Network Topologies and Devices

3.1 Network Topologies : Introduction, Definition,Selection Criteria,Types of Topologies –

Bus,Ring,Star,Mesh,Tree,Hybrid.

Introduction:

Definition:

- A Network Topology is the arrangement with which computer systems or network devices are connected to each other is called Network Topologies.
- Topologies may define both physical and logical aspects of the network. Both logical and physical topologies could be the same or different in the same network is called Topologies.
- Network topologies refer to the different ways devices are connected in a network. There are various types, like bus, star, ring, and mesh. Each has its own advantages and disadvantages.

Selection Criteria/Network Criteria:

- A network must be able to meet a certain number of criteria.
- The most important of these are performance, reliability, and security.

1. **Performance:**
    - Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.
    - The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
    - Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.
2. **Reliability:** In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.
3. **Security:** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Types of Topologies –

Bus Topology

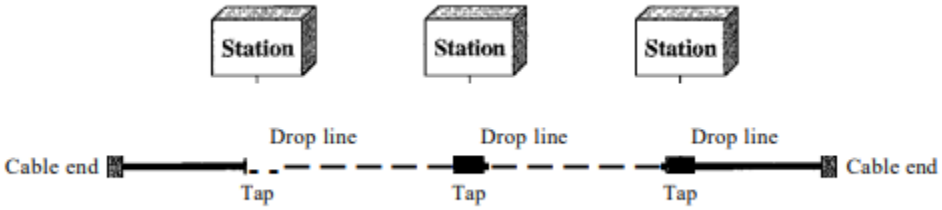


Figure: Bus Topology

- 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).
- The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure).

Advantages of Bus topology:

1. **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.
2. **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
3. **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
4. **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

1. **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
2. **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.
3. **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
4. **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
5. **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology

Figure: 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.
    a. **Token passing:** It is a network access method in which token is passed from one node to another node.
    b. **Token:** It is a frame that circulates around the network.

Working of Token passing:

1. A token moves around the network, and it is passed from computer to computer until it reaches the destination.
2. The sender modifies the token by putting the address along with the data.
3. 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.
4. In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

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

Disadvantages of Ring topology:

1. **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.
2. **Failure:** The breakdown in one station leads to the failure of the overall network.
3. **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
4. **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology:

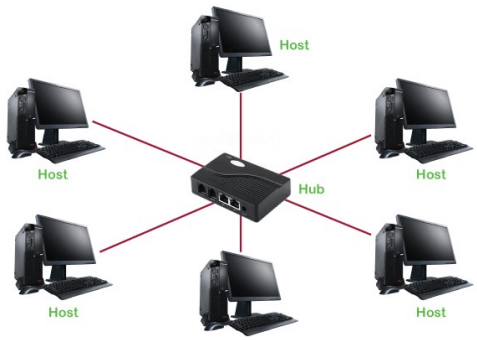


Figure: Star Topology

- All hosts in Star topology are connected to a central device, known as hub devices, using a point to point connection. Point to point connection between hosts & hub.
- In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.
- The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers.
- In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

Advantages of Star topology

1. **Efficient troubleshooting:** 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.
2. **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
3. **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
4. **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

1. **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.
2. **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

Mesh Topology:

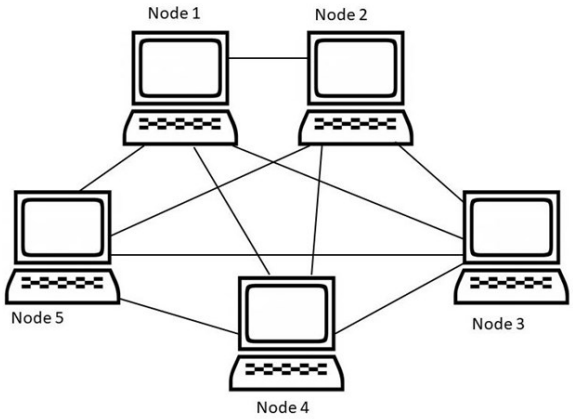


Figure: Mesh Topology

- **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.**
- In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are **AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.**
- 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.

Advantages of Mesh topology:

1. **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
2. **Fast Communication:** Communication is very fast between the nodes.
3. **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

1. **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
2. **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.
3. **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Tree Topology

