THE NEW COLLEGE (AUTONOMOUS), CHENNAI-14.

DEPARTMENT OF COMPUTER APPLICATIONS – SHIFT - II

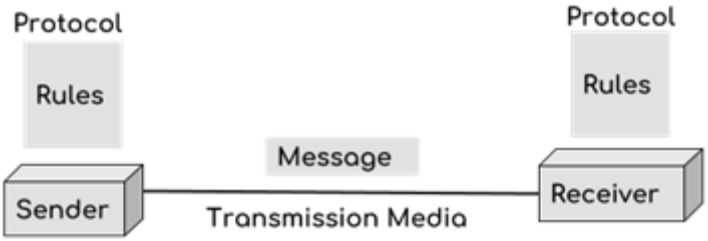
STUDY MATERIAL

SUBJECT: NETWORKING TECHNOLOGIES (20BHM513) Class: III BCA B

UNIT-I

1. INTRODUCTION

A computer network is **a group of devices connected with each other through a transmission medium such as wires, cables etc**. These devices can be computers, printers, scanners, Fax machines etc. The purpose of having computer network is to send and receive data stored in other devices over the network. These devices are often referred as nodes.



There are **five basic components** of a computer network

Message: It is the data or information which needs to be transferred from one device to another device over a computer network.

Sender: Sender is the device that has the data and needs to send the data to other device connected to the network.

Receiver: A receiver is the device which is expecting the data from other device on the network.

Transmission media: In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.

Protocol: A protocol is a set of rules for Communication that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol.

For example, http and https are the two protocols used by web browsers to **get** and **post** the **data to internet**; similarly **SMTP** protocol is used by **email services** connected to the internet.

2. APPLICATIONS OF COMPUTER NETWORKS

Following are some business applications of computer networks:

1. Resource Sharing:

The goal is to make all programs, equipments (like printers etc), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

2. Server-Client model:

One can imagine a company's information system as consisting of one or more databases and some employees who need to access it remotely. In this model, **the data is stored on powerful computers** called **Servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have **simple machines**, called **Clients**, on their desks, using which they access remote data.

3. Communication Medium:

A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication

4. e-Commerce:

A goal that is starting to become more important in businesses is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future.

5. Highly Reliable Systems − Computer networks allow systems to be distributed in nature, by the virtue of which **data is stored in multiple sources**. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.

6. Cost–Effective Systems − Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive **mainframes for computation and storage**. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.

7. VoIP − VoIP or **Voice over Internet protocol** has revolutionized **telecommunication systems.** Through this, **telephone calls are made digitally using Internet Protocols** instead of the regular analog phone lines.

3. LINE CONFIGURATION

Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A Link is the physical communication pathway that transfers data from one device to another.

For communication to occur, two devices must be connected in same way to the same link at the same time. There are two possible line configurations.

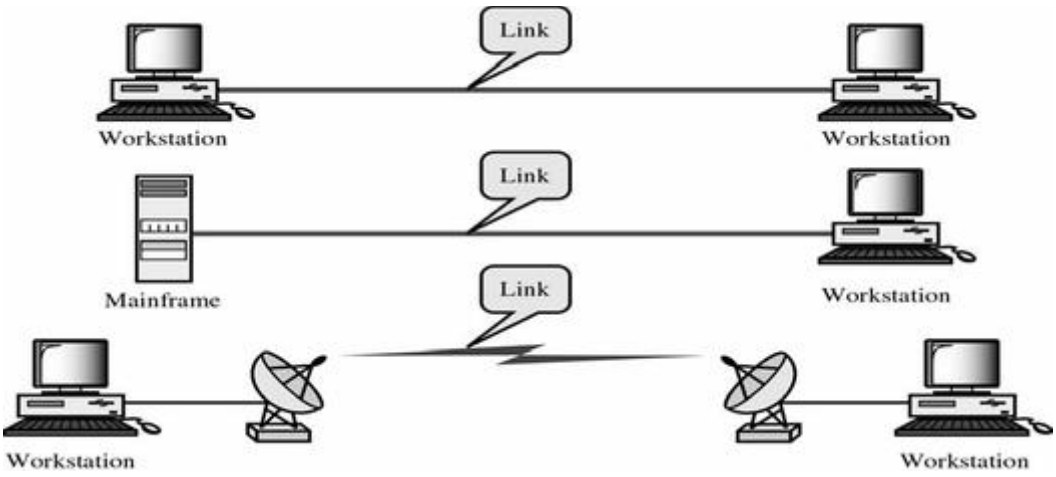
1. **Point-to-Point.**
2. **Multipoint.**

1. Point-to-Point

A **Point to Point Line Configuration** Provide dedicated link between two devices use actual length of wire or cable to connect the two end including microwave & satellite link. **Infrared remote control** & **TVs remote control**.

