Contents

CHAPTER ONE

INTRODUCTION TO COMPUTER NETWORKS

DATA & INFORMATION

Data refers to the raw facts that are collected while information refers to processed data that enables us to take decisions.

DATA COMMUNICATION

Data Communication is a process of exchanging data or information. In case of computer networks this exchange is done between two devices over a transmission medium. This process involves a communication system which is made up of hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes. The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a Protocol

Characteristics of Data Communication

Delivery: The data should be delivered to the correct destination and correct user.

Accuracy: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.

Timeliness: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.

Jitter: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

Components of Data Communication

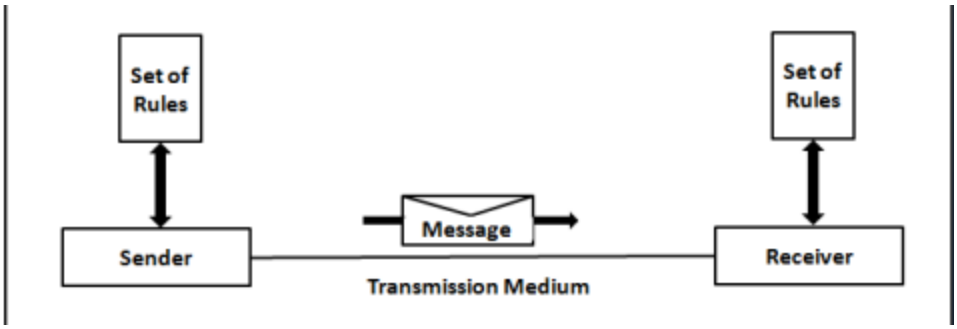
1. Message -is the information to be communicated by the sender to the receiver.

2. Sender -The sender is any device that is capable of sending the data (message).

3. Receiver- The receiver is a device that the sender wants to communicate the data (message).

4. Transmission Medium It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.

5. Protocol - It is an agreed upon set or rules used by the sender and receiver to communicate data. A protocol is a set of rules that governs data communication.



DATA REPRESENTATION

Text - includes combination of alphabets in small case as well as upper case. It is stored as a pattern of bits. Prevalent encoding system: ASCII, Unicode

Numbers include combination of digits from 0 to 9. It is stored as a pattern of bits. Prevalent encoding system : ASCII, Unicode

Images —

Audio Data can also be in the form of sound which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information. Audio data is continuous, not discrete.

Video -refers to broadcasting of data in form of picture or movie

DATA FLOW

Simplex

In Simplex, communication is unidirectional Only one of the devices sends the data and the other one only receives the data. Example: in the below diagram: a cpu send data while a monitor only receives data.

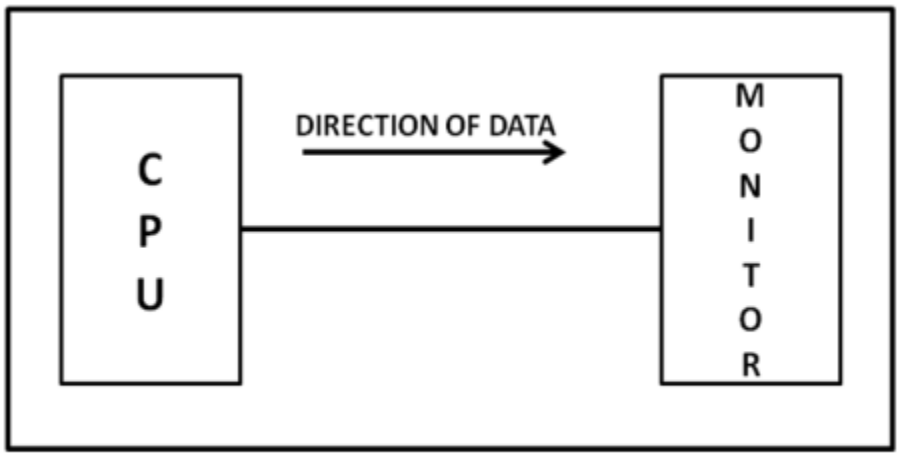


Figure: Simplex mode of communication

Half-duplex

In half duplex both the stations can transmit as well as receive but not at the same time. When one device is sending other can only receive and viceversa (as shown in figure below.)

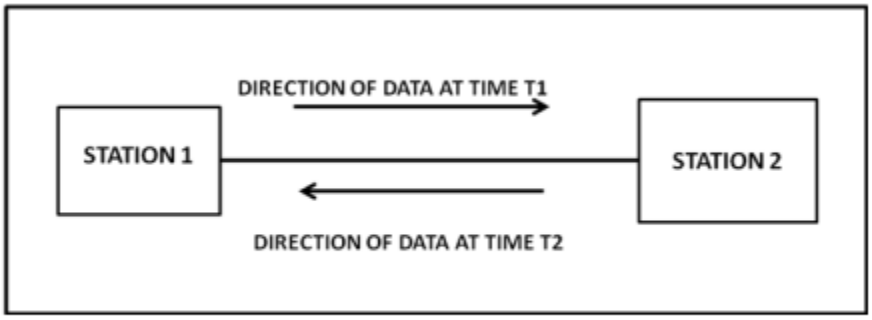


Figure: Half Duplex Mode of Communication

Full Duplex

In Full duplex mode, both stations can transmit and receive at the same time. Example: mobile phones

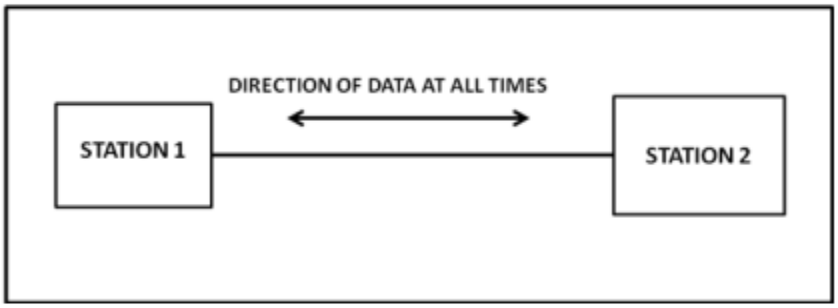


Figure: Full Duplex Mode of Communication

COMPUTER NETWORK

A computer network can be defined as a collection of nodes. A node can be any device capable of transmitting or receiving data. The communicating nodes have to be connected by communication links. A Computer network should ensure:

- **reliability** of the data communication process
- **security** of the data
- **performance** by achieving higher throughput and smaller delay times

Categories of Network

The 4 basic categories of computer networks are:

A.Local Area Networks (LAN) is usually limited to a few kilometers of area. It may be privately owned and could be a network inside an office on one of the floor of a building or a LAN could be a network consisting of the computers in a entire building.

B.Wide Area Network (WAN) is made of all the networks in a (geographically) large area. The network in the entire state of Maharashtra could be a WAN

C.Metropolitan Area Network (MAN) is of size between LAN & WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city like NAIROBI.

D. A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices.

PROTOCOL

A Protocol is defined as a set of rules that governs data communications. A protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated.

Elements of a Protocol

Syntax It means the structure or format of the data. It is the arrangement of data in a particular order.

Semantics It tells the meaning of each section of bits and indicates the interpretation of each section. It also tells what action/decision is to be taken based on the interpretation.

Timing It tells the sender about the readiness of the receiver to receive the data It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

TRANSMISSION MEDIUM

Transmission media is a means by which a communication signal is carried from one system to another. A transmission medium can be defined as anything that can carry information from a source to a destination.

Categories of transmission media

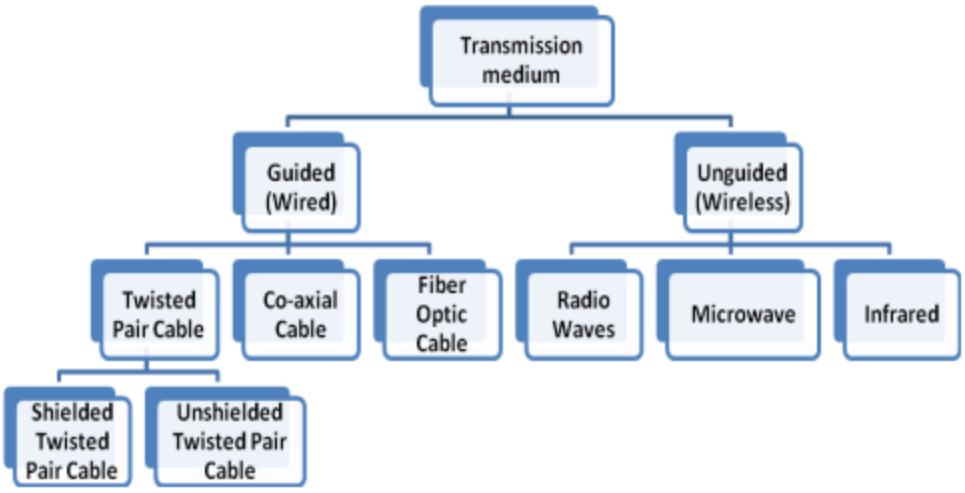


Figure : Categories of Transmission Medium

GUIDED MEDIA/BOUNDED/PYHSICAL/NON-WIRELESS

Guided Transmission media uses a cabling system that guides the data signals along a specific path. Include twisted-pair cable, coaxial cable, and fiber-optic cable.

Twisted-pair cable

Fig. Unshielded Twisted Pair Cable

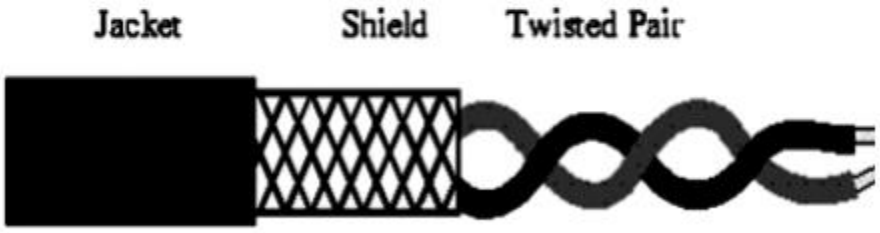


Fig. Shielded Twisted Pair Cable

Advantages

Cost-Effective: Twisted pair cables are relatively inexpensive compared to other types of cables, making them a cost-effective choice for many applications.

Flexibility: Twisted pair cables are flexible and easy to install. They can be bent and twisted without significant signal degradation, making them suitable for various environments.

Ease of Installation: Installation of twisted pair cables is straightforward, and they are commonly used in both residential and commercial settings. They are available in pre-terminated lengths or can be custom-cut.

Widespread Usage: Twisted pair cables are the most common type of cable used in local area networks (LANs) and telephone systems, making them widely available and compatible with various devices.

Easily Upgradable: Upgrading or expanding a network using twisted pair cables is relatively easy. New cables can be added without much disruption to the existing infrastructure.

Disavantages

Limited Distance: Twisted pair cables have a limited transmission distance compared to other types of cables, such as fiber optics. Signal quality may degrade over longer distances.

Vulnerability to Electromagnetic Interference: In environments with high levels of electromagnetic interference, twisted pair cables may be susceptible to signal degradation. Shielded twisted pair (STP) cables can be used in such situations.

Limited Power Transmission: Twisted pair cables are not ideal for applications that require significant power transmission. Power over Ethernet (PoE) is possible, but there are limits to the power that can be delivered.

Environmental Factors: Twisted pair cables are not well-suited for outdoor or harsh environmental conditions. Exposure to moisture, extreme temperatures, or physical stress can impact their performance.

Co-Axial Cable

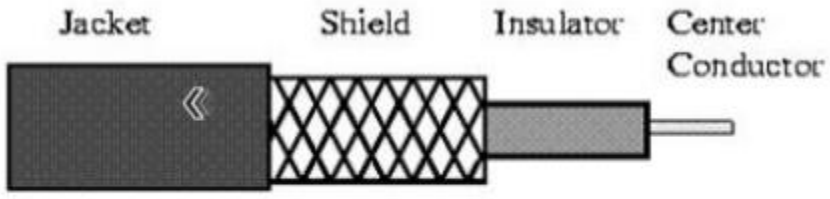


Figure: Co-axial cable

ADVANTAGES

Broad Usage: Coaxial cables are versatile and used for a variety of applications, including cable TV, internet connectivity, networking, and audio/video transmission.

High Bandwidth: Coaxial cables can support a high bandwidth, making them suitable for transmitting large amounts of data over short to medium distances.

Immunity to Interference: The design of coaxial cables, with a central conductor surrounded by insulating layers and a metallic shield, provides good protection against electromagnetic interference (EMI) and radio frequency interference (RFI).

Long Transmission Distances: Coaxial cables can transmit signals over relatively long distances without significant signal degradation. This makes them suitable for applications such as cable TV distribution.

Ease of Installation: Coaxial cables are relatively easy to install and terminate. The connectors are widely available, and the cables are flexible, allowing for easy routing**.**

Secure Transmission: The shielding of coaxial cables makes them less susceptible to signal eavesdropping or signal leakage, providing a degree of security for transmitted data.

Durability: Coaxial cables are often durable and can withstand physical stress, making them suitable for various environments, including outdoor installations**.**

Disadvantages:

Size and Bulk: Coaxial cables can be relatively bulky, especially compared to newer, smaller cables like twisted pair cables and fiber optics. This may limit their use in certain applications where space is a critical factor.

Signal Attenuation: Over very long distances, coaxial cables may experience signal attenuation, resulting in a degradation of signal strength. Repeaters may be needed to overcome this limitation.

Susceptibility to Moisture: Some coaxial cables are susceptible to moisture penetration, which can affect signal quality. Outdoor installations may require additional weatherproofing measures.

Fibre Optic Cable

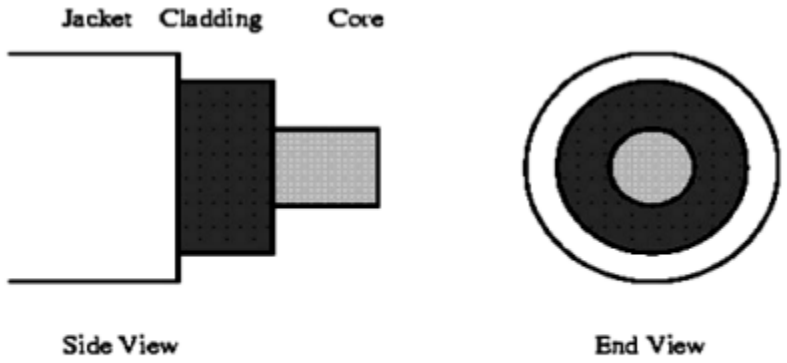


Figure Fiber Optic Cable

Optical fiber consists of thin glass fiber that can carry information at frequencies in the visible light spectrum.

Advantages:

Small size and light weight: The size of the optical fibers is very small. Therefore a large number of optical fibers can fit into a cable of small diameter.

Easy availability and low cost: The material used for the manufacturing of optical fibers is —Silica glass this material is easily available. So the optical fibers cost lower than the cables with metallic conductors.
No electrical or electromagnetic interference: Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic Interference.

Large Bandwidth: As the light rays have a very high frequency in GHz range, the bandwidth of the optical fiber is extremely large.

Other advantages: - No cross talk inside the optical fiber cable. Signal can be sent up to 100 times faster.

Disadvantages

Cost: Fiber optic cables are generally more expensive to install than traditional copper cables. The cost of the cables and the specialized equipment needed for installation can be a significant factor, especially for large-scale deployments.

Fragility: Fiber optic cables are more delicate than their copper counterparts. They can be damaged more easily during installation or if they are bent beyond their minimum bend radius. Special care is needed to avoid stress on the cables.

Termination Complexity: Terminating and splicing fiber optic cables requires specialized skills and equipment. This complexity can make the installation process more challenging and may necessitate the involvement of trained technicians.

Transmitter and Receiver Costs: The electronic components used in the transmitters and receivers for fiber optic systems can be expensive. This cost can be a factor in the overall expense of deploying fiber optic networks.

Complex Repairs: If a fiber optic cable is damaged, repairing it can be more complex and time-consuming compared to copper cables. This is especially true for cables installed underground or in hard-to-reach locations.

UNGUIDED (WIRELESS) TRANSMISSION MEDIUM

There are three types of Unguided Media

(i) Radio waves-Electromagnetic wave ranging in frequencies between 3 KHz and 1GHz are normally called radio waves.

(ii) Micro waves -Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

(iii) Infrared-Infrared signals with frequencies ranges from 300 GHz to 400 GHz can be used for short range communication.

TRANSMISSION MODES

Types of Transmission Modes: Serial and Parallel as shown in the figure below. Serial transmission is further categorized into Synchronous and Asynchronous Serial transmission.

