Mount Kenya University

**P.O. Box 342-01000 Thika**
**Email: info@mku.ac.ke**
**Web: www.mku.ac.ke**

# SCHOOL OF PURE AND APPLIED SCIENCES

# DEPARTMENT OF INFORMATION TECHNOLOGY

COURSE CODE: BIT 2204

**COURSE TITLE: DATA COMMUNICATION AND NETWORKS**

***Instructional manual for BBIT – Distance Learning***

# COURSE OUTLINE

## BIT 2204: DATA COMMUNICATION AND COMPUTER NETWORKS

**Purpose of the course**

To introduce the concepts of computer networking in order to provide basic skills needed in data transmission communication and computer network..

**TOPICS - DETAILS**

**I. Introduction to Networks**
- A. Definition of terms
- B. Network types, LAN, MAN, WAN
- C. Basic components of a Network, terminal, server etc
- D. Network types; peer to peer, client server, advantages

**II. Transmission medium**
- A. Guided Medium, twisted pair, coaxial cable, fiber optic
- B. Unguided medium, satellite, microwave
- C. Transmission impairments, noise, attenuation, delay distortion

**III. Network topologies**
- A. Star, ring, bus, mesh
- B. Advantages and disadvantages of the different network topologies
- C. Medium Access control, CMSA CD, Token, polling

**IV. OSI LAYER AND TCP/IP LAYERS**
- A. Advantages of a layered model
- B. Seven OSI layers
- C. Four TCP/IP layer

V. **Connecting Devices**
- A. Networking Devices, switch, hub, bridge, repeater
- B. Internetworking Devices, Router, gateway

**VI. Switching techniques**
- A. Circuit switching
- B. Packet switching
- C. Message switching

**VII. Multiplexing**
- A. Time division Multiplexing
- B. Frequency division Multiplexing

**Main course text**

Tanenbaum A.S.(1996), Computer Networks, Prentice Hall India

**Reference Books**


i. William Stallings (2010), **Data and Computer Communication,** 9th edition
ii. Behrouz A. Forouzan, (2006), **Data communication and networking**, 5th edition.
iii. Andrews. Tanenbaum, (2010) **Computer Networks**, 5th edition . Prentice-Hall PTR


**Assessment:** Examination - 70%: Coursework - 30%

# CHAPTER ONE

# INTRODUCTION TO NETWORKS

**Learning Objectives**

By the end of this chapter the learner shall be able to;

i. Explain the meanings of different terms used in networking
ii. Explain the basic components of a network
iii. The different types of networks such as the Local area network, Metropolitan area network and the Wide area Network.
iv. The benefits of establishing a computer network

## 1.1 Definition of terms

**Computer network -** A computer network (a network in short) is a combination of hardware and software that achieves communication between computers. It can also be defined as a collection of computers and devices interconnected by communications channels that facilitate communications and allows sharing of resources and information among interconnected devices. When put more simply, a computer network is a collection of two or more computers linked together for the purposes of sharing information, resources, among other things.

**A client** is a computer that allows a user or users to log on to the network and take advantage of the resources available on the network. A client computer will make a client operating system. The purpose of the client is to get user onto the network; therefore, client computers don't usually have the processing power, the storage space, or the memory found on a server because the client does not have to serve up resources to other computers on the network.

**A server**, on the other hand, is typically a much more powerful computer that runs a network operating system. The server provides centralized administration of the network and serves up the resources that are available on the network, such as printers and files. The administrator of

the server decides who can and cannot log on the network and which resources the various can access.

**Data communication** - electronic transmission of information that has been encoded digitally (as for storage and processing by computers).

**Data** are groups of information that represent the qualitative or quantitative attributes of a variable or set of variables. Data (plural of "datum", which is seldom used) are typically the results of measurements and can be the basis of graphs, images, or observations of a set of variables. Data are often viewed as the lowest level of abstraction from which information and knowledge are derived.

**Information** – Processed data that is in a meaningful form.

A **transmitter** is an electronic device which, usually with the aid of an antenna, propagates an electromagnetic signal such as radio, television, or other telecommunications.

**Receiver**, the receiving end of a communications channel

**Signal** a physical quantity that can carry information

**Channel** , the medium used to convey information from a sender to a receiver.

An **electric bus** is a bus powered by electricity that connect two devices

**Simplex communication** refers to communication that occurs in one direction only.

**A half-duplex system** provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.

An example of a half-duplex system is a two-party system such as a "walkie-talkie" style two-way radio, wherein one must use "Over" or another previously-designated command to indicate the end of transmission, and ensure that only one party transmits at a time, because both parties transmit on the same frequency.

**A duplex communication system** is a system composed of two connected parties or devices that can communicate with one another in both directions.

**A network** is an interconnection of two or more computers in order to share data and resources.

**Point to Point communication** A traditional point-to-point data link is a communications medium with exactly two endpoints and no data or packet formatting. The host computers at

either end had to take full responsibility for formatting the data transmitted between them. Computers in close proximity may be connected by wires directly between their interface cards.

**Multi point communication** - A system with at least one, and preferably at least two, end devices

**Why network computers?**

There are some compelling reasons why someone with more than a couple computers would want to connect those computers into a network. What the network will actually be used for will, of course, vary depending on the needs of the person or organization creating the network. Networks can be used for simple tasks, such as sharing a printer, or they can be used for more advanced applications, such as complex point-of-sale system and worldwide video conferencing.

All networks, whether big or small, are typically created so that users on the network can share resources and communicate. The list that follows breaks down some of the reasons for networking computers:

- File sharing. Networking computers makes it very easy for the users on the network to share application files
- Hardware sharing. Users can share devices such as printers, CD-ROM drives, and hard drives.
- Program sharing. Applications such as spreadsheets and word processors can be run over the network.
- User communication. Network allows users to take advantage of communication media such as electronic mail, newsgroups, and video conferencing.

**Network Types (classification based on Network size)**

**LAN - Local Area Network -** 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.

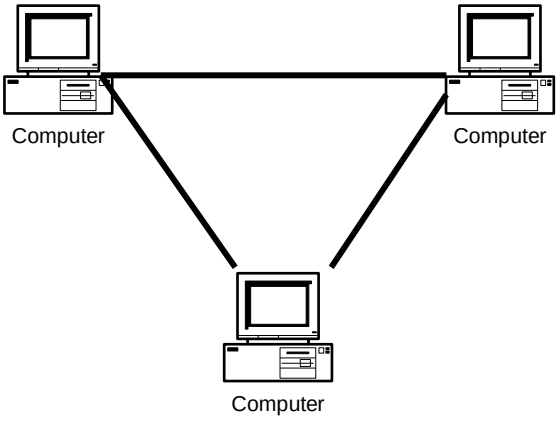
**Metropolitan Area Network -** a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned an operated by a single entity such as a government body or large corporation.

**WAN - Wide Area Network -** As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN.

## 1.2 Network Types (classification based on point of control)

The most elementary of all networks that consist of two (or more) computers, each connected to the other using some kind of wire or cable to permit information exchange. The connection can be done in two basic ways: Peer-To-Peer and Server-Based.

**Peer-To-Peer Network**




Computers of a Peer-To-Peer network can take both a client and a server role. There is no centralized control over shared resources, such as files or printer. Any individual machine can share its resources with any other computer on the same network, however and

whenever its users choose to do so. The Peer-To-Peer relationship also means that all computers have equal access and responsibility in the network.

**Advantages of Peer-To-Peer Network**

- Easy to install and configure.
- Individual machines do not depend on the presence of a dedicated server.
- Individual users control their own-shared resources.
- It's inexpensive to purchase and operate.
- No additional software or hardware beyond a suitable operating system is needed.
- No dedicated administrators are needed to run the network.
- It works best for network with 10 of fewer users.

**Disadvantages of Peer-To-Peer Network**

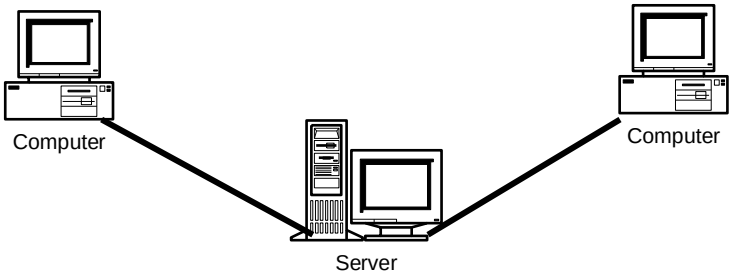
- Network security applies only to a single resource at a time.
- Users may be forced to use as many passwords as there are shared resources
- Each machine must be backed up individually to protect all shared data.
- There is no centralized organizational scheme to locate or control access to data.
- Not suitable for more than 10 users

**Suitability of Peer-To-Peer Network**

In the following situations peer-to-peer is appropriate.

- There are fewer than ten people in your organization
- The people in your organization are sophisticated computer users
- Security is not an issue or the user can be trusted to maintain good security
- There is no one central administrator who sets network policies.
- Costly to have an additional computer just to server files
- User can be relied upon to back up their own data
- User are physically close and no plans for expansion on the network

**Server-Based Network**




Server based networks provide centralized control over network resources, primarily by enforcing network security and control through the server's own configuration and setup. The computers used for servers usually incorporate faster CPUs, more memory, larger disk drives, ad extra peripherals (such as tape drives and CD ROM) when compare to end user machines (clients). In most cases, servers are dedicated to handle network requests from their clients.

**Advantages of Server-Based Network**

- Centralized user accounts, security, and access controls to simplify network administration.
- More powerful equipment means more efficient access to network resources.
- A single password for network login deliver access to all.
- Server-based networking makes the most sense for networks with 10 or more users or any networks where resources are used heavily.

**Disadvantages of Server-Based Network**

- At worst, server failure leads to whole network failure.
- Complex, special-purpose server software requires allocation of expert staff, which increases expanses.
- Dedicated hardware (server) and special software (NOS) add to the cost.

**Suitability of Server-Based Network**

In the following situations server-based is appropriate.

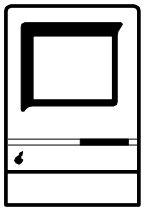
- There are more than ten people in your organization.
- Many of the people are not sophisticated computer users.
- Your organisation maintains information that must be centrally controlled.
- A central administrator will be Assigned for network setup and maintenance

## 1.3 Basic Components of Network

The most common components of a network are:

- Terminal
- Workstation
- Server
- Network interface card
- Communication media
- Network operating system
- Peripheral devices

### Terminal



Terminal

Over the years, the data terminal market has increased substantially and there are now literally hundreds of manufactures and many different kinds if terminal. However, the fact is that all of these terminals have been designed primarily to input and display information in some form or another. Therefore, even though specific characteristics such as screen size and keyboard layout may differ, they can generally be categorized into three simple groups.

**1. Dumb Terminals**

Dumb terminals are those which have limited functions and are driven with information from a host computer. Normally, they consist of a Cathode Ray Tube (CRT) display screen with a full alphanumeric keyboard and can be connected

directly to a computer system (host computer) through some sort of communications interface. In most cases, data is transmitted directly through the communication interface as it is typed on the keyboard.

**2. Intelligent Terminals**

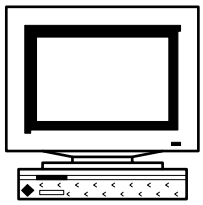
The category of intelligent or programmable terminals is probably the largest and widest ranging group. Unlike dumb terminals, intelligent terminals are equipped with a processor that can support an instruction set to direct the basic functions of the terminal. Like any other type of computer that has a processor, these terminals normally have additional memory and storage devices such as disc drives.

Intelligent terminal are, therefore, capable of stand-alone processing and can support a variety of software applications which, in turn, enable them to support a variety of communications interfaces through the use of emulation program. This is also means that, unlike dumb terminals, intelligent terminals are able to use addresses and sophisticated access method to transmit and receive messages.

**3. Graphic Terminals**

Graphic terminals are display devices that provide a means not only for displaying data in graphical form, but also for manipulating and modifying the data presented. Generally, graphic terminal keyboards have a number of specific or programmable function keys in addition to the full alphanumeric keys of a normal keyboard and the resolution of the display screen is normally a lot higher to enable more detailed displays

**Workstation**



Workstation

A workstation is a client. More specifically, it is a standalone computer equipped with it's own processor, system and application software. It can perform its functions independent of the network. To expand its resources and knowledge, it may get connected to a network.

**Server**

Network plays one of two basic roles at any given moment, the computer is either acting s a client or as a server. A server is a computer that shares its

Resources across the network, and a client are one that accesses shared resources. Depending on the size and requirements of the network, servers can be classified as below:

1. **File Server**

   A file server allows user to share files. It several LAN users need access to an application such as word processing, only one copy of the application software needs to reside on a file server. This copy can be shared among all the users. When a user requests to start an application, that application is downloaded into the users workstation.

   Consider the saving in disk space in a company having 100 users for application package that requires 10 MB of disk storage. Storage on the file server requires only 10 MB of disk space for all users. Storing the same application on 100 users' local disk drives will require 1,000 MB of disk space. This is only an example of one application. Same logic can be applied when hundreds of different application programs needed.

2. **Database Server**

   The database server was developed to solve the problem of passing an entire file over the medium. The most common example of a database server is the SQL server. Structured Query Language (SQL) is standard database definition, access, and update language for relational database. An SQL server accepts a database request, accesses all necessary records locally, and then sends only the result back to the requester (not the whole database).

3. **Print Server**

   Print server allows anyone on the network to have access to a printing service.

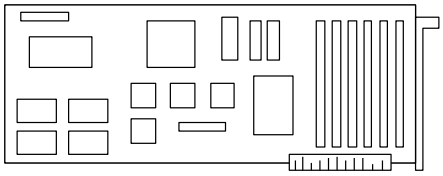
4. **Disk Server**

   It is server with large storage. A portion of storage is given to each user to store their files/data. It is very useful in university where each student is given a user account with password and some storage space in disk server. Once the student completes the education the same space can be assigned to new student.

5. **Dedicated Vs Non-Dedicated Server**

   **Many networks will let their user run** standard programs while their computer is simultaneously functioning as a server to others. A computer that both runs standard programs and lets other user see its data at the same time is said to be "non-dedicated server". Non-dedicated servers can be clever way of setting up a small LAN without having to buy any extra system. Dedicated server are specially assigned for network management and provided no general-purpose services.

**Network Interface Card**



NIC

Attaching a computer to a network requires a physical interface between computer and the networking medium. For PCs, this interface resides in a special network interface card (NIC), also known as network adapter or a network card that plugs into an adapter slot inside the computer's case. Laptops and other computers may include built-in interface or use special modular interface such as PC card interface, to accommodate a network adapter of some kind.

**For any computer, a NIC performs following crucial tasks:**

1. It establishes and manages the computer's network connection.
2. it translates digital data( of source computer) into signals (appropriate for the networking medium) for outgoing messages, and translates from signals into digital computer data for incoming messages.
3. Converts serial incoming data via cable into parallel data to for CPU, and vice versa.
4. It has some memory, which acts as a holding tank or buffer. It buffers the data to control the data flow.

**Chapter Review Questions**

1. Mount Kenya University has a network at the main campus. Which type of network do they have?
2. Mount Kenya University has started a centre in Kisumu with about 30 computers. Between a Peer-to-peer and client server network, which network type is the most appropriate and for what reasons?
3. Why would an organization choose to set-up a network?
4. Why is the client server network more common than the Peer-to-peer network in our current world?

