

UNIT-4

Introduction To Networks And LAN Components


4.1 Understand the Overview of Networking:

Human communication is a process that involves people communicating with each other. It has four components: the sender of the information, the receiver of the information, the language, and the medium through which communication is done.

A similar process is followed when there is communication between two computers.

Components of data communication:

- ✓ Sender
- ✓ Receiver
- ✓ Message
- ✓ Transmission media
- ✓ Protocols

 **Network:** "A network is a set of nodes connected by media links."

- A **node** can be a computer, printer, or any other device capable of sending and /or receiving data generated by other nodes on the network.
 - The link connecting the devices is often called communication channels. A **link** refers to a physical path that transfers data.
 - To be considered effective and efficient, a network must meet a number of criteria. The most important of these are performance, reliability and security.
1. **Performance:** can be measured in many ways, including transmit time, response time, number of users, type of transmission medium, the capabilities of the connected hardware and the efficiency of the software.
 2. **Network reliability:** is measured by frequency of failure, the time it takes to recover from a failure, and the network's robustness in a catastrophe.
 3. **Network security:** issues include protecting data from unauthorized access and viruses.

Computer Network:

"A computer network is an interconnected collection of autonomous computers."

- ✓ Two computers are said to be interconnected if they are able to exchange the information or data.

Applications of Computer Networks:

- ✓ Software applications, Electrical engineering, telecommunications, Resource sharing, Information sharing, E-commerce, Interactive entertainment, Person-to-person communication etc.

4.2 State the Need for Networking:

- ✓ For two computers to exchange the data, they must be connected or placed in a network.
- ✓ Network provides an improved interface between users, ensuring that information available to users at right time and at right place.

Networking plays a major role in:

1. Speed:

- ✓ User can quickly access files and other resources available on the network.
- ✓ If the network is not available, accessing the files will take time as user will require physical media such as floppy or external device to transfer the data.

2. Resource Sharing:

- ✓ Resources such as printers, fax machines, e-mail servers and scanners etc can be shared to multiple systems when connected in a network.
- ✓ Most organizations have a large number of computers and installing software on each computer is expensive. So to reduce the cost, we can install the software on one of the computer in the network and allows the user to install the software from that computer.

3. Communication facilities:

- ✓ Networking helps in sending and receiving e-mail messages anywhere in the world. An e-mail can contain voice, video and pictures.
- ✓ Can communicate with people by the chat service, video conferencing and teleconferencing.

4. Backups and Failover:

- ✓ Backups are used if the original data is lost (or) corrupted.
- ✓ If one computer fails, another computer on the same network can take over its functions.

4.3 Classification of Networks – LAN, MAN, WAN:

“Computer Network is a digital telecommunications network which allows nodes to share resources”.

- ✓ In computer networks computing devices exchange data with each other using connections between nodes.
- ✓ Connections established over cable media (Wires (or) optical cables) (OR) wireless media (Wi-fi).
- ✓ Classification based on its size, the distance it covers, and its physical architecture.
- ✓ There are three primary categories:
 1. Local Area Networks (LAN)
 2. Metropolitan Area Networks (MAN).
 3. Wide Area Networks (WAN)

1. LAN [Local Area Networks]:

- LAN is a computer network that interconnects computers within a limited area such as a residence, school, Laboratory, Offices etc.
- LAN is useful for sharing resources such as data storage & printers.
- LANs can be built with relatively inexpensive hardware such as hubs, Ethernet cables.
- LAN typically relies mostly on wired connection for increased speed & security but wireless connections also supported.
- LAN size is limited to few kilometers.
- The most common LAN topologies are bus, ring, and star.
- Today, however, speeds are increasing and can reach 100 Mbps with gigabit systems in development.

2. MAN [Metropolitan Area Networks]:

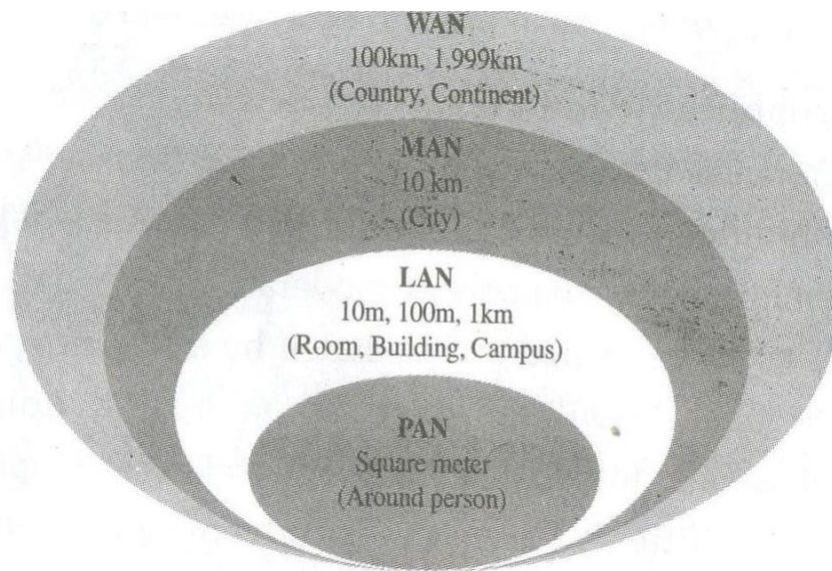
- MAN is often used to connect several LANs together to form a bigger network.
- MAN consists of a computer network across an entire city, universities.
- A MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company, such as a local telephone company.
- Most commonly used technologies to develop a MAN network are FDDI (Fiber distributed Data interface), ATM (Asynchronous Transfer Mode).

3. WAN [Wide Area Networks]:

- A WAN provides long-distance transmission of data, voice, image, and video information over large geographical areas they may comprise a country, a continent, or even the whole world.
- WAN contains multiple smaller networks such as LAN (or) MANs.
- WANs may utilize public, leased, or private communication devices, usually a combination.
- Internet is best example of public WAN.

Internetworks: When two or more networks are connected, they become an internetwork, or Internet. Individual networks are joined into internetworks by the use of internetworking devices (routers, gateways).

World Wide Web (WWW) is a distributed system that runs on the top of Internet.



Network Characteristics of LAN, MAN and WAN :

Network Characteristics	LAN	MAN	WAN
Geographic span	<10 km	5km - 50 km	> 10 km
Transmission speed	> 1 Mbps	150/60 Mbs (B-ISDN) or 41,100,140 Mbs (802.6 ^a)	> 9600 bps
Topology	Multi-point	Multi-point or point - to - point	Point-to-points
Network control	Medium access control	Medium access control store-&-forward	Store-&-forward
Ownership	Proprietary Independent of traffic	Proprietary or public ^b Independent of traffic or value-added	Public ^b Value-added

4.4 List the Hardware and Software Components:

In a network, the communication between two computers occurs in the form of signals. The data from a source computer is converted into signals and transmitted to the destination computer. On the destination computer; these signals are converted back to data

To connect two computers in a network, we need hardware & software components.

Hardware Components:

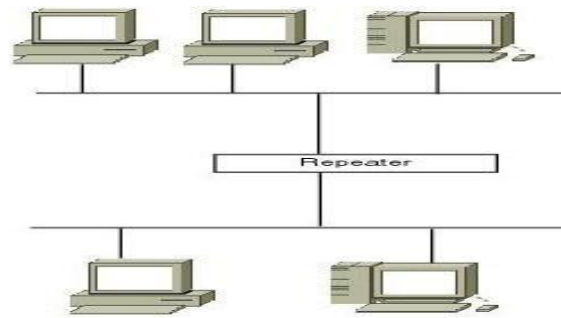
1. **Cables:** Cables are commonly used as a medium for transmitting data across networks. The most commonly used cables are coaxial, twisted-pair and optical fibercables.