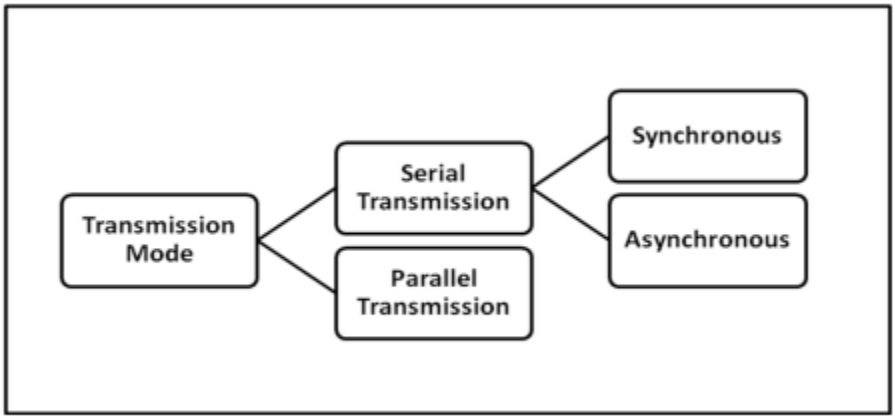


Fig. Types of Transmission Modes

Parallel Transmission

It involves simultaneous transmission of N bits over N different channels Parallel Transmission increases transmission speed by a factor of N over serial transmission Disadvantage of parallel transmission is the cost involved, N channels have to be used, hence, it can be used for short distance communication only

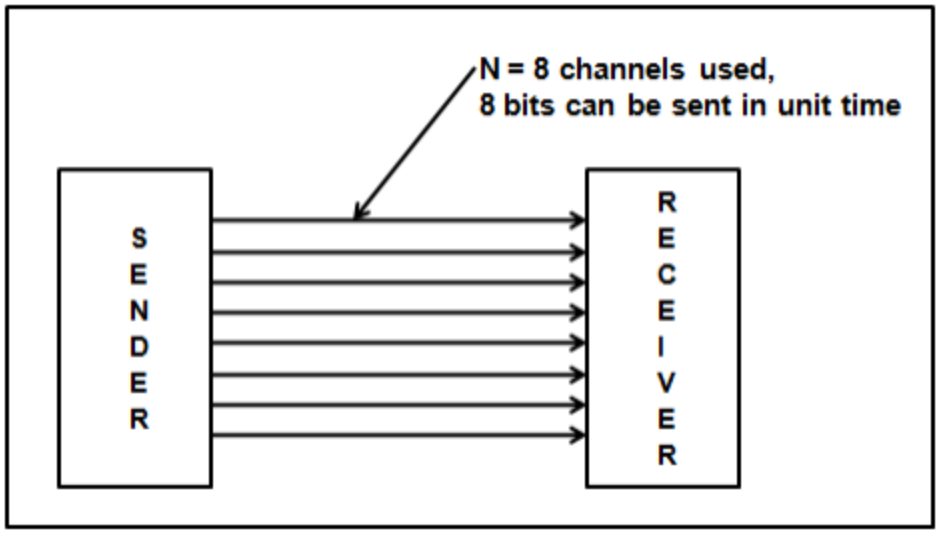


Fig. Parallel Transmission of Data over N = 8 channels

Serial Transmission

In Serial Transmission, as the name suggests data is transmitted serially, i.e., bit by bit, one bit at a time. Since only one bit has to be sent in unit time only a single channel is required.

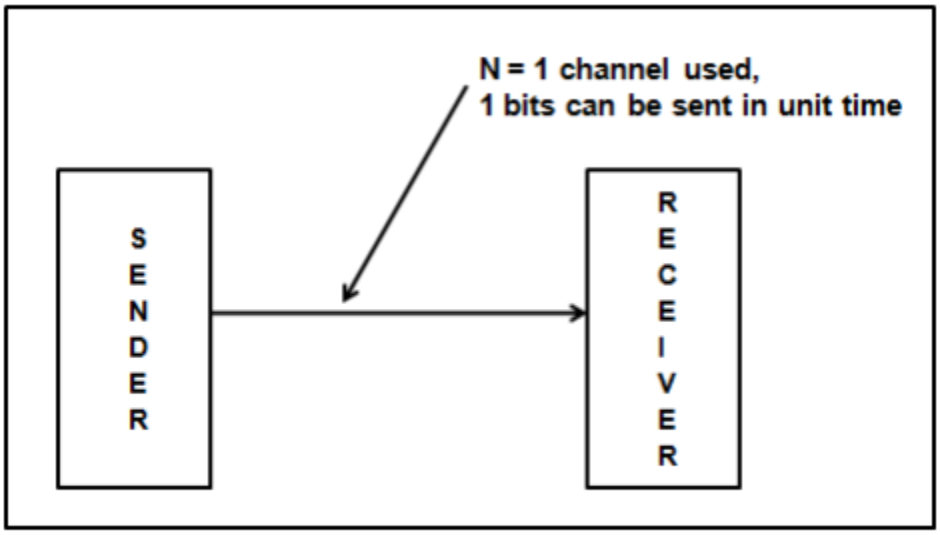


Fig. Serial Transmission of Data over N = 8 channels

Types of Serial Transmission:

1.ASynchronous Transmission

In asynchronous serial transmission the sender and receiver are not synchronized. The data is sent in group of 8 bits i.e., in bytes. The sender can start data transmission at any time instant without informing

the receiver. To avoid confusing the receiver while receiving the data, —start and —stop bits are inserted before and after every group of 8 bits as shown below.

The start bit is indicated by —0 and stop bit is indicated by —1

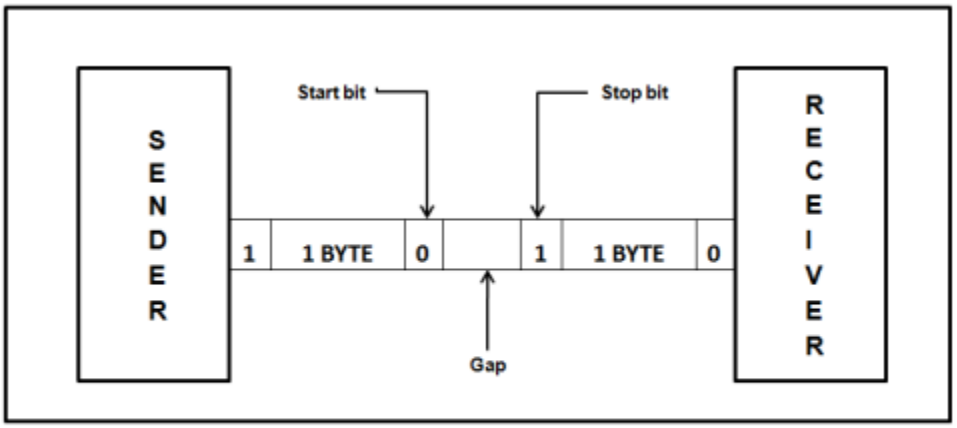


Fig: Asynchronous Serial Transmission

Advantages

- Cheap and Effective implementation
- Can be used for low-speed communication

Disadvantages

1.Insertion of start bits, stop bits and gaps make asynchronous transmission slow.

Application: Keyboard

2.Synchronous Serial Transmission,

The sender and receiver are highly synchronized. No start, stop bits are used. Instead, a common master clock is used for reference. The sender simply sends stream of data bits in group of 8 bits to the receiver without any start or stop bit

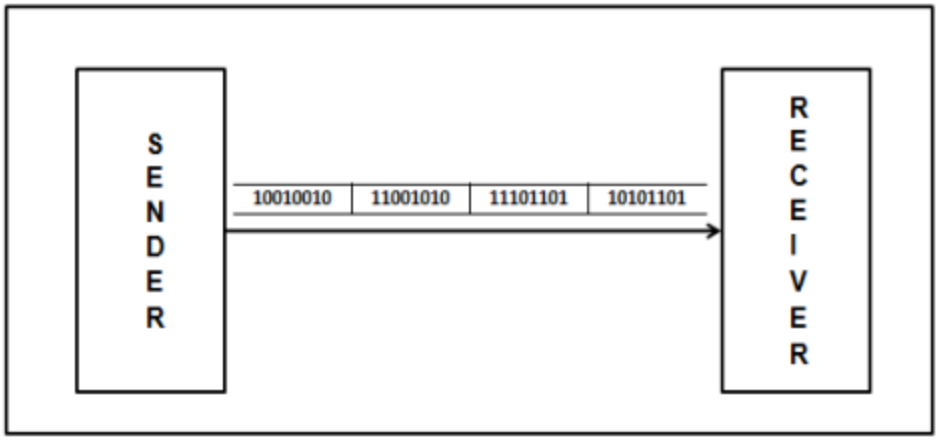


Fig: Asynchronous Serial Transmission

Advantages

- There are no start bits, stop bits or gaps between data units
- Since the above are absent data transmission is faster.
- Due to synchronization, there are no timing errors

Transmission Impairment Types

Attenuation-Attenuation results in loss of energy. When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. The electrical energy in the signal may converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

Distortion -Distortion changes the shape of the signal

Noise-Noise is any unwanted signal that is mixed or combined with the original signal during transmission. Due to noise the original signal is altered and signal received is not same as the one sent.

CHAPTER 2

INTRODUCTION TO NETWORKING

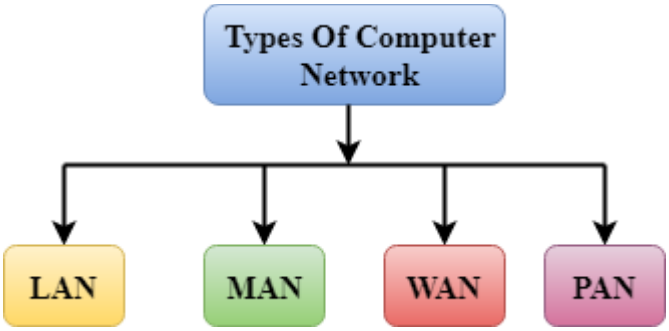
NETWORK FUNDAMENTALS

A network is simply a group of two or more Personal Computers linked together.

Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN (Local Area Network)
- PAN (Personal Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

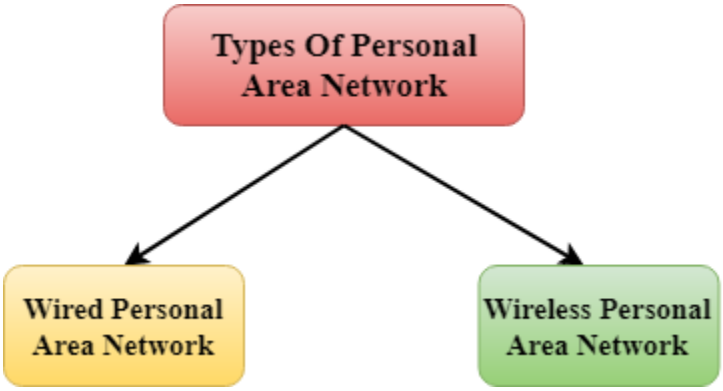
LAN (Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

PAN (Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:



- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

Examples of Personal Area Network:

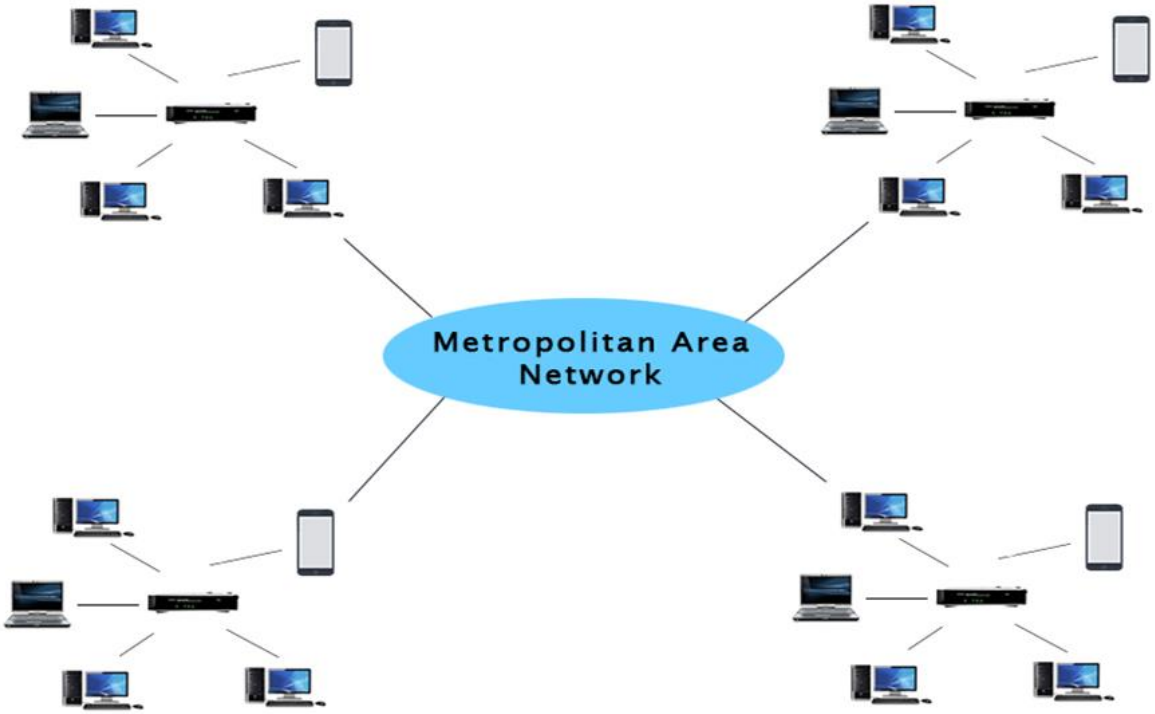
- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person

establishes a network connection and then creates a connection with another device to share the information.

- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
- **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN (Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

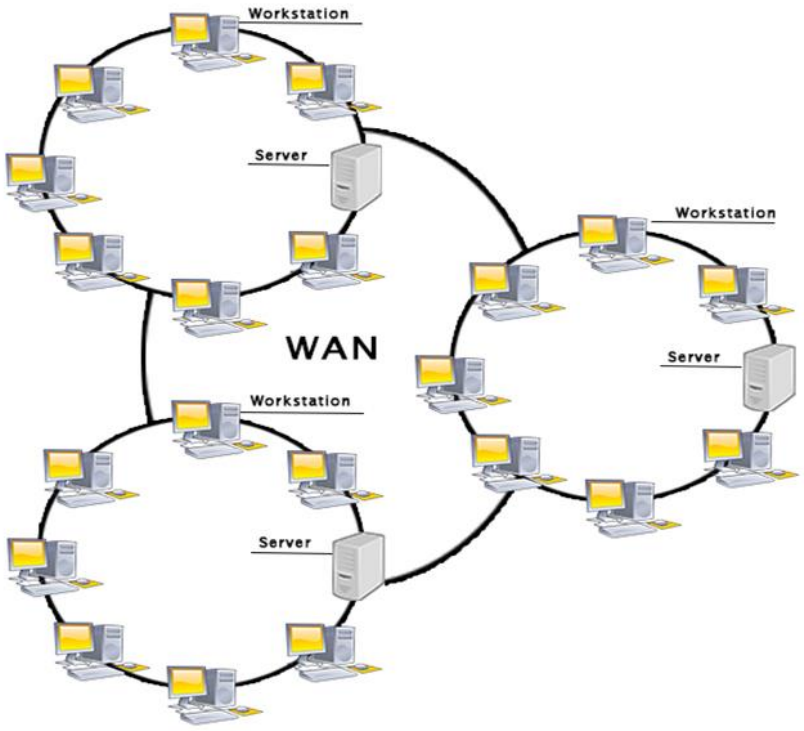


Uses of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN (Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.

- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used.

Some people can inject the virus in our system so antivirus is needed to protect from such a virus.

- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

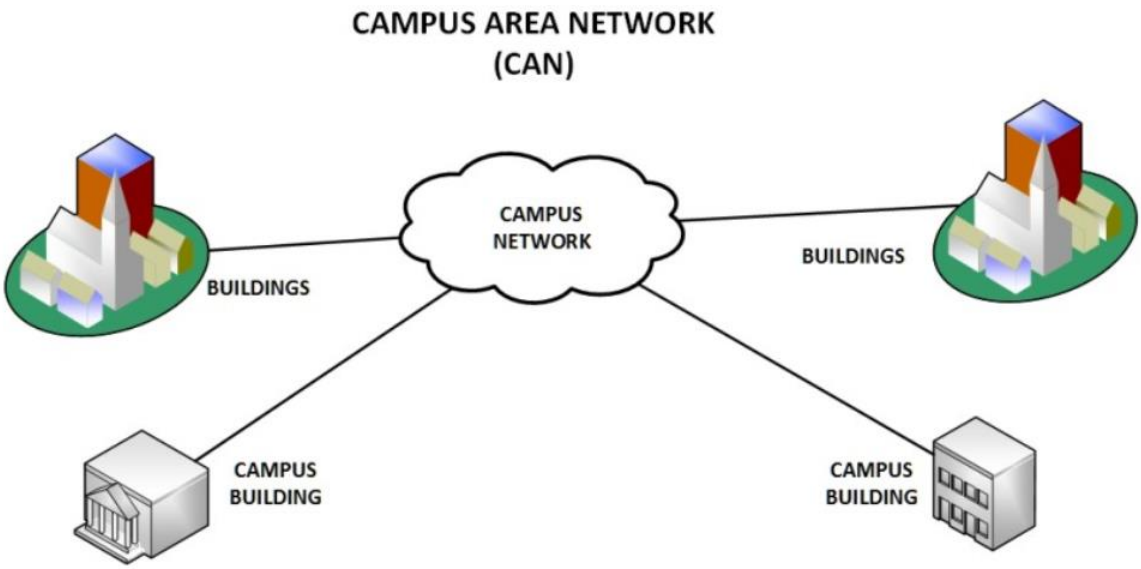
Other types of networks

Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.

