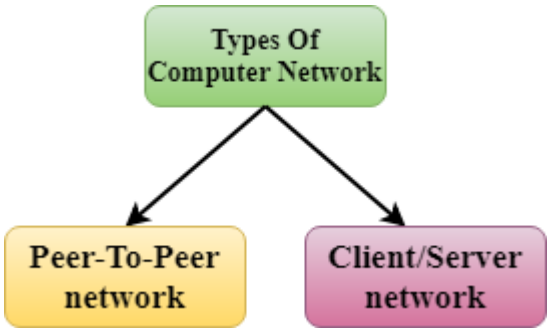
Topic 1: Computer Network Architecture

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

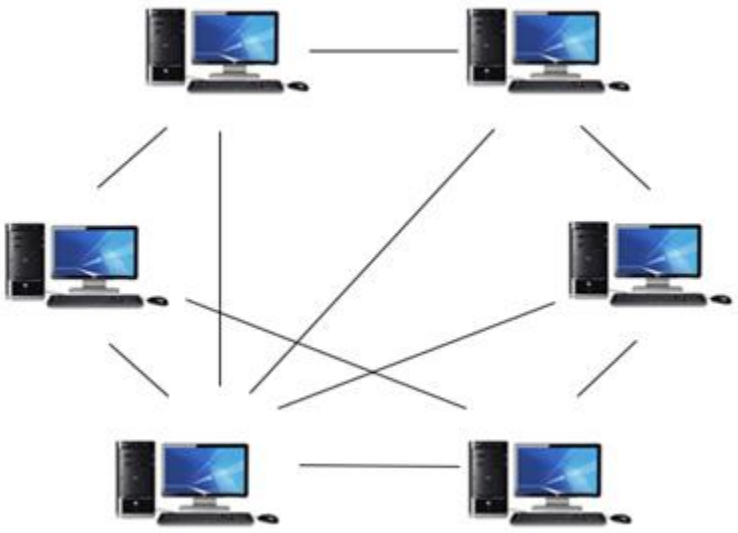
The two types of network architectures are used:



- Peer-To-Peer network
- Client/Server network

Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages of Peer-To-Peer Network:

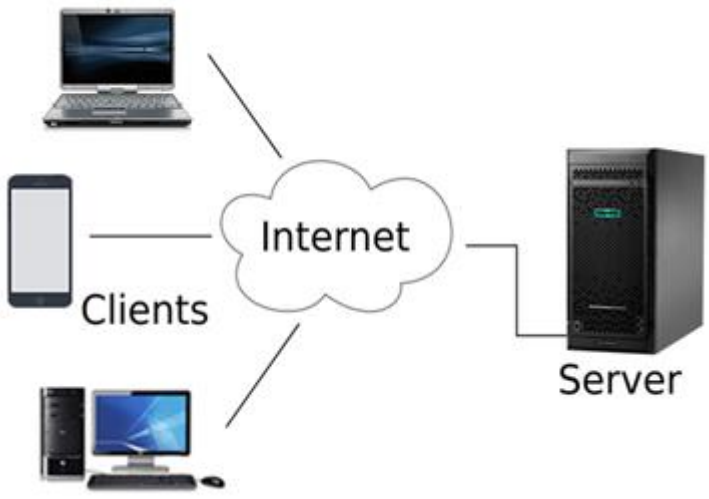
- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages of Client/Server network:

- A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Topic 2: PHYSICAL TRANSMISSION MEDIA

PHYSICAL TRANSMISSION MEDIA

Physical transmission media used in communications include twisted-pair cable, coaxial cable, and fiber-optic cable. These cables typically are used within or underground between buildings. Ethernet and token ring LANs often use physical transmission media.

Twisted-Pair Cable

One of the more commonly used transmission media for network cabling and telephone systems is twisted-pair cable. **Twisted-pair cable** consists of one or more twisted-pair wires bundled together (Figure 8-24). Each twisted-pair wire consists of two separate insulated copper wires that are twisted together. The wires are twisted together to reduce noise. **Noise** is an electri- cal disturbance that can degrade communications.

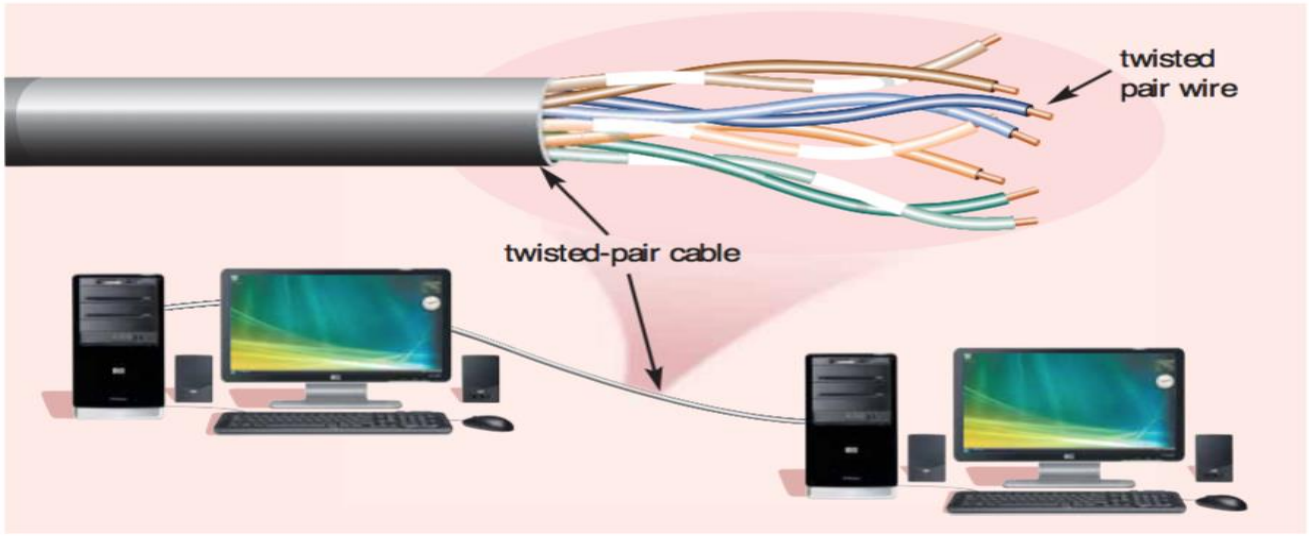


FIGURE 8-24 A twisted-pair cable consists of one or more twisted-pair wires. Each twisted-pair wire usually is color coded for identification.

Coaxial Cable

Coaxial cable, often referred to as coax (pronounced KO-ax), consists of a single copper wire surrounded by at least three layers: (1) an insulating material, (2) a woven or braided metal, and (3) a plastic outer coating (Figure 8-25).

Cable television (CATV) network wiring often uses coaxial cable because it can be cabled over longer distances than twisted-pair cable. Most of today's computer networks, however, do not use coaxial cable because other transmission media such as fiber-optic cable transmit signals at faster rates.

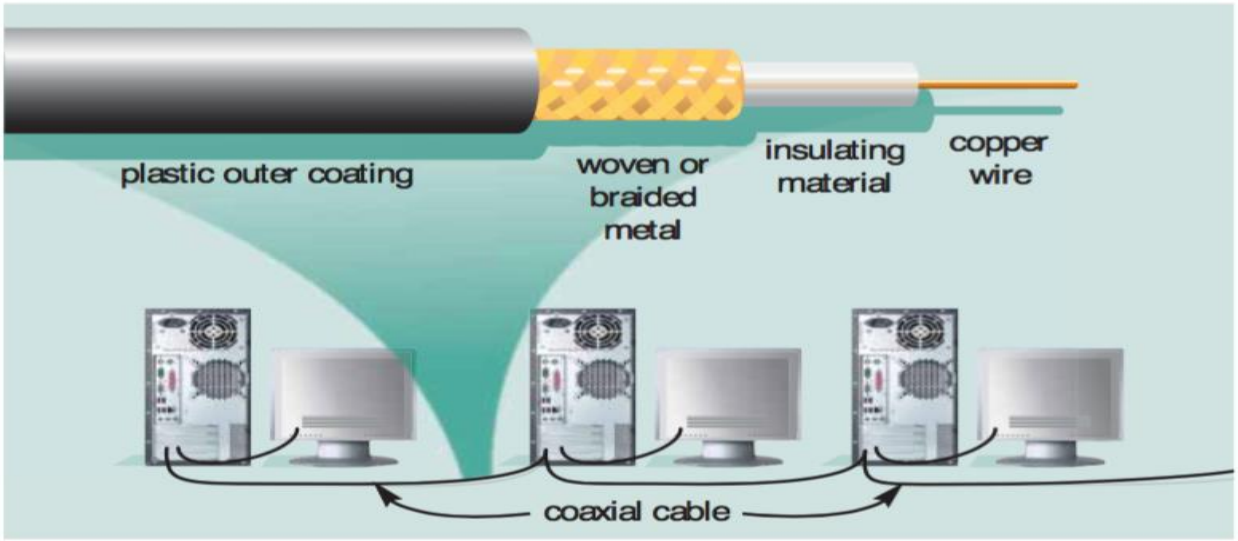


FIGURE 8-25 On a coaxial cable, data travels through a copper wire. This illustration shows computers networked together with coaxial cable.

Fiber-Optic Cable

The core of a **fiber-optic cable** consists of dozens or hundreds of thin strands of glass or plastic that use light to transmit signals. Each strand, called an optical fiber, is as thin as a human hair. Inside the fiber-optic cable, an insu- lating glass cladding and a protective coating surround each optical fiber (Figure 8-26).

