MALLA REDDY UNIVERSITY,HYDERABAD

L/T/P/C MR22–1ES0104 2/-/2/3

Adaptive Computer Technologies

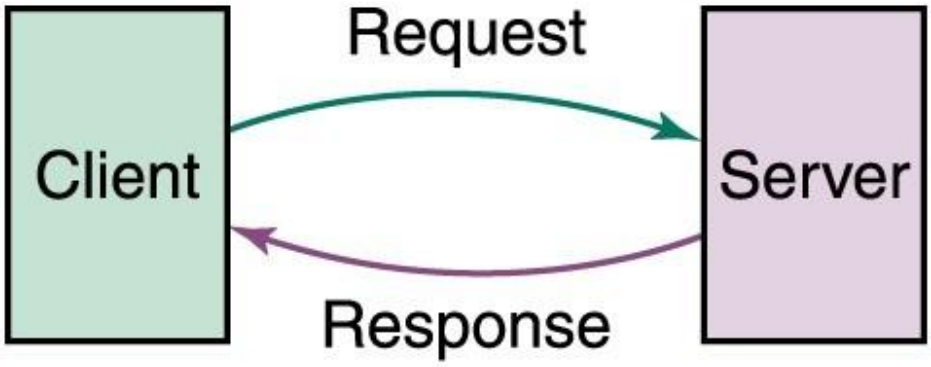
UNIT-I: Computer Networks and the Internet

Introduction to Computer Networks, Advantages of Computer Networks

A network: A group of devices that can communicate with each other over links. Each device is called a host. Each host has a unique address.

Computer networks are a set of interconnected devices, such as computers, printers, servers, and other network devices, that allow the sharing of resources and information. Networks can be categorized by their size, such as local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs).

Example:



Advantages of computer networks include:

- Resource sharing: With a computer network, resources such as printers, files, and databases can be shared among multiple users, reducing the need for duplicate resources and increasing efficiency.
- Communication: Networks allow users to communicate with each other through email, instant messaging, and video conferencing.
- Cost savings: Sharing resources on a network can save money by reducing the need for multiple devices or licenses.
- Centralized management: Networks can be managed centrally, making it easier to apply updates, configure security settings, and monitor usage.
- Improved security: Networks can be secured with firewalls, antivirus software, and other security measures, making it more difficult for unauthorized users to access resources.
- Increased flexibility: Networks allow users to access resources from any location, as long as they have the necessary permissions and network connectivity.
- Scalability: Networks can be scaled up or down depending on the needs of the organization, making it easier to adapt to changing requirements.

Explain the characteristics of computer networks:

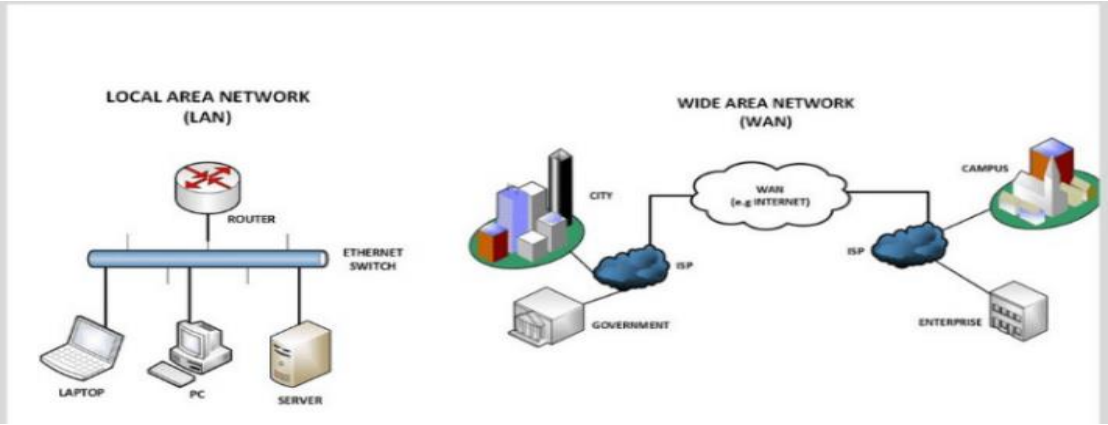
- Connectivity: Computer networks enable devices to connect and communicate with one another, allowing users to share resources such as data, printers, and storage devices.
- Scalability: Computer networks can be designed to accommodate a wide range of devices and users, making it easy to add new resources and expand the network as needed.
- Reliability: Computer networks are designed to be reliable, with redundant components and backup systems in place to ensure that the network remains operational even if some components fail.
- Security: Computer networks can be secured using a variety of tools and techniques, such as firewalls, encryption, and access controls, to protect data and prevent unauthorized access.
- Performance: Computer networks are designed to provide high performance and low latency, enabling users to access resources and communicate with one another quickly and efficiently.
- Manageability: Computer networks can be managed centrally, with tools and software that enable administrators to monitor and control access, troubleshoot problems, and maintain the network.
- Standards-based: Computer networks rely on standards-based protocols and technologies to ensure interoperability and compatibility between different devices and systems.

Types of Networks: Local Area Network, Wide Area Network, Metropolitan Area Network, Campus/Corporate Area Network, Personal Area Network, Peer-to-Peer Networks

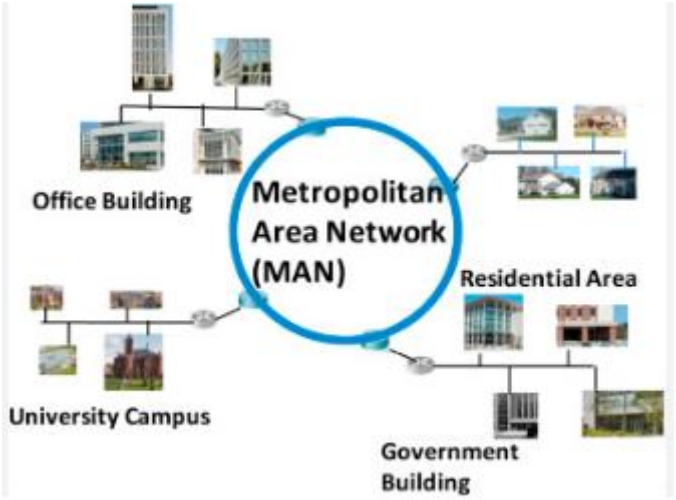
There are several types of networks, including:

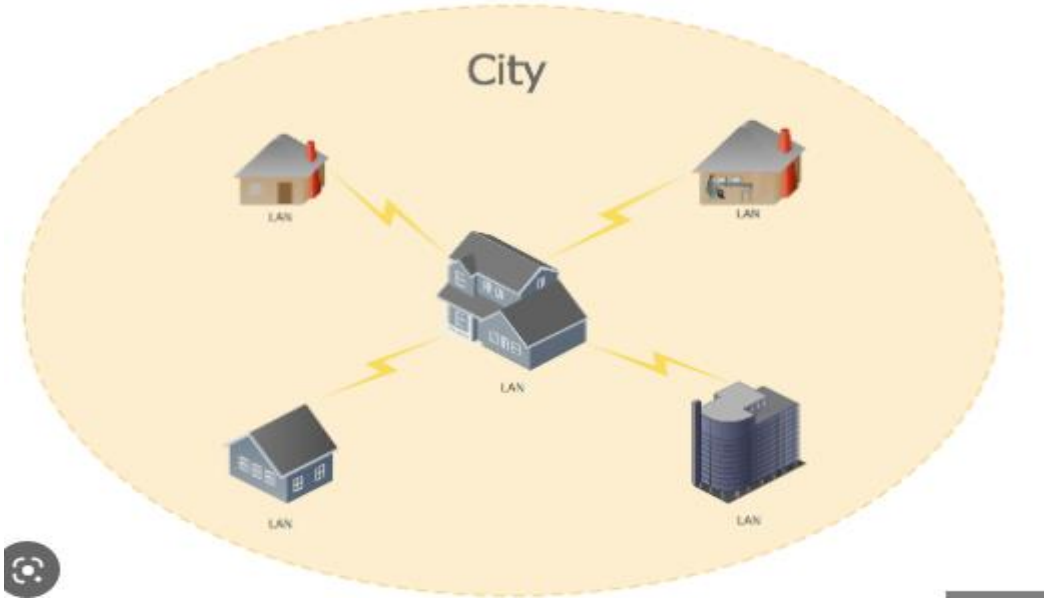
- Local Area Network (LAN): A LAN is a network that is limited to a small geographic area, such as a building, campus, or group of buildings. LANs are typically used to connect devices such as computers, printers, and servers, and are commonly found in homes, schools, and businesses.

