MODULE-1

NETWORKING FUNDAMENTALS

NETWORK:

- A network is a group of two or more devices (Nodes) that are interconnected with each other using a communication link/channel.
- A **network** is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.
- An excellent example of a network is the Internet, which connects millions of people all over the world.

DATA COMMUNICATIONS: Is the exchange of data between two devices via some form of transmission medium such as a wire cable.

FOUR FUNDAMENTAL CHARACTERISTICS OF DATA COMMUNICATION:

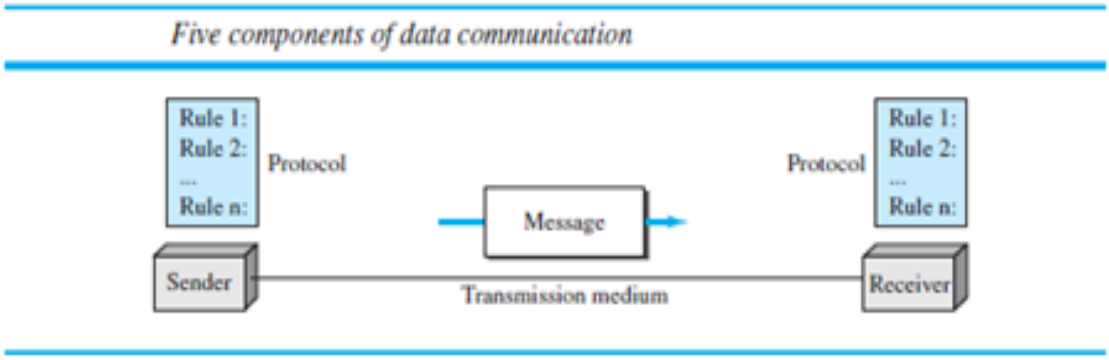
1. **Delivery.** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. **Accuracy.** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. **Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.

4. **Jitter.** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

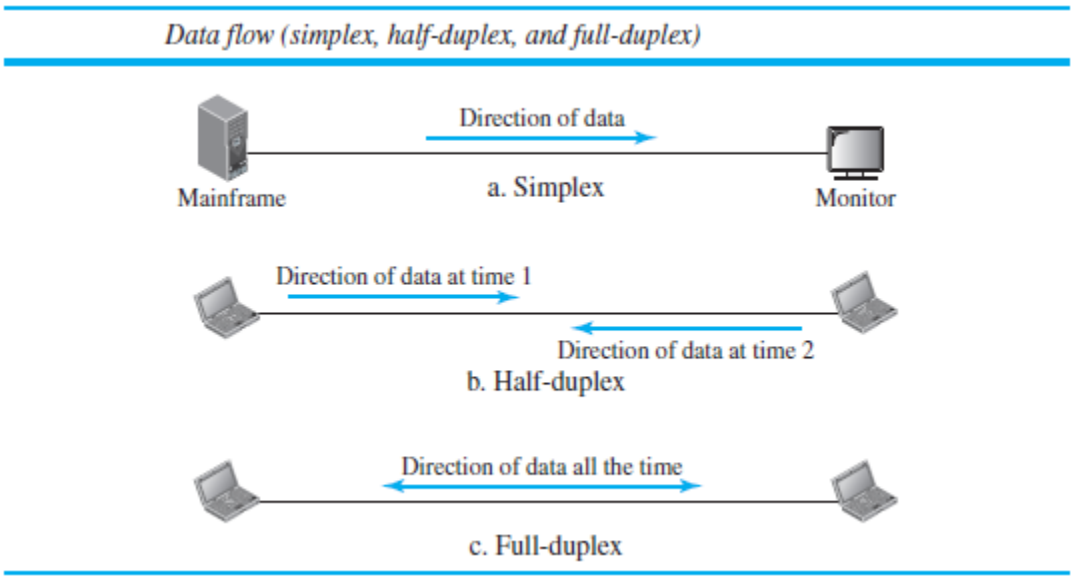
A DATA COMMUNICATIONS SYSTEM HAS FIVE COMPONENTS:



1. **Message.** The **message** is the information (data) to be communicated. Popular forms of information includes text, numbers, pictures, audio, and video.
2. **Sender.** The **sender** is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver.** The **receiver** is the device that receives the message. It can be a computer,
4. workstation, telephone handset, television, and so on.
5. **Transmission medium.** The **transmission medium** is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
6. **Protocol.** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Flow:

Communication between two devices can be simplex, half-duplex, or full-duplex as shown below:



Simplex

- In **simplex mode,** the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.
- Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex

- In **half-duplex mode,** each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.
- The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Full-Duplex

- In **full-duplex mode** (also called *duplex*), both stations can transmit and receive simultaneously.
- The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction.
- This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.
- One common example of full-duplex communication is the telephone network.

Network Criteria:

Performance

- **Performance** can be measured in many ways, including transit time and response time.
- Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.
- Performance is often evaluated by two networking metrics: **throughput** and **delay.** We often need more throughput and less delay.

- **THROUGHPUT** is the rate of production or the rate at which something is processed.
- **The delay** of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes.

Reliability

- In addition to accuracy of delivery, network **reliability** is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

- Network **security** issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Type of Connection

A network is two or more devices connected through links.
A link is a communications pathway that transfers data from one device to another.

There are two possible types of connections: point-to-point and multipoint.

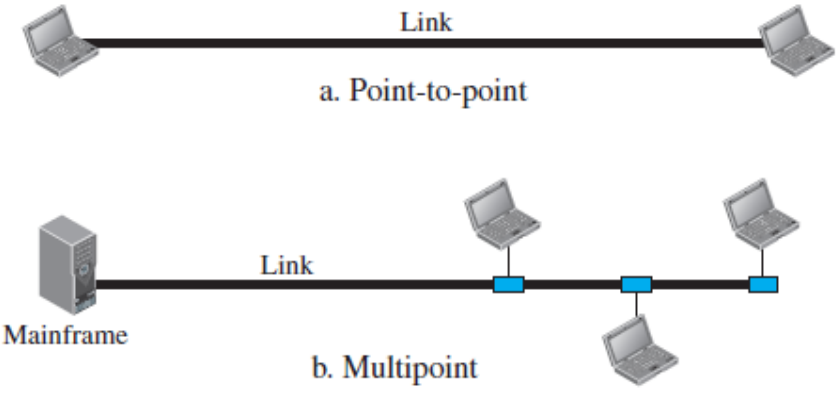
Point-to-Point

- A **point-to-point connection** provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.
- Most point-to-point connections 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
- **Example:** When we change television channels by infrared remote control, we are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint

A **multipoint** (also called **multidrop**) **connection** is one in which more than two specific devices share a single link.
In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

Types of connections: point-to-point and multipoint



TOPOLOGY:

Topology refers to the way in which a network is laid out physically.

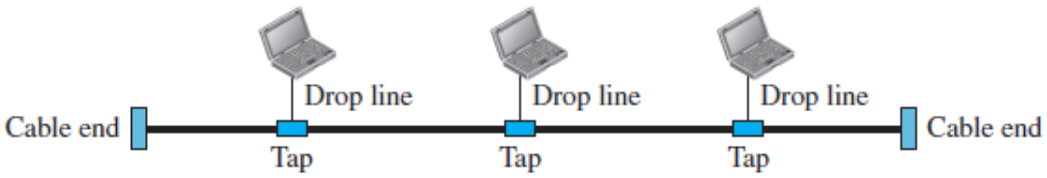
Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called ***nodes***) to one another.

There are four basic topologies possible: mesh, star, bus, ring & hybrid.

BUS TOPOLOGY:

Representation:

A bus topology connecting three stations



Explanation:

- A **bus topology** is multipoint. One long cable act as a **backbone** to link all the devices in a 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.
- As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages:

- Include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.

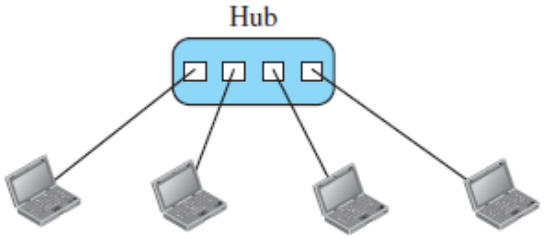
Disadvantages:

- Include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.
- Bus topology was the one of the first topologies used in the design of early local area networks. Traditional Ethernet LANs can use a bus topology, but they are less popular now for reasons.

STAR TOPOLOGY:

Representation:

A star topology connecting four stations



Explanation:

- In a **star topology,** each device has a dedicated point-to-point link only to a central controller, usually called a ***hub*.** The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.
- A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.

Advantages:

- Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Dis-advantages:

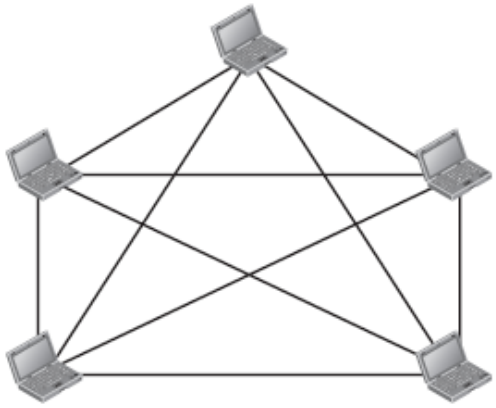
- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).
- The star topology is used in local-area networks (LANs).

MESH TOPOLOGY

Representation:

A fully connected mesh topology (five devices)

$n = 5$
10 links.



Explanation:

- In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.
- To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n – 1 node, node 2 must be connected to n – 1 node, and finally node n must be connected to n – 1 node. We need n (n – 1) physical links.
- However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n (n – 1) / 2 duplex-mode links.

Advantages:

- First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

- Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. When every message travel along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
- Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

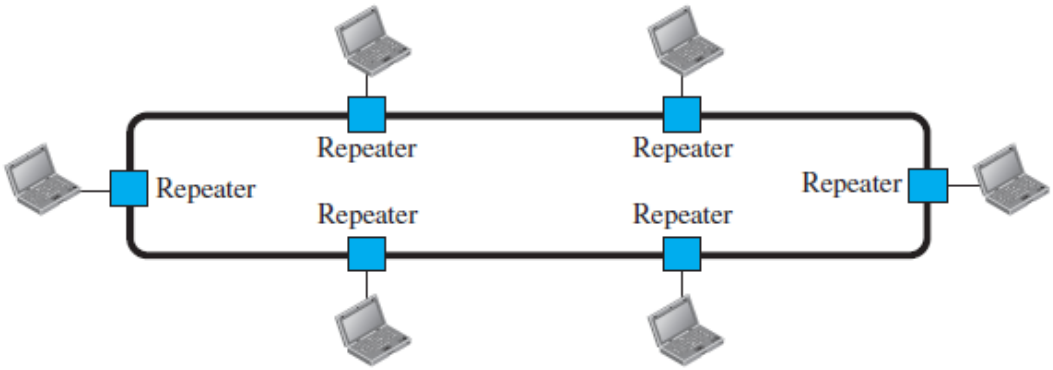
Dis-advantages:

- The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.
- One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

RING TOPOLOGY:

Representation:

A ring topology connecting six stations



Explanation:

- In a ring topology, each device has a dedicated point-to-point connection with only the 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 incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.
- A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections.
- The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified.
- Generally, in a ring a signal is circulating at all times. 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.

