fall into two categories: servers and clients or workstations.

Client computers, or workstations, are the normal computers that people sit at to get their work done. For example, when you use your Web browser, you are in fact using a Web client. When you type in the URL of a web page, you are actually providing the address of a Web server like www.bbc.co.uk is the address of the BBC's web server. Your Web browser or client asks this server for the web page you want, and the server 'serves' the page back to the browser or client for you to see.

On a broader description, a **Client** can be any node of the network that requires information or service from another node. A **Server** can be any node on the network that provides information or service to another node. A **Node** can be a desktop or a server. If a desktop shares a file to another desktop then it acts as a server.

Servers are special, powerful computers that provide "services" to the client computers on the network.

These services might include:

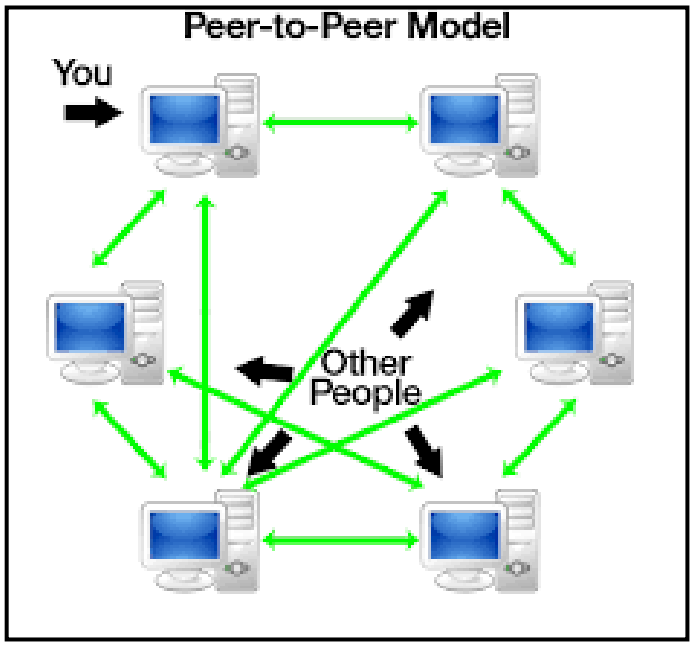
- Providing a central, common file storage area
- Sharing hardware such as printers
- Controlling who can or cannot have access the network
- Sharing Internet connections

Servers are built to be very reliable. This means that they are much more expensive that normal computers. In a small network, one server might provide all of these services. In a larger network there might be many servers sharing the work.

A network therefore is either a peer-to-peer network (also called a workgroup) or a server-based network (also called a client/server network). Let us study each in detail.

Peer-to-peer network

In a peer-to-peer network, a group of computers is connected together so that users can share resources and information. There is no central location for authenticating users, storing files, or accessing resources. This means that users must remember which computers in the workgroup have the shared resource or information that they want to access. It also means that users must log on to each computer to access the shared resources on that computer.



A representation of a Peer-to-peer network

Peer-to-peer networks are designed to make it as easy as possible to share resources. You can create a peer-to-peer network by simply connecting a few computers together, allowing you to move files from one machine to another with a minimum of configuration time or financial cost. However, security can be difficult to manage over peer-to-peer, as there is no central server to authenticate users. Rather, each individual network host must be configured with its own set of permissions regarding which users can access specific files. In addition, a peer-to-peer architecture makes data transfer inefficient for networks of more than around ten machines.

The concept behind peer-to-peer networking is to share files and printers as inexpensively as possible; therefore, there is no main server on the network. Instead, each client functions both as a client and as a server simultaneously. Since users are allowed to control access to the resources on their own computers, however, security becomes very risky in a peer-to-peer environment. There is no central security or any way to control who shares what. Users are free to create any network and share points on their computers. The only security on a peer-to-peer network is at the share level. When users create network shares, they may implement no security, which means that anyone can have full access to the share, or they may assign a password to the share. Depending on which networking platform you use, a user may be able to assign one password to a share for read-only access and another password for full control over the share.

Although, this arrangement may sound somewhat secure, it is not. The computer that contains the shared resources does not check on who is trying to access those resources. Any user can access them as long as the user knows the password. If someone happens to write down a password, anyone who finds that password can access the share.

In most peer-to-peer networks, it is difficult for users to track where information is located because data is generally stored on multiple computers. This makes it difficult to back up

critical business information, and it often results in small businesses not completing backups. Often, there are multiple versions of the same file on different computers in the workgroup.

Peer-to-peer networks are appropriate only for very small businesses or for home use. A peer-to-peer network can support about ten clients (workstations) before it begins to suffer from some serious performance and management problems. Usually, peer-to-peer networks are composed of a collection of clients that run either Windows NT Workstation or Windows 98. Windows 3.11, Windows 95, and Windows 2000 Professional also support peer-to-peer networking.

In some peer-to-peer networks, the small business uses one computer that is running a client operating system, such as Microsoft Windows 98 or Windows XP Professional, as the designated "server" for the network. Although, this helps with saving data in a central location, it does not provide a robust solution for many of the needs of a small business, such as collaborating on documents.

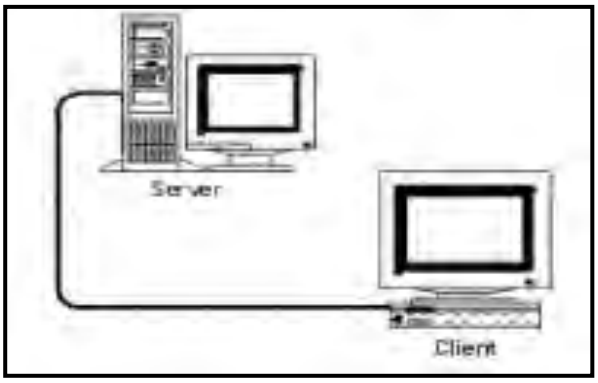
Peer-to-peer networks are best suited to home or very small office setups. For example, you might set up a peer-to-peer network in your home as a cost-effective way to share files between your computers and other devices. The relatively unsecured nature of the peer-to-peer architecture makes such networks unsuitable for dealing with sensitive files, however, especially if it was possible to access your network's clients over the Internet.

Server-based network

Server-based network, also known as client-based network has the server as the central location where users share and access network resources. The resources are located on and controlled by a central computer or the server.

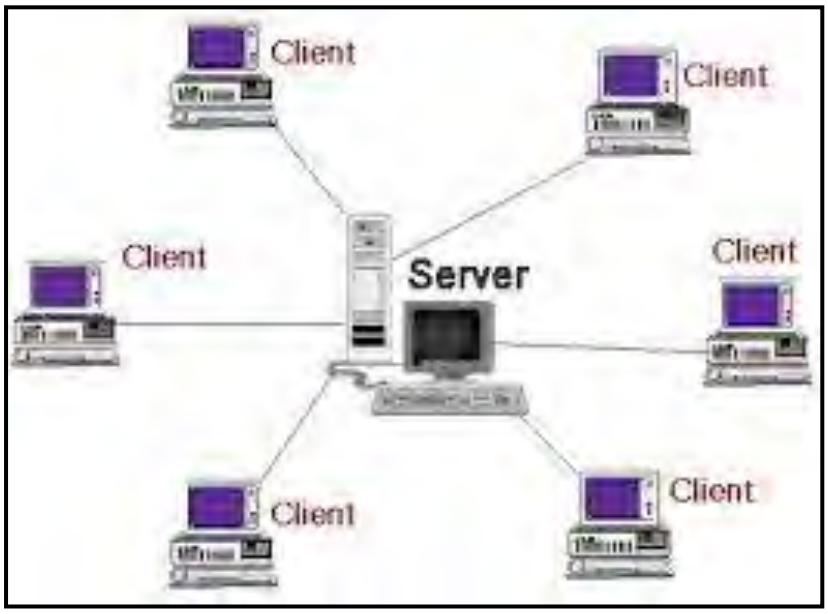
This dedicated computer controls the level of access that users have to share resources. Shared data is in one location, making it easy to back up critical business information. Each computer that connects to the network is called a client computer.

In a server-based network, users have one user account and password to log on to the server and to access shared resources. Server operating systems are designed to handle the load when multiple client computers access server-based resources.



A representation of a Client-based network

This architecture offers greater security than peer-to-peer, as all resources are located in the same place. By password-protecting the server, you can ensure that only authorised users can gain access to the network's files and hardware. However, client-server networks are often more expensive to set up than their peer-to-peer equivalents, as server hardware and software is more expensive than regular desktop computers.



A representation of a Client-based network

There are almost an infinite variety of client/server networks, but all of them have a couple of things in common. For one thing, all have centralised security databases that control access to shared resources on servers. In the world of Windows, the server usually runs NetWare, Windows NT, or one of the Windows 2000 Server products. The server contains a list of usernames and passwords. Users cannot log on to the network unless they supply valid usernames and passwords to the server. Once logged on, users may access only those resources that the network administrator allows them to access. Thus, client/server networks possess much more security than do peer-to-peer networks.

Client-server networks work best for larger setups, such as a full-scale office or school network -- especially if the networks are likely to grow in size. One should also use client-server architecture if the network has sensitive data to protect. For example, a school would be likely to store its pupil records in a client-server database, as this would reduce the chance of personal details falling into the wrong hands.

Both Peer-to-peer and Client-server network architectures have their advantages and disadvantages. On balance, however, a Client-server configuration is preferable to peer-to-peer, especially in a small business environment where there is an expectation of growth.

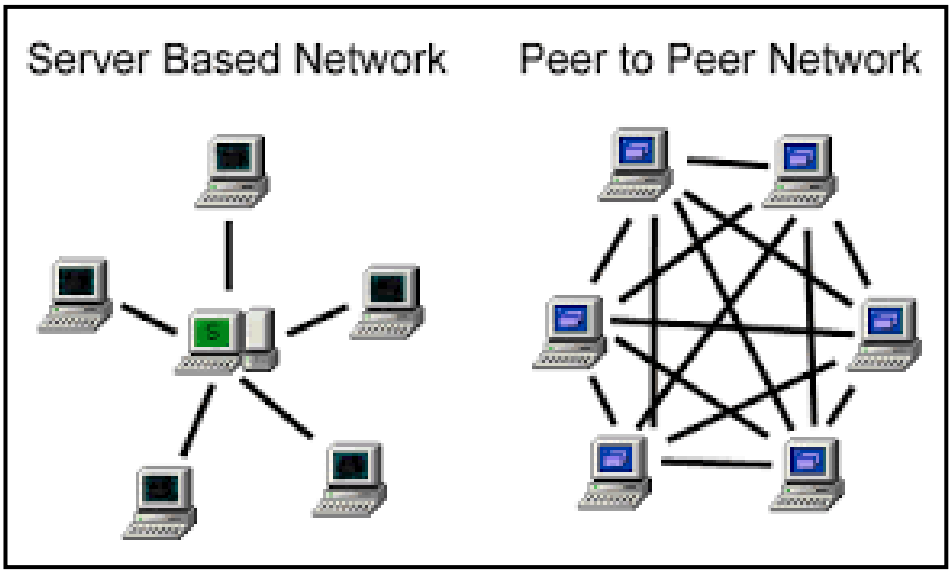
The advantage of the Peer-to-peer is that it is relatively inexpensive and fairly simple to set up and manage. The disadvantage is that it is limited in extensibility, tends to overburden user workstations by having them play the role of server to other users, is largely unsecured, and is typically unable to provide system-wide services since the typical workstation will run

a standard desktop operating system incapable of hosting any major service (e.g., a post office).

The upside of the Client-server is that it can extend to handle organisational growth, allows user workstations to function as unburdened clients, can provide sophisticated system-wide services, and is configurable for maximum security. The downside is obvious: higher initial capital investment to establish and a greater level of technology expertise required to configure and manage, as compared to the vanilla peer-to-peer network.

We can conclude that the primary difference between peer-to-peer and client-server networks is that peer-to-peer networks do not have a central server to manage network resources. Instead, resources on a peer-to-peer network are distributed among the various clients that make up that network. As a result, peer-to-peer networks are easy to configure, but can be less secure than client-server networks.

The illustration below will best identify the difference of the peer to peer and the client-based or server based networks.



Client-based or Server -based network and Peer to peer network

Student Activity 12.1.3.3

Answer the following.

1. Complete the information needed in the table below.

Network	Comparison	Contrast	Example	Main Advantages	Main Disadvantages
Peer to peer					
Client-server					

2. If you have a growing business, what will you use, Peer to peer or client-based network? Why?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

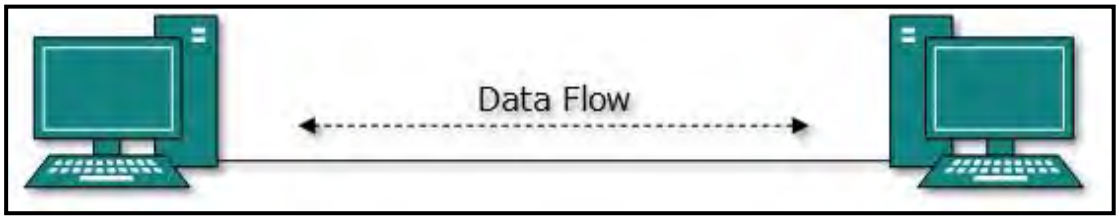
12.1.3.4 Network Topologies

The word topology means 'arrangement', so when we talk about the topology of a network, we mean how the different parts are arranged and connected together. Network Topology basically refers to layout of a network. It is how the different nodes in a network are connected to each other and how they communicate.

In communication networks, a topology is a usually schematic description of the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology. Hence, the different methods of connecting computers into a network are called topologies. Each topology has certain advantages and disadvantages that must be considered as one network of office. These topologies are changing and new hybrid topologies are being developed combining the best of these topologies.

Let us study each in detail.

1. Point-to-point networks contain exactly two hosts where the computer or switches or routers or servers are connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other end and vice-versa.



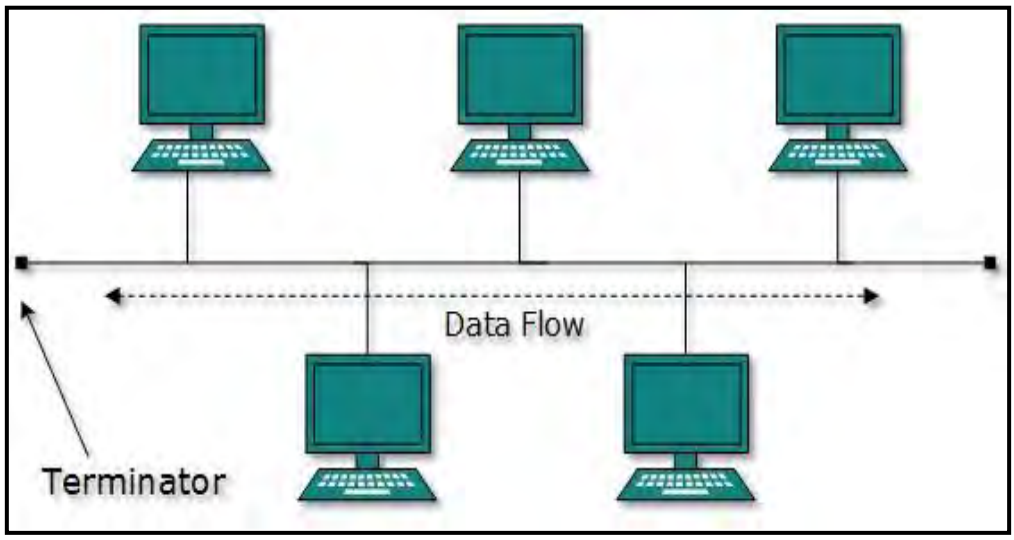
A representation of a Point-to-point network

If the hosts are connected point-to-point logically, they may have multiple intermediate devices. But, the end hosts are unaware of underlying network and see each other as if they are connected directly.

2. Bus topology computers are connected together to a central cable called a bus. Each computer has a short cable linking it to the 'bus'. The *bus* topology is one of the most common, and does not require as many cables as other systems; thus, it is less expensive.

   As new computers are added, they are connected to the main backbone, or bus. The system continues to work even if one of the client's cables fails.

   However, the whole network stops if the main cable or bus is severed or disconnected. The system may slow down as more data is transferred along this one main connection.



A representation of a Bus topology

A bus network has the following characteristics:

- It is cheaper to install with just one long cable.
- It can be quite slow since all computers share the same cable when communicating.
- It will stop working if there is a break in the central bus cable.

In contrast to point-to-point, in bus topology all devices share single communication line or cable. All devices are connected to this shared line. Bus topology may have problems when more than one hosts sending data at the same time.

Therefore, the bus topology either uses Carrier-sense multiple access with collision detection (CSMA/CD) technology or recognises one host as Bus Master to solve the issue. This will be elaborated when we will discuss the access methods.

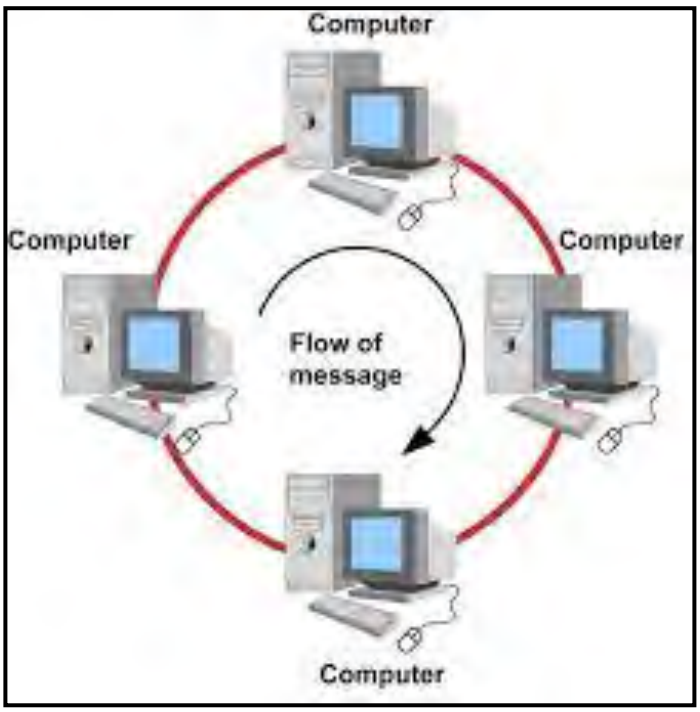
Bus topology is one of the simple forms of networking where a failure of a device does not affect the others. But failure of the shared communication line makes all other devices fail. Both ends of the shared channel have a line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Bus networks must not to be confused with the system bus of a computer since it uses a common backbone to connect all the devices. A single cable is the backbone which functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

3. The ring topology connects each PC to two other PCs in a ring formation. Each PC is set up to pass data from one machine to the next in this relay type of system. Each

computer has an in and out port. If one PC fails, the entire system fails. This system uses less cable than the others and thus, is less costly. Most integrators use the hybrid ring systems.

In this type of network each computer is connected to a loop of cable, the 'ring'. If you took a bus network and connected the ends of the bus cable together, you would have a ring network. A ring network can cope with a break in the ring cable since all computers are still joined together.



A representation of Ring topology

Moreover, in ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure administrator may need only one more extra cable.

In a ring network, every device has exactly two neighbours for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counter clockwise"). A failure in any cable or device breaks the loop and can take down the entire network. Failure of any host results in failure of the whole ring. Thus, every connection in the ring is considered a point of failure. There exist methods which employs one more backup ring.

4. In a star network, all the computers are connected through a central hub to the server. All hosts in star topology are connected to a central device, known as Hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and Hub.

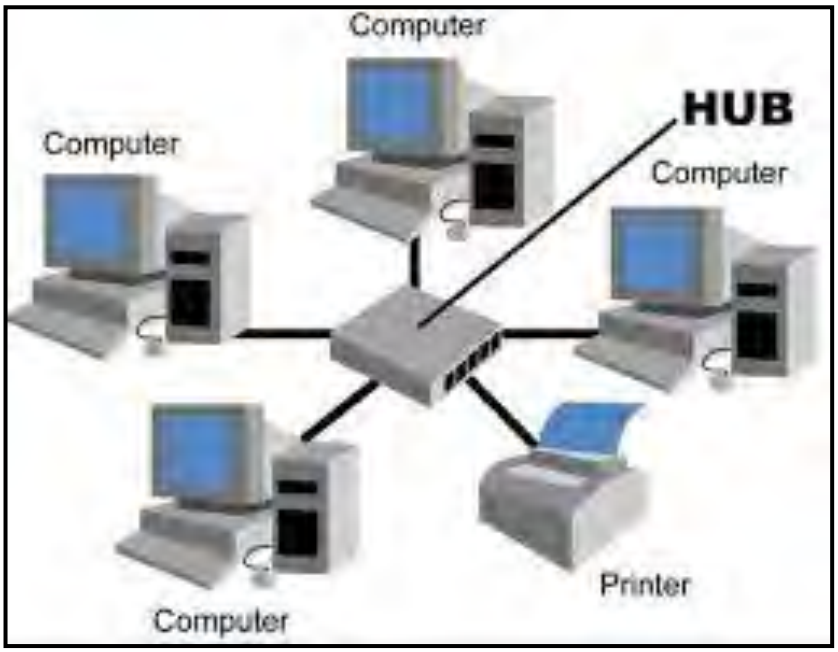
The advantage to this system is that if one cable or computer is disconnected the entire network continues to function. This configuration is considered one of the most reliable; however, it uses a lot of cable. Thus, it is more expensive. If the central hub fails, the system will not function.