**Books for further reading**


i. William Stallings (2010), **Data and Computer Communication,** 9th edition
ii. Behrouz A. Forouzan, (2006), **Data communication and networking**, 5th edition.
iii. Andrews. Tanenbaum, (2010) **Computer Networks**, 5th edition . Prentice-Hall PTR

# CHAPTER TWO

# TRANSMISSION MEDIA

**Learning Objectives**

By the end of this chapter the learner shall be able to;

i. Explain the different guided transmission medium such as the twisted pair, coaxial cable and fiber optic
ii. Explain different unguided transmission medium such as the satellite and microwave
iii. Explain the transmission impairments such as noise and attenuation

## 2.1 Introduction to Transmission Media

Communication is the activity or process of exchanging information in mutual understanding form. A computer system can be vast resource of information. Once this system is connected to a network, this information can be shared among all other users. A communication media is required to connect different computer systems to facilitate the information exchange. Following

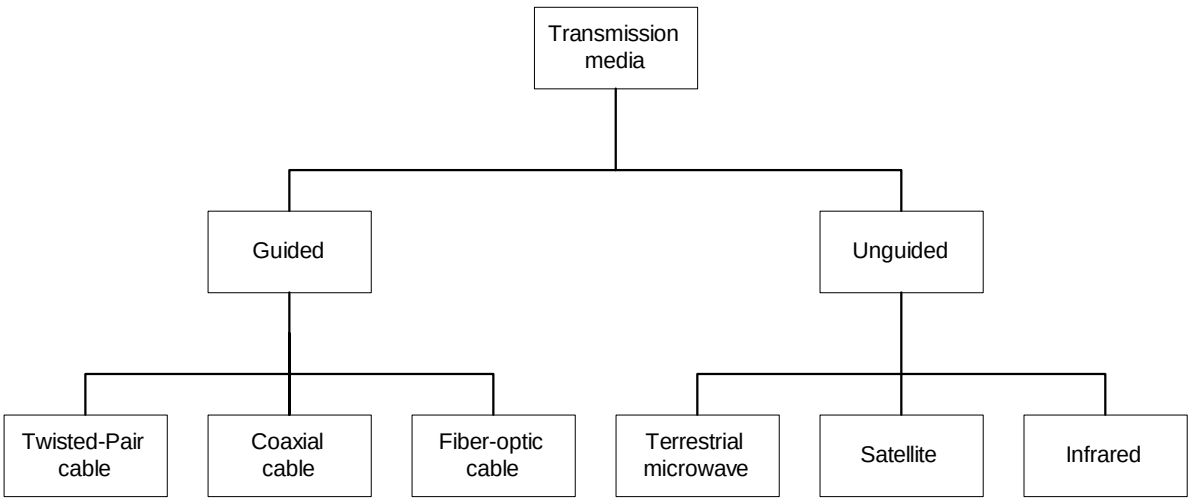



Figure 2.1 Types of transmission media

diagram will give a clear picture of different type of transmission media.

## 2.2 Guided Transmission Media

Guided/physical/non-wireless/bounded media have a physical link between sender and receiver. Mainly there are three categories of guided media: twisted-Pair, coaxial, and fiber-optic.

**Twisted-Pair Cable**

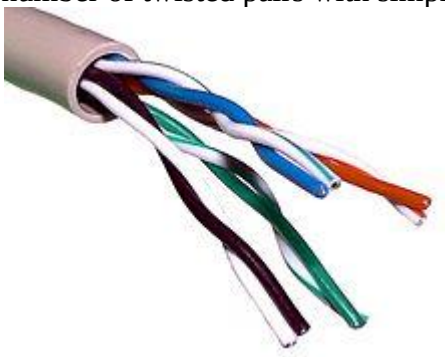
A twisted consist of two conductors (usually copper), each with its own colored plastic insulation. In the past, two parallel wires were used for communication. However, electromagnetic interference from devices such as a motor can create over noise those wires. If the two wires are parallel, the wire closest to the source of the noise gets more interference than the wire further away. Which results in an uneven load and a damaged signal.

If, however, the two wires are twisted around each other at regular intervals (between 2 to 12 twist per foot), each wire is the closer to the noise source for half the time and the further away the other half. With the twisting interference can be equalized for both wires. Twisting does not always eliminate the impact of noise, but does significantly reduce it

Twisted cable comes in two forms: unshielded and shielded.

**Unshielded Twisted Pair (UTP) cable**

UTP consists of a number of twisted pairs with simple plastic casing. UTP is commonly used in



telephone system.

The Electrical Industry Association (EIA) divides UTP into different categories by quality grade. The rating for each category refers to conductor size, electrical characteristics, and twists per foot.

**Category 1**: Applies to transmit traditional UTP telephones cabling, which is designed to carry voice but not data.

**Category 2**: Certifies UTP cabling for bandwidth up to 4 Mbps and consists of four pair of wires. Since 4 Mbps is slower than most networking technologies in the use today. Category 2 is rarely encountered in networking environment.

**Category 3**: Certifies UTP cabling for bandwidth up to 10Mbps. This includes most conventional networking technologies, such as 10BaseT Ethernet and 4Mbps token ring etc. Category 3 consists of four pairs, each having minimum 3 twist per foot.

**Category 4**: Certifies UTP cabling for bandwidth up to 10Mbps. This includes primarily 10BaseT Ethernet and 16Mbps token ring. Category 4 consists of four pairs.

**Category5**: Used for data transmission up to 100Mbps Category 5 also consists of four pairs.

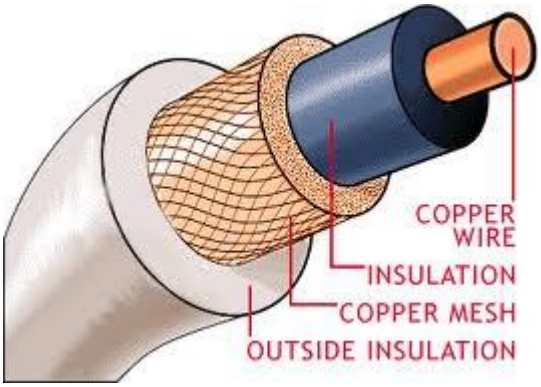
UTP is particularly prone to cross talk, and the shielding included with STP is designed specifically to reduce this problem.

**Shielded Twisted Pair (STP) cable**

STP includes shielding to reduce cross talk as well as to limit the effects of external interference. For most STP cables, this means that the wiring includes a wire braid inside the cladding or sheath material as well as a foil wrap around each individual wire. This shield improves the cable's transmission and interference characteristics, which, in tern, support higher bandwidth over longer distance than UTP.


**Coaxial Cable**: Coaxial cable, commonly called coax, has two conductors that share the same axis. A solid copper wire runs down the center of the cable, and this wire is surrounded by plastic foam insulation. The foam is surrounded by a second conductor, wire mesh tube, metallic foil, or

both. The wire mesh protects the wire from EMI. It is often called the shield. A tough plastic jacket forms the cover of the cable, providing protection and insulation.




Where Ethernet is concerned, there are two types of coaxial cable, called this Ethernet (also known as thinnet or thinwire,) and thick Ethernet (also known as thinnet or thickwire). The Institute of Electrical and Electronics Engineers (IEEE) designates these cable types as 10Base2 and 10Base5, respectively, where these notations indicates:

Total bandwidth for the technology: in this case, 10 means 10Mbps

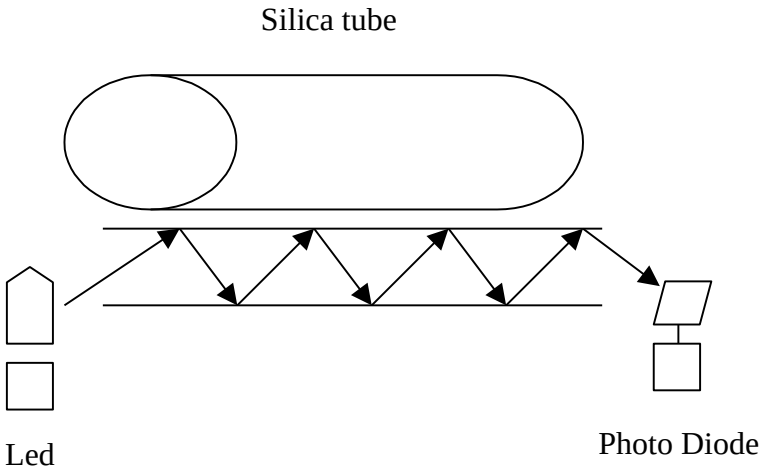
Base: indicates that the network uses baseband signaling and this applies to both types of cable.

2 or 5: a rough indicator of maximum segment length, measured in hundreds of meters; thinwire support a maximum segment length of 185 meters, which rounds up to 200; thickwire supports a maximum segment length of 500 meter

**Fiber Optic Cable**: fiber optic cable transmits light signals rather than electrical signals. It is enormously more efficient than the other network transmission media. As soon as it comes down in price (both in terms of the cable and installation cost), fiber optic will be the choice for network cabling.

A light pulse can be used to signal a ‘1’ bit; the absence of a pulse signals a ‘0’ bit. Visible light has a frequency of about 108 MHz, so the bandwidth of an optical transmission system is potentially enormous.

An optical transmission system has three components: the transmission medium, the light source and the detector. The transmission medium is an ultra-thin fiber of glass or fused silica. The light source is either a LED (Light Emit Diode) or a laser diode, both of which emits light pulses when a electrical current is applied. The detector is a photo diode, which generates an electrical pulse when light falls on it.




A cable may contain a single fiber, but often fibers are bundled together in the center of the cable. Optical fiber are smaller and lighter than copper wire. One optical fiber is approximately the same diameter as a human hair.

**Advantages of Fiber Optic**

- Noise resistance: it is immune to Electromagnetic Interference (EMI)
- Less signal attenuation: signal can run for miles without requiring regeneration
- Higher bandwidth: fiber optic cable can support dramatically higher bandwidths (and hence data rate) than all other cables. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available. A typical bandwidth for fiber optic is 100Mbps to 1Gbps.

**Disadvantages of Fiber Optic**

- Cost : most expensive among all the cables
- Installation / maintenance: is high
- Fragility : glass fiber is more easily broken than wire

**Summary Table of the Characteristic of All Cable Type**

| Factor | UTP | STP | Coaxial | Fiber Optic |
|---|---|---|---|---|
| Cost | Lowest | Moderate | Moderate | Highest |
| Installation | Easy | Fairly easy | Fairly easy | Difficult |
| Bandwidth Capacity | 10 Mbps | 16 Mbps | 10 Mbps | 100 Mbps – 1 Gbps |
| Node Capacity Per Segment | 2 | 2 | 30 (10Base2) 100 (10Base5) | 2 |
| Attenuation | High | High | Lower | Lowest |
| EMI | Most vulnerable to EMI | Less vulnerable than UTP | Less vulnerable than UTP | No effect by EMI |

## 2.3 Unguided Transmission Media

Unguided/non-physical/wireless/unbounded media have no physical link between sender and receiver.

There has been increasing need for mobile users to connect to a network. The answer for their needs is wireless. In wireless communications, space (air) is the medium for the signals.

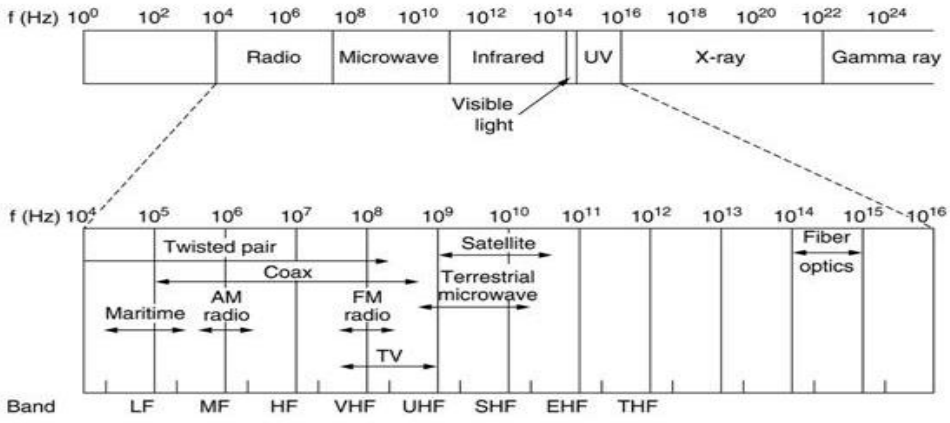
**Wireless networking has some advantages over wired networking:**

- No wires needed. Running wires can be difficult in some cases; such as wiring an existing building, wiring between buildings, wiring across mountains, etc.
- Staying connected is important for mobile users. Wireless networks allow users stay connected more hours each day. Users with laptops may roam their work space without losing network connection and without logging into another machine. This increases the productivity of workers.
- Wireless networks can grow without much difficulty compared with wired networks. Making a wired network larger often involves wiring and usually costly.
- Wireless networks are not confined to an area. There is no long term commitment as in the wired networks.

**Bandwidth for wireless transmission**

The principle of wireless communication is to send and receive electromagnetic wave using antenna. Several frequency bands are used for wireless communications.

- **Radio**—Frequencies between 30 MHz to 1 GHz
- **Microwave—**Frequencies between 1 GHz to 40 GHz
- **Infrared**—Frequencies between 3 x $10^{11}$ to 2 x $10^{14}$ Hz



The Electromagnetic spectrum used in communications
(From Tanenbaum Figure 2.11)

The Electromagnetic spectrum used in communications (From Tanenbaum Figure 2.11)

As you noticed from the above figure, there are some overlap between the bandwidths for wired media and wireless. The only difference is whether they have solid wires carrying signals or not.

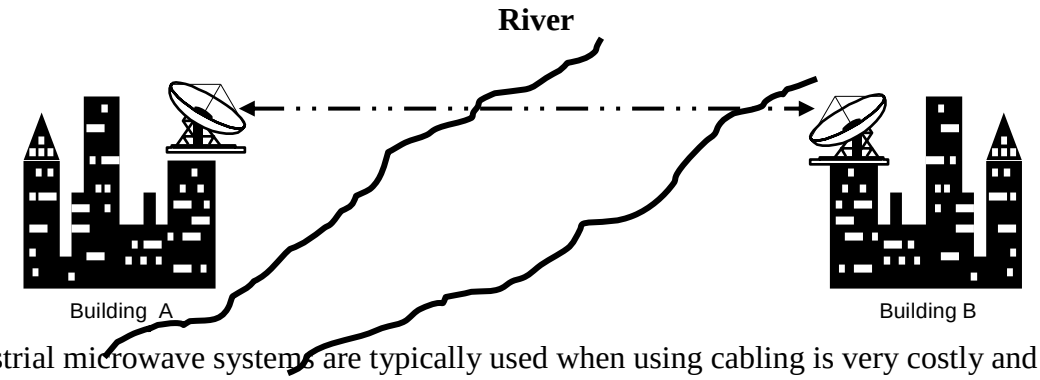
- Radio transmission: These are systems for AM or FM radio. They are one form of communications and not used for computer networks.
- Microwave transmission: We can classify them into three categories; Terrestrial microwave, Satellite

**Terrestrial Microwave**

Microwaves do not follow the curvature of the earth therefore require line of sight transmission and reception equipment. The distance coverable by line of sight signals depends to a large extend on the height of the antenna: the taller the antenna, the longer the sight distance. Height allows the signals to travel farther without being stopped by the curvature of the earth and raises

the signals above many surface obstacles, such as low hills and tall buildings that would otherwise block transmission.