- Wide Area Network (WAN): A WAN is a network that spans a larger geographic area, such as a city, country, or even the world. WANs are used to connect LANs and other networks together and can be used for things like Internet connectivity, cloud computing, and remote access.

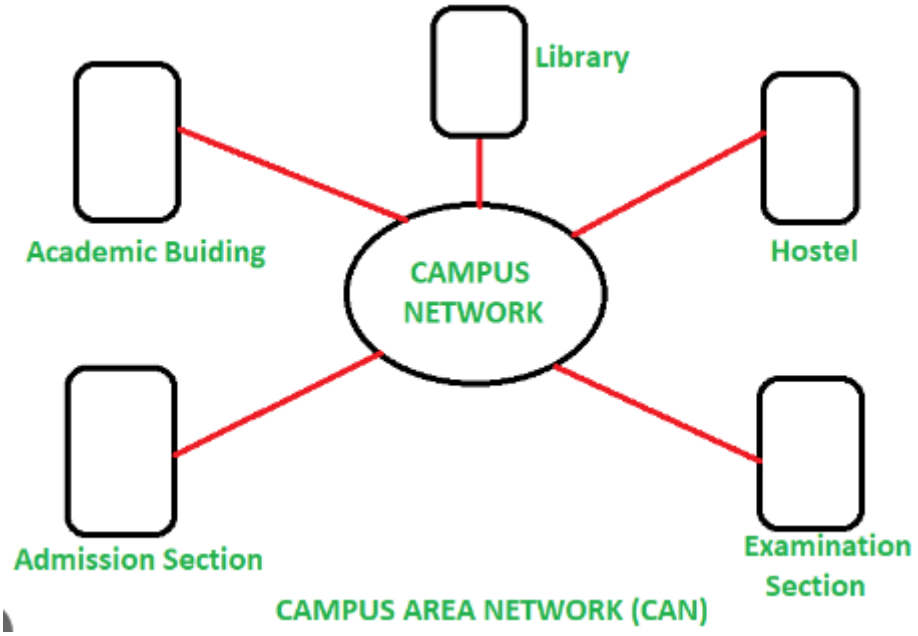


- Metropolitan Area Network (MAN): A MAN is a network that spans a larger geographic area than a LAN but smaller than a WAN, typically covering a city or a region. MANs are often used by service providers to offer broadband services to businesses and organizations.

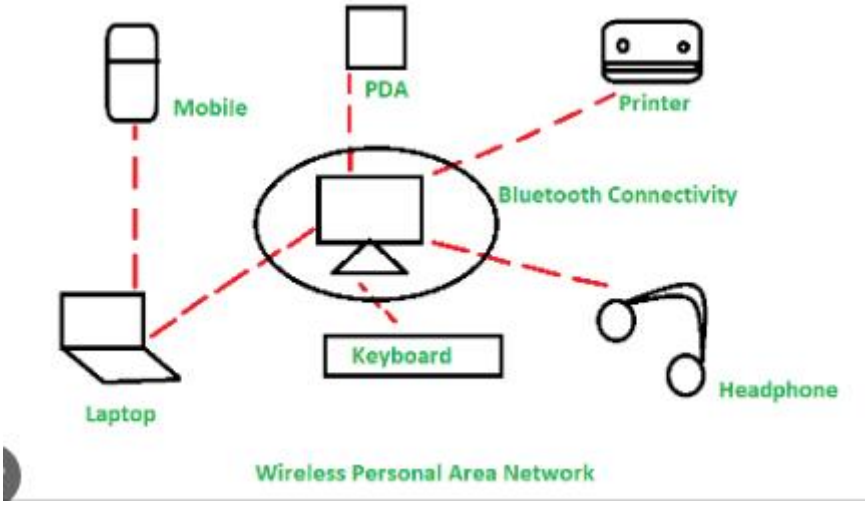




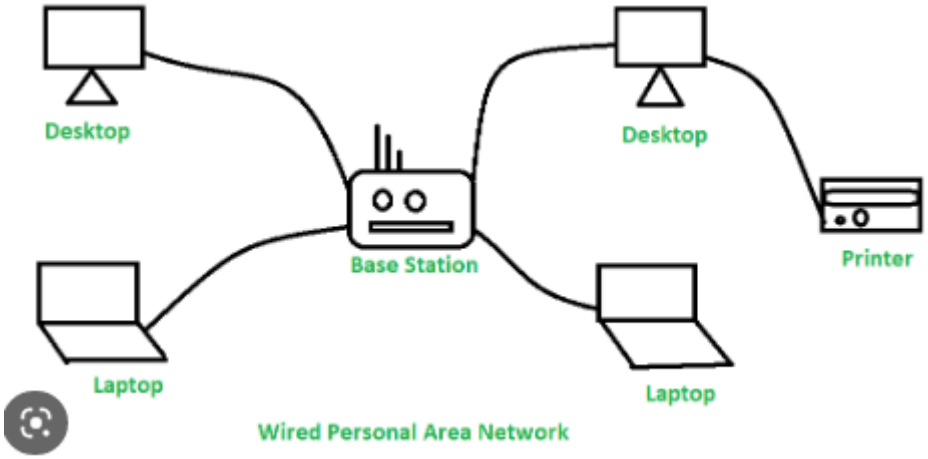
- Campus/Corporate Area Network (CAN): A CAN is a type of network that spans multiple buildings on a single campus or corporate site. CANs are commonly used by universities, hospitals, and large corporations to connect their various buildings and departments.



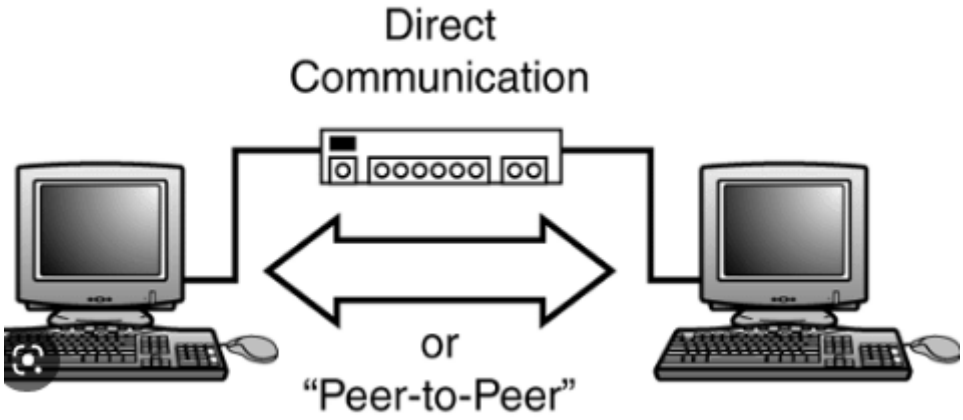
- Personal Area Network (PAN): A PAN is a network that connects devices within a very small area, typically within a person's personal space, such as their home, car, or body. Examples of PANs include Bluetooth and Wi-Fi Direct.