The entire capacity of the channel is reserved for transmission between those two devices. Most point-to-point line configurations use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

Point to point network is considered to be one of the easiest and most conventional network topologies. It is also the simplest to establish and understand. To visualize, one can consider point to point network topology as two phones connected end to end for a two way communication

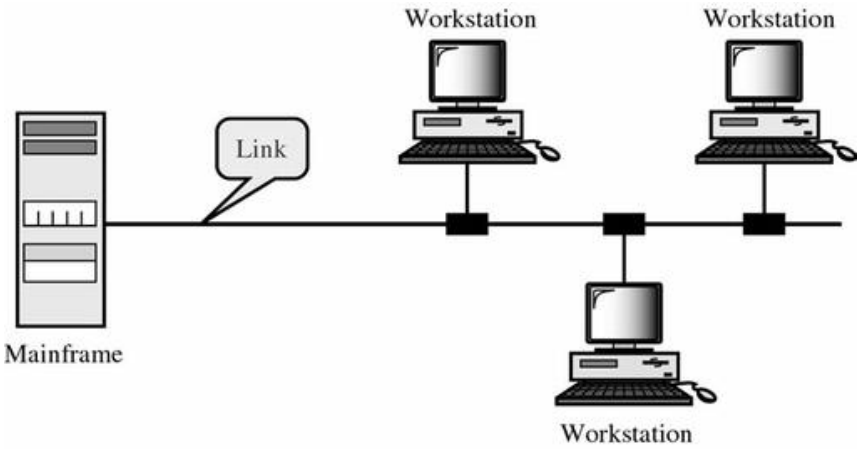


2. Multipoint Configuration

Multipoint Configuration also known as **Multidrop line configuration** one or more than two specific devices share a single link capacity of the channel is shared. More than two devices share the Link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line Configuration:

- **Spatial Sharing**: If several devices can share the link simultaneously, it's called Spatially shared line configuration

- **Temporal (Time) Sharing**: If users must take turns using the link , then it's called Temporally shared or Time Shared Line Configuration



4. TOPOLOGY

The term "**Topology**" refers to the way in which the end points or stations/computer systems, attached to the networks, are interconnected. We have seen that a topology is essentially a stable geometric arrangement of computers in a network. If you want to select a topology for doing networking. You have attention to the following points.

- Application S/W and protocols.
- Types of data communicating devices.
- Geographic scope of the network.
- Cost.
- Reliability.

Depending on the requirement there are **different Topologies** to construct a network.

(1) Mesh topology.

(2) Star topology.

(3) Tree (Hierarchical) topology.

(4) Bus topology.

(5) Ring topology.

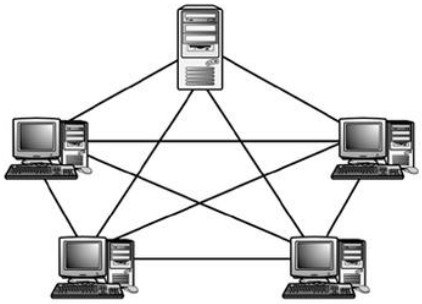
(6) Cellular topology.

- Ring and mesh topologies are felt convenient for peer to peer transmission.
- Star and tree are more convenient for client server.
- Bus topology is equally convenient for either of them.

1. Mesh Topology

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by **Reed's Law**.

The number of connections in a full mesh = n(n - 1) / 2

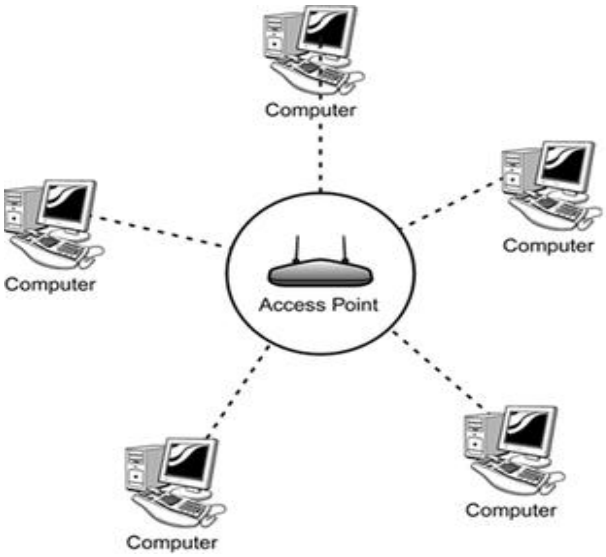


2. Star Topology

In a star topology, cables run from every computer to a centrally located device called a HUB. Star topology networks require a central point of connection between media segment. These central points are referred to as Hubs.

Hubs are special repeaters that overcome the electromechanical limitations of a media. Each computer on a star network communicates with a central hub that resends the message either to all the computers. (In a broadcast network) or only the destination computer. (In a switched network).

Ethernet 10 base T is a popular network based on the star topology.



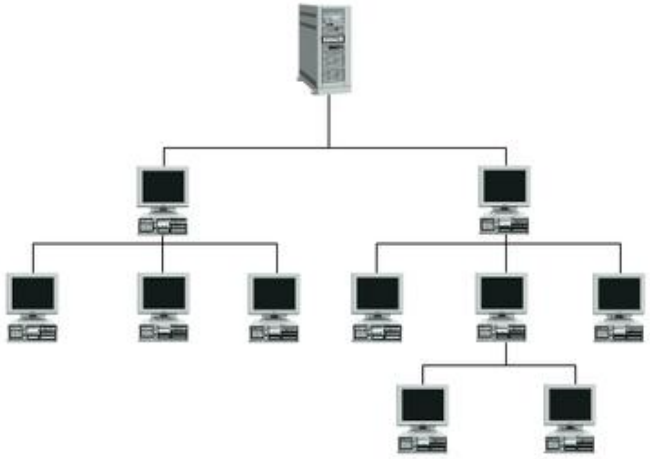
3. Tree (Hierarchical) topology

It is similar to the star network, but the nodes are connected to the secondary hub that in turn is connected to the central hub. The central hub is the active hub.