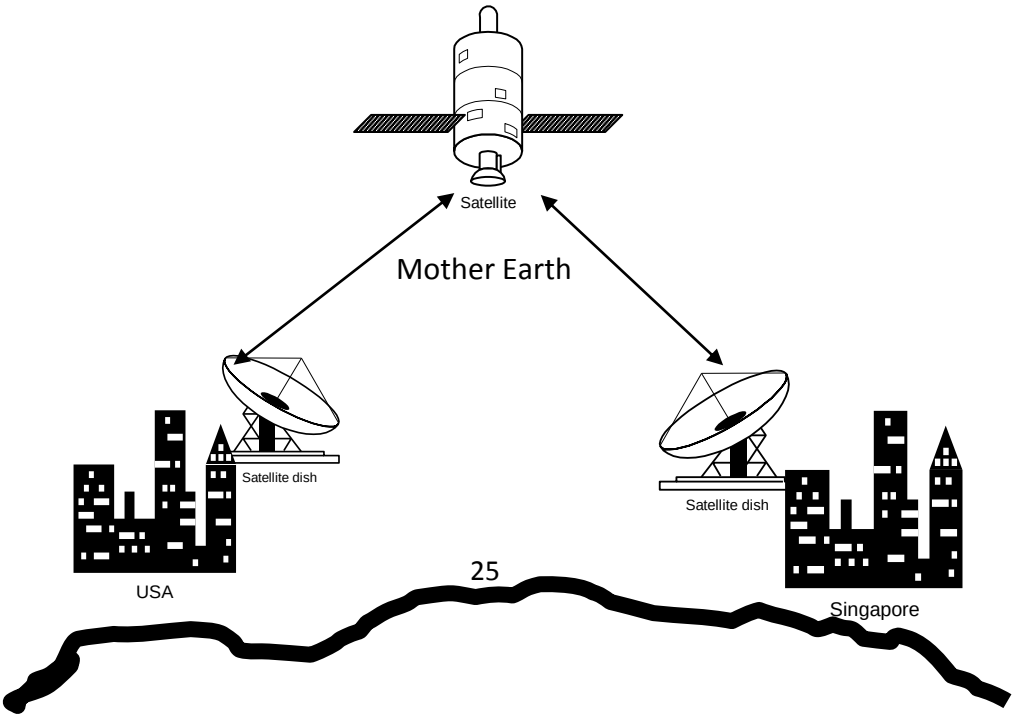
Microwave signals propagate in one direction at a time, which means that two frequencies are necessary for two ways communication such as telephone communication. One frequency is reserved for transmission in one direction and other for transmission in other. Each frequency requires its own transmitter and receiver. Today, both pieces of equipment usually are combined in a single piece of equipment called transceiver, which allows a single antenna to serve both frequencies and functions.




Terrestrial microwave systems are typically used when using cabling is very costly and difficult to set.

**Satellite Communication**

Satellite transmission is much like line of sight microwave transmission in which one of the stations is a satellite orbiting the earth. The principle is the same as terrestrial microwave, with a satellite acting as a super-tall antenna and repeater. Although in satellite transmission signals



must still travel in straight lines, the limitations imposed on distance by the curvature of the earth are reduced. In this way, satellite relays allow microwave signals to span continents and ocean with a single bounce.

Satellite microwave can provide transmission capability to and from any location on earth, no mater how remote. This advantage makes high quality communication available to undeveloped parts of the world without requiring a huge investment in ground based infrastructure. Satellite themselves are extremely expensive, of course, but leasing time or frequencies on one can be relatively cheap.

**Infrared Transmission**

Infrared media uses infrared light to transmit signals. LEDs transmit the signals, and photodiodes receive the signals. The remote control we use for television, VCR and CD player use infrared technology to send and receive signals.

Because infrared signals are in high frequency range, they have good throughput. Infrared signals do have a downside; the signals cannot penetrate walls or other objects, and they are diluted by strong light sources.

| Media | Advantages | Disadvantages | Bandwidth |
|---|---|---|---|
| Twisted Pair | Inexpensive<br>Easy to install<br>Experience | Sensitive to EMI<br>Short distance(100M)<br>Limited bandwidth<br>Easily tapped | Up to 600 MHz<br>Up to 1 Gbps |
| Coaxial cable | Higher bandwidth<br>Better noise immunity then Twisted Pair<br>Longer span than Twisted Pair | More expensive than Twisted Pair<br>Bigger than Twisted Pair<br>Easily tapped | Up to 1 GHz |
| Optical Fiber | Huge bandwidth<br>Longer repeater spacing<br>No EMI<br>High security<br>Small size | Expensive<br>Splicing/termination difficult | Up to few hundred GHz |
| Microwave | No wires | Cost high | 1 M – 10 Gbps |
| Satellite | No limit for location | Cost high<br>Long delay | 1 M – 10 Gbps |

## 2.4 Transmission Impairments:

With any communication system, there is a high possibility that the signal that is received will differ from the signal that is transmitted as a result of various transmission impairments. For analog signals, these impairments introduce various random modifications that degrade the signal quality. For digital signals, bit errors are introduced: A binary 1 is transformed into a binary 0, and vice versa.

The most significant impairments are the following:

- Attenuation
- Noise

**a) Attenuation**

When an electromagnetic signal is transmitted along any medium, it gradually become weaker at greater distances, this is referred to as attenuation. To solve this problem *amplifier* is used. The amplifier boosts the signals and extends the transmission distance.

**b) Noise**

Random electrical signals that can be picked up by the transmission medium and result in degradation of the data.

**c) Delay Distortion**

This is a common phenomenon with guided transmission media. The distortion is caused by the fact that the velocity of propagation of a signal through a guided medium varies with frequency. For a band limited signal, the velocity tends to be highest near the centre frequency and fall off toward the two edges of the band. Thus various frequency components of a signal will arrive at the receiver at different times. This effect is called delay distortion.

**d) Jitters**

Jitter is a variation or dislocation in the pulses of a digital transmission; it may be thought of, in a way, as irregular pulses. Jitter can manifest through variations in

amplitude, signal strength, and other elements of such waves. The usual causes include connection timeouts, connection time lags, data traffic congestion, and interference. Simply put, this jitter is an undesirable output of system flaws and interruptions.

**Chapter Review Questions**

1. Why do most organizations use guided media such as the twisted pair for their networks?
2. When is unguided media more appropriate to use than the guided media?
3. Explain the different transmission impairments.

**Books for further reading**


i. William Stallings (2010), **Data and Computer Communication,** 9th edition
ii. Behrouz A. Forouzan, (2006), **Data communication and networking**, 5th edition.
iii. Andrews. Tanenbaum, (2010) **Computer Networks**, 5th edition . Prentice-Hall PTR

# CHAPTER THREE

# NETWORK TOPOLOGIES

**Learning Objectives**

By the end of this chapter the learner shall be able to;

A. Explain the different network topologies and their operation in communication
B. Explain the advantages and the disadvantages of the different network topologies
C. Explain the different methods of medium access control such as CMSA/CD, token passing etc.

## 3.1 Introduction to Network topologies

The way in which the connections are made among all the computers is called the topology of the network. Network topology specifically refers to the physical layout of the network, specially the location of the computers and how the cable is run between them. Each topology has its own strengths and weaknesses.

The most common topologies are the bus, the star, the ring and the mesh.

### Bus Topology

The bus topology is the simplest and most common method for connecting computers. It is often used when a network installation is small, simple, or temporary. It is important to note that the bus topology is a Passive topology. This means that computers on the bus only listen for data being sent, they are not responsible for moving the data from one computer to the next. If one computer fails it has no effect on the rest of the network. In an active topology network, the computers regenerate signals and are responsible for moving the data through the network.

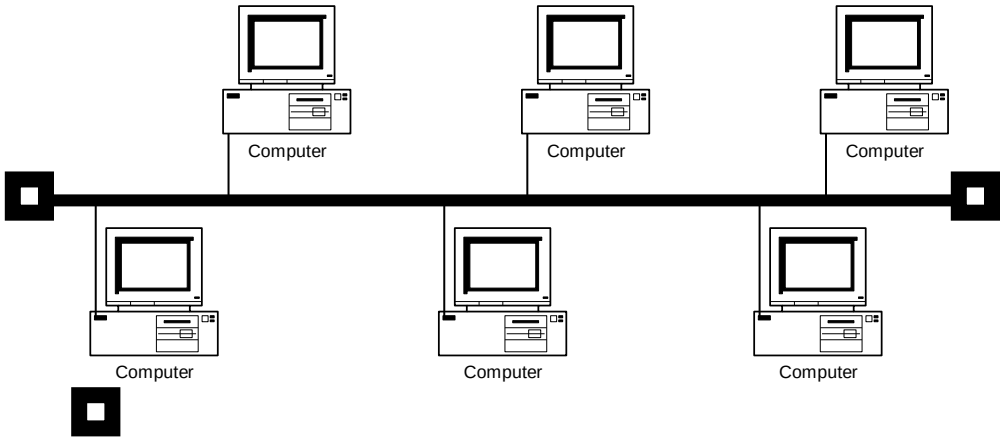



**Figure 3.1 Bus Network**

**How a Bus Network Works**

On a typical bus network, the entire computers are connected to a single cable. When one computer sends a signals using the cable, all the computers on the network receive the information, but only one (the one with the address that matches the one encoded in the message) accepts the information. The rest disregard the message.

Only one computer at a time can send a message; therefore, the number of computers attached to a bus network can significantly affect the speed of the network. A computer must wait until the bus is free before it can transmit.

Another important issue in bus network is termination. Without termination, when the signal reaches the end of the wire, it bounces back and travel back up the wire. When a signal echoes back and forth along the unterminated bus, it is called ringing. To stop the signals from ringing, terminators are attached at either end of the cable. The terminator absorbs the signals and stops the ringing.

**Advantages of Bus**

1. The bus is simple, reliable in very small network, and easy to use.
2. The bus requires the least amount of cable to connect the computers together and is therefore less expensive than other cabling arrangements.

3. It is easy to extend a bus. Two cables can be joined into one longer cable with a BNC barrel connector, making a longer cable and allowing more computers to jinn the network.

**Disadvantages of Bus**

1. Heavy network traffic can slow a bus considerably.
2. A break in the cable or lake of proper termination can bring the network down.
3. It is difficult to troubleshoot a bus.

**Bus topology is appropriate in following situation:**

- The network is small
- The network will not be frequently reconfigured.
- The least expensive solution is required.
- The network is not expected to grow much

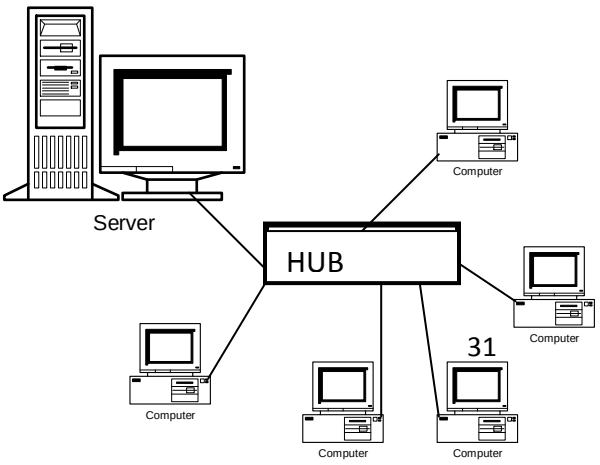
**Star Topology**

In a star topology, each device has a dedicated point to point link only to central controller, usually called a *hub*.

**How a Star Network Works**

Each computer on a star network communicates with a central hub that resends the message either to all the computers (in a *broadcast star* network) or only to the destination computer (in a *switched star* network). The hub can be active or passive.

Star topology



An active hub regenerates the electrical signal and sends it to all the computers connected to it. This type of hub is often called a multiport repeater. Active hub requires electrical power to run. A passive hub, such as wiring panels, merely acts as a connection point and does not amplify or regenerate the signal. Passive hubs do not require electrical power to run.

Using a hybrid hub, several types of cable can be used to implement a star network. Hybrid hub is used to connect different types of cables. It is used to maximise the network's efficiency and utilise the benefits different cables.

**Advantages of the Star**

1. It is easy to modify and add new computers to a star network without disturbing the rest of the network. You simply run a new line from the computer to the central location and plug it into the hub. When the capacity of the central hub is exceeded, it can be replaced with one that has a larger number of ports to plug lines into (or multiple hubs can be connected together to extend the number of ports)
2. The centre of a star network is a good place to diagnose network faults. Intelligent hubs (hubs with microprocessors that implement features in addition to repeating network signals) also provide for centralised monitoring and management of the network.
3. Single computer failure does not necessarily bring down the whole star network.
4. Several types of cable can be used in the same network with a hybrid hub.

**Disadvantages of Star**

1. If the central hub fails, the whole network fails to operate.
2. It cost more to cable a star network.

**Star topology is appropriate in following situation:**

1. It must be easy to add or remove client computer.
2. It must be easy to troubleshoot.
3. The network is large.

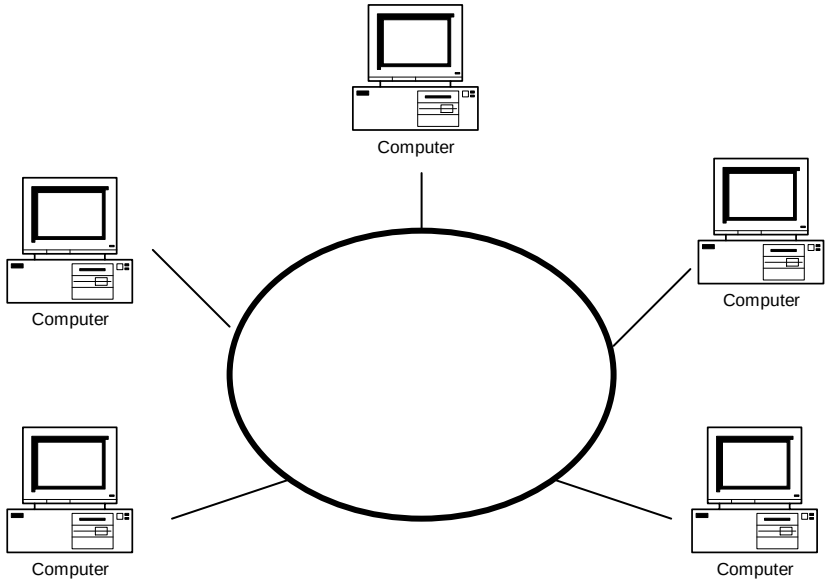
4. The network is expected to grow in the future.

**Ring Topology**

In a ring topology, each computer is connected directly to the next computer in line, forming a circle of cable. It uses token to pass the information from one computer to another.

**How a Ring Network Works**

Every computer is connected to the next computer in the ring, and each retransmit what it receives from the previous computer. The message flow around the ring in one direction. Since each computer retransmits what it receives, a ring is an active network and is not subject to the signal loss problem a bus experience. There is no termination because there is no end to the ring




Token passing a method of sending data in a ring. A small packet called the token passed around the ring to each computer in turn. If a computer has information to send, it modifies the token, adds address information and the data and sends it down the ring. The information travels around the ring until it either reaches its destination or returns to the sender. When the intended destination computer receives the packet, it returns a message to the sender including its arrival.

A new token is then created by the sender and sent down the ring, allowing another station to capture the token and begin transmission.

A token can circle a ring 200 meters in diameter at about 10,000 times a second.

**Advantages of Ring**

1. All the computers have equal access to the network.
2. Even with many users, network performance is even
3. Allows error checking, and acknowledgement.