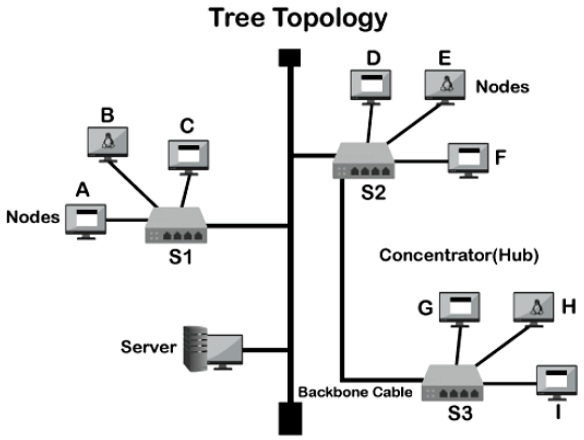


Figure: Tree Topology

- In computer networking, tree topology is a type of network topology that resembles a tree. In a tree topology, there is one central node (the “trunk”), and each node is connected to the central node through a single path. Nodes can be thought of as branches coming off of the trunk.
- Tree topologies are often used to create large networks. 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

1. **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
2. **Error detection:** Error detection and error correction are very easy in a tree topology.
3. **Limited failure:** The breakdown in one station does not affect the entire network.
4. **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

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

Hybrid Topology

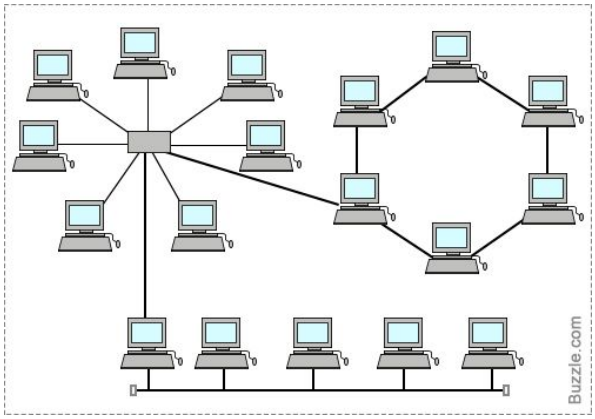


Figure: Hybrid Topology

- Hybrid topology is a type of network topology in which two or more different topologies are integrated or combined to lay out a network.
- In layman's terms, hybrid topology is the combination of two or more networks. The network type could be Star, Ring, Bus, or Mesh.
- 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

1. **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
2. **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
3. **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
4. **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

1. **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.
2. **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
3. **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

3.2 Network Connecting Devices: NIC (Network Interface Card),Hub,Switch,Router,Repeater,Bridge,Gateway,Modem,Wireless infrastructure Components.

NIC (Network Interface Card):

- Network Interface Card is an equipment unit, which is inbuilt inside a PC furnished with an opening, it associates the PC to a PC network for correspondence with different gadgets by means of transports.
- There are numerous equivalents for network interface card like network connector, neighborhood (LAN) card or actual Network interface card, ethernet regulator or ethernet connector, network regulator, and association card.

#Features of Network Interface Card :

1. Network interface card bolsters practically all standard transports for information move between the PCs or gadgets.
2. The connectors or transports go about as an intermediator for correspondence changes over the correspondence between different gadgets from sequential correspondence to resemble correspondence or equal correspondence to sequential correspondence.
3. It additionally designs information dependent on the engineering of the Network.
4. Network Interface Card card NIC is an equipment part, where network regulators are incorporated onto a circuit load up that utilizes a standard OSI model of 7 layers to impart and it acts like a trans-collector, where it can send and get simultaneously while speaking with different gadgets.

Advantages of Network Interface Card :

1. The information move is exceptionally dependable among the hubs.
2. The web speed for correspondence making conceivable is normally high in gigabytes.
3. By using numerous ports of NIC cards that are given, a few peripherals can get stopped.
4. The correspondence speed utilizing the Internet is high generally in Gigabytes.
5. Numerous fringe gadgets can be associated utilizing numerous ports of NIC cards.

Disadvantages of Network Interface Card :

1. Badly designed if there should arise an occurrence of wired link NIC, as it isn't convenient like a remote switch.
2. The design should be legitimate for better correspondence. Information is unstable.
3. By using numerous ports of NIC cards that are given, a few peripherals can get stopped.
4. Security is minimal low. To make fine correspondence the arrangement should be exact.
5. At the point when wired links are use in Network Interface Card transportability isn't economical and cause inconveniences.

Hub:

- **Hub in networking plays a vital role in data transmission, and broadcasting.**
- **Hub is a hardware device used at the physical layer to connect multiple devices in the network.**
- **Hubs are widely used to connect LANs. A hub has multiple ports and it is a non-intelligent device.**
- **In the hub, data is sent to all ports but each port accepts only that data whose destination address matches their MAC address.**

#How Does a Network Hub Work?