2. Network Interface Card(NIC):

- ✓ NIC is a hardware device that acts as an interface through which a computer connects to a network.
- ✓ NIC converts the data into electrical/optical signals and transfers them through cables from one computer to another on the network.
- ✓ On receiving data, the NIC on the destination computer converts the electrical signals back to data

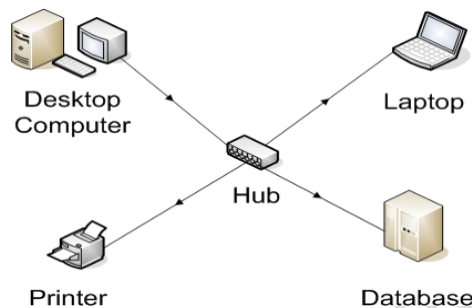
3. Repeaters:

- ✓ "A **Repeater** is a device that amplifies the incoming signals, creates a new copy of it, and transmits the signals back on the network."
- ✓ The signals transmitted can be attenuated due to some problem in the transmission media or the distance between the two locations.
- ✓ Attenuation of signals means the gradual degradation of signals strength across long distances.
- ✓ A repeater has only two ports and can connect only two segments of network.



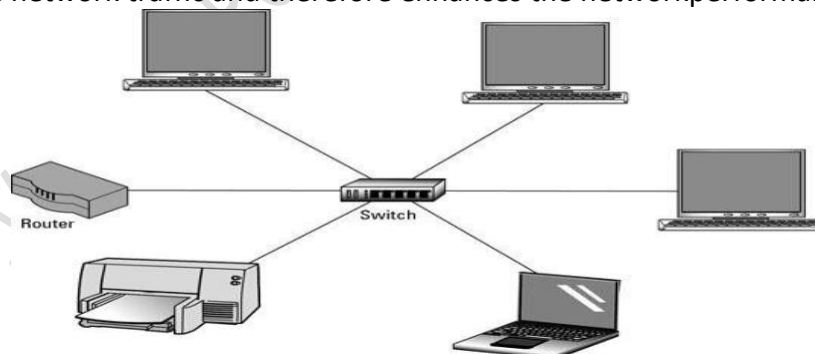
4. HUBS:

- ✓ HUB is a repeater with multiple ports.
- ✓ Hubs can be used to connect multiple segments of the same network, and transfer data from one segment to another.
- ✓ In a network, hub acts as a central point for various devices such as computers, printers and routers.



5. Switches:

- ✓ In a network, a switch acts as a central point for various devices such as computers, printers and routers.
- ✓ When the data frame is sent using a switch, the data frame carries the address of the destination computer.
- ✓ Switches can read this MAC (Media Access Control) address, and as a result, data is forwarded only to the intended computer rather than being forwarded to each computer on network.
- ✓ A switch reduces the network traffic and therefore enhances the network performance.



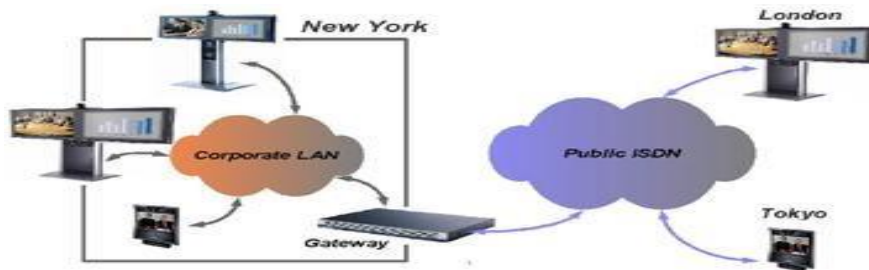
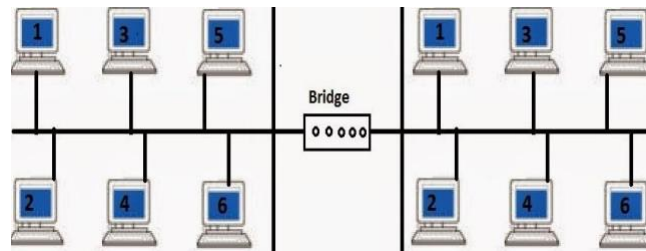
6. Routers:

- ✓ "A router is a device that uses the network address for filtering and forwarding information to different networks."
- ✓ A network address is the address of the computer on a network such as IP address.
- ✓ Router store the network addresses of computer in different networks in a table, called the **routing table**. It also contains information of path that should be used to transmit data.



7. Gateway:

- ✓ "A gateway is a device or service that translates communication protocols and enables two similar or dissimilar LAN's, to communicate with each other.

**8. Bridges:** "A bridge is a device that filters and forwards traffic between two networks."**The software components:**

1. **Protocols:** "Protocols are set of rules that the computers on the network must follow to communicate with each other."

2. **Device Drivers:**

"A device driver is a program that controls the functionality of the hardware device"

Example: NIC driver controls the functionality of the NIC, which acts as an interface through which a computer connects to a network.

4.5 Various Network Communication Standards:**Network communication standards:**

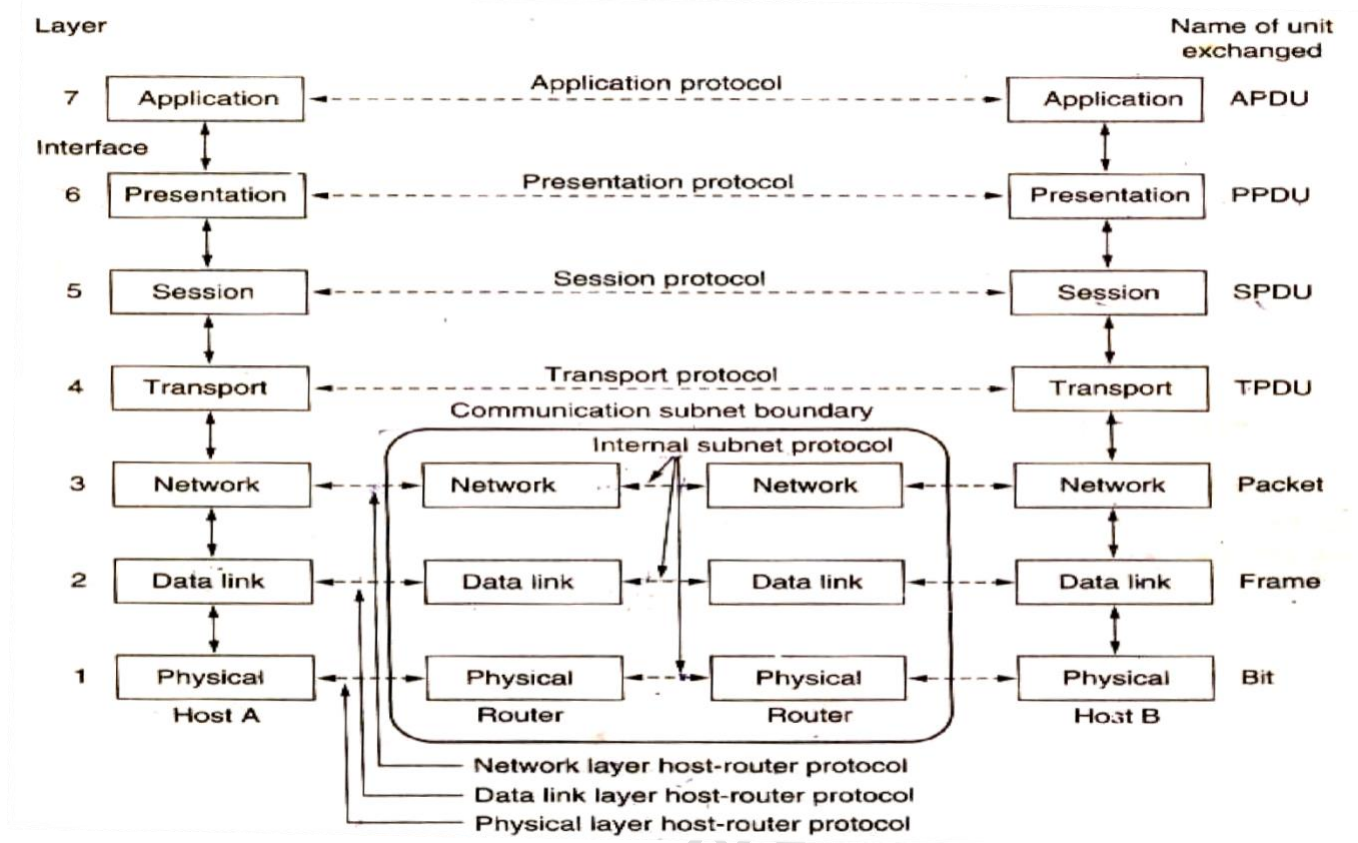
The computers on a network may use different software, hardware and protocols. For the two computers to communicate with each other, they need to follow certain communication standards.