**Disadvantages of Ring**

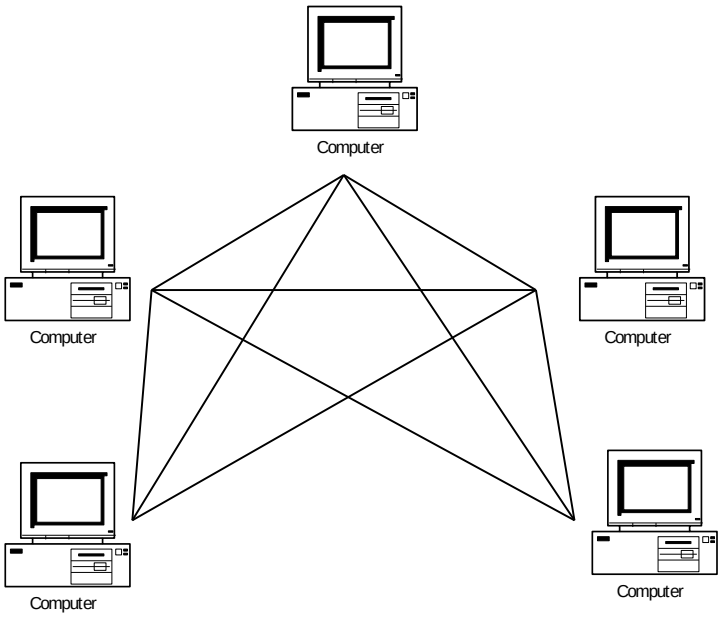
1. Failure of one computer can affect the whole network.
2. It is difficult to troubleshoot the ring network.
3. Adding or removing computers disturbs the network.

**Ring Topology is Appropriate in Following Situation:**

- The network must operate reasonably under a heavy load
- A higher-speed network is required.
- The network will not be frequently reconfigured.

**Mesh Topology**

In a mesh topology, every device has a dedicated point to point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. A fully connected mesh network therefore has n (n-1)/2 physical channels to link n devices. To accommodate that many links, every device on the network must have n-1 input/output ports.




Most mesh topology network are not true mesh networks. Rather, they are hybrid mesh networks, which contain some redundant links but not all.

**Advantages of Mesh**

1. Because of the dedicated link, no traffic between computers.
2. Failures of one node computer not affect rest of the network.
3. Because of the dedicated link privacy and security are guaranteed
4. Point to point links make fault identification and fault isolation easy.

**Disadvantages of Mesh**

1. Due to the amount of cabling and number of input output ports, it is expensive.
2. Large space is required to run the cables.
3. Installation and reconfiguration are difficult.

**When a Mesh Appropriates to Use**

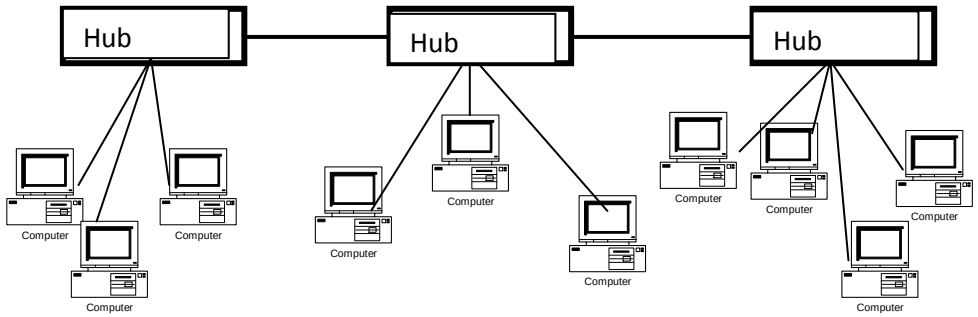
1. Direct transmission is required for privacy reason
2. Need to have dedicated lint for fast transmission.

**Variations of the Major Topologies**

## Hybrid Star

A star network can be extended by placing another star hub where a computer might otherwise go, allowing several more computers or hubs to be connected to that hub.

## Star Bus




## Star Bus Topology

The star bus topology combines the bus and the star, linking several star hubs together with bus trunks. If one computer fails, the hub can detect the fault and isolate the computer. If a hub fails, computers connected to it will not be able to communicate, and the bus network will be broken into two segments that can not reach each other.

## Hybrid Topologies

Often a network combines several topologies, as subnetworks linked together are a large topology. For instance one department of business may have decided to use a bus topology while another department has a ring. The two can be connected to each other a central controller in a star topology.

## 3.2 Medium access control methods

A network of computers based on multi-access medium requires a protocol for effective sharing of the media. As only one node can send or transmit signal at a time using the broadcast mode, the main problem here is how different nodes get control of the medium to send data, that is *"who goes next?".* The protocols used for this purpose are known as *Medium Access Control (MAC) techniques*. The key issues involved here are - *Where* and *How* the control is exercised. *'Where'* refers to whether the control is exercised in a *centralised* or *distributed* manner. In a centralised system a master node grants access of the medium to other nodes. A centralized scheme has a number of advantages as mentioned below:

- Greater control to provide features like priority, overrides, and guaranteed bandwidth.
- Simpler logic at each node.
- Easy coordination.

Although this approach is easier to implement, it is vulnerable to the failure of the master node and reduces efficiency. On the other hand, in a distributed approach all the nodes collectively perform a medium access control function and dynamically decide which node to be granted access. This approach is more reliable than the former one.
*'How'* refers to in what manner the control is exercised. It is constrained by the topology and trade off between cost-performance and complexity.

**Medium Access Control techniques are designed with the following goals in mind.**

- **Initialisation**: The technique enables network stations, upon power-up, to enter the state required for operation.
- **Fairness**: The technique should treat each station fairly in terms of the time it is made to wait until it gains entry to the network, access time and the time it is allowed to spend for transmission.
- **Priority**: In managing access and communications time, the technique should be able to give priority to some stations over other stations to facilitate different type of services needed.

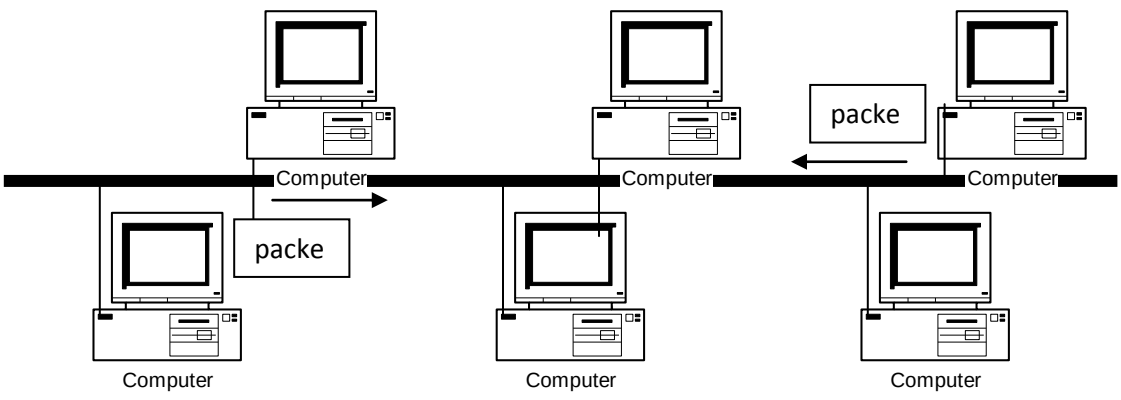
- **Limitations to one station**: The techniques should allow transmission by one station at a time.
- **Receipt**: The technique should ensure that message packets are actually received (no lost packets) and delivered only once (no duplicate packets), and are received in the proper order.
- **Error Limitation**: The method should be capable of encompassing an appropriate error detection scheme.
- **Recovery**: If two packets collide (are present on the network at the same time), or if notice of a collision appears, the method should be able to recover, i.e. be able to halt all the transmissions and select one station to retransmit.
- **Reconfigurability**: The technique should enable a network to accommodate the addition or deletion of a station with no more than a noise transient from which the network station can recover.
- **Compatibility**: The technique should accommodate equipment from all vendors who build to its specification.
- **Reliability**: The technique should enable a network to confine operating inspite of a failure of one or several stations.

For a successful data transmission, following access methods can be used in a network.

**Contention**

In contention based network, computers sent data whenever they had data to send. This might work well in a small environment when little data is being sent along the cable. But as more computers send data, the messages collide more frequently, must be resent, and then collide again. Soon there will be a communication breakdown.

**Figure 6.4 Collision in Contention Method**



To organize contention based network, two carrier access method were created:

1. **Carrier Sense multiple Access with Collision detection (CSMA/CD):** is one of the most popular ways to regulate network traffic. Used by Ethernet, this access method prevents collision by listening to the channel to see if another computer is sending data. If the computer does not sense data on the line, it sends its message. If another computer is using the channel, the computer waits a random amount of time and then checks again. This process is continued until the channel is free and the computer can send the data.

   **Advantages:**

   a) Inexpensive to implement.

   b) Fast in a small network with low traffic.

   **Disadvantages:**

   a) Slow in a large network with high traffic.

   b) Does not support priority. A single computer can block all other computer if it has very long message to send.

2. **Carrier senses multiple access with collision avoidance (CSMA/CA):** It uses collision avoidance, rather than detection, to prevent collision. With CSMA/CA, once the computer senses that no other computer is using the network, it signals its intent to transmit data. Any other computer with data to sensed wait when they receive the "intent-to-transmit" signal and send their intent-to-transmit signals when they see that channel is free. Although this method is more reliable than CSMA/CD in avoiding collision, the additional overhead created by the "intent-to-transmit" packets significantly reduces the speed of any network using this method.

**Network Architecture**

- Ethernet (CSMA/CD)
- LocalTalk (CSMA/CA)

**Token Passing**

Using this channel access method, a special packet called the "token" is passed from one computer to the next sequentially. Only the computer holding token can send data. A computer can keep token only a specific amount of time. If the computer with the token has no data to send, it passes the token to the next computer.

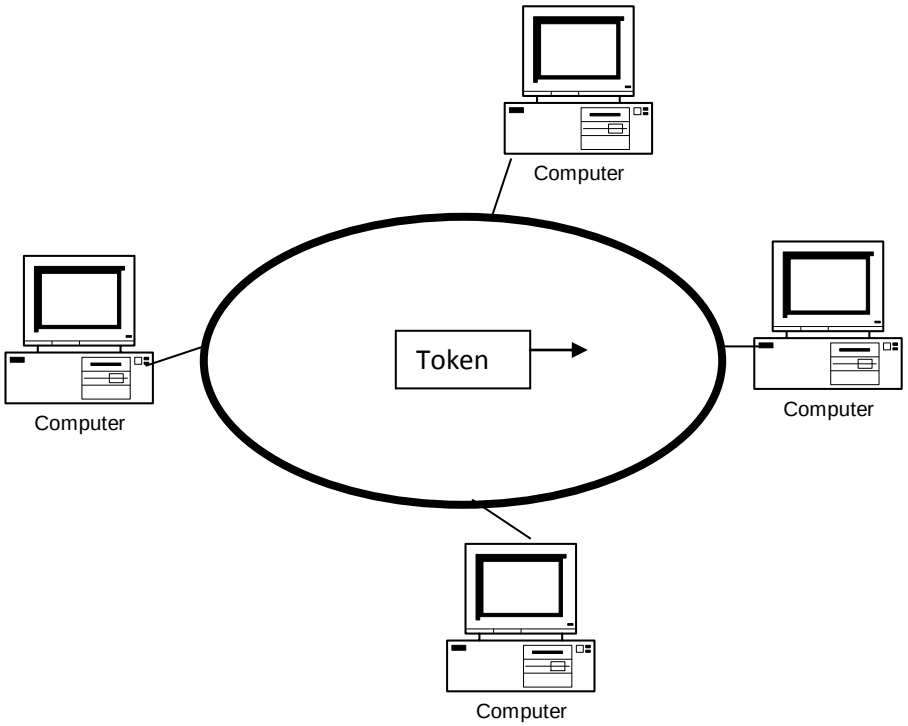



**Figure 6.5 Token Ring**

**Advantages:**

a) Because only the computer with the token can transfer data, collisions are avoided with this method.

b) All the computers have equal access to the channel. Because of this equality, token passing network is best suited for time-sensitive environment. For example banking transaction and database queries.

**Disadvantages:**

a) Even if only one computer on the network has data to send, it must wait until it receives the token. If its data is large enough it will more than one turns of token to finish the transmission, means further delay.

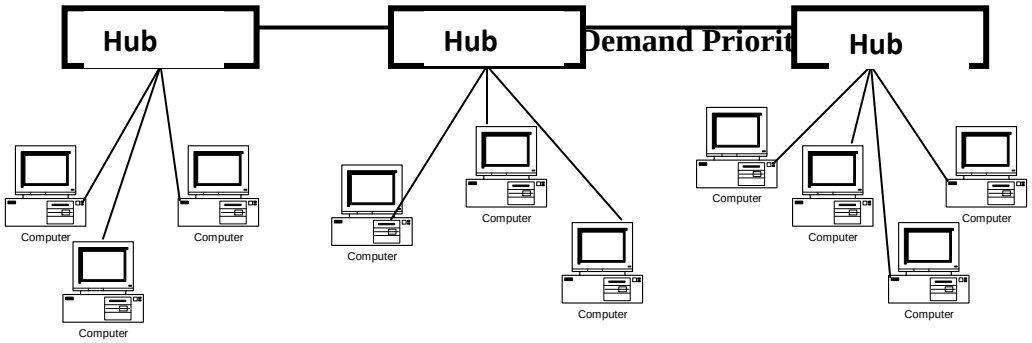
b) The process of creating and passing the token is complicated and requires more expensive equipment than contention based network.

**Network Architecture**

- Token ring
- ARCNet

**Demand Priority**

Demand priority is a recent channel access method and relies on following method.




Intelligent hubs are used to control access to the network. The hub searches all connections in a round robin fashion. When an end node (computer) has data to send, it transmits a "demand signal" to the hub. The hub then sends and acknowledgement that the node can start transmitting its data.

Unlike other channel access methods, demand priority allows for certain computers to be assigned a higher priority than other. If multiple computers make simultaneous demands, the computer with highest priority is allowed to transmit first. Demand priority makes the most efficient use of the available network media. Rather than wasting time addressing computers that do not have data to send, hubs using demand priority cannel access respond only when computers signal the hub for service. Also packets are not broadcast in demand priority network

as they are in CSMA/CD and CSMA/CA network but, instead, are sent from the computer to the hub and from the hub directly to the destination. This eliminates traffic on the network.

**Advantages:**

a) Very fast in high and low traffic environments

b) No collision

c) Provide priority

**Disadvantages:**

a) Expensive because special equipment is required.

b) Lower priority may starve for service

**Network architecture:**

- 100VG-AnyLAN

**Polling**

Polling is one of the oldest ways of controlling access to the network. a central controller, often referred to as the "primary device", ask each computer (the secondary device) on the network if it has data to send. If so, the computer is allowed to send data, up to a certain amount of time; then it is the next computer's turn.

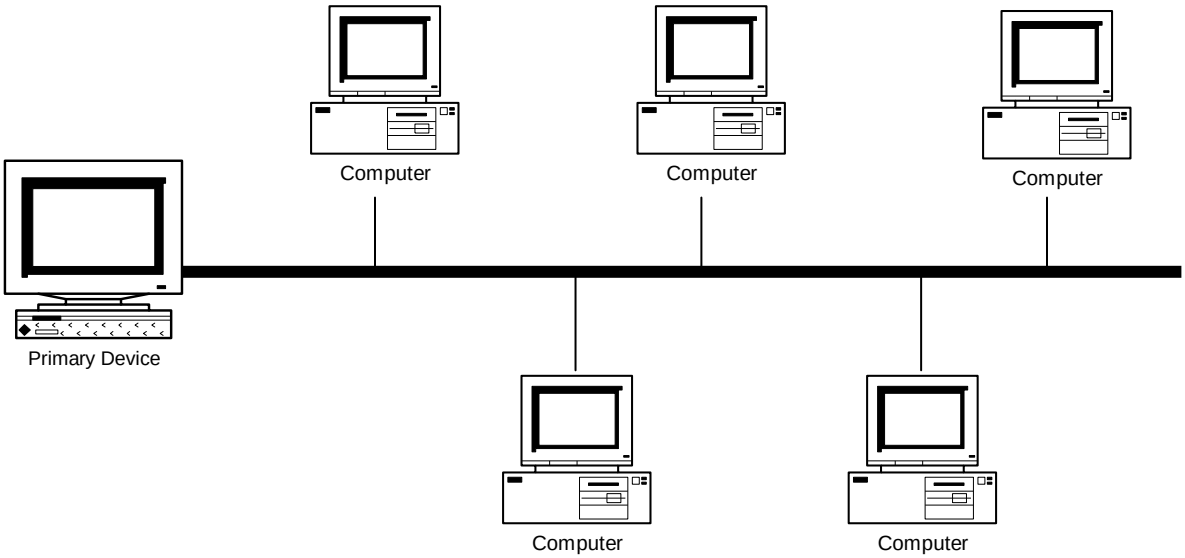



**Figure 6.7 Polling**

**Advantages:**

a) Like token passing, it allows all computers equal access to the channel, and no single computer can monopolize the media.

b) The central controller allows for centralized management, and certain computers can receive priority over other computers; they can be polled more often or be allowed to send data for longer period of time than the remaining computers.