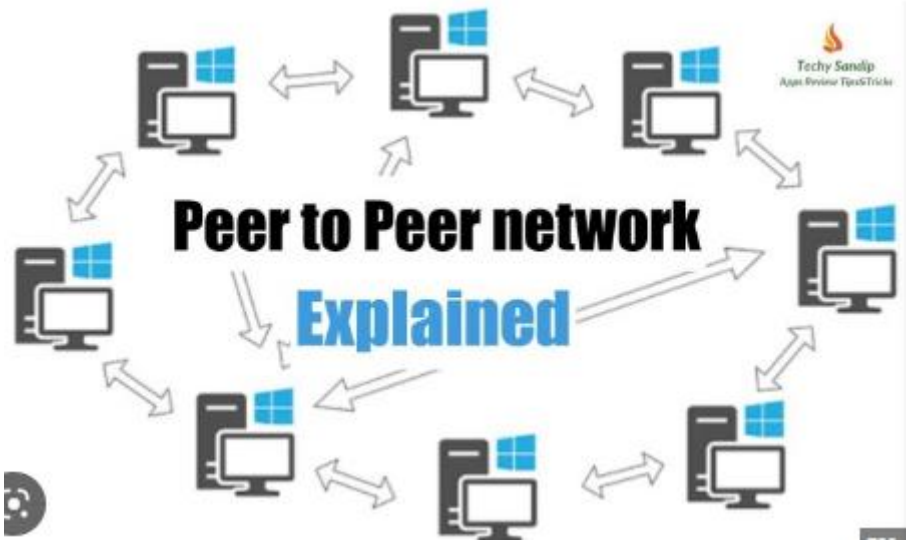
2



- Peer-to-Peer Networks: A peer-to-peer (P2P) network is a decentralized network where devices communicate directly with each other, without the need for a central server. P2P networks are often used for file sharing and messaging applications, such as BitTorrent and Skype.



2



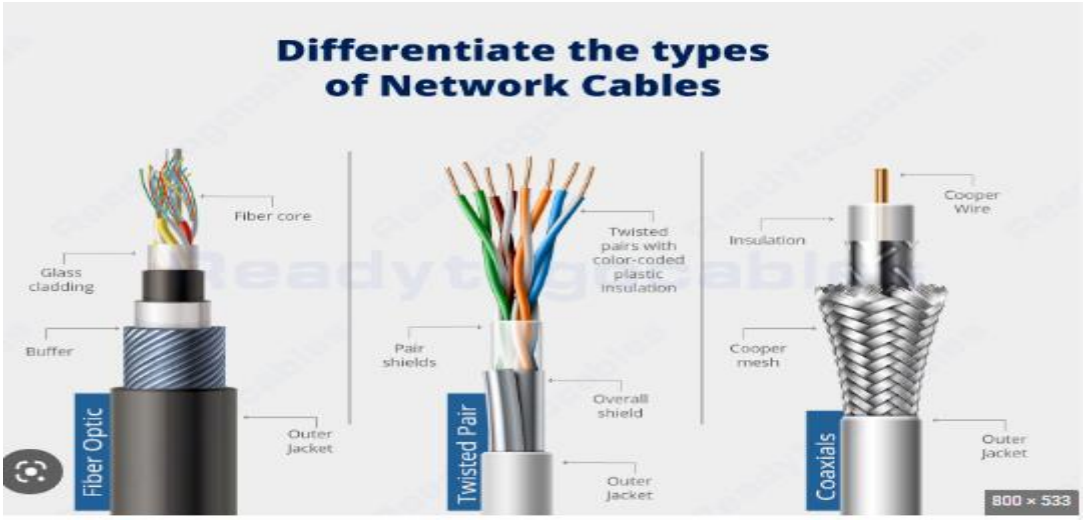
Physical Components of a Network

The physical components of a network are the physical devices and infrastructure that make up the network. Here are some of the key physical components of a network:

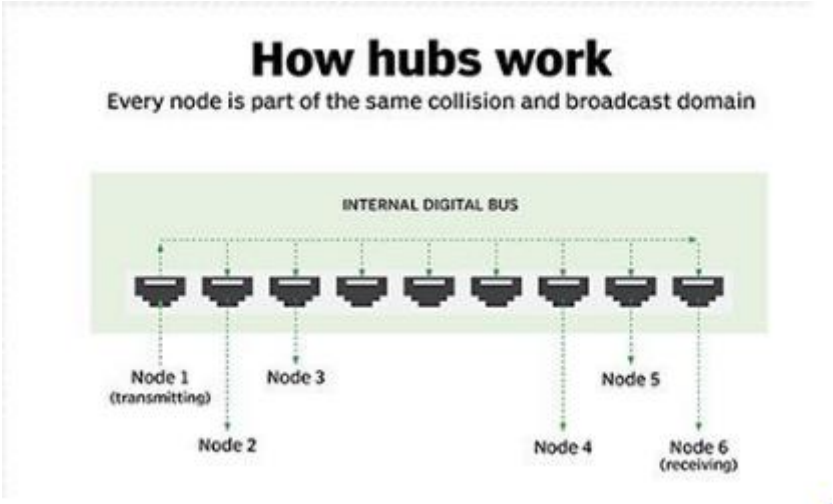
- **Network Interface Cards (NICs):** NICs are hardware components that are installed in each device on the network, such as a computer, printer, or router. They allow the device to connect to the network and communicate with other devices.

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

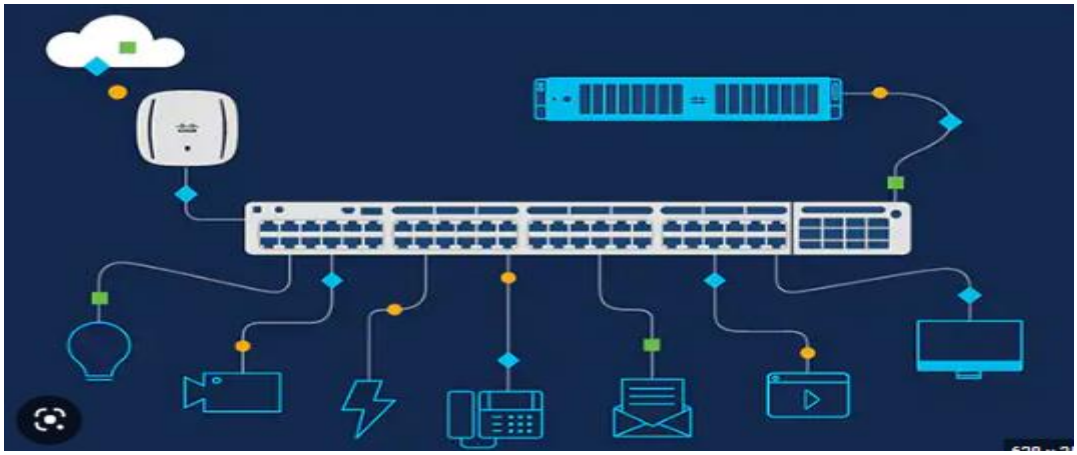
- **Cables:** Cables are used to connect devices to the network, such as Ethernet cables or fiber optic cable,including twisted-pair cable, coaxial cable, and fiber-optic cable. The type of cable used depends on the type of network and the distance between devices.



- **Hubs:** Hubs are used to connect multiple devices together on a network. They receive data from one device and broadcast it to all other devices on the network.



- **Switches:** Switches are similar to hubs, but they are more intelligent and can direct data to specific devices on the network, rather than broadcasting it to all devices.



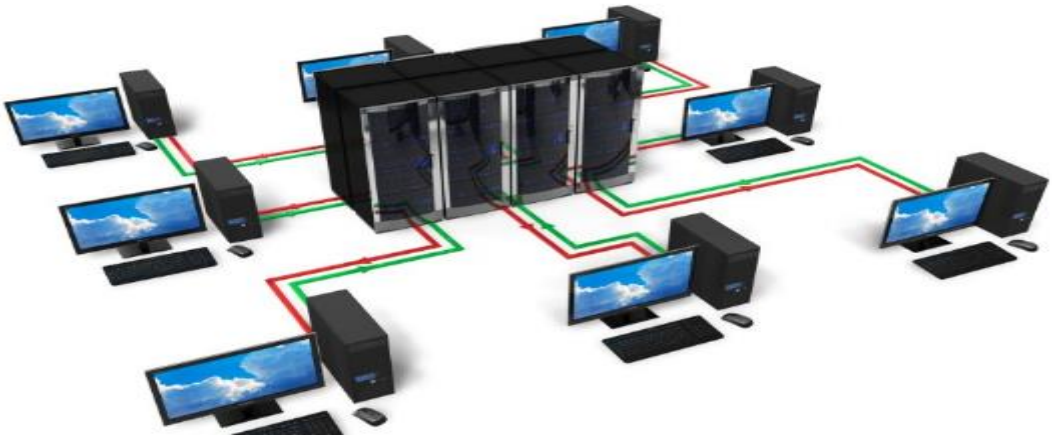
- **Routers:** Routers are used to connect multiple networks together, such as a LAN and a WAN. They use routing tables to determine the best path for data to take between networks.

