Unit 1
Introduction to Computer Network

Definition:

A computer network is a group of interconnected nodes or computing devices that exchange data and resources with each other. A network connection between these devices can be established using cable or wireless media.

Goals and Applications of Computer Networks: The following are some important goals of computer networks:

1. **Resource Sharing –** Many organizations have a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner, etc.

2. **High Reliability –** If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.

3. **Inter-process Communication –** Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.

4. **Flexible access –** Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.
5. **Security–** Computer networks must be secure to protect against unauthorized access, data breaches, and other security threats. This includes implementing measures such as firewalls, antivirus software,

and encryption to ensure the confidentiality, integrity, and availability of data.

6. **Performance**– Computer networks must provide high performance and low latency to ensure that applications and services are responsive and available when needed. This requires optimizing network infrastructure, bandwidth utilization, and traffic management.
7. **Scalability-** Computer networks must be designed to scale up or down as needed to accommodate changes in the number of users, devices, and data traffic. This requires careful planning and management to ensure the network can meet current and future needs.

   Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication, etc.

Advantages:

Resource sharing: Networks enable the sharing of resources such as printers, scanners, storage devices, and software applications, which can reduce costs and increase efficiency.

Communication and collaboration: Networks provide a platform for communication and collaboration among users, allowing for easy sharing of information and ideas.

Centralized management: Networks allow for centralized management of devices, users, and resources, making it easier to control and monitor the network.

Scalability: Networks can be scaled up or down to accommodate changes in the number of users, devices, or data volume.

Accessibility: Networks can provide remote access to resources, enabling users to work from anywhere and improving accessibility to information and resources.

Disadvantages:

Security vulnerabilities: Networks can be vulnerable to security threats such as hacking, viruses, and malware, which can compromise sensitive **data and disrupt network operations.**

Complexity: Networks can be complex to set up, configure, and maintain, requiring specialized knowledge and expertise.

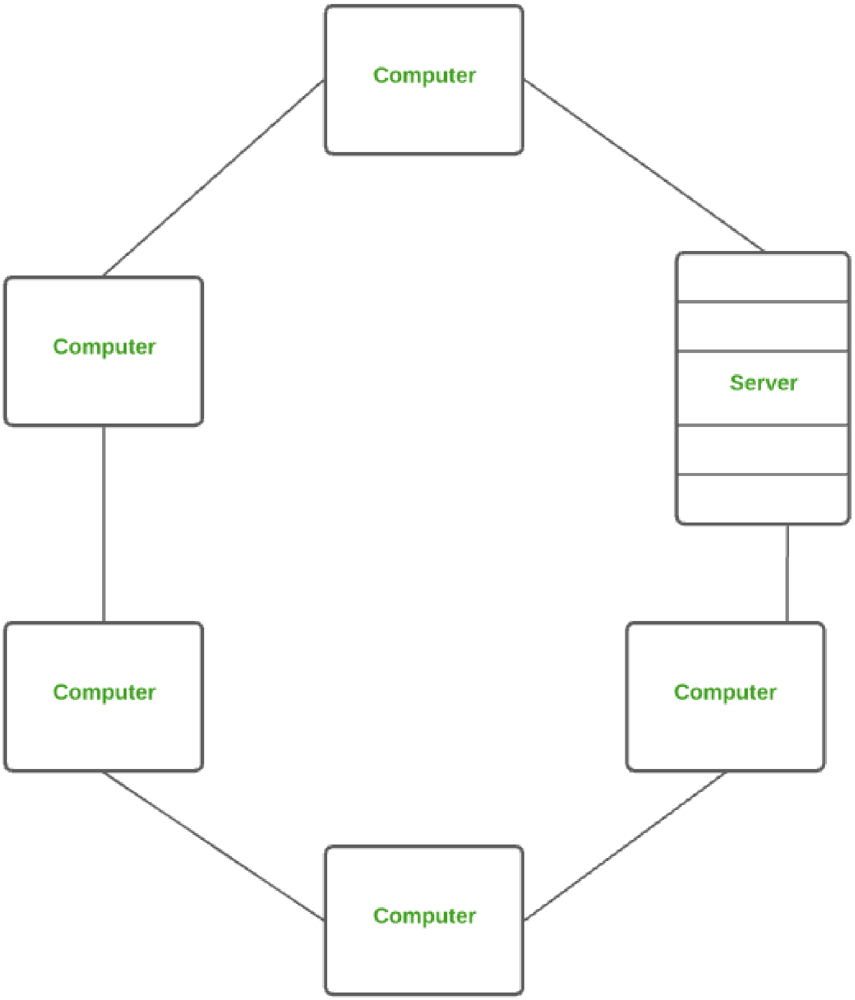
Dependence on infrastructure: Networks depend on the underlying infrastructure such as cables, routers, switches, and servers, which can be prone to failures or downtime, disrupting network operations.