The active hub contains the repeater, which regenerates the bits pattern it receives before sending them out.

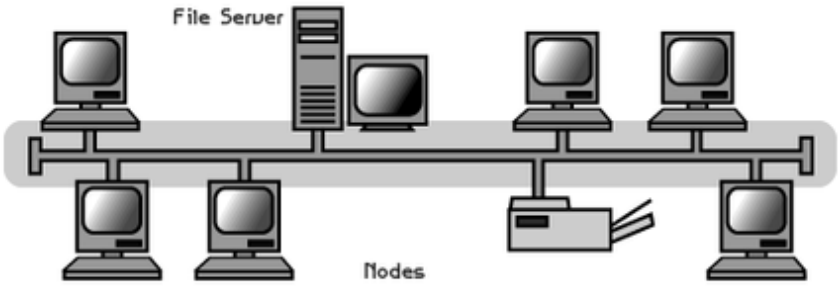
The secondary hub can be either active or passive.

A passive hub provides a simple physical connection between the attached devices.



4. Bus topology

A bus topology connects computers along a single or more cable to connect linearly. A network that uses a bus topology is referred to as a "bus network" which was the original form of Ethernet networks. Ethernet 10Base2 (also known as thinnet) is used for bus topology.



5. Ring topology

In ring topology, each device has a dedicated point-to-point line configuration only with two devices on either side of it.

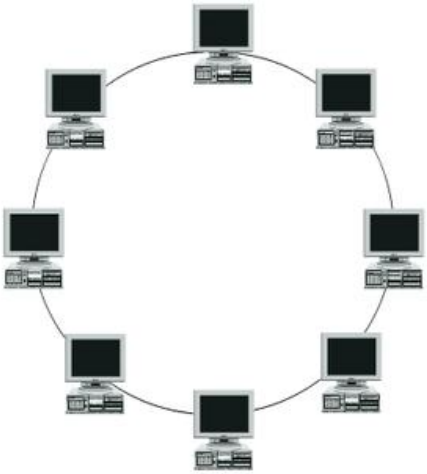
A signal is passed along the ring in one direction, from device to device until it reaches its destination.

Each device in the ring has a repeater. When the devices receive the signal intended for the other node, it just regenerates the bits and passes them along.

Ring network passes a token.

A token is a short message with the electronic address of the receiver.

Each network interface card is given a unique electronic address, which is used to identify the computer on the network.



6. Cellular topology

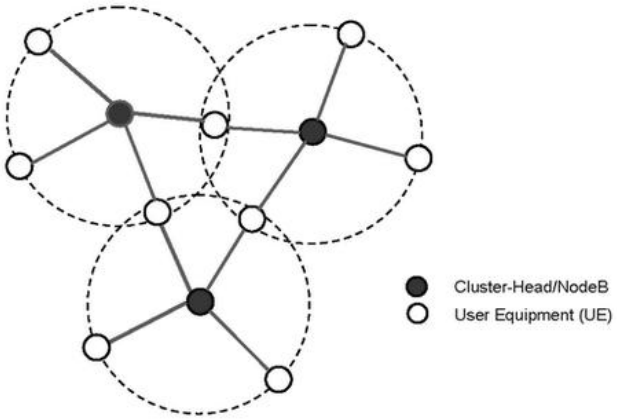
The cellular topology is applicable only in case of wireless media that does not require cable connection.

In wireless media, each point transmits in a certain geographical area called a cell.

Each cell represents a portion of the total network area.

Devices that are in the cell communicate through a central hub. Hubs in different cells are interconnected. They route data across the network and provide a complete network infrastructure.

The data is transmitted in the cellular digital packet data (CDPD) format.



5. TRANSMISSION MODE

A given transmission on a communications channel between two machines can occur in several different ways. The transmission is characterized by:

- the direction of the exchanges
- the transmission mode: the number of bits sent simultaneously
- synchronization between the transmitter and receiver

Types of Transmission mode

- Simplex
- Half Duplex
- Full Duplex

Simplex

A simplex connection is a connection in which the data flows in only one direction, from the transmitter to the receiver. This type of connection is useful if the data do not need to flow in both directions (for example, from your computer to the printer or from the mouse to your computer...).

Half Duplex

A half-duplex connection (sometimes called an *alternating connection* or *semi-duplex*) is a connection in which the data flows in one direction or the other, but not both at the same time. With this type of connection, each end of the connection transmits in turn. This type of connection makes it possible to have bidirectional communications using the full capacity of the line.

Full Duplex

A full-duplex connection is a connection in which the data flow in both directions simultaneously. Each end of the line can thus transmit and receive at the same time, which means that the bandwidth is divided in two for each direction of data transmission if the same transmission medium is used for both directions of transmission.