Advantages:

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Dis-advantages:

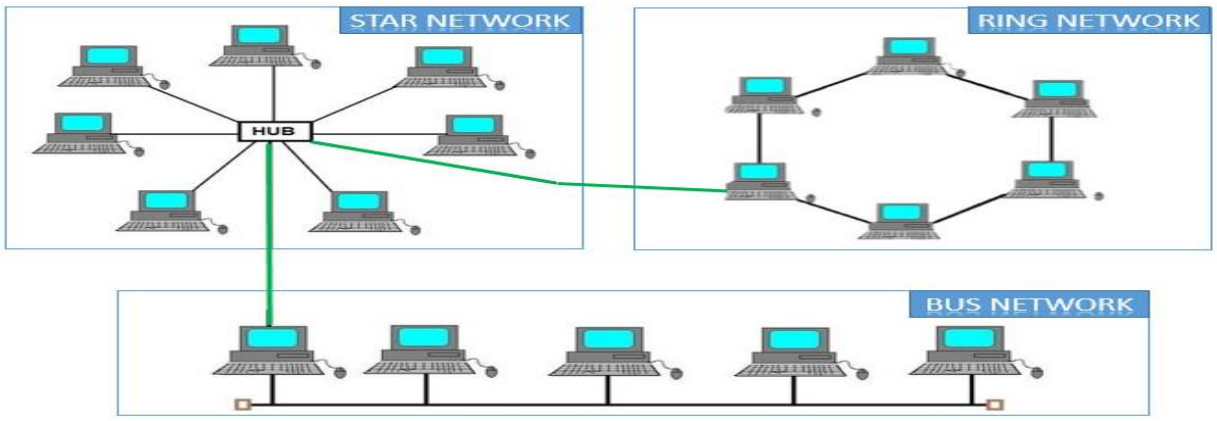
- Unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.
- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

Hybrid Topology:

Explanation:

- A hybrid topology is a type of network topology that uses two or more differing network topologies. These topologies include a mix of bus topology, mesh topology, ring topology, star topology, and tree topology.

Representation:



Advantages:

Reliable:

- It has far better fault tolerance. The section where fault is found could possibly be singled out from the rest of network and required restorative steps could be taken, without impacting the working of rest of the network.

Effective:

- The most important advantage of this topology is that the weakness of the different topologies connected are disregarded and only the strengths are taken into consideration. For instance, ring topology has good data reliability and star topology has high tolerance capability, so these two functions quite well in hybrid star-ring topology.

Flexible:

- One of the key advantages of this topology is its flexibility. The topology is created, so that it can be implemented for a variety of distinct network environment. Hybrid Network can be created in line with the demands of the corporation and by maximizing the available resources.

Dis-advantages:

Complexity:

- Due to the fact that different topologies connect in a hybrid topology, managing the topology gets challenging. It's not easy to design this type of architecture and it's a difficult job for designers. Configuration and installation process need to be very efficient.

Expensive:

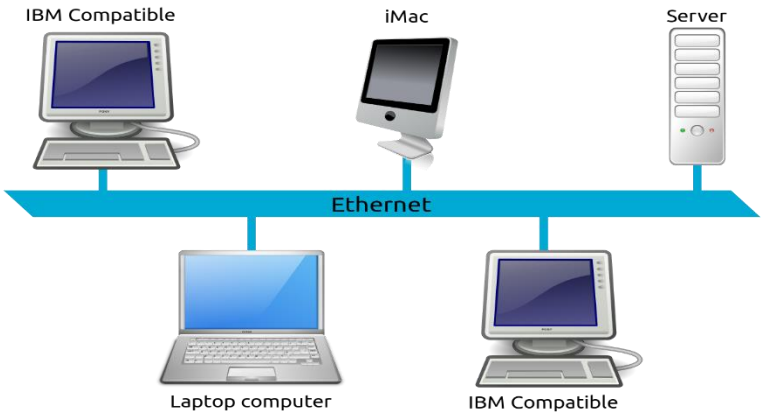
- The network hubs needed for hybrid topology networking are costly to purchase and maintain. The cost of this topology is higher in comparison to the other topologies. The hubs used to connect two distinct networks are expensive.

NETWORK TYPES:

LOCAL AREA NETWORK [LAN]:

- A local-area network (LAN) is a computer network that spans a relatively small area. Most often, a LAN is confined to a single room, building or group of buildings, however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.
- A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus. Depending on the needs of an organization, a LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include audio and video devices.
- Each host in a LAN has an identifier, an address that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.

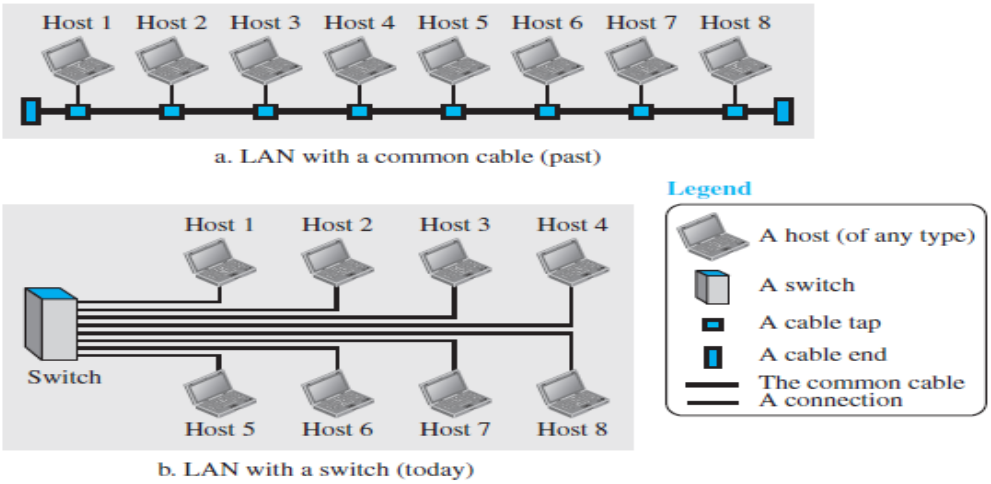
- **Representation:**



Local area network.

- In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts.
- The intended recipient kept the packet; the others dropped the packet.

An isolated LAN in the past and today

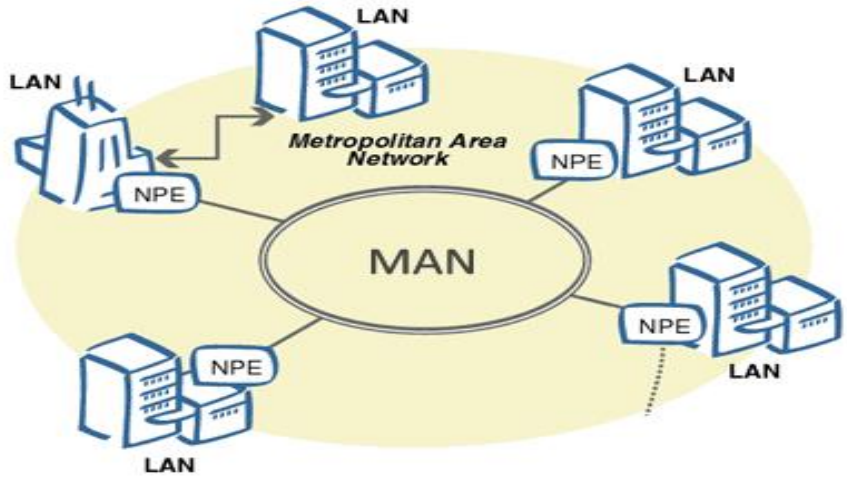


- Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts.
- The switch alleviates the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them.

Examples of LAN:

- Home Network
- Office Network
- Personal Network

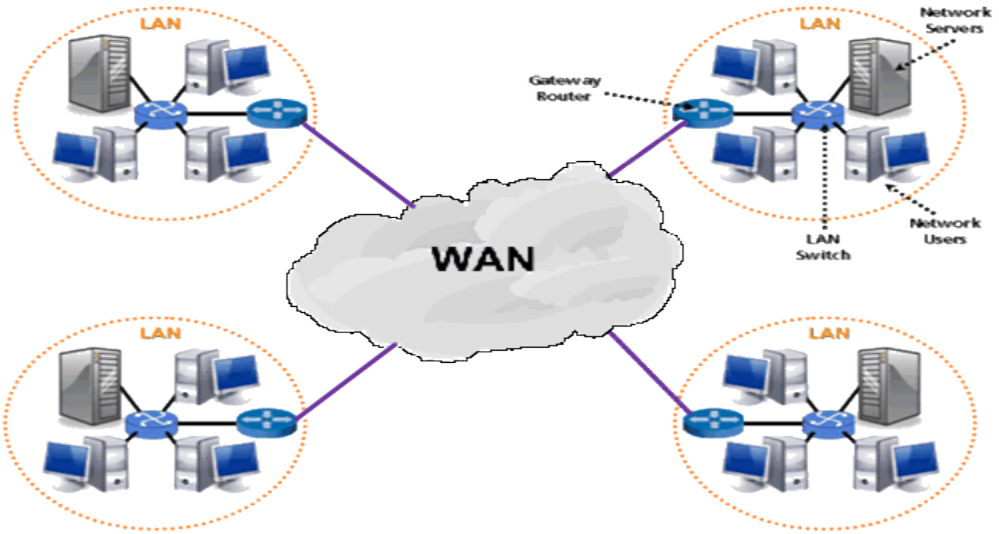
METROPOLITAN AREA NETWORK [MAN]:



- A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).
- The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network).
- It is also used to mean the interconnection of several local area networks by bridging them with backbone lines.
- MANs are extremely efficient and provide fast communication via high-speed carriers, such as fiber optic cables.
- The working mechanism of a MAN is similar to an Internet Service Provider (ISP), but a MAN is not owned by a single organization. Like a WAN, a MAN provides shared network connections to its users.
- A MAN mostly works on the data link layer, which is Layer 2 of the Open Systems Interconnection (OSI) model.