- **A hub is a multiport device, which has multiple ports in a device and shares the data to multiple ports altogether. A hub acts as a dumb switch that does not know, which data needs to be forwarded where so it broadcasts or sends the data to each port.**
- **Suppose there are five ports in a hub A, B, C, D, and E. consider A wants to send any data frame, or let's say A is acting as a sender, so the hub will forward the data transmitted by A to B, C, D, E. Now, if at the same time B also wants to send the data then data received from A and B will collide and can cause data loss. In this situation, the data gets destroyed, and the hosts send a jam signal to all the hosts informing them about the collision, and each sender needs to wait for a certain amount of time.**

#Types of Network Hubs:

1. **Active Hub: They have a power supply for regenerating, and amplifying the signals. When a port sends weak signaled data, the hub regenerates the signal and strengthens it, then send it further to all other ports. Active hubs are expensive in costs as compared to passive hubs.**
2. **Passive Hub: Passive hubs are simply used to connect signals from different network cables as they do not have any computerized element. They simply connect the wires of different devices in the star topology. Passive hubs do not do any processing or signal regeneration and that's why do not require electricity the most they can do is they can copy or repeat the signal. It can't clean the message, and it can't amplify or strengthen the signal.**
3. **Intelligent Hub: Intelligent hubs as the name suggests are smarter than active and passive hubs. The intelligent hub comprises a special monitoring unit named a Management Information Base (MIB).**

#Features of Hubs:

1. **It supports half-duplex transmission**
2. **It works with shared bandwidth and broadcasting.**
3. **The hub can provide a high data transmission rate to different devices.**
4. **It can detect collisions in the network and send the jamming signal to each port.**
5. **Hub does not support VLAN and spanning tree protocol.**
6. **It is unable to filter the data and hence transmit or broadcast it to each port.**

7. It cannot find the best route/ shortest path to send any data, which makes it an inefficient device.

#Advantages of Network Hubs:

1. Less expensive.
2. Does not impact network performance.
3. Support different network media.
4. Easily connects with different media.

#Disadvantages of Network Hubs:

1. It cannot find the best/ shortest path of the network.
2. No mechanism for traffic detection.
3. No mechanism for data filtration.
4. Not capable of connecting to different network topologies like token, ring, ethernet, etc.

Switch:

- The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments. It is responsible for filtering and forwarding the packets between LAN segments based on MAC address.
- Network switches operate primarily at Layer 2 (the data link layer) and Layer 3 (the network layer) of the OSI (Open Systems Interconnection) model.
- Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices.
- Different types of communication are supported here like unicast, multicast, and broadcast communication.

#Features of Network Switches

1. It operates in Data Link Layer in OSI Model. It performs error checking before forwarding data.
2. It transfers the data only to the device that has been addressed.
3. It operates in full duplex mode. It allocates each LAN segment a limited bandwidth.
4. It uses Unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) transmission modes.
5. Packet Switching techniques are used to transfer data packets from source to destination.
6. Switches have a more significant number of ports.

#Types of Switches

1. Virtual Switches: Virtual Switches are the switches that are inside Virtual Machine hosting environments.

2. Routing Switches: These are the switches that are used to connect LANs.They also have the work of performing functions in the Network Layer of the OSI Model.
3. Unmanaged Switches: Unmanaged Switches are the devices that are used to enable Ethernet devices that help in automatic data passing. These are generally used for home networks and small businesses. In case of the requirement of more switches, we just add more switches by plug and play method.
4. Managed Switches: Managed Switches are switches having more complex networks. SNMP (Simple Network Management Protocol) can be used for configuring managed switches. These types of switches are mostly used in large networks having complex architecture. They provide better security levels and precision control but they are more costly than Unmanaged switches.
5. LAN Switches: LAN (Local Area Network) Switches are also called ethernet switches or data switches. LAN switches always try to avoid overlapping of data packets in the network just by allocating bandwidth in such a manner.
6. PoE Switches: Power over Ethernet(PoE) are the switches used in Gigabit Ethernets. PoE help in combining data and power transmission over the same cable so that it helps in receiving data and electricity over the same line.
7. Stackable Switches: Stackable switches are connected through a backplane to combine two logical switches into a single switch.
8. Modular Switches: These types of switches help in accommodating two or more cards. Modular switches help in providing better flexibility.

#How Does a Network Switch Works?

- When the source wants to send the data packet to the destination, the packet first enters the switch and the switch reads its header and finds the MAC address of the destination to identify the device then it sends the packet out through the appropriate ports that lead to the destination devices.
- Switch establishes a temporary connection between the source and destination for communication and terminates the connection once the conversation is done. Also, it offers full bandwidth to network traffic going to and from a device simultaneously to reduce collision.
- Switching Techniques: Switching techniques are used to decide the best route for data transmission between source and destination. These are classified into three categories i.e. Circuit Switching, Message Switching & Packet Switching

#How To Set Up a Network Switch?

There are different kinds of switches that work according to the tasks defined. For a small network LAN, or for a home network, a network switch is used by plugging into a port of the router. Below mentioned are the steps which are used in setting up network switches.

Step 1: Switch has to be bought as per the requirement of the network.

Step 2: The switch port has to be connected directly to the router using the cable. Generally, if there is an uplink port present in the switch, the wire should be connected to that port, if the uplink power is not present, then the wire has to be connected to any port of the router.