The router is a physical or virtual internet working device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco, 3Com, HP, Juniper, D-Link, Nortel,** etc.

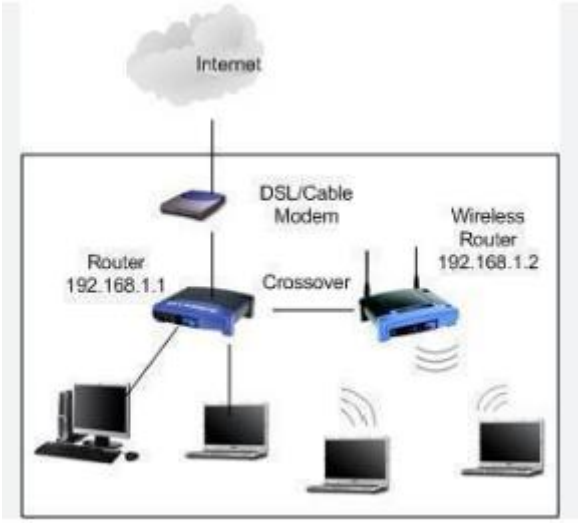
- **Modems:** Modems are used to connect a network to the Internet. They convert digital data from the network into analog signals that can be transmitted over telephone lines, cable lines, or satellite links.

- **Servers:** Servers are computers that are dedicated to providing services to other devices on the network. Examples of server services include file sharing, email, and web hosting.

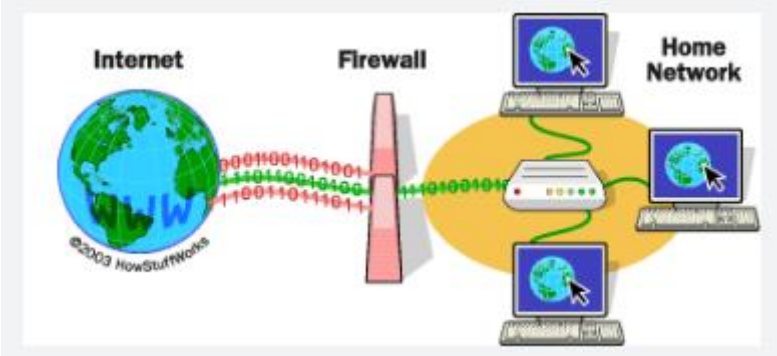
Network servers are dedicated computers connected to a network that run software intended to process client requests and provide appropriate responses. The server can more specifically relate to the software itself, but a network server tends to incorporate the physical system this software runs upon.



- **Wireless Access Points (WAPs):** WAPs are used to provide wireless connectivity to devices on the network. They allow devices to connect to the network without the need for cables.



- **Firewalls:** Firewalls are used to protect the network from unauthorized access and malicious attacks. They can block incoming and outgoing traffic based on predefined rules.



- **Power Supplies:** Power supplies are used to provide power to the network devices. They can be built-in or external, and can be AC or DC depending on the device.

Network Metrics: Downloading, Uploading, Buffering, Speed- Baud rate, Bandwidth

Network metrics are used to measure the performance and efficiency of a network. Here are some commonly used network metrics:

- **Downloading:** Downloading refers to the process of transferring data from a remote server to a local device. Download speed is usually measured in megabits per second (Mbps) or gigabits per second (Gbps).

Downloading-Downloading means your computer is receiving data from the Internet.
Examples: of downloading include opening a web page, receiving email, purchasing music files and watching online videos.

- **Uploading:** Uploading refers to the process of transferring data from a local device to a remote server. Upload speed is also usually measured in Mbps or Gbps.

Uploading-Uploading means data is being sent from your computer to the Internet.
Examples:of uploading include sending email, posting photos on a social media site and using your webcam. Even clicking on a link on a web page sends a tiny data upload.

- **Buffering:** Buffering occurs when there is a delay in the delivery of data, causing the playback of audio or video to pause or stutter. The buffer size determines how much data is stored in the buffer before it is played back, and it can affect the quality of the playback.

Buffering- Buffering refers to the process of temporarily storing data in memory (a buffer) before it is sent or received over a network.

- **Speed:** Speed refers to the rate at which data is transmitted over a network. It is usually measured in bits per second (bps), kilobits per second (Kbps), Mbps, or Gbps. The speed of a network can be affected by factors such as the type of network, the number of users, and the amount of data being transferred.

- **Baud rate:T**he rate at which signals on a wire may change. 1 baud is defined as one signal change per second. Units for baud rate are per second (/s).

Baud rate is a measure of the number of signal changes per second in a communication channel. It is commonly used to measure the speed of serial communication interfaces, such as RS-232 and RS-485.

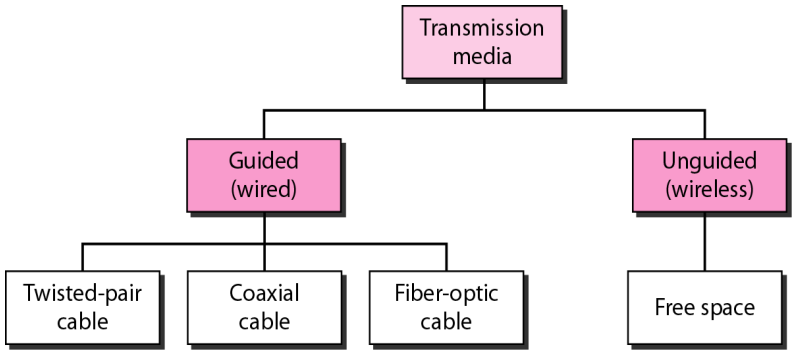
- **Bandwidth:** Bandwidth is the maximum amount of data that can be transmitted over a network in a given period of time. It is usually measured in Mbps or Gbps, and it can be affected by factors such as the type of network, the number of users, and the amount of data being transferred.

The range of signal frequencies that a transmission medium may transmit. The greater the bandwidth, the higher the bit rate.

- **Bit Rate** - The number of bits transmitted per second. Bit rate is measured in bits per second (also written as bps or bits/second.
- **Latency -** Time delay between the moment something is initiated and the moment its effect begins.
- **Jitter-** is the variation in time delay between when a signal is transmitted and when it's received over a network connection, measuring the variability in ping. This is often caused by network congestion, poor hardware performance and not implementing packet prioritization.

Wired Media: Twisted-pair Wires, Coaxial Cables, Fiber Optic Cables,5G- technologies

Classes of transmission media



Wired Media(Guided Media):

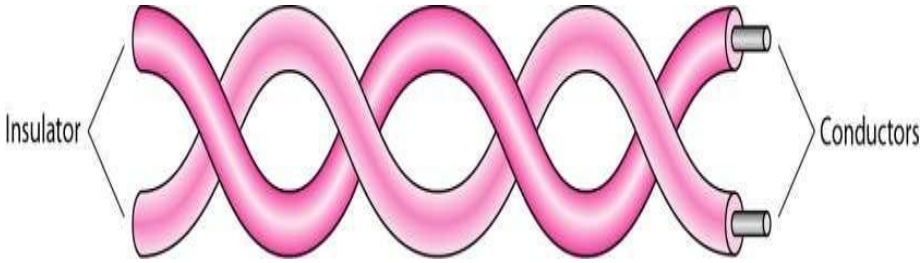
Guided media, which are those that provide a conduit(channel) from one device to another, include twisted-pair cable, coaxial cable, and fiber- optic cable.

Wired media are physical cables or wires that are used to transmit data signals over a network. Here are some common types of wired media:

1.Twisted-pair wires: Twisted-pair wires are a type of cable that consists of two copper wires twisted together to reduce interference from other sources. They are commonly used in Ethernet networks and can support data rates up to 10 Gbps.

- Often used at customer facilities and also over distances to carry voice as well as data communications
- Low frequency transmission medium

(Interference occurs when unwanted radio frequency signals disrupt the use of your television, radio or cordless telephone. Interference may prevent reception altogether, may cause only a temporary loss of a signal, or may affect the quality of the sound or picture produced by your equipment.)