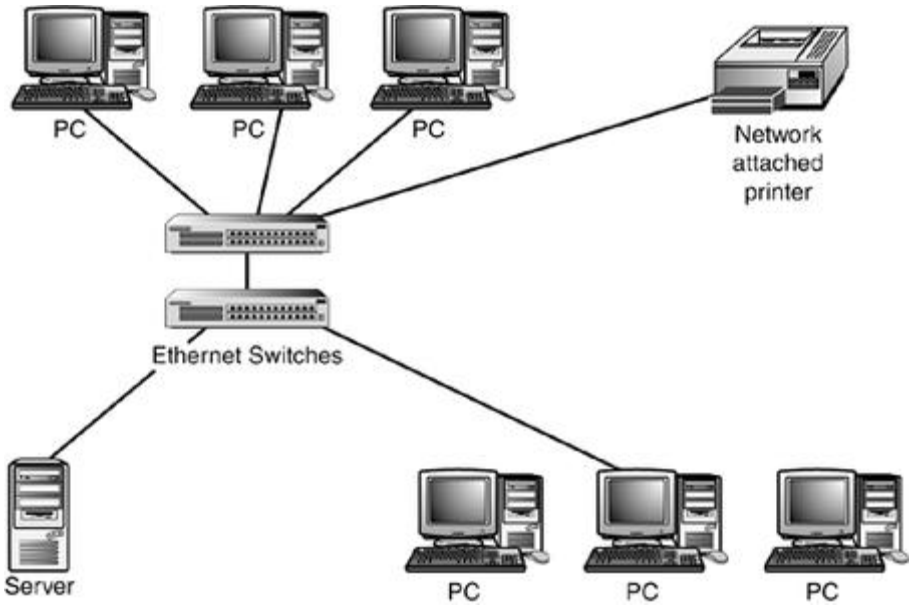
6. CATEGORIES OF NETWORK

One way to categorize the different types of computer network designs is by their scope or scale. For historical reasons, the networking industry refers to nearly every type of design as some kind of *area network*. Common examples of area network types are:

- LAN - Local Area Network
- WLAN - Wireless Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network

1. Local Area Network

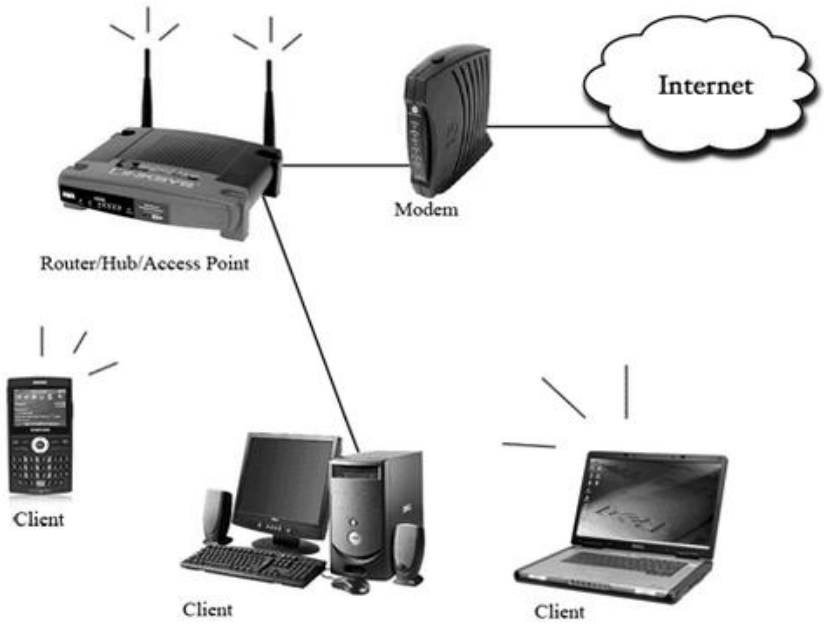
A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet. In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.



2. Wireless Local Area Network

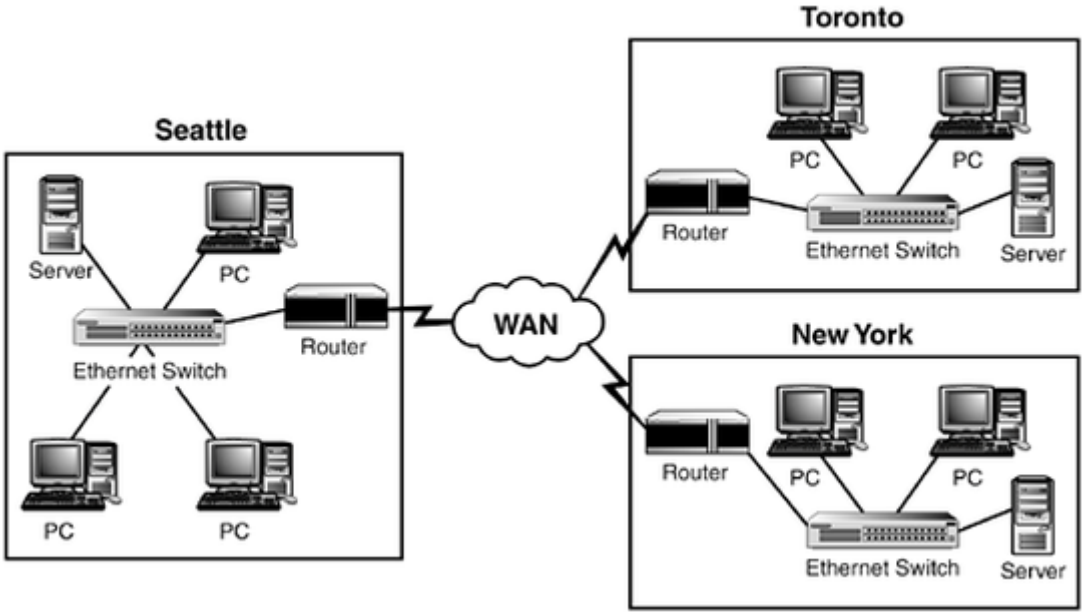
As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.