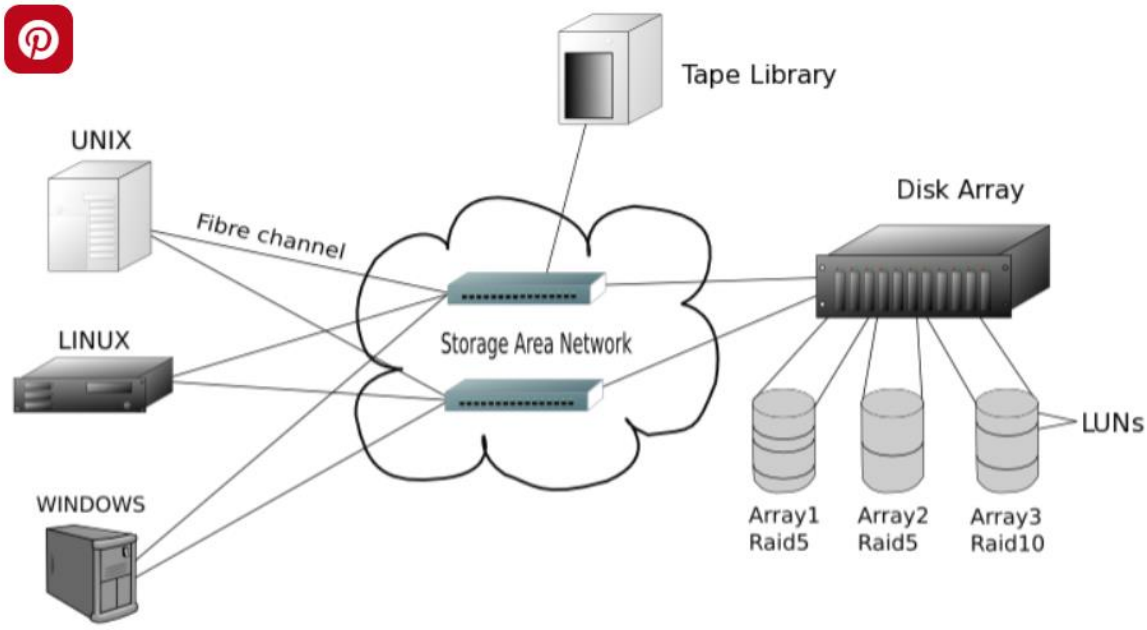
4. Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large school or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.



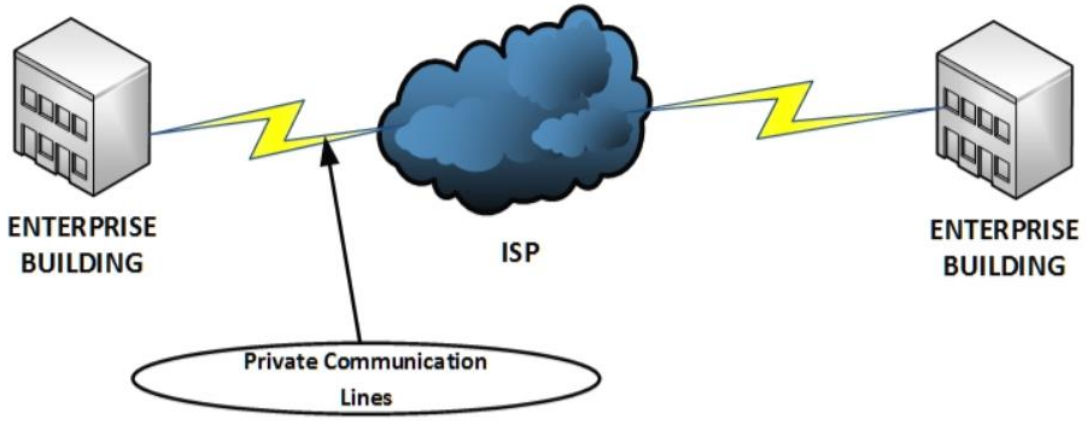
Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.



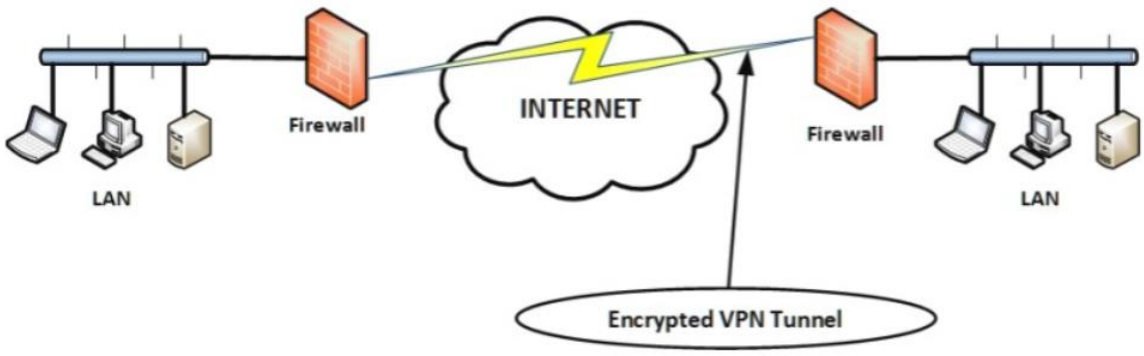
Enterprise Private Network (EPN)

These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.



Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection, users can access a private network remotely.



Internetwork

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
- An internetworking uses the **internet protocol**.
- The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.
2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
- **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
- **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
- **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.

- **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

Network Topologies

Network topology refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other. Think of your network as a city, and the topology as the road map. Just as there are many ways to arrange and maintain a city such as, making sure the avenues and boulevards can facilitate passage between the parts of town getting the most traffic. There are several ways to arrange a network. Each has advantages and disadvantages and depending on the needs of your company, certain arrangements can give you a greater degree of connectivity and security.

There are two approaches to network topology:

- Physical
- Logical.

Physical network topology, as the name suggests, refers to the physical connections and interconnections between nodes and the network, the wires, cables, and so forth.

Logical network topology is a little more abstract and strategic, referring to the conceptual understanding of how and why the network is arranged the way it is, and how data moves through it.

Why Is Network Topology Important?

The layout of your network is important for several reasons. Above all, it plays an essential role in how and how well your network functions. Choosing the right topology for your company's operational model can increase performance while making it easier to locate faults, troubleshoot errors, and more effectively allocate resources across the network to ensure optimal network health. A streamlined and properly managed network topology can increase energy and data efficiency, which can in turn help to reduce operational and maintenance costs.

The design and structure of a network are usually shown and manipulated in a software-created network topology diagram. These diagrams are essential for a few reasons, but

especially for how they can provide visual representations of both physical and logical layouts, allowing administrators to see the connections between devices when troubleshooting.

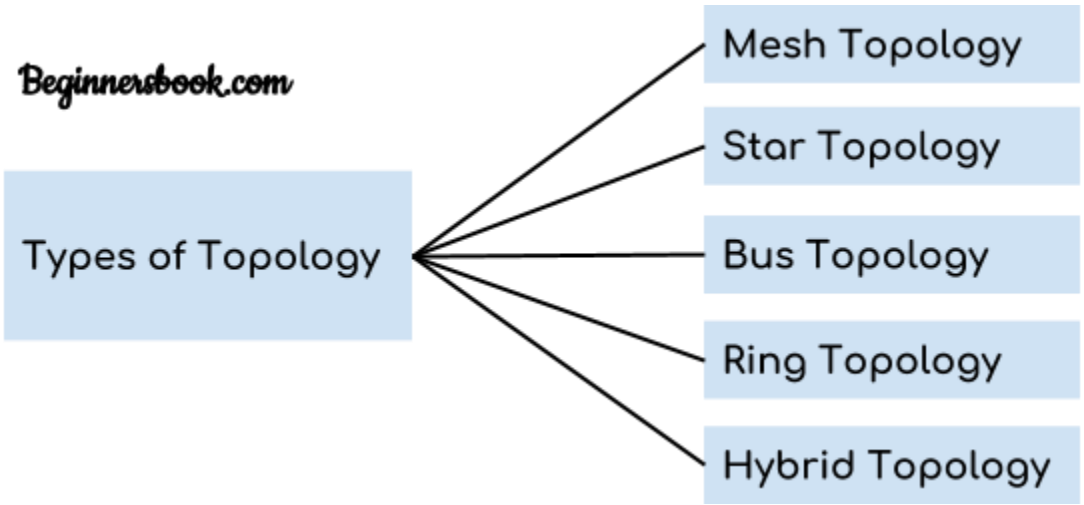
The way a network is arranged can make or break network functionality, connectivity, and protection from downtime. The question of, “What is network topology?” can be answered with an explanation of the two categories in the network topology.

1. Physical – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network.
2. Logical – The logical network topology is a higher-level idea of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources.

Effective network management and monitoring require a strong grasp of both the physical and logical topology of a network to ensure your network is efficient and healthy.

Types of Topology

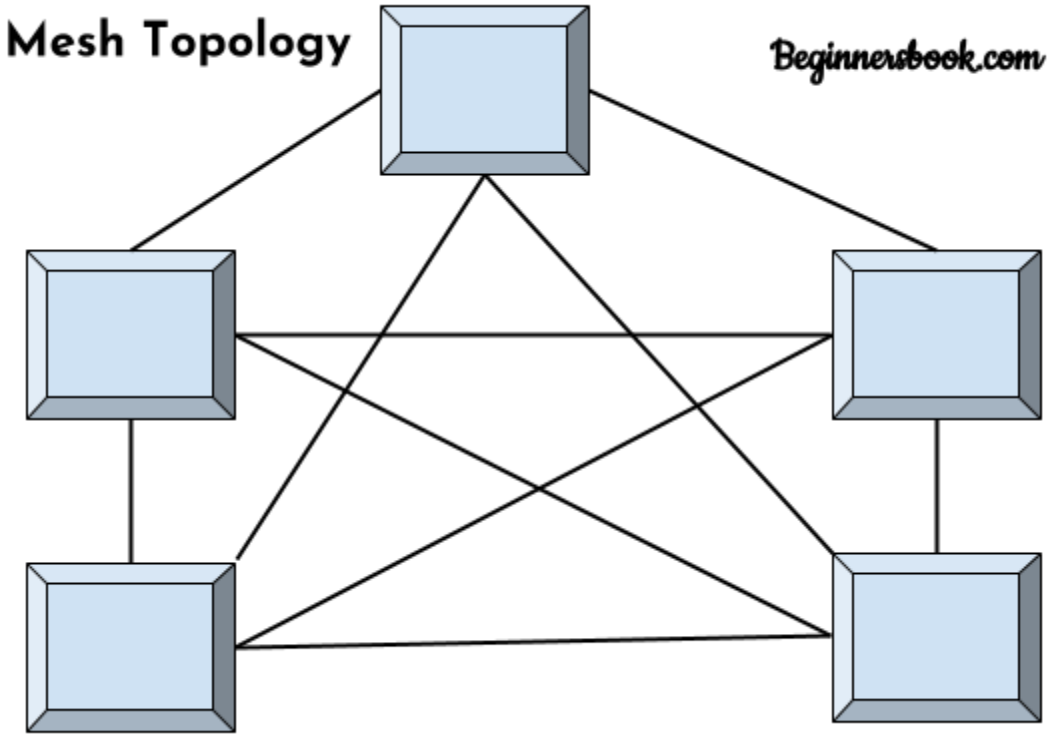
There are five types of topology in computer networks:



1. Mesh Topology
2. Star Topology
3. Bus Topology

4. Ring Topology
5. Hybrid Topology

Mesh Topology



In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

Advantages of Mesh topology

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point to point link thus unauthorized access

is not possible.

4. Fault detection is easy.

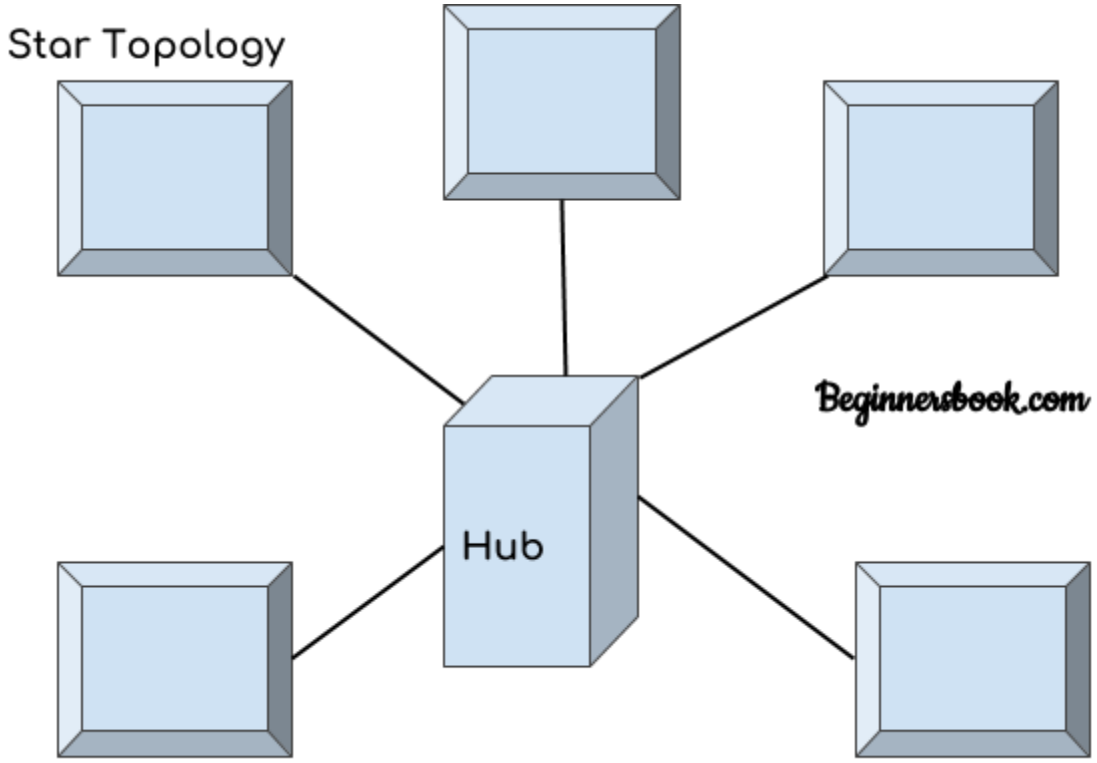
Disadvantages of Mesh topology

1. Amount of wires required to connected each system is tedious and headache.

2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.

3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

Star Topology



In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

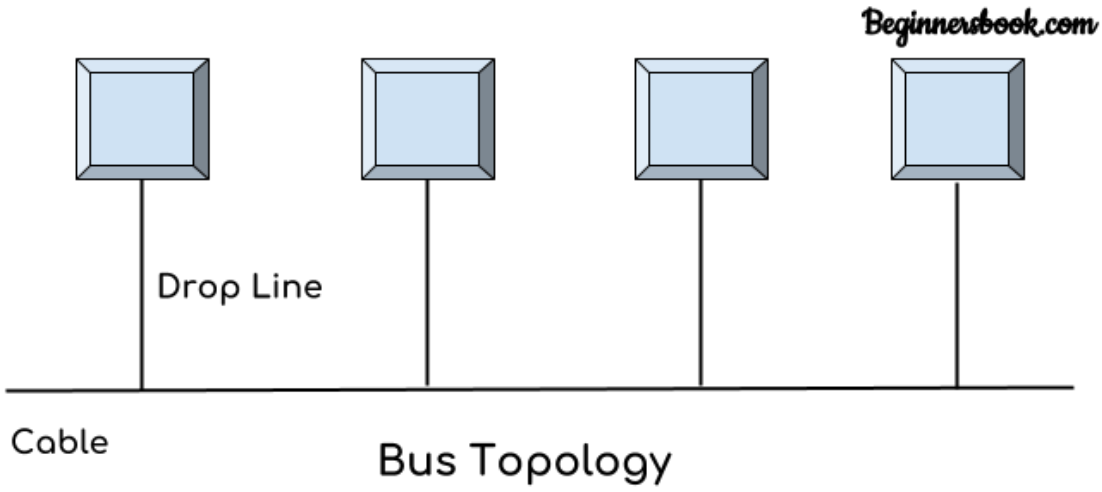
Advantages of Star topology

1. Less expensive because each device only need one I/O port and needs to be connected with hub with one link.
2. Easier to install
3. Less amount of cables required because each device needs to be connected with the hub only.
4. Robust, if one link fails, other links will work just fine.
5. Easy fault detection because the link can be easily identified.