- **ISO (International Standards Organization)** dedicated to worldwide agreement on international standards in a variety of fields. ISO's effort in the field of information technology has resulted in the creation of the Open System Interconnection (OSI) model for network communication.
- **ITU-T (International Telecommunication Union-Telecommunication standards Sector)** is an international standards organization that develops standards for telecommunication. Two popular standards developed by ITU-T are the V series (V.32, V.33, and V.42) and the X series (X.25, X.400, and X.500).
- **ANSI (American National Standards Institute)** is a private nonprofit organization. ANSI submits proposals to the ITU-T and is the designated voting member from the United States to the ISO.
- **IEEE (Institute of Electrical and Electronics Engineers)** is the largest national professional group involved in developing standards for computing, communication, electrical engineering, and electronics. It sponsored an important standard for local area networks called Project 802 (the 802.3, 802.4, 802.5 etc).
- **EIA (Electronics Industries Association)** is an association of electronics manufacturers in the US. It is responsible for developing the EIA-232D and EIA-530 standards that define serial transmission between two digital devices (Ex computer to Modem).
- **Internet Engineering Task Force (IETF)** is the standards body for the Internet itself. Important contributions include the development of Simple Network Management Protocol (SNMP).

4.5.1 Open System Interconnection(OSI) Reference Model:

- The International standards Organization (ISO) developed the OSI (Open System Interconnect) model in 1984. The ISO-OSI Reference Model deals with connecting **open systems** that is, systems that are open for communication with other systems.

- The OSI Model is represented in seven layers that define the entire process of communication between two computers on a network.
- At each layer header or a trailer can be added to the data unit as shown in below figure



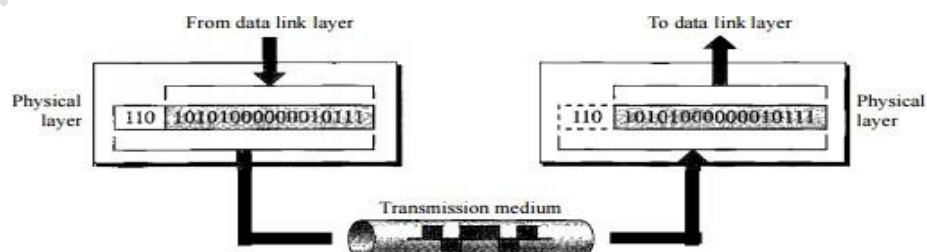
- The seven layers can be through as belonging to three groups.
 - Layers 1,2 and 3: (Network support layers) they deal with the physical aspect of moving data from one device to another
 - Layers 5,6,7: (user support layers) they allow interoperability among different software systems.
 - Layer 4: The transport layer ensures end-to- end reliable data transmission and links the other two sub groups.

Interface : Passing of data and network information through the layers of sending device and back up through layers of receiving device is made by interface.

Functions of Layers:

1) PHYSICAL LAYER:

- ✓ The physical layer transmits data in the form of **raw bits** using physical media such as coaxial cables, twisted-pair cables
- ✓ During transmission, the data is converted into an electrical signal before it is sent to the receiving device. The receiving device converts the signal into data.



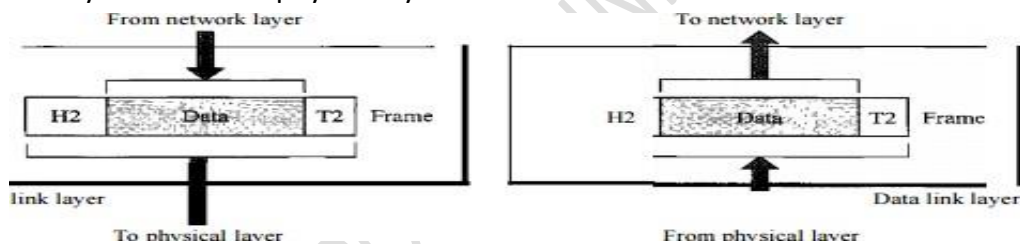
Responsibilities:

1. **Physical characteristics of interface and media:** -The physical layer defines the characteristics of the interface between devices and the transmission media. It also defines the type of transmission medium.
2. **Representation of Bits:** To be transmitted bits must be encoded into signal- electrical or optical. The physical later defines the type of encoding (how 0s and 1s are changed to signal)

3. **Data rate** [transmission rate]: The number of bits transmitted per second is also defined by the physical layer.
4. **Line configuration**: - Line Configuration refers to the way two or more communication devices attached to a link. The possible line configurations are:
 - point-to-point: Provides a link between two devices. The entire capacity of the channel is reserved for transmission between those two devices.
 - multipoint (multi drop): Link is shared among several devices.
5. **Physical Topology**: - The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, star, ring, bus etc.,
6. **Transmission mode**: - The term transmission mode is used to define the direction of signal flow between two linked devices.
 - Simplex mode: The communication is unidirectional. One device can send and other can receive it.
Ex: Radio
 - Half-Duplex: Each station can both transmit and receive, but not at the same time, when one device is sending, the other will only receive and vice-versa.
Ex: Walkie-talkies.
 - Full-Duplex: Devices can send and receive at same time.
Ex: Telephone

2) DATA LINK LAYER:

- ✓ The data-link layer receives the data from the network layer, packages it into frames, and then sends it bit-by-bit on to the physical layer.

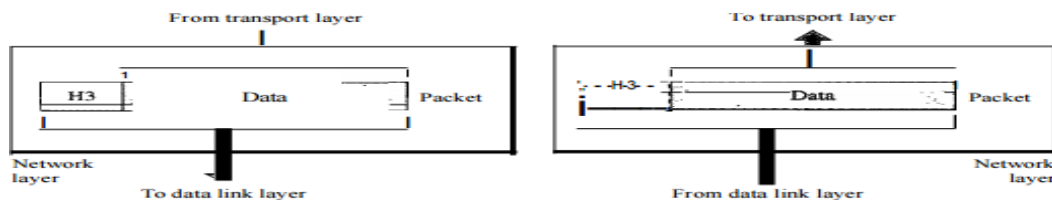


Responsibilities:

1. **Framing**: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
2. **Physical addressing**:
 - ✓ The data-link layer maintains the device address that determines the particular device on the network. This is known as **physical address or Media Access Control (MAC) address**, which is unique to a NIC card.
 - ✓ The data-link layer adds a header to the frame to define the physical address of sender and receiver of frame.
3. **Flow Control**: If the rate at which the receiver absorbs the data is less than the rate produced by the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.
4. **Error Control**: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. Error control is achieved through a trailer added to the end of frame.
5. **Access Control**: When two or more devices are connected to the same link, data link protocols are necessary to determine which device has control over the link at any given time.

3) NETWORK LAYER:

- ✓ The network layer is responsible for the delivery of data from the source to the destination computer.
- ✓ This can be achieved by arranging the data into data packets and adding a header to it.



Responsibilities:

1. **Logical addressing:** If a packet passes the network boundary, we need another addressing system to distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
2. **Routing:** Routing is a process of finding the path among which the data packets can be delivered.
3. **Congestion control:** If too many packets are present in the subnet at the same time, they will get in one another's way, forming *bottlenecks*. The control of such congestion also belongs to network layer.

4) TRANSPORT LAYER:

- ✓ The transport layer is responsible for process-to-process delivery of the entire message. It is responsible for delivery of message from one process to another.