Fiber-optic cables have the following advantages over cables that use wire, such as twisted-pair and coaxial cables:

- Capability of carrying significantly more signals than wire cables
- Faster data transmission
- Less susceptible to noise (interference) from other devices such as a copy machine
- Better security for signals during transmission because they are less susceptible to noise
- Smaller size (much thinner and lighter weight)

Disadvantages of fiber-optic cable are it costs more than twisted-pair or coaxial cable and can be difficult to install and modify. Despite these limitations, many local and long- distance telephone companies are replacing existing telephone lines with fiber-optic cables, enabling them to offer fiber Internet access to home and business users.

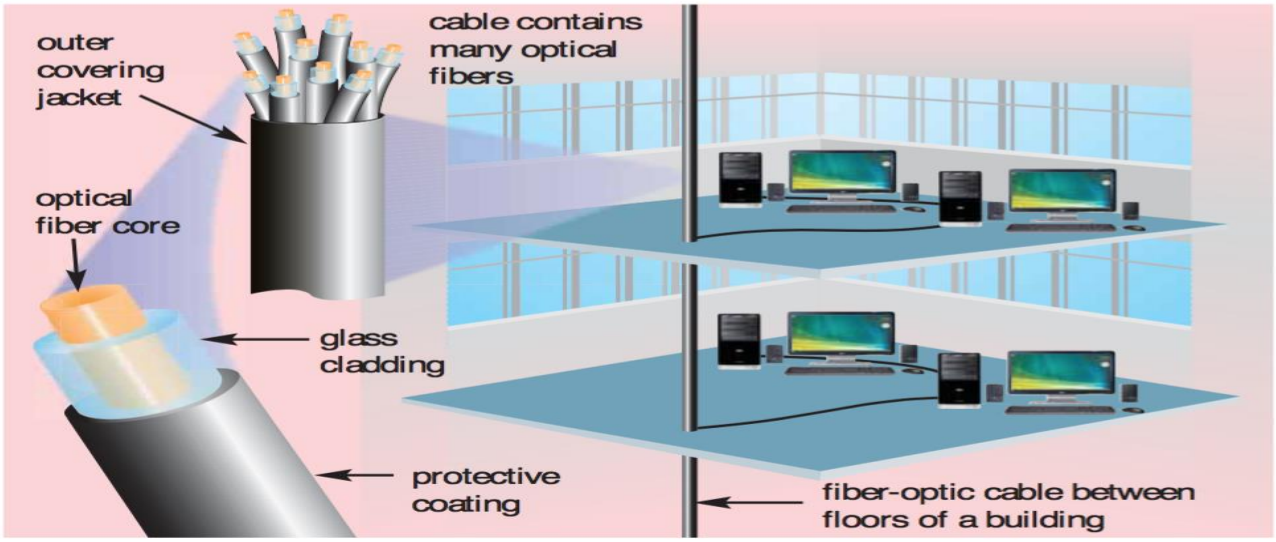


FIGURE 8-26 A fiber-optic cable consists of hair-thin strands of glass or plastic that carry data as pulses of light.

Topic 3: WIRELESS TRANSMISSION MEDIA

Many users opt for wireless transmission media because it is more convenient than installing cables. In addition, businesses use wireless transmission media in locations where it is impossible to install cables. Types of wireless transmission media used in communications include infrared, broadcast radio, cellular radio, microwaves, and communications satellites.

Infrared

As discussed earlier in the chapter, infrared (IR) is a wireless transmission medium that sends signals using infrared light waves. Mobile computers and devices, such as a mouse, printer, and smart phone, often have an IrDA port that enables the transfer of data from one device to another using infrared light waves.

Broadcast Radio

Broadcast radio is a wireless transmission medium that distributes radio signals through the air over long distances such as between cities, regions, and countries and short distances such as within an office or home. Bluetooth, UWB, Wi-Fi, and WiMAX communications technologies discussed earlier in this chapter use broadcast radio signals.

Cellular Radio

Cellular radio is a form of broadcast radio that is used widely for mobile communications, specifically wireless modems and cell phones. A cell phone is a telephone device that uses high-frequency radio waves to transmit voice and digital data messages.

Some mobile users connect their notebook computer or other mobile computer to a cell phone to access the Web, send and receive e-mail, enter a chat room, or connect to an office or school network while away from a standard telephone line. Read Looking Ahead 8-2 for a look at the next generation of cellular communications.

Personal Communications Services (**PCS**) is the term used by the United States Federal Communications Commission (FCC) to identify all wireless digital communications. Devices that use PCS include cell phones, PDAs, pagers, and fax machines.

Microwaves

Microwaves are radio waves that provide a high-speed signal transmission. Microwave transmission, often called fixed wireless, involves sending signals from one microwave station to another (shown in Figure 8-1 on page 296). Microwaves can transmit data at rates up to 4,500 times faster than a dial-up modem.

A microwave station is an earth-based reflective dish that contains the antenna, transceivers, and other equipment necessary for microwave communications. Microwaves use line-of-sight transmission. To avoid possible obstructions, such as buildings or mountains, microwave stations often sit on the tops of buildings, towers, or mountains.

Microwave transmission is used in environments where installing physical transmission media is difficult or impossible and where line-of-sight transmission is available. For example, microwave transmission is used in wide-open areas such as deserts or lakes; between buildings in a close geo- graphic area; or to communicate with a satellite. Current users of microwave transmission include universities, hospitals, city governments, cable television providers, and telephone companies. Home and small business users who do not have other high-speed Internet connections available in their area also opt for lower-cost fixed wireless plans.

Communications Satellite

A **communications satellite** is a space station that receives microwave signals from an earth-based station, amplifies (strengthens) the signals, and broadcasts the signals back over a wide area to any number of earth-based stations.

These earth-based stations often are microwave stations. Other devices, such as smart phones and GPS receivers, also can function as earth-based stations. Transmission from an earth-based station to a satellite is an uplink. Transmission from a satellite to an earth-based station is a downlink.

Applications such as air navigation, television and radio broadcasts, weather forecasting, video conferencing, paging, global positioning systems, and Internet connections use communications satellites. With the proper satellite dish and a satellite modem card, consumers access the Internet using satellite technology. With satellite Internet connections, however, uplink transmissions usually are slower than downlink transmissions. This difference in speeds usually is acceptable to most Internet satellite users because they download much more data than they upload. Although a satellite Internet connection is more expensive than cable Internet or DSL connections, sometimes it is the only high-speed Internet option in remote areas.

Topic 4: Making Ethernet Cables

HOW TO MAKE AN ETHERNET CABLE

Purchasing Ethernet cables can be quite expensive and pre-made lengths are not always the length you need. Making Ethernet cables is easy with a box of bulk Category 5e Ethernet cable and RJ-45 connectors that are attached to the cut ends of your preferred cable length.

Bulk Ethernet Cable - Category 5e or CAT5e

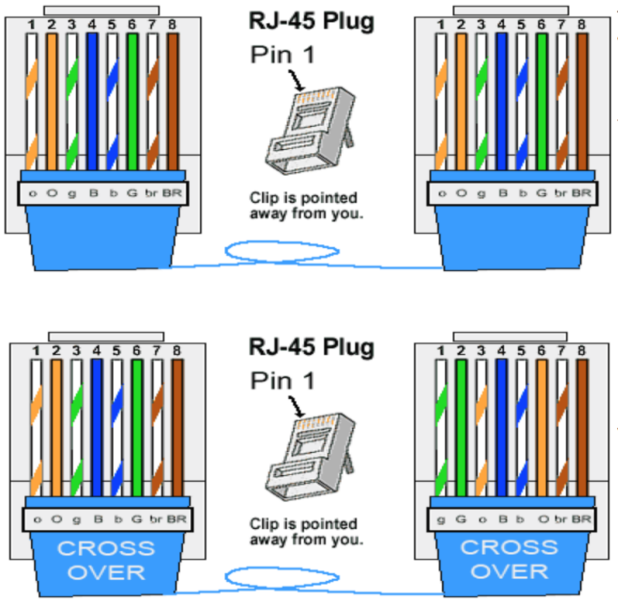
(You may also use Category 6 or CAT6 cabling which has higher performance specifications and is about 20% more expensive than CAT5e.)

Bulk RJ45 Crimpable Connectors for CAT-5e
or
Bulk RJ45 Crimpable Connectors for CAT-6

RJ-45 Crimping tool

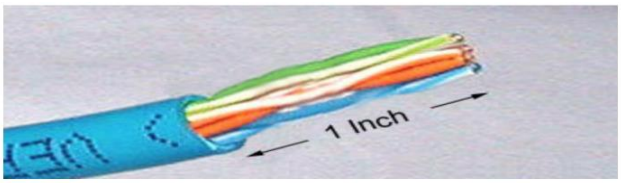
There are two kinds of Ethernet cables you can make, **Straight**

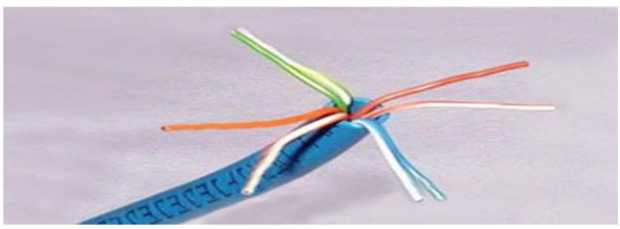
Through and **Crossover**.