WIDE AREA NETWORK [WAN]:

Representation:



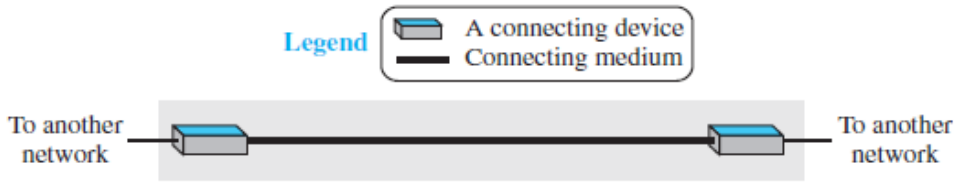
- A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LANs) and metro area networks (MANs).
- This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.
- A wide area network (WAN) is also an interconnection of devices capable of communication.
- A WAN has a wider geographical span, spanning a town, a state, a country, or even the world.
- A WAN interconnects connecting devices such as switches, routers, or modems.
- A WAN is normally created and run by communication companies and leased by an organization that uses it.

Distinct examples of WANs today: point-to-point WANs and switched WANs.

Point-to-Point WAN:

- A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).

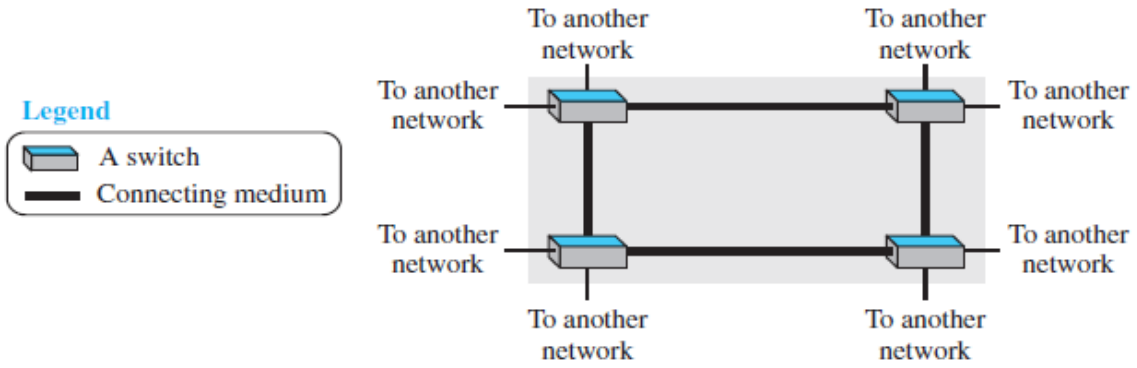
A point-to-point WAN



Switched WAN:

- A switched WAN is a network with more than two ends.
- We can say that a switched WAN is a combination of several point-to-point WANs that are connected by switches.
- As the name indicates, a switched WAN network is used to connect multiple end nodes through a common WAN network. The end nodes connect to a switched WAN network to either reach other nodes connected to the switched network or to connect to the public Internet.
- X.25, Frame Relay, ATM, MPLS are examples of popular switched WAN protocols.
- All switched WAN networks work on the principle of VC (Virtual Circuit) based packet switching.

A switched WAN



Personal area network [PAN]:

- A personal area network (PAN) is a computer network for interconnecting devices centered on an individual person's workspace. A PAN provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.
- PANs can be used for communication among the personal devices themselves, or for connecting to a higher-level network and the Internet where one master device takes up

the role as gateway. A PAN may be wireless or carried over wired interfaces such as USB.

- A personal area network (PAN) is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters.
- For example, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology. Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks.

Representation:

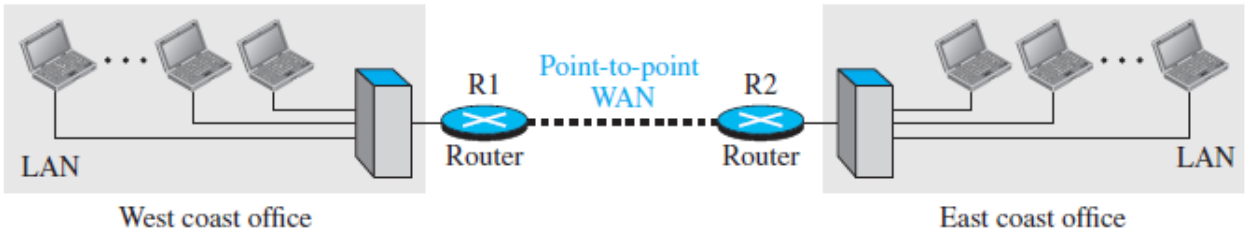
.

- **Wireless personal area network (WPAN)** which is virtually a synonym since almost any personal area network would need to function wirelessly.
- Conceptually, the difference between a PAN and a wireless LAN is that the former tends to be centered around one person while the latter is a local area network (LAN) that is connected without wires and serving multiple users.

Internetwork:

- When two or more networks are connected, they make an internetwork, or internet.
- As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. Each office has a LAN that allows all employees in the office to communicate with each other.
- To make the communication between employees at different offices possible, the management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs.
- Now the company has an internetwork, or a private internet (with lowercase i). Communication between offices is now possible.

An internetwork made of two LANs and one point-to-point WAN



- When a host in the west coast office sends a message to another host in the same office, the router blocks the message, but the switch directs the message to the destination.
- On the other hand, when a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination.

Advantages of Networking:

1. **It enhances communication and availability of information.**
   - Networking, especially with full access to the web, allows ways of communication that would simply be impossible before it was developed.
   - Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world, which is a huge boon for businesses.
2. **It allows for more convenient resource sharing.**
   - This benefit is very important, particularly for larger companies that really need to produce huge numbers of resources to be shared to all the people.
   - Since the technology involves computer-based work, it is assured that the resources they wanted to get across would be completely shared by connecting to a computer network which their audience is also using.
3. **It makes file sharing easier.**
   - Computer networking allows easier accessibility for people to share their files, which greatly helps them with saving more time and effort, since they could do file sharing more accordingly and effectively.
4. **It boosts storage capacity.**
   - Since you are going to share information, files and resources to other people, you have to ensure all data and content are properly stored in the system.
   - With this networking technology, you can do all of this without any hassle, while having all the space you need for storage.

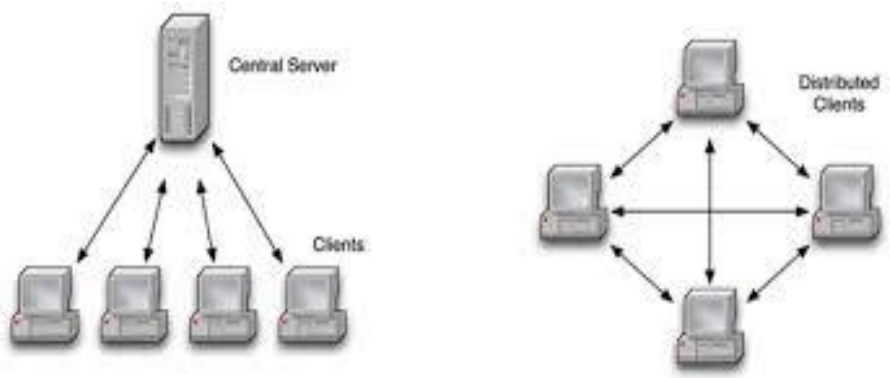
5. **It is highly flexible.**

- This technology is known to be very flexible, as it gives users the opportunity to explore everything about essential things, such as software without affecting their functionality. Plus, people will have the accessibility to all information they need to get and share.

Types of network architecture:

Peer to Peer architecture:

- Peer-to-peer architecture (P2P architecture) is a commonly used computer networking architecture in which each workstation, or node, has the same capabilities and responsibilities.
- It is often compared and contrasted to the classic client/server architecture, in which some computers are dedicated to serving others.
- P2P may also be used to refer to a single software program designed so that each instance of the program may act as both client and server, with the same responsibilities and status.
- P2P networks have many applications, but the most common is for content distribution. This includes software publication and distribution, content delivery networks, streaming media and peer casting for multicasting streams, which facilitates on-demand content delivery.
- P2P architecture is often referred to as a peer-to-peer network.



Client / Server Peer to Peer

- Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources,
- In contrast to the traditional client-server model in which the consumption and supply of resources is divided.

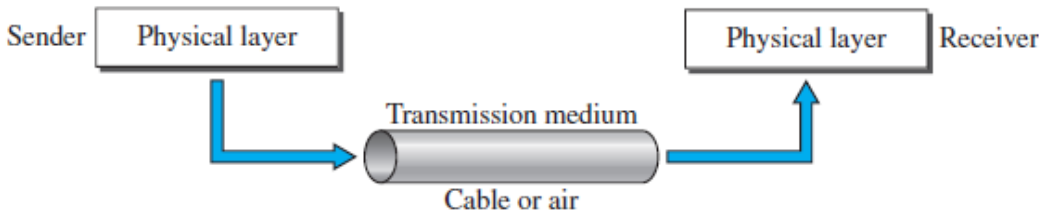
Client-Server Architecture:

- Client/server architecture is a computing model in which the server hosts, delivers and manages most of the resources and services to be consumed by the client.
- This type of architecture has one or more client computers connected to a central server over a network or internet connection. This system shares computing resources.
- Client/server architecture is also known as a networking computing model or client/server network because all the requests and services are delivered over a network.
- Client/server architecture is a producer/consumer computing architecture where the server acts as the producer and the client as a consumer.
- The server houses and provides high-end, computing-intensive services to the client on demand. These services can include application access, storage, file sharing, printer access and/or direct access to the server's raw computing power.

Transmission media/communication modes:

- Transmission media are actually located below the physical layer and are directly controlled by the physical layer.
- A transmission medium can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air.
- The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane.

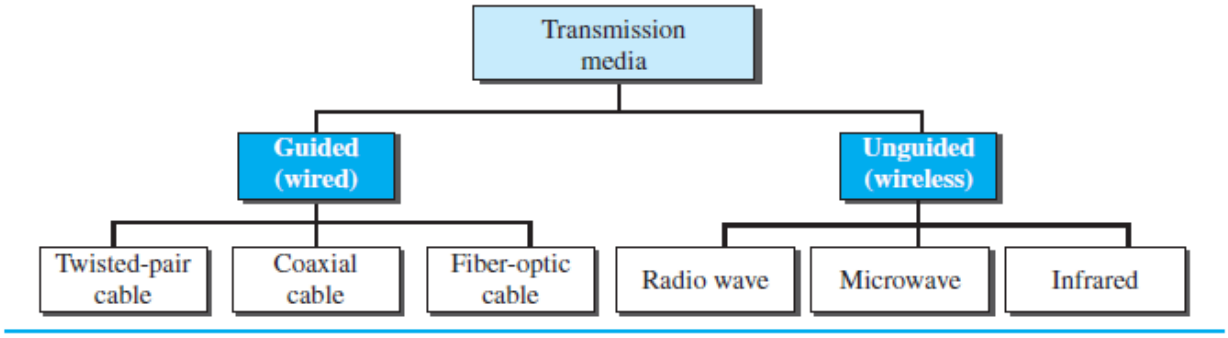
Transmission medium and physical layer



- The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.
- In telecommunications, transmission media can be divided into two broad categories: guided and unguided.
- **Guided media** include twisted-pair cable, coaxial cable, and fiber-optic cable.

- **Unguided medium** is free space.