Responsibilities:

1. **Service-point addressing:** The transport layer header includes a type of address called a service point address (or **port address**). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
2. **Segmentation and reassembly:** A message is divided into transmittable segments, each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly.
3. **Connection control:** The transport layer can be either connectionless or connection-oriented.
 - Connection-oriented:** Transport layer makes a connection with the destination machine first, after all the data is transferred, the connection is terminated.
 - Connectionless:** Transport layer treats each segment as an independent packet and delivers it.
4. **Flow Control:** Like data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across single link.
5. **Error Control:** Like data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link.

5) SESSION LAYER:

- ✓ The session layer helps in establishing interaction between two computers on a network. This interaction between two computers is referred to as a session.
- ✓ The session layer allows applications to organize and to manage data exchange.

Responsibilities:

1. **Dialog control:** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place either in
 1. half-duplex
 2. Full-duplex.
2. **Token Management:** Preventing two parties from attempting the same critical operations at the same time.
3. **Synchronization:** The session layer allows a process to add checkpoints (Synchronization points) into a stream of data.

6) PRESENTATION LAYER:

- ✓ It is concerned with syntax and semantics of information exchanged between two systems.

Responsibilities:**1. Translation:**

- ✓ The information should be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer at the sender changes the information from its sender-dependent format into a common format.
- ✓ The presentation layer at the receiving machine changes the common format into receiver-dependent format.

2. Encryption:

- ✓ To carry sensitive information, a system must be able to ensure privacy.
- ✓ Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.
- ✓ Decryption reverses the original process to transform the message back to its original form.

3. Compression: Data compression is essential on a network when the amount of data being transferred is very large. It reduces the number of bits to be transmitted.**7) APPLICATION LAYER:**

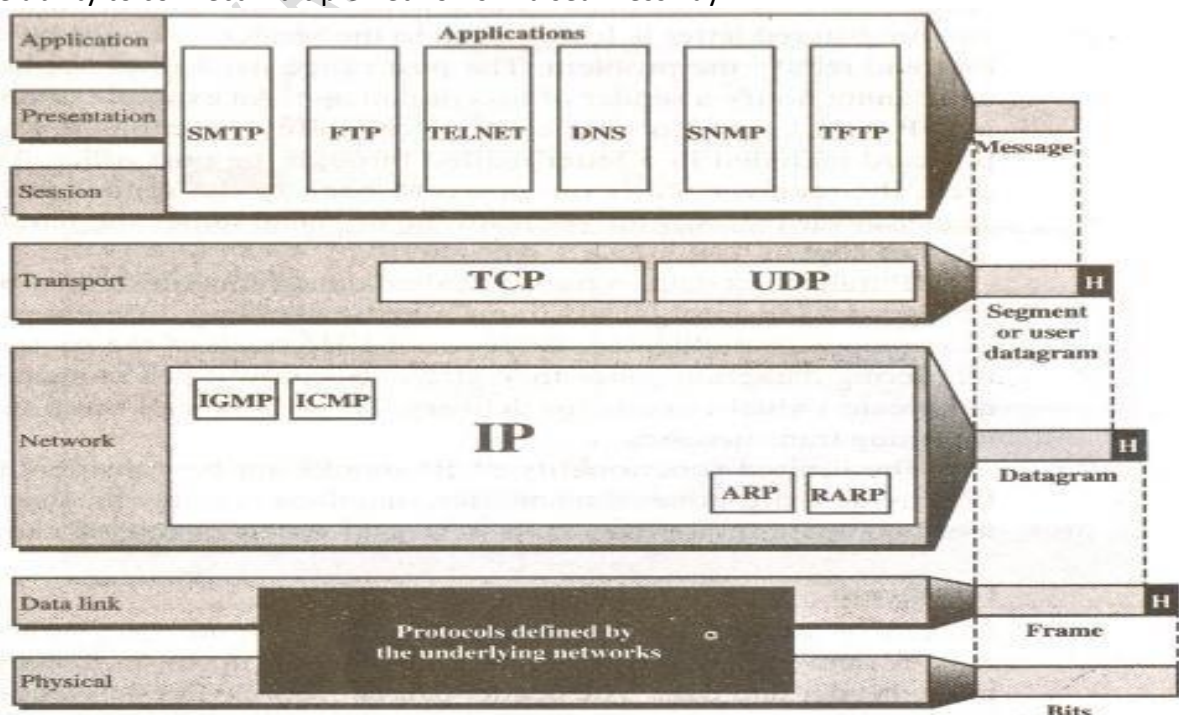
Application layer is responsible for providing services to the user.

Services are:

- ✓ **Network virtual terminal:** A network virtual terminal is a software version of a physical terminal and it allows a user to log on to a remote host.
- ✓ **File transfer, access, and management:** This allows a user to access files in a remote host.
- ✓ **Mail services:** This application provides the basis for e-mail forwarding and storage.
- ✓ **Directory services:** This application provides distributed database sources and access for global information.

4.5.2 TCP/IP REFERENCE MODEL:

- ✓ The TCP/IP reference model is a network model used for internet communication.
- ✓ The Advanced Research Projects Agency Network (ARPANET) uses this model. The research on the TCP/IP reference model was sponsored by the Department of Defense (DOD) in United States.
- ✓ The TCP/IP reference model is concerned with the ability to connect multiple networks together.
- ✓ The ability to connect multiple networks in a seamless way.



1. HOST TO NETWORK LAYER (NETWORK ACCESS):

- This is the lowest layer responsible for connecting source computer with destination computer using protocols such as Ethernet and tokenring.
- Every data packet moves through this layer before it goes through transmission medium to destination.

2. INTERNET LAYER (NETWORK LAYER):

- The internet layer is below the transport layer.
- This layer manages the connection across network to ensure that the transfer of data between the source and destination computers is successful.
- The internet layer accepts the data from the transport layer and passes it to the network layer.
- This layer is also responsible for locating the shortest route for sending the data if multiple routes are available.
- A **route** is a path taken by the packet to reach the destination computer.

PROTOCOLS:**1. Internet protocol (IP):**

- Responsible for creating network layer packets called IP datagram's and sending them to the destination.
- IP datagram is a variable length packet (up to 65,536 bytes) consisting of two parts: header and data.

2. Address Resolution Protocol (ARP):

- It is used to associate logical address with physical address.
- Also, used to find the physical address (MAC address) of the node when its IP address is known.

3. Reverse Address Resolution Protocol (RARP) :

- Allows a host to discover its internet address when it knows only its physical address.

4. Internet Control Message Protocol (ICMP):

- ICMP is a mechanism used by host and routers to send notifications of datagram problems back to the sender.
- ICMP uses echo test/replay to test whether a destination is reachable and responding.

5. Internet Group Message Protocol (IGMP):

- Used for simultaneous transmission of message to group of recipients. IP addressing supports multicasting.

3) TRANSPORT LAYER:

- The transport layer is responsible for reliable transfer of data from the source computer to the destination computer.
- It uses protocols like: 1. TCP
2. UDP

1. TCP (Transmission Control Protocol):

- Connection-oriented protocol that confirms the delivery of packets over the network (provides Acknowledgment)
- Reliable.
- TCP also handles flow control.
- At sending end of transmission, TCP divides data into smaller units called segments.

2. UDP (User Datagram Protocol):

- Connectionless protocol and does not confirm the delivery of packets over the network (does not provide Acknowledgment)
- Unreliable
- It is widely used in applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

4) APPLICATION LAYER:

- The application layer is the top most layers in the TCP/IP reference model.
- This layer provides services that help the user application to communicate with the network. All the high – level protocols, which help to deliver data over the network, reside within this layer.

PROTOCOLS:

1. **File Transfer Protocol (FTP)**: Used to transfer files from one computer to another on a TCP network.
2. **TErминаl NETwork (TELNET)**: Used to access and operate a remote computer on a network.
3. **Simple Mail Transfer Protocol (SMTP)**: Used to transfer e-mails b/w mail services on a network.
4. **Hyper Text Transfer Protocol (HTTP)**: Used to exchange text, audio, video and image files over the World Wide Web (www).
5. **Domain Name System (DNS)**: is the way that internet domain names are located and translated into IP addresses.
6. **Simple Network Management Protocol (SNMP)**: is used to manage and monitor network devices and their functions.
7. **Trivial File Transfer Protocol (TFTP)**: used for transferring files. TFTP uses the UDP to transport data from one end to another.