Cost: Networks can be expensive to set up and maintain, requiring investments in hardware, software, and personnel.

Performance limitations: Networks have performance limitations such as bandwidth constraints, latency, and congestion, which can affect the speed and reliability of network operations.

What is LAN(Local Area Network)?

LAN stands for **Local-area Network**. It is a Computer Network that covers a relatively small area such as within a building or campus of up to a few kilometers in size. LANs are generally used to connect personal computers and workstations in company offices to share common resources, like printers, and exchange information. A number of experimental and early commercial LAN technologies were developed in the 1970s. LANs nearly always connect devices to the network via Ethernet, WiFi, or both of these technologies.



How Do LANs Work?

A router serves as the hub where the majority of LANs connect to the Internet. Home LANs often utilize a single router, but bigger LANs may also use network switches to transmit packets more effectively.

Benefits of a LAN?

- **Privacy:** LAN is a private network, thus no outside regulatory body controls it, giving it privacy.
- **High Speed:** LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.
- **Supports different transmission mediums:** LAN supports a variety of communications transmission medium such as an Ethernet

cable (thin cable, thick cable, and twisted pair), fiber and wireless transmission.

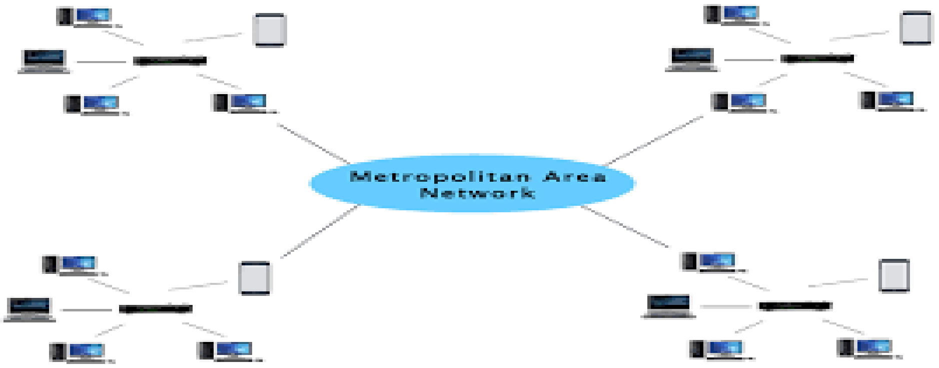
- **Inexpensive and Simple:** A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively easy to use, good scalability.

Drawback of LAN?

- The initial setup costs of installing Local Area Networks is high because there is special software required to make a server.
- Communication devices like an ethernet cable, switches, hub, routers, cables are costly.
- LAN administrators can see and check personal data files as well as Internet history of each and every LAN user. Hence, the privacy of the users are violated
- LANs are restricted in size and cover only a limited area
- Since all the data is stored in a single server computer, if it can be accessed by an unauthorized user, it can cause a serious data security threat.

What is a metropolitan area network (MAN)?

A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network but smaller than a . MANs do not have to be in urban areas; the term "metropolitan" implies the size of the network, not the demographics of the area that it serves. Like WANs, a MAN is made up of interconnected LANs. Because MANs are smaller, they are usually more efficient than WANs, since data does not have to travel over large distances. MANs typically combine the networks of multiple organizations, instead of being managed by a single organization.Most MANs use fiber optic cables to form connections between LANs. Often a MAN will run on "dark fiber" — formerly unused fiber optic cables that are able to carry traffic. These fiber optic cables may be leased from private-sector Internet service providers (ISP).In some cases, this model is reversed: a city government builds and maintains a metropolitan fiber optic network, then leases dark fiber to private companys.



Advantages and disadvantages of metropolitan area network

The term MAN full form is a metropolitan area network. It is in between LAN and WAN technology and that covers the entire city. It is very similar to LAN technology. Here this article gives information about the advantages and disadvantages of MAN to know more details about it.

Advantages of MAN :

- It provides higher security compare to WAN
- It is wider than LAN
- It helps in cost-effective sharing of common resources such as printer etc

- It helps people interface fast LANs together. This is due to easy implement of links
- MAN require fewer resources compare to WAN. This saves the implementation cost
- The dual bus used in MAN help the transmission of data in both direction simultaneously
- It provides a good backbone for a large network and also provides greater access to WAN
- A MAN is usually encompasses several block of city or an entire city
- Increases the efficiency of handling data
- Increases the speed of transfer data
- Easy to implement link
- Save the cost attach to establish a wide area network

Disadvantages of MAN :

- More cable require for a MAN connection from one place to another
- The data rate is slow compared to LAN
- It is difficult to make a system secure from hackers
- The large network difficult to manage
- It is difficult to secure the network once its becomes large
- Network installation requires skilled technicians and network administrators. This increases overall installation and management costs
- Cost is higher than LAN
- While we move our network to another city or area it doesn't work

What Is a WAN?