Disadvantages of Star topology

1. If hub goes down everything goes down, none of the devices can work without hub.
2. Hub requires more resources and regular maintenance because it is the central system of star topology.

Bus Topology



In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

Advantages of bus topology

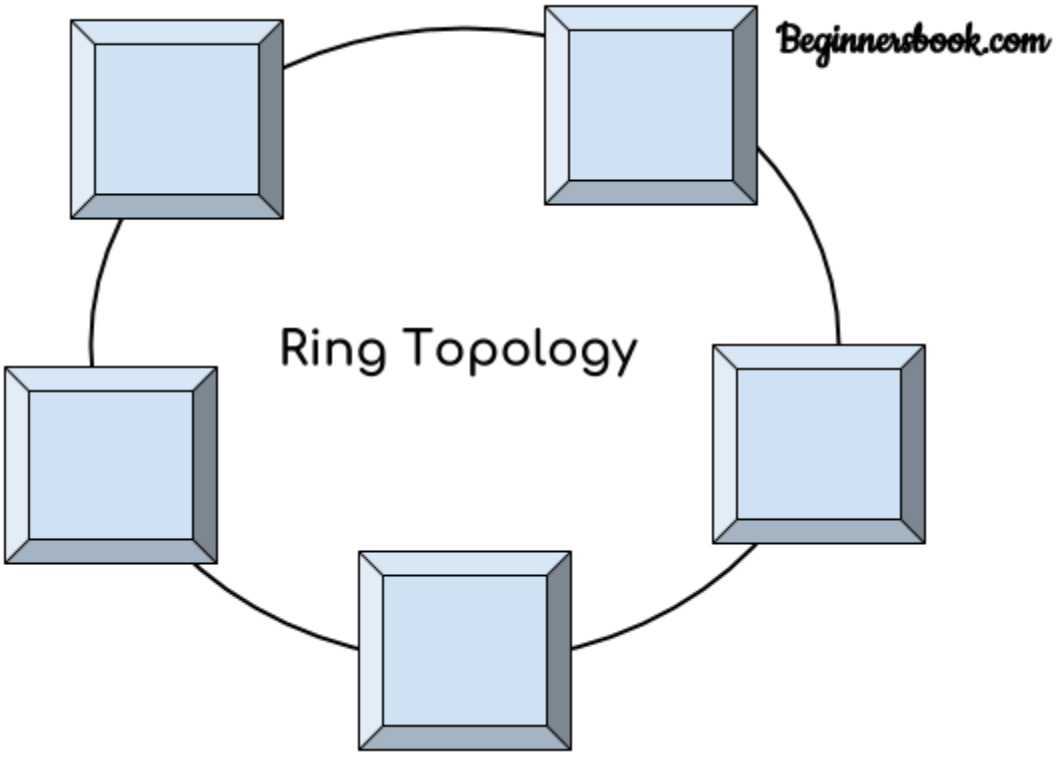
1. Easy installation, each cable needs to be connected with backbone cable.
2. Less cables required than Mesh and star topology

Disadvantages of bus topology

1. Difficultly in fault detection.

2. Not scalable as there is a limit of how many nodes you can connect with backbone cable.

Ring Topology



In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

Advantages of Ring Topology

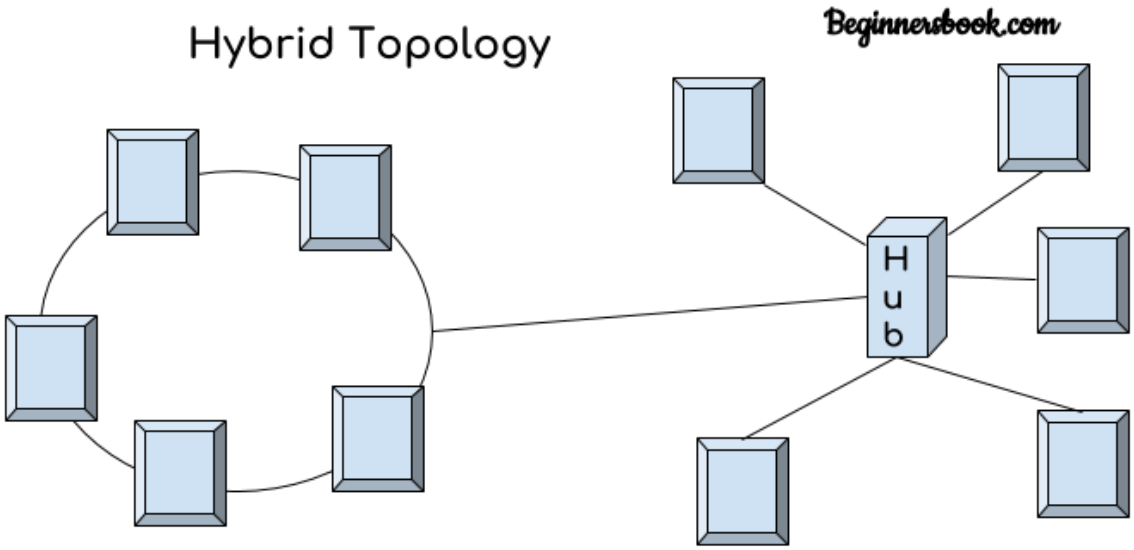
1.Easy to install.

2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.

Disadvantages of Ring Topology

1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.

Hybrid topology



A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

Disadvantages of Hybrid topology

1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive.

CHAPTER 3

DATA & SIGNALS

-To be transmitted, data must be transformed to electromagnetic signals.

Data can be Analog or Digital.

1. **Analog data** refers to information that is continuous; ex. sounds made by a human voice

2. **Digital data** refers to information that has discrete states. Digital data take on discrete values.

Signals can be of two types:

1. **Analog Signal:** They have infinite values in a range.

2. **Digital Signal:** They have limited number of defined values

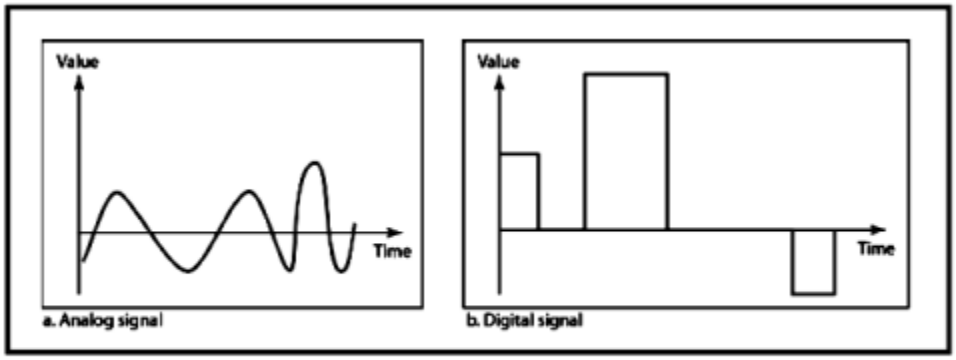


Figure: a. Analog Signal b. Digital Signal*

Periodic & Non-Periodic Signals

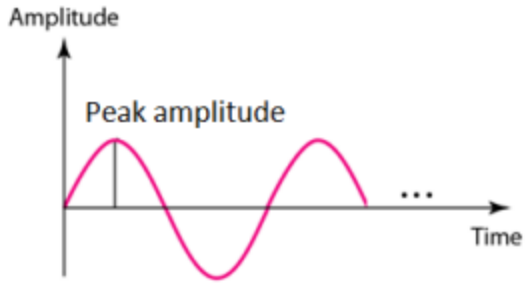
Signals which repeat itself after a fixed time period are called **Periodic Signals**

Signals which do not repeat itself after a fixed time period are called **Non-Periodic Signals.**

In data communications, we commonly use periodic analog signals and non-periodic digital signals.

Characteristics of an Analog Signal

1.Amplitude - The amplitude of a signal is the absolute value of its intensity at time t. The peak amplitude of a signal is the absolute value of the highest intensity.



2. Frequency - refers to the number of cycles completed by the wave in one second.

3.Period refers to the time taken by the wave to complete one second

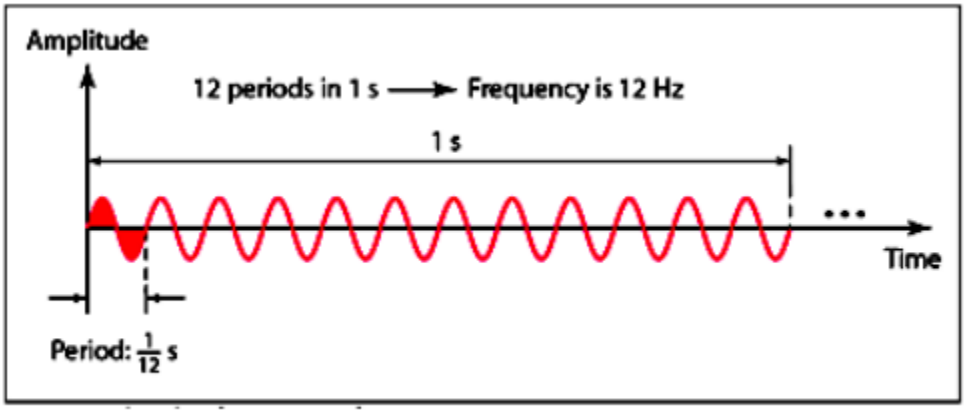
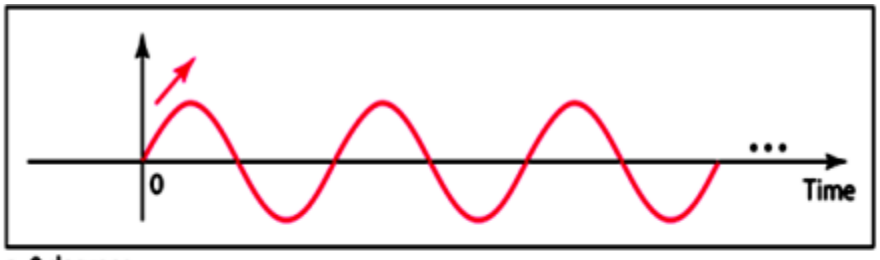
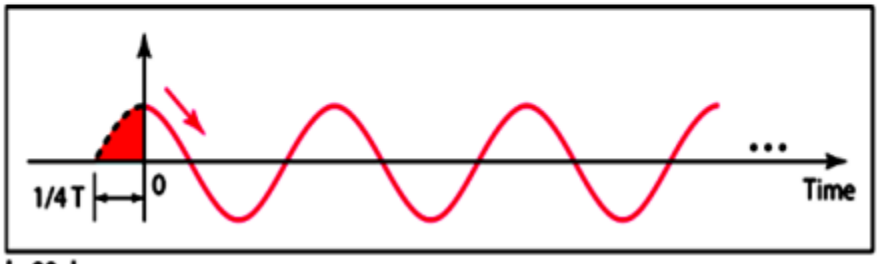


Fig: Frequency & Period of a sine wave

4. Phase - Phase describes the position of the waveform with respect to time (specifically relative to time O). Phase indicates the forward or backward shift of the waveform from the axis. It is measured in degrees or radian.



a. 0 degrees



b. 90 degrees

5. Wavelength

The wavelength is the distance a signal travels in one period. The wavelength of a signal refers to the relationship between frequency (or period) and propagation speed of the wave through a medium.

Transmission of Digital signal

1. **Baseband Transmission**

The signal is transmitted without making any change to it (ie. Without modulation). In baseband transmission, the bandwidth of the signal to be transmitted has to be less than the bandwidth of the channel.

2. **Broad band Transmission**

Given a bandpass channel, a digital signal cannot be transmitted directly through it. In broadband transmission we use modulation, i.e we change the signal to analog signal before transmitting it. The digital signal is first converted to an analog signal, since we have a bandpass channel we cannot directly send this signal through the available channel.

BANDWIDTH OF A SIGNAL

Bandwidth can be defined as the portion of the electromagnetic spectrum occupied by the signal. It may also be defined as the frequency range over which a signal is transmitted. Different types of signals have different bandwidth. Ex. Voice signal, music signal, etc Bandwidth of analog and digital signals are calculated in separate ways; analog signal bandwidth is measured in terms of its frequency (hz) but digital signal bandwidth is measured in terms of bit rate (bits per second, bps). Bandwidth of signal is different from bandwidth of the medium/channel

Bandwidth of an analog signal - Bandwidth of an analog signal is expressed in terms of its frequencies. It is defined as the range of frequencies that the composite analog signal carries. It is calculated by the difference between the maximum frequency and the minimum frequency. It has a minimum frequency of F1 = 30Hz and maximum frequency of F2 = 90Hz.

Bandwidth of a digital signal - It is defined as the maximum bit rate of the signal to be transmitted. It is measured in bits per second.

BANDWIDTH OF A CHANNEL

A channel is the medium through which the signal carrying information will be passed. In terms of analog signal, bandwidth of the channel is the range of frequencies that the channel can

carry. In terms of digital signal, bandwidth of the channel is the maximum bit rate supported by the channel. i.e. the maximum amount of data that the channel can carry per second. The bandwidth of the medium should always be greater than the bandwidth of the signal to be transmitted else the transmitted signal will be either attenuated or distorted or both leading in loss of information. The channel bandwidth determines the type of signal to be transmitted i.e. analog or digital.

THE MAXIMUM DATA RATE OF A CHANNEL

Data rate depends on three factors:

- The bandwidth available
- The level of the signals we use
- The quality of the channel (the level of noise)

The quality of the channel indicates two types:

a) A Noiseless or Perfect Channel - An ideal channel with no noise. The Nyquist Bit rate derived by Henry Nyquist gives the bit rate for a Noiseless Channel.

b) A Noisy Channel - A realistic channel that has some noise. The Shannon Capacity formulated by Claude Shannon gives the bit rate for a Noisy Channel

Nyquist Bit Rate

The Nyquist bit rate formula defines the theoretical maximum bit rate for a noiseless channel

Bitrate = 2 x Bandwidth x Log2 L

Where,

- ✓ Bitrate is the bitrate of the channel in bits per second
- ✓ Bandwidth is the bandwidth of the channel
- ✓ L is the number of signal levels.

Example

What is the maximum bit rate of a noiseless channel with a bandwidth of 5000 Hz transmitting a signal with two signals

levels.

Solution:

The bit rate for a noiseless channel according to Nyquist Bit rate can be calculated as follows:

BitRate = 2 x Bandwidth x Log2 L

= 2 x 5000 x log2 2 =10000 bps

Shannon Capacity

The Shannon Capacity defines the theoretical maximum bit rate for a noisy channel

Capacity=bandwidth X log2 (1 +SNR)

Where,

- ✓ Capacity is the capacity of the channel in bits per second
- ✓ Bandwidth is the bandwidth of the channel
- ✓ SNR is the Signal to Noise Ratio

Shannon Capacity for calculating the maximum bit rate for a noisy channel does not consider the number of levels of the

signals being transmitted as done in the Nyquist bit rate.

Example:

Calculate the bit rate for a noisy channel with SNR 300 and bandwidth of 3000Hz

Solution:

The bit rate for a noisy channel according to Shannon Capacity can be calculated as follows:

Capacity=bandwidth X log2 (1 +SNR)

= 3000 x log2 (1 + 300)

= 3000 x log2 (301)

= 3000 x 8.23

= 24,690bps

SIGNAL ENCODING

Signal encoding is the conversion from analog/digital data to analog / digital signal.