Classes of transmission media



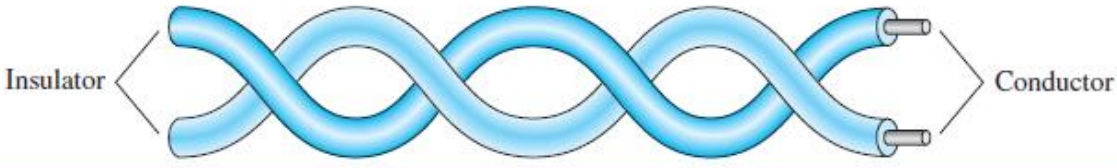
GUIDED MEDIA

- Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- A signal traveling along any of these media is directed and contained by the physical limits of the medium.
- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport
- signals in the form of electric current.
- Optical fiber is a cable that accepts and transports signals in the form of light.

Twisted-Pair Cable:

- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown.
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.
- In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

Twisted-pair cable

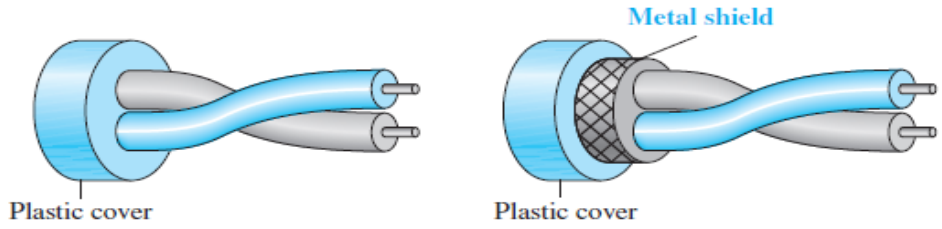


- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e.g., one is closer and the other is farther).
- This results in a difference at the receiver. By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true.
- Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals.
- The unwanted signals are mostly canceled out. From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.

Unshielded Versus Shielded Twisted-Pair Cable:

- The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP).
- IBM has also produced a version of twisted-pair cable for its use, called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
- Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

UTP and STP cables



The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into categories.

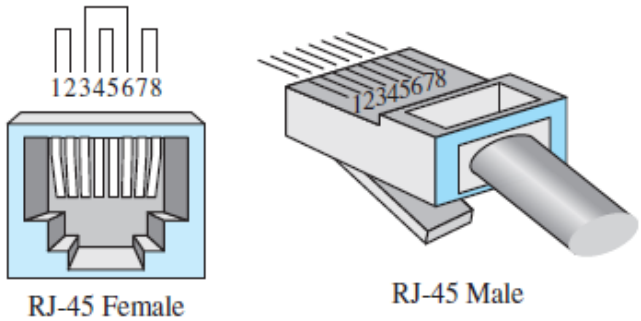
Categories of unshielded twisted-pair cables

Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs

Connectors:

- The most common UTP connector is RJ45 (RJ stands for registered jack), as shown.
- The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.

UTP connector



RJ-45 Female RJ-45 Male

Performance:

- One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance.

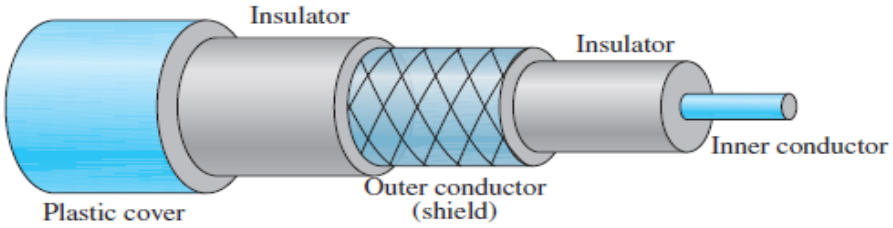
Applications:

- Twisted-pair cables are used in telephone lines to provide voice and data channels.
- The local loop—the line that connects subscribers to the central telephone office—commonly consists of unshielded twisted-pair cables.
- The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
- Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

Coaxial Cable:

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

Coaxial cable



Coaxial Cable Standards:

- Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing.

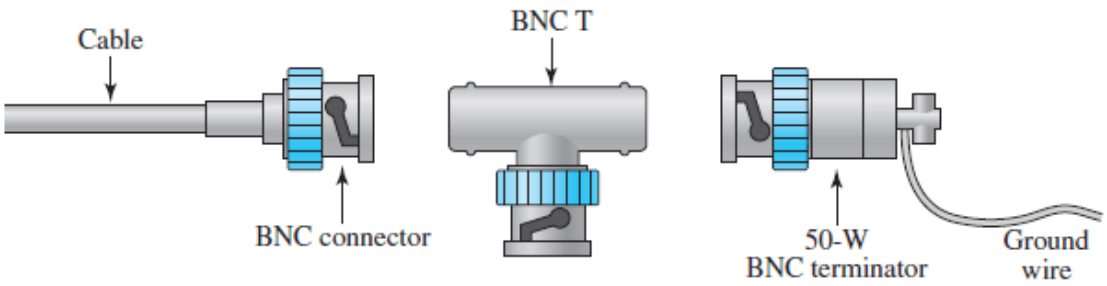
Categories of coaxial cables

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Coaxial Cable Connectors:

- To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector.
- Three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator.

BNC connectors



- The BNC connector is used to connect the end of the cable to a device, such as a TV set.
- The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device.
- The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

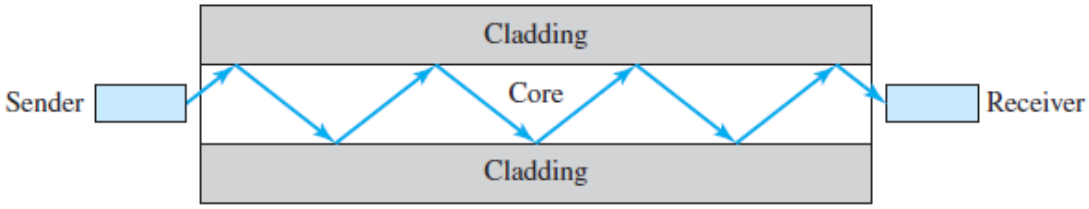
Applications:

- Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals.
- Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiberoptic cable.
- Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable.
- Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable.
- Another common application of coaxial cable is in traditional Ethernet LANs.

FIBER-OPTIC CABLE:

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- To understand optical fiber, we first need to explore several aspects of the nature of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.
- If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction.

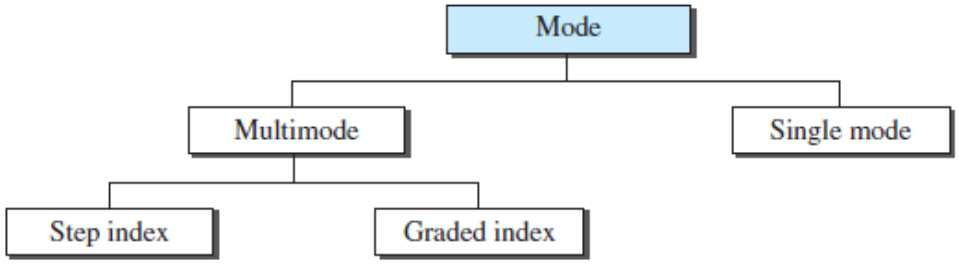
Optical fiber



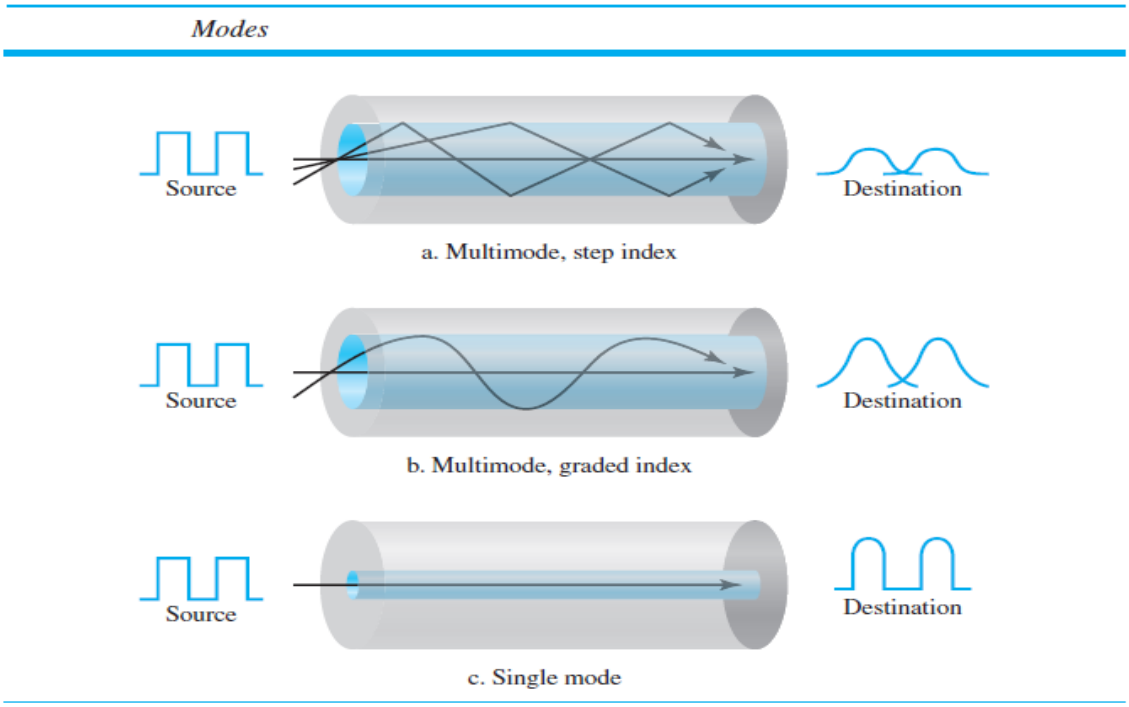
- Optical fibers use reflection to guide light through a channel. A glass or plastic **core** is surrounded by a **cladding** of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

PROPAGATION MODES:

Propagation modes



- Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index.
- Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core.



- In multimode step-index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.
- At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term step-index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.
- Multimode graded-index fiber, decreases this distortion of the signal through the cable. The word index here refers to the index of refraction. As we saw above, the index of refraction is related to density.
- A graded index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge.

SINGLE-MODE:

- Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.
- The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction). The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal.
- Fiber Sizes Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers.

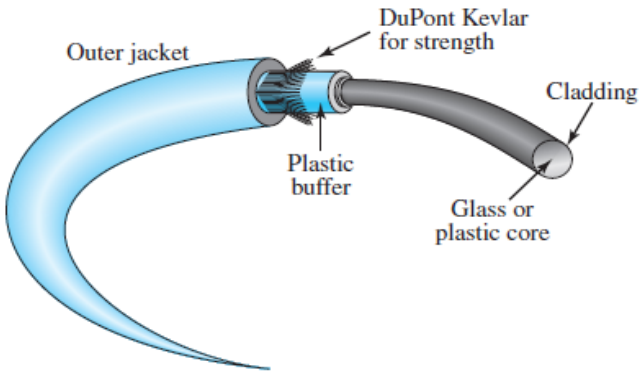
Fiber types

Type	*Core (μm)*	*Cladding (μm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

CABLE COMPOSITION:

- The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable.
- Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.