Types of twisted-pair cable:

- **STP (shielded twisted pair)**

the pair is wrapped with metallic foil or braid(thread of metal) to insulate(prevents the loss of heat) the pair from electromagnetic interference(is unwanted noise or interference in an electrical path)

- **UTP (unshielded twisted pair)**

each wire is insulated with plastic wrap, but the pair is encased in an outer covering

Twisted Pair Advantages:

- Inexpensive and readily available
- Flexible and light weight
- Easy to work with and install

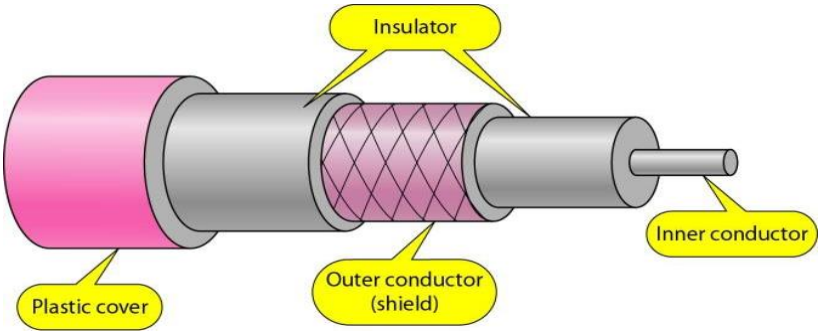
Twisted Pair Disadvantages:

- Susceptibility(harmed by a particular thing) to interference and noise
- Attenuation problem

-For analog, repeaters needed every 5-6km
-For digital, repeaters needed every 2-3km

- Relatively low bandwidth (3000Hz)

2.Coaxial cables: Coaxial cables consist of a copper conductor surrounded by an insulating layer, a metal shield, and an outer jacket. They are commonly used for cable television, Internet access, and other applications that require high-bandwidth data transmission. They can support data rates up to 10 Gbps.



Coax Advantages:

- Higher bandwidth

– 400 to 600Mhz
– up to 10,800 voice conversations

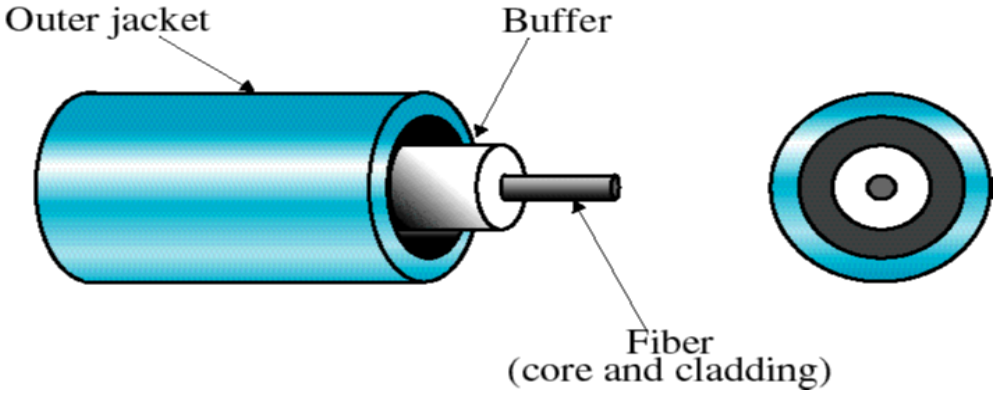
- Can be tapped easily (pros and cons)(Tapping of optical fiber allows diverting some of the signal being transmitted in the core of the fiber into another fiber or a detector.)
- Much less susceptible to interference than twisted pair

Coax Disadvantages:

- High attenuation rate makes it expensive over long distance
- Bulky

3.Fiber optic cables: Fiber optic cables use glass or plastic fibers to transmit data signals using light waves. They are commonly used in high-speed data networks and can support data rates up to 100 Gbps or higher.

- Relatively new transmission medium used by telephone companies in place of long-distance trunk lines
- Also used by private companies in implementing local data communications networks
- Require a light source with injection laser diode (ILD) or light-emitting diodes (LED)



Fiber Optic Types:

- multimode step-index fiber

-the reflective walls of the fiber move the light pulses to the receiver

- multimode graded-index fiber

-acts to refract the light toward the center of the fiber by variations in the density single mode fiber

- the light is guided down the center of an extremely narrow core

Fiber Optic Advantages:

- ✓ greater capacity (bandwidth of up to 2 Gbps)
- ✓ smaller size and lighter weight
- ✓ lower attenuation
- ✓ immunity to environmental interference(without being disturbed by the electromagnetic fields.)
- ✓ highly secure due to tap difficulty and lack of signal radiation

Fiber Optic Disadvantages:

- ✓ expensive over short distance
- ✓ requires highly skilled installers
- ✓ adding additional nodes is difficult

4.5G technologies: 5G is the fifth generation of wireless technology that uses high-frequency radio waves to transmit data signals. Unlike wired media, it does not require physical cables and can transmit data wirelessly over long distances. 5G technology can support data rates up to 20 Gbps or higher.

In summary, twisted-pair wires and coaxial cables are commonly used wired media for Ethernet networks and high-bandwidth data transmission, while fiber optic cables offer high-speed data transmission and 5G technology provides wireless data transmission over long distances.

5G technologies applications

- Enhanced mobile broadband (eMBB): 5G networks provide significantly faster download and upload speeds, allowing users to stream high-definition video, download large files, and engage in real-time online gaming and virtual reality experiences.
- Internet of Things (IoT): 5G networks enable the deployment of a vast number of IoT devices, such as sensors and smart devices, which can be used in a variety of industries, including healthcare, transportation, and manufacturing.
- Smart cities: 5G networks enable the deployment of smart city technologies, such as intelligent traffic management systems, smart grids, and environmental monitoring systems, which can improve the efficiency of city services and enhance the quality of life for citizens.
- Autonomous vehicles: 5G networks enable the deployment of autonomous vehicles, which can communicate with one another and with infrastructure in real-time, enabling safer and more efficient transportation.
- Remote surgery: 5G networks enable the deployment of remote surgery technologies, which allow surgeons to perform procedures on patients located in different locations using robotic systems and real-time video communication.

Wireless Media: Terrestrial Microwaves, Satellite Communication, Infrared Communication

Radio waves are a type of electromagnetic radiation that have longer wavelengths than microwaves. They are commonly used for wireless communication, including broadcast radio and television, mobile phones, and two-way radios.

One example of radio wave communication is FM radio broadcasting. FM radio signals are transmitted by radio stations from a transmitter tower and received by radio receivers, which convert the radio waves back into sound waves that can be heard by the listener. Another example is the use of radio waves for mobile phone communication. Mobile phones use radio waves to communicate with nearby cell towers, which then relay the communication to other phones or the internet.

Radio waves have a lower frequency than other types of wireless media, which can limit their data transmission capacity. However, they have the advantage of being able to travel long distances and penetrate solid objects, making them useful for communication in a variety of settings.

Examples:

Here are some additional examples of the use of radio waves for wireless communication:

- AM Radio Broadcasting: AM radio broadcasting is another example of the use of radio waves for wireless communication. AM radio signals are transmitted at lower frequencies than FM radio signals and can travel long distances, making them ideal for broadcasting news, sports, and music to a wide audience.
- Two-Way Radios: Two-way radios, also known as walkie-talkies, use radio waves to communicate wirelessly between two or more people. They are commonly used in outdoor settings, such as camping trips, construction sites, and emergency situations.
- Wireless Local Area Networks (WLANs): Wireless Local Area Networks (WLANs), also known as Wi-Fi networks, use radio waves to provide wireless access to the internet or other computer networks. Wi-Fi networks are commonly used in homes, offices, and public spaces to enable wireless internet access for smartphones, laptops, and other devices.
- Bluetooth: Bluetooth is a wireless technology that uses radio waves to connect devices, such as smartphones, headphones, and speakers, to each other. Bluetooth is commonly used for wireless audio streaming and for connecting peripherals, such as keyboards and mice, to computers and other devices.
- Radio Frequency Identification (RFID): RFID is a wireless technology that uses radio waves to identify and track objects or people. RFID tags can be attached to items such as merchandise, pets, or people, and can be used for inventory management, tracking shipments, and identifying individuals in secure locations.