Step 3: After proper connection, the IP addresses of devices are configured.

Router:

- A Router is a networking device that forwards data packets between computer networks.
- One or more packet-switched networks or subnetworks can be connected using a router.
- By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.
- Routers are the devices that are operated on the Network Layer of the OSI Model, these are the most common devices used in networking.

#How Does Router Work?

- A router determines a packet's future path by examining the destination IP address of the header and comparing it to the routing database. The list of routing tables outlines how to send the data to a specific network location. They use a set of rules to determine the most effective way to transmit the data to the specified IP address.
- To enable communication between other devices and the internet, routers utilize a modem, such as a cable, fiber, or DSL modem. Most routers include many ports that can connect a variety of devices to the internet simultaneously. In order to decide where to deliver data and where traffic is coming from, it needs routing tables.
- A routing table primarily specifies the router's default path. As a result, it might not determine the optimum path to forward the data for a particular packet. For instance, the office router directs all networks to its internet service provider through a single default channel.
- Static and dynamic tables come in two varieties in the router. The dynamic routing tables are automatically updated by dynamic routers based on network activity, whereas the static routing tables are configured manually.

#Types of Router

1. **Broadband Routers:** These are one of the important kinds of routers. It is used to do different types of things. it is used to connect computers or it is also used to connect to the internet.
2. **Wireless routers:** These routers are used to create a wireless signal in your office or home. Wireless routers receive data packets over wired broadband, convert the packets written in binary code into radio signals that are picked up by electronic devices, and then convert them back into previous packets.
3. **Wired Routers:** Wired Router is used to connects multiple wired devices using a Ethernet cable, It takes the transmission data from the modem and distribute it to a further network, it is widely used in schools and small offices.
4. **Edge Routers:** As the name indicates, these are located at the edges usually connected to an Internet Service Provider, and distribute packets across multiple packets.
5. Core Routers: Core routers distribute packets within the same network. The main task is to carry heavy data transfers.
6. **Virtual Router:** They are implemented using a software on the virtual machine , and they are more flexible and scalable.
7. **Portable Routers:** They are used to create private Wi-Fi and hence designed for easy portability.

#Functions of Router

1. **Forwarding:** The router receives the packets from its input ports, checks its header, performs some basic functions like checking checksum, and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.
2. **Routing:** Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table that is made using different algorithms by the router only.
3. **Network Address Translation (NAT):** Routers use NAT to translate between different IP address ranges. This allows devices on a private network to access the internet using a single public IP address.
4. **Security:** Routers can be configured with firewalls and other security features to protect the network from unauthorized access, malware, and other threats.
5. **Quality of Service (QoS):** Routers can prioritize network traffic based on the type of data being transmitted. This ensures that critical applications and services receive adequate bandwidth and are not affected by lower-priority traffic.
6. **Virtual Private Network (VPN) connectivity:** Routers can be configured to allow remote users to connect securely to the network using a VPN.

7. **Bandwidth management:** Routers can be used to manage network bandwidth by controlling the amount of data that is allowed to flow through the network. This can prevent network congestion and ensure that critical applications and services receive adequate bandwidth.
8. **Monitoring and diagnostics:** Routers can be configured to monitor network traffic and provide diagnostics information in the event of network failures or other issues. This allows network administrators to quickly identify and resolve problems.

#Advantages of Router

- Easier Connection: Sharing a single network connection among numerous machines is the router's main job. This enables numerous people to connect to the internet, boosting total productivity. In addition, routers have connections between various media and network designs.
- Security: Undoubtedly, installing a router is the first step in securing a network connection. Because using a modem to connect directly to the internet exposes your computer to several security risks. So that the environment is somewhat secure, routers can be utilized as an intermediary between two networks. While not a firewall or antivirus replacement.
- NAT Usage: Routers use Network Address Translation (NAT) to map multiple private IP addresses into one public IP address. This allows for a better Internet connection and information flow between all devices connected to the network.
- Supports Dynamic Routing: The router employs dynamic routing strategies to aid in network communication. The internet work's optimum path is chosen through dynamic routing. Additionally, it creates collision and broadcast domains. Overall, this can lessen network traffic.
- Filtering of Packets: Switching between packets and filtering packets are two more router services. A collection of filtering rules are used by routers to filter the network. The packets are either allowed or passed through.

#Disadvantages of Router

- **Slower:** Routers analyze multiple layers of information, from the physical layer to the network layer, which slows down connections. The same issue can also be encountered when multiple devices are connected to these network devices, causing "connection waiting".
- **High Cost:** They are more expensive than some other tools for systems administration. This includes security, extension, and the focal point. As a result, routers are typically not the greatest option for issues.