STRAIGHT THROUGH Ethernet cables are the standard cable used for almost all purposes, and are often called "patch cables". It is highly recommending you duplicate the color order as shown on the left. Note how the green pair is not side-by-side as are all the other pairs. This configuration allows for longer wire runs.

CROSSOVER CABLES - The purpose of a Crossover Ethernet cable is to directly connect one computer to another computer (or device) without going through a router, switch or hub.





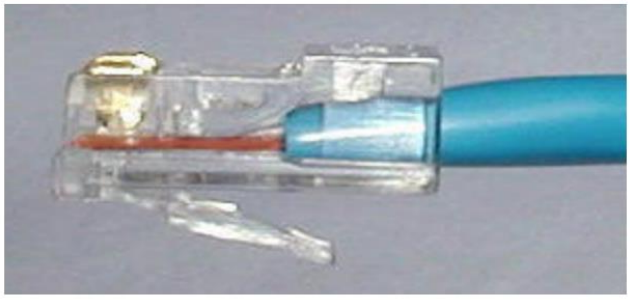
Here's how to make a standard cable:

Cut into the plastic sheath about **1 inch** (2.5 cm) from the end of the cut cable. The crimping tool has a razor blade that will do the trick with practice.

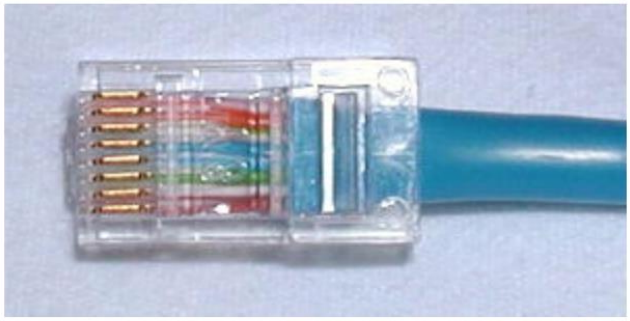
Unwind and pair the similar colors.

Pinch the wires between your fingers and straighten them out as shown. The color order is important to get correct.

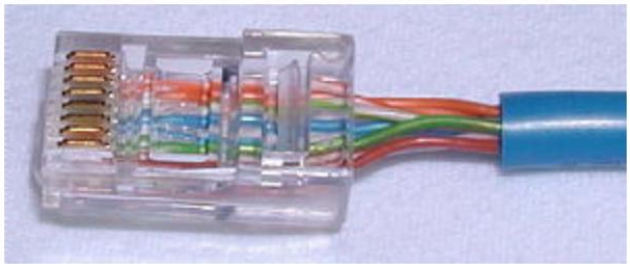
Use scissors to make a straight cut across the 8 wires to shorten them to **1/2 Inch** (1.3 cm) from the cut sleeve to the end of the wires.



Carefully push all 8 unstripped colored wires into the connector. Note the position of the blue plastic sleeve. Also note how the wires go all the way to the end.

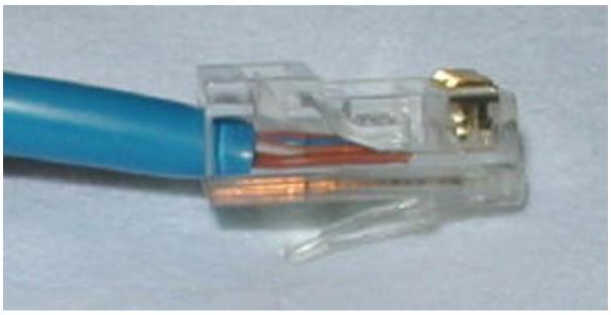


A view from the top. All the wires are all the way in. There are no short wires.



WRONG WAY - Note how the blue plastic sleeve is not inside the connector where it can be locked into place. The wires are too long. The wires should extend only 1/2 inch from the blue cut sleeve.

WRONG WAY - Note how the wires do not go all the way to the end of the connector.



CRIMPING THE CABLE ... carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There is also a locking tab that holds the blue plastic sleeve in place for a tight compression fit. When you remove the cable from the crimper, that end is ready to use.

For a standard "Straight Through" cable, repeat all steps and wire color order on the other end of cable. For a cross-over cable, the other end will have a different color order as shown by the crossover picture above.

Topic 5: Computer Network Components

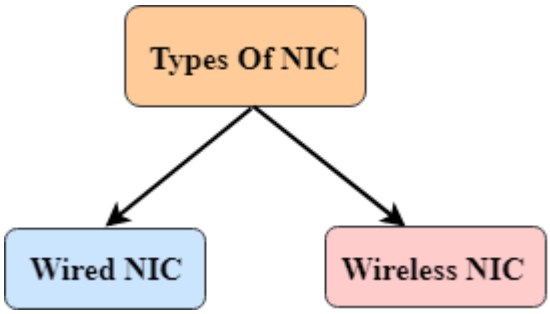
Computer network components are the *major parts* which are needed to *install the software*. Some important network components are **NIC**, **switch**, **cable**, **hub**, **router**, and **modem**. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

Following are the major components required to install a network:

NIC

- NIC stands for network interface card.
- NIC is a hardware component used to connect a computer with another computer onto a network
- It can support a transfer rate of 10,100 to 1000 Mb/s.
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

There are two types of NIC:



1. Wired NIC
2. Wireless NIC

Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

Wireless NIC: The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

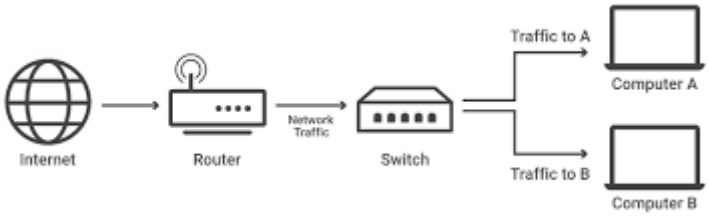
Hub

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switch

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.



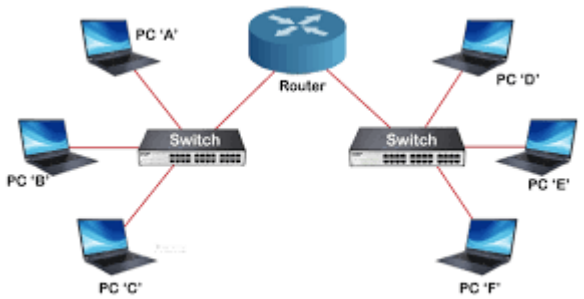
Router

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Advantages of Router:

- **Security:** The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.

- **Reliability:** If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
- **Performance:** Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic. This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.
- **Network range**



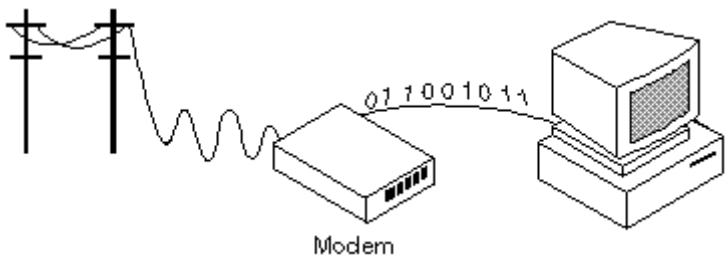
Connection of networks through Router

Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

- Standard PC modem or Dial-up modem
- Cellular Modem
- Cable modem



Cables and Connectors

Cable is a transmission media used for transmitting a signal.

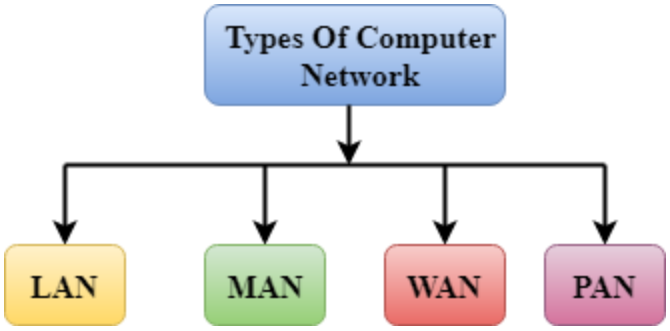
There are three types of cables used in transmission:

- Twisted pair cable
- Coaxial cable
- Fibre-optic cable

Topic 6: Computer Network Types

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

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



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

LAN(Local Area Network)

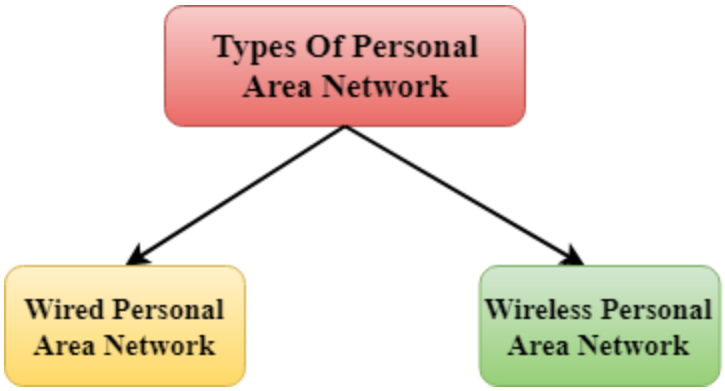
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware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

- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

PAN(Personal Area Network)

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

There are two types of Personal Area Network:



- Wired Personal Area Network
- Wireless Personal Area Network

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

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

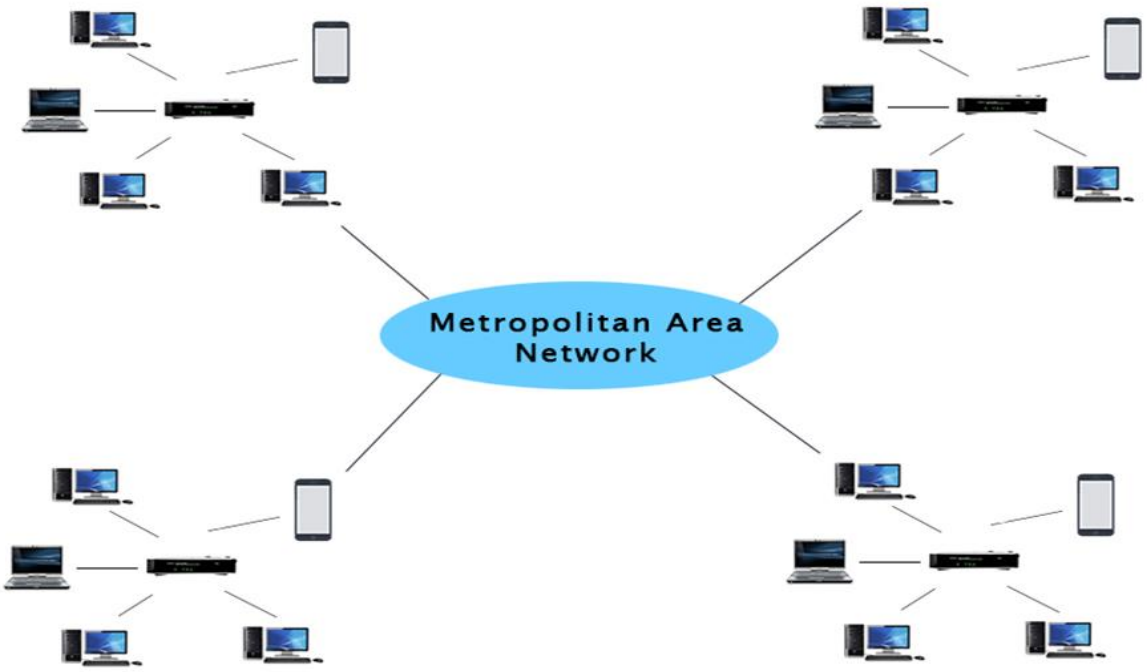
Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.

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

MAN(Metropolitan Area Network)

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



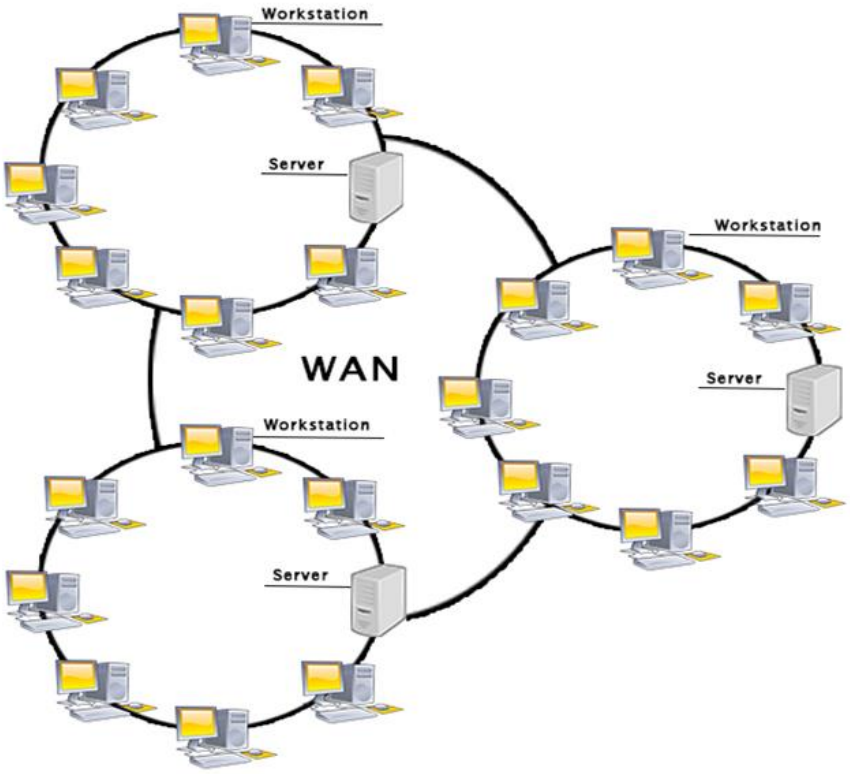
Uses of Metropolitan Area Network:

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

- It can also be used for communication in the military.

WAN (Wide Area Network)

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



Examples of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages of Wide Area Network:

Following are the advantages of the Wide Area Network:

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

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

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

Types of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

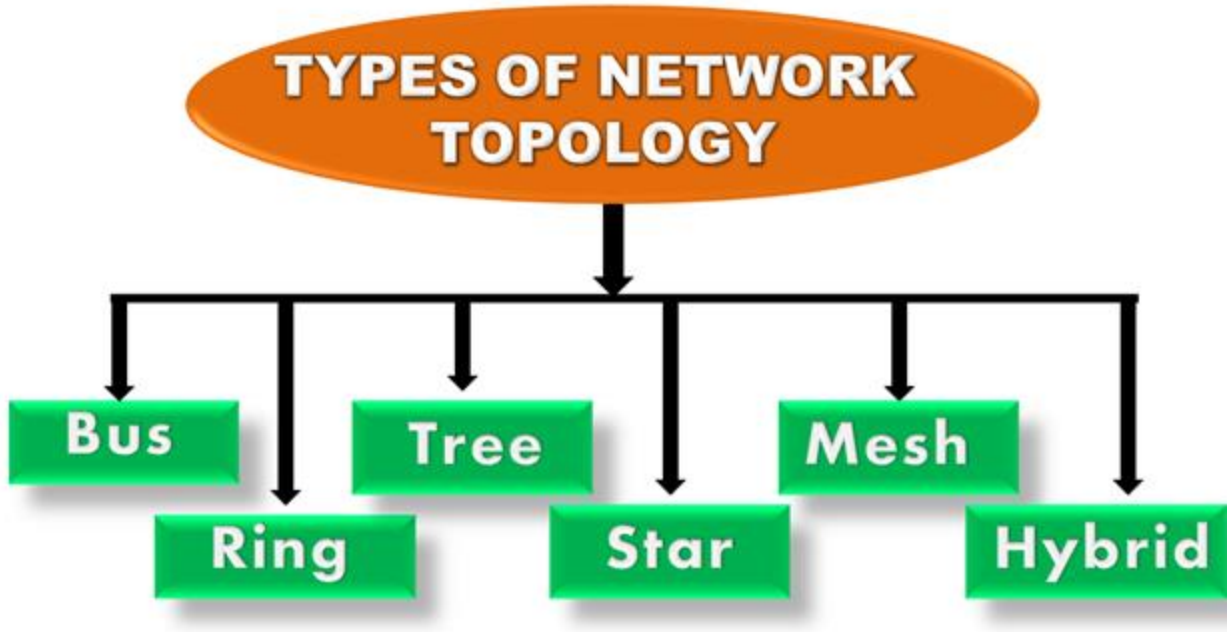
- **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
- **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
- **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
- **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
- **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

Topic 7: What is Network Topology?

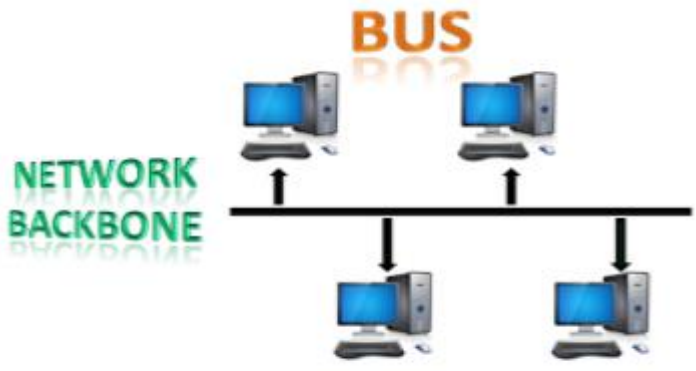
Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Types of Network Topology

Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.



1) Bus Topology



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.

- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA: CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

---

2) Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
    - **Token passing:** It is a network access method in which token is passed from one node to another node.
    - **Token:** It is a frame that circulates around the network.

Working of Token passing

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

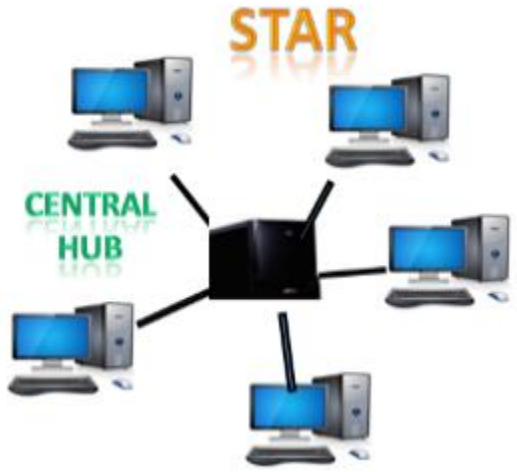
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

---

3) Star Topology



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.