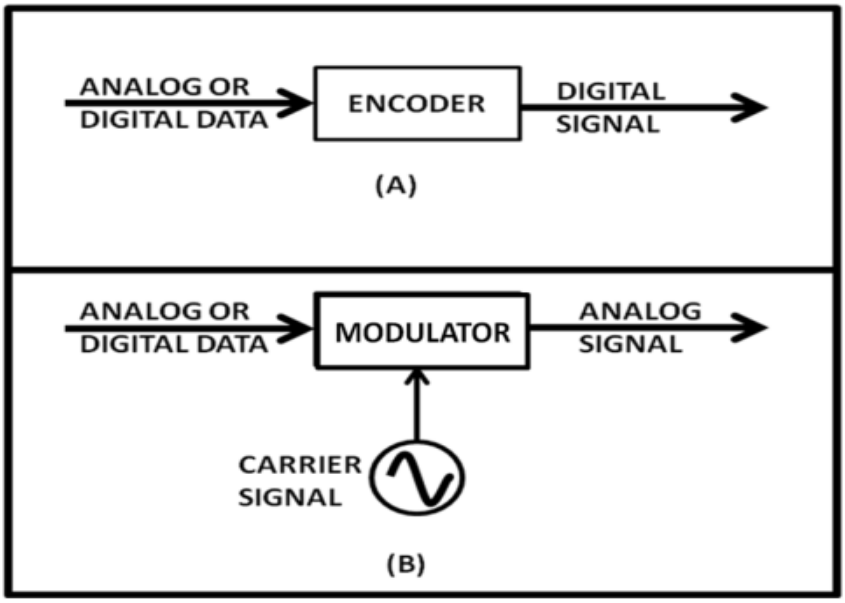


Figure: Signal Encoding

The possible encodings are:

- ✓ Digital data to Digital Signal
- ✓ Digital data to Analog Signal
- ✓ Analog data to Digital Signal
- ✓ Analog data to Analog Signal

Digital Data to Digital Signal

- ✓ Non Return to Zero NRZ

NRZ Codes has **1** for High voltage level and **0** for Low voltage level. The main behavior of NRZ codes is that the voltage level remains constant during bit interval. The end or start of a bit will not be indicated and it will maintain the same voltage state, if the value of the previous bit and the value of the present bit are same.

- ✓ **NRZ - I NRZ–INVERTED**

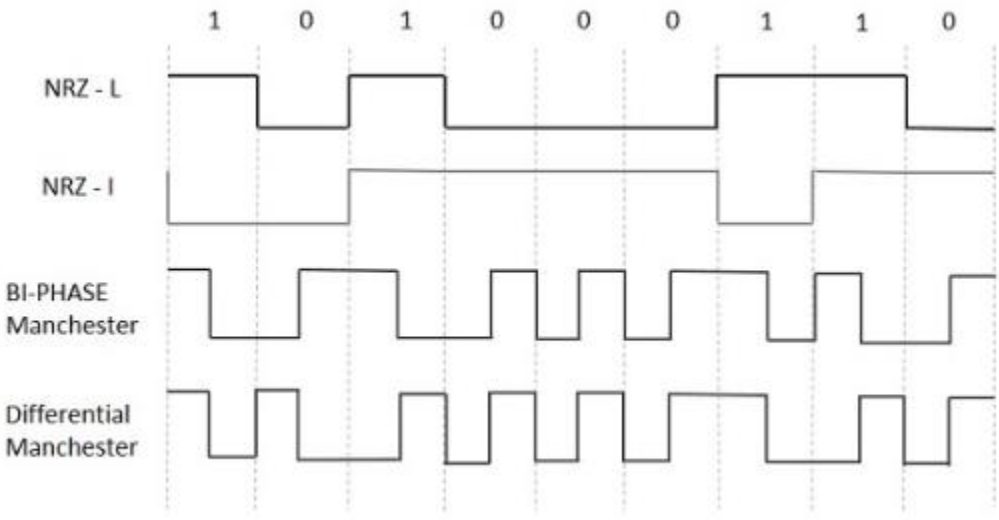
If a **1** occurs at the incoming signal, then there occurs a transition at the beginning of the bit interval. For a **0** at the incoming signal, there is no transition at the beginning of the bit interval.

- ✓ **Bi-phase Manchester**

In this type of coding, the transition is done at the middle of the bit-interval. The transition for the resultant pulse is from High to Low in the middle of the interval, for the input bit 1. While the transition is from Low to High for the input bit **0**.

- ✓ **Differential Manchester**

In this type of coding, there always occurs a transition in the middle of the bit interval. If there occurs a transition at the beginning of the bit interval, then the input bit is **0**. If no transition occurs at the beginning of the bit interval, then the input bit is **1**.



Analog data to analog signal

Modulation - The Process of converting analog data to analog signal is called Modulation. Modulation is used to send an information bearing signal over long distances. Modulation is the process of varying some characteristic of a periodic wave with an external signal called carrier signal. These carrier signals are high frequency signals and can be transmitted over the air easily and are capable of traveling long distances. The characteristics (amplitude, frequency, or phase) of the carrier signal are varied in accordance with the information bearing signal(analog data).The information bearing signal is also known as the modulating signal.

Types of Modulation:

Signal modulation can be divided into two broad categories:

- ✓ Analog modulation and
- ✓ Digital modulation.

Analog Modulation can be accomplished in three ways: *Amplitude modulation (AM), Frequency modulation, Phase modulation (PM)*

- ✓ **Amplitude modulation (AM) -** Amplitude modulation is a type of modulation where the amplitude of the carrier signal is varied in accordance with modulating signal. The envelope, or boundary, of the amplitude modulated signal embeds modulating signal.

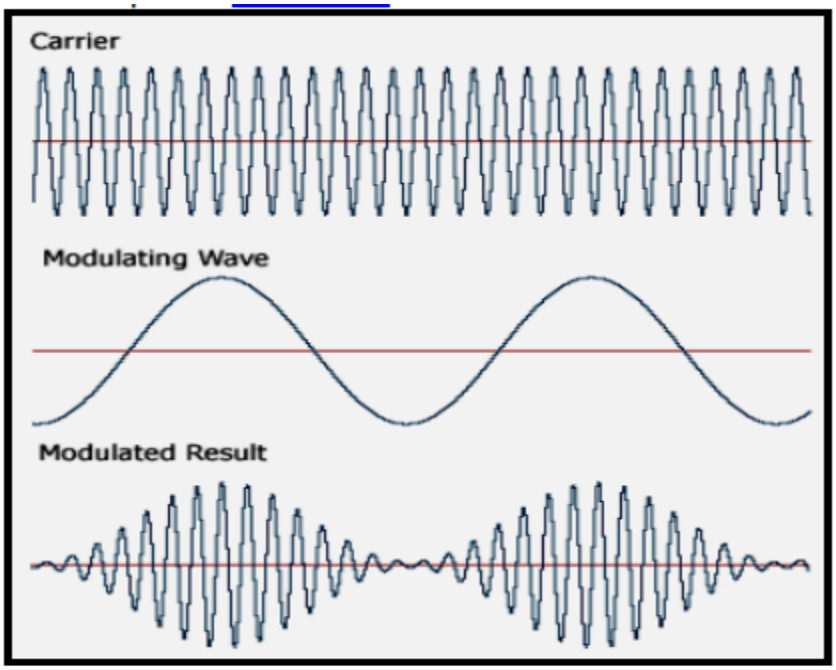


Figure : Amplitude modulation (AM)

- ✓ **Frequency modulation (FM)** Frequency modulation is a type of modulation where the frequency of the carrier is varied in accordance with the modulating signal. The amplitude of the carrier remains constant. The information-bearing signal (the modulating signal) changes the instantaneous frequency of the carrier. Since the amplitude is kept constant, FM modulation is a low-noise process and provides a high quality modulation technique which is used for music and speech in hifidelity broadcasts.

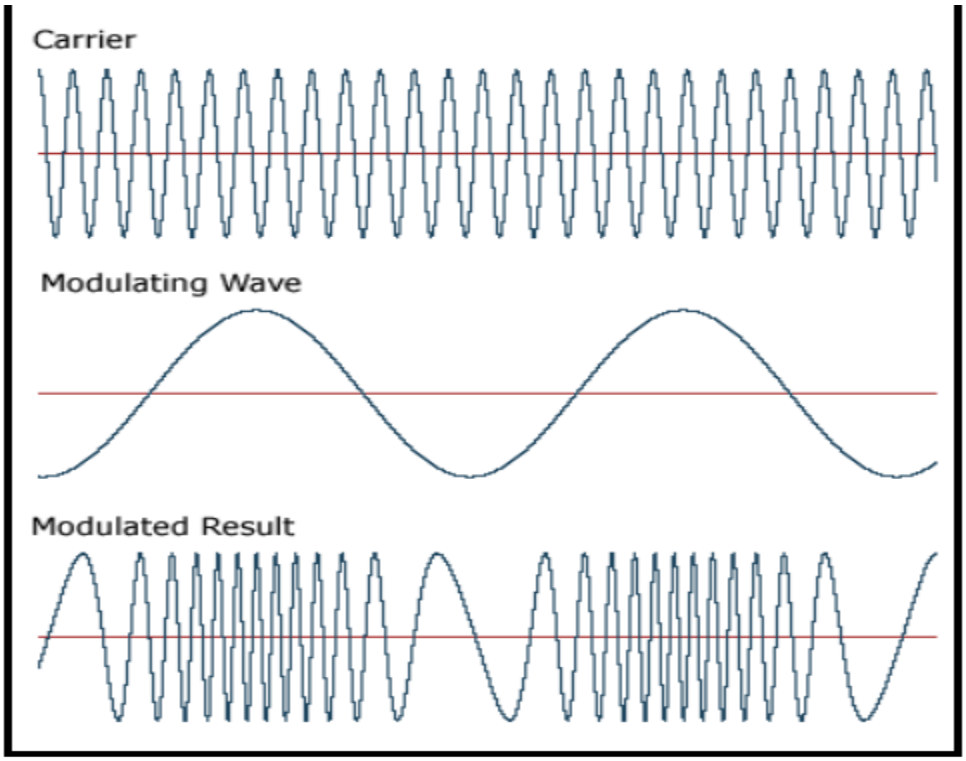


Figure : Frequency modulation (FM)

- ✓ **Phase modulation (PM).** In phase modulation, the instantaneous phase of a carrier wave is varied from its reference value by an amount proportional to the instantaneous amplitude of the modulating signal.

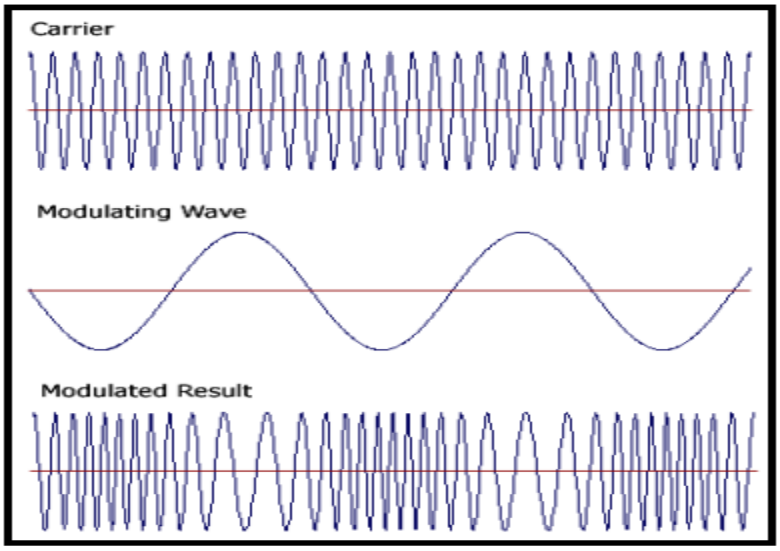


Figure : Phase modulation (PM).

Digital Modulation Types(Digital to Analog signal conversion)

Digital modulation is used to convert digital data to analog signal.

It can be accomplished in the following ways:

- ✓ Amplitude Shift Keying (ASK)
- ✓ Binary ASK (BASK)
- ✓ Frequency Shift Keying (FSK)
- ✓ Phase Shift Keying (PSK)

- **Amplitude Shift Keying (ASK)** In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes.
- **Binary ASK** - is normally implemented using only two levels and is hence called binary amplitude shift keying. Bit 1 is transmitted by a carrier of one particular amplitude. To transmit Bit 0 we change the amplitude keeping the freqQ\uency is kept constant

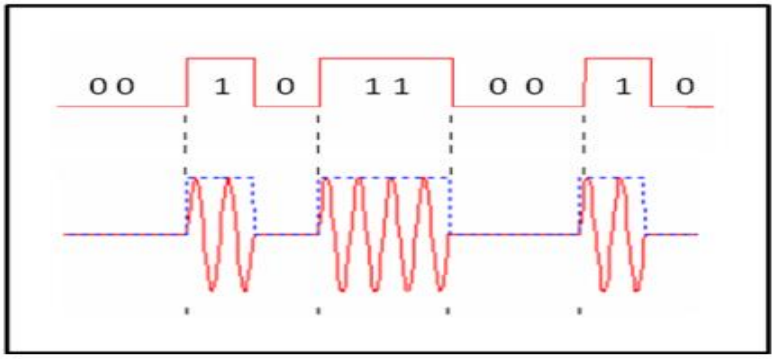


Figure : Amplitude Shift Keying (ASK

- **Frequency Shift Keying (FSK)** In Frequency shift keying, we change the frequency of the carrier wave. Bit 0 is represented by a specific frequency, and bit 1 is represented by a different frequency. In the figure below frequency used for bit 1 is higher than frequency used for bit 0

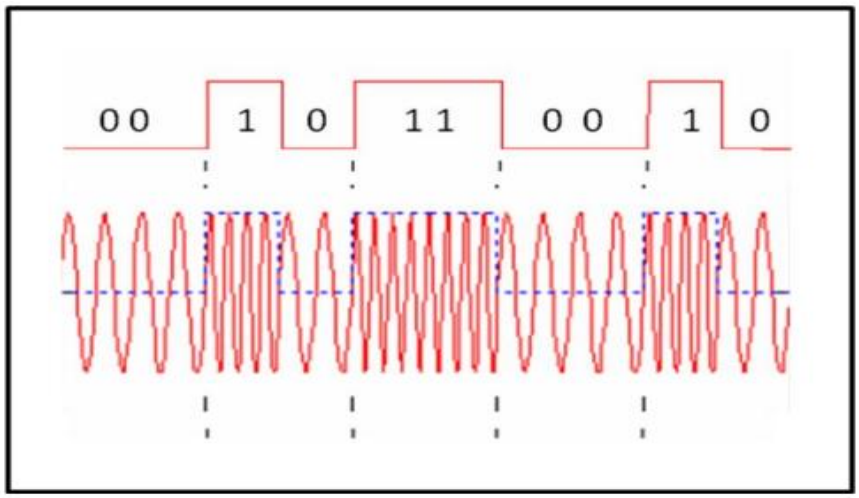


Figure : Frequency Shift Keying (FSK)

- **Phase Shift Keying (PSK)** Phase shift keying (PSK) is a method of transmitting and receiving digital signals in which the phase of a transmitted signal is varied to convey information. Both amplitude and frequency remain constant as the phase changes. The simplest from of PSK has only two phases, 0 and 1. If the phase of the wave does not change, then the signal state stays the same (low or high). If the phase of the wave changes by 180 degrees, that is, if the phase reverses, then the signal state changes (from low to high or from high to low)

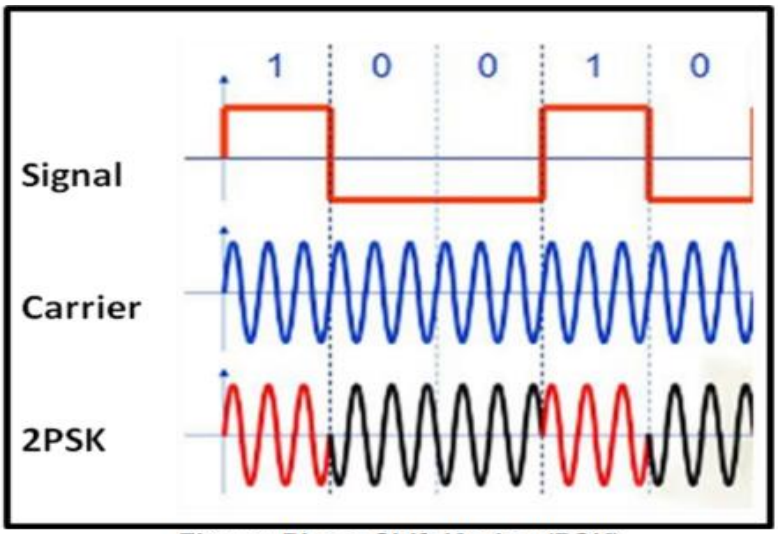


Figure: Phase Shift Keying (PSK)

Analog to Digital Conversion using modulation

- PAM (Pulse Amplitude Modulation)
- PCM (Pulse Code Modulation)
- PWM (Pulse Width Modulation)

Pulse Amplitude Modulation refers to a method of carrying information on a train of pulses, the information being encoded in the amplitude of the pulses.

PCM is a general scheme for transmitting analog data in a digital and binary way, independent of the complexity of the analog waveform. With PCM all forms of analog data like video, voice, music and telemetry can be transferred. To obtain PCM from an analog waveform at the source (transmitter), the analog signal amplitude is sampled at regular time intervals. The sampling rate (number of samples per second), is several times the maximum frequency of the analog waveform. The amplitude of the analog signal at each sample is rounded off to the nearest binary level (quantization). The number of levels is always a power of 2 (4, 8, 16, 32, 64, ...). These numbers can be represented by two, three, four, five, six or more binary digits (bits) respectively. At the destination (receiver), a pulse code demodulator converts the binary numbers back into pulses having the same quantum levels as those in the modulator. These pulses are further processed to restore the original analog waveform.