**Disadvantages:**

a) Does not make efficient use of the media.

b) If the primary device fails, the whole network fails.

c) Increased expenses because of the primary device.

**Network Architecture**

- IBM's SNA

**Chapter Review Questions**

1. Mount Kenya University main campus has about 400 computers. Recommend a network topology for the university giving reasons for your choice.
2. Give reasons why the bus and ring topologies are inappropriate for today's networks.
3. Explain the concept of the token and how a computer gains access to the network.

**Books for further reading**


1. William Stallings (2010), **Data and Computer Communication,** 9th edition
2. Behrouz A. Forouzan, (2006), **Data communication and networking**, 5th edition.
3. Andrews. Tanenbaum, (2010) **Computer Networks**, 5th edition . Prentice-Hall PTR

# CHAPTER FOUR

# OSI LAYER AND TCP/IP LAYERS

**Learning Objectives**

By the end of this chapter the learner shall be able to;

A. Explain the advantages of a layered model
B. Explain the seven layers of the Open Systems Interconnection (OSI) and it's importance in networking
C. Explain the four TCP/IP layers

## 4.1 Introduction

### OSI Reference Model

OSI (Open System Interconnection) is the most widely accepted model for understanding the network communication. It is developed by ISO (International Standards Organization) in 1977. ISO is a multinational body dedicated to worldwide agreement on international standards. It covers all aspects of network communications in OSI reference model. An open system is a set of protocols that allows any two different systems to communicate regardless of the underlying architecture. Vendor-specific protocol close off communication between unrelated systems.

The purpose of OSI model is to open communication between different system without requiring changes to the logic of the underlying hardware and software. The OSI is not a protocol; it is model for understanding and designing a network architecture that is flexible, robust and open for communication with other systems.

### Layered Architecture of OSI

The OSI model has seven layers. Number of layers in any model is derived on following principles.

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well define function.
3. The function of each layer should be chosen with an eye towards defining internationally standardized protocol

4. The layer boundaries should be chosen to minimize the information flow across the interface.
5. The number of layers should be large enough that distinct function need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy

## 4.2 Advantages of a Layered Network Architecture

**Advantages of Layered Network Architecture**

- Provide modular approach for any network architecture
- A new layer can be introduced any time (if required) without interfering other layers.
- A layer can be removed easily if it's functions become obsolete.
- Modification to a particular layer can be done without interfering other layers.

**Disadvantages of Layered Network Architecture**

- Increases the address overhead in data packet as it travels from bottom layer to the top layer.

## 4.3 The OSI 7 layer model

The 7 layers of the OSI model can be split into 2 halves, those which provides *interconnection* services and those which provide *internetworking* services. Each layer within the model provides a set of services to the layer above and enhances the service provided by the layer below.

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

**a) The Interconnection Layers**

Interconnection group of standards makes up the bottom 4 layers of the OSI model, which are known as the *physical, data link, network and transport layers.*

- The *physical layer* defines the functional, procedural and physical interfaces of communication links between equipment. For example, plug specifications, and pin allocations.
- The *data link* layer adds error-checking information and formats data for physical transmission.
- The *network layer* provides routing and multiplexing services.
- The *transport layer* includes error detection and correction as well as multiplexing. Its basic function is to enhance the quality provided by the network layer below, if this is necessary.

**b) The Internetworking Layers**

The internetworking group includes the top 3 layers of the OSI model and basically provides the support services for the user applications. They are known as the *session, presentation, and application* layers.

- The *session layer* provides the organization, synchronization and timing of the exchange of the data between end systems.
- The *presentation layer* is concerned with now the information to be exchanged. This includes resolving character set differences, such as ASCII to EBCDIC, providing text compression and encryption/decryption services.
- The *application layer* provides support for the user applications, which wish to exchange information. (i.e. file transfer)

**Functions Each Layer**

**1. Physical Layer**

The physical layer co-ordinates the functions required to transmit a bit streams over a physical medium. It deals with the mechanical and electrical specifications of the primary connections, such as cables and connectors.

It also handles:

- **Line configuration:** how can two or more devices be linked physically? Are transmission lines to be shared or limited to use between two devices?
- **Data transmission mode:** Is the transmission mode simplex or duplex?
- **Topology:** How are the networking devices arranged?
- **Bit synchronization:** deals with synchronization between sender and receiver

2. **Data Link Layer**

The main purpose of the data link layer is to deliver data units (group of bits) from one station to the next station (node-to-node) without error. It accepts packets from the network layer and packages the information into data units called frames to be presented to the physical layer for transmission. The data link layer adds header (contains sender's and receiver's address) and trailer (contains control information, such as routing, segmentation, CRC etc) to the data being sent.

**Data link layer is responsible for following:**

- **Node to node delivery:** the data link layer is responsible for node to node delivery.
- **Addressing:** Adds header and trailer to the data packet.
- **Flow control:** It regulates the amount of data that can be transmitted at one time.
- **Error handling:** Data link layer protocols provide for data recovery, usually by having the entire frame retransmitted.

3. **Network Layer**

The network layer is responsible for the source to destination delivery of packet across multiple network links. Whereas the data link layer oversees station to station (node to node) delivery. The network layer ensures that each packet gets from its point of origin to its

destination successfully and efficiently. For this purpose the network layer provides two reliable services switching and routing.

Switching refers to temporary connection between physical links, resulting in longer links for network transmission; i.e. long distance telephone services.

Routing means selecting the best path for sending a packet from one point to another when more than one path is available. In this case, each packet may take a different route to the destination. Where the packets are collected and resembled into their original order.

**Network layer is responsible for following:**

- **Source to destination delivery:** moving the packet from its point of origin to its intended destination across multiple network links.
- **Routing:** Deciding which of the multiple paths a packet should take. Routing considerations include speed and cost.
- **Multiplexing:** using a single physical line to carry data between many devices at the same time.

4. **Transport Layer**

The transport layer is responsible for source to destination (end to end) delivery of the entire message. Whereas the network layer oversees end to end delivery of individual packets, it does not recognize any relationship between those packets.

**Transport layer is responsible for following:**

- **End to end message delivery:** conforms the transmission and arrival of all packets of a message at the destination point.
- **Segmentation and reassembling:** The transport layer Header contains sequence, or segmentation number. These numbers enable the transport layer to reassemble the message correctly at the destination and to identify and replace packet lost in transmission.

5. **Session Layer**

The session layer is the network *dialog controller.* It establishes, maintains, and synchronizes the link between communicating devices. It also ensures that each session close appropriately rather than shutting down abruptly and leaving the user hanging.

**Session layer is responsible for following:**

- **Session management:** Dividing a session into subsessions by the introduction of checkpoint ad separating *long messages* into shorter units, called dialog units appropriate for transmission.
- **Synchronization:** Deciding in what order to pass the dialog units to the transport layer, and where in the transmission to require conformation from the receiver.
- **Dialog control:** Deciding who sends, and when.
- **Graceful close:** Ensuring that the exchange has been completed appropriately before the session close.

**6. Presentation Layer**

The presentation layer ensures interoperability among communicating devices. It is responsible for code conversion (e.g. from ASCII to EBCDIC and vice versa), if required.

The presentation layer is also responsible for the encryption and decryption of data for security purposes. It also handles the compression and expansion of data when necessary for transmission efficiency.

**Presentation layer is responsible for following:**

- **Translation:** changing the format of message (e.g. from ASCII to EBCDIC and vice versa).
- **Encryption/Decryption:** handles encryption and decryption of data for security purposes.
- **Compression: It** also handles the compression and expansion of data when necessary for transmission efficiency.
- **Security:** validates passwords and log-in codes.

## 7. Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interface and support for services such as electronic mail, remote file access and transfer.

**Presentation layer is responsible for following:**

- **Mail services:** provides the basis for electronic mail forwarding and storage.
- **Directory services: Provides** distributed database sources and access for global information about various object and services.
- **File access, transfer, and management:** Allows a user at a remote computer to access files in another host (to make changes or read data); to retrieve files from a remote computer for use in the local computer.

**Assuming two hosts follow OSI model, example of files transferring from host A to host B.**

**Host A:**

1. User will issue a file transfer command to the Application Layer. (initiates or accepts a request)
2. The Application Layer then passes the file to the Presentation Layer, which may reformat the data. (handles protocol conversion, data encryption or decryption, text compression)
3. The data is then passed to the Session Layer, which requests that a connection be provided to the destination host and passes the data to Transport Layer.(handles session setup and Session close)
4. Transport Layer breaks the file into manageable chunks of data for transmission and passes them to network layer. (Handles flow control, error recovery).
5. Network Layer selects the data's route and then passes the data to the data link layer. (handles addressing, route discovery and route selection, error control)
6. Data link Layer adds extra information to the data so that it can be checked for errors at the receiving end. And passes the data to the physical layer. (handles CRC cyclic redundancy check).
7. Physical Layer takes the resulting data stream and transmit it across the physical link to the Host B (handles mechanical and electrical characteristic to provide and maintain physical connection)

**Host B**

1. Host B's physical layer receives the bits and passes them on to the
2. Data link layer.
3. Data link layer verifies that no errors occurred, and then passes the data onto the network layer.
4. Network Layer ensures that the selected route is proving reliable, and then passes the data onto the transport layer.
5. Transport Layer reassembles the small chunks of data into the file being transferred, and then passes it onto the session layer.
6. Session Layer determines if the transfer is complete, and if so, may break down the session, in effect ending the communication. It passes the data onto presentation layer.
7. Presentation Layer may reformat the data, performing any necessary conversion, data are passed on to application layer.
8. Host B's user can then access the transferred information through the Application Layer.

## 4.4 The TCP/IP Model Layers

The TCP/IP model uses four layers that logically span the equivalent of the top six layers of the OSI reference model; this is shown below. (The physical layer is not covered by the TCP/IP model because the data link layer is considered the point at which the interface occurs between the TCP/IP stack and the underlying networking hardware.) The following are the TCP/IP model layers, starting from the bottom.

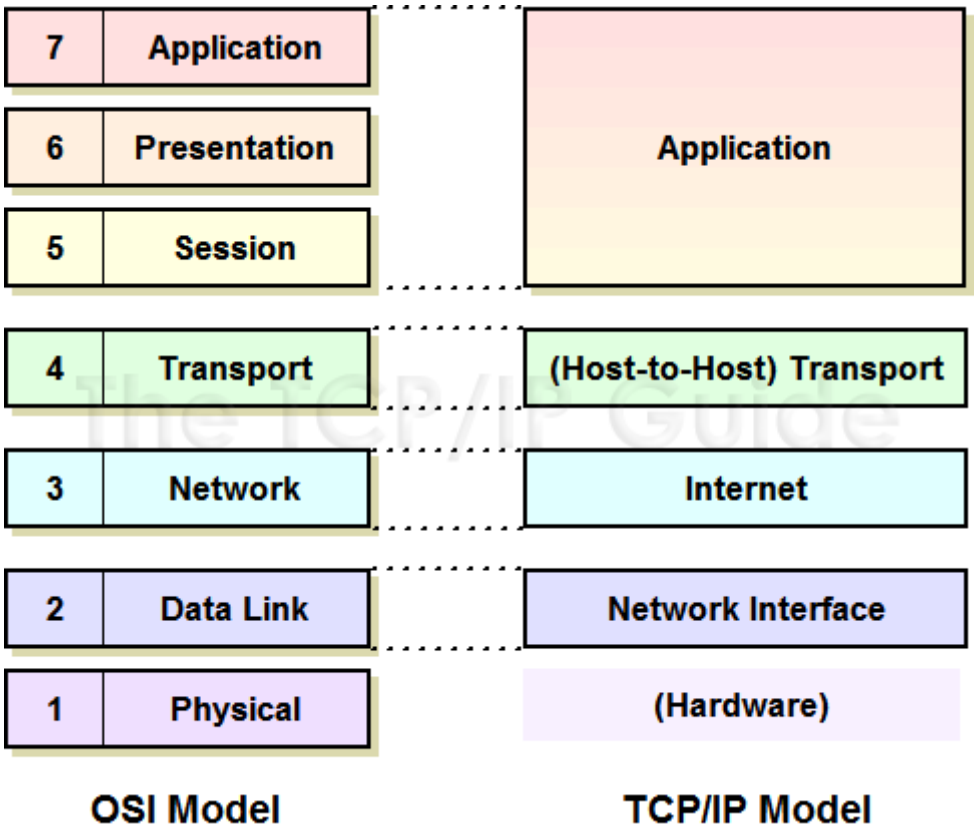



**Figure 20: OSI Reference Model and TCP/IP Model Layers**

The TCP/IP architectural model has four layers that approximately match six of the seven layers in the OSI Reference Model. The TCP/IP model does not address the physical layer, which is where hardware devices reside. The next three layers—*network interface*, *internet* and *(host-to-host) transport*—correspond to layers 2, 3 and 4 of the OSI model. The TCP/IP *application* layer conceptually "blurs" the top three OSI layers. It's also worth noting that some people consider certain aspects of the OSI session layer to be arguably part of the TCP/IP host-to-host transport layer.

**Network Interface Layer / Host- to-network**

As its name suggests, this layer represents the place where the actual TCP/IP protocols running at higher layers interface to the local network. It is equivalent to the data link layer (layer two) in the OSI Reference Model and is also sometimes called the *link layer*. You may also see the name *network access layer*.

### Internet Layer

This layer corresponds to the network layer in the OSI Reference Model (and for that reason is sometimes called the *network layer* even in TCP/IP model discussions). It is responsible for typical layer three jobs, such as logical device addressing, data packaging, manipulation and delivery, and last but not least, routing. At this layer we find the Internet Protocol (IP), arguably the heart of TCP/IP, as well as support protocols such as ICMP and the routing protocols (RIP, OSFP, BGP, etc.) The new version of IP, called IP version 6, will be used for the Internet of the future and is of course also at this layer.

### (Host-to-Host) Transport Layer

This primary job of this layer is to facilitate end-to-end communication over an internetwork. It is in charge of allowing logical connections to be made between devices to allow data to be sent either unreliably (with no guarantee that it gets there) or reliably (where the protocol keeps track of the data sent and received to make sure it arrives, and re-sends it if necessary). It is also here that identification of the specific source and destination application process is accomplished

The formal name of this layer is often shortened to just the *transport layer*; the key TCP/IP protocols at this layer are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The TCP/IP transport layer corresponds to the layer of the same name in the OSI model (layer four) but includes certain elements that are arguably part of the OSI session layer. For example, TCP establishes a connection that can persist for a long period of time, which some people say makes a TCP connection more like a session.

### Application Layer

This is the highest layer in the TCP/IP model. It is a rather broad layer, encompassing layers five through seven in the OSI model. While this seems to represent a loss of detail compared to the OSI model, I think this is probably a good thing! The TCP/IP model better reflects the “blurry” nature of the divisions between the functions of the higher layers in the OSI model, which in practical terms often seem rather arbitrary. It really is hard to separate some protocols in terms of which of layers five, six or seven they encompass. (I didn't even bother to try in this Guide which

is why the higher-level protocols are all in the same chapter, while layers one through four have their protocols listed separately.)