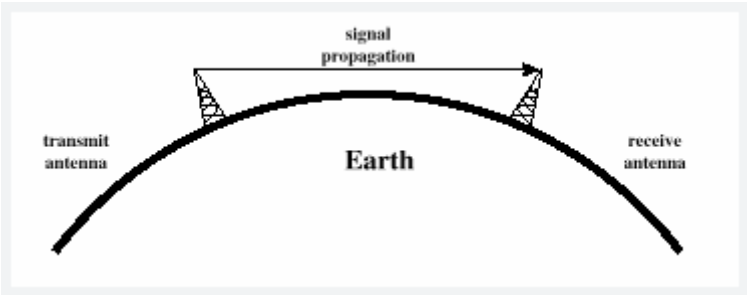
Microwave transmission is a type of wireless communication that uses high-frequency radio waves in the microwave frequency range to transmit information between two or more devices.

Here are some examples of the use of microwave transmission:

- Point-to-Point Microwave Links: Point-to-Point microwave links are used to connect two fixed locations, such as two buildings or two cell towers, using microwave radio waves. These links are commonly used by telecommunications companies to provide high-speed internet connections, as well as by television broadcasters to transmit television signals between stations.
- Microwave Ovens: Microwave ovens use microwave radiation to heat and cook food. The microwaves produced by the oven cause water molecules in the food to vibrate, which generates heat and cooks the food.
- Radar: Radar (which stands for Radio Detection and Ranging) uses microwave radio waves to detect and locate objects in the air, on land, or at sea. Radar is used in a variety of applications, such as air traffic control, weather forecasting, and military surveillance.
- Satellite Communications: Satellite communications use microwave transmission to communicate between ground stations and satellites in orbit. The satellites relay the communication to other ground stations or to other satellites, enabling global communication coverage.
- Wireless Local Area Networks (WLANs): Wireless Local Area Networks (WLANs) can also use microwave transmission to provide wireless access to the internet or other computer networks. However, WLANs typically use radio waves in the higher-frequency end of the microwave frequency range, known as the millimeter wave range, to provide higher data transmission rates.

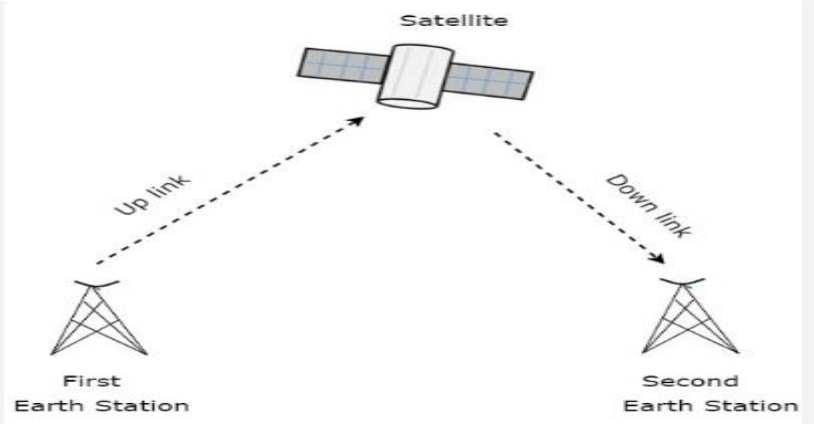
- Wireless media refer to the transmission of data signals over the airwaves without the use of physical cables. Here are some common types of wireless media:

Terrestrial microwaves: Terrestrial microwaves are high-frequency radio waves that are used for point-to-point communication over short distances. They are commonly used for wireless communication between buildings or across campuses and can support data rates up to several Gbps.



Examples: Terrestrial Microwaves: A common example of terrestrial microwaves is the use of wireless internet (Wi-Fi) in homes, offices, and public spaces. Wi-Fi networks use radio waves in the microwave frequency range to transmit data wirelessly between devices, such as smartphones, laptops, and smart home devices. Another example is the use of microwave links to connect cell towers in a mobile network, enabling fast and reliable cellular communication.

Satellite communication: Satellite communication involves the transmission of data signals between two or more ground stations via a network of satellites orbiting the Earth. It is commonly used for long-distance communication, such as television broadcasting and global positioning systems (GPS). It can support data rates up to several Gbps.



Applications of Satellite Communication

- Telephone.
- Television.
- Digital cinema.
- Radio broadcasting.
- Amateur radio.
- Internet access.
- Military.
- Disaster Management.

Examples: Satellite Communication: One example of satellite communication is the Global Positioning System (GPS), which uses a network of satellites to provide accurate location information to GPS receivers on the ground. Another example is satellite television, which transmits television signals from satellites in

orbit to television receivers on the ground, providing access to a wide range of channels and programming from around the world.

Infrared communication: Infrared communication uses infrared light waves to transmit data signals between devices. It is commonly used for short-range communication between devices such as remote controls, computer peripherals, and smartphones. It can support data rates up to several Mbps.

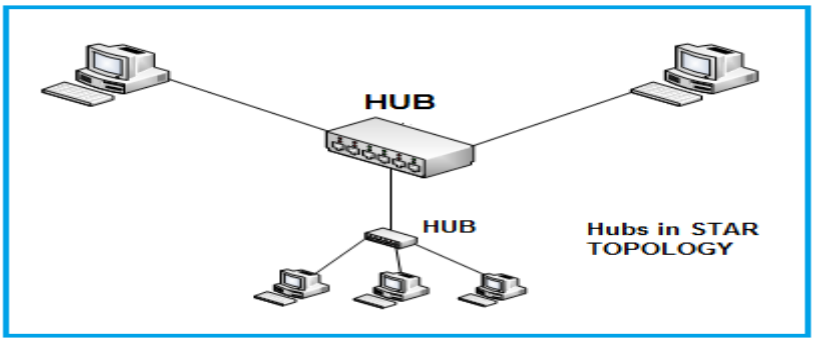
Examples: Infrared Communication: Infrared communication is commonly used in remote controls for televisions, DVD players, and other home entertainment devices. The infrared signals from the remote control are received by a sensor on the device, allowing the user to control it wirelessly. Another example of infrared communication is the use of infrared data transmission (IrDA) to share data between two mobile devices, such as smartphones or tablets, by pointing them at each other and transferring the data through infrared light waves.

In summary, terrestrial microwaves are used for short-range wireless communication between buildings or across campuses, satellite communication is used for long-distance communication, and infrared communication is used for short-range communication between devices.

Networking Devices: Hub ,Repeater, Switch, Bridge, Router, Gateway , Network Interface Card, RJ45

Networking devices are hardware components used to interconnect devices and facilitate data communication over a network. Here are some common types of networking devices:

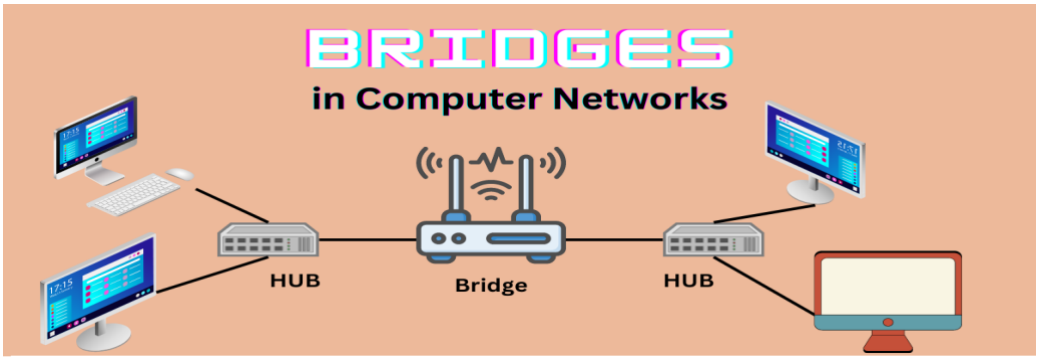
- Hub: A hub is a simple device that connects multiple devices in a network, allowing them to communicate with each other. It operates on the physical layer of the OSI model and broadcasts incoming data to all connected devices, which can result in network congestion and performance issues. Network hubs are best suited for small, simple local area network (LAN) environments



- Repeater: A repeater is a device that amplifies and retransmits signals to extend the reach of a network. It operates on the physical layer of the OSI model and can improve signal strength and network performance over long distances.