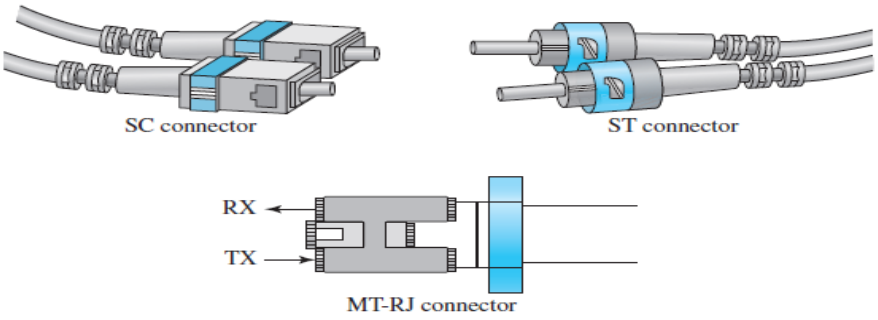
Fiber construction



FIBER-OPTIC CABLE CONNECTORS:

- There are three types of connectors for fiber-optic cables. The subscriber channel (SC) connector is used for cable TV.
- It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices.
- It uses a bayonet locking system and is more reliable than SC. MT-RJ is a connector that is the same size as RJ45.

Fiber-optic cable connectors



APPLICATIONS:

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer
- data at a rate of 1600 Gbps.
- Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides the connection to the user premises.
- This is a cost-effective configuration since the narrow bandwidth requirement at the user end does not justify the use of optical fiber.
- Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

ADVANTAGES AND DISADVANTAGES OF OPTICAL FIBER:

Advantages:

Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

❑ **Higher bandwidth:** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

❑ **Less signal attenuation:** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

❑ **Immunity to electromagnetic interference:** Electromagnetic noise cannot affect fiber-optic cables.

❑ **Resistance to corrosive materials**: Glass is more resistant to corrosive materials than copper.

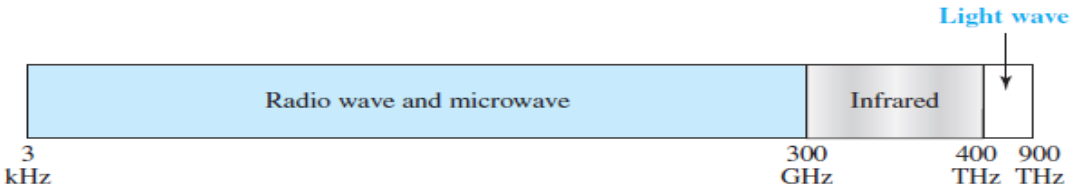
❑ **Light weight**: Fiber-optic cables are much lighter than copper cables.

❑ **Greater immunity to tapping:** Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

UNGUIDED MEDIA: WIRELESS

- Unguided medium transport electromagnetic waves without using a physical conductor.
- This type of communication is often referred to as wireless communication.
- Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.
  shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

Electromagnetic spectrum for wireless communication



Bands

Band	*Range*	*Propagation*	*Application*
very low frequency (VLF)	3–30 kHz	Ground	Long-range radio navigation
low frequency (LF)	30–300 kHz	Ground	Radio beacons and navigational locators
middle frequency (MF)	300 kHz–3 MHz	Sky	AM radio
high frequency (HF)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft
very high frequency (VHF)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
ultrahigh frequency (UHF)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
superhigh frequency (SF)	3–30 GHz	Line-of-sight	Satellite
extremely high frequency (EHF)	30–300 GHz	Line-of-sight	Radar, satellite

Radio Waves:

- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves.

- Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna. The omnidirectional property has a disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building.
- It is a disadvantage because we cannot isolate a communication to just inside or outside a building. The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into sub-bands, the sub-bands are also narrow, leading to a low data rate for digital communications.
- Radio waves use omnidirectional antennas that send out signals in all directions.
- Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas.

Omnidirectional antenna

Applications:

- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.
- Radio waves are used for multicast communications, such as radio and television, and paging systems.

Microwaves:

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

- Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.
- The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

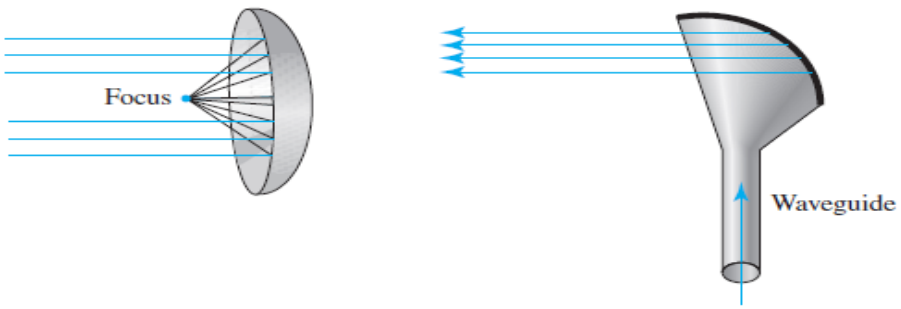
The following describes some characteristics of microwave propagation:

- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.
- The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for long distance communication.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned, and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna:

- Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn.

Unidirectional antennas



a. Parabolic dish antenna b. Horn antenna

- A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus.
- The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

- Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaves hit the dish and are deflected outward in a reversal of the receipt path.
- A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem (resembling a handle) and deflected outward in a series of narrow parallel beams by the curved head.
- Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications:

- Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

Infrared:

- Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls.
- This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.
- When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication.
- In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications:

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

ROUTER:

- A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet.
- A router is a physical or virtual appliance that passes information between two or more packet-switched computer networks - analyzing a given data packet's destination IP address, calculating the best way for it to reach that destination and then forwarding it accordingly.
- A routing table often specifies a default route, which the router uses whenever it fails to find a better forwarding option for a given packet. For example, the typical home office router directs all outbound traffic along a single default route to its internet service provider (ISP).

- Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.
- A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination.
- Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

SWITCH:

- A switch is a multi-port bridge with a buffer and a design that can boost its efficiency (large number of ports imply less traffic) and performance.
- Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
- In other words, switch divides collision domain of hosts, but broadcast domain remains same.
- A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.
- A switch is more intelligent than an Ethernet hub, which simply retransmits packets out of every port of the hub except the port on which the packet was received, unable to distinguish different recipients, and achieving an overall lower network efficiency.
- A switch is a device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices.

- Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended.
- Each networked device connected to a switch can be identified by its network address, allowing the switch to direct the flow of traffic maximizing the security and efficiency of the network.

HUB:

- A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
- Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub:

- **Active Hub: -** These are the hubs which have their own power supply and can clean, boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.

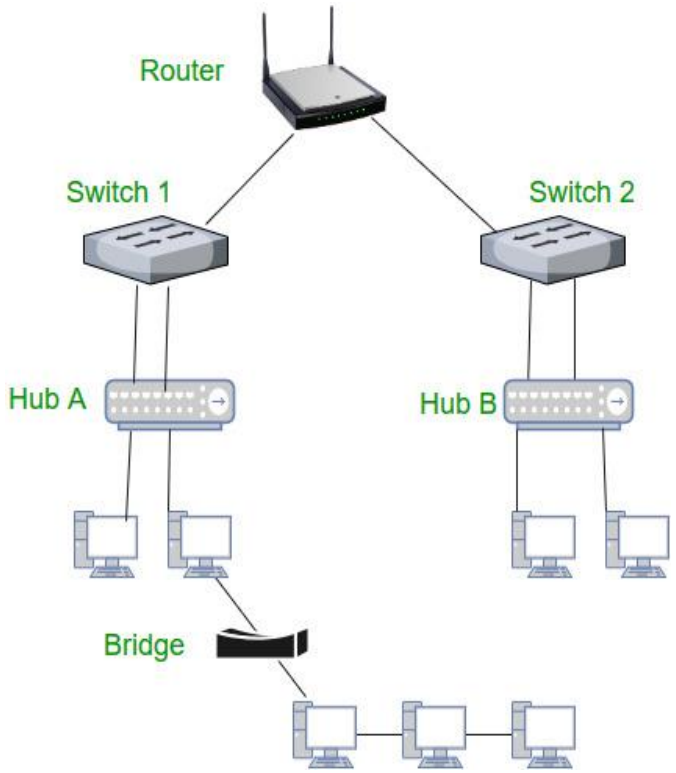
- **Passive Hub: -** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

REPEATER:

- A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.

- A repeater is implemented in computer networks to expand the coverage area of the network, repropagate a weak or broken signal and or service remote nodes.
- Repeaters amplify the received/input signal to a higher frequency domain so that it is reusable, scalable and available.
- Repeaters were introduced in wired data communication networks due to the limitation of a signal in propagating over a longer distance and now are a common installation in wireless networks for expanding cell size.
- Repeaters are also known as signal boosters.

Classification of all the connecting devices:

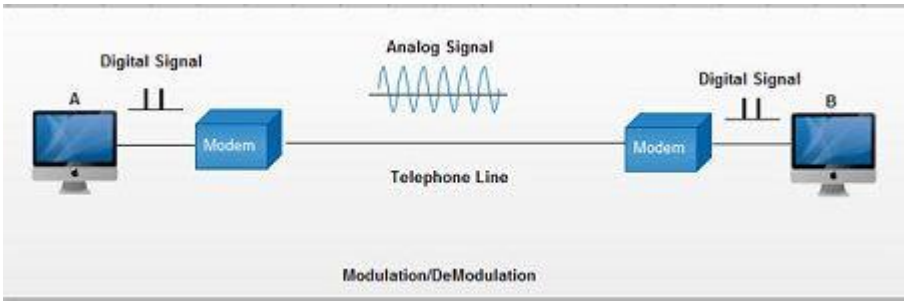


Gateway:

- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.
- They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

Modem:

- Modem is abbreviation for Modulator – Demodulator.
- is a device or program that enables a computer to transmit data over, for example, telephone or cable lines.
- Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms.
- When an analog facility is used for data communication between two digital devices called Data Terminal Equipment (DTE), modems are used at each end. DTE can be a terminal or a computer.