In this type of network every computer is connected to a central device. The device passes messages between computers.

At the center of a star network one might use a hub which is cheap, but slow or a switch which is more expensive, but faster.

A star network then has the following characteristics:

- It is quite expensive to install since one needs to buy lots of cable and the central device.
- It is very fast since each computer has its own cable which it does not need to share.
- It can cope with a broken cable wherein only one computer will be affected.
- It will stop working if the central device breaks.
- It is the most common network topology.



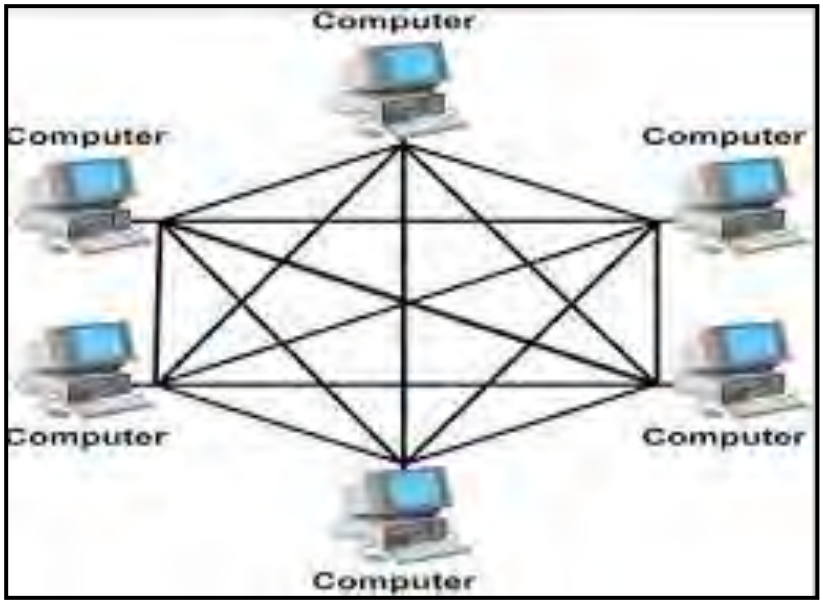
A representation of a Star network

Therefore, in bus topology, the hub acts as single point of failure. If the hub fails, connectivity of all hosts to all other hosts fails. All communication that happens between hosts goes through the hub only. Star topology is not expensive, as to connect one more host, only one cable is required and configuration is simple.

Many home networks use the star topology. A star network features a central connection point called a "hub node" that may be a network hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.

Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN. If the hub fails, however, the entire network also fails.

5. Mesh topology is the type of topology where a host is connected to one or two or more than two hosts. This topology may have hosts having point-to-point connection to every other host or may also have hosts which have point to point connection to a few hosts only.



A representation of Mesh topology

Hosts in mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes in two types:

a. Full Mesh is where all hosts have a point-to-point connection to every other host in the network. It provides the most reliable network structure among all network topologies.

b. Partially Mesh is where not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrary fashion. This topology exists where we need to provide reliability to some host whereas others are not as necessary.

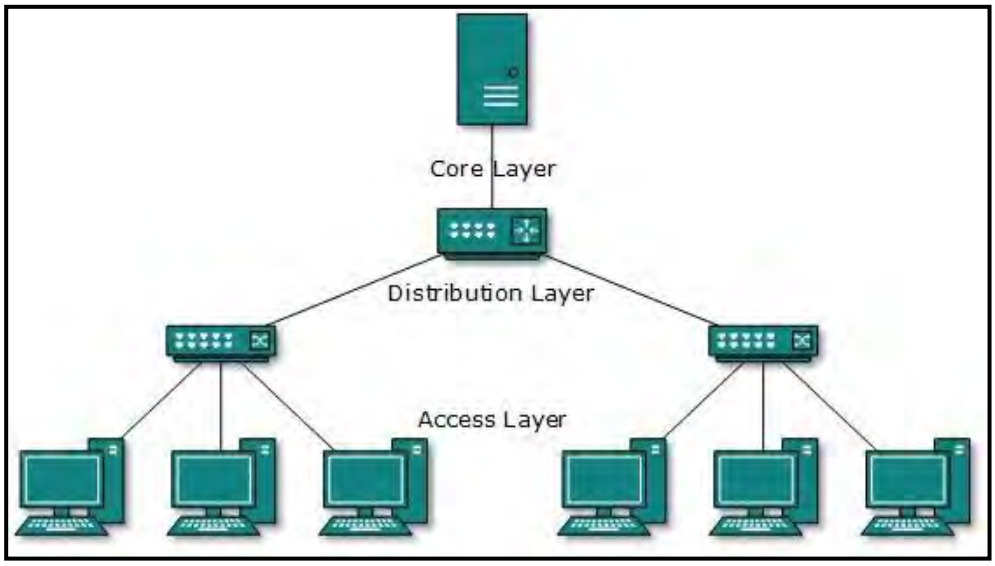
A mesh network in which each device connects to each other is called a full mesh. As shown in the illustration, partial mesh networks also exist in which some devices only connect indirectly to others.

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of the possible paths

from the source to the destination. Remember that even in a ring, although two cable paths exist, messages can only travel in one direction. Some WANs , most notably the Internet, employ mesh routing.

6. Tree topology is also known as Hierarchical Topology. It is the most common form of network topology in use today. This topology imitates the extended Star Topology and inherits properties of Bus topology.

This topology divides the network into multiple levels/layers of network. Mainly in LANs, a network is divided into three types of network devices. The lowest is the access-layer where the users' computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The top layer is known as core layer, and is the central point of the network, like the root of the tree from which all nodes fork.

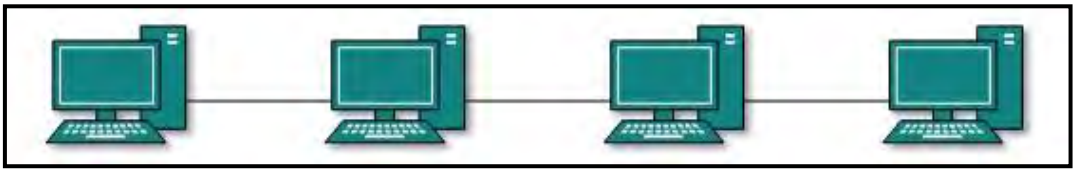


A representation of a Tree topology

All neighbouring hosts have point-to-point connection between them. Like bus topology, if the root goes down, the entire network suffers though it is not the single point of failure. Every connection serves as a point of failure, failing of which divides the network into unreachable segment and so on.

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus and each hub functions as the root of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.

7. Daisy topology is a topology that connects all its hosts in a linear fashion. Similar to Ring topology, all hosts in this topology are connected to two hosts only, except the end hosts. That is, if the end hosts in Daisy Chain are connected then it represents Ring topology.

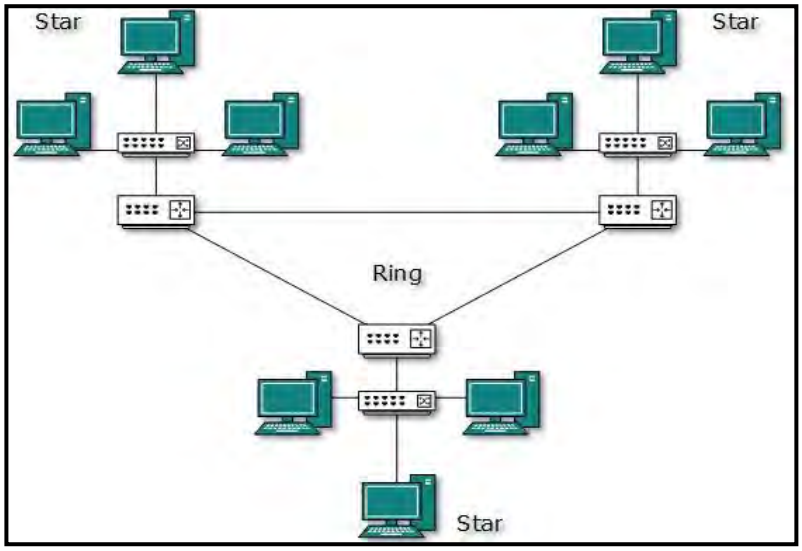


A representation of a Daisy topology

Each link in Daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

8. A hybrid network is the one that combines two or more of the above basic topologies**.** A network that has several star networks linked together is a hybrid network.

The picture below represents an arbitrary Hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus and Daisy-chain topologies. Most WANs are connected by means of dual Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology



A representation of a Hybrid network

A network structure whose design contains more than one topology is said to be Hybrid Topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.

Topologies remain an important part of network design theory. One can probably build a home or small business computer network without understanding the difference between a bus design and a star design, but becoming familiar with the standard topologies gives you a better understanding of important networking concepts like hubs, broadcasts, and routes.

Student Activity 12.1.3.4

Answer the following.

1. Explain network topology.

_____

_____

_____

_____

2. Complete the information needed in the table below.

Network Topology	Description	Example	Advantages	Disadvantages
Point to point				
Bus				
Ring				
Star				

Mesh				
Tree				
Daisy				
Hybrid				

3. What is the importance of the different topologies?

_____

_____

_____

_____

12.1.3.5 Network Access Methods

In computing, an access method is a program or a hardware mechanism that moves data between the computer and an outlying device such as a hard disk (or other form of storage) or a display terminal.

An access method is a function of a mainframe operating system that enables access to data on disk, tape or other external devices. They were introduced in 1963 in IBM OS/360 operating system. Access methods provide an application programming interface (API) for programmers to transfer data to or from a device, and could be compared to device drivers in non-mainframe operating systems.

In networking, to access a resource is to be able to use that resource. This lesson introduces the role of access methods in putting data on a network cable. It focuses on three major access methods: carrier-sense multiple-access methods, token passing, and demand priority.

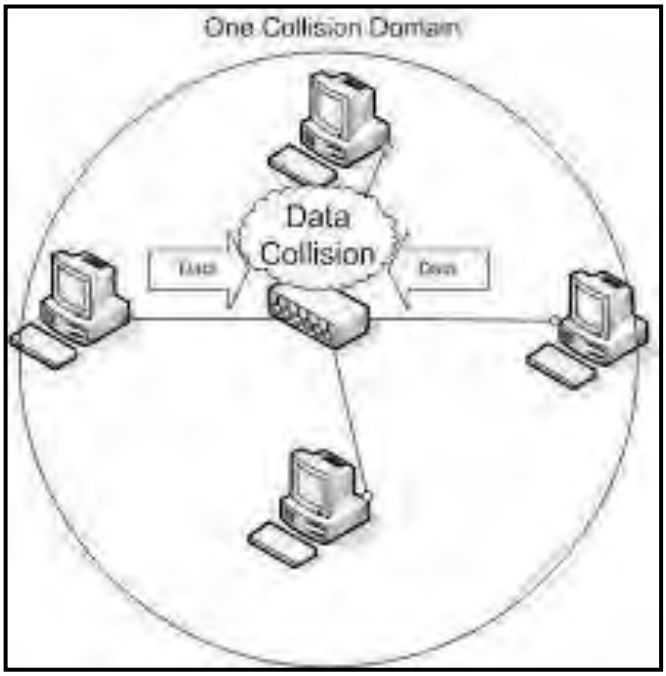
Access method is the set of rules that defines how a computer puts data onto the network cable and takes data from the cable. Once data moves on the network, access methods help to regulate the flow of network traffic.

To understand traffic on a computer network, it is better to use an analogy. A network is in some ways like a railroad track, along which several trains run. The track is intermixed with occasional railway stations. When a train is on the track, all other trains must abide by a procedure that governs how and when they enter the flow of traffic. Without such a procedure, entering trains would collide with the one already on the track.

A picture representation of a railroad track

There are important differences between a railroad system and a computer network. On a network, all traffic appears to move simultaneously, without interruption. Actually, this appearance of simultaneity is an illusion; in reality, the computers take turns accessing the network for brief periods of time. The more significant difference arises from the higher speed at which network traffic moves.

Multiple computers must share access to the cable that connects them. However, if two computers were to put data onto the cable at the same time, the data packets from one computer would collide with the packets from the other computer, and both sets of data packets would be destroyed. The figure below shows what happens when two computers try to access the network at the same time.



A representation of how collision occurs if two computers put data on the cable at the same time

If data is to be sent over the network from one user to another, or accessed from a server, there must be some way for the data to access the cable without running into other data. And the receiving computer must have reasonable assurance that the data has not been destroyed in a data collision during transmission.

Access methods need to be consistent in the way they handle data. If different computers were to use different access methods, the network would fail because some methods would dominate the cable.

Access methods prevent computers from gaining simultaneous access to the cable. By making sure that only one computer at a time can put data on the network cable, access methods ensure that the sending and receiving of network data is an orderly process.

After learning what access methods are and their functions, let us study the three commonly used access methods. The three methods designed to prevent simultaneous use of the network media include:

1. Carrier-sense multiple access methods (with collision detection or with collision avoidance).

2. Token-passing methods that allow only a single opportunity to send data.

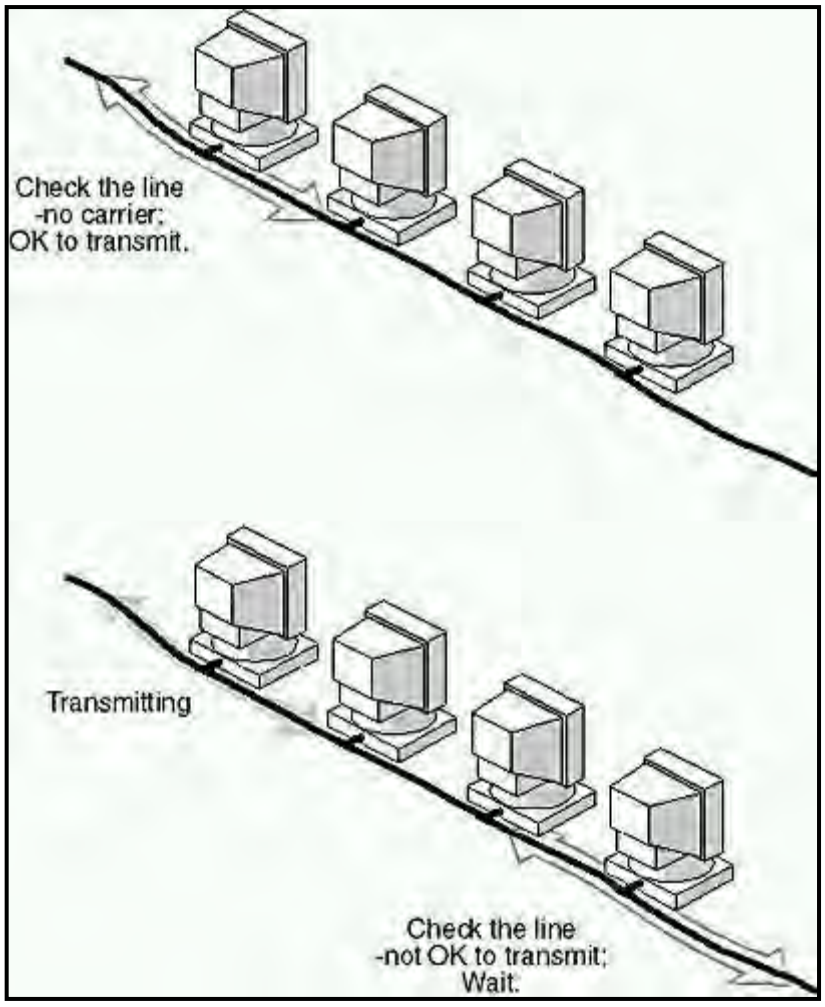
3. Demand-priority methods.

Let us discuss each in detail.

1. **Carrier-sense multiple access methods (with collision detection or with collision avoidance)**

1a. **Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) Access Method**

Using the method known as *carrier-sense multiple access with collision detection (CSMA/CD),* each computer on the network, including clients and servers, checks the cable for network traffic. The figure below illustrates when a computer can and cannot transmit data.



A representation of how computers can transmit data only if the cable is free

Only when a computer detects that the cable is free, and that, there is no traffic on the cable can it send data. Once the computer has transmitted data on the cable, no other computer can transmit data until the original data has reached its destination and the cable is free again. Remember, if two or more computers happen to send data at exactly the same time, there will be a data collision. When that happens, the two computers involved stop transmitting for a random period of time and then attempt to retransmit. Each computer determines its own waiting period; this reduces the chance that the computers will once again transmit simultaneously.

With these points in mind, the name of the access method—carrier-sense multiple access with collision detection (CSMA/CD) makes sense. Computers listen to or "sense" the cable (carrier-sense). Commonly, many computers on the network attempt to transmit data (multiple access); each one first listens to detect any possible collisions. If a computer detects a possible collision, it waits for a random period of time before retransmitting (collision detection).

The collision-detection capability is the parameter that imposes a distance limitation on CSMA/CD. Due to **attenuation**, the weakening of a transmitted signal as it travels farther from its source, the collision detection mechanism is not effective beyond 2500 meters (1.5 miles). Segments cannot sense signals beyond that distance and, therefore, might not be aware that a computer at the far end of a large network is transmitting. If more than one computer transmits data on the network at the same time, a data collision will take place that will corrupt the data.

Moreover, CSMA/CD is known as a **contention** method because computers on the network contend, or compete, for an opportunity to send data.

This might seem like a burdensome way to put data on the cable, but current implementations of CSMA/CD are so fast that users are not even aware they are using a contention access method.

There are considerations on the use of CSMA/CD. The more computers there are on the network, the more network traffic there will be. With more traffic, collision avoidance and collisions tend to increase, which slows the network down, so CSMA/CD can be a slow-access method.

After each collision, both computers will have to try to retransmit their data. If the network is very busy, there is a chance that the attempts by both computers will result in collisions with packets from other computers on the network. If this happens, four computers (the two original computers and the two computers whose transmitted packets collided with the original computer's retransmitted packets) will have to attempt to retransmit. These proliferating retransmissions can slow the network to a near standstill.

The occurrence of this problem depends on the number of users attempting to use the network and which applications they are using. Database applications tend to put more traffic on the network than word-processing applications do.

Depending on the hardware components, the cabling, and the networking software, using a CSMA/CD network with many users running several database applications can be very frustrating because of heavy network traffic.

In CSMA/CD (Carrier Sense Multiple Access/Collision Detection) access method, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. When a host want to place data on the wire, it will "sense" the wire to find whether there is a signal already on the wire. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the

medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted, to avoid collision again.

1b. **Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) Access Method**

Carrier-sense multiple access with collision avoidance (CSMA/CA) is the least popular of the three major access methods. In CSMA/CA, each computer signals its intent to transmit before it actually transmits data. In this way, computers sense when a collision might occur. This allows them to avoid transmission collisions. Unfortunately, broadcasting the intent to transmit data increases the amount of traffic on the cable and slows down network performance.

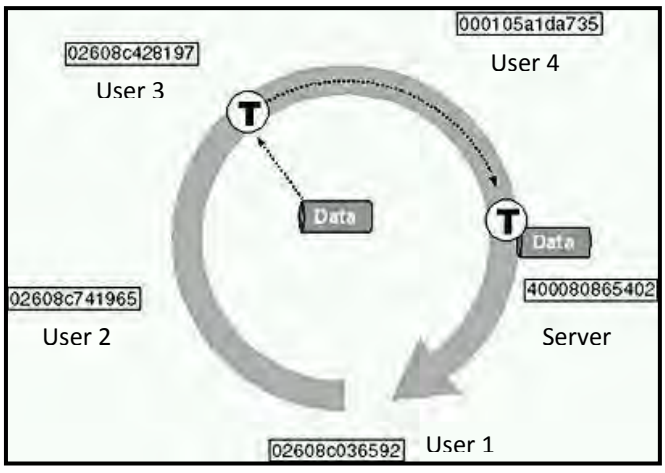
In CSMA/CA, before a host sends real data on the wire it will "sense" the wire to check if the wire is free. If the wire is free, it will send a piece of "dummy" data on the wire to see whether it collides with any other data. If it does not collide, the host will assume that the real data also will not collide.

2. **Token-Passing Access Method**

In the access method known as *token passing*, a special type of packet, called a token, circulates around a cable ring from computer to computer. When any computer on the ring needs to send data across the network, it must wait for a free token. When a free token is detected, the computer will take control of it if the computer has data to send.

The computer can now transmit data. Data is transmitted in frames, and additional information, such as addressing, is attached to the frame in the form of headers and trailers.

From the figure below, the server is shown transmitting data. It takes control of the free token on the ring and sends data to the computer with the address 400080865402.