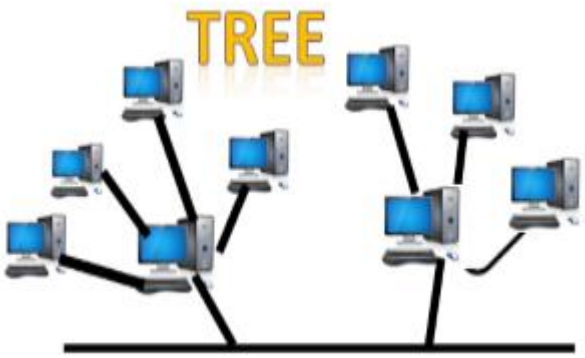
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

---

4) Tree topology



- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.

- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

---

5) Mesh topology

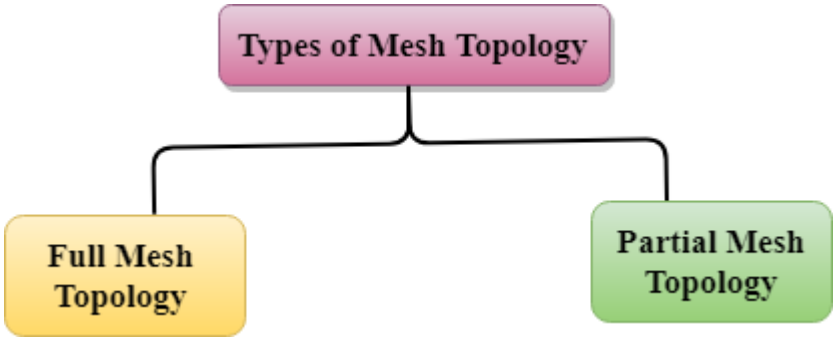
- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.

- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;**

Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology



- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

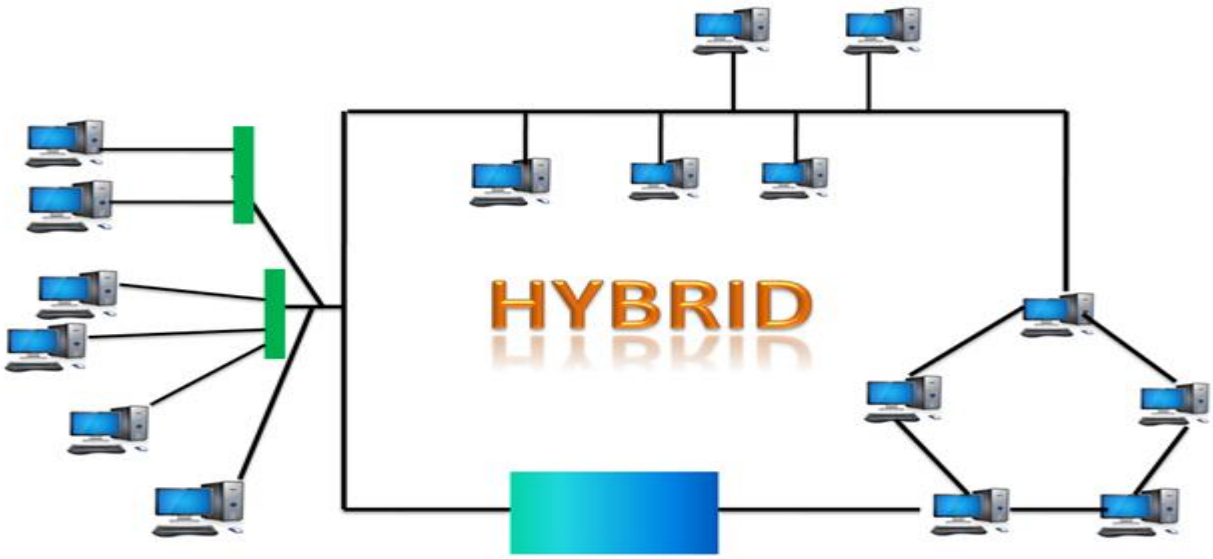
Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.

- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

---

6) Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.

- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

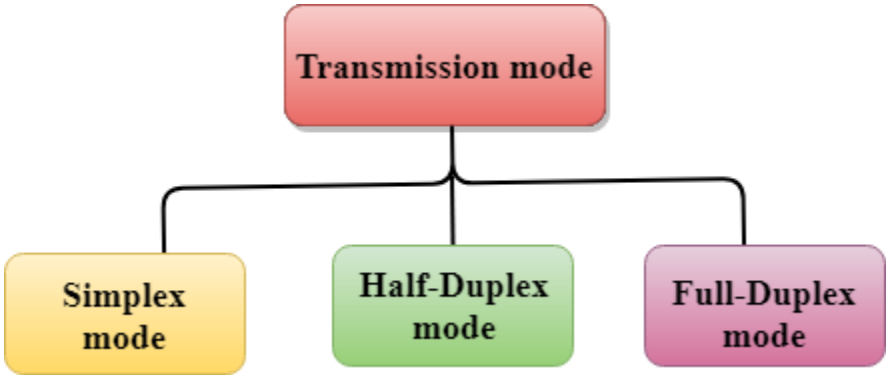
Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Topic 8: Transmission modes

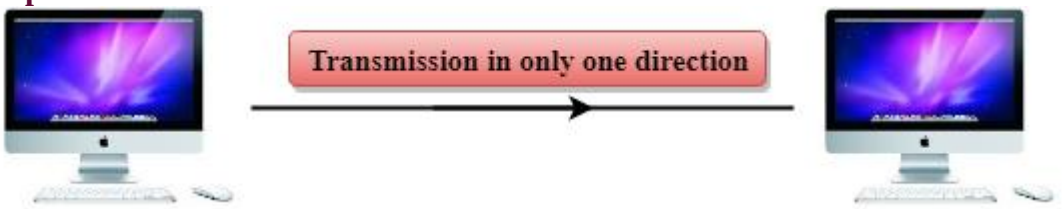
- The way in which data is transmitted from one device to another device is known as **transmission mode**.
- The transmission mode is also known as the communication mode.
- Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The transmission mode is defined in the physical layer.

The Transmission mode is divided into three categories:



- Simplex mode
- Half-duplex mode
- Full-duplex mode

Simplex mode



- In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
- This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.
- The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
- Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.
- The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.

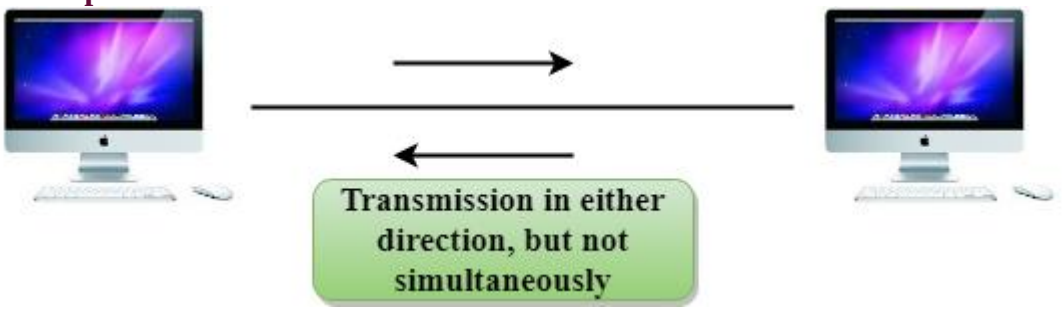
Advantage of Simplex mode:

- In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

Disadvantage of Simplex mode:

- Communication is unidirectional, so it has no inter-communication between devices.

Half-Duplex mode



- In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
- Messages flow in both the directions, but not at the same time.
- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
- A **Walkie-talkie** is an example of the Half-duplex mode. In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.

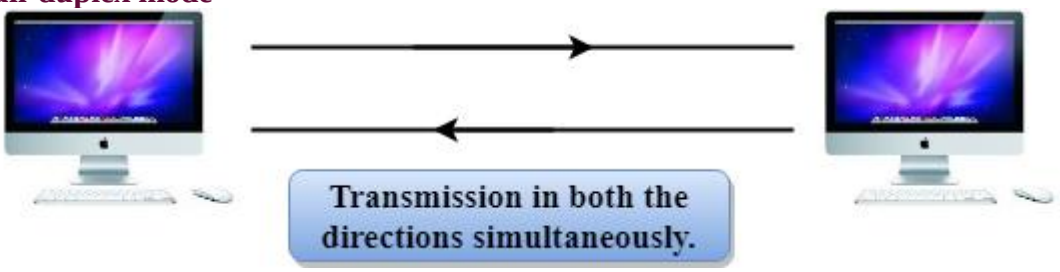
Advantage of Half-duplex mode:

- In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

- In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

Full-duplex mode



- In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.
- Both the stations can send and receive the message simultaneously.
- Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
- The Full-duplex mode is the fastest mode of communication between devices.
- The most common example of the full-duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

Advantage of Full-duplex mode:

- Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

- If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

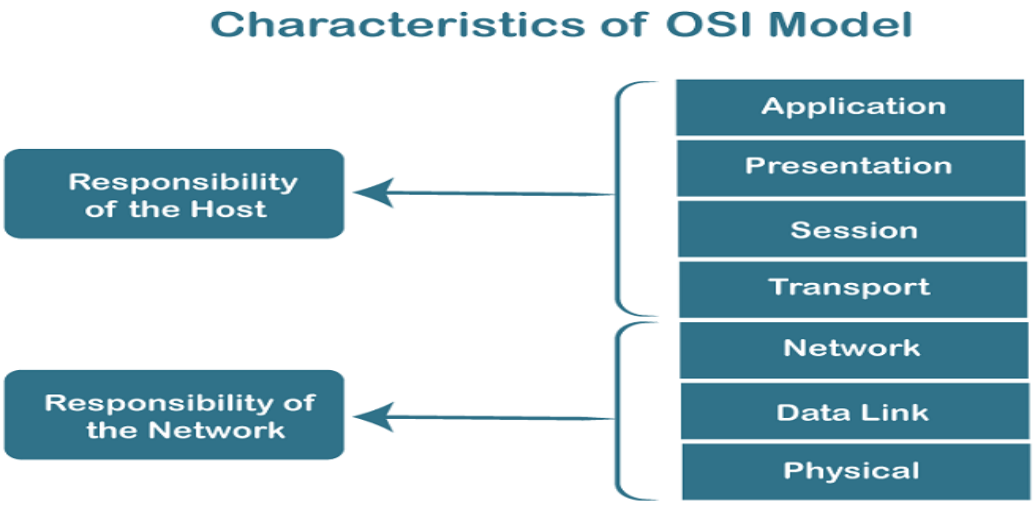
Differences b/w Simplex, Half-duplex and Full-duplex mode