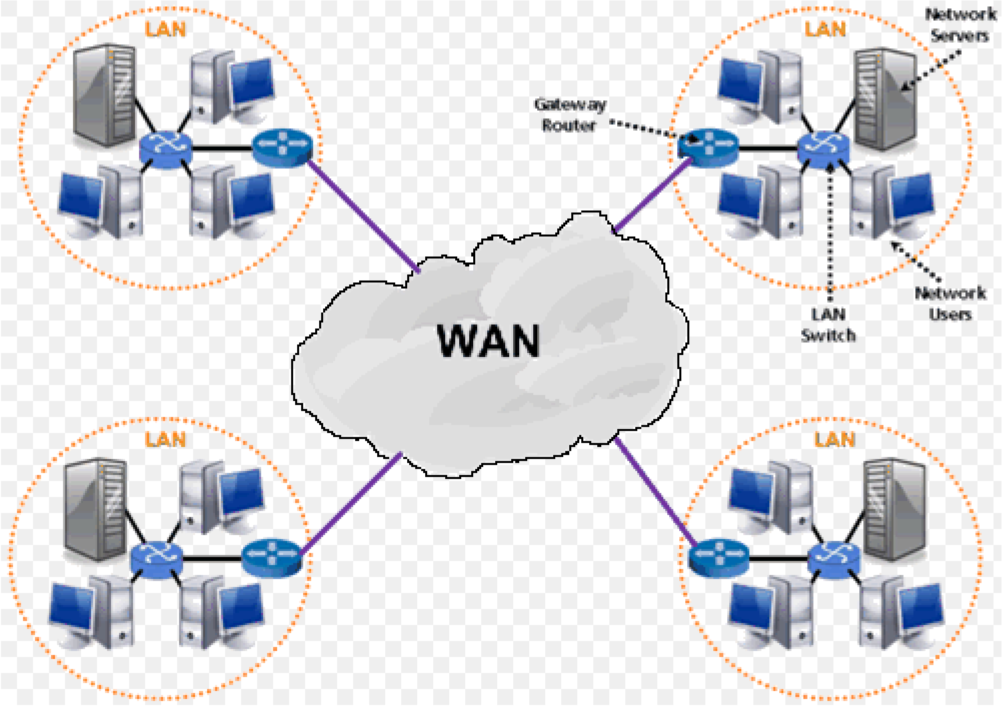
A wide area network (WAN) is a computer network that covers a large geographical area comprising a region, a country, a continent or even the whole world. WAN includes the technologies to transmit data, image, audio and video information over long distances and among different LANs and MANs.

The distinguishing features of WAN are

- WANs have a large capacity, connecting a large number of computers over a large area, and are inherently scalable.
- They facilitate the sharing of regional resources.
- They provide uplinks for connecting LANs and MANs to the Internet.
- Communication links are provided by public carriers like telephone networks, network providers, cable systems, satellites etc.
- Typically, they have low data transfer rate and high propagation delay, i.e.they have low communication speed.
- They generally have a higher bit error rate.