Pulse Width Modulation refers to a method of carrying information on a train of pulses, the information being encoded in the width of the pulses. In applications to motion control, it is not exactly information we are encoding, but a method of controlling power in motors without (significant) loss. There are several schemes to accomplish this technique. One is to switch voltage on and off, and let the current recirculate through diodes when the transistors have switched off. Another technique is to switch voltage polarity back and forth with a full-bridge switch arrangement, with 4 transistors.

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 circuitfor an exchange between two or more parties. On an

Ethernetlocal area network (LAN), a switch determines from the physical device (Media Access Control or MAC) address in each incoming message framewhich output port to forward it to and out of. In a wide area packet-switchednetwork such as the Internet, a switch determines from the IPaddressin each packetwhich 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 2or Data-link layerfunction. 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 :

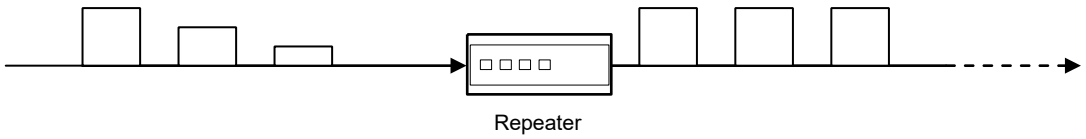
Attenuation: Loss of signal strength as the signal travels along a medium.

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.

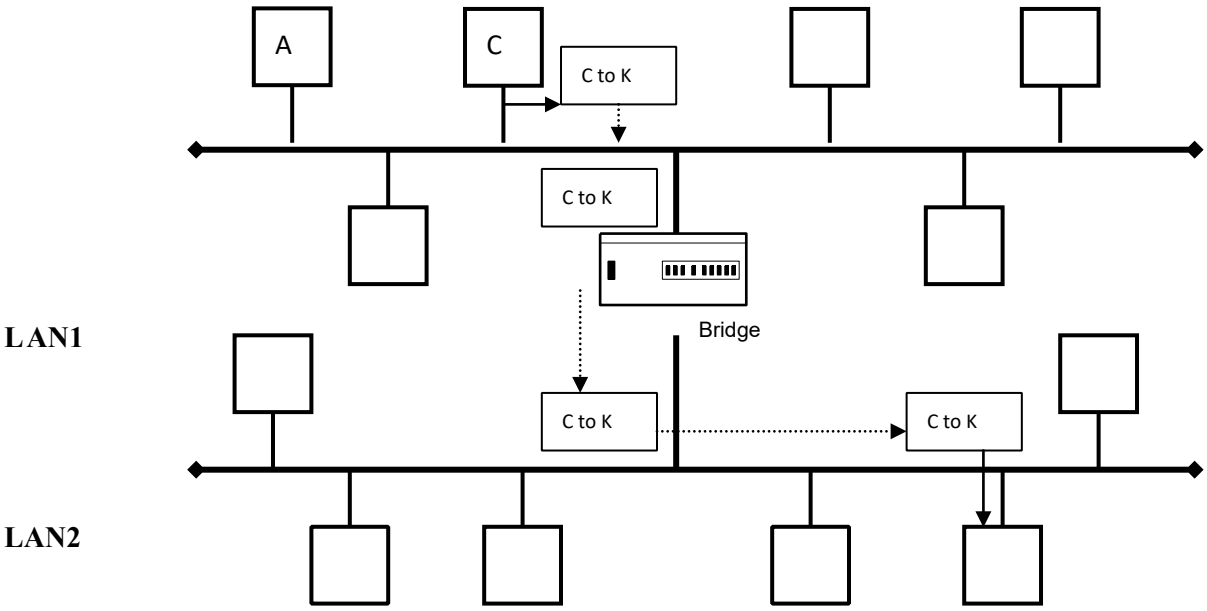
Bridge

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

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:

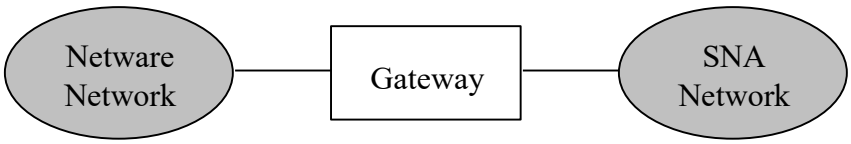
- Can connect networks of different physical media and network architectures
- Can choose the best path for a packet through an internetwork
- reduces network traffic by not forwarding corrupt packets Limitation:
- More expensive a more complex than bridges or repeaters.
- Slower than bridge because 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.

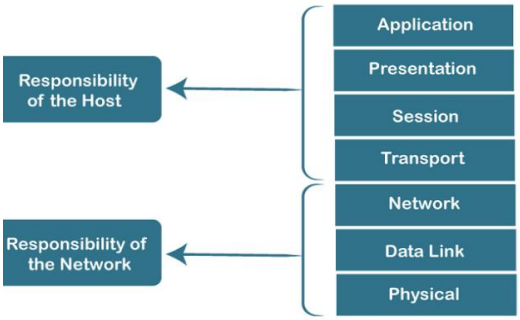
Greater processing requirements men they are slower than other devices.

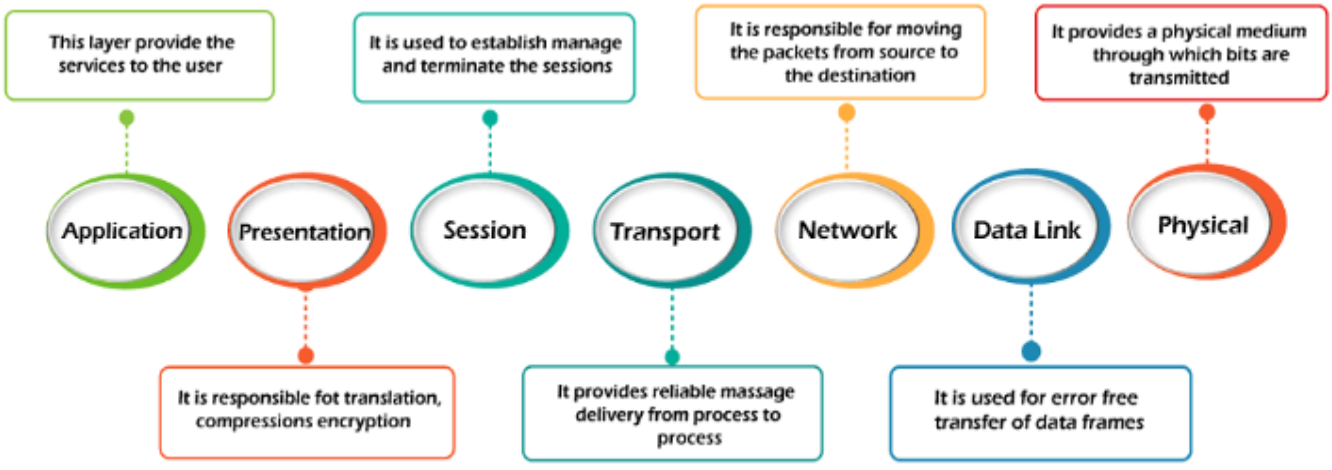
CHAPTER 4

NETWORK MODELS

Open Systems Interconnection (OSI) Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.





1) Physical layer

- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

2) Data-Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - **Logical Link Control Layer**
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.
        - It also provides flow control.
    - **Media Access Control Layer**

- A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
- It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.
- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3) Network Layer

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.

- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4) Transport Layer

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.

- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5) Session Layer

- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.
-

6) Presentation Layer

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different

encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

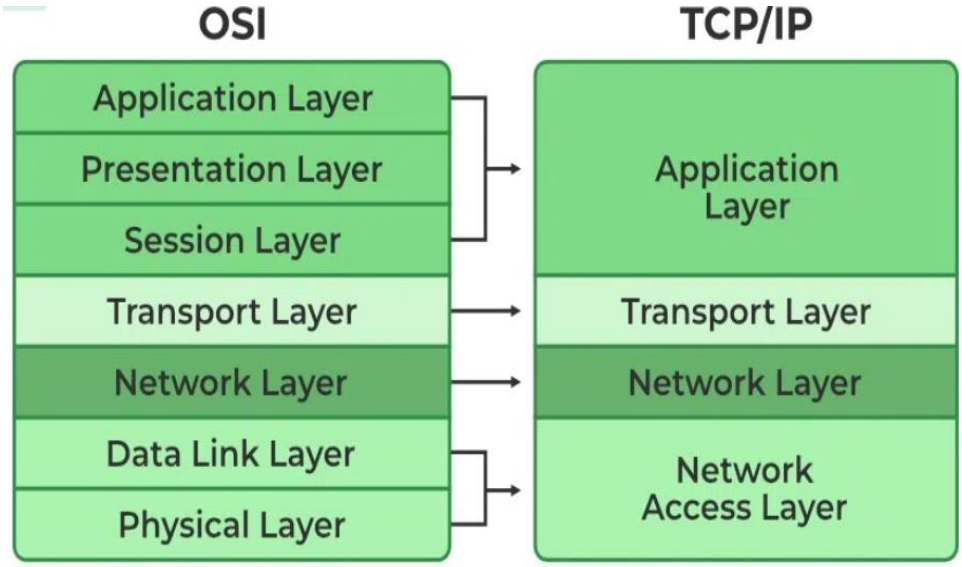
7) Application Layer

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP MODEL



Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer/ network layer.

- An internet layer is the second layer of the TCP/IP model.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

CHAPTER 5

MULTIPLE ACCESS PROTOCOL/MEDIA ACCESS CONTROLS

CSMA/CD (Collision Detection): This is an extension of CSMA used in Ethernet networks. In CSMA/CD, devices listen while transmitting to detect collisions. If a collision is detected, the devices involved in the collision wait for a random amount of time before attempting to retransmit.

CSMA/CA (Collision Avoidance): Unlike CSMA/CD, CSMA/CA is used in wireless networks where collision detection is not feasible. Devices using CSMA/CA attempt to avoid collisions by waiting for random periods before transmitting data.

Token Passing: In token passing networks, a token is passed sequentially between devices. Only the device holding the token can transmit data. This method ensures fair access to the network and eliminates collisions.

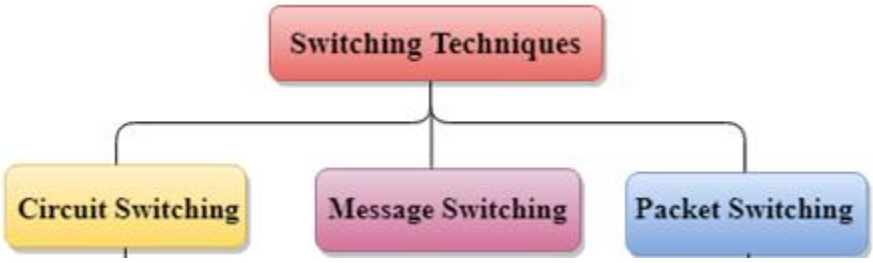
Polling: In polling, a central controller polls each device in the network in turn, granting permission to transmit data when it's their turn. This method is commonly used in centralized networks but can suffer from inefficiency and delays.

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

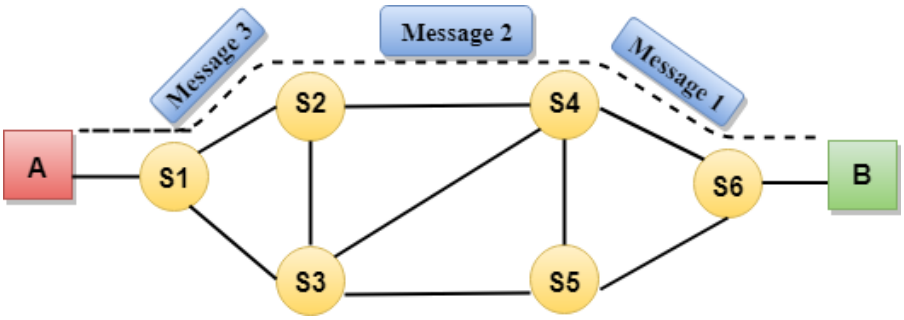
Classification Of Switching Techniques



Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.

- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.



Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

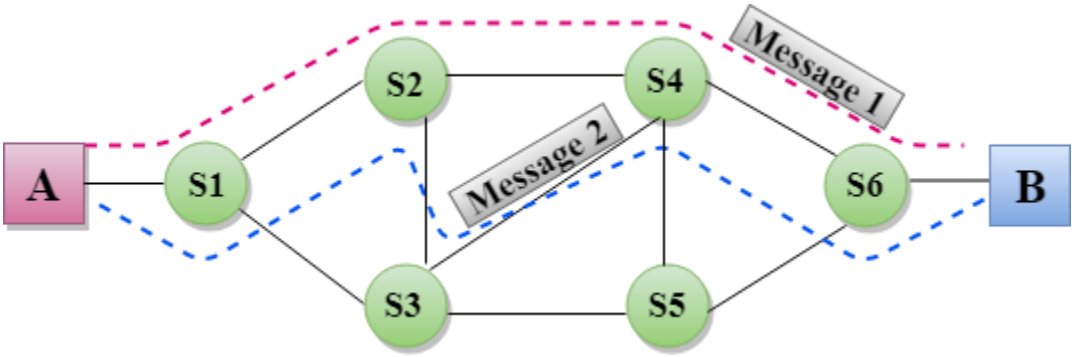
Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.

- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

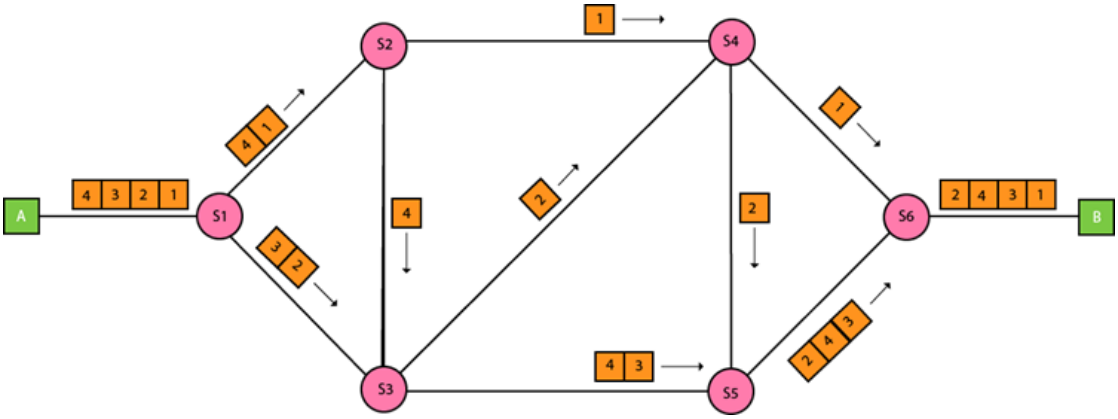
Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.

- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.

The protocols used in a packet switching technique are very complex and requires high implementation cost.

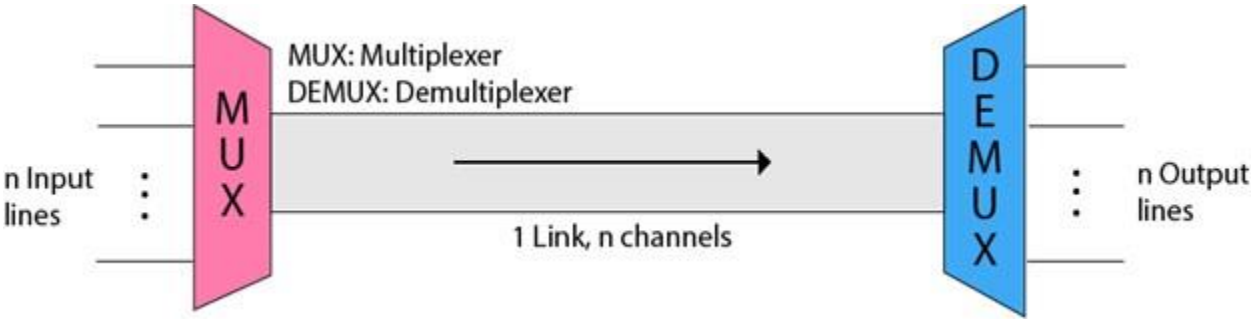
If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered

Multiplexing

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer (MUX).

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs).