A representation of Token-passing access method

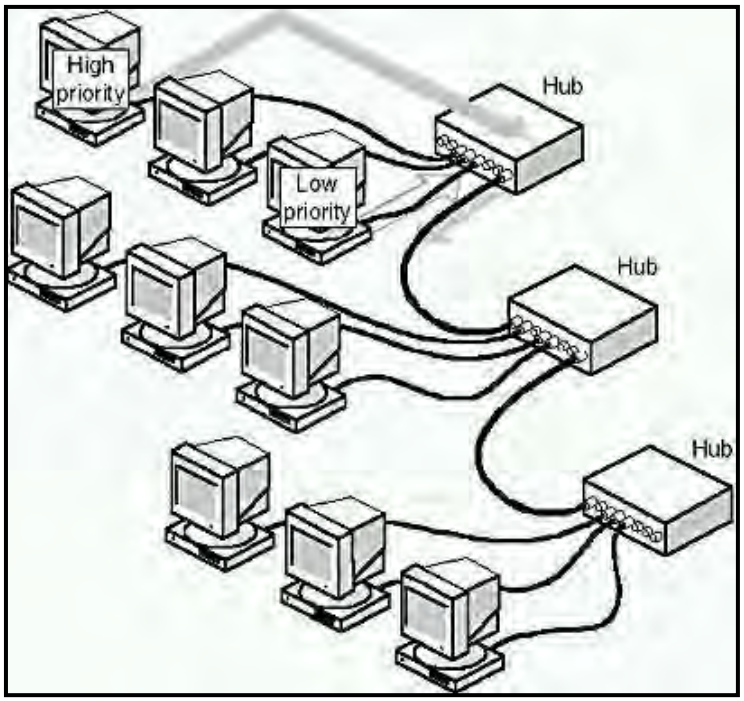
While the token is in use by one computer, other computers cannot transmit data. Because only one computer at a time can use the token, no contention and no collision take place, and no time is spent waiting for computers to resend tokens due to network traffic on the cable.

In CSMA/CD and CSMA/CA the chances of collisions are there. As the number of hosts in the network increases, the chances of collisions also will become more. In token passing, when a host wants to transmit data, it should hold the token, which is an empty packet. The token circles the network in a very high speed. If any workstation wants to send data, it should wait for the token. When the token has reached the workstation, the workstation can take the token from the network, fill it with data, mark the token as being used and place the token back to the network.

3. **Demand Priority Access Method**

Demand priority is a relatively new access method designed for the 100-Mbps Ethernet standard known as 100VG-AnyLAN. It has been sanctioned and standardised by the Institute of Electrical and Electronic Engineers (IEEE) in its 802.12 specification, which is discussed later.

This access method is based on the fact that repeaters and end nodes are the two components that make up all 100VG-AnyLAN networks. The figure below shows a demand-priority access network. The repeaters manage network access by doing round-robin searches for requests to send from all nodes on the network. The repeater, or hub, is responsible for noting all addresses, links, and end nodes and verifying that they are all functioning. According to the 100VG-AnyLAN definition, an end node can be a computer, bridge, router, or switch.



A representation of a Star-bus network access method which is a demand priority

Moreover, as in CSMA/CD, two computers using the demand-priority access method can cause contention by transmitting at exactly the same time. However, with demand as a priority, it is possible to implement a scheme in which certain types of data will be given priority if there is contention. If the hub or repeater receives two requests at the same time, the highest priority request is serviced first. If the two requests are of the same priority, both requests are serviced by alternating between the two.

In a demand-priority network, computers can receive and transmit at the same time because of the cabling scheme defined for this access method. In this method, four pairs of wires are used, which enables quartet signalling, transmitting 25 MHz signals on each of the pairs of wire in the cable.

Like the other access methods, demand priority has some considerations. In a demand-priority network, there is communication only between the sending computer, the hub, and the destination computer. This is more efficient than CSMA/CD, which broadcasts transmissions to the entire network. In demand priority, each hub knows only about the end nodes and repeaters directly connected to it, whereas in a CSMA/CD environment, each hub knows the address of every node in the network.

The advantages of a demand-priority access method are the following:

- The use of four pairs of wires. By using four pairs of wires, computers can transmit and receive at the same time.
- Transmissions through the hub.

Transmissions are not broadcast to all the other computers on the network. The computers do not contend on their own for access to the cable, but operate under the centralised control of the hub.

After a thorough discussion on the access methods, the table below summarises the major features of each access method.

Feature or function	**CSMA/CD**	**CSMA/CA**	**Token passing**	**Demand priority**
Type of Communication	Broadcast-based	Broadcast-based	Token-based	Hub-based
Type of access method	Contention	Contention	Non-contention	Contention
Type of network	Ethernet	Local Talk	Token Ring ArcNet	100VG- Any LAN

Therefore in brief, we can say that:

- Managing data on a network is a form of traffic control.
- The set of rules that governs how network traffic is controlled is called the access method.
- When using the CSMA/CD access method, a computer waits until the network is quiet and then transmits its data. If two computers transmit at the same time, the data will collide and have to be re-sent. If two data packets collide, both will be destroyed.
- When using the CSMA/CA access method, a computer transmits its intent to transmit before actually sending the data.
- When using the token-ring access method, each computer must wait to receive the token before it can transmit data. Only one computer at a time can use the token.
- When using the demand-priority access method, each computer communicates only with a hub. The hub then controls the flow of data.

Student Activity 12.1.3.5

Answer the following.

1. What is a network access method?

_____

_____

_____

_____

2. What is the importance of access methods?

_____

_____

_____

3. List the commonly used access methods.

_____

_____

_____

4. Complete the information need in the table below.

Type of access method	Description	Advantage
CSMA/CD		
CSMA/CA		
Token passing		
Demand priority		

12.1.3.6 Security of Information

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is of great importance because of intellectual property that can be easily acquired through the internet. Network security is a big topic and is growing into a high profile and often highly paid Information Technology (IT) specialty area. Computer security involves many aspects, from protection of the physical equipment to protection of the electronic bits and bytes that make up the information that resides on the network.

A generic definition of security from the American Heritage Dictionary is “freedom from risk or danger; safety”. This definition is perhaps a little misleading when it comes to computer and networking security, as it implies a degree of protection that is inherently impossible in the modern connectivity-oriented computing environment. This is why the same dictionary provides another definition specific to computer science: “The level to which a program or device is safe from unauthorised use.” Implicit in this definition is the warning that the objectives of security and accessibility which are the two top priorities on the minds of many network administrators are, by their very natures, diametrically opposed. The more accessible your data is and the less secure it is. Likewise, the more tightly you secure it, the more you impede accessibility. Any security plan is an attempt to strike the proper balance between the two.

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorised access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorisation of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organisations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name like the password which is sometimes termed as one-factor authentication. But with the two-factor authentication, the user 'has' is also used for example a security token or 'dongle', an ATM card, or a mobile phone. Lastly, with three-factor authentication, something the user 'is' is also used for example his fingerprint or a retinal scan.

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorised access, this component may fail to check potentially harmful content such as computer worms

or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wire shark traffic and may be logged for audit purposes and for later high-level analysis. Communication between two hosts using a network may be encrypted to maintain privacy.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered:

1. Access – authorised users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavour.

To lessen the vulnerability of the computer to the network, there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools. “Intranets” are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

The types of attacks through the internet need to also be studied to be able to detect and guard against them. Intrusion detection systems are established based on the types of attacks most commonly used. Network intrusions consist of packets that are introduced to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource’s intended function

- To gain system knowledge that can be exploited in later attacks

The last reason for a network intrusion is most commonly guarded against and considered by most as the only intrusion motive.

Typical security currently exists on the computers connected to the network. Security protocols sometimes usually appear as part of a single layer of the OSI network reference model. The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. Current work is being performed in using a layered approach to secure network design. The layers of the security model correspond to the OSI model layers. This security approach leads to an effective and efficient design which circumvents some of the common security problems.

Common internet attack methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and Trojans. The other form of attack is when the system's resources are consumed uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well-known as DoS attacks, but they are used in some form or another even if they are not mentioned by name.

Let us study each common attack to the network in detail. Remember that some of these were discussed already in Grade 11 Information and Communication Technology in the topic Measures to Protect Computers and Data.

a. **Eavesdropping**
   Interception of communications by an unauthorised party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way.

b. **Viruses**
   Viruses are self-replication programs that use files to infect and propagate [8]. Once a file is opened, the virus will activate within the system.

c. **Worms**
   A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate. There are two main types of worms, mass-mailing worms and network-aware worms. Mass mailing worms use email as a means to infect other computers.

Network-aware worms are a major problem for the Internet. A network-aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

d. **Trojans**
Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus.

e. **Phishing**
Phishing is an attempt to obtain confidential information from an individual, group, or organisation. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

f. **Spoofing Attacks**
Spoofing is a term that refers to having the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP spoofed packets cannot be eliminated.

g. **Denial of Service**
Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. The following are the different defense and detection mechanisms which were developed to deal with these attacks.

a. **Cryptographic systems**
Cryptography is a useful and widely used tool in security engineering today. It involves the use of codes and ciphers to transform information into unintelligible data.

b. **Firewall**
A firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defense mechanism against intruders. It is a system designed to prevent unauthorised access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

c. **Intrusion Detection Systems**
An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack.

IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

d. **Anti-Malware Software and scanners**
Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.

e. **Secure Socket Layer (SSL)**
The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.

The businesses today use combinations of firewalls, encryption, and authentication mechanisms to create “intranets” that are connected to the internet but protected from it at the same time. Intranet is a private computer network that uses internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organisation while extranets can generally be accessed by customers, suppliers, or other approved parties.

There does not necessarily have to be any access from the organisation's internal network to the Internet itself. When such access is provided it is usually through a gateway with a firewall, along with user authentication, encryption of messages, and often makes use of Virtual Private Networks (VPNs). Although intranets can be set up quickly to share data in a controlled environment, that data is still at risk unless there is tight security. The disadvantage of a closed intranet is that vital data might not get into the hands of those who need it. Intranets have a place within agencies.

For broader data sharing, it might be better to keep the networks open, with these safeguards:

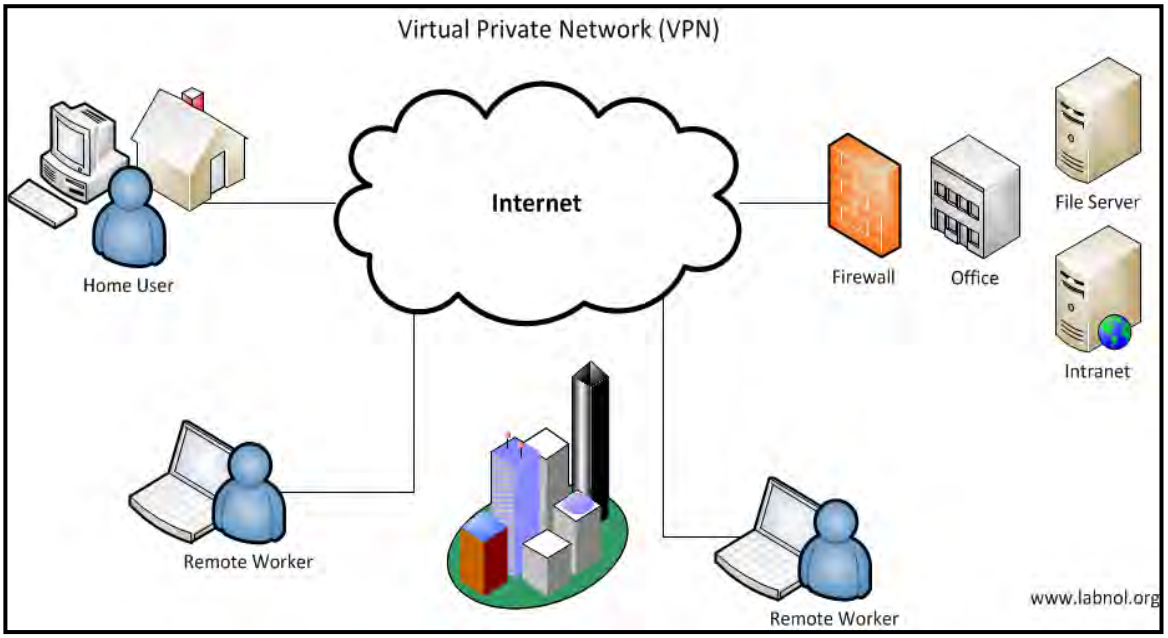
1. Firewalls that detect and report intrusion attempts
2. Sophisticated virus checking at the firewall
3. Enforced rules for employee opening of email attachments
4. Encryption for all connections and data transfers
5. Authentication by synchronised, timed passwords or security certificates

It was mentioned that if the intranet wanted access to the internet, virtual private networks are often used. Intranets that exist across multiple locations generally run over separate

leased lines or a newer approach of VPN can be utilised. VPN is a private network that uses a public network which is usually the Internet to connect remote sites or users together.

Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

The figure on the next page is a graphical representation of an organisation and VPN network.



A representation of an organisation of a Virtual Private Network (VPN)

A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field.

The following are some useful network security tips:

- Use Virus Protection Software
- Do not open unknown email attachments
- Use regular backup of your critical data
- Make boot disk
- Use Firewall program
- Authenticate users
- Implement Security Policy in your network
- Keep an inventory of your software and hardware and make a list of all the devices.

- Scan TCP/UDP services
- Do not provide more rights to the system resources than necessary.
- Perform the network security testing and find the holes and fix them.
- Place your server at very safe place.
- Prepare an Assistant Network Administrator and train him/her about all the security related matters so that he/she can control the network in your absence.
- Monitor the user's activities on the internet and block all the unwanted websites, web applications which have security risks.

The following methods are very helpful in securing a wireless network.

1. **Wi-Fi Protected Access (WPA and WPA2)**

   Wi-Fi Protected Access encrypts information and makes sure that the network security key has not been modified. Wi-Fi Protected Access also authenticates users to help ensure that only authorised people can access the network.

   There are two types of WPA authentication: WPA and WPA2. WPA is designed to work with all wireless network adapters, but it might not work with older routers or access points. WPA2 is more secure than WPA, but it will not work with some older network adapters. WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. This is referred to as WPA-Enterprise or WPA2-Enterprise. It can also be used in a pre-shared key (PSK) mode, where every user is given the same passphrase. This is referred to as WPA-Personal or WPA2-Personal.

2. **Wired Equivalent Privacy (WEP)**

   WEP is an older network security method that is still available to support older devices, but it is no longer recommended. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

   It is recommended using WPA2, if possible. It is not recommend using WEP. WPA or WPA2 are more secure. If you try WPA or WPA2 and they do not work, you must upgrade the network adapter to one that works with WPA or WPA2.

3. **802.1X authentication**

   802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks. 802.1X uses an authentication server to validate users and provide network access. On wireless networks, 802.1X can work with WPA, WPA2, or WEP keys. This type of authentication is typically used when connecting to a workplace network.

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorised access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented.

Student Activity 12.1.3.6

Answer the following.

1. In the area of computing, what does network security mean?

_____

_____

_____

_____

_____

2. List at least two reasons why network security is important.

_____

_____

_____

_____

_____

_____

3. In your own words, why do we need to secure information?

_____

_____

_____

_____

_____

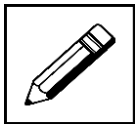
_____

_____

_____

4. Complete the needed information in the table below.

Network security method	Description	Threats that can be prevented
Cryptographic systems		
Firewall		
Intrusion Detection Systems		
Anti-Malware Software and scanners		
Secure Socket Layer (SSL)		
Wi-Fi Protected Access (WPA and WPA2)		



Summative Activity 12.1.3

Answer the following.

1. Write TRUE if the statement is correct and write FALSE if it is incorrect. Write your answers on the space provided.

    1. WPA is an older network security method that is still available to support older devices, but it is no longer recommended. _____
    2. There are two types of WPA authentication: WPA and WPA2. _____
    3. WEP encrypts information and makes sure that the network security key has not been modified. _____
    4. It was mentioned that if the intranet wanted access to the internet, virtual private networks are often used. _____
    5. Secure Socket Layer detects and reports intrusion attempts. _____
    6. The Secure Socket Layer is a standard way to achieve a good level of security between a web browser and a website. _____
    7. Firewall is an additional protection measure that helps ward off computer intrusions. _____
    8. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. _____
    9. Network security involved the use of codes and ciphers to transform information into unintelligible data. _____
    10. When considering network security, it must be emphasised that the whole network is secure. _____
    11. Data transmission that starts with authenticating, commonly with a username and a password is termed as one-factor authentication. _____
    12. When using the CSMA/CA access method, a computer transmits its intent to transmit before actually sending the data. _____
    13. When using the CSMA/CA access method, a computer waits until the network is quiet and then transmits its data. _____
    14. Managing data on a network is a form of traffic control. _____
    15. In a token passing network, there is communication only between the sending computer, the hub, and the destination computer. _____

16. In token passing, a special type of packet, called a token, circulates around a cable ring from computer to computer. _____

17. In CSMA/CD, before a host sends real data on the wire it will “sense” the wire to check if the wire is free. _____

18. In CSMA/CD (Carrier Sense Multiple Access/Collision Detection) access method, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. _____

19. Network security prevents computers from gaining simultaneous access to the cable. _____

20. Access method is the set of rules that defines how a computer puts data onto the network cable and takes data from the cable. _____

21. A network structure whose design contains more than one topology is said to be Star Topology. _____

22. In daisy topology, all hosts in this topology are connected to two hosts only, except the end hosts. _____

23. Mesh topology divides the network into multiple layers of network. _____

24. Mesh topologies involve the concept of routes. _____

25. In ring network, every computer is connected to a central device. _____

26. In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. _____

27. Daisy topology is one of the simple forms of networking where a failure of a device does not affect the others. _____

28. Point-to-point networks contain exactly two hosts where the computer or switches or routers or servers are connected back to back using a single piece of cable. _____

29. A hybrid topology is a usually schematic description of the arrangement of a network. _____

30. A Client-server configuration is preferable to peer-to-peer, especially in a small business environment where there is an expectation of growth. _____

31. Client server are easy to configure, but can be less secure than client-server networks. _____

32. Server-based network is also known as client-based network. _____

33. Client server networks are appropriate only for very small businesses or for home use. _____

34. Hosts, routers & links form the hardware side. Protocols & applications form the software side. _____

35. Data signals are computers that convert one protocol to another protocol. _____

36. Fiber Optic network cable uses light instead of electrical impulses to carry the network signal. _____

37. Fiber Optic provides the best security and integrity in data transmission at the present time. _____

38. Network interface cards are the link between your computer and the cabling to connect your computers to the other computers on the network. _____

39. The wide area network is the best-known example of a personal area network. _____

40. A wide area network is often created by joining several LANs together. _____

41. A personal area network is larger than a local area network. _____

42. It is much more convenient to use wireless connections instead of running long wires all over a building. _____

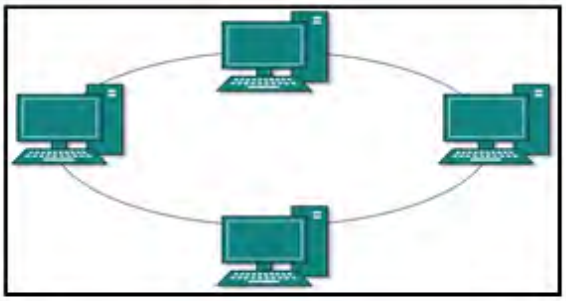
43. A wide area network connects network devices over a relatively short distance. _____

44. A personal area network is a computer network organised around an individual person within a single building. _____

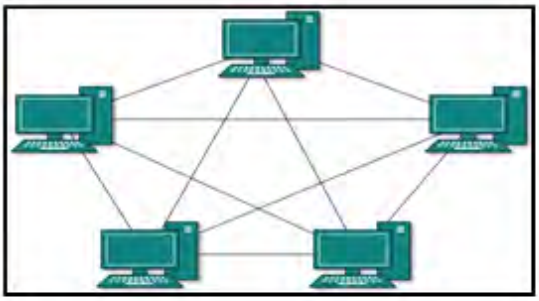
45. The quality of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. _____

2. The following are the different network topologies. Identify each topology and describe them in your own words. Write your answers on the spaces provided.

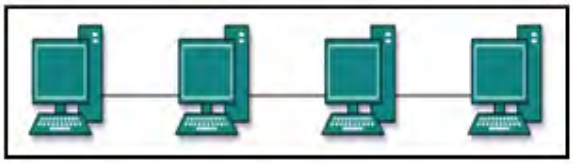
a.



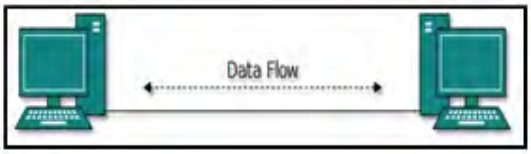
b.