Comparison of OSI and TCP/IP Reference Models:

	OSI	TCP/IP
1	OSI model was devised before the corresponding protocols were invented. Therefore, the model is not biased towards one particular set of protocols.	With TCP/IP the protocols came first, and the model was really just a description of the existing protocols. The trouble with the model is that it did not fit any other Protocols.
2	When people started to build real networks using the OSI model, it was discovered that these networks did not match the required service specifications (When broadcast networks came, a new sub layer called MAC is added into data link layer)	There was no problem with the protocols fitting the model.
3	OSI model has seven layers	TCP/IP model has four layers

4.6 Know About LAN Cables and Connectors, Wireless Network Adapter:

The hardware components of a LAN are devices operating at physical layer or the data link layer and are responsible for transmission of electric signals from one device to another.

1. CABLES: “Cables are capable of transmitting signals from one device to another.” Cables are a physical medium of connecting computer in a network. Transmission media can be divided into guided & unguided media.

1. Guided media: It means wired media

- Co-axial cable
- Twisted-pair
- Optical fiber cable

2. Unguided media: It means wireless media

- Radio waves
- Infrared waves
- Micro waves
- Lasers through the air

- When transmitting electric or optical signals from one device to another, the following factors must be considered:

1. Bandwidth:

- Bandwidth is defined as the amount of data that can be transmitted by a cable for a fixed period of time.
- Bandwidth is usually measured in terms of bits of data (bits) transferred per second (bps).
Example: Bandwidth of 10Mbps.

2. Distance:

- When the distance between the devices is greater, the bandwidth decreases because the signal needs to travel over a greater distance.
- The signal strength decreases as the length of the cable increases.
- Also, an increase in the distance increases the chance of external disturbances such as Electromagnetic Interference (EMI) and Radio frequency interference (RFI), or physical stress.

3. Attenuation:

- "The gradual decrease of signal strength across long distance is called **attenuation**".
- Attenuation is overcome in LAN's by the following methods:
 1. Short cable length
 2. Amplifier

4. Distortion:

- The gradual degradation of a signal due to internal or external disturbances is called **distortion**.
- Unlike attenuation, which decreases the signal strength, distortion modifies the signal itself.
- When a signal is modified, the data transmitted by a signal becomes corrupt.

The following methods are commonly used to prevent distortion

- The communication media resistant to EMI or RFI effect are used
- Cables are not passed through region of high interference.

2. CONNECTORS:

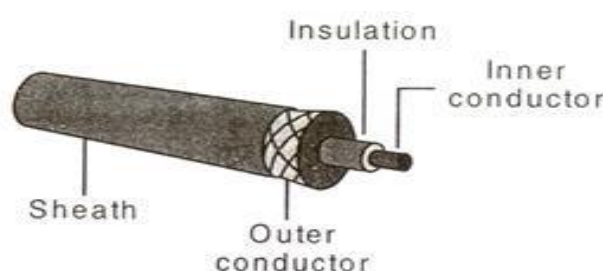
- Connectors act as an interface between NIC of the *computer* and the *cable* that transmit the signal.
- As a result, the type of the connector depends on the cable type used.
- The most common UTP cable connector is RJ45,
- Coaxial cable connector is BNC and Fiber optic cable is ST and SMA connectors.

3. WIRELESS NETWORK ADAPTOR:

- A Wireless Network Adapter allows a computing device to join a wireless LAN.
- Wireless network adapters contain a built-in radio transmitter and receiver.
- Each adapter supports one or more of 802.11a, 802.11b, 802.11n, 802.11g Wi-Fi standards.
- Wireless network adapters also exist in different form factors.

4.7 Know About Coaxial Cables, Twisted-Pair Cables, Optical Fiber Cables & Connectors:**1. COAXIAL CABLES:**

- A Coaxial cable consists of two concentric conductors separated by insulation.
- The inner conductor transmits electronic signals, and the outer conductor acts as a ground, the entire assembly is enclosed in a protective plastic sheath of Teflon or PVC.
- The conductor used in coaxial cables is copper wire. It is used for both inner and outer conductors.



Advantages: Supports high bandwidth and can transmit signals up to 10 kilometers.

Disadvantages: Support only bus topology, it does not support star topology, which is most common topology used in LAN's.

➤ The most commonly used coaxial cables in Ethernet LAN's are:

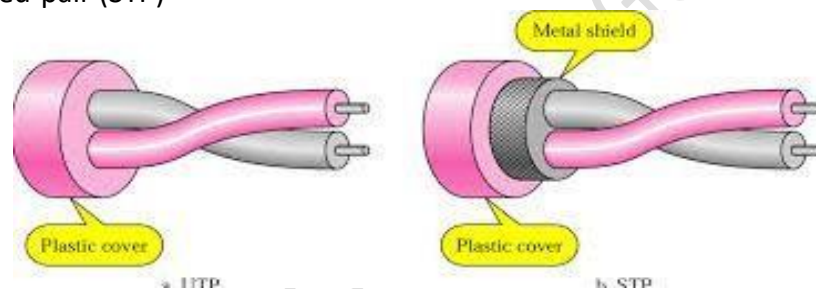
1. **10 base 2** (thin Ethernet/thinnet): supports a data transfer rate 10 MBPS and can transmit signals without attenuation over a distance of 185 meters.
2. **10 base 5** (thick Ethernet/thicknet): supports a data transfer rate 10 MBPS over a distance of 500 meters.

2 TWISTED PAIR CABLE:

- A twisted pair cable consists of 4 pairs of thin copper wires coated with PVC or Teflon, spiraled around one another.
- The spiraling results in the cancellation of the effect of EMI.
- Twisted pairs can run several kilometers without amplification, but for longer distance, repeaters are needed.
- The most common application of the twisted pair is the telephone system.

Types of twisted pairs in LAN are:

1. Unshielded Twisted Pair (UTP)
2. Shielded twisted-pair (STP)



1. Unshielded Twisted Pair (UTP):

- UTP cables are most commonly used communication medium in LANs.
- Of the 4 pairs in a UTP cable, only two pairs are actually used for communication.

Advantages:

UTP is cheap, flexible and easy to install.

CATEGORIES OF UTP CABLES: The Electronic Industries Association (EIA) has developed standards to grade UTP cable by quality.

Category 1 (Cat-1): Supports analog voice data and is commonly used for telephone systems

Category 2 (Cat-2): Supports digital voice communication up to speed 4 Mbps. Commonly used in IBM token ring networks.

Category 3 (Cat-3): Maximum data transfer rate is 16 Mbps

Category 4 (Cat-4): Maximum data transfer rate is 20 Mbps.

Category 5 (Cat-5): Higher data transfer rate up to 100 Mbps. An enhancement of cat 5 called **cat-5E** which supports transfer rate of 1000 mbps.

Category 6 (Cat-6): Data transfer rates of up to 1000 Mbps, CAT-6 is more resistant to crosstalk than CAT-5E. A **crosstalk** is a cable may sometimes pick up signal intended for another cable.

Category 7 (Cat-7): Resistant to signal attenuation and crosstalk.

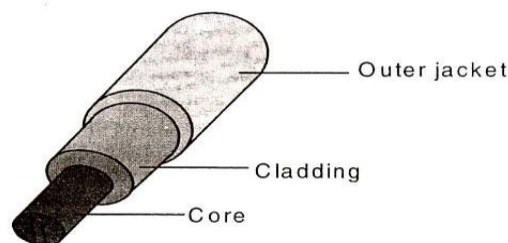
2. Shielded Twisted Pair (STP):

- In STP, an extra layer of metal foil is present between the twisted pairs of copper wires and the outer sheath. The purpose of this layer is to provide additional protection from EMI and RFI.
- However, this shielding reflects back the radiation emitted by the wires. This radiation may interfere with the signals transmitted by a cable, and as a result, corrupts the signal.
- To prevent the reflection, a coating of dielectric insulator, which absorbs the radiation, is provided on the internal surface of the metal foil.