- **Need for configuration:** The router must be properly configured to work properly. In general, the more complex the intended use, the more configuration is required. This requires professional installation, which can add to the cost of buying a router.
- **Quality Issues:** The time transitions are not always accurate. Even yet, some modern devices use the 2.4GHz band, which is frequently deactivated. These kinds of separations are frequently possible for those who live in apartments and condominiums.

- **Bandwidth shortages:** Dynamic routing techniques used by routers to support connections tend to cause network overhead, consuming a lot of bandwidth. This leads to a bandwidth shortage that significantly slows down the internet connection between connected devices.

Repeater:

- Repeaters are defined as a networking device that is used to amplify and generate the incoming signal.
- Repeaters work at the physical layer of the OSI model. The main aim of using a repeater is to increase the networking distance by increasing the strength and quality of signals.
- The performance of Local Area Networks (LANs) and Wide Area Networks (WANs) repeaters are used. Using repeaters helps to reduce error, and loss of data and provides with delivery of data at specified locations only.
- The major advantage of using a repeater is that it provides with transfer of data with more security and over a long distance.

#Features of Repeaters

1. **Repeater can regenerate the signal without modifying it.**
2. **Repeaters can be used in analog signals and digital signals.**
3. **Repeaters can extend the range of networks.**
4. **Dynamic networking is supported by repeater.**
5. **Use of Repeaters reduces error and loss of data.**
6. **Power is required for working of repeaters.**
7. **Using repeater can add complexity in the network.**

#Working of Repeaters

- **Initially the source system transmits the signals. This source systems can be a mobile phone, laptop or radio. This transmitted signal from the source system travels in air if it's wireless network or through the cable if it is wired network. As the signal goes away from the source it's strength gets weak.**

- **The signal received to the repeater is not the actual signal sent by source system but a weak signal. Therefore repeater amplifies this weak signal to get it strengthen.**
- **The strengthen signal is now being sent from the repeater to its destination. This signal is more stronger and can travel at longer distance. In short, it extends the network without losing the quality of signal.**
- **Repeaters are therefore used in various wireless technologies such as Wi-Fi and wired technologies such as ethernet.**

#Types of Repeaters

According to the functions and features repeaters are divided into four types. They are as follow:

1. According to the type of Signals

According to the type of signal being generated by the Repeater they are classified as:

- **Analog Repeater:** Analog repeaters are used to amplify only the analog signals. Analog repeaters receives the analog signal, amplifies it and then regenerates it as the output. Analog repeaters were mostly used in the older network technologies where analog signal was used.
- **Digital Repeater:** Digital repeaters are the type of repeaters that does not amplify digital signal but regenerates it directly. Digital repeaters are mostly used in the modern technologies where digital signal is being used. Digital repeaters are also capable to reconstruct a distorted signal.

2. According to the type of Connected Network

Based on the type of network the repeaters can connect they are categorized as below:

- **Wired Repeaters:** Wired repeaters are used in wired Local Area Networks(LANs). Wired repeater receives the signal and repeats it. This helps to extend the network travel data without loosing it's strength and data.
- **Wireless Repeaters:** Wireless repeaters are used in wireless Local Area Networks(LANs) and Cellular networks. A router connected in the network sends wireless signal to the repeater. Once received, repeater broadcast the signal to increase the coverage of network.

3. According to the Domain of LAN Networks

Based on the location of the Repeater in network they are connected, Repeaters are classified as below:

- **Local Repeaters:** Local Repeaters are used in Local Area Networks where the network is very small. The distance between the devices connected in network is very small.
- **Remote Repeaters:** Remote Repeaters are used in Local Area Networks where network is very large. The distance between the devices connected in network is more.

4. Based on Technologies

According to the technology used Repeater are further classified as:

- **Microwave Repeater:** Microwave repeaters are defined as a type of repeater that are embedded between the source and destination that is transmitting station and receiving station. The use of microwave repeater depends upon the distance between two devices. In microwave repeaters high power transmitters and sensitive receivers are used.
- **Optical Repeater:** Optical repeaters are defined as a type of repeaters that are used for the communication of fibre optic communication systems. Optical repeaters can amplify and reshape the operations before they are being transmitted. The optical repeater grabs all the signals from optical fiber cable into electronic form.
- **Radio Repeater:** Radio repeater is a type of repeater that transmits all the received data into radio signals. Radio repeaters has two different ports namely radio receiver and radio transmitter. Radio transmitter is used to retransmit the data that is received from repeater and radio receiver collects all the incoming data in form of signals.
- **Telephone Repeater:** Telephone repeaters are type of repeaters used for long distance networks. Amplifiers having transistors are used in telephone repeater. Telephone repeater is a bidirectional communication system. Telephone repeaters are majorly used for communication in submarines.