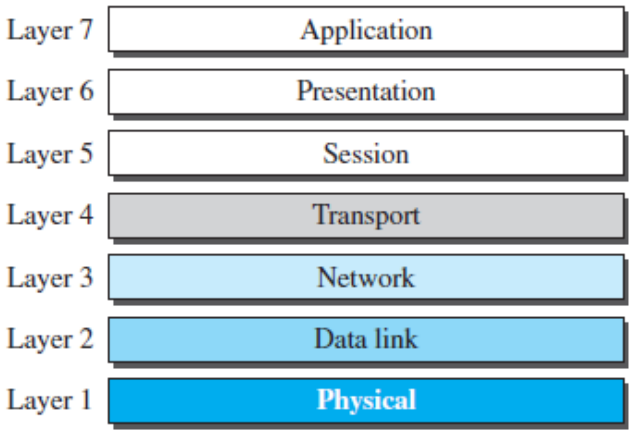


OSI-ISO REFERENCE MODEL:

- International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- Almost three-fourths of the countries in the world are represented in the ISO. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.
- It was first introduced in the late 1970s.

ISO is the organization; OSI is the model.

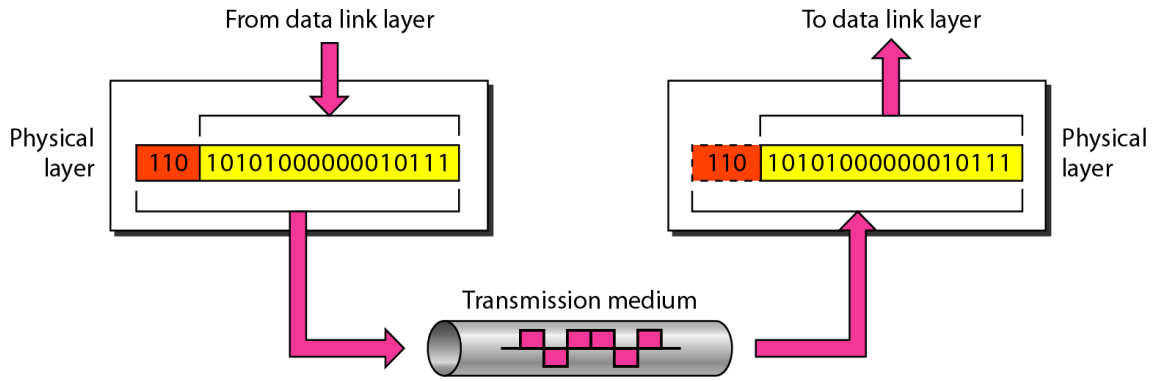
The OSI model



- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separates but related layers, each of which defines a part of the process of moving information across a network

Physical Layer (Layer 1):

- The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of bits. It is responsible for the actual physical connection between the devices.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are:

Bit synchronization:

- The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

Bit rate control:

- The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

Physical topologies:

- Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.

Transmission mode:

- Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

*Hub, Repeater, Modem, Cables are Physical Layer devices.

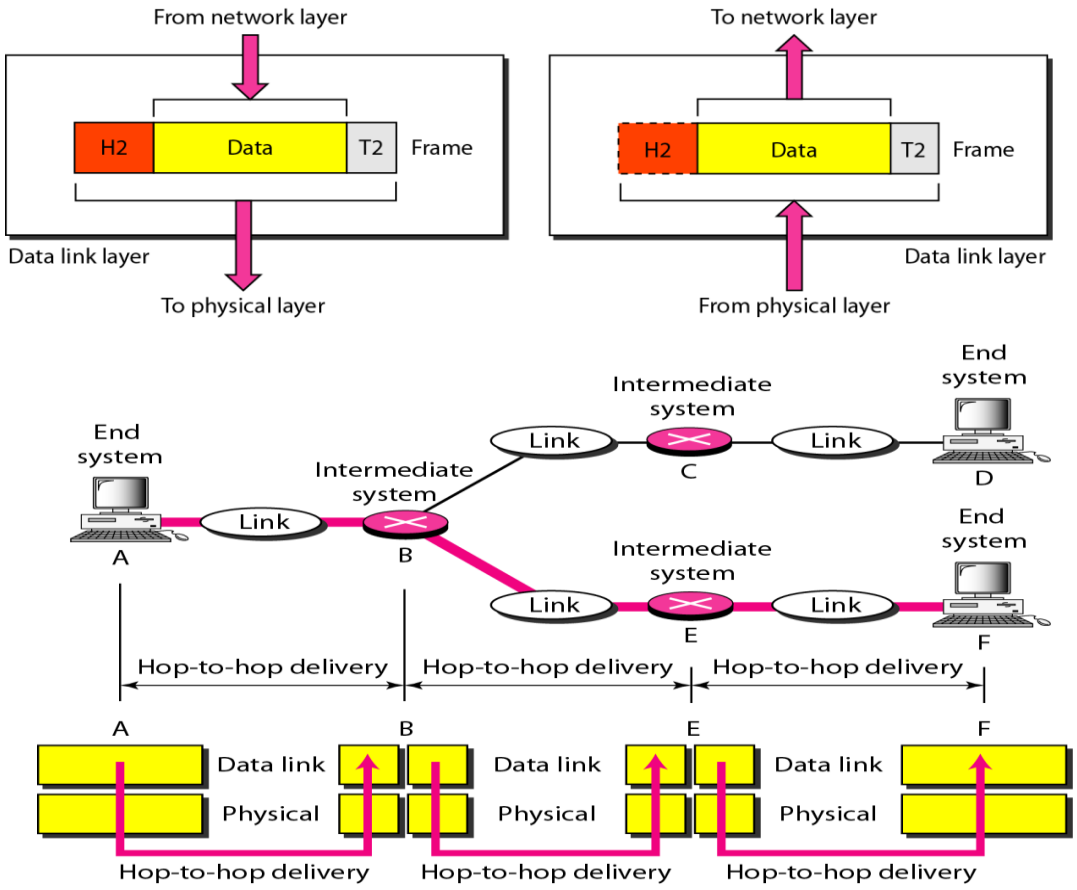
Data Link Layer (DLL) (Layer 2):

- The data link layer is responsible for the node to node delivery of the message.

- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
- Data Link Layer is divided into two sub layers:
    - Logical Link Control (LLC)
    - Media Access Control (MAC)

- The packet received from Network layer is further divided into frames depending on the frame size of NIC (Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

- The Receiver's MAC address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.



The functions of the data Link layer are:

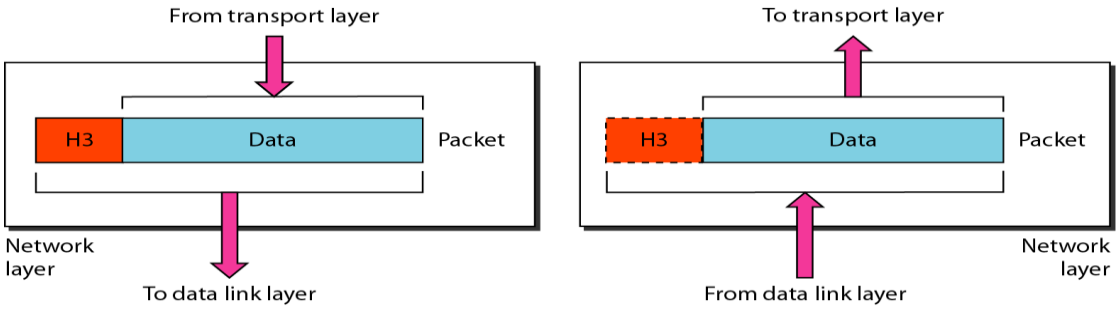
Framing:

- Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical addressing:**
  After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
- **Error control:**
  Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

- **Flow Control:**
  The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates that amount of data that can be sent before receiving acknowledgement.
- **Access control:**
  When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.
  *Packet in Data Link layer is referred as Frame.
  *Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
  *Switch & Bridge are Data Link Layer devices.

Network Layer (Layer 3):

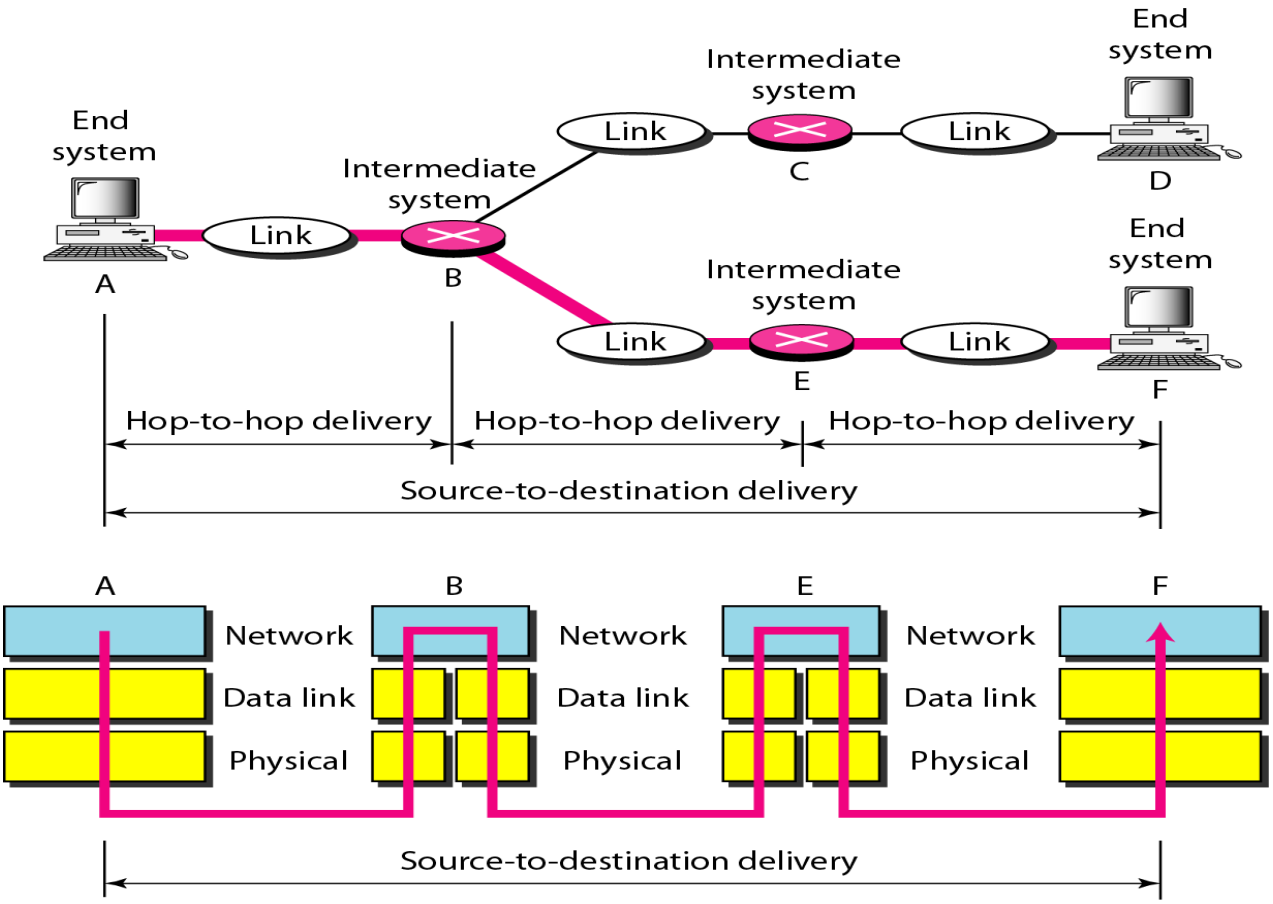
- Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP address are placed in the header by network layer.