Basis for comparison	Simplex mode	Half-duplex mode	Full-duplex mode
Direction of communication	In simplex mode, the communication is unidirectional.	In half-duplex mode, the communication is bidirectional, but one at a time.	In full-duplex mode, the communication is bidirectional.
Send/Receive	A device can only send the data but cannot receive it or it can only receive the data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
Performance	The performance of half-duplex mode is better than the simplex mode.	The performance of full-duplex mode is better than the half-duplex mode.	The Full-duplex mode has better performance among simplex and half-duplex mode as it doubles the utilization of the capacity of the communication channel.
Example	Examples of Simplex mode are radio, keyboard, and monitor.	Example of half-duplex is Walkie-Talkies.	Example of the Full-duplex mode is a telephone network.

Topic 9: OSI Model

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

Characteristics of OSI Model:

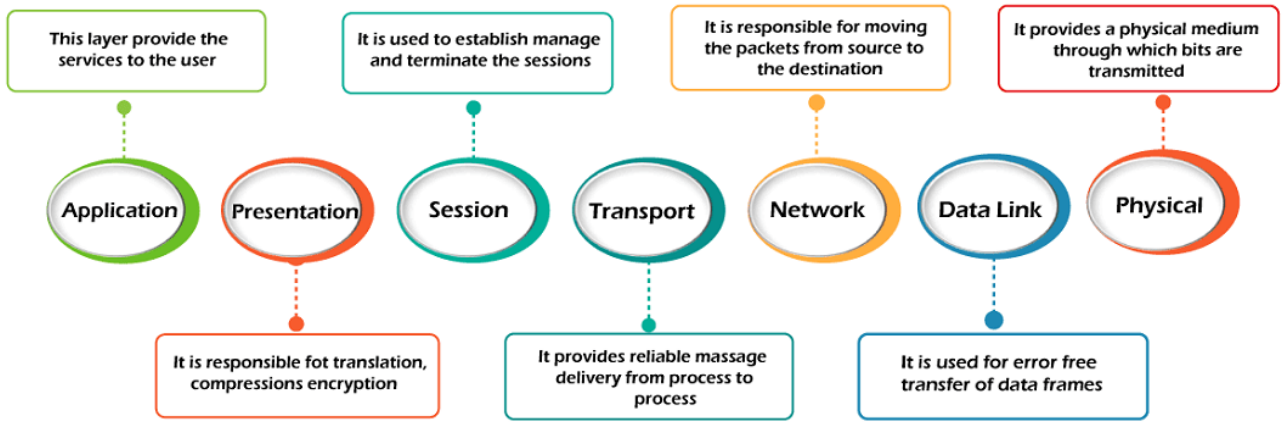


- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

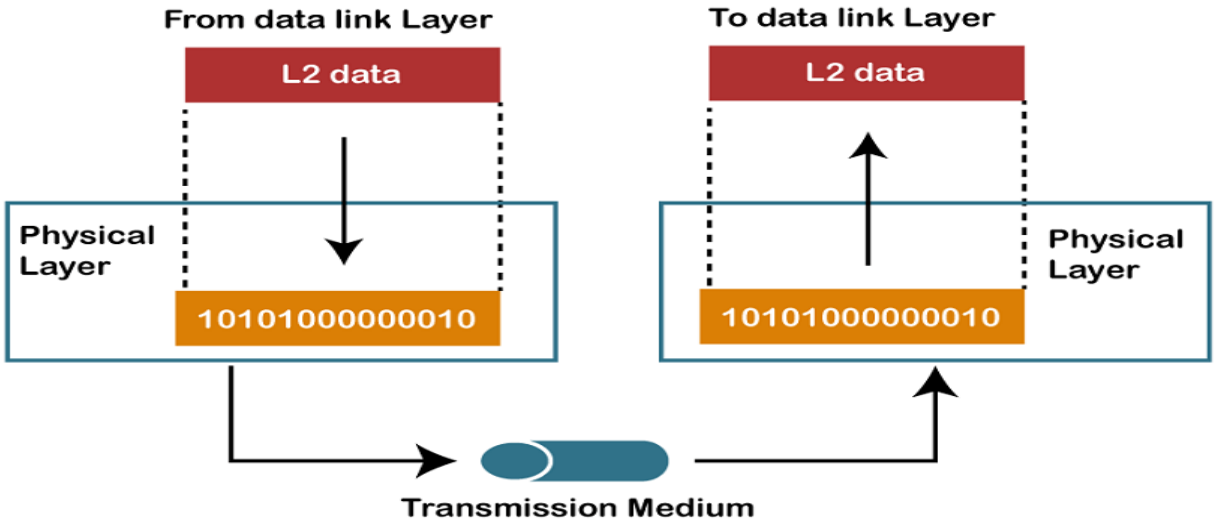
7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

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



1) Physical layer



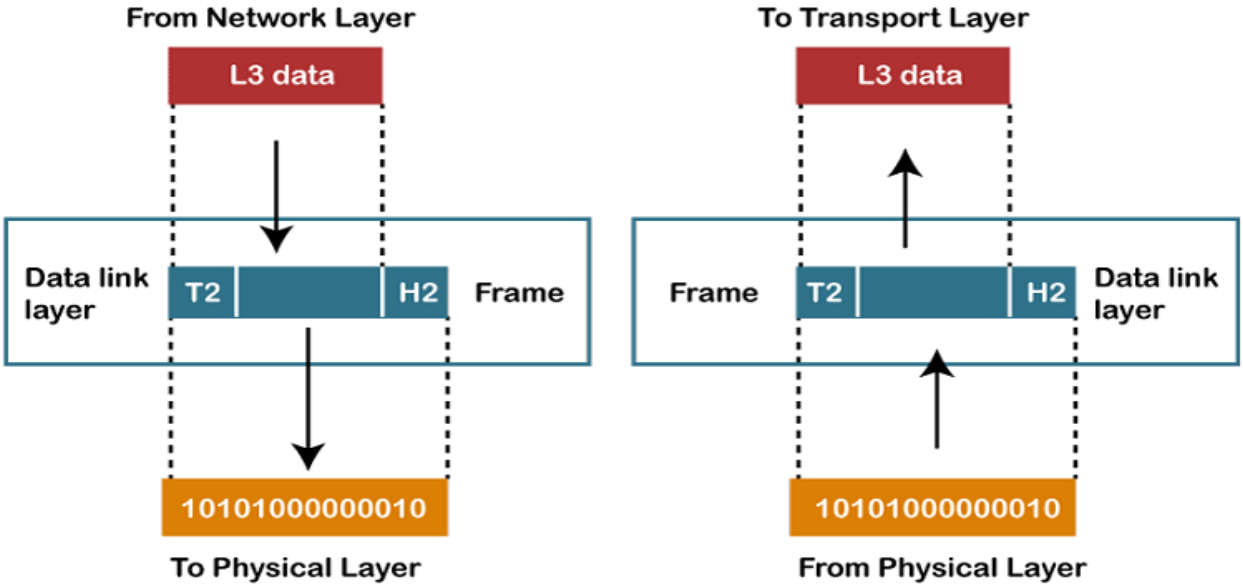
- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.

- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

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

2) Data-Link Layer



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

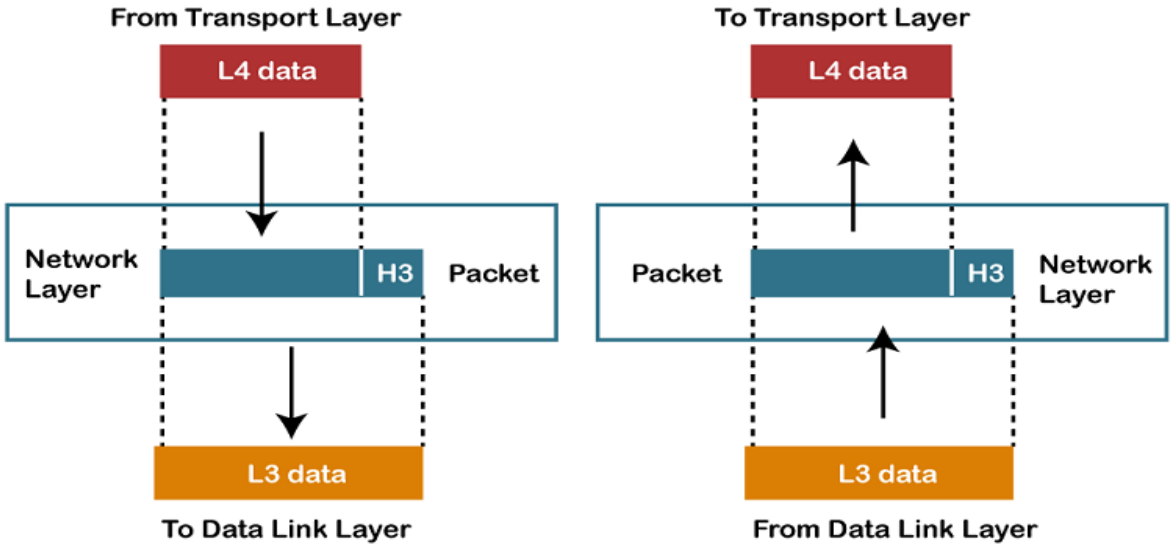
- **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