Numerous protocols reside at the application layer. These include application protocols such as HTTP, FTP and SMTP for providing end-user services, as well as administrative protocols like SNMP, DHCP and DNS.

**Chapter Review Questions**

1. Explain the functions of the seven layers of the OSI model?
2. What are the advantages of a layered model
3. Compare and contrast the OSI model and the TCP/IP model

**Books for further reading**


i. William Stallings (2010), **Data and Computer Communication,** 9th edition
ii. Behrouz A. Forouzan, (2006), **Data communication and networking**, 5th edition.
iii. Andrews. Tanenbaum, (2010) **Computer Networks**, 5th edition . Prentice-Hall PTR

# CHAPTER FIVE

# CONECTING DEVICES

**Learning Objectives**

By the end of this chapter the learner shall be able to;

i. Explain the different devices used in constructing a computer network
ii. Explain the different networking devices such as the Hub, switch etc.
iii. Explain the different internetworking devices such as the Router, Bridge etc.

## 1.1 Introduction to Networking devices

Networking means connecting two or more devices for the purpose of sharing data and resources. Setting a small network is fairly simple task but once the network start to grow and become a local area network it may need to cover more distance than its media can handle effectively. Or the number of station may be too great for efficient communication or management of the network, and the network may need to e subdivided.

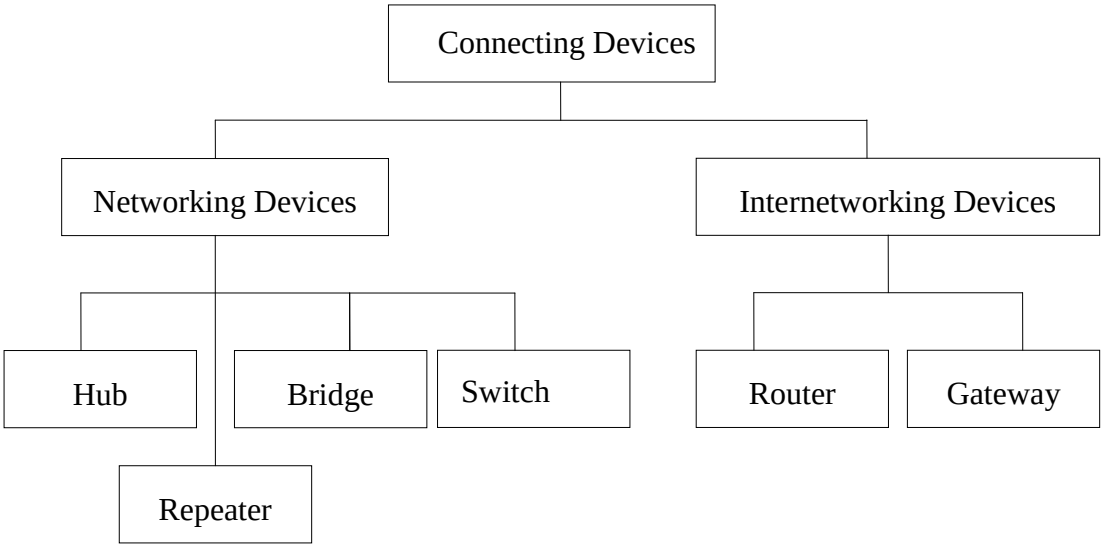
When two or more separate networks are connected for exchanging data or resources, they become an internetwork (or internet). The devices required to link number of LANs into an Internet are known as internetworking devices.

There is several ways that you can expand network capability such as:

- Physically expending to support additional computers
- Segmenting to filter network traffic
- Extending to connect separate LANs
- Connecting two separate computing environments

There are many devices available to accomplish these tasks. Following diagram will help to understand different types of connective devices.

**Figure 4.1 Networking & Internetworking Devices**




## 1.2 Networking Devices

Expansion within a single network, called *network connectivity.* And to expand a single network the following networking devices can be used.

- Hub
- Switch
- Repeaters
- Bridges

**Hub**

A **hub** is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater.

A hub is a fairly unsophisticated broadcast device. Hubs do not manage any of the traffic that comes through them, and any packet entering any port is regenerated and broadcast out on all other ports. Since every packet is being sent out through all other ports, packet collisions result—which greatly impedes the smooth flow of traffic.

**Switch**

In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. In the traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties. On an Ethernet local area network (LAN), a switch determines from the physical device (Media Access Control or MAC) address in each incoming message frame which output port to forward it to and out of. In a wide area packet-switched network such as the Internet, a switch determines from the IP address in each packet which output port to use for the next part of its trip to the intended destination.

In the Open Systems Interconnection (OSI) communications model, a switch performs the Layer 2 or Data-link layer function. That is, it simply looks at each packet or data unit and determines from a physical address (the "MAC address") which device a data unit is intended for and switches it out toward that device.

**Repeater**

Because of the electrical and mechanical limitations of any wiring system a network has physical limitations. Such as :

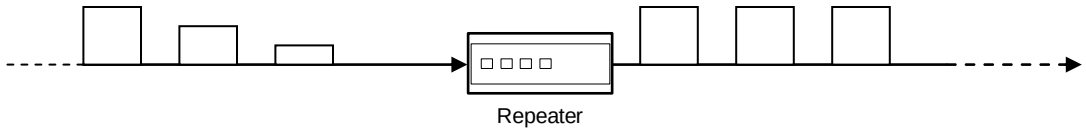
**Attenuation**: Loss of signal strength as the signal travels along a medium.

**Segment length:** longest successful data transmission through a continuous single cable.

Node capacity per segment: number of nodes can be connected on a media

Signal that carry information within a network can travel a fixed distance before attenuation or other interference from noise endangers the integrity of the data. A repeater installed on a link receive the signal before it becomes too week or corrupted, regenerates the original bit pattern, and puts the refreshed signals back onto the link. A repeater allows is to extend only physical length of the network.

Repeaters operate at the physical layers of the OSI model and have no concern for the type of data being transmitted, the packet address, or the protocol being used. They are unintelligent electronic device unable to perform any filtering or translation on the actual data.




Incoming weak signals Regenerated signals

Repeaters retransmit the data at the same speed as the network. However there is a slight delay as the repeater regenerate the signal. If there are a number of repeaters in a row, a significant propagation delay can be crated. Therefore, many network architectures limits the number of repeaters on the network.

The location of a repeater on a link is vital. A repeater must be placed so that a signal reaches it before any noise changes the meaning of any of its bits. A little noise can alter the precision of a bit's voltage without destroying its identity. If the corrupted bit travels much farther, however, accumulated noise can change its meaning completely. At that point the original voltage become unrecoverable and the error can be corrected only by retransmission.

**Strengths and Limitations of Repeaters**

- Strength:
  - Allows easy expansion of the network over large distance.
  - Has very little impact on the speed of the network.
  - Allows connection between different media.
- Limitations:
  - Provide no addressing information.
  - Can not connect two different architectures.
  - Does not help ease congestion problem.
  - The number of repeaters in a network is limited.

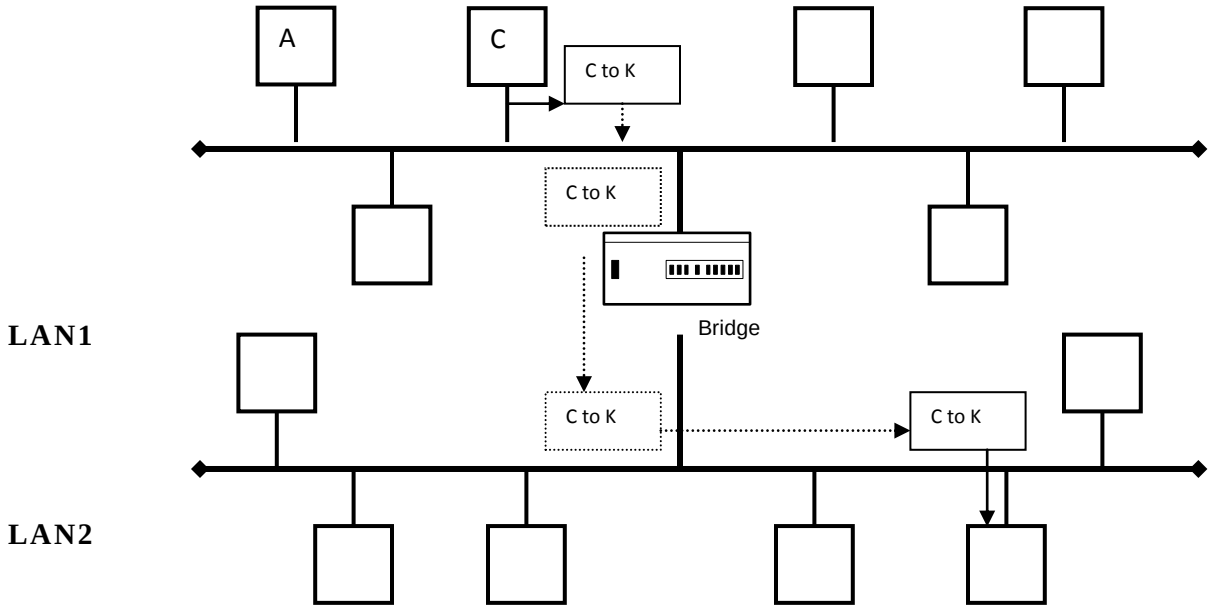
**Bridge**

Bridges operate in both the physical and data link layer of OSI model. Like repeaters, bridges also can be used to connect two network segments and can connect dissimilar physical media. However, bridges can also limit the traffic on each segment and eliminate bottlenecks.

**How Does Bridge Works?**

A bridge's primary function is to filter traffic between network segments. As a packet is received from a network segment, the bridge looks at the physical destination address of the packet before forwarding the packet on to other segments. If the packet's destination is on another network segment, the bridge retransmits the packet. However, if the destination is on the same network segment, on which the packet was received, the bridge assumes the packet has already reached its destination and the packet is discarded. As a result, network traffic is greatly reduced.

Bridges work at the data link layer of the OSI model. At this layer the hardware address, both source and destination, is added to the packet. Because bridges function at this layer, they have access to this address information. Each computer in the network is given a unique address. Bridges analyze these address to determine whether or not to forward a packet.



In above figure, the packet generated by computer C is intended for computer K. The bridge allows the packet to cross and relay it to the entire lower segment where it is received by computer K. IF a packet is destined on a same segment (for example from computer A to computer F) the bridge will block the packet from crossing into lower segment to reduce the traffic.

**Strengths and Limitations of Bridges**

- Strength:
  - Easy to extend network distances
  - Can filter traffic to ease congestion
  - Can connect network with different media
  - Translation bridges can connect different network architectures
- Limitation:
  - Slower than repeaters
  - More expensive than repeaters
  - Cannot handle multiple paths

## 1.3 Internetworking Devices

Expansion that involves and joins two separate networks called *internetworking connectivity*. Following devices can be used for internetworking.

- Routers
- Brouters
- Gateways
- Switches

**Router**

Routers are combination of hardware and software and used to connect separate networks to form an internetwork. Router can be used like bridges to connect multiple network segments and filter traffic. Also, unlike bridges, routers can be used to connect two or more *independent* networks.

Routers can connect complex networks with multiple paths between network segments. Each network segment, also called a subnetwork, is assigned a network address. Each node on a subset is assigned an address as well. Using a combination of the network and node address, the router can route a packet from the source to a destination address somewhere else on the network.

Router has access to first three layers(physical, data link, and network) but works in the network layer. To successfully route a packet through the internetwork, a router must determine packet's path. When the router receives a packet, it analyzes the packet's destination network address and look up that address in its *routing table.* The router than repackages the data ad sends it to the next router in the path.

Because operate at the higher layers of the OSI model than bridges do, routers can easily send information over different network architectures. For example, a packet received from a token ring network can be sent over an Ethernet network. The router removes the token ring frame, examines the packet to determine the network address, repackages the data into Ethernet frames, and sends the data out onto the Ethernet networks.

With this kind of translation, however, network speed is affected. As an example, Ethernet frames have a maximum data frame size of approximately 1,500 bytes, whereas token ring frames range in size from 4,000 to 18,000 bytes. So, for a single token ring frame of maximum size (18,000 bytes), 12 Ethernet frames must be created. Although routers are very fast, this type of translation does affect the network's speed.

Unlike bridges routers have ability to select the best path that is faster and economical. When a router receives a packet whose destination address is unknown, it simply discards the packet but if the same packet received by a bridge the bridge will forward it to all connected network segments

**Routing Table**

Routing has a routing table that contains network addresses and the address of the routers that handle those networks. Following table shows a sample routing table for router A. it includes the next hop (i.e., where transmission will go next) and cost (i.e., number of hops the packet must take).

1. **Static Routing**

   If router uses static routing, the routing table must be updated manually by the administrator. Each individual route must be added manually. The router will always use the same path to a destination, even if it is not necessarily the shortest or most efficient route.

2. **Dynamic Routing**

   Dynamic routers communicate with each other and are constantly receiving and are constantly receiving updated routing tables from other routers. If multiple routes are available to a particular network, the router will decide which route is best and enter that route into its routing table.

**Strengths and Limitations of Routers**

- Strength:
  - Can connect networks of different physical media and network architectures
  - Can choose the best path for a packet through an internetwork
  - reduces network traffic by not forwarding corrupt packets
- Limitation:
  - More expensive a more complex than bridges or repeaters.
  - Slower than bridge because they perform more complex calculations on the packet
  - Only work with routable protocols (TCP/IP, IPX/SPX, DECnet, OSI, XNS).

**Brouters**

Brouters combines the best of both bridges and routers. When brouters receive packets that are routable, they will operate as a router by choosing the best path for the packet and forwarding it to its destination. However, when a nonroutable packet is received, the brouter functions as a bridge, forwarding the packet based on hardware address. To do this brouters maintain both bridging table, which contains hardware address, and a routing table, which contains network address.

**Gateway**

Gateways operate in all seven layers of OSI model. A gateway is a protocol converter. A router itself transfers, accepts, and relays packets only across network using similar protocols. A gateway on the other hand, can accept a packet formatted for one protocol (e.g. AppleTalk) and convert it to a packet formatted for another protocol (e.g. TCP/IP) before forwarding it.


A gateway is generally software installed within a router. The gateway understands the protocol used by each network linked into the router and is therefore able to translate from one to another.

**Strengths and limitations of Gateway**

- Strength:
  - Can connect completely different systems.
  - Dedicated to one task and perform that task well.
- Limitation:
  - More expensive than other devices.
  - More difficult to install and configure.
  - Greater processing requirements men they are slower than other devices.

**Chapter Review Questions**

1. You have been asked to construct a Local area network for Mount Kenya University. What networking devices would you use to construct the network?
2. Why is the hub becoming obsolete in modern networks?
3. Why is a router very common in the current world's networks?

**Books for further reading**


i. William Stallings (2010), **Data and Computer Communication,** 9th edition
ii. Behrouz A. Forouzan, (2006), **Data communication and networking**, 5th edition.
iii. Andrews. Tanenbaum, (2010) **Computer Networks**, 5th edition . Prentice-Hall PTR

# CHAPTER SIX

# SWITCHING TECHNIQUES

**Learning Objectives**

**By the end of this chapter the learner shall be able to;**

i. Explain Circuit switching as applied in networking
ii. Explain packet switching as applied in networking
iii. Explain message switching as applied in networking

## 6.1 Introduction to Switching

The main objective of networking is to connect all the devices so that resources and information can be shared efficiently. Whenever we have multiple devices, we have problem of connecting them to make one-to-one connection possible. One solution is to install a point to point link between each pair of devices such as in mesh topology or between a central device and every other device as in star topology. These methods, however, are impractical and wasteful when applied to very large network. The number and length of the links require too many infrastructures to be cost efficient; and majority of those links would be idle most of the time.