- STP is more expensive than UTP and is generally used in networks where cables pass closer to devices that cause high EMI.
- STP cable uses a D-Shell (or DB-9) connector.

3. OPTICAL FIBER CABLES:

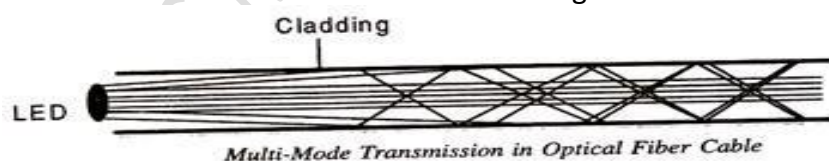
- Optical fiber cables transmit data in the form of a light. Optical fiber cable contains long thin strands of pure glass, called the fiber, with each strand having a diameter of about 5 microns. It has three components:
 1. **Core:** The core contains the optical fiber conductor (Glass or Plastic) that transmits light.
 2. **Cladding:** The core is surrounded by another optical material to prevent any light from escaping the core. The function of cladding is to reflect the light back into the core.
 3. **Sheath or Outer Jacket:** The core and cladding are covered with a sheath, usually made of plastic, to protect the fiber from damage.



- In optical fiber cables, the data to be transmitted is converted into light by **codec** (coder & decoder) present at each end of the fiber.
- The **codec** converts the data from the computer to light, and the light is then transmitted across the cable using either a Light Emitting Diode (LED) or an Injection Laser Diode (ILD). At the destination, a **decoder** receives the light beam and converts it into data.
- If an LED is used, the transmission is called **multi-mode transmission**.
- If an ILD is used, the transmission is called **single-mode transmission**.

1. Multi-Mode Transmission:

A **mode** is defined as the angle at which a ray of light enters the core of the optical fiber cable. If the light enters the core at different angles, it is called **multi-mode transmission**. Multi-mode transmission occurs when an LED is used as the light source.



The rays of light beam disperse after travelling a certain distance through the fiber. The rays in the center of the beam do not disperse, whereas rays on the circumference of the light beam disperse and hit the cladding and are reflected back into the core.

Advantages:

1. Multi-mode transmission is inexpensive because the cost of LED is less.
2. Multi-mode transmission is preferred in LANs and in networks that connect computers in a large area, which span across a few miles.

Disadvantages:

The collision of light beams due to dispersion and reflection. These collisions weaken the signal strength, resulting in attenuation.

2. Single-Mode Transmission:

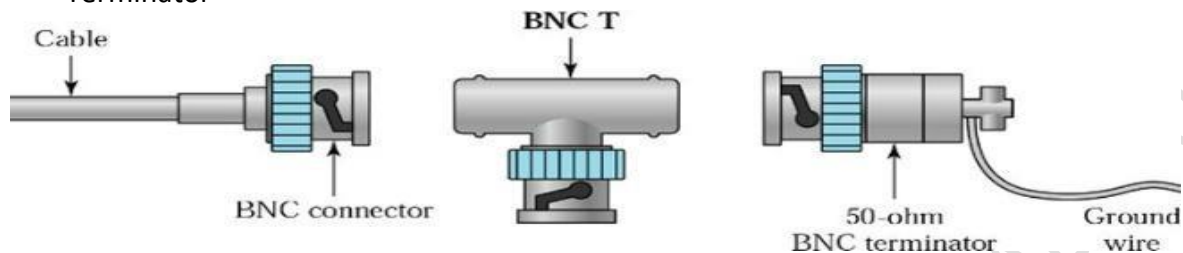
- ✓ In single mode transmission ILD is used to emit a light beam (laser) that carries data.
- ✓ ILD is an extremely concentrated light source and therefore the laser beams do not disperse when traveling through the fiber. In addition, the beams do not collide, thereby preventing any attenuation of the light signals.
- ✓ ILDs are expensive.

2. CONNECTORS:

“Connectors act as an interface between the NIC of the computer and the cable that transmits the signal.”

➤ Coaxial cable connectors:

- BNC connector (Bayonet -nail-concelman)
- T-Connector
- Terminator



➤ Twisted-Pair cable connectors:-

- A UTP cable connects to an NIC with an RJ-45 connector
- An STP cable used D-shell (or DB-9)connector.

➤ Optical fiber cables use either

- Screw Mounted Adapter (SMA) (or) Spring load twist (ST)Connectors.
- SMA uses a screw to connect to the end of cable, and ST clamps to connect to end of cable.
- Connector loss is more in SMAconnectors.
- Connector loss is defined as the loss of signal at the interface between the connector and the NIC. It occurs when the end of connector is not tightly plugged to the port on NIC.

Comparison of various Cables:

Cable	Speed	Cable length	advantages	Disadvantages	Connectors
Coaxial	10 Mbps	185 meters/ 500meters/10 kilo meters.	1. Easy to install 2. Less sensitive to EMI thanUTP/STP	1. Expensive compared to UTP	BNC connector, T connector and Terminator
STP	100 Mbps	100 meters	1. Resistant to EMI	Expensive compared to UTP	D- Shell Connector
UTP	100 Mbps	100 meters	1. Inexpensive 2. Easy toInstall	1. Non-Resistant to EMI	RJ-45 connector
Optic al fiber	155 Mbps & greater	10 Kilometers	1. Resistant toEMI 2. High data transferrates.	1. Expensive 2. Difficult to install	ST orSMA connector

4.8 Explain LANDevices:

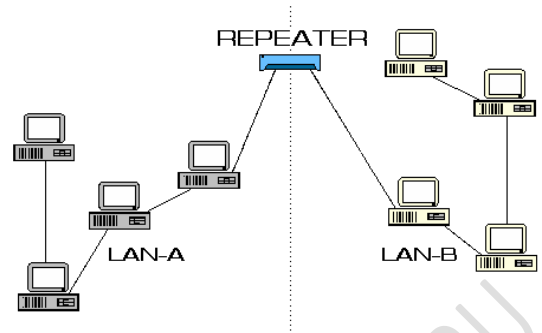
Cable cannot transmit the signal beyond a certain distance. In addition, there may be multiple computers present in a network, and to connect these computers, we need a control concentrator. A concentrator is a device with two or more ports through which computers and devices can be connected.

LAN devices are:

1. Repeaters
2. Hubs
3. switches
4. Network interfacecards(NIC'S)

4.8.1 Repeaters:

- It is an electronic device that operates at the Physical Layer of OSIModel.
- Repeaters are used to amplify the signal strength. Repeaters amplify a weak signal so that the signal stays as strong as the original one.
- A repeater installed on a link receives the signal before it becomes too weak or corrupted; it regenerates the original bit pattern and puts the refreshed copy back onto the link.
- Repeater has only two ports and can connect only two segments of a same network. Segments refer to a logical section of the same network, whereas different networks means the networks are located in geographically different areas.



4.8.2 HUBS:

- A HUB is a repeater with multiple ports.
- Hubs operate at the physical layer of the OSIModel.
- Hubs can be used to connect multiple segment of the same network and transfer data from one segment to another.
- The ports on the hub are used to connect devices such as other hubs, switches, bridges or routers.
- Based on their functions, hubs can be classified as:



1. Passivehub:

- A passive hub does not regenerate or amplify the signal.
- It only acts as an interface between two segments of a network or between different computers in a network.
- It is used when a network is divided into multiple segments, but the segments should be close to prevent signal attenuation.
- Do not require electric power.

2. Activehub:

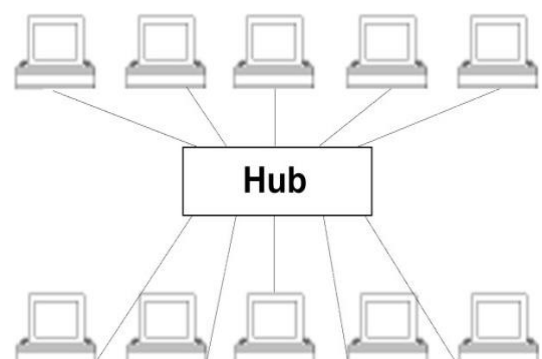
- An active hub is most commonly used powered device that amplifies the signal to its original strength.
- They are useful when the segments of a network are not close to one another and the signals may require amplification.