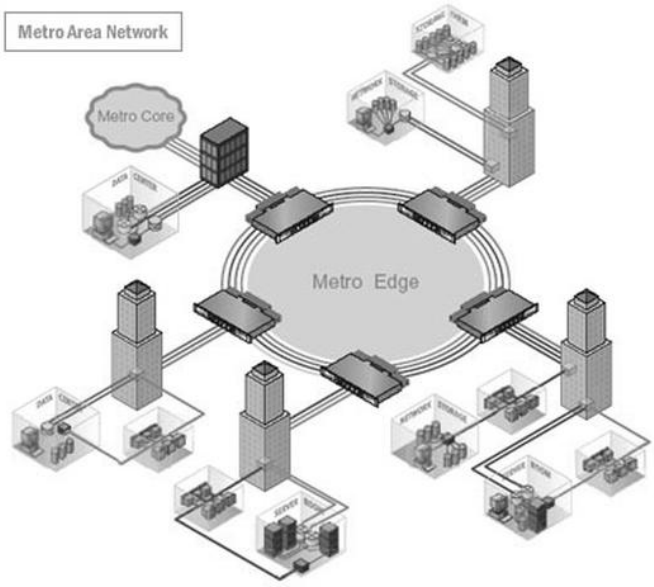
3. Wide Area Network

A WAN is a network that spans more than one geographical location often connecting separated LANs. WANs are slower than LANs and often require additional and costly hardware such as routers, dedicated leased lines, and complicated implementation procedures.



4. Metropolitan Area Network

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



7. OSI LAYERS

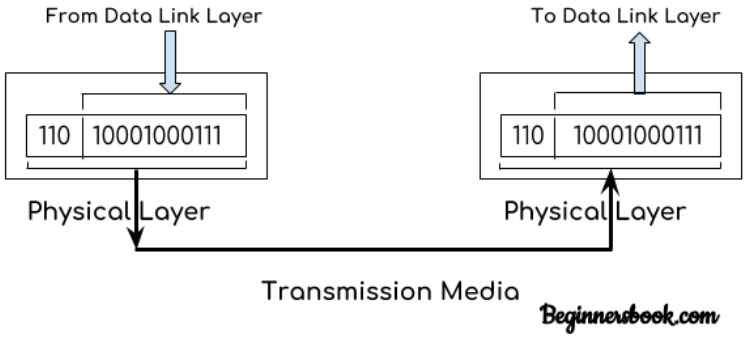
OSI Model stands for **Open System interconnection** model. **OSI Model** defines how data is transferred from one computer to another computer. In a very basic scenario two computers connected with a LAN and connectors transfer data using the NIC. This forms a computer network, however if both the system uses different operating systems.

For example one system runs on windows and other one runs on MacOS then how can data be transferred between these two different systems, here comes the role of an OSI model which is a seven layered model that defines how a data can be transferred between different systems.

OSI model was introduced by International Organisation for Standardisation (ISO) in 1984. There are **seven layers** in an OSI model

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

Physical Layer



We now learned that a transport layer converts the data into segments, network layer converts the segments into packets and data link layer converts the packets into frames. A frame is nothing but a sequence of bits such as 1001011.

Physical layer converts these binary sequences into signals and transfer it through a transmission media such as cables etc.

The signals generated by physical layer is based on the transmission media. For example an electrical signal is generated if the media is copper cable, light signal if media is optical fibre and radio signal in case of transmission media is air. This generated signal is received by the physical layer at the receiver side and converts it into bits.

Main functions of Physical Layer:

Digital Transmission:

One of the main functions of physical layer is to transfer data in form of signals. In this guide, we will learn about digital transmission. A data can be either analog or digital. To transfer the data over a transmission media such as wire, cable etc. physical layer must need to convert the data to its digital signal.

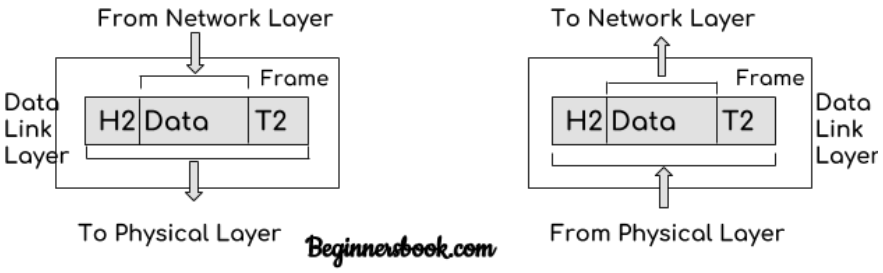
Digital data to Digital signal conversion:

In this section we will learn how physical layer converts digital data to digital signal. It uses two techniques to do this conversion: Line coding and block coding.