Concept of Multiplexing

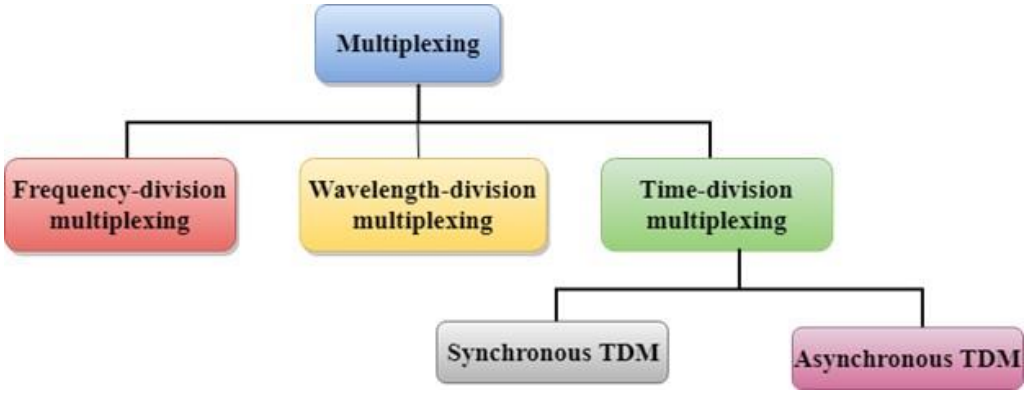


- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

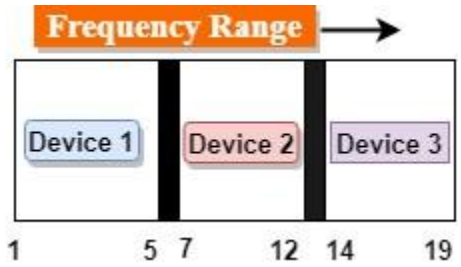
- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

Multiplexing Techniques



Frequency-division Multiplexing (FDM)

It is an analog technique. **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.

The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.

The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.

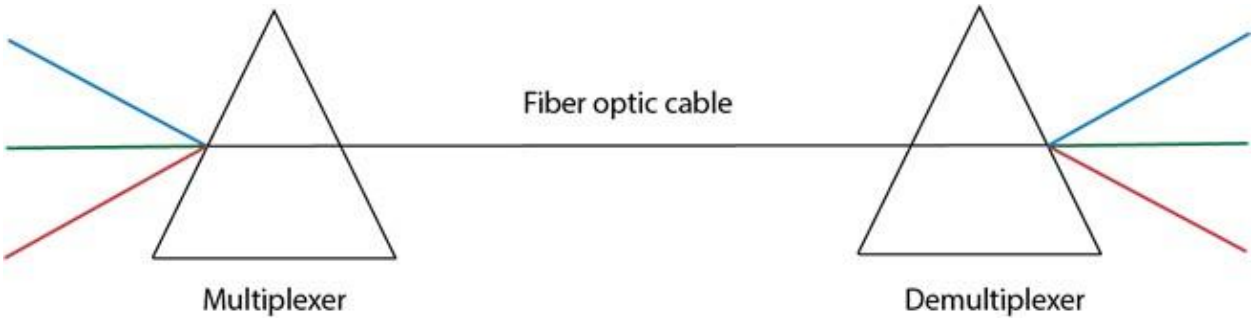
Applications Of FDM:

- FDM is commonly used in TV networks.
- It is used in FM and AM broadcasting.

Wavelength Division Multiplexing (WDM)

Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable. WDM is used on fibre optics to increase the capacity of a single fibre. It is used to utilize the high data rate capability of fibre optic cable. It is an analog multiplexing technique.

Optical signals from different source are combined to form a wider band of light with the help of multiplexer. At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.



Time Division Multiplexing

- It is a digital technique. In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.

There are two types of TDM:

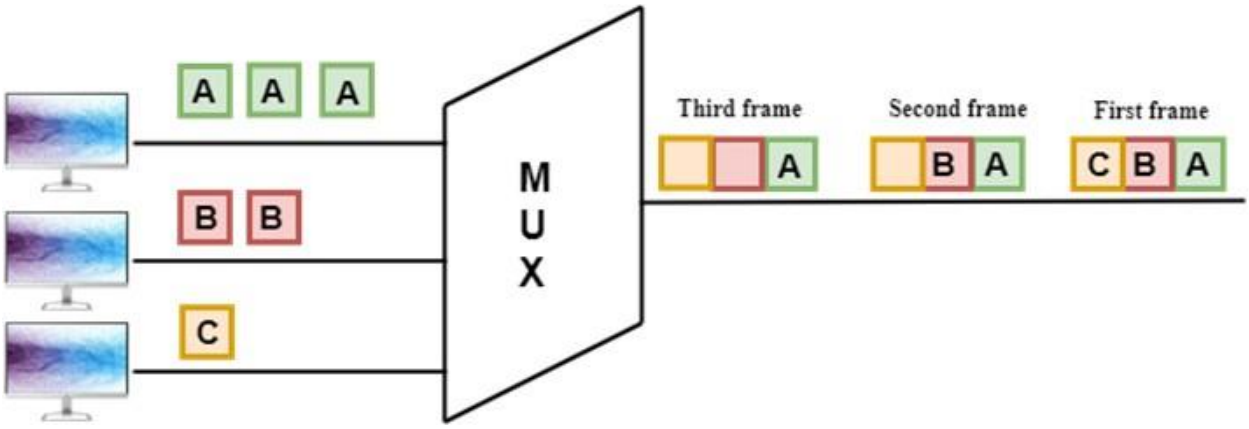
- Synchronous TDM ○ Asynchronous TDM

Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.

- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not. If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.

Concept Of Synchronous TDM



In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Disadvantages Of Synchronous TDM

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data.

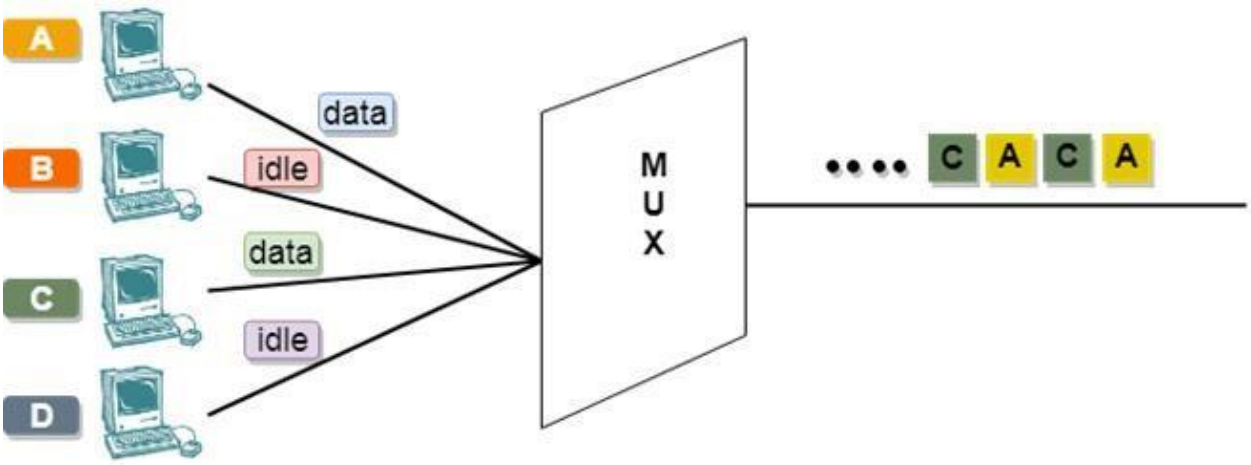
Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send.

Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.

- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.

Concept Of Asynchronous TDM



In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Error Detection

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types Of Errors

- **Single-Bit Error:**
  The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.
- **Burst Error:**
  The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

Error Detecting Techniques**: (Read more)**
The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Error Correction
Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

- **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

CHAPTER 6 Network Layer

Classful Addressing

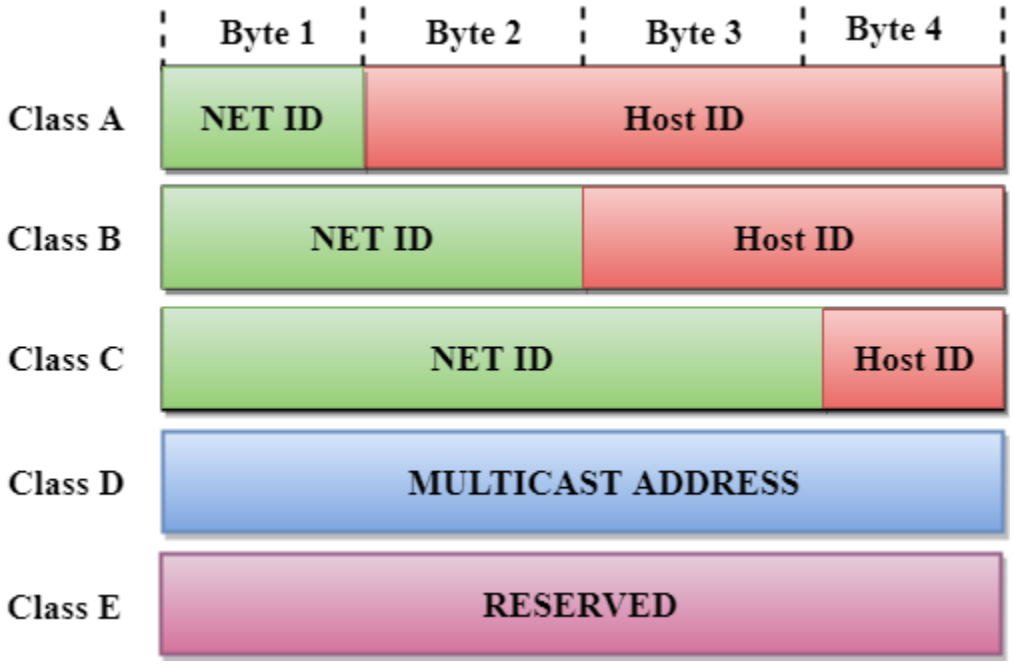
An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A (0.0.0.0 – 127.255.255.255)

- Class B (128.0.0.0 – 191.255.255.255)
- Class C (192.0.0.0 – 223.255.255.255)
- Class D (224.0.0.0 – 239.255.255.255)
- Class E (240.0.0.0 – 255.255.255.254)

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Routing

- A Routing is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.

Types of Routing

- Static Routing
- Default Routing
- Dynamic Routing

Static Routing

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

Advantages Of Static Routing

Following are the advantages of Static Routing:

- **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
- **Bandwidth:** It has not bandwidth usage between the routers.
- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantages of Static Routing:

Following are the disadvantages of Static Routing:

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

Default Routing

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.

When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table

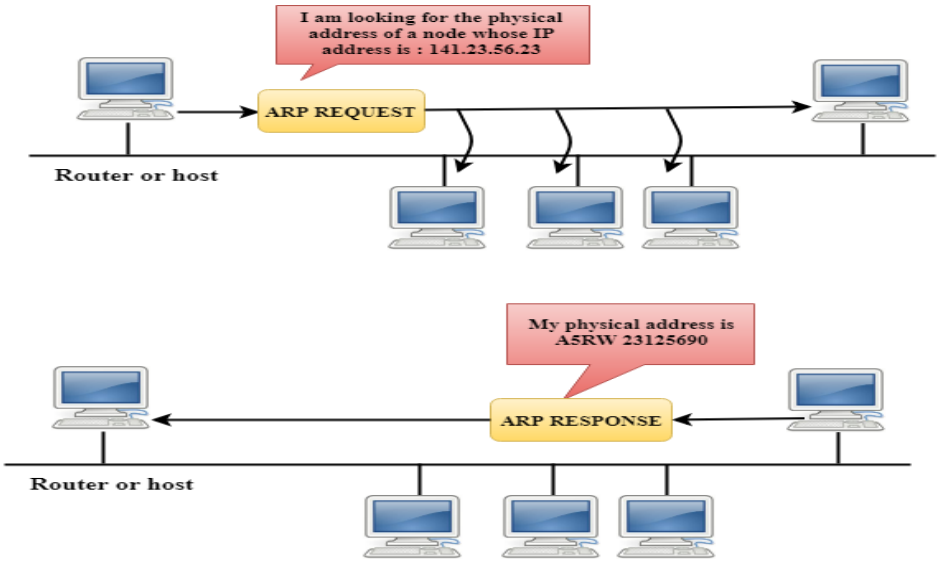
Network Layer Protocols

TCP/IP supports the following protocols:

- ARP - Address Resolution Protocol.
- RARP - Reverse Address Resolution Protocol.
- ICMP - Internet Control Message Protocol
- IGMP - Internet Group Message Protocol.

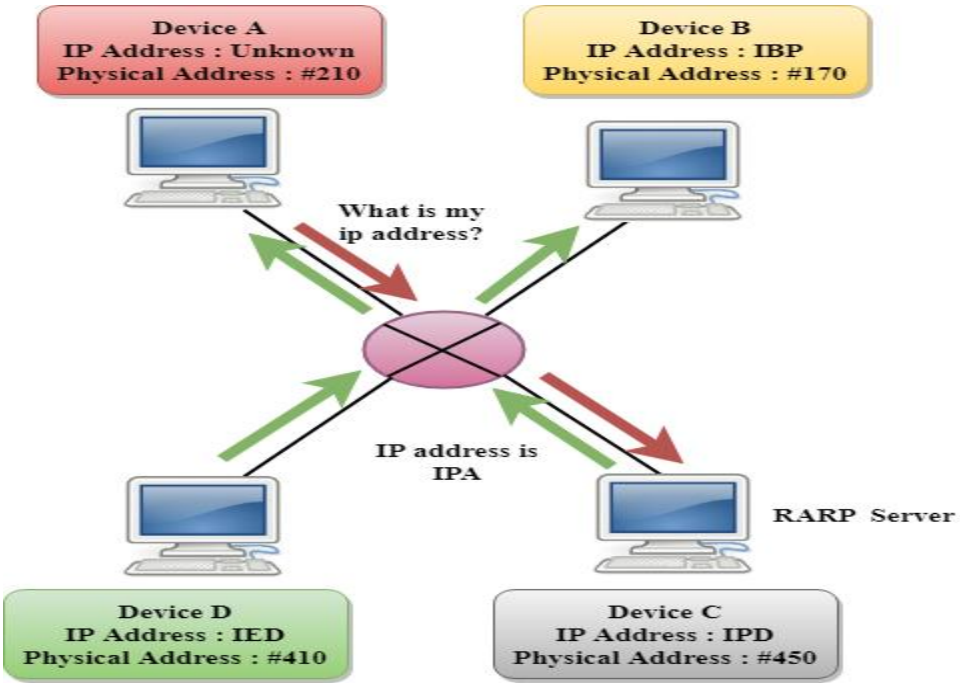
ARP

If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.



RARP

- RARP stands for **Reverse Address Resolution Protocol**.
- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

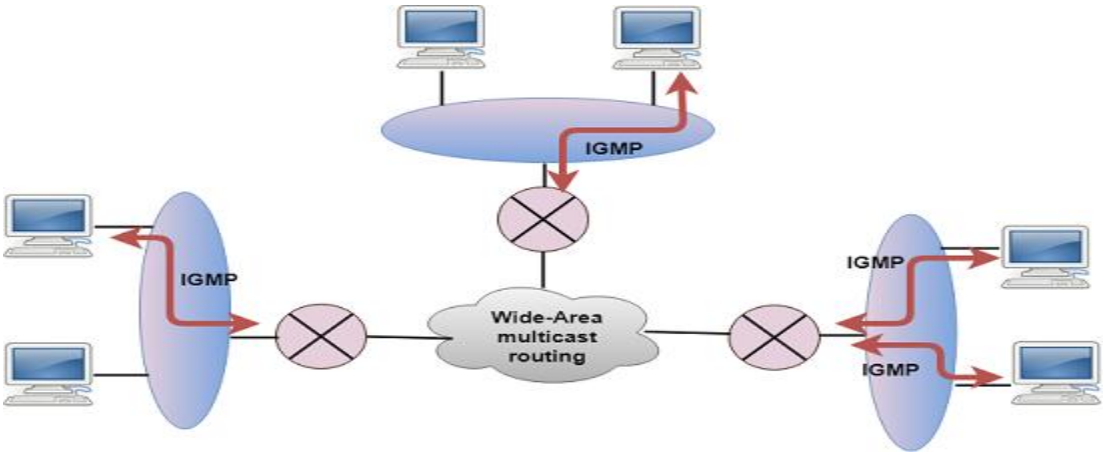


ICMP

- ICMP stands for Internet Control Message Protocol.
- The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
- ICMP uses echo test/reply to check whether the destination is reachable and responding.
- ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
- An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
- ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
- ICMP messages are transmitted within IP datagram.
- IGMP stands for **Internet Group Message Protocol**.
- The IP protocol supports two types of communication:
    - **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.

- **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.

- The IGMP protocol is used by the hosts and router to support multicasting.
- The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.



Transport Layer protocols

Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destinatio computer without verifying whether the receive is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes

acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor retransmits the damaged frame.