3. Intelligent hub(Manageable):

- An intelligent hub is an active hub with additional features such as network monitoring capabilities.

For example, as intelligent hub supporting **SNMP** (simple network management protocol) can provide information about things as activity on each port or network error logs, it can also be used to prevent unauthorized computer from connecting to the segments of the network.

- Hubs are inexpensive devices. However, they can considerably increase network traffic because they broadcast data to the device connected on all the



ports. Therefore, hubs are preferred in small LAN'S of about 8 to 10 devices.

4.8.3 SWITCHES:

- Switches connect computers in a network or different segments of same network.
- Switch works at the data link layer of OSI reference model. So, it treats data in the form of frames.
- A data frame contains MAC address of the destination computer.
- Switches read this MAC address and, forward the data only to the port that is associated with this MAC address. For this purpose, switches maintain a list of MAC address and port number associated with it.
- The process of reading MAC address of a data frame and forwarding the data to the appropriate port is known as switching.
- Methods to transmit data:



1. Cut-through switching:

Switch reads the destination MAC address of a data frame and immediately forwards the frame to the respective port.

Advantages: Switch forwards the frames as soon as it receives the frame, and therefore data transfer rate is not affected.

Disadvantages: Does not employ error –checking mechanism, as a result corrupt frames may be forwarded.

2. Store-and- forward switching:

- Switch receives all the data frames corresponding to a particular transmission. The frames are then checked for integrity and errors.
- If the frames are found to be error free, the switch forwards the frame to the respective port. -If the frames are corrupt, they are not forwarded to the destination, and the source device has to resend the frames.

Advantages: Corrupted frames are dropped and error free data is forwarded.

Disadvantages: It is slower because each frame is checked and forwarded after the switch receives all the frames.

4.8.4 Network Interface Cards(NICs):

- An NIC is a hardware device that acts as an interface through which a computer connects to a network.
- NICs work at both the data link and the physical layers of the OSI reference model.
- At the data link layer: the NIC converts the data packets into data frames and add the MAC address to the data frame.
- At the physical layer: it is responsible for converting the data into signals, and transmitting them across the communication medium.
- The MAC address is a unique hardware number present on the NIC, its size is 48 bits and written in hexadecimal hyphen notation.

Various roles of NIC:

1. Host-to-Card communication: NIC communicates with the computer using IRQ and receives data present in the memory of the computer.
2. Buffering: The data received from the computer is buffered in NIC to ensure that the NIC has complete data packet before converting it into frames.
3. Frame Creation: Once the NIC has all the data that needs to be transmitted, it divides the data into frames. A frame has three parts: header, data and trailer.
4. Parallel-to-Serial conversion: The NIC receives data from the computer in parallel form. However, the data must be converted into serial form because LANs generally transmit data bit after bit, and not multiple bits at a time.

5. **Encoding:** The serial bits are converted into electrical signals for transmission across the cable.

Factors affecting the performance are:

Bus speed: the type of expansion card (PCI slot or ISA slot) determines the bus speed.

Memory: Computers with more memory perform better than those with lesser memory.

Memory-access method: NIC can access the main memory using different methods such as, Direct Memory Access (DMA)

4.8.5 Routers (CISCO, DAX, Etc.):

- “A router is a network communication device that is used to connect two or more logically and physically different networks”.
- A router can be used to connect any two networks.
- A router acts as a post office where sorting and distribution of the posts (packets in case of routers) is done. A router works on the basis of an IP address. Every router has built in operating system known as IOS.
- A router works on the network layer of the OSI model and it routes the data towards the optimal path.
- Router uses the header information of the packets and forwarding table to define the best shortest possible path of the data

4.8.6 Modem (56KBPS Internal or external, ADSL Modems, etc):

A modem is a communication device that performs two different functions such as modulation and demodulation i.e. it converts the digital data into analog and analog into digital. The faster types of the modems are used by the internet

Internal Modem: A modem that resides on an expansion board that plugs into a computer.

External Modem: An external modem is a box that attaches to a computer's COM port via cable.

ADSL: ADSL stands for Asymmetric Digital Subscriber Line. It is a technology that allows copper telephone pairs to be used to provide a broadband connection. It provides always-on Internet connection that is automatically established once the PC and ADSL modem is switched on.

4.9 Overview of Network Topologies:

Network Topology:

- Topology refers to the way in which network of computers is connected.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to each other. There are 5 basic topologies: mesh, star, tree, bus and ring.

Line Configuration: Line Configuration refers to the way two or more communication devices are attached to a link.

- A **point-to-point** line configuration provides a dedicated link between two devices. The entire capacity of the channel is reserved for transmission between those two devices.
- A **multi-point** (also called multi drop) line configuration is one in which more than two specific devices share a single link (the capacity of the channel is shared).

Addressing: when a station receives a frame, it checks to see if the destination address matches one of its three addresses.

- o Unicast -> one-to-one communication
- o Multicast -> one-to-many communication
- o Broadcast -> one-to-all communication
- o A group of stations can have a common **multicast** address.
- o **Broadcast:** A station sends a frame that can be received by all other stations.

Baseband transmission: Baseband transmission normally uses Digital signaling. The whole capacity of the medium is occupied by the signal and frequency multiplexing is not possible.

Broadband transmission: Broadband transmission normally uses analog signaling. The capacity of the medium is divided into channels using multiplexing.

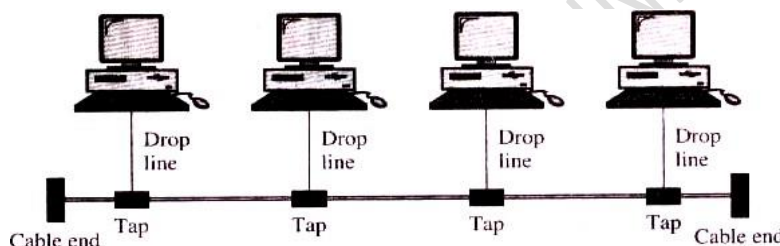
4.10 Understand the Basic Topologies Such as Bus, Ring, Star, Complex Topologies-Mesh & Hybrid:

Basic Topologies: A particular topology which is selected on the basis of number of devices, speed and budget.

Different Types of basic topologies are:

1. BUSTOPOLOGY:

- The Bus topology is the simplest of all the topologies.
 - All the devices on the network are connected to each other through a central cable called the bus.
 - One large cable acts as a backbone to link all the devices in network.
 - Nodes are connected to the bus cable by drop lines and taps.
 - A **drop line** is a connection running between the device and the main cable.
 - A **tap** is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- BUS topology allows unicast, multicast and broadcast addressing.
 - BUS topology supports Baseband and Broadband Transmission.
 - In a baseband bus topology, transmission is bi-directional.
 - In a broadband bus topology, the transmission is unidirectional.



Transmission Medium: coaxial cable.

Advantages:

- All the computers in the bus topology network are connected to each other through a cable. Therefore, this topology is easy of installation.
- This topology is extendable because new devices can be easily added to the existing bus network.
- This topology is not very expensive, because only one central cable (coaxial cable) is required for setting up the network.

Disadvantages:

- The network collapses, if the cable is damaged.
- The limited length of the cable (up to 10-20 computers) in a network may restrict the number of devices that can be connected.
- The network slows down if additional computers are connected to a network. As additional computers and devices are added, the amount of data transmitted increases and network traffic. High network traffic slows down the network considerably.

Some Characteristics of BUS topology:

- The failure of the medium seriously affects the network.
- Because the interfaces are passive, their malfunctioning does not seriously affect the performance of the network.
- Because the interfaces are passive, there is a limit on the length of the network unless repeaters are used.
- The propagation delay is independent of the number of stations on the network.