#Advantages of Repeater

1. **Better Performance of Network:** Repeaters provide with better performance of network because they do not always depend on processing overheads at the time.
2. **Cost Effective:** Repeaters are more cost effective as compared to other network devices therefore they are cost effective.
3. **Extends the network:** Repeaters provides with an advantage to extend the available network for transmission of data.
4. **No Physical barriers:** Using physical devices can led to some barrier while transmission of signals. With the help of wireless repeaters such issues are resolved.
5. **Enhanced Signals:** When computer devices and routers are connected in a network over long distance it weakens the strength of signals. While using repeaters it improves the strength of signals even over long distances.

#Disadvantages of Repeater

1. **Network Traffic:** Repeaters do not have features to segment the network traffic. Therefore repeaters do lack with the property to congestion.

2. **Network Segmentation:** As repeaters do not have feature to segment the network traffic repeaters cannot create a separate traffic from one cable to another.
3. **Limited number of repeaters:** Use of limited number of repeaters is supported by the network. If more number of repeaters are used that the specified one, it can even create collision of packets and increase the noise.
4. **Collision Domain:** The information is passed from various domains repeater is not able to separate the devices.

Bridge:

- Bridge is a local internetworking device that is used to connect two or more network segments together. A bridge operates at the Data Link Layer (Layer 2) of the OSI model and uses the MAC addresses of devices to make forwarding decisions.
- Bridges were first introduced in the 1980s as a way to connect Ethernet segments together and extend the reach of a network. They were initially used to overcome the distance limitations of Ethernet networks, allowing multiple segments to be connected together to form a larger network.
- Bridges work by examining the MAC addresses of devices on each network segment and forwarding packets only to the segment where the destination device is located. This helps to reduce network congestion and improve performance by limiting unnecessary traffic.
- Bridges can be used to connect different types of network segments, including Ethernet, Token Ring, and FDDI. They can also be used to connect wireless networks to wired networks, providing a way to extend the range and coverage of a wireless network.
- Local Internetworking is one which is within the same organization i.e. same building or same campus, then for the networking, we may not require the full power of the router. We can do it with a data link layer device called a bridge.
- Bridges: Bridges are a data link layer device and can connect to different networks as well as connect different networks of different types.
- Bridges from 802.x to 802.y where x & y may both be ethernet or one can be ethernet and other may be a token ring, etc. It locally connects small LANs, whereas if LANs are big then bridges can no longer handle them. Bridge follows a protocol in IEEE format execute 802.1 which is a spanning tree of bridges.

#Applications of Bridges:

1. **Network segmentation:** Bridges are used to divide large networks into smaller segments to improve network performance and reduce network congestion. By creating separate collision domains, bridges can help to reduce the number of data collisions on the network, improving overall network efficiency.

2. **Extension of network reach:** Bridges are used to extend the reach of a network by connecting multiple network segments together. This allows devices that are physically located in different segments to communicate with each other as if they were on the same segment.
3. **Interconnection of different network types:** Bridges can be used to connect different types of network segments, including Ethernet, Token Ring, and FDDI networks. This allows networks using different technologies to communicate with each other, improving interoperability between different network systems.
4. **Wireless network bridging:** Bridges are commonly used to connect wireless networks to wired networks. This allows wireless access points to be connected to the wired network, providing a way to extend the range and coverage of the wireless network.
5. **Network redundancy:** Bridges can be used to create redundant network paths, which provide a backup in case the primary network path fails. This improves network reliability and reduces the risk of network downtime.

#Advantages of Bridges:

1. **Improved Network Performance:** Bridges can improve network performance by reducing network congestion and improving data transmission speeds, resulting in faster network speeds and reduced latency.
2. **Better Network Security:** Bridges can help to improve network security by creating logical isolation between different network segments, preventing unauthorized access and reducing the risk of network attacks.
3. **Flexible Network Design:** Bridges allow for flexible network design by enabling the connection of different network technologies and types, including Ethernet, Token Ring, and FDDI, among others.
4. **Easy to Install and Configure:** Bridges are relatively easy to install and configure, requiring minimal configuration and maintenance, making them an ideal solution for small to medium-sized networks.

#Disadvantages of Bridges:

1. **Limited Scalability: Bridges may not be scalable in larger networks, as the number of devices and network segments increases, which can lead to network congestion and performance degradation.**
2. **Single Point of Failure: Bridges can be a single point of failure in the network, and if they fail, it can cause network downtime until the bridge is replaced.**
3. **Limited Functionality: Bridges have limited functionality compared to other network devices, such as routers and switches, and may not be suitable for all network configurations and requirements.**

Gateway:

- Gateway is connecting point of any network that helps it to connect with different networks.
- The gateway monitors and controls all the incoming and outgoing traffic of the network. Suppose there are two different networks and they want to communicate with each other. So to communicate with each other they need to set up a path between them. Now that path will be made between gateways of those different networks.
- Gateways are also known as protocol converters because they help to convert protocol supported by traffic of the different networks into that are supported by this network. Because of that, it makes smooth communication between two different networks.