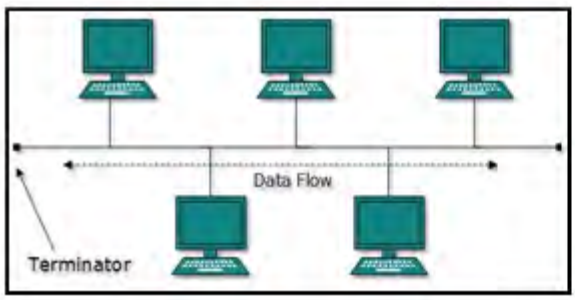
c.



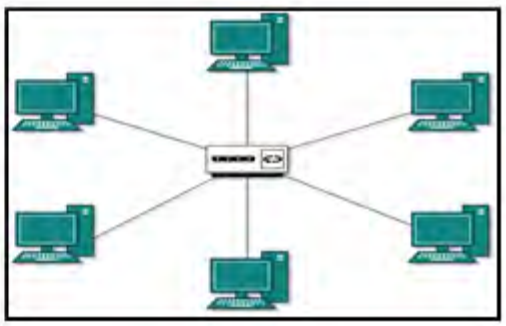
d.



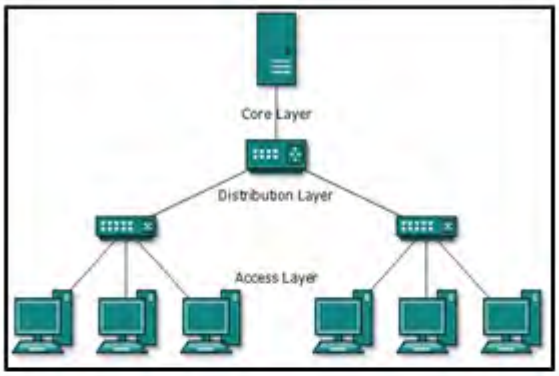
e.



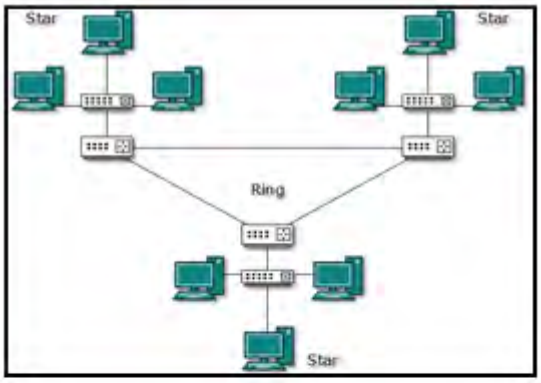
f.



g.


Core Layer
Distribution Layer
Access Layer

h.


Star
Star
Ring
Star

Answers to Student Activity 12.1.3

Student Activity 12.1.3.1

Answers may be similar to these ones below.

1.

a. Personal Area Network and Home Area Network

Comparison
Both are organised within a single building.

Contrast
PAN is organised around an individual person within a single building while HAN includes multiple individuals use the same network within a residence.

b. Local Area Network and Wireless Local Area Network

Comparison
Both are found within an office building where people share resources among themselves but not to the outside world.

Contrast
A local area network, or LAN, consists of a computer network at a single site, typically an individual office building while WLAN is a local area network, or LAN that is entirely wireless.

c. Metropolitan Area Network and Campus Area Network

Comparison
Both are within a large city, campus or small region where it can cover an area from several miles to ten of miles.

Contrast
A metropolitan area network, or MAN, consists of a computer network across an entire city, college campus or small region while a CAN is network is specifically designed for a college campus.

d. Wide Area Network and Metropolitan Area Network

Comparison
Both can operate at high speed and can cover great geographic distances.

Contrast
A WAN (Wide Area Network or extended network) connects multiple LANs to one another over great geographic distances while a MANs (Metropolitan Area

Networks) connect multiple geographically nearby LANs to one another (over an area of up to a few dozen kilometers) at high speeds.

2.

a. Document and file sharing

b. Printer sharing

c. Internet use

Student Activity 12.1.3.2

Answer can be similar to this one below.

1. There are three primary components to understanding networks: physical connections, network operating system and application component. The physical connections are the physical components which include the network topology and network connecting devices, which include network interface cards (NIC), cabling, connections, and all other hardware to connect the computers. All of these are the hardware parts. Next, in order to communicate on a network, computers must use the appropriate operating protocol selected for the network. This protocol enables the computer to exchange information and ensure correct data transmission. The network operating system (NOS) is the controlling software that enables a server to accommodate multiple clients and provide the communication network between them. Lastly, the value of networking lies in the capability of sharing up-to-date information, software and hardware resources with other users on the system which now covers the application.

2. The components of a network are important because these enable the putting up, maintenance and functioning of a network.

Student Activity 12.1.3.3

Answers may be similar to these ones below.

1.

Network	Comparison	Contrast	Example	Main Advantages	Main Disadvantages
Peer to peer	Both are kinds of networks that serve for	In a peer-to-peer network, a group of computers is connected	The small business uses one computer that is	The upside of the Peer-to-peer is that it is relatively inexpensive	it is limited in extensibility, tends to overburden user

	particular purposes	together so that users can share resources and information. There is no central location for authenticating users, storing files, or accessing resources while Server-based network, also known as client-based network has the server as the central location where users share and access network resources. The resources are located on and controlled by a central computer or the server.	running a client operating system, such as Microsoft Windows 98 or Windows XP Professional, as the designated "server" for the network.	and fairly simple to set up and manage.	workstations by having them play the role of server to other users, is largely unsecured, and is typically unable to provide system-wide services since the typical workstation will run a standard desktop operating system incapable of hosting any major service
Client-server			Client-server networks work best for larger setups, such as a full-scale office or school network especially if the networks are likely to grow in size. One should also use client-server architecture if the network has sensitive data to protect.	It can extend to handle organisational growth, allows user workstations to function as unburdened clients, can provide sophisticated system-wide services, and is configurable for maximum security.	Higher initial capital investment to establish and a greater level of technology expertise required to configure and manage, as compared to the vanilla peer-to-peer network.

2. Client-server since it can extend to handle organisational growth, allows user workstations to function as unburdened clients, can provide sophisticated system-wide services, and is configurable for maximum security.

Student Activity 12.1.3.4

The answers may be similar to these ones below.

1. The word topology means 'arrangement', so when we talk about the topology of a network, we mean how the different parts are arranged and connected together. Network Topology basically refers to layout of a network. It is how the different nodes in a network are connected to each other and how they communicate.

2.

Network Topology	Description	Example	Advantages	Disadvantages
Point to point	Point-to-point networks contain exactly two hosts where the computer or switches or routers or servers are connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other end and vice-versa.	Two computers connected by a single cable	If the hosts are connected point-to-point logically, then may have multiple intermediate devices.	But the end hosts are unaware of underlying network and see each other as if they are connected directly.
Bus	Bus topology computers are connected together to a central cable called a bus. Each computer has a short cable linking it to the 'bus'	Computers having a shared lines	The bus topology is one of the most common, and does not require as much cable as other systems; thus, it is less expensive.	The whole network stops if the main cable or bus is severed or disconnected. Limited in the number of devices due to the broadcast traffic it generates
Ring	The ring topography	Each computer is connected to a	Each host machine connects to exactly	A failure in any cable or

	connects each PC to two other PC's in a ring formation. Each PC is set up to pass data from one machine to the next in this relay type of system.	loop of cable, the 'ring'. If you took a bus network and connected the ends of the bus cable together, you would have a ring network. A ring network can cope with a break in the ring cable since all computers are still joined together.	two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.	device breaks the loop and can take down the entire network. Failure of any host results in failure of the whole ring. Thus every connection in the ring is point of failure.
Star	In a star network, all the computers are connected through a central hub to the server. All hosts in star topology are connected to a central device, known as Hub device, using a point-to-point connection.	Network every computer is connected to a central device. The device passes messages between computers.	The advantage to this system is that if one cable or computer is disconnected the entire network continues to function. This configuration is considered one of the most reliable	It uses a lot of cable. Thus, it is more expensive. If the central hub fails, the system will not function. Limited by the number of hub connection points
Mesh	Mesh topology is the type of topology where a host is connected to one or two or more than two hosts. This topology may have hosts having point-to-point connection to every other host or may also have hosts which are having point to point connection to few hosts only.	Host computer is connected to one or two or more than two hosts.	Messages sent on a mesh network can take any of several possible paths from source to destination.	

Tree	This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is divided into three types of network devices.	Multiple layers of network	All neighbouring hosts have point-to-point connection between them.	Like bus topology, if the root goes down, the entire network suffers though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment and so on.
Daisy	Daisy topology is a topology that connects all its hosts in a linear fashion.	Computers connected in a linear fashion	Connects all its hosts in a linear fashion. Similar to Ring topology, all hosts in this topology are connected to two hosts only, except the end hosts.	Each link in Daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediat e host works as relay for its immediate hosts.
Hybrid	A hybrid network is simply one that combines two or more of the basic topologies. A network that has	The combining topologies may contain attributes of Star, Ring, Bus and Daisy-chain topologies	Hybrid topology inherits merits all the incorporating topologies.	Hybrid topology inherits the demerits of all the incorporatin

	several star networks linked together is a hybrid network.			g topologies.

3. Topologies remain an important part of network design theory. One can probably build a home or small business computer network without understanding the difference between a bus design and a star design, but becoming familiar with the standard topologies gives you a better understanding of important networking concepts like hubs, broadcasts, and routes.

Student Activity 12.1.3.5

Answers may be similar to these ones below.

1. An access method is a program or a hardware mechanism that moves data between the computer and an outlying device such as a hard disk (or other form of storage) or a display terminal.

2. To access a resource is to be able to use that resource. Access methods provide an application programming interface (API) for programmers to transfer data to or from device, and could be compared to device drivers in non-mainframe operating systems.

3.

Type of access method	Description	Advantage
CSMA/CD	Using the method known as carrier-sense multiple accesses with collision detection (CSMA/CD), each computer on the network, including clients and servers, checks the cable for network traffic.	Current implementations of CSMA/CD are so fast that users are not even aware they are using a contention access method.
CSMA/CA	Carrier-sense multiple access with collision avoidance (CSMA/CA) is the least popular of the three major access methods. In CSMA/CA, each computer signals its intent to transmit before it actually transmits data.	In this way, computers sense when a collision might occur. This allows them to avoid transmission collisions.
Token passing	In the access method known as token passing, a special type of packet, called a token, circulates around a cable ring from computer to computer. When	While the token is in use by one computer, other computers cannot transmit data. Because only one

	any computer on the ring needs to send data across the network, it must wait for a free token. When a free token is detected, the computer will take control of it if the computer has data to send.	computer at a time can use the token, no contention and no collision take place, and no time is spent waiting for computers to resend tokens due to network traffic on the cable.
Demand priority	Demand priority is a relatively new access method designed for the 100-Mbps Ethernet standard known as 100VG-AnyLAN.	It is possible to implement a scheme in which certain types of data will be given priority if there is contention. If the hub or repeater receives two requests at the same time, the highest priority request is serviced first. If the two requests are of the same priority, both requests are serviced by alternating between the two.

Student Activity 12.1.3.6

Answers may be similar to these ones below.

1. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorised access, misuse, modification, or denial of a computer network and network-accessible resources.

2. List at least two reasons why network security is important.

   To avoid unauthorised access.

   To prevent potentially harmful content such as computer worms or Trojans being transmitted over the network.

3. Information must be secured as these are valuable assets of the organisation which can be misused and abused which will bring detrimental effects to the organisation if not properly guarded against unauthorised access and use.

4.

Network security method	Description	Threats that can be prevented
Cryptographic systems	Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.	Spoofing, phishing and eavesdropping
Firewall	A firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside.	Trojans, worms and viruses
Intrusion Detection Systems	An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions.	Spoofing, phishing, eavesdropping and unauthorised access
Anti-Malware Software and scanners	Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.	Trojans, worms and viruses
Secure Socket Layer (SSL)	The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website.	Create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.
Wi-Fi Protected Access (WPA and WPA2)	Wi Fi Protected Access encrypts information and makes sure that the network security key has not been modified.	Wi Fi Protected Access also authenticates users to help ensure that only authorized people can access the network.

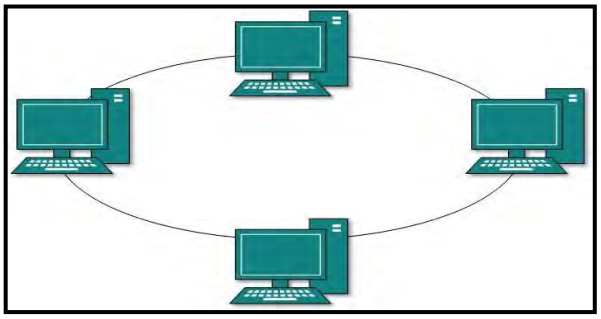
Answers to Summative Activity 12.1.3

1.

1. FALSE	11. FALSE	21. FALSE	31. FALSE	41. FALSE
2. TRUE	12. TRUE	22. TRUE	32. TRUE	42. TRUE
3. FALSE	13. FALSE	23. FALSE	33. FALSE	43. FALSE
4. TRUE	14. TRUE	24. TRUE	34. TRUE	44. TRUE
5. FALSE	15. FALSE	25. FALSE	35. FALSE	45. FALSE
6. TRUE	16. TRUE	26. TRUE	36. TRUE	
7. FALSE	17. FLASE	27. FALSE	37. FALSE	
8. TRUE	18. TRUE	28. TRUE	38. TRUE	
9. FALSE	19. FALSE	29. FALSE	39. FALSE	
10. TRUE	20. TRUE	30. TRUE	40. TRUE	

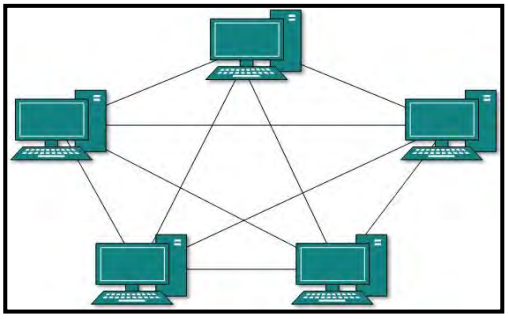
2.

a.



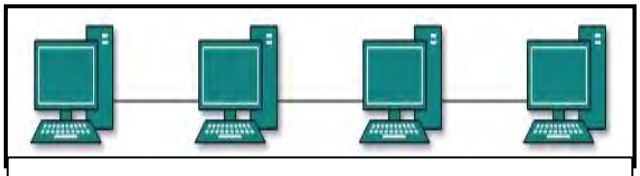
The ring topography connects each PC to two other PC's in a ring formation. Each PC is set up to pass data from one machine to the next in this relay type of system. Each computer has an in and out port.

b.



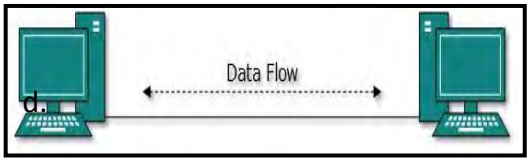
Mesh topology is the type of topology where a host is connected to one or two or more than two hosts. This topology may have hosts having point-to-point connection to every other host or may also have hosts which are having point to point connection to few hosts only.

c.



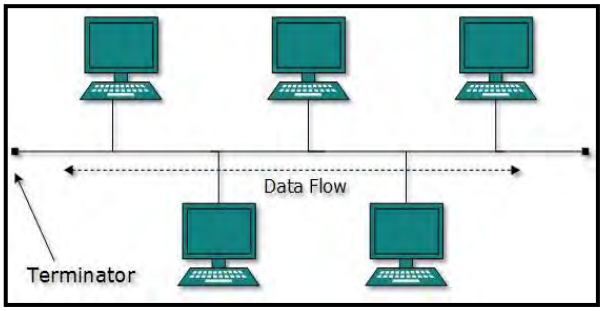
Daisy topology is a topology that connects all its hosts in a linear fashion. Similar to Ring topology, all hosts in this topology are connected to two hosts only, except the end hosts.

d.



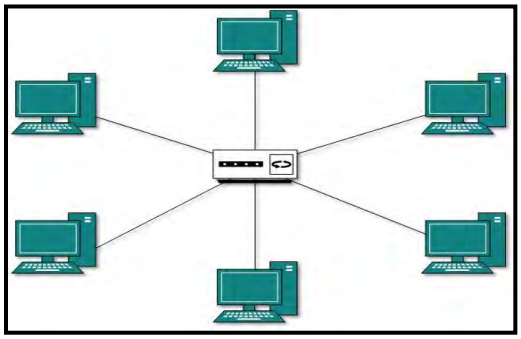
Point-to-point networks contain exactly two hosts where the computer or switches or routers or servers are connected back to back using a single piece of cable.

e.



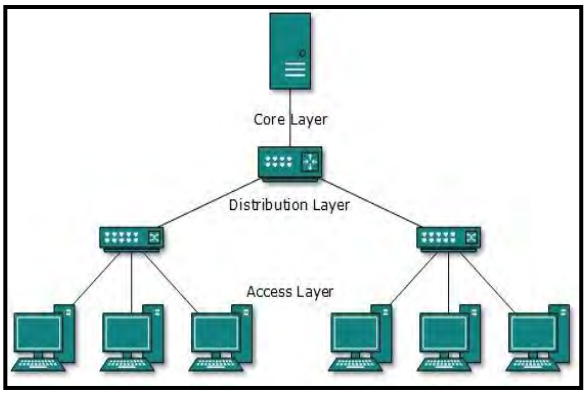
Bus topology computers are connected together to a central cable called a bus. Each computer has a short cable linking it to the 'bus'.

f.



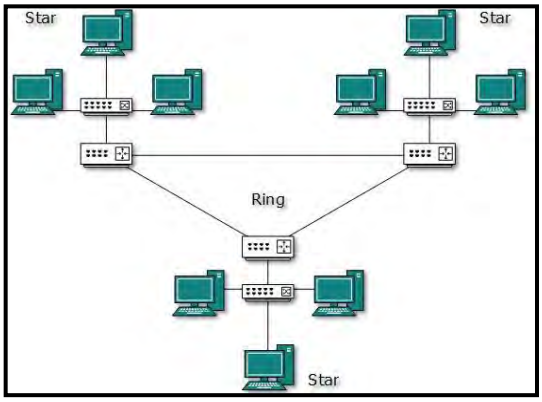
In a star network, all the computers are connected through a central hub to the server. All hosts in star topology are connected to a central device, known as Hub device, using a point-to-point connection.

g.



Tree topology is also known as Hierarchical Topology is the most common form of network topology in use present day. This topology imitates as extended Star Topology and inherits properties of Bus topology.

h.



A hybrid network is simply one that combines two or more of the above basic topologies. A network that has several star networks linked together is a hybrid network.

12.1.4 Network Software

12.1.4.1 Network Operating Systems

A network operating system (NOS) is a computer operating system that is designed primarily to support workstation and personal computer. It includes special functions for connecting computers and devices into a local-area network (LAN). Artisoft's LANtastic, Banyan VINES, Novell's NetWare, and Microsoft's LAN Manager are examples of network operating systems. In addition, some multi-purpose operating systems, such as Windows NT and Digital's OpenVMS come with capabilities that enable them to be described as a network operating system. Also, some operating systems, such as UNIX and the Mac OS, have networking functions built in.

The term network operating system is generally reserved for software that enhances a basic operating system by adding networking features. It refers to software that implements an operating system of some kind that is oriented to computer networking. For example, one that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions. It is further designed to allow shared file and printer access among multiple computers in a network, a local area network (LAN), a private area network or to other networks.

Depending on a network operating system's manufacturer, a desktop computer's networking software can be either added to the computer's own operating system or integrated with it.

Novell's NetWare is the most familiar and popular example of NOS in which the client computer's networking software is added on to its existing computer operating system. The desktop computer needs both operating systems in order to handle stand-alone and networking functions together.

The salient features of network operating systems are:

1. Basic operating system features support like protocol support, processor support, hardware detection and multiprocessing support for applications which also maintains the network connection to the server(s).

2. Security features like authentication, restrictions, authorisations and access control which deals with users logging on.

   - Features for file, Web service, printing and replication

3. Directory and name services management which also provides security to separate user accounts from each other.

4. User management features along with provisions for remote access and system management which expands the file system to view folders on other computers

- Internetworking features like routing and WAN ports
- Clustering capabilities

The following are some types of network operating systems. Let us study each in detail.

1. **Real-time**

   A real-time operating system is a multitasking operating system that aims at executing real-time applications. Real-time operating systems often use specialised scheduling algorithms so that they can achieve a deterministic nature of behaviour. The main objective of real-time operating systems is their quick and predictable response to events. They have an event-driven or time-sharing design and often aspects of both. An event-driven system switches between tasks based on their priorities or external events while time-sharing operating systems switch tasks based on clock interrupts.

   Time-sharing operating systems schedule tasks for efficient use of the system and may also include accounting software for cost allocation of processor time, mass storage, printing, and other resources.