Line coding:

A digital data is in form of binary sequence such as 1000111 (combination of 0s and 1s). Line coding uses three schemes to represent these binary sequences in form of signals that can be transferred.

Data Link Layer



Data link layer receives the data from network layer.

There are two types of addressing done to the packets transfers from one computer to another computer.

Logical addressing: Logical addressing is assigning sender and receiver IP addresses to data packets. This is done at the network layer.

Physical addressing: Physical addressing is done at data link layer where MAC addresses of sender and receiver are assigned to each data packets.

Data unit in the data link layer is called frame. A frame is transferred from one computer to another computer and transmission is done through a transmission media such as wire, cable etc. Both sender and receiver computer has NIC that helps in sending and receiving frame. These NICs presents at sender and receiver provides a physical link between sender and receiver.

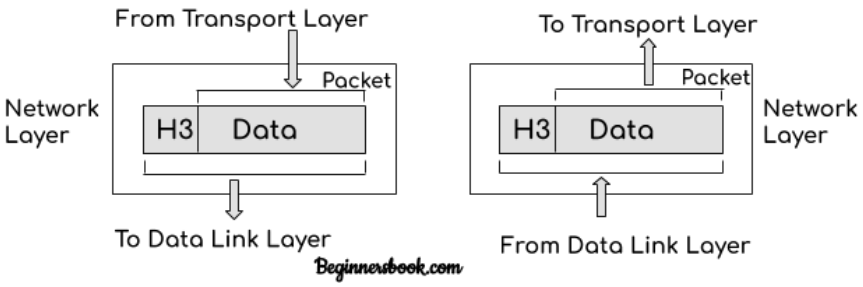
Main functions of data link layer:

Access the Media: Allows upper layers of OSI model to use the media using a technique called framing.

Media Access control: How data is placed and received from the media.

Error Detection: Tail of the each frame transferred contains certain bits to check whether the data received on the side is corrupted or not.

Network layer



The main purpose of network layer is to receive the data segments from transport layer and transfer them from one computer to another computer on different network.

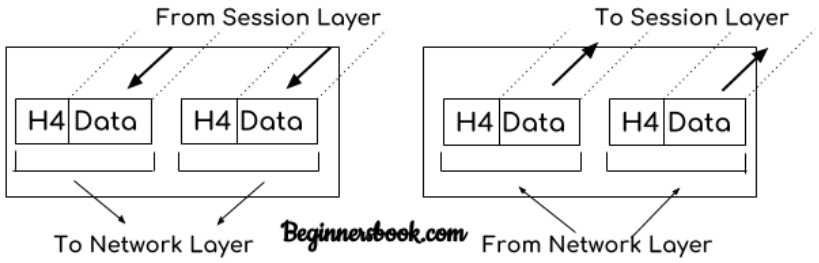
The main functions of network layer:

Logical Addressing: Every computer on a network has a unique IP address. Network layer assigns the sender and receiver IP address to the data packets before transmitting them so that the data packet reach the correct destination.

Routing: It is a method of transferring data packets from source to destination. It uses the combination of Mask and IP address to transfer the data to correct destination. Each data packets contains three addition components mask, sender IP, receiver IP. The Mask determines the computer network to which the data needs to be delivered and then the IP address determines which computer on that particular network needs to receive the data packet.

Path determination: A computer can be connected to another computer in number of ways. Network layer determines the optimal path for data transmission so that the data can be transmitted faster to the receiver. OSPF, BGP, IS-IS protocols are used to determine best possible path for data delivery.

Transport layer



The main role of transport layer is to check the reliability of data communication.

The main functions of transport layer are:

Segmentation: Data received from session layer is divided into small data units called segments. Each segment contains the sender and receiver port number along with the sequence number. Port number helps to direct the data segments to the correct application and the sequence number helps to reassemble the data from data segments in correct order.

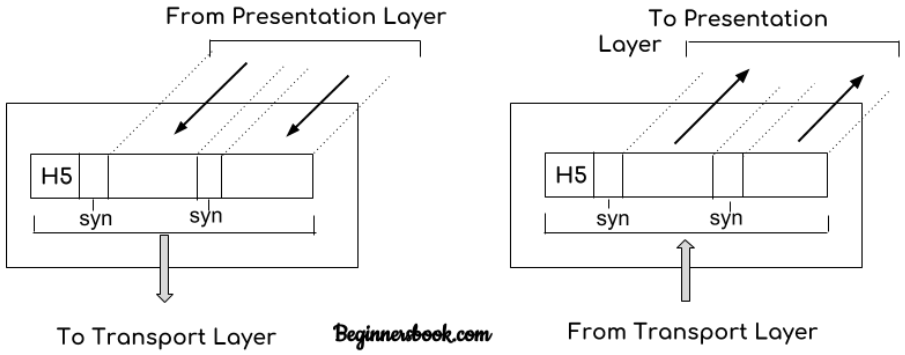
Flow control: It controls the flow of data. It checks the capability of the receiver device receiving capability before transmitting data. For example a sender server can send the data at a rate of 200Mbps but a receiving data can only receive data at a rate of 10 Mbps then it controls the flow of data to 10Mbps so that the data doesn't get lost during transmission.