CHAPTER 7

Ethernet Standards

- Ethernet protocols describe the rules that control how communication occurs on an Ethernet network.
- **IEEE 802.3** Ethernet standard specifies that a network implement the CSMA/CD access control method.
- In **CSMA/CD** all end stations "listen" to the network wire for clearance to send data. When the end station detects that no other host is transmitting, the end station will attempt to send data. Unfortunately collisions might occur.

Cabled Ethernet standards

10BASE-T

- The IEEE 802.3 standard defines several physical implementations that support Ethernet. Some of the common implementations are described here.
- 10BASE-T is an Ethernet technology that uses a star topology. 10BASE-T is a popular Ethernet architecture whose features are indicated in its name:
    - The ten (10) represents a speed of 10 Mbps.
    - BASE represents baseband transmission. In baseband transmission, the entire bandwidth of a cable is used for one type of signal.
    - The T represents twisted-pair copper cabling.

Advantages of10BASE-T:

- Installation of cable is inexpensive compared to fiber-optic installation.
- Cables are thin, flexible, and easier to install than coaxial cabling.
- Equipment and cables are easy to upgrade.

Disadvantages of 10BASE-T:

- The maximum length for a 10BASE-T segment is only 328 ft (100 m).
- Cables are susceptible to Electromagnetic Interference (EMI).

100BASE-TX “FastEthernet”

- The high bandwidth demands of many modern applications, such as live video conferencing and streaming audio, have created a need for higher data-transfer speeds. Many networks require more bandwidth than 10 Mbps Ethernet. 100BASE-TX is much faster than 10BASE-T and has a theoretical bandwidth of 100 Mbps. The "X" indicates that you can use many different types of copper and fiber-optic cabling.
- Advantages of 100BASE-TX:
    - At 100 Mbps, transfer rates of 100BASE-TX are ten times that of 10BASE-T.
    - 100BASE-X uses twisted-pair cabling, which is inexpensive and easy to install.
- Disadvantages of 100BASE-TX:
    - The maximum length for a 100BASE-TX segment is only 328 ft (100 m).
    - Cables are susceptible to Electromagnetic Interference (EMI).

1000BASE-TX "Gigabit Ethernet"

1000BASE -T is commonly known as Gigabit Ethernet. Gigabit Ethernet is a LAN architecture.

Advantages of 1000BASE-T:

- The 1000BASE-T architecture supports data transfer rates of 1 Gbps. At 1 Gbps, it is ten times faster than Fast Ethernet, and 100 times faster than Ethernet. This increased speed makes it possible to implement bandwidth-intensive applications, such as live video.
- The 1000BASE-T architecture has interoperability with 10BASE-T and 100BASE-TX.

Disadvantages of 1000BASE-T:

- The maximum length for a 1000BASE-T segment is only 328 ft (100 m).
- It is susceptible to interference.
- Gigabit NICs and switches are expensive.
- Additional equipment is required.

Wireless Ethernet standards

IEEE 802.11 is the standard that specifies connectivity for wireless networks.

IEEE 802.11, or Wi-Fi (wireless fidelity), refers to the collective group of standards, 802.11 (the original specification), 802.11b, 802.11a, 802.11g, and 802.11n. These

protocols specify the frequencies, speeds, and other capabilities of the different Wi-Fi standards.

- **802.11a** - Devices conforming to the 802.11a standard allow WLANs to achieve data rates as high as 54 Mbps. IEEE 802.11a devices operate in the 5 GHz radio frequency range and within a maximum range of 150 feet (45.7 m).
- **802.11b** operates in the 2.4 GHz frequency range with a maximum theoretical data rate of 11 Mbps. These devices operate within a maximum range of 300 feet (91 m).
- **802.11g** provides the same theoretical maximum speed as 802.11a, which is 54 Mbps, but operates in the same 2.4 GHz spectrum as 802.11b. Unlike 802.11a, 802.11g is backward-compatible with 802.11b. 802.11g also has a maximum range of 300 feet (91 m).
- **802.11n** is a newer wireless standard that has a theoretical bandwidth of 540 Mbps and operates in either the 2.4 GHz or 5 GHz frequency range with a maximum range of 984 feet (250 m).

CHAPTER 9
Computer Network Security

What is Network Security?

All the measures used to safeguard a computer network's integrity and the data on it are collectively referred to as network security. Network security is crucial because it protects sensitive data from online threats and guarantees the network's dependability. Multiple security measures are used in successful network security plans to shield users and organizations from malware and online threats like distributed denial of service.

Aspects of Network Security

- **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and

more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.

- **End-point authentication:** Authentication means that the receiver is sure of the sender?s identity, i.e., no imposter has sent the message.
- **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

How is Network Security Implemented?

1. Secret Key Cryptography

The sender and the receiver share one secret key. The data is encrypted at the sender's end using this secret key. Data is encrypted before being transferred to the recipient via a public network. The recipient may readily decipher the encrypted data packets because they are both aware of and possess the Secret Key.

The Data Encryption Standard (DES) is an illustration of secret key encryption. It is challenging to administer Secret Key encryption since each computer on the network needs a unique key.

2. Public Key Cryptography

Each user in this encryption scheme has a unique Secret Key that is not kept in the common domain. The secret key is kept from the public. Every user has a unique but public key in addition to a secret key. Senders encrypt the data using a public key that is always made available to the public. Using the user's personal Secret Key, he can quickly decode the encrypted data once he receives it. Rivest-Shamir-Adleman (RSA), a kind of public key encryption, is an illustration.

3. Message Digest

In this approach, a hash value is computed and delivered in place of actual data. The second end user generates its hash value and contrasts it with the most recent one. It is approved if both hash values match; otherwise, it is refused.

Message Digest example using MD5 hashing.

Tools and Software for Network Security

1. Firewalls

Web pages, pop-ups, and other service entry and departure decisions are made by firewalls, which are guardian services or devices. Depending on the needs, these firewalls utilize a preset set of rules to help block or allow traffic. Depending on the requirements of the system, firewalls might be either software- or hardware-based, or both.

2. Access Control

Access control enables businesses to stop unauthorized people and devices from connecting to a specific network and to stop prospective attackers from accessing sensitive data. This limits network access to users who are authorized to utilize the specified resources.

3. Virtual Private Networks (VPN)

In most cases, a VPN encrypts the communication between an endpoint device and a network via the internet. Additionally, VPN enables experts to verify the connection between the network and the device. As a consequence, an online tunnel that is encrypted and safe is created.

4. Intrusion Prevention Systems

Intrusion prevention systems scan network traffic to identify and stop assaults. This is accomplished by connecting network activity with databases of attack methods that experts are familiar with.

5. Wireless Security

In comparison to wireless networks, wired networks could be more secure. It would help if you had control over the computers and people who may access the network of your business. It would help if you had wireless security, especially in light of the fact that fraudsters are increasingly extorting people for their private information.

Best Tools for Network Security

1. Wireshark
2. Nessus
3. Snort
4. Netcat

5. Metasploit
6. Aircrack

Attack Types in Network Security

1. Virus

It is a malicious file that may be downloaded, and after a user has opened it, it begins to overwrite the computer's code with a new set of codes. The system files on the computer will become corrupt as the infection spreads, which may cause the files on other computer systems in the network to become corrupt as well.

2. Malware

It is one of the swiftest, most severe, and worst attack methods that aid in gaining unauthorized access to a system or network of systems.

Objectives of network security

Confidentiality: Covering two related concepts:

— Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals (encryption)

—Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity: Also covers two related concepts:

—Data integrity: Assures that information and programs are changed only in a specified and authorized manner

—System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability: Assures that systems work promptly and service is not denied to authorized users

Authenticity:

- The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability:

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Network troubleshooting

Troubleshooting Process

Step 1 Identify the problem

- **Hardware/Software information**
  - Manufacturer, model, OS, network environment, connection type
- **Open-ended questions**
  - When did the problem start?
  - What problems are you experiencing?
  - Is there anything else you can tell me about the problem?
  - What other users are having problems?
  - Can you describe your network configuration?
- **Closed-ended questions**
  - Has any network equipment changed?
  - Have any peripherals been added to your computer?
  - Have any other computers been added to the network?
  - Have you rebooted your computer?

Step 2 Establish a theory of probable causes

- Problem may be simpler than the customer thinks.
- Create a list of the most common reasons why the error would occur:
  - Incorrect IP information
  - Examine the network equipment LEDs
  - Incorrect wireless configuration
  - Disable network connection
  - Verify the wireless router configuration
  - Verify the network equipment settings

Step 3 Determine an exact cause

- Testing your theories of probable causes one at a time, starting with the quickest and easiest.
    - Restart the network equipment.
    - Examine the network equipment LEDs.
    - Renew the IP address.
    - Reconnect all of the network cables.
    - Verify the wireless router configuration.
    - Ping the local host.
    - Ping the default gateway.
    - Ping an external website.
    - Verify the network equipment settings.
- If the exact cause of the problem has not been determined after you have tested all your theories, establish a new theory of probable causes and test it.

Step 4 Implement a solution

- Sometimes quick procedures can determine the exact cause of the problem or even correct the problem.
- If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.
- Divide larger problems into smaller problems that can be analyzed and solved individually.

Step 5 Verify solution and full system functionality

- Verifying full system functionality and implementing any preventive measures if needed. Ensures that you have not created another problem while repairing the computer.
    - Reboot all of the network equipment.
    - Reboot any computer that experienced network problems.
    - Validate all LEDs on the network equipment.
    - Use the **ipconfig/all** command to display IP addressing information for all network adapters.

- Use the **ping** command to check network connectivity to an external website.
- Use the **nslookup** command to query your DNS server.

Step 6 Document findings

Document the process

- Problem description
- Solution
- Components used
- Amount of time spent in solving the problem

CHAPTER 10

COMMUNICATION SOFTWARE

Communication is defined as the process of transferring information involving at least one sender, a message, and a recipient from an individual or a group to another. An application or program that is created to pass information from one system to another digitally is known as "communication software."

Types Of Communications Software

- ***Web conferencing*.** This involves text, audio, and video exchange capabilities and is used for several purposes such as video presentations, employee training, conference calls
- ***Live chat*.** This is a standalone app that can be embedded within digital channels such as a website, social media page, newsletter, and custom app
- Email Software
- Phones & VoIP
- Collaboration & Productivity Software

Network software

- is a broad term referring to a range of software applications designed to enhance the functioning, management, and optimization of a computer network. This software facilitates communication among various interconnected devices, manages network operation, and monitors network performance.

How to choose networking software

1. Assess organizational requirements

Before selecting networking software, it's important to thoroughly understand your organization's specific needs. Consider factors like network size, user count, types of devices connected, and specific industry requirements. For instance, a healthcare organization might prioritize security features to comply with HIPAA regulations, while a tech company may focus on scalability and performance.

2. Evaluate security features

Given the critical importance of cybersecurity, assess the security features of the networking software. Look for capabilities like intrusion detection, zero-trust architecture, and encrypted communications. It's essential for the software to not only protect against current threats but also be adaptable to future security challenges.

3. Consider scalability and flexibility

Choose networking software that can grow and adapt with your organization. Scalability ensures that the software can handle an increasing number of users and devices, while flexibility allows for adjustments in response to changing organizational needs. This is particularly important for organizations with plans for expansion or those undergoing rapid growth.

4. Review ease of use and support

The user-friendliness of the software and the quality of customer support are crucial. Software that is intuitive and easy to manage can significantly reduce the learning curve and operational burden on IT staff. Additionally, reliable customer support ensures prompt assistance when issues arise, minimizing potential downtime.

5. Analyze cost-effectiveness

Finally, consider the total cost of ownership, which includes not only the initial purchase price but also ongoing maintenance and support costs. A cost-effective solution provides the necessary features and performance while staying within budget constraints. It's important to balance cost with functionality to ensure long-term value.

The types of network software

Network operating systems (NOS)

Network Operating Systems form the backbone of network management, allowing control over resources and facilitating essential services. Large enterprises extensively use NOS for the centralized management of complex networks, streamlining administrative tasks and enhancing efficiency.

Asset management software

Asset management software, on the other hand, is designed to track and manage assets within an organization. This encompasses physical assets like equipment, hardware, and real estate, as well as intangible assets like software licenses and intellectual property.

Network monitoring tools

Crucial for real-time oversight, network monitoring tools provide insights into traffic flow, network utilization, and potential issues. They enable organizations to proactively manage network performance, making them indispensable in maintaining optimal network health.

Network security software

This category encompasses firewalls, anti-malware tools, and intrusion detection systems, vital for protecting networks against cyber threats. In an era of increasing digital risks, network security software is a must-have for organizations to safeguard their data and network integrity.

Data archiving software

Data archiving software plays a crucial role in efficiently storing, securing, and managing digital data over extended periods. These tools ensure that data remains accessible and intact for future reference, compliance, or recovery needs.

Network configuration and change management (NCCM)

NCCM tools are essential for managing network configurations and tracking changes. They ensure compliance and reduce risks associated with network modifications, particularly critical for organizations with evolving and extensive network landscapes.

Network virtualization software

This software allows the creation of virtual network resources, enhancing resource utilization and network management efficiency. It's especially beneficial for large organizations with intricate network needs, providing flexibility and improved resource management. Network virtualization software supports rapid network configuration and deployment, reducing the time and effort required for network setup and changes. By abstracting the physical hardware, it allows for easier replication and scaling of network environments, which is invaluable in testing and development scenarios as well as in disaster recovery planning.

CHAPTER 11

INTERNET AND EMAIL

Introduction to the Internet

It is a large no. of connected computers (or a large set of computer networks) linked together that communicate with each other, over telephone lines.
It is a worldwide computer network connecting thousands of computer networks, through a mixture of private & public data using the telephone lines.
It is a worldwide (global or an international) network of computers that provide a variety of resources and data to the people that use it.
Internet refers to a global inter-connection of computers and computer networks to facilitate global information transfer. It is an interconnection of computers throughout the world, using ordinary telecommunication lines and modems.

Functions of the Internet

- Communication
- Information retrieval
- Easy-to-use offerings of information and products

Internet Services

The following are some of the services offered by Internet:
(i). Electronic mail (e-mail).
(ii). Fax services.
(iii). Conference services.
(iv). Online chatting.
(v). Downloading of programs.
(vi). Online shopping.
(vii). File transfer.

(viii). Entertainment (Games, Music and Movies).
(ix). Free information retrieval (e.g., Educational information).
(x). Formation of Discussion groups, e.g. Usenet Newsgroups.
(xi). Video Conferencing.
(xii). Access & Use of other computers

Browsing the Web

This is also known as Navigating or 'Surfing' the Web.
To Browse is to navigate the Internet or the contents of your computer. Browsing can also be defined as moving around and between Web pages.
Using a Web browsing software you can read documents, listen to music, watch videos, make purchases, participate in surveys, advertise products, do research, share interests and download files on the Web.

EXPLORING / BROWSING THE INTERNET.

Use the Internet Explorer on your Windows desktop to browse the Web.
There are several ways in which you can browse the Web pages or "surf the net".
(a). When viewing a Web page, you can navigate the Internet by clicking Links, Underlined text or special features that cause you to jump to another Web page.
(b)You can also use the Standard toolbar buttons in the Internet Explorer to move between Web pages, or to search the Internet.

History.

Internet Explorer remembers the Websites and Web pages that you have visited. It keeps record of each Web page as it is downloaded. This is the History feature. You can therefore, easily return to the page you have visited. To redisplay the page you have just left, click on the Back button. To move to the next page (available only if you have moved back), click the Forward button.

Web Hosting.

A World Wide Web Server is a computer with programs that answer requests for documents from Clients (browsers) over the Internet. Files containing Web sites are placed on these servers. A Host computer is any computer connected to the Internet and stores information that has been made available to the Web.

Web Address (Uniform Resource Locator – URL). An Address is the location of a file.

Finding Web pages (information) on the Web.

There are 3 ways you can use to find interesting and useful Web pages on the Web;
1). You could get the Web address from an advertisement. Many businesses include their Web addresses in their Television and Print advertisements.
2). You click a link that will enable you jump from one page to another. Many industries or organizations, magazines and topic experts maintain pages that provide links from page to page.
3). Use of Search Engines - software that helps in locating information in the Web

Electronic Mail (E-Mail).

Electronic mail (also known as e-mail) is one of the common services provided by the Internet.

E-Mail is a worldwide system for sending & receiving electronic messages from one computer to another.

E-Mail (Electronic mail) refers to electronic messages sent over the Internet or a network. Email can contain both text & files.

Components required.

For one to be able to communicate using e-mail, the following components are needed:

1). A Computer - where you will send or receive the e-mail messages.

2). An E-mail program. Your computer must be installed with an e-mail program that lets you send, receive and manage your e-mail messages. Examples of E-mail programs; • Microsoft Outlook, Outlook Express, & Microsoft Exchange from Microsoft. • Communicator from Netscape. • Lotus Notes. • Eudora.

3). E-mail address of the sender & the address of the receiver.

4). An Internet Service Provider (ISP) - company who will deliver your message to the receiver