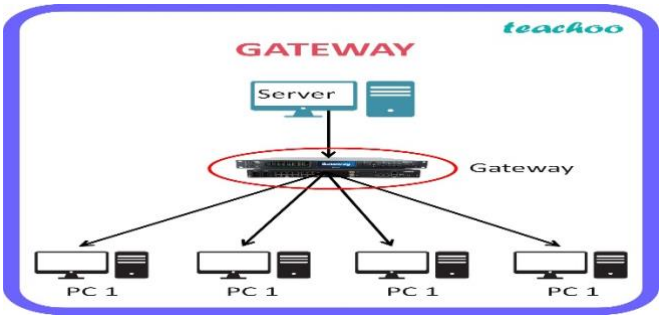
- Switch: A switch is a device that connects multiple devices in a network and intelligently forwards data only to the intended recipient. It operates on the data link layer of the OSI model and can improve network performance and security.

- Bridge: A bridge is a device that connects multiple network segments and forwards data between them based on their MAC addresses. It operates on the data link layer of the OSI model and can improve network performance and security.



- Router: A router is a device that connects multiple networks and forwards data between them based on their IP addresses not on the MAC(Hardware) address. It operates on the network layer of the OSI model and can improve network performance and security.

- Gateway: A gateway is a device that connects a network to other networks with different protocols or architectures. It translates between different protocols and can allow different types of networks to communicate with each other.



- Network Interface Card (NIC): A NIC is a hardware component that enables a device to connect to a network. It is typically installed inside a device and provides a physical interface for connecting to a network.

- RJ45: RJ45 (registered jack)is a type of connector commonly used for Ethernet networking. It is used to connect Ethernet cables to devices such as computers, switches, and routers. The "45" simply refers to the number of the interface standard. Each RJ45 connector has eight pins, which means an RJ45 cable contains eight separate wires. which are each a different color.

In summary, hubs and repeaters are used for simple network connectivity, switches and bridges improve network performance and security, routers connect multiple networks, gateways translate between different protocols, NICs enable devices to connect to a network, and RJ45 connectors are used for Ethernet networking.

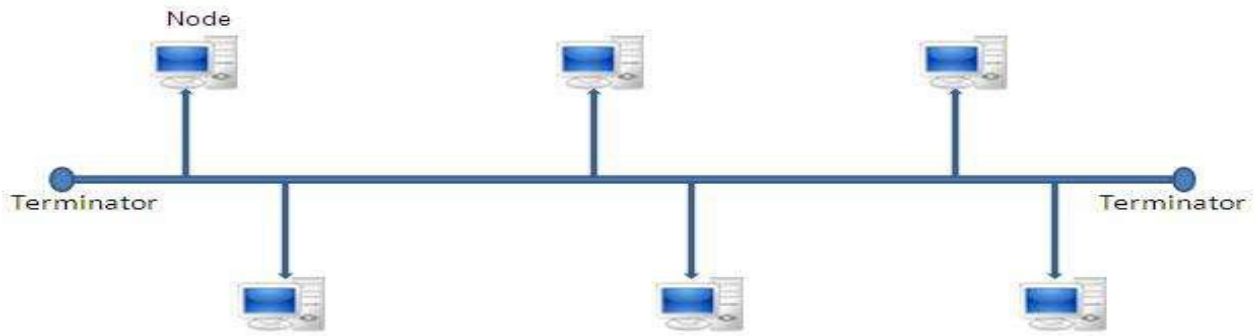
Network Topologies: Bus Topology, Star Topology, Ring Topology, Mesh topology, Hybrid Topology

- A topology is a way of "laying out" the network. Topologies can be either physical or logical.
- Physical topologies describe how the cables are run.
- Logical topologies describe how the network messages travel

Types of network topology:

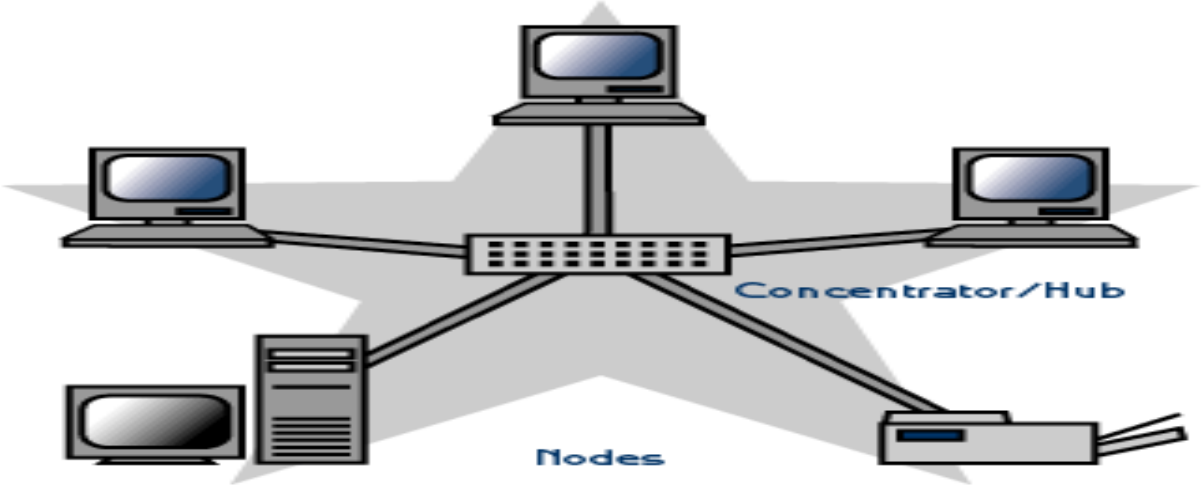
- Bus (can be both logical and physical)
- Star (physical only)
- Ring (can be both logical and physical)
- Mesh (can be both logical and physical)
- Hybrid

- Bus topology: In a bus topology, all devices are connected to a single communication line called a bus. Data is transmitted in both directions along the bus, and all devices receive the same data. A bus topology is simple and inexpensive to set up, but it can suffer from performance issues if too many devices are connected. If any one of the cables breaks, the entire network is disrupted. Therefore, it is very expensive to maintain.

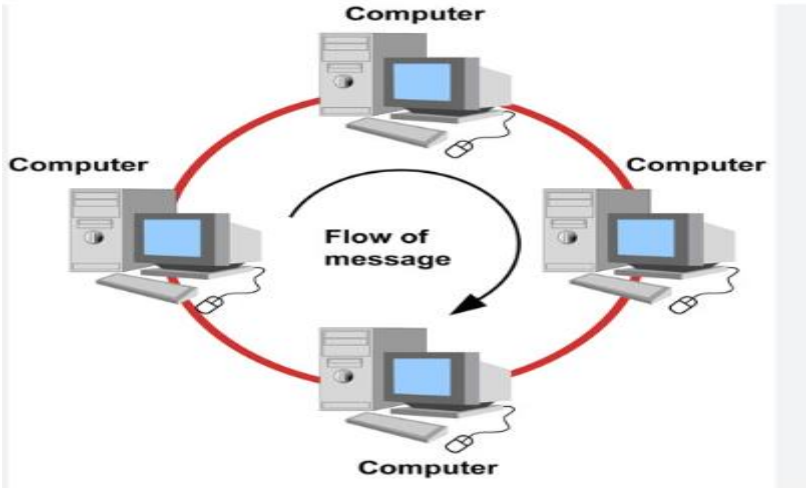


- Star topology: In a star topology, all devices are connected to a central hub or switch. Data is transmitted between devices via the hub or switch, and each device has its own dedicated connection. A star topology is easy to set up and can improve network performance, Star topologies are more expensive to install than