Error control: Transport layer also performs error control using Automatic Repeat Request, if a data is lost during transmission, it is send again using automatic repeat request. Transport layer also adds a group of bits called checksum with each segment to check whether the data received at receiver side is not corrupt.

Connection oriented transmission: Connection oriented transmission is done using transmission control protocol (TCP). TCP is considerably slower than UDP because it provides the feedback that the data is received or not, thus a data can be sent again if it is not received.

Connectionless transmission: Connectionless transmission is done using User Datagram protocol (UDP). UDP is faster than TCP because it doesn't provide the feedback that the data is actually received at the receiver side or not.

Session Layer



The main role of session layer is to setup and maintain the connection between different systems.

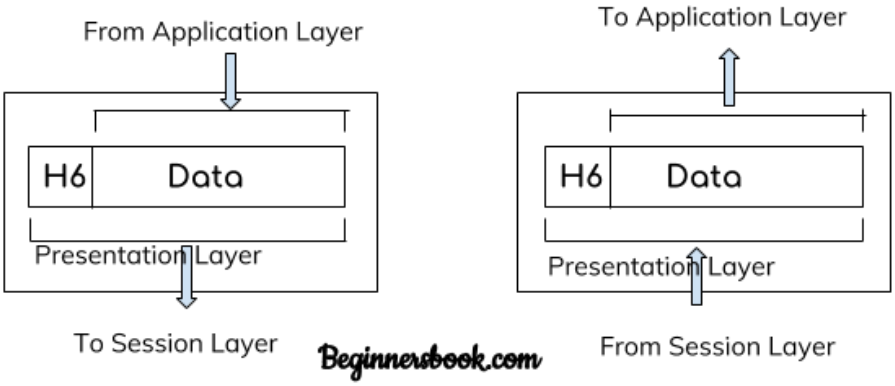
Main functions of session layer:

Authentication: Before a computer can be connected to a server, the computer has to provide user name and password for the authentication. The function of authentication and setting up a connection after authentication is performed by session layer.

Authorization: Once a connection is established, session layer checks whether the connected computer is authorised to access the data, this function of authorisation checking is also performed by session layer.

Session management: Session layer also checks that the data which is received from the server in form of data packets belongs to which application for example when you access Facebook profile through your browser, the data transferred from the Facebook server is transferred to your web browser application, thus the session layer helps in session management.

Presentation Layer



Presentation layer receives the data from top most layer which is application layer.

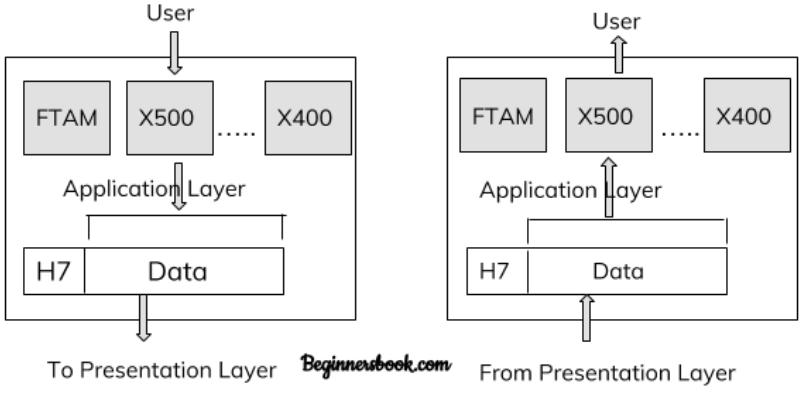
Functions of Presentation layer:

Translation: The data received from application layer is in form of characters and numbers such as 1234, ERFF etc. The presentation layer converts these characters and numbers into machine understandable format which is known as binary format for example 100111101.

Encryption: To protect the sensitivity of data, presentation layer encrypts the data at the sender side before the transmission and the receiver side this data is decrypted by the presentation layer at the receiver side. Secure sockets layer protocol (SSL) is used by the presentation layer for encryption and decryption.

Compression: Compress the data to small size so that it can be transferred faster over a network. This compression can be lossy or lossless compression.

Application layer



Application layer is used by computer applications such as google chrome, outlook, FireFox, Skype etc. Application layer defines the protocols that are used by computer applications

For example

HTTP and HTTPS protocols are used by web browsers such as google chrome, FireFox, Safari etc.

FTP protocol is used for file transfer between two or more computers.

SMTP protocol is used for emails

Telnet is used for virtual terminals.

There are dozens of other protocol that forms the application layer, such as NFS, FMTP, DHCP, SNMP, POP3, IRC, NNTP etc.

In short you can say that application layer provides the services to computer applications with the help of protocols that are defined in it.