A better solution is to uses switching. A switch network consists of a series of inter-linked nodes, called switches. Switched are hardware and/or software capable of creating temporary connection between two or more devices linked to switch but not to each other.

Traditionally, three methods of switching have been important:

- Circuit switching
- Packet switching and
- Message switching

## 6.2 Circuit Switching

Communication via circuit switching implies that there is a dedicated communication path between two stations. The path is a connected sequence of links between network nodes. On each physical link, a channel is dedicated to the connection. A common example of circuit switching is the telephone network..

Communication via circuit switching involves three phases:

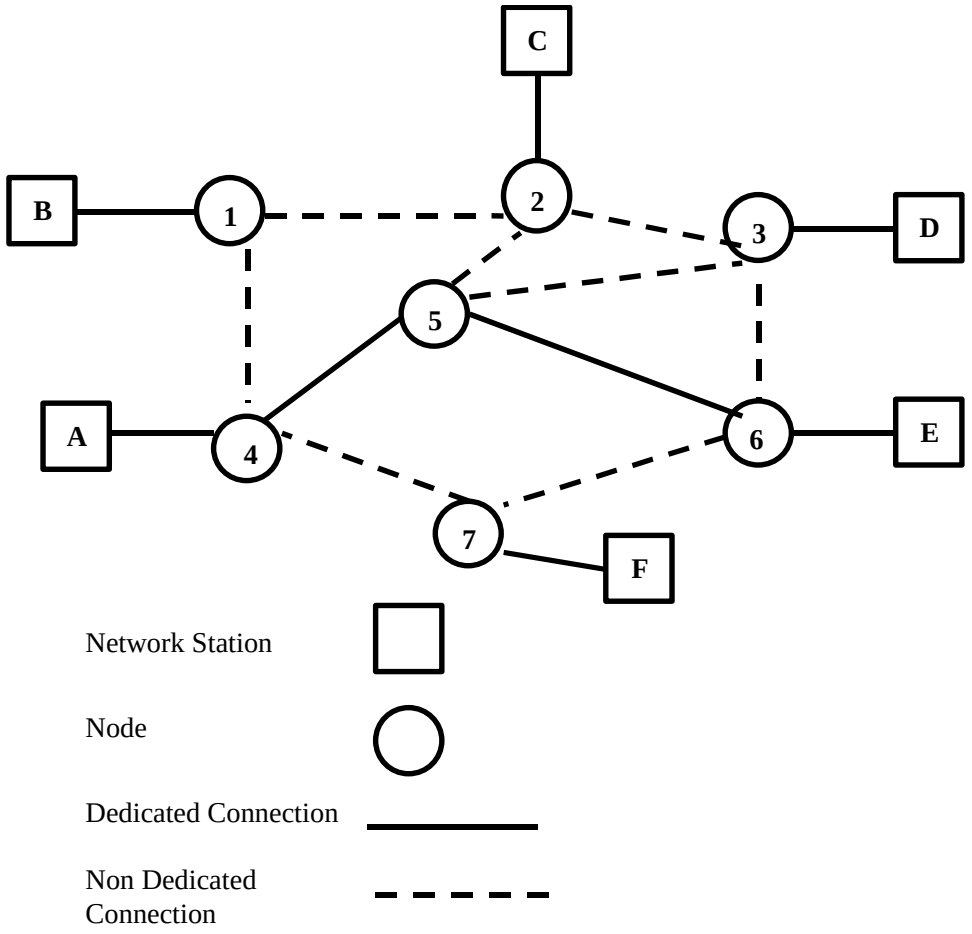



**Figure 6.1 Circuit Switching Network**

1. **Circuit Establishment**

Before any signals can be transmitted, an end-to-end (station to station) circuit must be established. For example, station A wants to communicate with station E. station A sends a request to node 4 requesting a connection to station E. typically, the link from A to 4 is a dedicated line, so that part of connection already exists. On the basis of routing information and measures availability and perhaps cost, lets assume that node 4,5, and 6 are used to complete the connection. In completing the connection, a test is made to determine if station E is busy or is prepared to accept the connection.

**2. Information Transfer**

Information now can transmit from A through the network to E the transmission may be analog voice, or binary data. Generally the connection is full duplex, and signals may be transmitted in both direction simultaneously.

**3. Circuit Disconnection**

One the transmission is completed, the connection is terminated, usually by the action of one of the two station. Signals must be propagated to the nodes 4,5, and 6 to deallocate the dedicated resources.

Circuit switching can be rather inefficient. Channel capacity is dedicated for the duration of a connection, even if no data are being transferred. The connection provides for transmission at a constant data rate. Thus, each of the devices that are connected must transmit and receive at the same data rate as the other.

## 6.3 Packet Switching

In a packet switching data are transmitted in short packets. A typical packet length is 1000 byte. If a source has longer message to send, the message is broken up into a series of packets. Each packet contains a portion (or the entire short message) of the user's data plus some control information. These packets are routed to the destination via different available nodes.

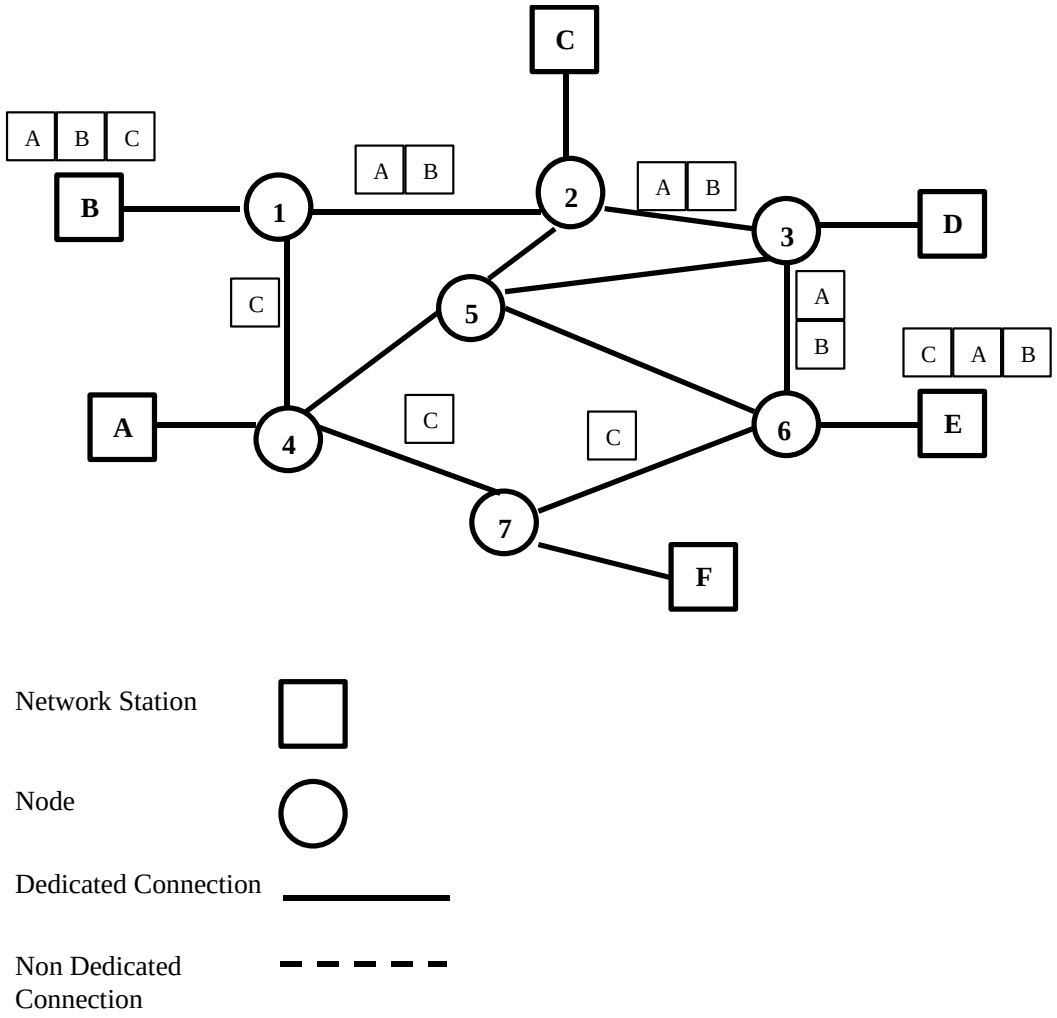


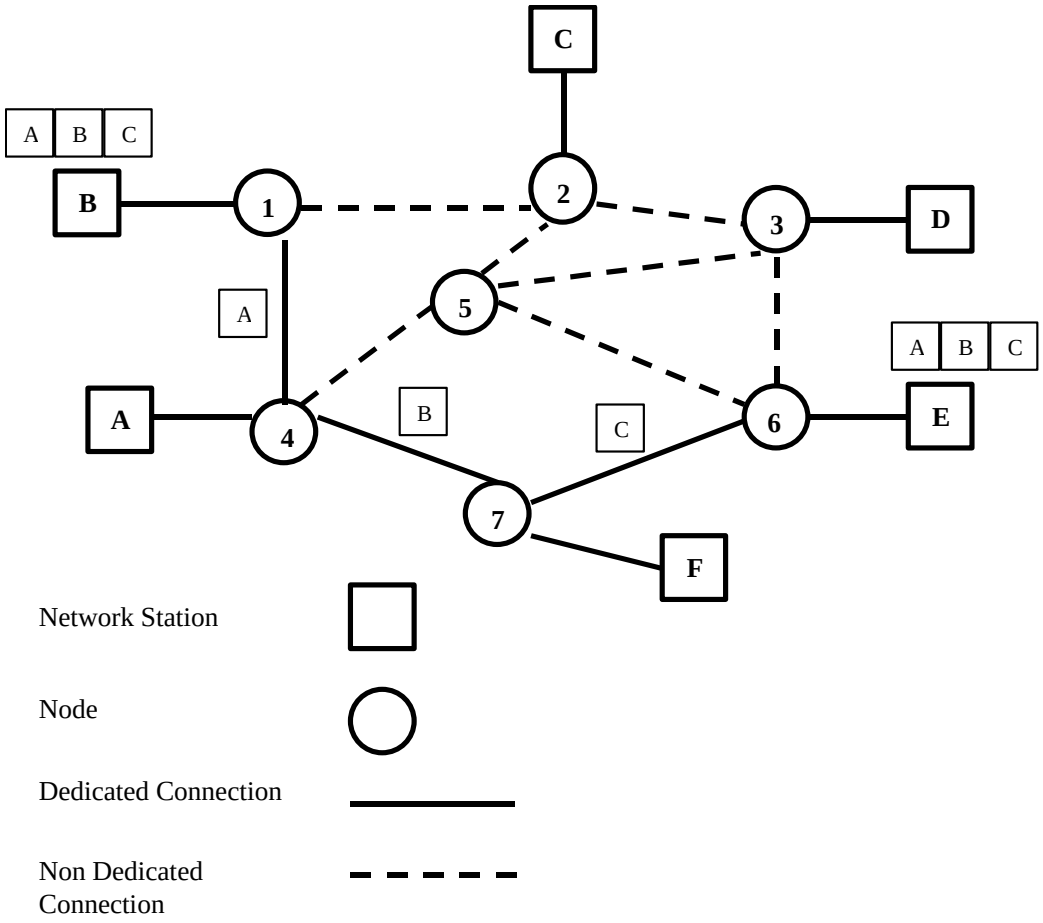

**Figure 6.2 Packet Switching Networks**

Above figure illustrate the basic operation. A transmitting computer or other device sends a message as a sequence of packets. Each packet includes control information including the destination station. The packets are initially sent to the node to which the sending station attaches. As each packet arrives at these nodes, the node stores the packet briefly, and determines the next available link. When the link is available, the packet is transmitted to the next node. The entire packet eventually delivered to the intended node.

There are two popular approaches to packet switching: datagram and virtual circuit.

**a) Datagram Approach**

In the datagram approach to packet switching, each packet is treated independently from all others and each packet can be sent via any available path, with no reference to packet that have gone before. In the datagram approach packets, with the same destination address, do not all follow the same route, and they may arrive out of




sequence at the exit point.

**Figure 6.3 Virtual Switching Network**

**b) Virtual Circuit**

In this approach, a preplanned route is established before any packets are sent. Once the route is established, all the packets between a pair of communicating parties follow this same route through the network. Each packet now contains a virtual circuit identifier as well as the data. Each node on the pre-established route knows where to direct such packet. No routing decisions are required. At any time, each station can have more than one virtual circuit to any other station and can have virtual circuits to more than one station.

## 6.4 Message Switching

The descriptive term store and forward best know message switching. In this mechanism, a anode (usually a special computer with number of disks) receives a message, stores it until the appropriate route is free, then send it along. Note that in message switching the messages are stored and relayed from the secondary storage (disk), while in packet switching the packets are stored and forward from primary storage (RAM).

The primary uses of message switching have been to provide high-level network service (e.g. delayed delivery, broadcast) for unintelligent devices. Since such devices have been replaced, message switching has virtually disappeared. Also delays inherent in the process, as well as the requirement for large capacity storage media at each node, make it unpopular for direct communication.

**Chapter Review Questions**

1. Explain the stages involved in establish a circuit connection.
2. Explain the reasons why packet switching is commonly used in data networks..
3. What are the application areas of message switching?

**Books for further reading**


i. William Stallings (2010), **Data and Computer Communication,** 9th edition
ii. Behrouz A. Forouzan, (2006), **Data communication and networking**, 5th edition.
iii. Andrews. Tanenbaum, (2010) **Computer Networks**, 5th edition . Prentice-Hall PTR

## CHAPTER SEVEN

## MULTIPLEXING

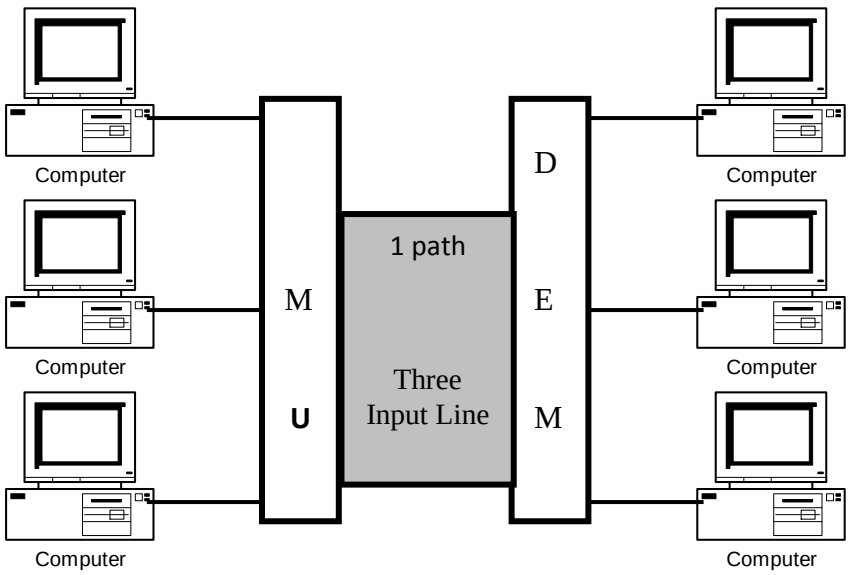
**Learning Objectives**

By the end of this chapter the learner shall be able to;

i. Explain the concept of multiplexing
ii. Explain the concept of Time division multiplexing
iii. Explain the concept of Frequency division multiplexing

### 7.1 Introduction to multiplexing

Multiplexing is the process of combining separate signal channels into one composite stream. It is carried out to increase the utilization of transmission channel. In a multiplexed system, n devices share the capacity of one link. In the following figure, four devices on the left direct their transmission stream to a multiplexer (MUX) which combines them into a single stream (many to one). At the receiving end, the stream is fed into a demultiplexer (DEMX), which separates the stream back into its component




transmissions (one to many) and directs them to their receiving devices.