2. **Multi-user**

   A multi-user operating system allows multiple users to access a computer system at the same time. Time-sharing systems and Internet servers can be classified as multi-user systems as they enable multiple-user access to a computer through the sharing of time. Single-user operating systems have only one user but may allow multiple programs to run at the same time.

   Unlike single tasking, a multi-tasking operating system allows more than one program to run at the same time, from the point of view of human time scales. A single-tasking system has only one running program**.**

   Multi-tasking can be of two types: pre-emptive and co-operative. In pre-emptive multitasking, the operating system slices the CPU time and dedicates one slot to each of the programs. Unix-like operating systems such as Solaris and Linux support pre-emptive multitasking, as does Amiga OS. Multi-tasking will be discussed further in our next lesson on network operating system tasks.

   Cooperative multitasking is achieved by relying on each process to give time to the other processes in a defined manner. 16-bit versions of Microsoft Windows use the cooperative multi-tasking. Let us take note that the 32-bit versions of both Windows NT and Win 9x, are using the pre-emptive multi-tasking. Mac OS prior to OS X used to support cooperative multitasking.

3. **Distributed**

   A distributed operating system manages a group of independent computers and makes them appear to be a single computer. The development of networked computers that could be linked and communicate with each other gave rise to distributed computing. Distributed computations are carried out on more than one

machine. When computers in a group work in cooperation, they make a distributed system.

4. **Templated**
   Gagne (2012) mentioned that in an o/s, distributed and cloud computing context, templating refers to creating a single virtual machine image as a guest operating system, then saving it as a tool for multiple running virtual machines. The technique is used both in virtualisation and cloud computing management, and is common in large server warehouses. In computing, **virtualization** refers to the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, operating systems, storage devices, and computer network resources.

5. **Embedded**
   Embedded operating systems are designed to be used in embedded computer systems. They are designed to operate on small machines like PDAs with less autonomy. They are able to operate with a limited number of resources. They are very compact and extremely efficient by design. Windows CE and Minix 3 are some examples of embedded operating systems.

The list of network operating systems includes Artisoft's LANtastic, Banyan VINES, Novell's NetWare and Microsoft's LAN Manager. Some of the main functions of a network operating system are printer sharing, common file systems, database sharing, application sharing, managing network name directory and the ability to do housekeeping for the network's system. Let us study each in detail.

1. **Artisoft's LANtastic**
   LANtastic supports a wide variety of PC operating systems like Windows NT 4.0/2000/2003 (Workstation and/or Server), and Windows XP. It comes with an enhanced multi-platform support. The installation and operation of the system is fast and user friendly, along with an improved interface that allows all networked PCs to be able to communicate by just using the Chat feature. Users are not required to employ a dedicated server or a full-time network manager because the system is simple and easy to maintain.

2. **Banyan VINES**
   Banyan Virtual Integrated Network Service (VINES) is a network operating system based on proprietary protocol family. The protocol is basically derived from Xerox Network Systems (XNS) protocols, where it uses a client-server architecture that enables clients to request specified services like file and printer access from servers.

3. **Novell's NetWare**
   This network operating system is a protocol suite designed based on the XNS protocol architecture. It provides comprehensive support to most of the desktop operating systems in the market, including DOS, Windows, Macintosh, OS/2 and UNIX. Novell also supports the local area networks and asynchronous wide area communications.

4. **Microsoft's LAN Manager**
   LAN Manager is a network operating system by Microsoft that works as a server application. It runs under Microsoft OS/2, and was developed in conjunction with 3Com. The file server may concurrently be used for other tasks like database services. In other words, the system provides a good multi-tasking function. It also supports most desktop operating systems like DOS, Windows and OS/2 clients. Currently, the LAN Manager feature has been superseded by Microsoft Windows NT Server and most parts of the LAN Manager are being used in the Windows NT and Windows 2000.

Unlike operating systems, such as Windows that are designed for single users to control one computer network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly. The two types of network operating systems are either peer-to-peer or client server which we have discussed in our previous discussions. Nearly all modern networks are a combination of both. The networking design can be considered independent of the servers and workstations that will share it.

In our previous discussion of planning and designing an information system, we saw that network planning decisions must take into account the services and resources expected or required of the network. Those resources, and how they are shared and accessed, are determined by the network operating system.

In planning a network, the choice among network operating systems can be narrowed significantly if you first determine which network architecture whether it is a client/server or peer-to-peer that would best meet your needs. This choice can often be made by deciding which kinds of security are called for. Server-based networking allows you to include security capabilities well beyond those available to a peer-to-peer network. If security is not an issue, a peer-to-peer networking environment might be appropriate.

After your network security needs have been identified, the next step is to determine the kinds of interoperability necessary for the network as a whole. Each network operating system (NOS) addresses interoperability in different ways, so one should keep his interoperability needs in mind when evaluating each NOS. If the network choice is peer-to-peer, the options for security and interoperability will be diminished because of the limitations inherent in that architecture. If the network choice is server-based, further assessment is needed to determine whether interoperability will be dealt with as a service on the network server or as a client application on each networked computer. Server-based interoperability is easier to manage because, like other services, it is centrally located; client-based interoperability requires installation and configuration at each computer, making interoperability much more difficult to manage.

It is not uncommon to find both methods which are a network service on the server and network client applications at each computer in a single network. For example, a NetWare server is often implemented with a service for Apple computers, whereas Microsoft Windows network interoperability is achieved with a network client application at each personal computer.

When choosing a network operating system, first determine the networking services that will be required. Standard services include security, file sharing, printing and messaging; additional services include interoperability support for connections to other operating systems. For any given NOS, determine which interoperability services or networking clients are best implemented to suit the needs.

In a nutshell, we can say that first, without a network operating system of some kind, individual computers cannot share resources, and other users cannot make use of those resources. Second, a network operating system can be part of a computer operating system or a separate application that runs on top of the computer operating system. Third, Windows NT is an example of an operating system that incorporates both computer and network operating systems in one system. Fourth, by multitasking, computers can perform more than one task at a time. Lastly, the first step in choosing a network operating system is to decide which network architecture whether it is server-based or peer-to-peer- best meets the needs which can often be accomplished by determining what level of security the network requires.

Student Activity 12.1.4.1

Answer the following.

1. Define an operating system.

_____

_____

_____

_____

2. Complete the needed information in the table below.

Network Operating System	Description	Advantage
Microsoft's LAN Manager		
Novell's NetWare		

Banyan VINES		
Artisoft's LANtastic		

3. List down the importance of a network operating system.

_____

_____

_____

_____

_____

12.1.4.2 Network Operating Systems Tasks

We have previously learned that just as a computer cannot operate without a computer operating system, a network of computers cannot operate without a network operating system. Without a network operating system of some kind, individual computers cannot share resources, and other users cannot make use of those resources.

All network operating systems (NOS), from the simplest to the most complex, must provide certain core functions. It is the most fundamental of all system software programs. It is an operating system designed for the sole purpose of supporting workstations, database sharing, and application sharing and file and printer access sharing among multiple computers in a network. Hence, a network operating system provides printer sharing, common file system and database sharing, application sharing, and the ability to manage a network name directory, security, and other housekeeping aspects of a network.

Network operating system tasks are the services provided by a network operating system. These are its core function. Generally, the common tasks associated with network operating systems include:

- User administration
- System maintenance activities like backup
- Tasks associated with file management
- Security monitoring on all resources in the network
- Setting priority to print jobs in the network

Specifically, let us look into its tasks of support and file sharing. Study the following discussions below.

On network support, network operating systems (NOS) must support a wide variety of networking protocols in order to meet the needs of its users. That is because a large network typically consists of a mixture of various versions of Windows, as well as a few scattered Macintosh (mostly in the art department) and possibly some Linux computers. The computers often have distinct protocols.

Many servers have more than one network interface card installed. In that case, the NOS must be able to support multiple network connections. Ideally, the NOS should have the ability to balance the network load among its network interfaces. In addition, in the event that one of the connections fails, the NOS should be able to seamlessly switch to another connection.

Finally, most network operating systems include a built-in ability to function as a router that connects two networks. The NOS router functions should also include firewall features in order to keep unauthorised packets from entering the local network.

While on file-sharing services, one of the most important functions of a network operating system is its ability to share resources with other network users. The most common resource that is shared is the server's file system. A network server must be able to share some or all of its disk space with other users so that those users can treat the server's disk space as an extension of their own computers' disk spaces.

The NOS allows the system administrator to determine which portions of the server's file system to share. Although an entire hard drive can be shared, it isn't commonly done. Instead, individual directories or folders are shared. The administrator can control which users are allowed to access each shared folder.

Because file sharing is the reason many network servers exist, network operating systems have more sophisticated disk management features than are found in desktop operating systems. For example, most network operating systems have the ability to manage two or more hard drives as if they were a single drive. In addition, most can create mirrors, which automatically keep backup copies of drives on a second drive.

A computer's operating system coordinates the interaction between the computer and the programs or applications which it is running. It controls the allocation and use of hardware resources such as:

- Memory
- CPU time
- Disk space
- Peripheral devices

In a networking environment, servers provide resources to the network clients, and client network software makes these resources available to the client computer. The network and the client operating systems are coordinated so that all portions of the network function properly.

A multitasking operating system, as the name suggests, provides the means for a computer to process more than one task at a time. A true multitasking operating system can run as many tasks as there are processors. If there are more tasks than processors, the computer must arrange for the available processors to devote a certain amount of time to each task, alternating between tasks until all are completed. With this system, the computer appears to be working on several tasks at once.

There are two primary forms of multitasking:

a. Pre-emptive- In pre-emptive multitasking, the operating system can take control of the processor without the task's cooperation.

b. Non-pre-emptive (cooperative)- In non-pre-emptive multitasking, the task itself decides when to give up the processor. Programs written for non-pre-emptive multitasking systems must include provisions for yielding control of the processor. No

other program can run until the non-pre-emptive program has given up control of the processor.

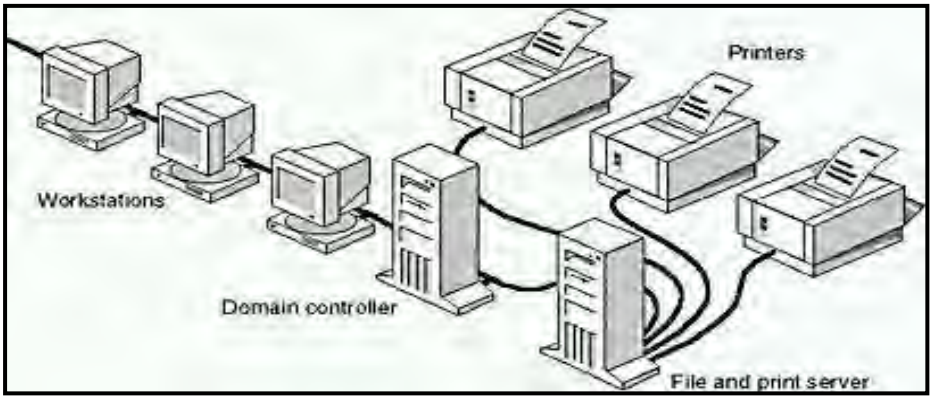
Because the interaction between the stand-alone operating system and the NOS is ongoing, a pre-emptive multitasking system offers certain advantages. For example, when the situation requires it, the pre-emptive system can shift CPU activity from a local task to a network task.

For computer operating systems that do not include networking functions, network client software must be installed on top of the existing operating system. Other operating systems, such as Windows NT, integrate the network and the computer operating systems. While these integrated systems have some advantages, they do not preclude using other NOSs.

When setting up multivendor network environments, it is important to consider the issue of interoperability. Elements or components of computer operating systems are said to "interoperate" when they can function in different computer environments. A NetWare server, for instance, can interoperate with other servers such as Windows NT, and users of Apple computers can interoperate with that is, access resources on both NetWare and Windows NT servers.

A network operating system such as the one shown in the figure below does the following tasks:

- Ties together all computers and peripherals.
- Coordinates the functions of all computers and peripherals.
- Provides security by controlling access to data and peripherals.

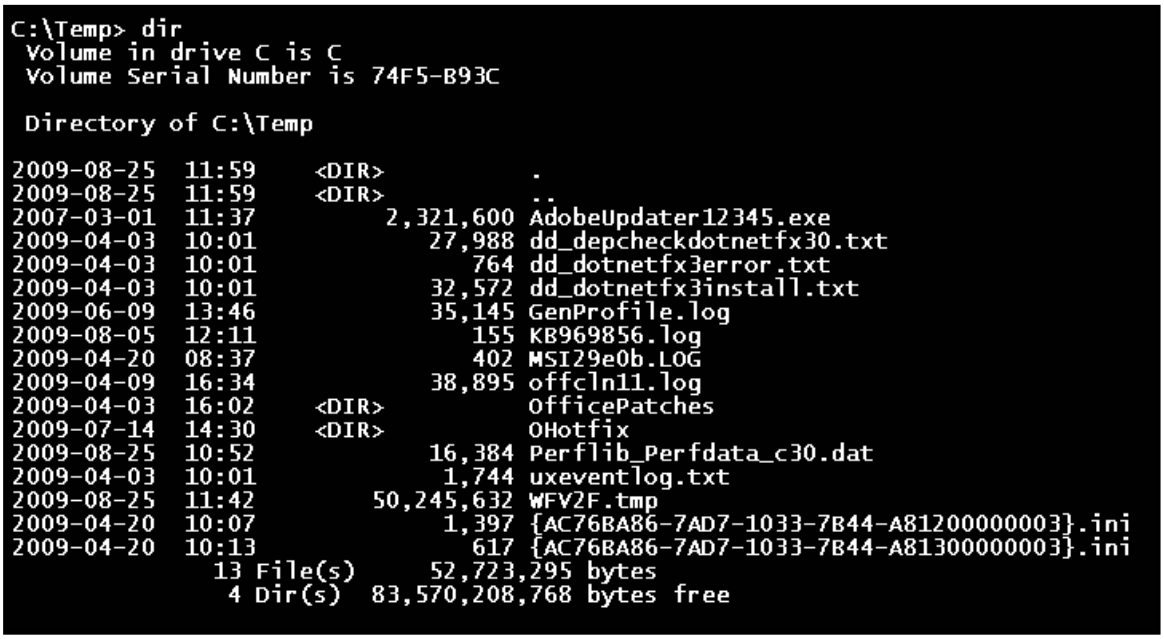


A representation of how a network server ties the network together

As mentioned, the two major types of network software are:

- Network software that is installed on clients.
- Network software that is installed on servers.

In client software where there exists a stand-alone system, when the user types a command that requests the computer to perform a task, the request goes over the computer's local bus to the computer's central processing unit (CPU). The figure below shows this. For example, if you want to see a directory listing on one of the local hard disks, the CPU



interprets and executes the request and then displays the results in a directory listing in the window.

A representation of a directory listing request on a local hard disk

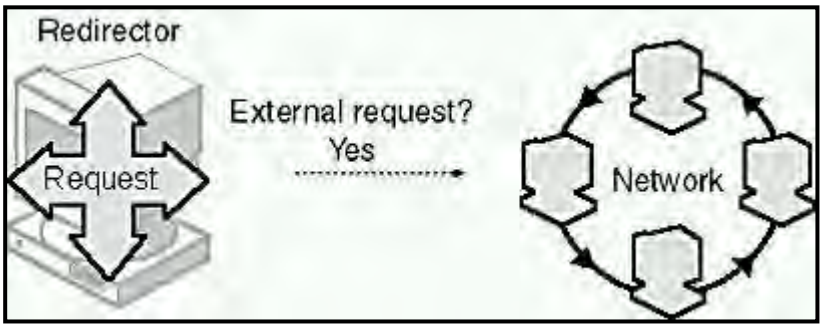
In a network environment, however, when a user initiates a request to use a resource that exists on a server in another part of the network, the request has to be forwarded, or redirected, away from the local bus, out onto the network, and from there to the server with the requested resource. This forwarding is performed by the redirector.

A redirector processes forwarding requests. Depending on the networking software, this redirector is sometimes referred to as the "shell" or the "requester." The redirector is a small section of code in the NOS that does the following:

- Intercepts requests in the computer.
- Determines if the requests should continue in the local computer's bus or be redirected over the network to another server.

Redirector activity originates in a client computer when the user issues a request for a network resource or service. The figure on the next page shows how a redirector forwards requests to the network. The user's computer is referred to as a client because it is making a request of a server. The request is intercepted by the redirector and forwarded out onto the network.

The server processes the connection requested by client redirectors and gives them access to the resources they request. In other words, the server services or fulfils the request made by the client.

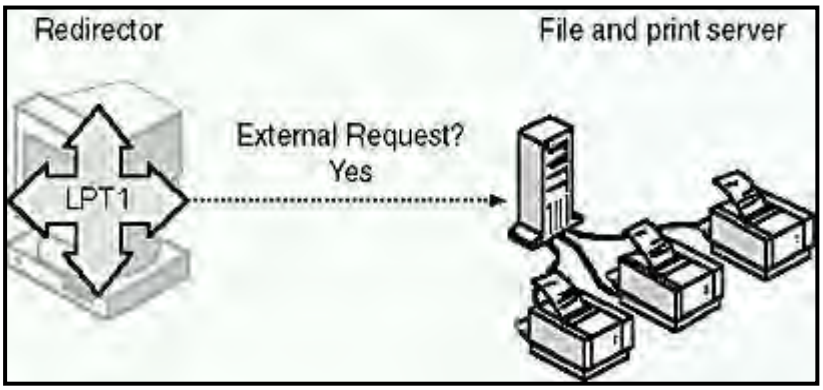


A representation of the redirector forwards requests for remote resources onto the network

Moreover, if you need to access a shared directory, and you have permission to access it, your operating system will usually provide several choices for how to access the directory. For example, with Windows NT you could use Windows Explorer to connect to the network drive using the Network Neighbourhood icon. You can also map to the drive. Drive mapping is the assignment of a letter or name to a disk drive so that the operating system or network server can identify and locate it. To map to the drive, right-click the directory icon from the Network Neighbourhood; a dialogue box will prompt you to assign an available letter of the alphabet as a drive designator, such as G:. Thereafter, you can refer to the shared directory on the remote computer as G:, and the redirector will locate it. The redirector also keeps track of which drive designators are associated with which network resources.

Redirectors can send requests to peripherals as well as to shared directories. The figure below depicts the redirector on a local computer sending a request to a print server. The request is redirected away from the originating computer and sent over the network to the target. In this case, the target is the print server for the requested printer.

With the redirector, LPT1 or COM1 can refer to network printers instead of local printers. The redirector will intercept any print job going to LPT1 and forward it out of the local machine to the specified network printer.

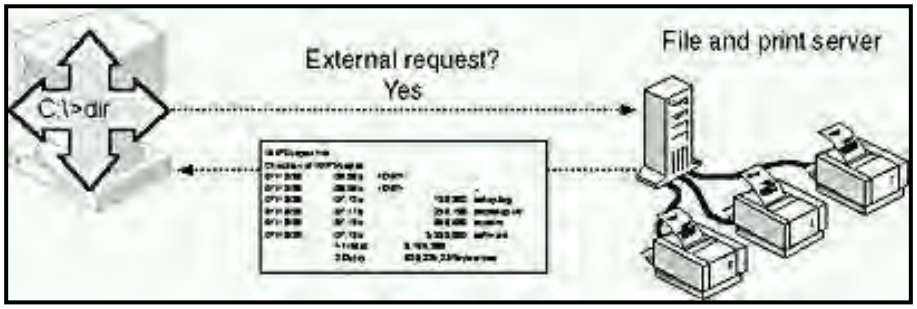


A representation of a request to print redirected out LPT1 to a printer on the network

Using the redirector, users do not need to be concerned with the actual location of data or peripherals, or with the complexities of making a connection. To access data on a network

computer, for example, a user need only type the drive designator assigned to the location of the resource, and the redirector determines the actual routing.

With server software, users at other machines, the client computers, can share the server's data and peripherals including printers, plotters, and directories. From the figure below, it is showing a user requesting a directory listing on a shared remote hard disk. The request is forwarded by the redirector on to the network, where it is passed to the file and print server containing the shared directory. The request is granted, and the directory listing is provided.



A representation of a directory-listing request on a remote hard drive

Sharing is the term used to describe resources made publicly available for access by anyone on the network. Most NOSs not only allow sharing, but also determine the degree of sharing. Options for sharing include:

- Allowing different users different levels of access to the resources.
- Coordinating access to resources to make sure that two users do not use the same resource at the same time.

For example, an office manager wants everyone on the network to be familiar with a certain document or file, so she shares the document. However, she controls access to the document by sharing it in such a way that:

- Some users will be able only to read it.
- Some users will be able to read it and make changes in it.

Network operating systems also allow a network administrator to determine which people, or groups of people, will be able to access network resources. A network administrator can use the NOS to:

- Create user privileges, tracked by the network operating system, that indicate who gets to use the network.
- Grant or deny user privileges on the network.
- Remove users from the list of users that the network operating system tracks.