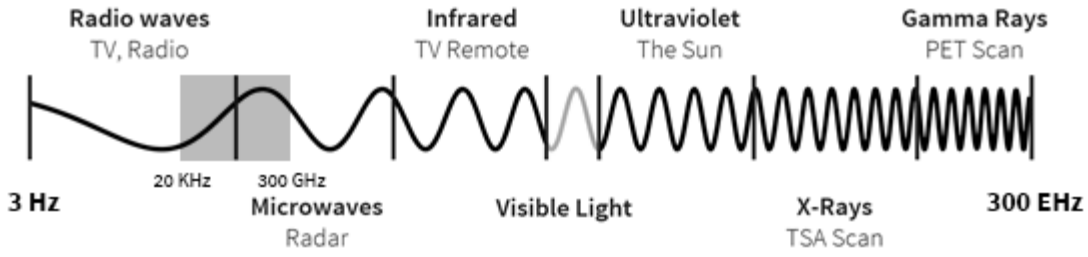
8. SPECTRUM

Spectrum refers to the invisible radio frequencies that wireless signals travel over. Those signals are what enable us to make calls from our mobile devices, tag our friends on Instagram, call an Uber, pull up directions to a destination, and do everything on our mobile devices.

The frequencies we use for wireless are only a portion of what is called the electromagnetic spectrum.

The entire electromagnetic spectrum encompasses other frequencies we interact with daily, even if we don't think about them. You may remember ROYGBIV from elementary school. That's the acronym for the colors that make up the visible part of spectrum—the spectrum we see. Other parts of spectrum carry broadcast radio and television or serve other everyday functions.

Portions of electromagnetic spectrum are grouped in "bands" depending on their wavelengths—the distance over which the wave's shape repeats. The full electromagnetic spectrum ranges from three Hz (extremely low frequency) to 300 EHz (gamma rays). The portion used for wireless communication sits within that space and ranges from about 20 KHz to 300 GHz.



Spectrum wavelengths are classified into different bands within the electromagnetic spectrum range.

When we talk about radio spectrum, we are talking about the range of radio frequencies that are used for communicating. Think of your radio dial. As you go up and down the dial, you locate the radio stations operating on particular frequencies. Now just imagine that radio dial expanding much, much further in both directions—that's where you would encounter frequencies assigned to other uses, whether it's mobile phones, or satellite TV, or air traffic control, or police radios. Spectrum is the entire range of frequencies.

How Does Spectrum Work?

Because a range of spectrum frequencies can be used for cellular communications, different bands have slightly different characteristics. For the purposes of wireless communication, we can think of spectrum in three categories: low-, mid-, and high-band spectrum.

You might have read that we need more of all three for robust 5G networks. That's because each band of spectrum is essential for a different kind of communication and use case:

- Low-band spectrum (under 3 GHz) travels longer distances with minimal signal interruption. Today's wireless networks are built primarily on low-band spectrum, and the wireless industry has used this spectrum to build high-speed wireless networks that cover 99.7 percent of Americans.
- High-band spectrum (above 24 GHz) travels much shorter distances—think meters, not miles—compared to low-band spectrum, but offers high capacity and ultra-fast speeds.
- Mid-band spectrum (between 3 and 24 GHz) blends the characteristics of both low- and high-band spectrum—providing a mix of coverage and capacity.

These spectrum frequencies are transmitted between cell sites and our mobile devices. The most common cell sites in use today are the 150 foot cell towers we are accustomed to seeing along highways or atop tall buildings. But small cells—small scale antennas—are now being rapidly deployed to densify network coverage and provide more frequent connection points for 5G's mid- and high-band spectrum.

9. SIGNALS

In the fields of communications, signal processing, and in electrical engineering more generally, a **signal** is any time-varying or spatial-varying quantity.
In a communication system, a transmitter encodes a message into a signal, which is carried to a receiver by the communications channel.

For example, the words "Mary had a little lamb" might be the message spoken into a telephone. The telephone transmitter converts the sounds into an electrical voltage signal. The

signal is transmitted to the receiving telephone by wires; and at the receiver it is reconverted into sounds. Signals can be categorized in various ways. The most common distinction is between discrete and continuous spaces that the functions are defined over, for example discrete and continuous time domains. Discrete-time signals are often referred to as Time Series in other fields. Continuous-time signals are often referred to as continuous signals even when the signal functions are not continuous; an example is a square-wave signal.

10. ANALOG SIGNALS

An **analog** or **analogue signal** is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. It differs from a digital signal in terms of small fluctuations in the signal which are meaningful. Analog is usually thought of in an electrical context; however, mechanical, pneumatic, hydraulic, and other systems may also convey analog signals.

DIGITAL SIGNALS

A **digital signal** is a chemical signal that is a representation of a sequence of discrete values (a quantified discrete-time signal), for example of arbitrary bit stream, or of a digitized (sampled and analog-to-digital converted) analog signal. The term digital signal can refer to A continuous-time waveform signal used in any form of digital communication.

1. a pulse train signal that switches between a discrete number of voltage levels or levels of light intensity, also known as a a line coded signal, for example a signal found in digital electronics or in serial communications using digital baseband transmission in, or a pulse code modulation (PCM) representation of a digitized analog signal.

A signal that is generated by means of a digital modulation method (digital pass band transmission), produced by a modem, is in the first case considered as a digital signal, and in the second case as converted to an analog signal.

..... End of Unit –I .....