## 7.2 Frequency Division Multiplexing

FDM is an analogue technique that works by dividing slicing the total bandwidth of a media into a number of narrow bandwidth units known as channels.

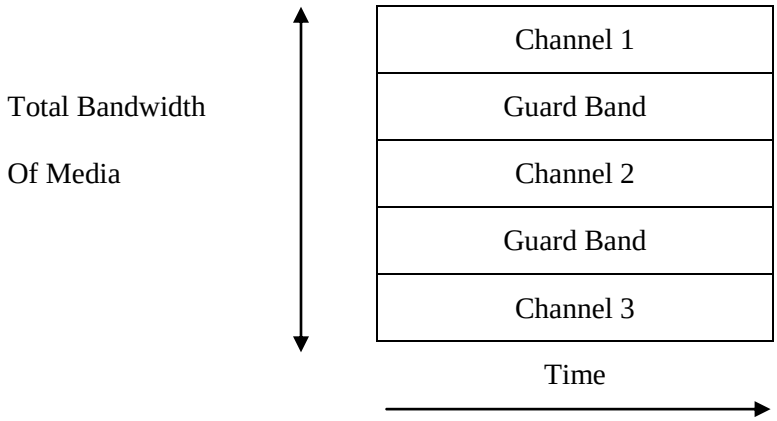
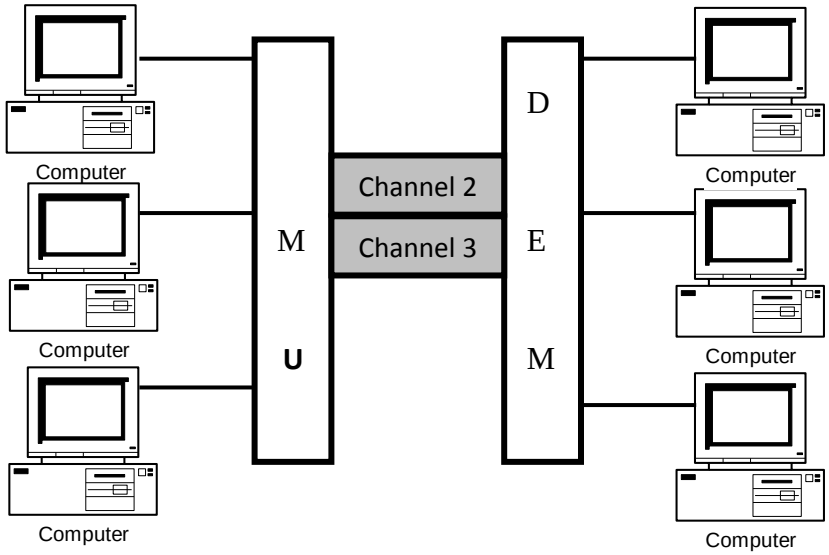



**Figure 6.9 Frequency Division of Media Bandwidth**

These channels are separated by further narrower slices, known as guard bands, to prevent inter-channel interface. This actual waste of bandwidth is offset by the lower costs of the filter (frequency selection device). The closer the channels are together (the narrower the guard bands (the more critical and expensive the channel filter become.

Bellow figure gives a conceptual view of FDM. In this illustration, the transmission path is divided into three parts (based on different frequencies), each representing a channel to carry one



transmission.

**Figure 6.10 Frequency Division Multiplexing**

As an analogy, imagine a point where three separate narrow roads merge to form a three-lane highway. Each of the three roads corresponds to a lane of the highway. Each car merging into the highway from one of the road still has its own lane and can travel without interfering with cars in other lane.

**Example: Cable Television**

A familiar application of FDM is cable television. The coaxial cable used in a cable television system has a bandwidth of approximately 500 MHz. An individual television channel requires about 6 MHz of bandwidth for transmission. The coaxial cable, therefore, can carry many multiplexed channels (theoretically 83 channels, but actually fewer to allow for guard band). A demultiplexer at your television allows you to select which of those channels you wish to receive.

## 7.3 Time Division Multiplexing

### Synchronous TDM

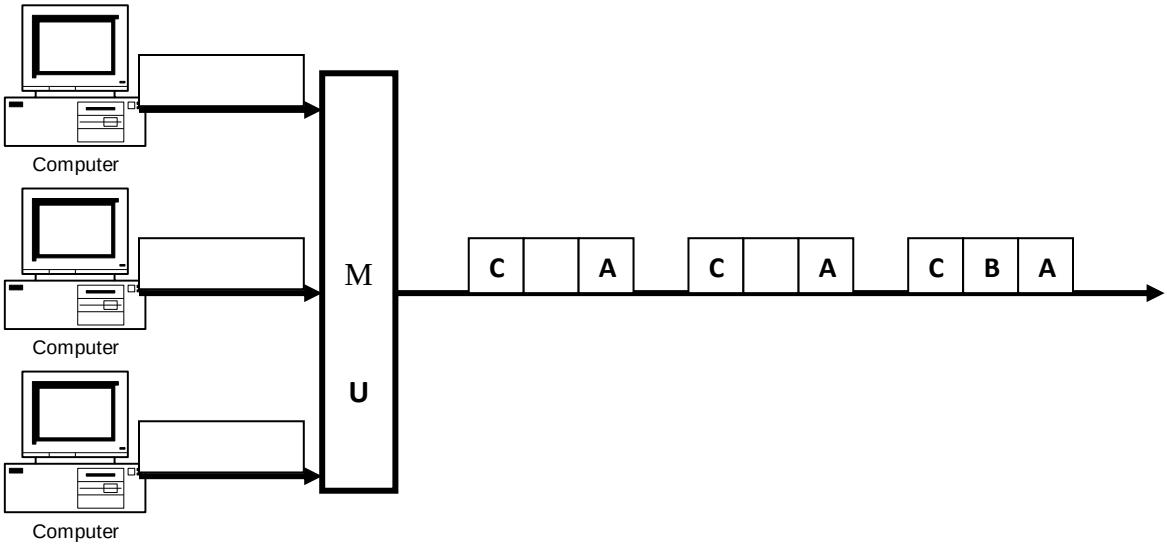



**Figure 6.12 Synchronous TDM**

In this method, multiplexer allocates the same time slot to each device at all time, whether or not a device has anything to transmit. IF there are *n* input line than there must be *n* time slots in the frame (time slots are grouped into frames). Time slot (lets say T), for example, is assigned to device (lets say D) alone and can not be used by any other device. Each time its allocated time slot comes in (in a round robin fashion), Device D has the opportunity to send a portion of its data for time slot T. If the device D is unable to transmit or does not have data to send, its time slot remains empty and no other device can use it, another words it is wasted.

### Asynchronous TDM(Statistical TDM)

Asynchronous TDM provide better utilization of media. Like synchronous TDM, asynchronous TDM allows a number of lower speed input lines to be multiplexed to a single higher speed line. Unlike synchronous TDM, however, in asynchronous TDM the total speed of input line can be greater than the capacity of the media. In asynchronous TDM the number of slots in the frame are less than numbers of input lines. Slots are not preassigned, each slot is available to any of the attached input lines that has data to send. The multiplexer scans the input line, accepts the portion of data until a frame is filed, and then sends the frame across the link.

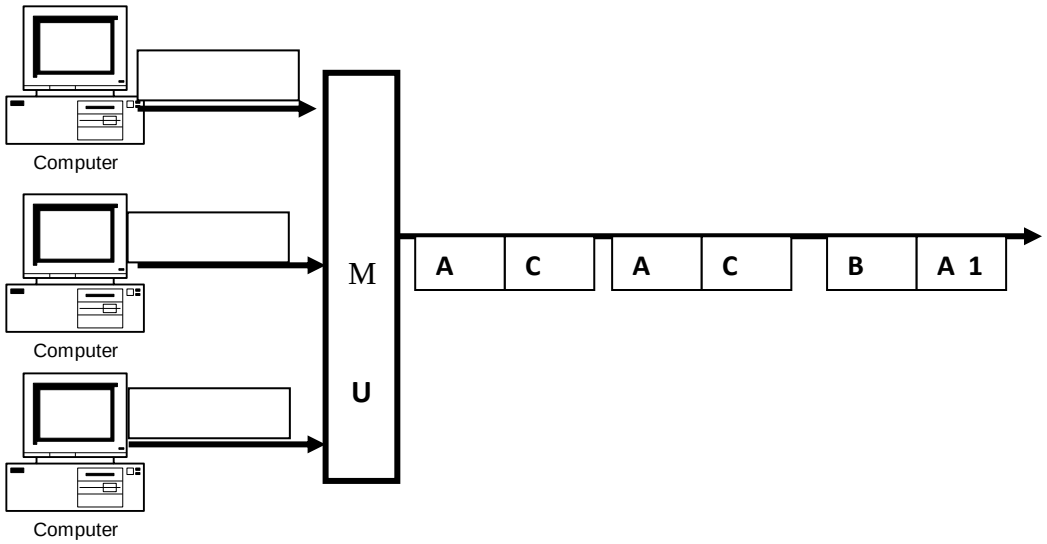



**Figure 6.13 Asynchronous TDM**

Since the slots are not pre-assigned for each input line, line address must be added along with the data to send.

**Chapter Review Questions**

1. Explain the term multiplexing.
2. Explain the concept of time division multiplexing.
3. Which is the most appropriate multiplexing method for today's networks? Give reasons for your answer.

**Books for further reading**


i. William Stallings (2010), **Data and Computer Communication,** 9th edition
ii. Behrouz A. Forouzan, (2006), **Data communication and networking**, 5th edition.
iii. Andrews. Tanenbaum, (2010) **Computer Networks**, 5th edition . Prentice-Hall PTR

**SAMPLE EXAM QUESTIONS**

# Mt Kenya University

**UNIVERSITY EXAMINATIONS 2010/2011**

**SCHOOL OF APPLIED SOCIAL SCIENCES**

**DEPARTMENT OF I.T**

**END OF SEMESTER EXAMINATION FOR THE BACHELOR OF BUSINESS INFORMATION TECHNOLOGY DEGREE**

**BIT 2204 DATA COMMUNICATION AND NETWORKS**

**DATE: April 2011 Time: 2 HRS**

**QUESTION 1**

Mount Kenya University requires a Network that will cater for their administrative and students needs. The users range from lecturers, administrative assistants and students. All types of users need to access the internet through the network. The university management also requires the network to support WIFI access. The university members of staff need to access the university management information system, which should not be accessed by the students. The total number of expected users is 500 at any given time.

(a) Which is the most appropriate network topology for this network. Give the reasons for your answer (2 marks)
(b) What network devices will be used while designing the network? Briefly explain their use (8 Marks)
(c) What transmission impairments is the network likely to experience? (8 marks)
(d) What transmission medium will be used to connect the network? Give reasons for your answer (2 marks)
(e) Briefly explain how the user computers will be configured to access the network (4 marks)
(f) How will this network be secured from intruders and students who might attempt to access confidential information such as examinations? (4 marks)
(g) What switching technique might be appropriate for the network. Give reasons for your answer (2 marks)

**QUESTION 2**

There are several different network topologies:
**(a)** Bus
**(b)** Ring
**(c)**Mesh

**(d)** Modern Star
From the above **four** of the above topologies:
(i) Draw a clearly labelled diagram;
(ii) Briefly describe its layout;
(iii) Discuss its advantages and disadvantages. **(5 marks each)**
**(Total 20 marks)**

**QUESTION 3**
The Open Systems Interconnection (OSI) 7 layer model, sometimes called the International Standards Organisation (ISO) 7 layer model, is a critical model for modern computer networking.
**(a)** In the correct sequence from either end, identify the **seven** layers of the ISO/OSI 7 layer model. **(4 marks)**

(b) Briefly explain the function of each layer. (2 marks each - 14 marks)

(c) What are the advantages of the OSI model? (2 marks)

**Question 4**

**(a)** With the aid of diagrams, describe the main features of modulation and demodulationwhen used for transmitting data across the Public Switched Telephone Network (PSTN).
**(8 marks)**

**(b)** With the aid of diagrams, explain what is meant by each of the terms: amplitude modulation, frequency modulation and phase modulation. **(12 marks)**

**(Total 20 marks)**

**Question 5**

**(a)** Local Area Networks (LANs) require an 'access method' which determines how computers share a common transmission medium. Write down the **two** main approaches for controlling this sharing in wired networks. Briefly explain how each approach operates.
**(8 marks)**

**(b)** Compare **four** transmission media used in LANs and WANs in terms of maximum data rates and other limitations. **(12 marks)**

# Mt Kenya University

**UNIVERSITY EXAMINATION 2010**

**SCHOOL OF APPLIED SOCIAL SCIENCES**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**BACHELOR OF BUSINESS INFORMATION TECHNOLOGY**

**END OF SEMESTER EXAMINATION**

**COURSE CODE: BBIT 2204**

**COURSE TITLE: INTRODUCTION TO DATA COMMUNICATION AND COMPUTER NETWORKS.**

TIME: 2HRS

**Instructions:** Question ONE is **COMPULSORY** and any other TWO from section B.

SECTION A.

**QUESTION ONE.**

(a) You have the task of designing a network for a medium-sized company.

Identify the ways in which the following factors might influence the design decisions you make:

i) The geographical area to be covered by the network.

ii) The number of users.

iii) The types of application used within the company.

iv) The type of business of the company.

v) The extent to which E-Commerce is used between the company and its (external) trading partners.

vi) The size of the budget available.

vii) The expected growth rate of the company. (14 marks)

(b) Compare and contrast Half and Full Duplex communication (4 marks)

(c) Discuss the main differences between Synchronous and Asynchronous Transmission, emphasising signal timing issues. (4 marks)

(d) Describe the main elements of the Local Area Network model. (6 marks)

(e) Briefly explain the Open Systems Interconnection (OSI) network reference model by emphasising the importance of layers for functional communication requirements.
(2 marks)

**Question 2**

Describe the seven layers of the OSI model by focusing on the responsibilities and interface of each layer.
**(20 marks)**

**Question 3**

(a) Briefly describe circuit switching. (4 marks)

(b) Explain how a packet-switched network works. (4 marks)

(c) Briefly discuss the main differences between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). (8 marks)

(d) Which of these services in (b) is most suitable for developing a 'real time' application? Briefly explain your reasoning. (4 marks)

**Question 4.**

a) Video conferencing was expected to eliminate much of the need for

business travel but has not been as widely adopted as was hoped.

i) Give THREE limitations of video conferencing. **( 6 marks)**

ii) Video Voice Over Internet Protocol (VOIP) may be more likely to be

widely adopted.

A) What equipment other than a PC, monitor and broadband

connection is required for video VOIP? **(2 marks)**

B) Explain how you would find, download and install the software

needed to run video VOIP. **(4 marks)**

b) Many homes and small offices now have a wireless local area network

(WLAN).

i) What should the owner do to protect his WLAN from eavesdroppers? **(4 marks)**

ii) Give TWO advantages of using a WLAN rather than a cabled network. **(4 marks)**

**(Total 20 marks)**

**Question 5**

**(a)** Local Area Networks (LANs) require an 'access method' which determines how computers share a common transmission medium. Write down the **two** main approaches for controlling this sharing in wired networks. Briefly explain how each approach operates.

**(8 marks)**

**(b)** Three physical topologies associated with LANs are: the bus, ring and star topologies. Describe **each one**, highlighting their strengths and weaknesses from a reliability point of view.

**(12 marks)**

**(Total 20 marks)**