To simplify the task of managing users in a large network, NOSs allow for the creation of user groups. By classifying individuals into groups, the administrator can assign privileges to the

group. All group members have the same privileges, which have been assigned to the group as a whole. When a new user joins the network, the administrator can assign the new user to the appropriate group, with its accompanying rights and privileges.

Some advanced NOSs include management tools to help administrators keep track of network behaviour. If a problem develops on the network, management tools can detect signs of trouble and present these in a chart or other format. With these tools, the network manager can take corrective action before the problem stops the network.

In a nutshell, the basic purpose of a network operating system or NOS is that it controls the accesses of files from multiple users. It is used to run the computers that are to act as servers so that they can carry out all the functions for the network. It supports the hardware and also ensures the security by authentication procedures while logging in, restrictions as to who can and cannot access the system and the authorisation access to various locations in the system. It also provides directory services, replication, storage, printing and remote access.

Hence, we can summarise that a network operating system provide the following functions:

- For installed components: client functionality and server functionality
- For functions provided: account administration for users, security file and print sharing
- For network services: file sharing, print sharing, user administration and backing up data

Student Activity 12.1.4.2

Answer the following.

1. What is a network operating system task?

_____

_____

_____

_____

_____

_____

_____

_____

2. Identify three network operating system tasks.

a. _____

b. _____

c. _____

3. Explain the following network operating system tasks.

- file sharing

_____

_____

_____

_____

- print sharing

_____

_____

_____

- user administration

_____

_____

_____

- backing up data

_____

_____

_____

12.1.4.3 Log-on and Log-off Procedures

We have discussed thoroughly what a network operating system (NOS) is and its functions. We can say now that the NOS is indispensable on how a network functions because when the user logs on. In logging in, the users will provide a username and password. This is checked by the operating system.

With a network operating system, the user will have access to a network drive where his files and folders will be stored. The user will usually also have accesses to a shared drive where he can use and share files with other people on the network. These drives appear as extra letters, perhaps D drive or S drive. As far as the user is concerned, as a network user, they are appearing to be an extension of his local hard disk.

The user can read and write to the folders as if they are on his own machine. This is possible as long as the network administrator has set up his file permissions to allow him to do this. Log in is a procedure of accessing a network by a user to use and share files with other people in the network while log off is the procedure where the user exits the network.

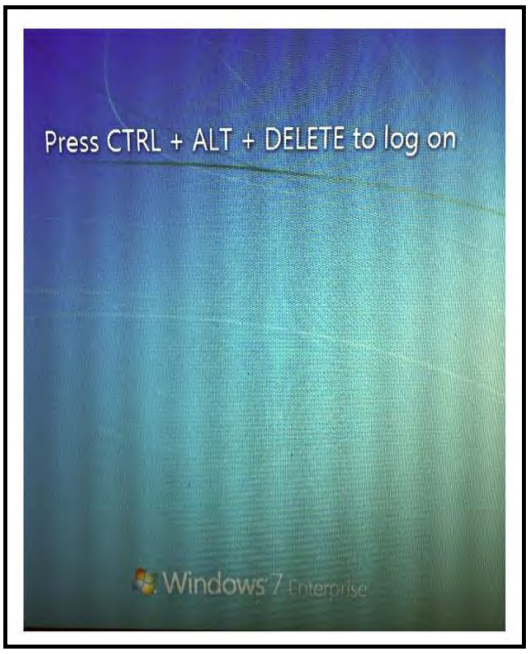
There may be many users making use of the same machine but not at the same time. Think about the computers at school. Students might use a computer in room A for their ICT lesson. They log off, and the next class arrives and a different student logs onto the same computer. This happens many times throughout the week. This is not a multi-user system, because the processing power of the machine is only being used by one person at a time.

Discussing specifically now, the log in and log out procedures in a network would vary depending on how the administrator had set it up for the network users. But basically, the procedures below are comparative for all network users.

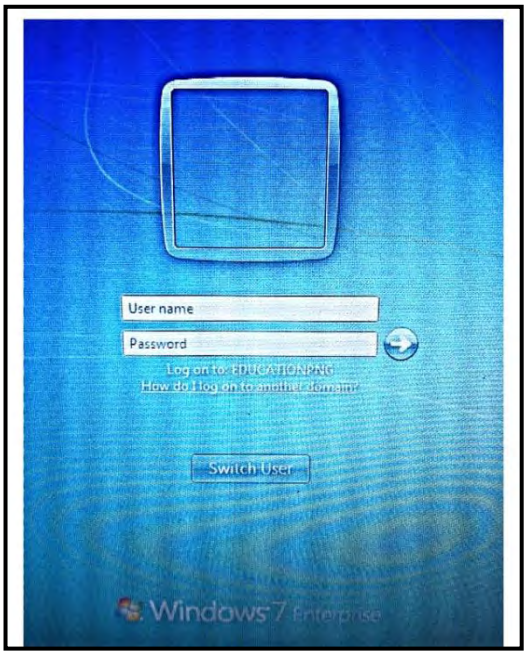
In logging in, the user will have his login name where it can be a username (Jdoe), user name (J Doe), or user id (jd1721) which will be in the form of <first initial>+<last name>. For example, the username for John Doe will be jdoe. Usernames are not case sensitive. However, it is the passwords which are case sensitive.

The picture on the next page shows an example of a computer screen before a user can log into the computer.

1



2



Screenshots on how the computer screen will look like before a user can log on the computer

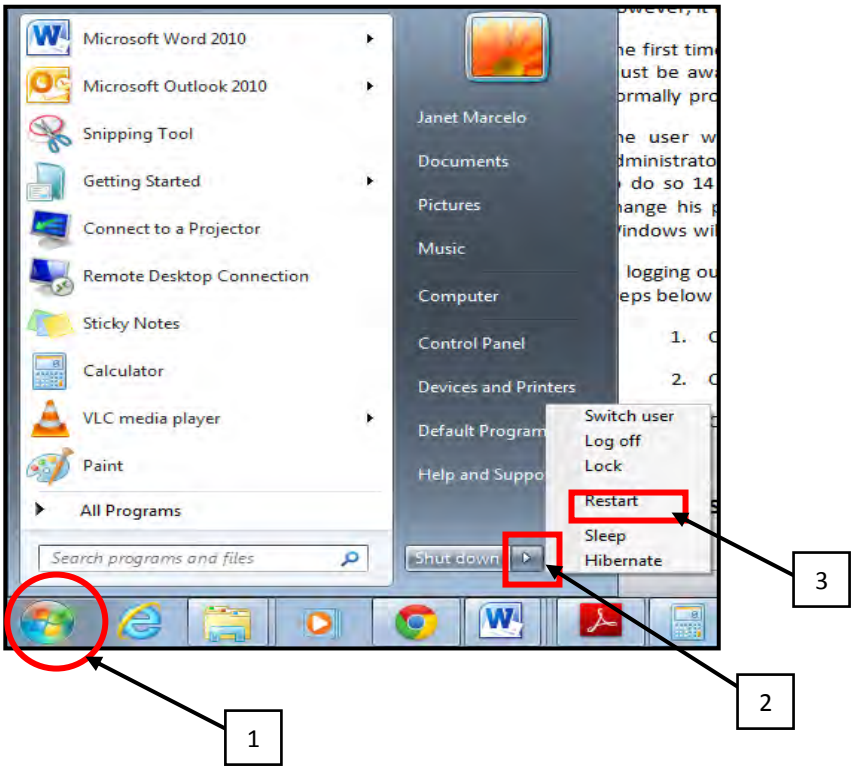
The first time the user logs into his workstation he will be prompted to enter a password. He must be aware of the existing password policy guide in choosing a secure password which is normally provided by the administrator.

The user will be prompted every month or every six months, depending on how the administrator had set it up, to change his password. The user normally receives a reminder to do so fourteen days or so before the current password expires. The user must make sure to change his password during the fourteen days grace period. After the fourteen days grace period or so, Windows will require that you change your password before allowing the user to proceed.

In logging out, the user must restart the computer at the end of his everyday use. Follow the steps below on how to restart a Windows computer:

1. Click on **Start** button.
2. Click on the arrow next to Shut down.
3. Click on **Restart**.

Study the picture below.



In summary, logging in provides the user the opportunity to connect to a network and use its services while logging off enables the user to exit temporarily from the network connection.

Student Activity 12.1.4.3

Answer the following.

1. Define the following in your own words.

   a. Log in

   _____

   _____

   _____

   _____

   b. Log off

   _____

   _____

   _____

   _____

2. Describe the process of logging in and logging out.

Logging in

_____

_____

_____

_____

_____

_____

_____

Logging out

_____

_____

_____

_____

_____

_____

_____

3. What is the importance of logging in and logging out?

_____

_____

_____

_____

_____

_____

_____

12.1.4.4 Antivirus Software and Firewall

It has been mentioned in the lesson discussions in Grades 9 and 10 Design and Technology Computing and reiterated in Grade 11 Information Communication Technology topic module discussion and previously in our discussions on networking what antivirus and firewalls are with their functions and importance.

The two play a significant role in computer and data protection as much as security is concerned. More so that in networking as we have discussed, it is prone to multiple threats and attacks caused by unwanted and unauthorised users.

Let us study them once again to identify their differences and importance in networking security.

Whenever, a computer is connected to the Internet, it is communicating with other computers, which means it can potentially be subjected to attack from malicious programs such as viruses, Trojans and spyware. Antivirus and Firewall software are two different methods of protecting the computer from infectious malicious software. These two are types of internet security programs that can help limit the chances that a computer becomes infected.

Firewall and antivirus software are both designed to protect an individual's computer system from invasion and assault.

A firewall is set up to block access from unwanted network communications, often including both incoming and outgoing messages. It comes built in but can also be added separately and works to make networks secure from malicious software to enter the computer using a network connection. Antivirus works by scanning the computer to detect and remove already infected files and also prevents from viruses from affecting any files.

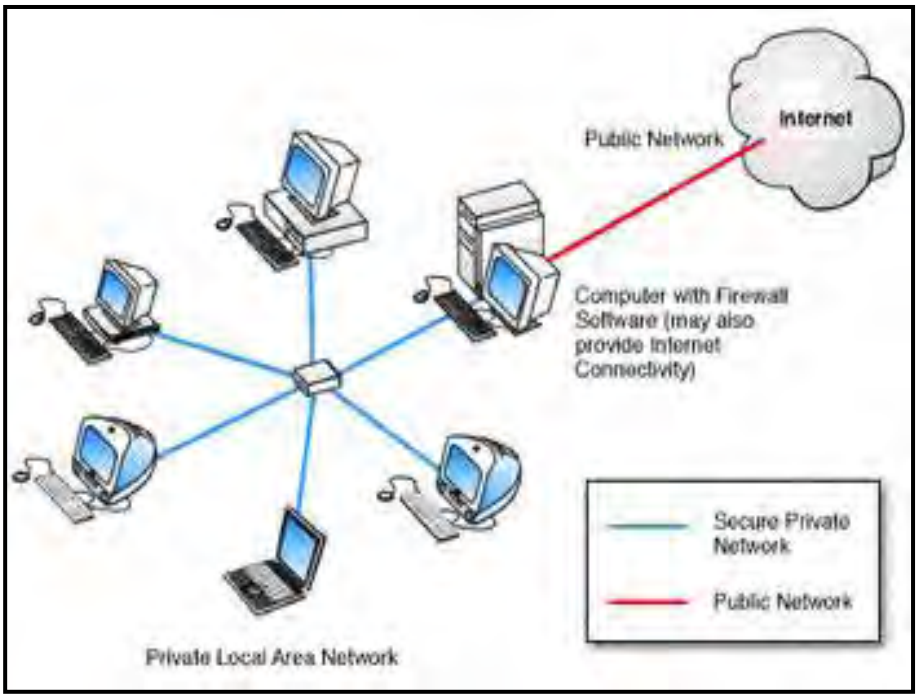
Almost everything can be found online and it has also become the best place to target people for personal information. There are many different malware that are looking out to harm the computer system or collect private data about the user. There are built in software and programs that can protect the user’s system. These are known as Antivirus and Antimalware software.

Antivirus or anti-virus software is software that is used to prevent viruses from entering the computer system and infecting files. Many antivirus programs these days like the AVG, Avira and Norton also eliminate different kinds of malware in addition to viruses. The main purpose of antivirus software is to scan, detect, prevent and remove many different kinds of software. The software employs a variety of strategies to detect viruses including searching for known patterns of data within executable code. However, the computer is still vulnerable to new types of viruses that may use different codes. Antivirus programs are software packages designed to scan the registry and files on the computer itself for the activity of malicious programs, and then attempt to remove any threats it finds. Antivirus programs can actively search and destroy threats, and have virus definitions that can allow them to identify specific threats.

Antivirus software is designed to deal with maliciously designed programs that find their way onto a person's computer. Firewall and antivirus software are often distributed together as part of a single software package, and because of the nature of some network threats, they often work together to protect a person's system in different ways from the same menaces.

Viruses are constantly changing as malicious programmers come up with new ways to corrupt computer systems, and antivirus software has to change along with the threats. Most antivirus applications are designed to monitor running programs for new threats, and usually the user can run a scan for infected files, removing any that are found. Sometimes a new virus will be developed that the program does not recognise. Most antivirus applications are set up for daily or weekly updates to the core program that help expand capabilities and allow for the recognition of new threats.

In order to counter this, many antivirus programs use heuristics, which is a technique that is designed to solve a problem more quickly than a classic method. This is done by creating an approximate solution when the classical solution fails. Initially, only executable files were corrupted or infected with viruses but with the new viruses, many files could also become infected requiring antivirus programs to manually search all files and folders that are available in the system. There are also drawbacks to having antivirus programs such as false-positive. This is when the antivirus program detects a non-malicious file as a virus and deletes it from the system. If the file is an important file, it could cause the operating system to stop working or certain applications to crash. Hence, files should be reviewed before they are deleted from the system.



An illustration of a secure private network and a public network where firewall helps in security

Firewall software is software that controls the incoming and outgoing network traffic by analysing the number of data packets that is sent. Firewall is a hardware based network security system that works based on a rule set. A firewall is like the fence built around the

house of your computer or network. It basically monitors traffic going in and out of the network and stops suspicious traffic from entering or leaving.

As previously mentioned, there are two main kinds of firewalls, software and hardware. Most computers come with software firewalls, such as Windows Firewall in Windows XP, Vista and 7, which makes them a quick and easy firewall solution. A hardware firewall is installed between the internet and the rest of the network, so your entire network is protected, regardless of whether or not each individual computer has firewall software installed. Today, most routers include firewall capabilities and would be a basic example of a hardware firewall.

Moreover, firewalls are programs that attempt to block threats and unwanted access to a network. A network protected by a firewall will have to pass data entering or leaving the network through the firewall, and if it does not meet the firewall's security standards, the message will be blocked. A firewall can be thought of as a screen or sieve that categorically strains out potentially harmful data.

The term firewall was originally used to describe a wall that is responsible for confining a fire to one particular room or building. This terminology was later adapted to refer to the current firewall technology that we have. Firewall software is designed to protect against unwanted network communication on a computer. Malicious individuals sometimes try to access other people's systems through a network connection in order to gain access to an individual's private information or install malicious software. Firewall programs can recognise unauthorised communications and block them. Sometimes the software is set up with specific rules about what sort of communication is allowed, and in other cases, the rules may be user-defined with different levels of security for different situations.

In many cases, firewall and antivirus software packages can often be very complimentary in the way that they function. For example, many viruses are designed so that they try to send messages out to the Internet; distributing private information about a person's browsing habits along with credit card numbers and other data to malicious individuals. A good firewall will recognise these sorts of attempts and block them, which can be helpful in cases where the virus is too new to be recognised by the antivirus program. Another situation where firewall and antivirus software can work in tandem is when malicious individuals attempt to access a system through the network for the purposes of implanting a virus. In these cases, if someone finds a way through the firewall, the antivirus software can serve as backup protection.

In summary, firewalls and antivirus software are important components of Internet safety. Firewalls are used to limit incoming transmissions to those that are least likely to contain bad data, while antivirus programs actually look at the effect that the incoming data has on the system. Firewalls cannot be used to remove threats if they happen to get past the firewall. Moreover, antivirus or anti-virus software is software that is used to prevent viruses from entering the computer system and infecting files. Many antivirus programs these days also eliminate different kinds of malware in addition to viruses. Firewall software is software that controls the incoming and outgoing network traffic by analysing the number of data packets that is sent. Firewall is a hardware based network security system that works based on a rule set. It works to protect between private and public networks.

Student Activity 12.1.4.4

Answer the following.

1. Define the following terms in your own words.

   a. Anti-virus software

   _____

   _____

   _____

   b. Firewall

   _____

   _____

   _____

2. List down two differences between an anti-virus software and a firewall.

   a. _____

   _____

   _____

   b. _____

   _____

   _____

3. What is the importance of a firewall and anti-virus software?

   _____

   _____

   _____

   _____

12.1.4.5 General Purpose Software

In Grade 9 Design and Technology-Computing Unit 1 Topic 4, software was introduced and along with it came the discussions on utility software, software packages and custom software. From these, the general purpose software was introduced.

Software is the detailed instructions used to direct the hardware to perform a particular task. It controls the processing and movement of data within a computer system. A computer needs software to tell it what to do and it needs hardware to carry out the actual work. There are two main types of software known as system software and application software.

Application software is a program used for a specific task. It allows the computer to achieve the task for which it was bought. Application software consists of software packages and custom software.

A software package which is also called as general purpose software is a complete and documented set of programs supplied to several users. Software packages can be bought to cover nearly all requirements. They include word processing, desktop publishing, spreadsheets, database management systems, paint programs, draw programs, web browsers, video editing software, animation software, presentation software and authoring software.

Now, let us discuss more on general software as an important application for computers in a network.

General purpose software normally refers to the types of software used by computer operators to perform simple tasks, including writing, data recording and presentations. This software is some of the most commonly used software as it performs a variety of tasks, making it very beneficial to the user. It is sometimes known as ‘off-the-shelf’ (pre-written software purchased by a customer) as it is the sort of software that you use at home and school.

The following are of the general software and their uses:

- Word processing application is for writing reports, memos and letters
- Spreadsheet application is for keeping simple company accounts, calculating employee commission payments, simple stock control system modelling
- Database application is for keeping records like sales records and appointments system
- Desktop publishing application is for creating leaflets, posters and business cards
- Presentation software is for creating presentations

- Graphics application is for manipulating images that can be used at home, school or a business

- Web design application is for creating personal or business websites

Moreover, general-purpose software refers to computer applications that are not designed for a particular business, industry or department. These applications may, therefore, be adopted and applied by many professionals, including engineers, security analysts, accountants, chemists, medical officers and attorneys.

According to Wikipedia, general-purpose software is widespread and popular because of its horizontal application. Teach-ICT.com reveals that general-purpose applications are preferred because they are cheap, easily available, have user support and are tested for bugs. They include spreadsheets, word processors, bookkeeping applications, statistics software, graphics packages, communication programs, desktop publishing applications, web-design applications and presentation software.

Let us study the three most commonly used general purpose software in detail.

1. **Spreadsheet Software**
   Spreadsheet software provides users with the ability to perform a variety of tasks with data, allowing users to keep track of data, perform calculations and remain organised when attempting to store information. An example of Spreadsheet software is Microsoft Excel.

   The software consists of cells arranged in rows and columns in which the user can manually enter data, including symbols, fractions and special characters. The user can format and analyse the entered data in different ways, such as shading and un-shading cells, using formatting features, hiding and un-hiding rows and columns and creating tables based from the data.

2. **Word Processors**
   Word processor software provides its users the opportunity to write efficiently and effectively with many options to format the document. Microsoft Word is one of the most common general purpose word processors; the software provides users with a ton of editing and formatting options; for example, they can find or replace text, analyse word counts, automatically insert symbols, set an address for hyperlinks, change fonts and insert images. Word processors also offer users the opportunity to save a document in many different file formats, which means that it is compatible with many other programs.

3. **Presentation Software**
   You can use presentation program software for displaying information, usually in the form of a slide show. These are very common for formal meetings, including business and school presentations. One of the most widely used programs for making slide show presentations is Microsoft PowerPoint. Some of the presentation creation options offered by the software include adding captions to pictures, inserting action buttons, adding a photo album and adding text to slides. The overall goal of

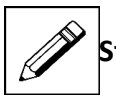
PowerPoint presentations is to provide information, data, and visuals where sometimes there is sound to relay a set of information more efficiently. PowerPoint enables users to save files in a variety of formats, such as .pptx, .pptm, .pdf, .pot and .mhtml.

Hence, this type of software tries to be a 'jack-of-all-trades'. It provides many features that the majority of users will want e.g. formatting text, creating charts, organising tables. But it does try to be all things to all people' and so there will be a vast number of features that you may never use e.g. statistical functions, mail merge. This makes the storage size of these applications fairly large.

The following below would now summarise why this software is important:

- It is relatively cheap
- It is well tested, and has wide support (example:. easy to use manuals and tutorials).
- It is easily available from most computer shops
- It will have been thoroughly tested so there will not be any serious problems or bugs
- There will be lots of user support like. books, user guides, online help and discussion forums on the Internet

However, it has a disadvantage and that is it is being very basic and may not answer a user's very specific needs in relation to a business or an organisation's needs.