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

3) Network Layer

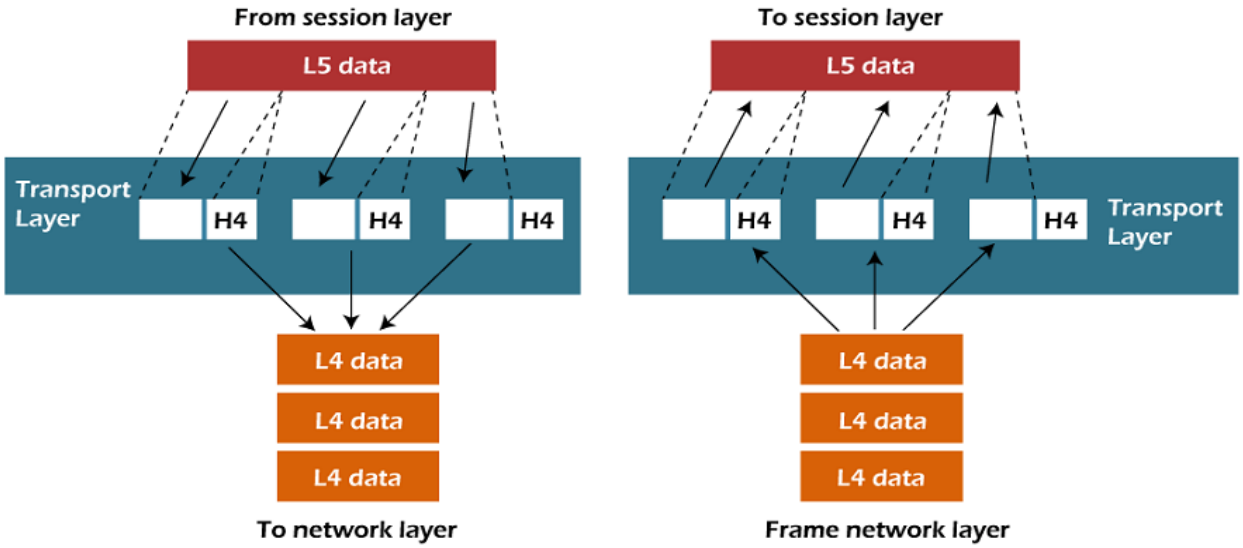


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

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

4) Transport Layer



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

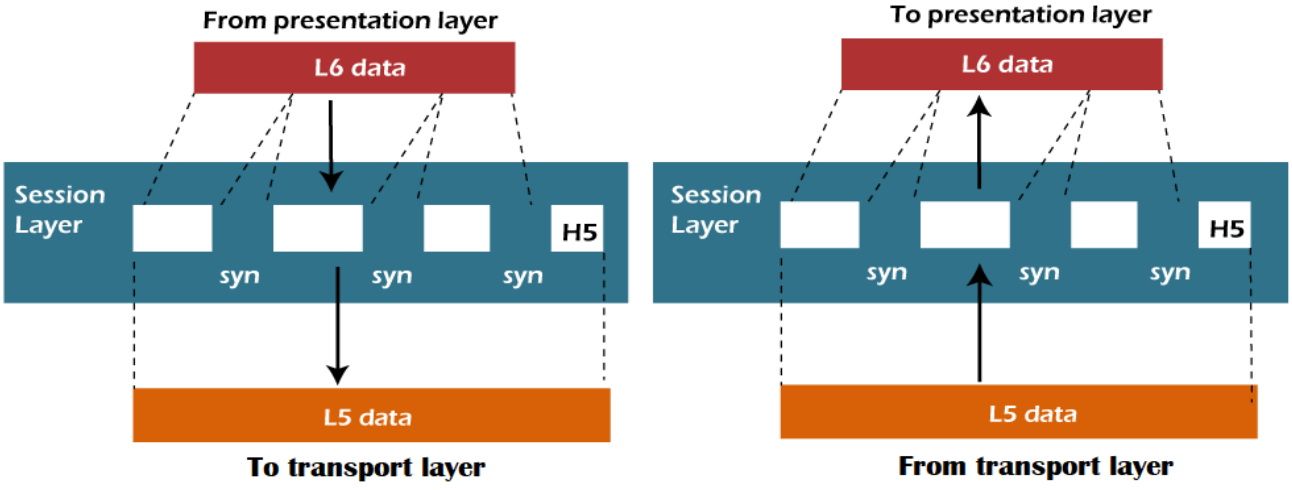
The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5) Session Layer

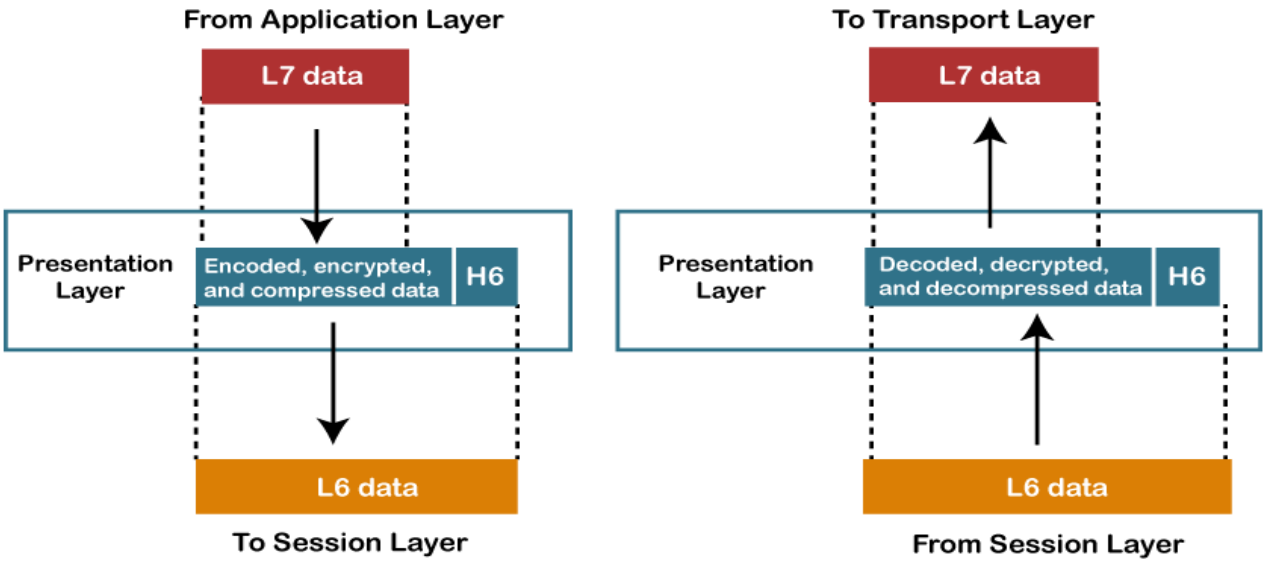


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

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

6) Presentation Layer



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

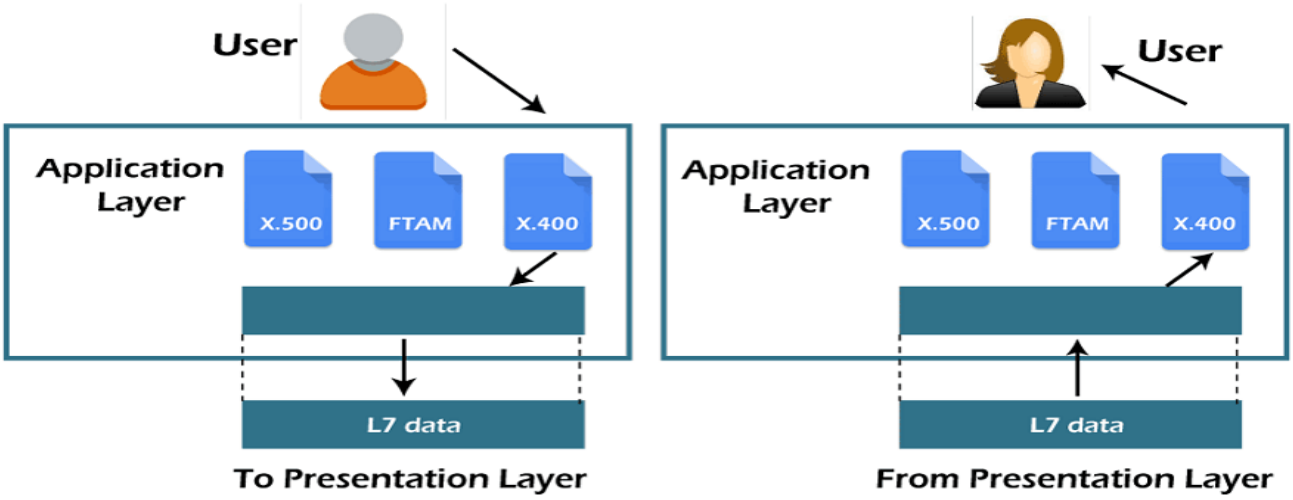
Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different

encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

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

7) Application Layer



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

Functions of Application layer:

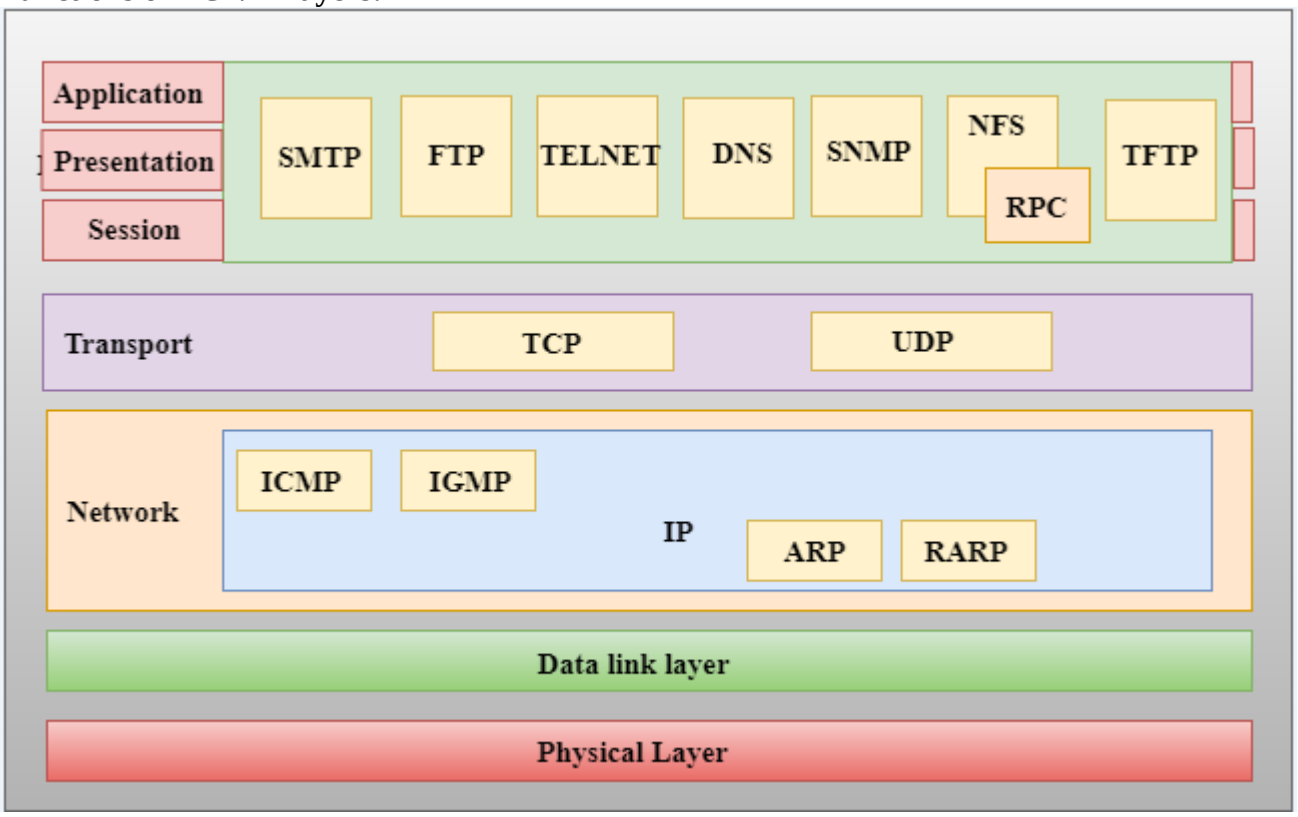
- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and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

Topic 10: TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.

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

Internet Layer

- 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

ICMP Protocol

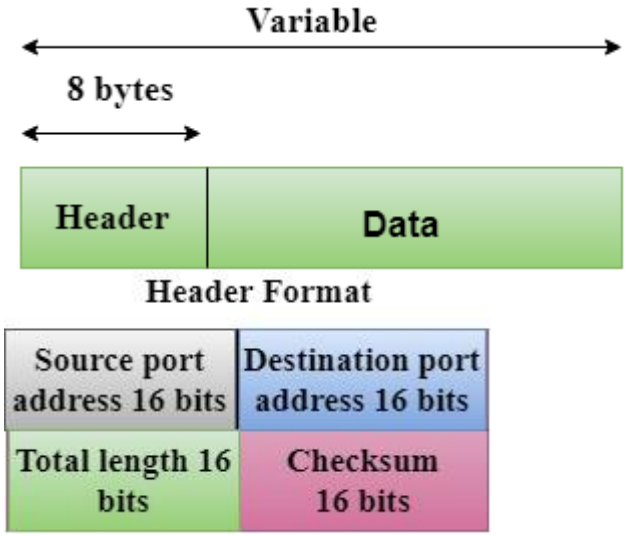
- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because 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.
- 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.

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.

Application Layer

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

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.

- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote 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.

Physical Layer

Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types of Guided media:

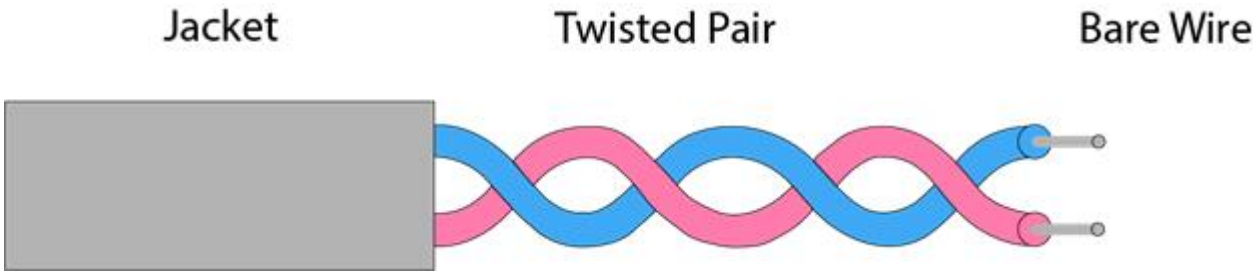
Twisted pair:

Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

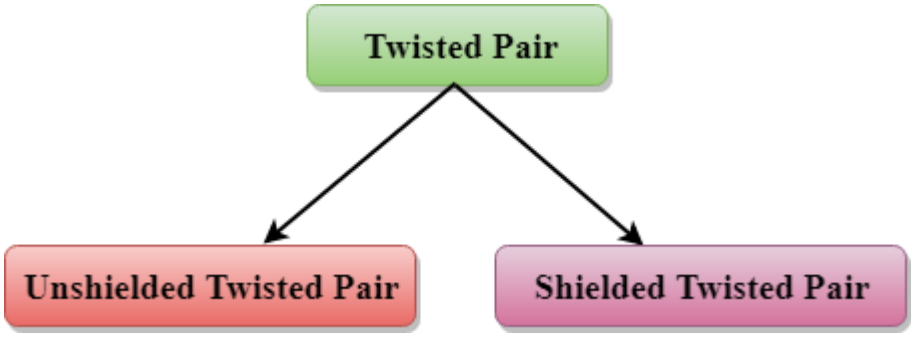
A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

Play Video

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.

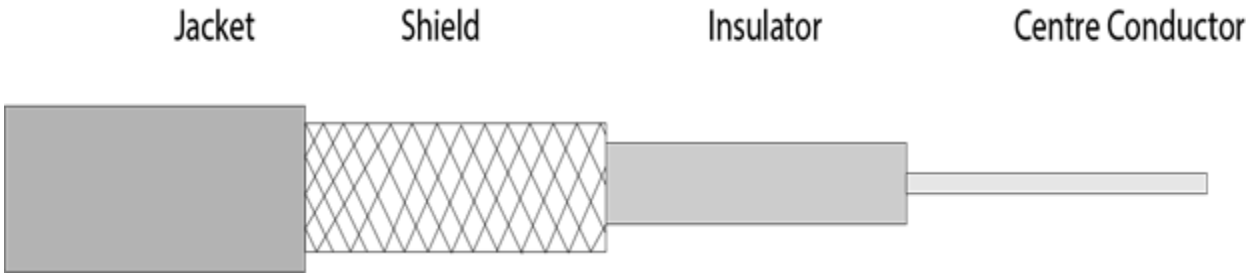
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

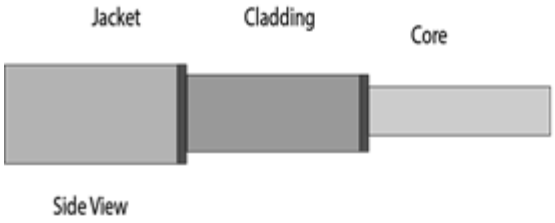
Disadvantages Of Coaxial cable:

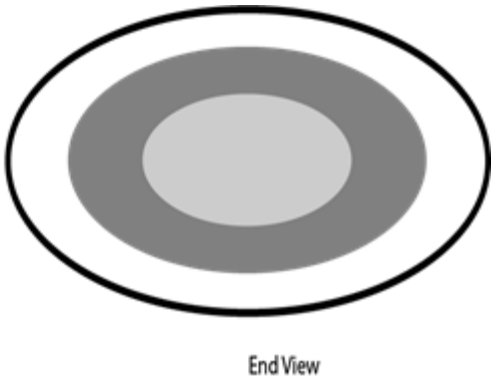
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

Fibre Optic

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:





Basic elements of Fibre optic cable:

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the

core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.

- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.