- **The functions of the Network layer are:**

- **Routing**: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
- **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* Segment in Network layer is referred as Packet.
*Network layer is implemented by networking devices such as routers.



Transport Layer (Layer 4):

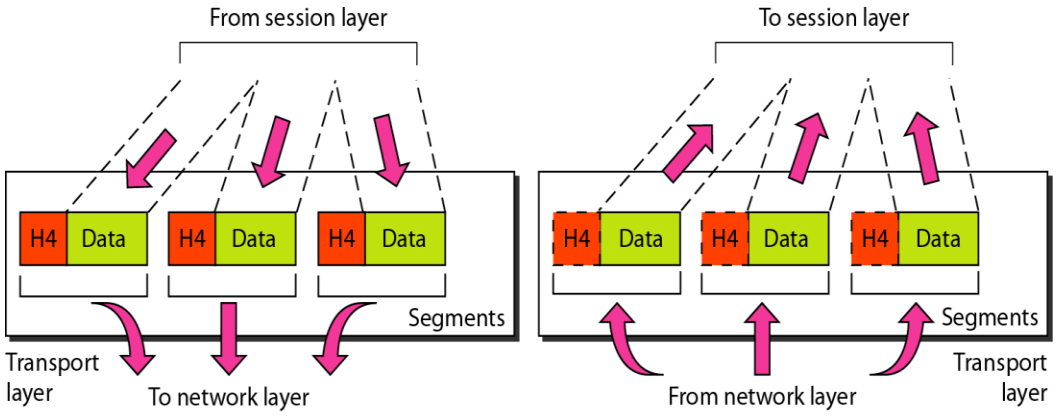
- Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments.
- It is responsible for the End to End delivery of the complete message.
- Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

• At sender's side:

- Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission.
- It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.
- **Note:** The sender needs to know the port number associated with the receiver's application.
- Generally, this destination port number is configured, either by default or manually.
- **For example**, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

• At receiver's side:

- Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application.
- It also performs sequencing and reassembling of the segmented data.



The functions of the transport layer are:

Segmentation and Reassembly:

- This layer accepts the message from the (session) layer, breaks the message into smaller units. Each of the segment produced has a header associated with it.
- The transport layer at the destination station reassembles the message.

Service Point Addressing:

- In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address.
- Thus, by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer:

- **Connection Oriented Service:** It is a three-phase process which include
  - Connection Establishment
  - Data Transfer
  - Termination / disconnection
- In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.
- **Connection less service:** It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet.
- This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

* Data in the Transport Layer is called as Segments.
*Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
*Transport Layer is called as Heart of OSI model.

Session Layer (Layer 5):

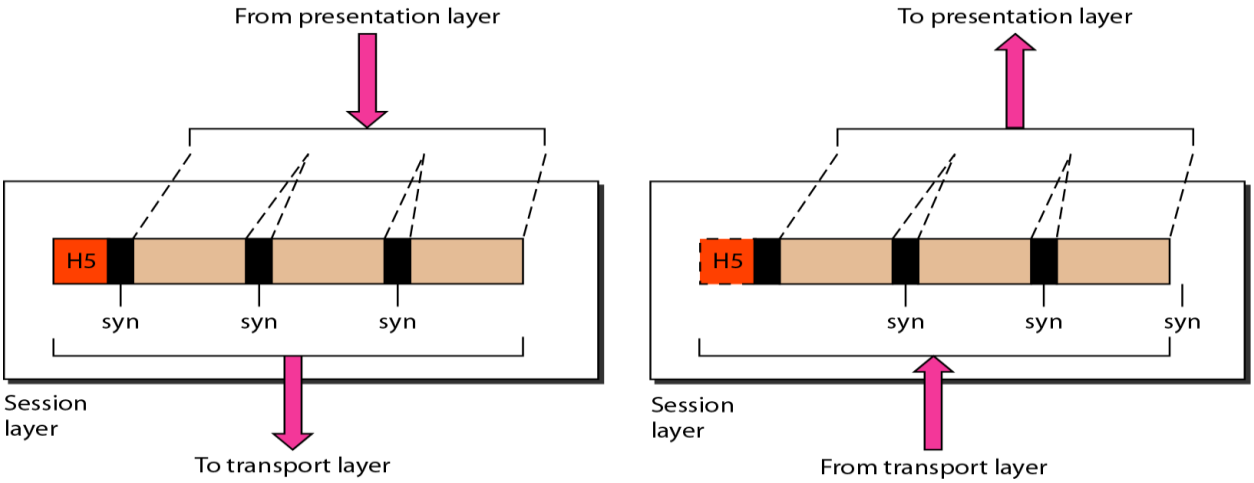
- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
- The functions of the session layer are:
  - Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.

Synchronization:

- This layer allows a process to add checkpoints which are considered as synchronization points into the data.
- These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

Dialog Controller:

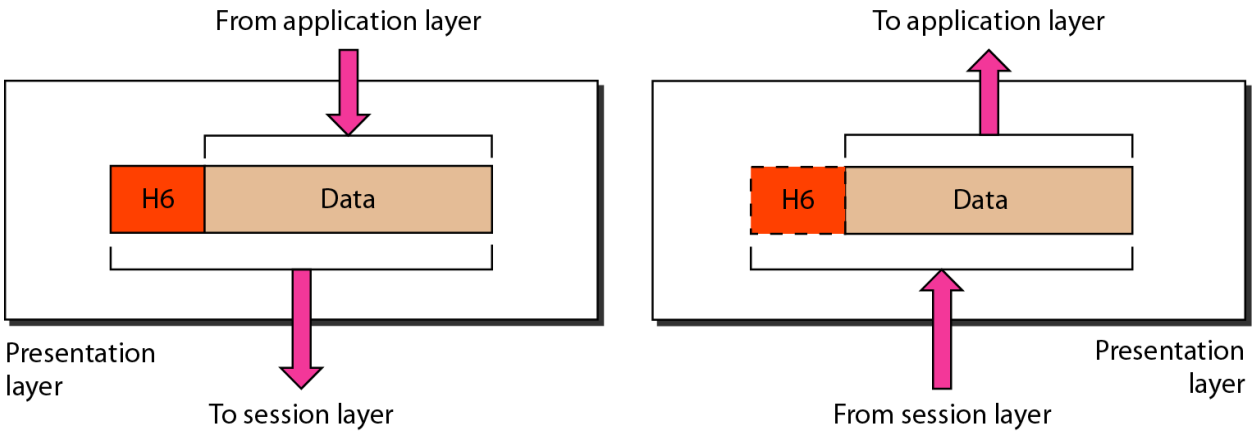
- The session layer allows two systems to start communication with each other in half-duplex or full-duplex.



*All the below 3 layers (including Session Layer) are integrated as a single layer in TCP/IP model
as "Application Layer".
*Implementation of these 3 layers is done by the network application itself. These are also known
as Upper Layers or Software Layers.

Presentation Layer (Layer 6):

- Presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
- The functions of the presentation layer are:
- Translation: For example, ASCII to EBCDIC. **(American Standard Code for Information Interchange, Extended Binary Coded Decimal Interchange Code).**



Encryption/ Decryption:

- Data encryption translates the data into another form or code.

- The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

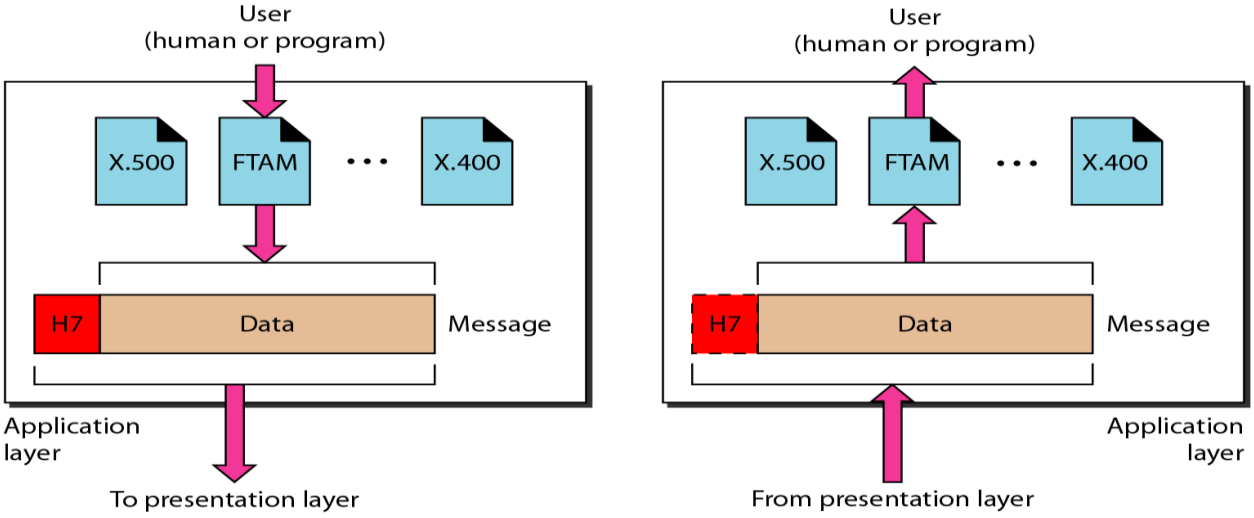
Compression:

- Reduces the number of bits that need to be transmitted on the network.