Student Activity 12.1.4.5

Answer the following.

1. What is **general purpose software**?

_____

_____

_____

_____

2. List down three examples of a general purpose software and give its uses.

a. _____

_____

_____

_____

_____

b. _____

_____

_____

_____

_____

c. _____

_____

_____

_____

3. List down three advantages of general purpose software.

_____

_____

_____

_____

_____

_____

4. What is the disadvantage of general purpose software?

_____

_____

_____

_____

_____

_____

_____

_____

_____

12.1.4.6 Specialised Software

Even though software packages or general application software are very flexible they cannot be used for some specific tasks. Custom software also known as specialised software is written for a customer and is not for several users. Some custom software is developed for a single customer or client. It is written to fit the exact requirements of the problem and is labour intensive. For these reasons, custom software is very expensive. Custom software is written by a programmer using a programming language.

Hence, specialised software is software that is written for a specific task rather for a broad application area. These programs provide facilities specifically for the purpose of what they were designed.

Unlike, a general purpose software which is an application software design for users who want to perform common task on a computer system, a special software package are developed specially for a user using high level programming language. In general purpose software you may be using MS Office, Mavis beacon, CorelDraw, and the like for anyone who wants to create a letter, edit a picture can use MS Word and CorelDraw or Photoshop. These mentioned software examples are programmed to solve users' common tasks (General tasks). However, in specialised software it is used more specifically by an organisation to fulfil its needs in its day to day operation like the Database Management software designed for Barclays Bank for customer credits and debits items will be of no use to Sogeri National High School which will be so much interested in students' examination reports or results.

Below is a list of specialist software used by White Spire School in United Kingdom.

Software Name	Software Description
2 Simple Collection	Educational numeracy/literacy software
Clicker 5	Literacy teaching package
Clicker Paint	Literacy teaching package
Communicate in print	Desktop publishing program for creating symbol-supported resources for printing
2d Design	CAD design software
Flowol	Sequencing / Programming package
BeeBot	Robot learning package
Kar2ouche	Animation creation package
Microsoft Office Pro	Microsoft office suite - Word, Excel, Publisher, Access and Powerpoint

Serif Draw Plus x5	Computer drawing tool
Serif Movie Plus x6	Video editing package
Serif Page Plus x6	Desktop publishing package
Serif Panorama Plus x4	Photo stitching application
Serif Photo Plus x5	Photo editing package
Serif Web Plus x5	Website design package
Word Shark	Literacy teaching package
Number Shark	Numeracy teaching package
Education City	Online teaching aid

Take note that some of the specialised software used in White Spire School in United Kingdom is also used in the different schools here in Papua New Guinea like the CAD design software and Microsoft Office Suite. Software choice depends on the need of the students enrolled in the different computing courses.

The latest technological developments have created an opportunity for home users to take advantage of software previously used only in professional environments. For example, it is now possible, and quite common, for people to create their own Web sites. Home users also have access to software that helps manipulate and create graphic images. Many musicians and artists work from home to create complex and beautiful work using specialised applications.

Some of these same technological advances have allowed researchers and computer scientists to make advances in the field of artificial intelligence that previously were envisioned only in science fiction. Robots now provide security and assistance in homes. Virtual reality is providing opportunities in the fields of medicine and science but also commonly appears in video games.

Competent end users need to be aware of specialised applications. They need to know who uses them, what they are used for, and how they are used. These advanced applications include graphics programs, audio and video editing software, multimedia, Web authoring, and artificial intelligence, including virtual reality, knowledge-based systems, and robotics.

Student Activity 12.1.4.6

Answer the following.

1. What is specialised software?

_____

_____

_____

_____

2. List down three examples of specialised software and give its uses.

a. _____

_____

_____

_____

_____

b. _____

_____

_____

_____

_____

c. _____

_____

_____

_____

3. List down three advantages of specialised software.

a. _____

_____

_____

_____

b. _____

_____

_____

c. _____

_____

_____

_____

4. What is the disadvantage of specialised software?

_____

_____

_____

_____

_____

_____

_____

Summative Learning Activity 12.1.4

Answer the following.

1. Contrast the following terms.

   a. Network operating system and Network operating system tasks

_____

_____

_____

_____

_____

_____

_____

b. Log on procedure and Log off procedure

_____

_____

_____

_____

_____

_____

c. Anti-virus and Firewall

_____

_____

_____

_____

_____

d. Generalised software and specialised software

_____

_____

_____

_____

_____

2. Briefly explain the following in your own words.

a. Why is generalised software preferred to specialised software?

_____

_____

_____

_____

_____

_____

_____

b. When is specialised software used?

_____

_____

_____

_____

_____

_____

_____

_____

c. Why is it necessary to install both an anti-virus and firewall?

_____

_____

_____

_____

_____

d. Give an example of a situation on how a network administrator can control user access to files and folders in a network.

_____

_____

_____

_____

_____

Answers to Student Activities 12.1.4

Student Activity 12.1.4.1

1. A network operating system (NOS) is a computer operating system that is designed primarily to support workstation and personal computer.

2.

Network Operating System	Description	Advantage
Microsoft's LAN Manager	LAN Manager is a network operating system by Microsoft that works as a server application. It runs under Microsoft OS/2, and was developed in conjunction with 3Com. The file server may concurrently be used for other tasks like database services.	The system provides a good multi-tasking function. It also supports most desktop operating systems like DOS, Windows and OS/2 clients.
Novell's NetWare	This network operating system is a protocol suite designed based on the XNS protocol architecture.	It provides comprehensive support to most of the desktop operating systems in the market, including DOS, Windows, Macintosh, OS/2 and UNIX. Novell also supports the local area networks and asynchronous wide area communications.
Banyan VINES	Banyan Virtual Integrated Network Service (VINES) is a network operating system based on proprietary protocol family.	It uses a client-server architecture that enables clients to request specified services like file and printer access from servers.
Artisoft's LANtastic	LANtastic supports a wide variety of PC operating systems like Windows NT 4.0/2000/2003 (Workstation and/or Server), and Windows XP. It comes with an enhanced multi-platform support.	The installation and operation of the system is fast and user friendly, along with an improved interface that allows all networked PCs to be able to communicate by just using the Chat feature. Users are not required to employ a dedicated server or a full-time network manager because the system is simple and easy to maintain.

3. Network operating system refers to software that implements an operating system of some kind that is oriented to computer networking. It is the one that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions. It is further designed to allow shared file and printer access among multiple computers in a network, a local area network (LAN), a private area network or to other networks.

Student Activity 12.1.4.2

Answer may be similar to this one below.

1. Network operating system tasks are the services provided by a network operating system. These are its core function.

2. Any three of the following can be the answers.

   a. User administration

   b. System maintenance activities like backup

   c. Tasks associated with file management

   d. Security monitoring on all resources in the network

   e. Setting priority to print jobs in the network

3. Answers may be similar to these ones below.

   - file sharing
     Users can share files with the network.

   - print sharing
     Users can share the same network printer.

   - user administration
     Each user is designated with a user name and password where no other person can access to other's person's account except when the password of the user is compromised.

   - backing up data
     The network allows the users to store their files within the network which can be retrieved anytime upon connecting to the network.

Student Activity 12.1.4.3

Answers may be similar to these ones below.

1.

a. Log in is done when the user access network connection by signing in to his account.

b. Log off is done when the user sign out of the network.

2.

Logging in
The user will input his user name or log in name as set by the network administrator. He will input his unique password to access the network.

Logging out
The user will log off or sign out from the network by clicking on the Start button then the Shutdown button. He may be asked to re restart the computer at the end of his everyday use.

3. Logging in and logging out is important to ensure that the user can have proper access to his network files alone and to retain proper security of any files. This also ensures proper machine care and maximised use of the network.

Student Activity 12.1.4.4

Answers may be similar to these ones below.

1.

a. Anti-virus software
Antivirus or anti-virus software is software that is used to prevent viruses from entering the computer system and infecting files.

b. Firewall
Firewall and antivirus software are both designed to protect an individual's computer system from invasion and assault.

2.

a. Firewalls are used to limit incoming transmissions to those that are least likely to contain bad data, while antivirus programs actually look at the effect that the incoming data has on the system.

b. Antivirus or anti-virus software is software that is used to prevent viruses from entering the computer system and infecting files while firewall software is

software that controls the incoming and outgoing network traffic by analysing the number of data packets that is sent.

3. Firewalls and antivirus software are important components of Internet safety. These two play a significant role in computer and data protection in as much as security is concerned.

Student Activity 12.1.4.5

Answer can be similar to this one below.

1. General purpose software normally refers to the types of software used by computer operators to perform simple tasks, including writing, data recording and presentations. This software is some of the most commonly used software as it performs a variety of tasks, making it very beneficial to the user. It is sometimes known as 'off-the-shelf' is the sort of software that you use at home and school.

2. Any three of the following can be the answers.

   - Word processing application is for writing reports, memos and letters
   - Spreadsheet application is for keeping simple company accounts, calculating employee commission payments, simple stock control system modeling
   - Database application is for keeping records like sales records and appointments system
   - Desktop publishing application is for creating leaflets, posters and business cards
   - Presentation software is for creating presentations
   - Graphics application is for manipulating images that can be used at home, school or a business
   - Web design application is for creating personal or business websites

3. Any three of the following can be the answers.

   - It is relatively cheap
   - It is well tested, and has wide support (e.g. easy to use manuals and tutorials).
   - It is easily available from most computer shops
   - It will have been thoroughly tested so there won't be any serious problems or bugs

- There will be lots of user support i.e. books, user guides, online help and discussion forums on the Internet

---

Student Activity 12.1.4.6

1. Specialized software is software that is written for a specific task rather for a broad application area. These programs provide facilities specifically for the purpose for which they were designed.

2. Any three of the following can be the answers

   - 2 Simple Collection
   - Clicker 5
   - Clicker Paint
   - 2d Design
   - Flowol
   - BeeBot
   - Microsoft Office 2007 Pro
   - Serif Draw Plus x5
   - Serif Movie Plus x6
   - Serif Page Plus x6
   - Serif Panorama Plus x4
   - Serif Photo Plus x5
   - Serif Web Plus x5
   - Word Shark
   - Number Shark
   - Education City

3. Unlike a general purpose software which is an application software design for users who want to perform common task on a computer system, a special software package are developed specially for a user using high level programming language.

The latest technological developments have created an opportunity for home users to take advantage of software previously used only in professional environments.

Some of these same technological advances have allowed researchers and computer scientists to make advances in the field of artificial intelligence that previously were envisioned only in science fiction. Robots now provide security and assistance in homes. Virtual reality is providing opportunities in the fields of medicine and science but also commonly appears in video games.

4. Custom software is very expensive.

Answers to Summative Activity 12.1.4

1. Answers may be similar as these ones below.

   a. A network operating system (NOS) is a computer operating system that is designed primarily to support workstation and personal computer while network operating system tasks are the services provided by a network operating system. These are its core function.

   b. Log on procedures are the ways on how a user can access the network while log off procedure is how the user will exit the network.

   c. A firewall is set up to block access from unwanted network communications, often including both incoming and outgoing messages while Antivirus works by scanning the computer to detect and remove already infected files and also prevents from viruses from affecting any files.

   d. General purpose software normally refers to the types of software used by computer operators to perform simple tasks, including writing, data recording and presentations while specialized software is software that is written for a specific task rather for a broad application area.

2.

   a.

   The following below would now summarise why generalised software is preferred than specialised software.

   - It is relatively cheap
   - It is well tested, and has wide support (e.g. easy to use manuals and tutorials).
   - It is easily available from most computer shops

- It will have been thoroughly tested so there won't be any serious problems or bugs
- There will be lots of user support i.e. books, user guides, online help and discussion forums on the Internet

b. Specialised software is used more specifically by an organisation to fulfil its needs in its day to day operation.

c. Antivirus and Firewall software are two different methods of protecting the computer from infectious malicious software. These two are types of internet security programs that can help limit the chances that a computer becomes infected.

d. The network administrator can limit access or view to a user or group of users to certain files and folders in a network. He may create groups where users are categorized to belong to each with certain privileges. Some users may access all files and folders are necessary to their position and functions while others may not necessarily be granted access to other files and folders as these are confidential of some category and are not needed by them in performing their day to day routines.

Summary

Information is now made easy with the availability of network communications.

The information society challenges the education system. In recent years, the speedy, effective and global communication of knowledge has created a new foundation for co-operation and teamwork, both nationally and internationally. The increasing role played by information technology in the development of society calls for an active reaction to the challenges of the information society.

Already, new and greater demands are being made as to the core qualifications of individuals, as well as to their understanding and knowledge of the consequences of the introduction of information technology for the work and purpose of an organisation. The result is the efficient handling, processing, co-ordination and administration of organisation's resources, which is decisive for its competitiveness.

In a society which is becoming increasingly dependent on information and the processing of knowledge, great demands are therefore made that the individual should have a solid and broad educational foundation on which to build. Educational policy in the information society must ensure the following:

1. Information Technology (IT) qualifications are developed by means of their integration in all activities in the education sector and

2. The individual citizen must have an active and critical attitude to developments and not passively allow technological development to set the pace.

This module had provided the basic and necessary content and skills for networking capabilities. Upon its completion, the module topics on information and communication systems which specifically include information system, networking system, networking basics and networking software should have provided an achievement of the following:

- The capacity to analyse and describe an information system in terms of the information processes and equipment required
- The capability to describe the effects of information systems on the individual, society and the environment
- The ability to describe and set up a simple local area network (LAN)
- The capacity to describe communications hardware, software and methods of connection
- The ability to describe suitable data protection and security procedures for a network.

References

1. Andrew Anderson 1996. The Network Information System. www.tldp.org . 20 December 2014

2. Andy Walton.What Is the Primary Difference Between Peer-to-Peer & Client-Server Architectures?. http://classroom.synonym.com . Synonym.com © 2001-2014, Demand Media. 20 December 2014

3. Armin Anders (2010). http:// www.hpac.com . Copyright © 2014 Penton. 20 December 2014

4. Ask.com. http://www.ask.com . 20 December 2014

5. B. Bashir (2014). http:// www.streetdirectory.com .© 2014 Streetdirectory. 20 December 2014

6. Basic Networking Client-Server and Peer-to-Peer. http://www.enterprise-technology.net/network3.htm. 20 December 2014

7. Best Business deal at BGWDealer. http://www.bgwdealer.com/. Copyright © 2014 Best Business Deal at BGWDealer. 20 December 2014

8. Bhavya Daya. Network Security: History, Importance, and Future. University of Florida Department of Electrical and Computer Engineering

9. Bradley Mitchell (2014). Protocol (network). http:// www. compnetworking.about.com. 2014 About.com. 20 December 2014

10. C Kapoor (2011). Benefits Of Computer Networking. http://www.benefitof.net . 20 December 2014

11. Chapter 3 Understanding Network Architecture. http:// www.miscrosoft.com . MCSE Training Kit, Networking Essentials Plus, Third Edition. © 2001 Microsoft Corporation. 20 December 2014

12. CIS307: Data Transmission

13. College of Education, University of South Florida. Network Operating System Software. http://www.fcit.usf.edu. © 1997-2013. 20 December 2014

14. Computer Network Toplogies.http://www.tutorialspoint.com. Copyright © 2014 by tutorialspoint. 20 December 2014

15. Computer Networking Lecture Notes.18 February 2013 • Wired Transmission Media. FBI DATA REELS (UN-Classified) and unreadable to me! by spike55151 under a Creative Commons BY NC SA license.Twisted Pair by Wolf Wings in the public domain.CAT5e Cable.jpg eler under the GNU Free Documentation License. Cat7.jpg by Bewareircd in the public domain.RG-59.jpg by Arj under a Creative Commons BY SA license.Optikai

kábel.jpg by Zátonyi Sándor under a Creative Commons BY SA license.Speed-vs-length.svg by Alexander Stohr under a Creative Commons BY SA license.

16. D3LTA (2012).Different types of Network Security. http://windows.microsoft.com/en-US/windows-vista/What-are-the-different-wireless-network-security-methods .Copyright 2014 Tangient LLC. 20 December 2014

17. Data transmission - Transmission modes (2014). http:// www.en.kioskea.net . 20 December 2014

18. Data Transmission Modes - Types of Data Transmission Modes. http://greatinformer.blogspot.com .Copyright © 2012-2014 All Rights Reserved Great Info. 20 December 2014

19. Definition of network operating system. http://www.computerlanguage.com. Copyright © 1981- 2014. The Computer Language Company Inc. 20 December 2014

20. DINESH THAKUR (2014) . What is Data Transmission? Types of Data Transmission.http:// www. ecomputernotes.com/article . 20 December 2014

21. DINESH THAKUR (2014) .Transmission Modes - What are the different Transmission Modes?. http:// www. ecomputernotes.com/article . 20 December 2014

22. Donald Amoroso 2003. ITMGT-8: Social Issues in Information Systems. 20 December 2014

23. Education Portal

24. Euromed Marseille School of Management, World Med MBA Program - Information Systems and Strategy Course. http://www.chris-kimble.com/Courses/World_Med_MBA/Session_1.html#types . 20 December 2014

25. ICT Global. Networking Basics: The Importance of Computer Networks. www.ictglobal.com. 20 December 2014

26. IGCEICT. http://www.igcseict.info/index.html

27. Infocheese. http://www.infocheese.com/index.html. Copyright 2008. 20 December 2014

28. Information Technology Help Desk. Login and Logout Procedures. © Copyright -- 2008 -- California Western School of Law. http://www.helpdesk.cwsl.edu . 20 December 2014

29. Introduction to Data Communications. http:// www.telecomworld101.com . 20 December 2014

30. ITBusinessEdge. Data transfer rate. http:// www.webopedia.com . Copyright 2014 QuinStreet Inc. 20 December 2014

31. Julie Davoren 2014. Types of Information Systems in an Organisation. http://www.chron.com/ 20 December 2014

32. Ken Foote 2015. Ethical Issues in Electronic Information Systems. 20 December 2014

33. Lesson 1: Access Methods. http://pluto.ksi.edu . 20 December 2014

34. Lesson 1: Introduction to Network Operating Systems. http://pluto.ksi.edu . 20 December 2014

35. Michael M. Gorman 1999. Information Systems Plan:The Bet-Your-Business Project. Copyright 1997-2014, The Data Administration Newsletter, LLC -- www.TDAN.com. 20 December 2014

36. Network Access Methods, CSMA/CD, CSMA/CA and Token Passing, Difference between CSMA/CD CSMA/CA and Token Passing. http:// www.omnisecu.com . Copyright 2008 - 2014 OmniSecu.com. 20 December 2014

37. Network Categories. http:// www.googleads.g.doubleclick.net. 20 December 2014

38. Network Operating System Features - Support and File Sharing. http://www.dummies.com. Copyright © 2014 & Trademark by John Wiley & Sons, Inc. 20 December 2014

39. Network Protocol - Types of Network Protocols. http://www.edrawsoft.com . Copyright EdrawSoft 2004-2014. 20 December 2014

40. Networking Basics: Peer-to-peer and server-based networks. http://www.technet.microsoft.com . 20 December 2014

41. Slideshare. http://www.slideshare.net/. Copyright 2015. 20 December 2014

42. TeachICT. http://www.teachict.com. 20 December 2014

43. Technopedia. http:// www.technopedia.com

44. TechTerms.com. http:// www.techterms.com

45. Webopedia. http://www.webopedia.com. 20 December 2014

46. Webster's New World Telecom Dictionary Copyright © 2010 by Wiley Publishing, Inc., Indianapolis, Indiana. Used by arrangement with John Wiley & Sons, Inc.

47. White Spire School. http://www.whitespireschool.org.uk .2014 White Spire School. 20 December 2014

48. Wikipedia. http://www.wikipedia.com . 20 December 2014

49. WildPackets. http://www.wildpackets.com/resources/compendium/glossary_of_networking_terms. © 2015 WILDPACKETS, INC

50. Wired and Wireless Transmission Media. http:// www.itechere.com . Copyright © 2011 - 2014 Bill Kishen iTechere, LLC. 20 December 2014

GLOSSARY

Adapter
Hardware that allows a computing device physical access to a network

ADC
Analog to digital converter converts analog data to digital

Address
A numerical designation that uniquely refers to a specific communication entity

Analog
Referring to a system or component that uses a system of measurement, response or storage in which values are expressed as a magnitude using a continuous scale of measurement

Analog Transmission
Signal transmission over wires or through the air in which information is conveyed through variation of some combination of signal amplitude, frequency, and phase

Architecture
The sum total of all of the specifications, protocols and implementations that define a particular networking system

ADSL
Short for asymmetric digital subscriber line, ADSL is a form of DSL Broadband. It is asymmetric because of its two-way bandwidth devoted to the downstream and a small section devoted to upstream transfer. This allows for a much higher download transfer rate, often up to 6.1 megabits per second

Asynchronous
A system of communication in which each discreet delivery of information establishes its own timing impulse rather than having to conform to the timing impulse of previous deliveries

Term describing digital signals that are transmitted without precise clocking. Such signals generally have different frequencies and phase relationships. Asynchronous transmissions usually encapsulate individual characters in control bits (called start and stop bits) that designate the beginning and end of each character. Compare with Isochronous transmission, plesiochronous transmission, and synchronous transmission

Attenuation
Term describing the weakening or reduction of transmitted signal.