#How does Gateway work?

Gateway has a simple working methodology of five steps-

1. It gets data from the network
2. It intercepts and analyzes the received data.
3. It routes the data to the destination address
4. It converts the received data to make that compatible with the receiver network
5. It sends the final data inside the network

#Different Functionality of Gateways

There are various functionality that is supported by any gateway-

1. **LAN to WAN connections-** It can be used to connect a group of personal computers i.e. LAN(Local Area Network) to the Internet i.e. WAN(Wide Area Network).
2. **Controls incoming and outgoing data–** It is located on the boundary of any network, so it controls incoming and outgoing data packets from/to any network.
3. **Works as a Protocol Converter-** It makes sure that the data packet from another network is compatible with this network. So it converts their protocols into supported protocols and other stuff of the data packets before it enters into the network.
4. **Information Collector-** It collects data from different sections of the network to make a better diagnosis of any data packets. In this process, it collects information.
5. **Routing of data packets-** It is responsible for routing data packets to different networks because it knows about the routing path of different networks that are in communication with its own network.

#Different Types of Gateways

1. **Unidirectional Gateways-** It allows the flow of data in only one direction. It means the changes that occurred in the source can be copied to the destination but the changes that occurred in the destination can't be copied to the source.
2. **Bidirectional Gateways:** It allow the flow of data in both directions. It means changes occurred in the source can be copied to the destination and changes that occurred in the destination can be copied to the source.
3. **Email Security Gateway-** It scans email for any type of malicious content before allowing it to enter into the network.
4. **Cloud Storage Gateway-** It helps in data transfer between the cloud and the nodes of the network. It converts different API requests into that form which can be understandable by cloud platforms.

#Advantages

1. It helps in connecting two different network
2. It filters and does not allow anything that can harm to the network
3. It helps by doing protocol conversion
4. It provides security from external attacks

#Disadvantages

1. It's implementation is difficult and costly
2. It is hard to manage
3. It causes time delay because the conversion of data according to the network takes time
4. Failure of the gateway can cause the failure of connection with other network

Modem:

- Modem stands for Modulator/Demodulator. The modem is defined as a networking device that is used to connect devices connected in the network to the internet.
- The main function of a modem is to convert the analog signals that come from telephone wire into a digital form. In digital form, these converted signals are stored in the form of 0s and 1s.
- The modem can perform both the task of modulation and demodulation simultaneously. Modems are majorly used to transfer digital data in personal systems.

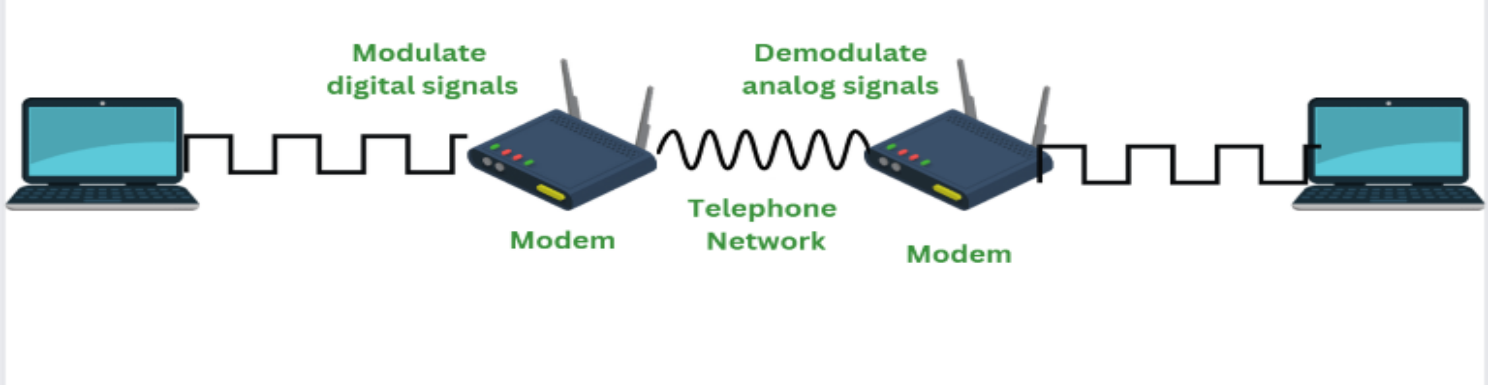
- The modem is also known as a signal translator as it translates one signal into another signal by modulating the digital signal into an analog signal for transmission and then demodulates receiving analog signals into digital signals.

#Features of Modem

1. Modems can modulate as well as demodulate the signals simultaneously.
2. Modem allows to connect only a specific number of devices to the internet.
3. According to the features of modem, it's price ranges.
4. Modems can be upgraded with the help of a specific software patch.
5. To use the devices over the internet with a modem devices need to be configured with an Internet Service Provider(ISP).
6. When the modem is connected to Hub it slows down its process.