Application Layer (Layer 7):

- At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications.
- These applications produce the data, which has to be transferred over the network.
- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

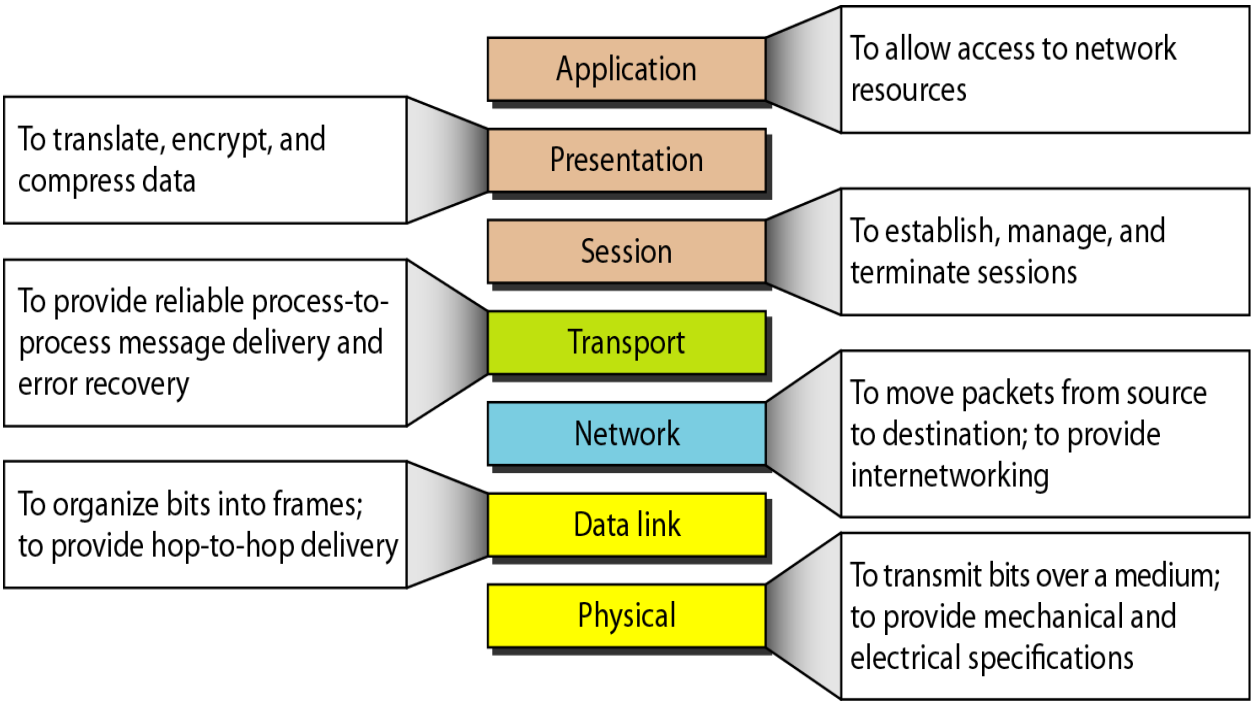
- Ex: Application – Browsers, Skype Messenger etc.
  *Application Layer is also called as Desktop Layer.



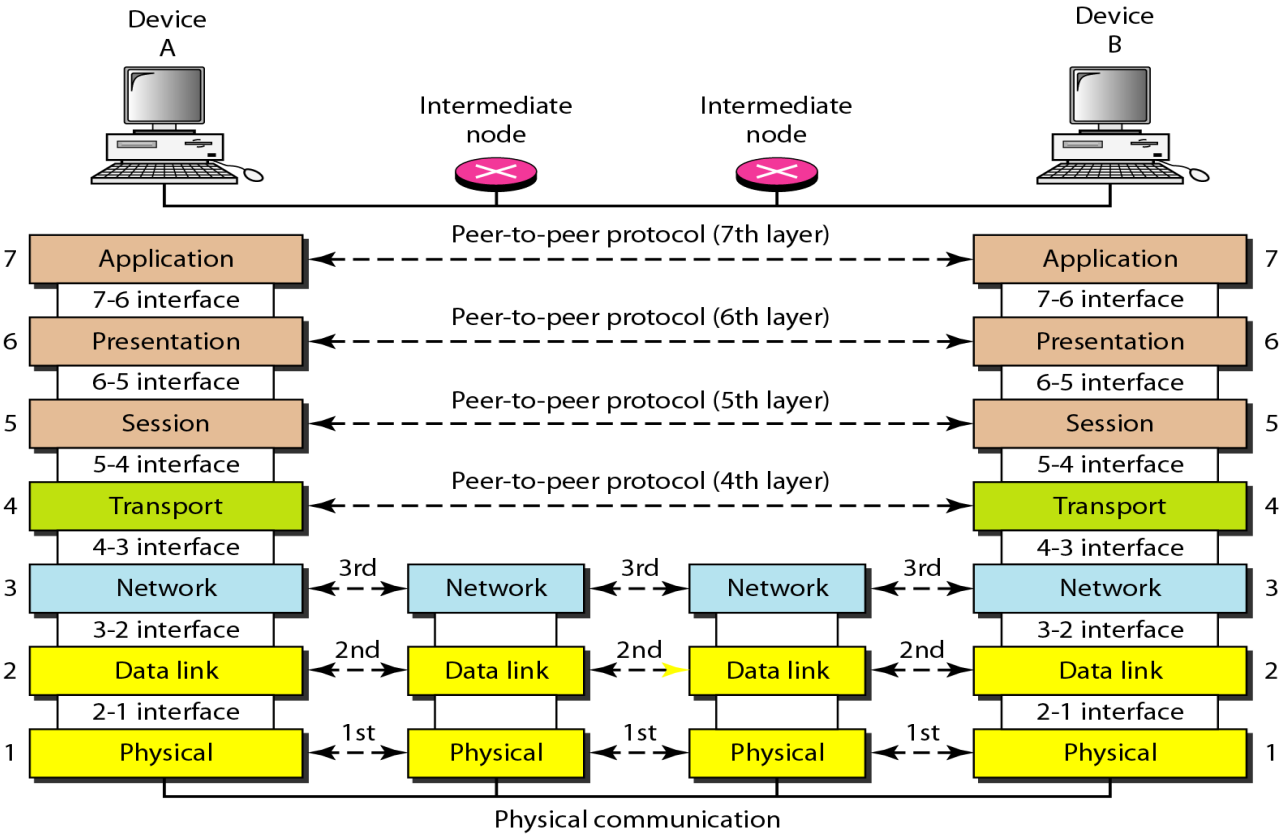
The functions of the Application layer are:

- Network Virtual Terminal
- FTAM-File transfer access and management
- Mail Services
- Directory Services

Summary of ISO/OSI Reference model.

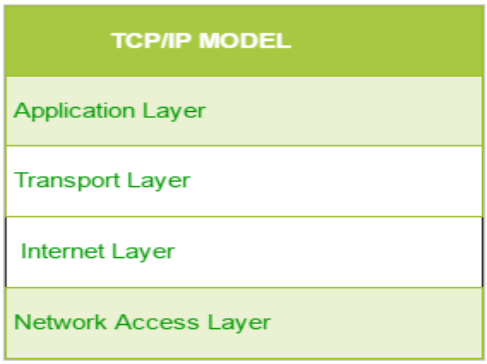


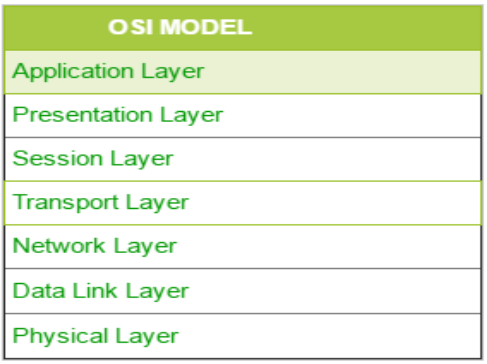
The interaction between layers in the OSI model:



TCP/IP Model:

- The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol.
- The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.
- The layers are:
    - Process/Application Layer
    - Host-to-Host/Transport Layer
    - Internet Layer
    - Network Access/Link Layer





1: Network Access Layer:

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

2: Internet Layer:

- An internet layer is the second layer of the TCP/IP model.

- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Following are the protocols used in this layer are:
- IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU).
- If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network.
- Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol:

- ARP stands for Address Resolution Protocol.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- The two terms are mainly associated with the ARP Protocol:
- **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
- **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its

physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header.

- Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long.
- In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

- In Information and communications technology,

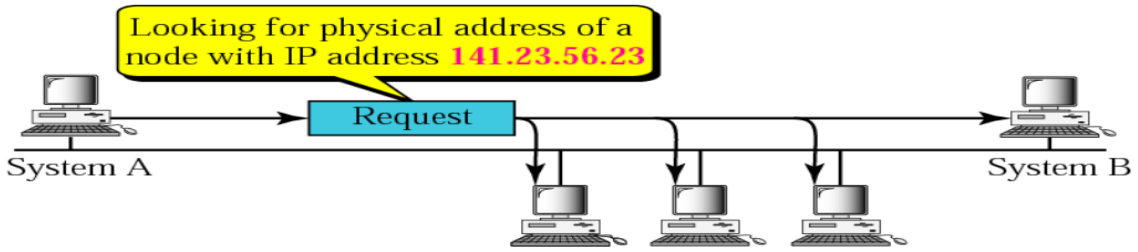
- A **Request for Comments (RFC)** is a type of publication from the technology community. RFCs may come from many bodies including from the

- **Internet Engineering Task Force (IETF)**,

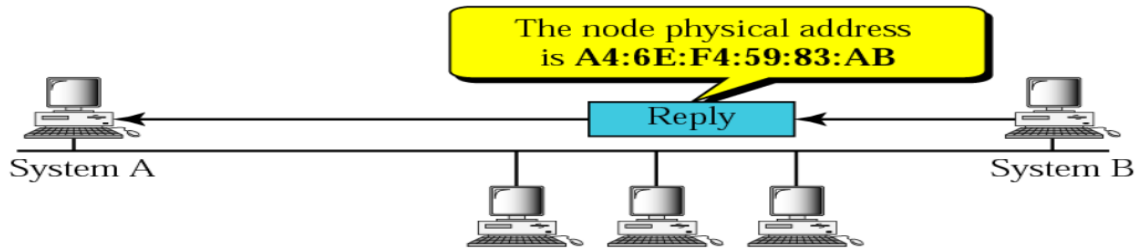
- The **Internet Research Task Force (IRTF)**,

- The **Internet Architecture Board (IAB)** or from independent authors.

- The RFC system is supported by the **Internet Society (ISOC).**



a. ARP request is broadcast



b. ARP reply is unicast

How ARP Works:

- When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address.
- The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.
- If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.
- A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

*There is a Reverse ARP (RARP) for host machines that don't know their IP address. RARP enables them to request their IP address from the gateway's ARP cache.

- The Reverse Address Resolution Protocol (RARP) is an obsolete computer networking protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.
- The client broadcasts the request and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request.
- RARP is described in Internet Engineering Task Force (IETF) publication RFC 903.

ICMP Protocol:

- ICMP stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- ICMP is part of the Internet protocol suite as defined in RFC 792. ICMP messages are typically used for diagnostic or control purposes or generated in response to errors in IP operations (as specified in RFC 1122). ICMP errors are directed to the source IP address of the originating packet.
- Many commonly used network utilities are based on ICMP messages. The trace route command can be implemented by transmitting IP datagrams with specially set IP TTL header fields, and looking for ICMP time exceeded in transit and Destination unreachable messages generated in response.

- The related ping utility is implemented using the ICMP echo request and echo reply messages.

An ICMP protocol mainly uses two terms:

- **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
- **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

3: Transport Layer:

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- UDP consists of the following fields:
- Source port address: The source port address is the address of the application program that has created the message.
- Destination port address: The destination port address is the address of the application program that receives the message.
- Total length: It defines the total number of bytes of the user datagram in bytes.
- Checksum: The checksum is a 16-bit field used in error detection.
- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

Transmission Control Protocol (TCP):

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.

- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

4: Application Layer:

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.