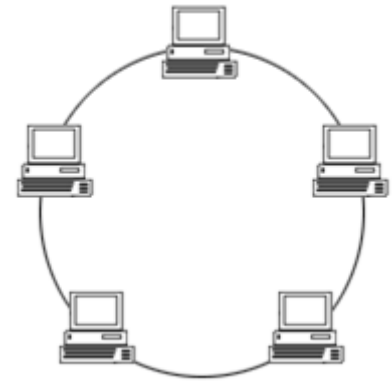
Applications (Protocols):

- 10Base5, 10Base2, Token Bus (Physically topology is Bus, While Logically topology is a ring), DQDB

(Distributed Queue DualBus).

2. RING TOPOLOGY:

- All the devices on the network are connected to each other in the form of a ring.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.
- Uses token passing methodology to provide media access to devices.
- A computer that needs to transmit data, wait for the token.
- Allows unicast, multicast, and broadcast addressing.



Point-to-point Connection:

- ✓ The connection between any two medium interfaces is point-to-point.
- ✓ Transmission is unidirectional and baseband.

Transmission Medium: Twisted pair cable, coaxial cable (or) Fiber optic cable.

Characteristics:

- As the interfaces are active, there is no limitation on the length of the network and malfunctioning affects the performance of network.

Advantages:

- Easy to install and reconfigure.
- Fault isolation is simplified. If one device does not receive a signal within a specified period. It can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

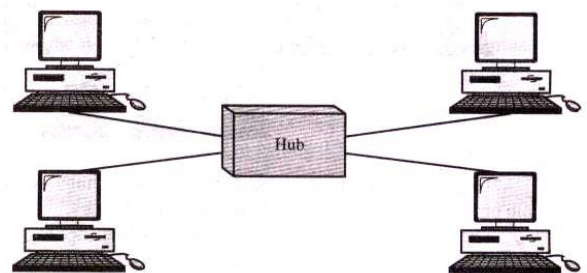
- Unidirectional traffic.
- In a simple ring, a break in the ring can disable the entire network.
- The failure of the medium seriously affects the network.

Applications:

- Token Ring, Fiber Distributed Data Transfer (FDDT)

3. STAR TOPOLOGY:

- All the devices are connected to each other through a central concentrator (hub, switch).
- If one device wants to send data to another, it sends the data to the central hub, which then transmits the data to the other connected device.
- The computers are connected to the hub or switch using UTP, STP or optical fiber cables.
- The connection between any station and the hub is a point-to-point connection.
- Transmission is usually unidirectional.
- Transmission can be either baseband (or) Broadband.
- When a station receives a frame, it is automatically removed from the station.
- A hub in a star topology can be either passive (or) Active.



HUB(OR) SWITCH:

- ✚ By using Hub, the topology is physically a star, but logically a bus. With the use of a switch, only the intended recipient receives a frame sent by a station.

Addressing:

- If the star topology uses a switch, the switch makes the decision.
- If the address is a unicast, the switch sends the frame to only the intended recipient. If the address is a multicast, then the frame is sent out to several output links.
- If the address is a broadcast, the frame is sent out to all output links.

Advantages:

- ☐ Easy to install and reconfigure.
- ☐ The failure of one device does not affect the network.
- ☐ No disturbance when devices are added to or removed from the network.
- ☐ Easy fault identification and fault isolation.

Disadvantages:

- ☐ More cabling is required than in some other topologies (ring, Bus).
- ☐ If a concentrator fails, the entire network will go down.

Applications:

- ☐ 10BaseT, Fast Ethernet, Gigabit Ethernet, Wireless LAN

Complex topologies:

The complex topologies are those topologies that use one or more basic topologies in a network.

1. Mesh topology
2. Hybrid topology

1. MESHTOPOLOGY:

- Separate cables are used to connect individual devices on the network.

The mesh topology is of two types:

- a) Full-mesh
- b) Partial-mesh

a) FULL-MESH:

- ✓ Each device is interconnected with all the devices on the network, by a dedicated cable.
- ✓ The term dedicated means that the link carries traffic only between the two devices it connects.
- ✓ If one device fails, the data travelling along the network can be routed through another device attached to the active device.
- ✓ The number of physical links in a full mesh network with n nodes is $n(n-1)/2$.

b) PARTIAL-MESH:

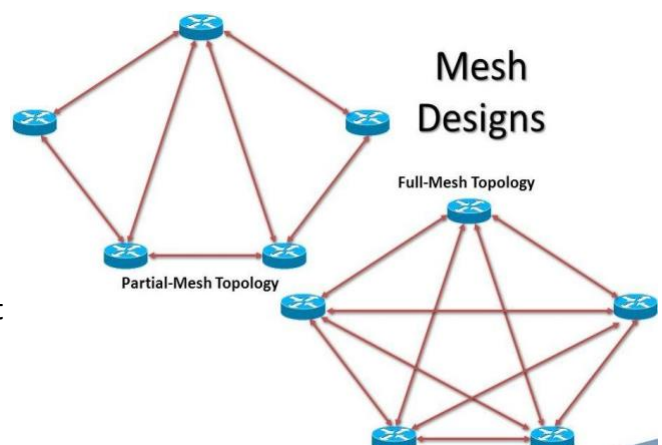
- ✓ Only few devices on the network are interconnected while others are not at all connected.

Advantages:

1. Avoids traffic problems (each connection carries its own load)
2. It is robust, that is, if one link fails, it does not affect the entire system.
3. Privacy or security is provided.

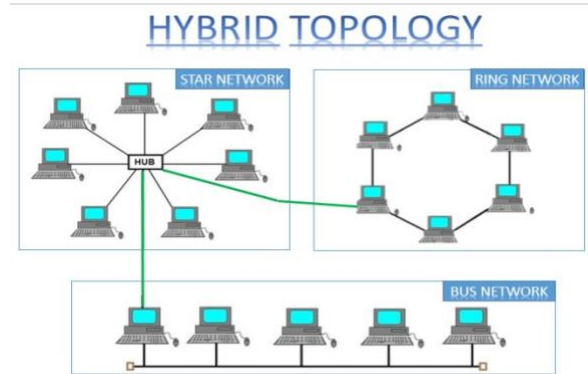
Disadvantages:

1. As every device must be connected to every other device, more cabling is required.
2. Hardware required to connect each link is expensive.



2. HYBRID TOPOLOGY:

- It is a combination of bus, star and ring networks. In other words, this topology combines multiple topologies to form a large topology. The hybrid topology is widely implemented in WAN.
- However, the connection between the two networks is established using the bus topology.
- In a star bus topology, the star topology of each network is linked to the bus topology.
- If any one of the computer fails on the star topology, it will not affect the entire network.
- However, if the central hub of the star topology fails, then the entire network goes down because the cables are connected directly to the central hub of the star network.
- As a result, computers on the network are not able to communicate with each other.



4.11 GATEWAYS:

1. "Gateway is a generic term used to represent devices that connect two dissimilar networks."
2. Gateways can be hardware devices, software running on a computer, or a combination of both. Depending on the types of protocols they support.
3. Gateways are capable of transmitting data across network's that use different network layer protocols.
4. Types of Gateways:
 1. Network gateways.
 2. Protocol gateways
 3. Tunneling gateways.

1. Network gateways:

1. Network gateways connect different network's that use the same network layer protocol.
2. Network gateways are usually routers, which contain routes to reach nodes outside the network to which the router is connected.
3. Network gateways can operate at any level of the [OSI model](#).

2. Protocol gateways:

1. Protocol gateways connect network's that use different network layer protocols.
2. Protocol gateways are usually computer running protocol conversion software.

Example:

A protocol gateway can transmit data between network that uses IPX/SPX and another network that uses TCP/IP. Protocol gateways convert the addressing format of the data packet from the source network to match the addressing format used in the destination network.

3. Tunneling gateways:

1. Tunneling gateways encapsulate the data packet the data packet of the source network in a protocol that is recognized by the destination network.

Example: Gateways used in Virtual Private Networks (VPNs)