#Working of Modem

The two main components of a modem are modulation and demodulation. Where the modem can perform both tasks simultaneously. The step-by-step working of the modem is given below:



Step 1: Data Generation: When data needs to be transmitted it is first generated. Therefore computer system generated the data which is in digital form of 0s and 1s.

Step 2: Modulation: Modulation is defined as a process of converting digital data signals of the computer into analog data signals so that these signals can travel on the internet. The digital data is encoded onto a carrier wave.

Step 3: Transmission: The resultant of modulation that is modulated data is transmitted over the communication line to the modem that is receiving it.

Step 4: Demodulation: Demodulation is defined as a process in which analog data signals from the internet are converted into digital data signals so they can be understood by computer systems. In the process of demodulation the digital data from the carrier wave is decoded.

Step 5: Decoding: The resultant of demodulation that is demodulated data is being sent to the computer systems for their further use.

#Types of Modem

1. Optical Modem : In modem, different type of media is used to transfer the signals. Optical Modem is the type of modem that makes use of optical cables instead of using another metallic type of media. The digital data is converted into the pulse of light that is transmitted on the optical fiber used in the optical Modem.

2. Digital Modem : Digital Modem is defined as a type of modem that is used to convert digital data into digital signals. Digital data is in form of 0s and 1s. For this, it performs the process of modulation. Digital Modem modulates the digital data on digital carrier signals for transmission.

3. Cable Modem : Cable modems are defined as a type of modem used to establish a communication between computer systems and the Internet Service Providers. A cable modem helps to access high-speed data through cable TV networks. Such modems are usually connected to desktops or systems and work like external devices.

4. Satellite Modem: Satellite Modems are defined as a type of modem that provides with the internet connection through satellite dishes. This type of modem works by sending the input bits into output radio signals and vice versa. The internet network that is provided by such types of modems is more reliable and efficient as compared to other types of modems.

5. Dial Modem : A Dial Modem is a type of modem that converts data used in telephone and data used on computers. In short dial modem converts between analog form and digital form. The networking devices connected to the computer are all at one end and the telephone line is at another end. This type of modem transmits the data at a speed of 56000 per/sec.

#Advantages of Modem

1. A modem converts digital signals into an analog signal.
2. The cost of a modem increases according to the features it has.
3. The modem helps to connect the LAN to the internet.
4. Modem performs both modulation and demodulation processes simultaneously

#Disadvantages of Modem

1. The working of the modem slows down when connected to the hub.
2. The modem cannot track the traffic between the LAN and the internet.
3. When using a modem a limited number of network devices can be connected to the internet.
4. Modems have a high rock of security-related attacks.
5. The modem does not provide maintenance of traffic.

Wireless infrastructure Components:

1. **Access Points (APs):** Access points serve as the central points of connection in a wireless network. They enable wireless devices, such as laptops or smartphones, to connect to the wired network infrastructure.
2. **Wireless Routers:**
    - Wireless routers combine the functionality of a traditional wired router with that of a wireless access point.
    - They facilitate both wired and wireless communication within a network.
3. **Wireless Network Interface Cards (NICs):**
    - NICs are hardware components that allow devices like computers or laptops to connect to a wireless network.
    - These are often integrated into devices or added externally.
4. **Wireless Bridges:**
    - Wireless bridges connect two separate wired networks over a wireless link, extending the network without the need for physical cables.
5. **Wireless Repeaters/Range Extenders:**
    - These devices amplify and retransmit wireless signals, extending the range of a wireless network.
    - Repeaters help overcome obstacles or improve coverage in areas with weak signals.
6. **Wireless Controllers:**
    - In larger wireless networks, controllers manage and coordinate multiple access points.
    - They provide centralized management, security, and configuration settings for the entire wireless infrastructure.
7. **Antennas:**
    - Antennas are crucial components for transmitting and receiving wireless signals.
    - Different types of antennas, such as omni-directional and directional antennas, are used based on the network's requirements.
8. **Wireless Security Devices:**
    - Devices like firewalls and intrusion detection/prevention systems are important for securing wireless networks.
    - Encryption protocols (e.g., WPA, WPA2, WPA3) and authentication mechanisms add layers of security.

9. **Wireless LAN Controllers (WLC):**
    - WLCs manage and control multiple access points in a wireless local area network (WLAN).
    - They assist in load balancing, roaming, and enforcing security policies.
10. **Mobile Devices:** End-user devices, such as smartphones, tablets, laptops, and other mobile devices, are integral parts of a wireless network.
11. **Power over Ethernet (PoE) Equipment:** PoE equipment enables the delivery of power and data over a single Ethernet cable, commonly used to power devices like access points and IP cameras.