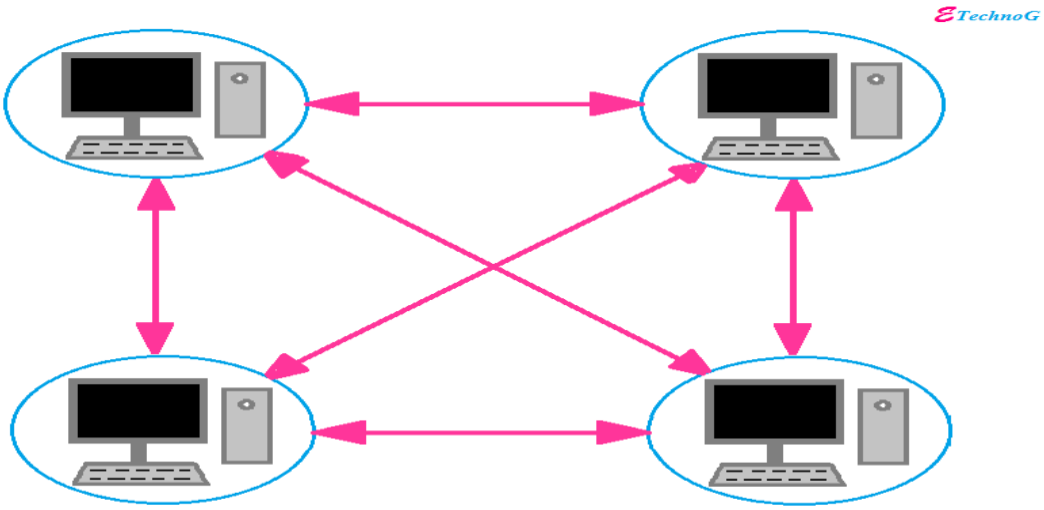
bus networks, because there are several more cables that need to be installed, plus the cost of the hubs that are needed. Also, if any workstation goes down it does not affect the entire network.



- Ring topology: In a ring topology, devices are connected in a circular ring, with each device connected to two neighboring devices. Data is transmitted in a single direction around the ring, and each device receives and retransmits (regenerates) the data until it reaches its destination. A ring topology can provide good performance and fault tolerance, but it can be difficult to troubleshoot if a device fails. The ring makes it difficult to add new computers. Unlike a star topology network, the ring topology network will go down if one entity is removed from the ring.

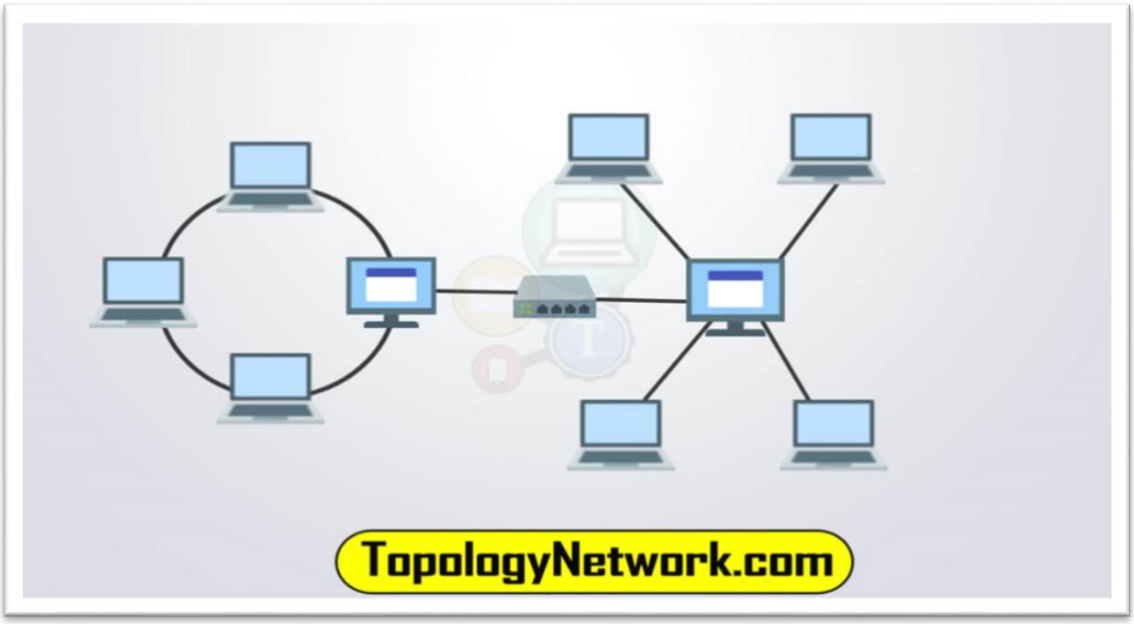


- Mesh topology: In a mesh topology, devices are connected to each other in a network of interconnected nodes. Data is transmitted between devices via multiple paths, which can improve network performance and fault tolerance. A mesh topology can be expensive to set up and maintain, but it can provide high reliability and scalability. This topology is rarely found in LANs, mainly because of the complexity of the cabling.
- If there are x computers, there will be $(x \times (x–1)) \div 2$ cables in the network. For example, if you have five computers in a mesh network, it will use $4 \times (4 – 1) \div 2$, which equals 6 cables. This complexity is compounded when you add another workstation.



Mesh Topology

- Hybrid topology: A hybrid topology combines two or more types of topologies, such as a star-ring or a mesh-bus topology. This can provide the benefits of each topology while minimizing their limitations.

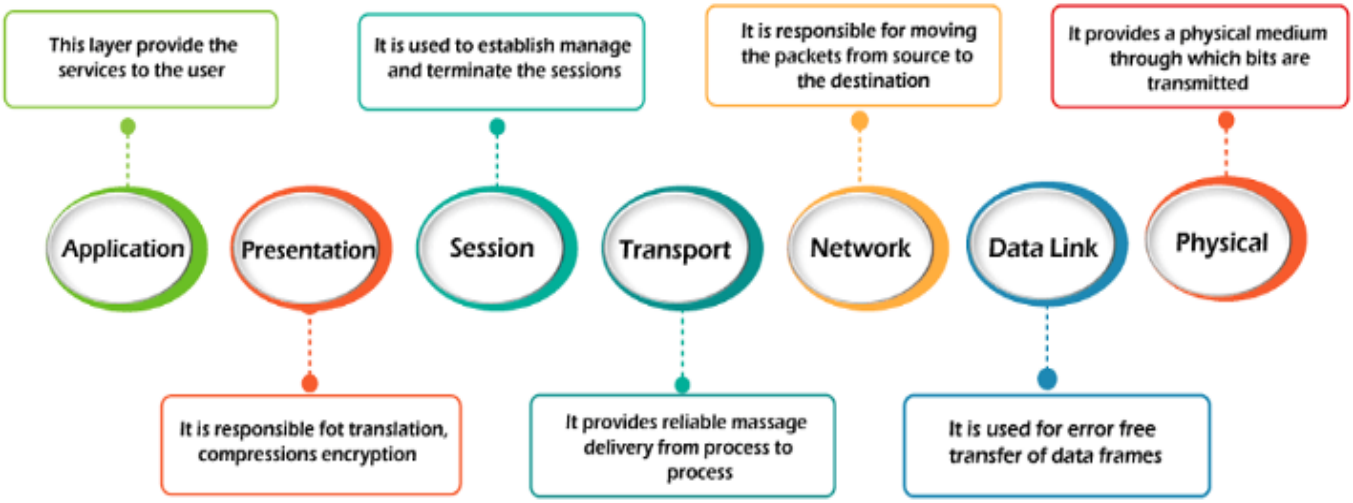


In summary, bus and star topologies are simple and commonly used in small networks, ring topology provides good fault tolerance, mesh topology provides high reliability and scalability, and hybrid topology can provide the benefits of multiple topologies.

Note OSI Model is not in syllabus for Extra Knowledge purpose mentioned here

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.



https://www.geeksforgeeks.org/layers-of-osi-model/
https://www.javatpoint.com/computer-network-features

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization for Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

1. 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 transmitting individual bits from one node to the next.
- 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.

2. 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.
  - It defines the format of the data on the network.
- When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
- 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.

3. Network Layer (Layer 3) :

- The network layer works for the transmission of data from one host to the other located in different networks.
- 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.
- 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 addresses are placed in the header by the network layer.

4. Transport Layer (Layer 4) :

- The transport layer provides services to the application layer and takes services from the network layer.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- It is responsible for the End to End Delivery of the complete message.
- The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

5. Session Layer (Layer 5) :

- This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.

6. Presentation Layer (Layer 6):

- The 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 Presentation layer is also known as the syntax layer.

7. Application Layer (Layer 7) :

- At the very top of the OSI Reference Model stack of layers, we find the 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.
- This layer provides the network services to the end-users.