ATM
Asynchronous Transfer Mode. A broadband transmission system using 53-octet packets over a cell-switched network at speeds up to 2.2 GBPS

ATP
AppleTalk Transaction Protocol. Transport-level protocol that allows reliable request-response exchanges between two socket clients

Band
In analog communications, the range of frequencies over which a communication system operates

Bandwidth
In analog communications, the difference between the highest and lowest frequencies available in the band. In digital communications, bandwidth is loosely used to refer to the information-carrying capacity of a network or component of a network

Bit
The basic unit of data representation in digital computers. a memory location that can have one of two values

Bit rate
The rate at which bits are transmitted or received during communication, expressed as the number bits in a given amount of time, usually one second

Bitmap
A data structure that uses bits to represent the attributes of an object that is not character-based

Boot
A computer's start-up operation

Boot Drive
The disk that contains a computers' start-up instructions

BOOTP
Bootstrap Protocol. An IP protocol used by diskless workstations to receive boot information from a boot server

Bridge
A Data Link Layer device that limits traffic between two network segments by filtering the data between them based on hardware addresses

Broadband
A transmission system capable of carrying many channels of communication simultaneously by modulating them on one of several carrier frequencies

Buffer
A temporary memory storage area for information

Bug
A flaw in a software program

Bundled
Refers to the practice of automatically including an additional application or capability in the sale or delivery of a computing component that is not ordinarily associated with that component

BUS
Broadcast and unknown server. Multicast server used in ELANs that is used to flood traffic addressed to an unknown destination, and to forward multicast and broadcast traffic to the appropriate clients

Bus
A type of network topology in which nodes are connected along a continuous path that is not a closed circuit. Also refers to a communications channel used by a single computer such as Nubus, SCSI, etc.

Byte
A group of 8 bits

Cable
The transmission media of a network

Carrier
Electromagnetic wave or alternating current of a single frequency, suitable for modulation by another, data-bearing signal

CATV
Cable television. Communication system where multiple channels of programming material are transmitted to homes using broadband coaxial cable. Formerly called Community Antenna Television

CDDI
Copper Distributed Data Interface. Implementation of FDDI protocols over STP and UTP cabling. CDDI transmits over relatively short distance (about 100 meters), providing data rates of 100Mbps using a dual-ring architecture to provide redundancy. Based on the ANSI Twisted-Pair Physical Medium Dependent (TPPMD) standard

Cellular Radio
Technology that uses radio transmissions to access telephone-company networks. Service is provided in a particular area by a low-power transmitter

CSMA/CD
Carrier sense multiple access collision detect. Media-access mechanisms wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays retransmissions from those devices for some random length of time. CSMA/CD access is used by Ethernet and IEEE 802.3

Collision
Term used to describe when one or more computers or networking devices attempt to send data at the same time to one computer, server, or other network device. When collisions are encountered, the computer, server, or network device will send back a request to try sending the data again

DAC
Digital to analog data is a function that converts digital data usually binary into an analog signal like current, voltage or electric charge.

Demodulation
Process of returning a modulated signal to its original form. Modems perform demodulation by taking an analog signal and returning it to its original (digital) form

Demultiplexing
The separating of multiple input streams that have been multiplexed into a common physical signal back into multiple output streams

DOS
The operating system of IBM-compatible personal computers

Ethernet
A specification for a transmission system including Layers 1 and2 of the OSI 7-layer model using the CSMA/CD access method. In common usage, "Ethernet" refers to both the DIX (DEC - Intel - Xerox) version of this specification or to the IEEE version, more formally known as "802.3". The DIX version is distinguished by the reference "Ethernet V.2"

Fast Ethernet
A 100 MB network using 4 twisted pairs

FDDI
Fiber Data Distributed Interface. A specification (ANSI X 3T9.5)for 100 MBits/sec. on dual counter-rotating token passing ring implemented on fiber optic cabling

Fiber optic
A transmission media that uses a light wave for signalling

Fiber-optic Cable
Physical medium capable of conducting modulated light transmission. Compared with other transmission media, fiber-optic cable is more expensive, but is not susceptible to electromagnetic interference and is capable of higher data rates. Sometimes called optical fiber

File Transfer
Popular network application that allows files to be moved from one network device to another

Firewall
Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network

FireWire
High-speed external data bus intended to replace the SCSI bus in the Macintosh system architecture, as the bus of choice for the connection of storage devices, external video and image I/O, etc.

Firmware
A collection of programmed routines and instructions that is implemented in a computer chip or similar hardware form instead of a software form

FTP
File Transfer Protocol. Lowest-common-denominator protocol for the point-to-point transfer of text and binary files between IP connected hosts

Full-duplex
A communication system between two entities in which either entity can transmit simultaneously

Full Mesh
Term describing a network in which devices is organised in a mesh topology, with each network node having either a physical circuit or a virtual circuit is connecting it to every other network node. A full mesh provides a great deal of redundancy, but because it can be prohibitively expensive to implement, it is usually reserved for network backbones. See also mesh and partial mesh.

Gateway
1. A device that performs a protocol translation at the Session Layer or higher. 2. Archaic. A TCP/IP router that routes packets between different network numbers

Gateway Host
In SNA, a host node that contains a gateway SSCP

GHz
Gigahertz

Giga
A prefix denoting a billion

GB
Gigabyte

GBps
Gigabytes per second

Gb
Gigabit

Gbps
Gigabits per second

GDP
Gateway Discovery Protocol. Cisco protocol that allows hosts to dynamically detect the arrival of new routers as well as determine when a router goes down

Ghosting
Disk cloning and back up tool

Hacker
1. An expert computer programmer

2. A knowledgeable but disruptive computer user

Half Duplex
Capability for data transmission in only one direction at a time between a sending station and a receiving station. Compare with full duplex and simplex

Host
In terminal emulation, the remote computer that is being controlled by the terminal emulation software

Heuristics
Any approach to problem solving, learning or discovery that employs a practical method not guaranteed to be optimal or perfect but sufficient for immediate goals

Hub

1. Generally, a term used to describe a device that serves as the center of a star-topology network
2. Hardware of software devices that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat, but merely split, signals sent through them)
3. In Ethernet and IEEE 802.3, an Ethernet multiport repeater, sometimes referred to as a concentrator

Hybrid Network
Internetwork made up of more than one type of network technology, including LANs and WANs

Hypertext
Electronically-stored text that allows direct access to other texts by way of encoded links. Hypertext documents can be created using HTML, and often integrate images, sound, and other media that are commonly viewed using a WWW browser. See also HTML and WWW browser

IBM
International Business Machines

I/O
Input/Output. A computer activity where data is either loaded into (input) or extracted from (output) RAM

IP
Internet Protocol. The Network Layer protocol in the TCP/IP stacks offering a connectionless internetwork service. IP provides features for addressing, type-of-service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Documented in RFC 791

IP Address
32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated with periods (dotted decimal format). Each address consists of a network number, an optional subnet work number, and a host number. The network and sub network numbers together are used for routing, while the host number is used to address an individual host within the network or sub network. A subnet mask is used to extract network and sub network information from the IP address. Also called an Internet address

IPTV
Internet Protocol Television

ISDN
Integrated Services Digital Network. Communication protocol, offered by telephone companies, that permits telephone networks to carry data, voice, and other source traffic. See also BISDN, BRI, N-ISDN, and PRI.

KB
Kilobyte

Kb
Kilobit

KBPS
A unit of measure used to describe the rate of data transmission equal to 1000 bits per second

KByte
A unit of measure used to describe an amount of information equal to 1024 (210) bytes

Kinking
Form or cause to form a sharp twist or curve

LAN
A communication infrastructure that supports data and resource sharing within a small area (<2 km diameter) that is completely contained on the premises of a single owner

LED
Light emitting diode. Semiconductor device that emits light produced by converting electrical energy. Status lights on hardware devices are typically LEDs

LF
Low frequency

LocalTalk

A Data Link Layer protocol defined in Inside AppleTalk by Apple Computer that covers the transmission of data on twisted pair wire using CSMA/CA at 230.4 Kilobits per second

Login
A formal procedure where a computing device initiates a sustained connection to another computing device for the purpose of using a resource managed by the computer

Logout
A Formal procedure where a computing device severs its connection to another computing device

Loop
Route where packets never reach their destination, but simply cycle repeatedly through a constant series of network nodes

MAN
metropolitan-area network. Network that spans a metropolitan area. Generally, a MAN spans a larger geographic area than a LAN, but a smaller geographic area that a WAN

Mbps
Millions of bits per second

MF
Medium Frequency

MIS
Management Information System. Used to describe the set of computing resources that hold and allow access to the information owned by an organisation

Mode
1. One particular method or way of accomplishing a goal.

2. In fiber optic transmission, a particular path between a light source and a receiver.

3. In statistics, the result with the highest frequency within the sample group.

Modem
A device that can covert data signals between analog and digital signalling systems

Modem eliminator
Device allowing connection of two DTE devices without modems

Modulation
Process by which the characteristics of electrical signals are transformed to represent information. Types of modulation include AM, FM, and PAM

Multiplexing
Scheme that allows multiple logical signals to be transmitted simultaneously across a single physical channel

Multi-user
A term used to describe a computing process that can handle the requirements of several users simultaneously

Multitasking
A descriptive term for a computing device whose operating system can handle several tasks concurrently. In mono processors, each active task is given short periods of time to use the CPU in a rotational fashion

System
Collectively to the proprietary protocols and network file systems that computers use to exchange data with their LAN Servers

Network Operator
Person who routinely monitors and controls a network, performing tasks such as reviewing and responding to traps, monitoring throughput, configuring new circuits, and resolving problems

NFS
Network File System. A file metalanguage and set of procedure calls to access and manage files that is standard issue on nearly every computer that uses TCP/IP protocols as its standard network protocols. Designed by Sun Microsystems, NFS is now a standard feature of nearly all UNIX systems

NIC
1. Network Information Center. The group responsible for the assignment of IP addresses
2. Network Interface Card. A network adapter on a circuit board that plugs into computer internal bus architecture

3. A 16-bit Ethernet chip designed by Texas Instruments

NIS
Network Information System. Protocol developed by Sun Microsystems for the administration of network-wide databases. The service essentially uses two programs: one for finding a NIS server and one for accessing the NIS databases

Node
A networked computing device that takes a protocol address and can initiate and respond to communication from other networked devices that employ similar protocols

Noise
Undesirable electrical or electromagnetic signals

Packet
A discrete chunk of communication in a pre-defined format

Reboot
A user activity where the user starts a computing device without interrupting its source of electrical power

Receiver
The node or process for which a packet or other information is intended

Remote Access
AppleTalk Remote Access. Apple's protocol that allows a single user to gain network access over a modern connection

Response Time
The gap between the time when a user initiates an action and the time that the action displays its results

RF Interference
Radio Frequency signals that degrade the integrity of a data signal

Router
A device that forwards packets between networks according to the rules of a network layer protocol such as DDP and information it has gathered during its service concerning the structure of the internet

SCSI
Small Computer Systems Interface. A specification (ANSI X3T9.2) for a short distance ((6 meters max.) Local Area Network using bus topology for up to eight devices. The Macintosh uses this network for attaching devices such as external disk drives and scanners

Serial Port
A port on a computing device that is capable of either transmitting or receiving one bit at a time. Examples include the Mac's printer and modem ports

Server
A device that is shared by several users of a network

Signal
The means of conveyance for a communication, typically an electromagnetic wave that is modulated to encode the information communicated

Skew
To change or alter in particular direction

SMTP
Simple Mail Transfer Protocol. The standard protocol for exchanging mail over TCP/IP networks

SQL
Structured Query Language. A widely used metalanguage for data base access and management. AN IBM and ANSI standard

STP
Shielded twisted-pair. Two-pair wiring medium used in a variety of network implementations. STP cabling has a layer of shielded insulation to reduce EMI

Subnet Address
Portion of an IP address that is specified as the sub network by the subnet mask. See also IP address, subnet mask, and sub network

Switch
A switch is a device that forwards packets between nodes based on the packet's destination node address (either hardware or protocol), typically with a buffer time longer than a repeater but shorter than the transmission time of the packet

Synchronization
Establishment of common timing between sender and receiver

Synchronous
A communication system where stations may only transmit at prescribed intervals and must provide a timing pulse with their packet

Synchronous Transmission
Term describing digital signals that are transmitted with precise clocking. Such signals have the same frequency, with individual characters encapsulated in control bits (called start bits and stop bits) that designate the beginning and end of each character. Compare with asynchronous plesiochronous transmission.

System
Any computer system that can be controlled by a user consisting of a CPU and optional equipment such as display monitors, disk drives, and other peripherals

System File
The Macintosh file that contains system software for the Macintosh OS, including patches or replacements to obsolete code contained in ROM

System Folder
The directory in which the System File resides

System Management
Activities that focus on the care and management of individual computer systems

System Software
Software in a computing system that provides basic functionality like file management, visual display, and keyboard input and is used by application software to accomplish these functions

TCP
Transmission Control Protocol. A reliable Transport Layer Protocol for managing IP that supports re-transmission, sequencing and fragmentation

TCP/IP
Transmission Control Protocol/Internet Protocol. A Transport and Network Layer Protocol, respectively, used by a large number of computers

Telephony
The science and practice of telecommunications

THz
Terahertz is a unit of electromagnetic wave frequency equal to one trillion hertz

Terminal
Simple device at which data can be entered or retrieved from a network. Generally, terminals have a monitor and a keyboard, but no processor or local disk drive

Terminal Adapter
Device used to connect ISDN BRI connections to existing interfaces such as EIA/TIA-232. Essentially, an ISDN modem

Token
Frame that contains control information. Possession of the token allows a network device to transmit data onto the network

Token bus
LAN architecture using token passing access over a bus topology. This LAN architecture is the basis for the IEEE 802.4 LAN specification

Token Passing
A MAC method where stations may only transmit when they are in possession of a special bit sequence (token) passed from station to station.

Token Ring
A ring topology network that uses token passing for MAC

Topology
1. The arrangement of computing devices in a network

2. A term describing such an arrangement

Transmission
The activity of sending or conveying information

Transmit
To send information

Transport Protocol
The Protocol Layer of the OSI 7-Layer Model that is concerned with management of the data flow between source and destination

Transport
Any of the functions carried out by protocols in the Network or Transport Layers

Trunk
A synonym for bus

Tweak
A minor adjustment

UNIX
A 32-bit multi-tasking, multi-user operating system invented by Bell Labs that is used on many type of computer systems

Upload
The activity of transferring a file from a user's computer system to a remote system

UPS
Uninterruptable Power Supply. An electrical supply system that conditions electrical power for a computer system and will allow continued operating in the event of a power failure

User
A person who uses a computer system to accomplish a non-computing goal, as compared to a programmer or network manager

User Interface
The collection of display symbols and other sensory stimuli made by a computer that present information to a human and the collection of physical action that a human can take to present data to a computer

VLF
Very Low Frequency

VOIP
Voice Over Internet protocol

VPN
Short for Virtual Private Network, VPN is a network that allows a user to connect to a network through a tunnelling protocol and access internal Internet and intranet websites and e-mail. Virtual Private Networks are commonly used to allow an employee with a large company to connect to the company's intranet

Workstation
A name given to a single computer that is connected to another computer or network. A workstation has no important function and is not a necessity for a network to operate. A workstation is only needed for a single user to connect to the network. For example, almost all users who utilize a computer at their job or school are using a workstation

FODE SUBJECTS AND COURSE PROGRAMMES

GRADE LEVELS	SUBJECTS/COURSES
Grades 7 and 8	1. English
	2. Mathematics
	3. Personal Development
	4. Social Science
	5. Science
	6. Making a Living
Grades 9 and 10	1. English
	2. Mathematics
	3. Personal Development
	4. Science
	5. Social Science
	6. Business Studies
	7. Design and Technology- Computing
Grades 11 and 12	1. English – Applied English/Language& Literature
	2. Mathematics - Mathematics A / Mathematics B
	3. Science – Biology/Chemistry/Physics
	4. Social Science – History/Geography/Economics
	5. Personal Development
	6. Business Studies
	7. Information & Communication Technology

REMEMBER:

- For Grades 7 and 8, you are required to do all six (6) subjects.
- For Grades 9 and 10, you must complete five (5) subjects and one (1) optional to be certified. Business Studies and Design & Technology – Computing are optional.
- For Grades 11 and 12, you are required to complete seven (7) out of thirteen (13) subjects to be certified.

Your Provincial Coordinator or Supervisor will give you more information regarding each subject and course.

GRADES 11 & 12 COURSE PROGRAMMES

No	Science	Humanities	Business
1	Applied English	Language & Literature	Language & Literature/Applied English
2	Mathematics A/B	Mathematics A/B	Mathematics A/B
3	Personal Development	Personal Development	Personal Development
4	Biology	Biology/Physics/Chemistry	Biology/Physics/Chemistry
5	Chemistry/ Physics	Geography	Economics/Geography/History
6	Geography/History/Economics	History / Economics	Business Studies
7	ICT	ICT	ICT

Notes: You must seek advice from your Provincial Coordinator regarding the recommended courses in each stream. Options should be discussed carefully before choosing the stream when enrolling into Grade 11. FODE will certify for the successful completion of seven subjects in Grade 12.

CERTIFICATE IN MATRICULATION STUDIES		
No	**Compulsory Courses**	**Optional Courses**
1	English 1	**Science Stream:** Biology, Chemistry, Physics
2	English 2	**Social Science Stream:** Geography, Intro to Economics and Asia and the Modern World
3	Mathematics 1	
4	Mathematics 2	
5	History of Science & Technology	

REMEMBER: You must successfully complete 8 courses: 5 compulsory and 3 optional.

FODE PROVINCIAL CENTRES CONTACTS

PC NO.	FODE PROVINCIAL CENTRE	ADDRESS	PHONE/FAX	CUG PHONES	CONTACT PERSON		CUG PHONE
1	DARU	P. O. Box 68, Daru	6459033	72228146	The Coordinator	Senior Clerk	72229047
2	KEREMA	P. O. Box 86, Kerema	6481303	72228124	The Coordinator	Senior Clerk	72229049
3	CENTRAL	C/- FODE HQ	3419228	72228110	The Coordinator	Senior Clerk	72229050
4	ALOTAU	P. O. Box 822, Alotau	6411343 / 6419195	72228130	The Coordinator	Senior Clerk	72229051
5	POPONDETTA	P. O. Box 71, Popondetta	6297160 / 6297678	72228138	The Coordinator	Senior Clerk	72229052
6	MENDI	P. O. Box 237, Mendi	5491264 / 72895095	72228142	The Coordinator	Senior Clerk	72229053
7	GOROKA	P. O. Box 990, Goroka	5322085 / 5322321	72228116	The Coordinator	Senior Clerk	72229054
8	KUNDIAWA	P. O. Box 95, Kundiawa	5351612	72228144	The Coordinator	Senior Clerk	72229056
9	MT HAGEN	P. O. Box 418, Mt. Hagen	5421194 / 5423332	72228148	The Coordinator	Senior Clerk	72229057
10	VANIMO	P. O. Box 38, Vanimo	4571175 / 4571438	72228140	The Coordinator	Senior Clerk	72229060
11	WEWAK	P. O. Box 583, Wewak	4562231/ 4561114	72228122	The Coordinator	Senior Clerk	72229062
12	MADANG	P. O. Box 2071, Madang	4222418	72228126	The Coordinator	Senior Clerk	72229063
13	LAE	P. O. Box 4969, Lae	4725508 / 4721162	72228132	The Coordinator	Senior Clerk	72229064
14	KIMBE	P. O. Box 328, Kimbe	9835110	72228150	The Coordinator	Senior Clerk	72229065
15	RABAUL	P. O. Box 83, Kokopo	9400314	72228118	The Coordinator	Senior Clerk	72229067
16	KAVIENG	P. O. Box 284, Kavieng	9842183	72228136	The Coordinator	Senior Clerk	72229069
17	BUKA	P. O. Box 154, Buka	9739838	72228108	The Coordinator	Senior Clerk	72229073
18	MANUS	P. O. Box 41, Lorengau	9709251	72228128	The Coordinator	Senior Clerk	72229080
19	NCD	C/- FODE HQ	3230299 Ext 26	72228134	The Coordinator	Senior Clerk	72229081
20	WABAG	P. O. Box 259, Wabag	5471114	72228120	The Coordinator	Senior Clerk	72229082
21	HELA	P. O. Box 63, Tari	73197115	72228141	The Coordinator	Senior Clerk	72229083
22	JIWAKA	c/- FODE Hagen		72228143	The Coordinator	Senior Clerk	72229085