Example of WAN

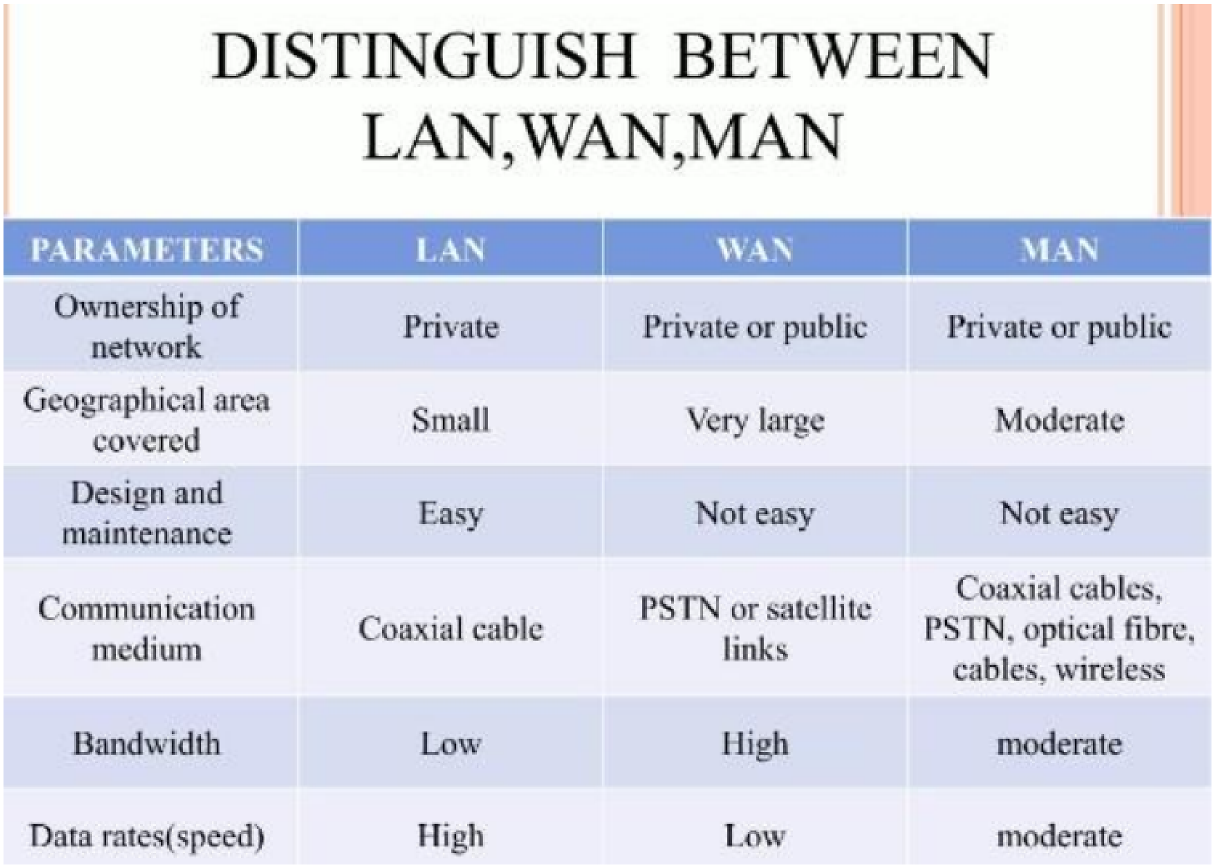
The Internet



4G

Mobile Broadband Systems

Difference between LAN, MAN and WAN:



DISTINGUISH BETWEEN LAN,WAN,MAN

PARAMETERS	LAN	WAN	MAN
Ownership of network	Private	Private or public	Private or public
Geographical area covered	Small	Very large	Moderate
Design and maintenance	Easy	Not easy	Not easy
Communication medium	Coaxial cable	PSTN or satellite links	Coaxial cables, PSTN, optical fibre, cables, wireless
Bandwidth	Low	High	moderate
Data rates(speed)	High	Low	moderate

What is client server architecture?

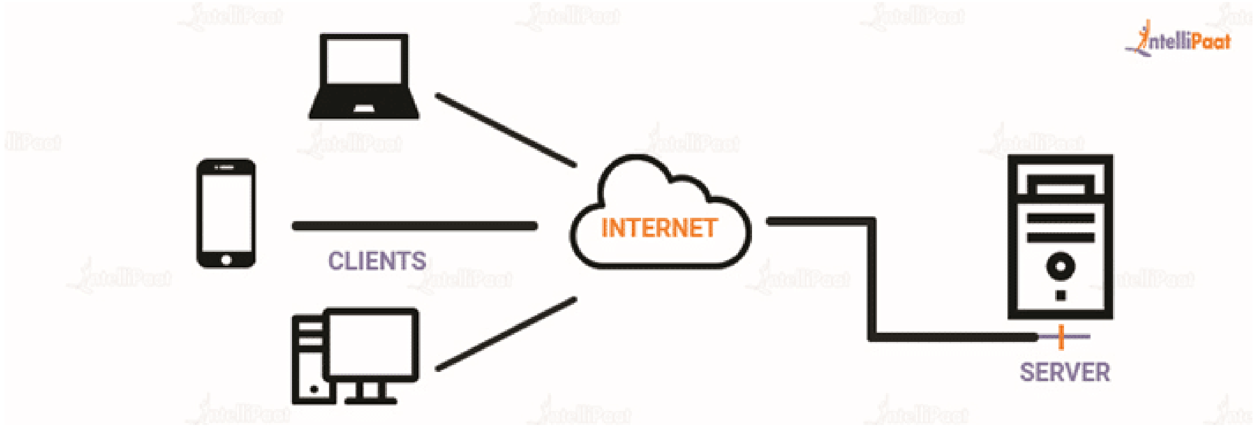
Before we explain client server architecture and you start reading words such as servers, service, network, data, and files, and start feeling overwhelmed with jargon, let us first understand about this architecture in layperson's terms.

The notion of client-server architecture can be understood by the analogy of ordering a pizza for delivery. You call the store to order a pizza and someone picks up the call, takes your order, and then delivers it. Simple, right? Yes, this analogy pretty much answers the fundamental principle of client server architecture.

Simply put, two factors are involved :

- A server is the one who provides requested services.

- Clients are the ones who request services.

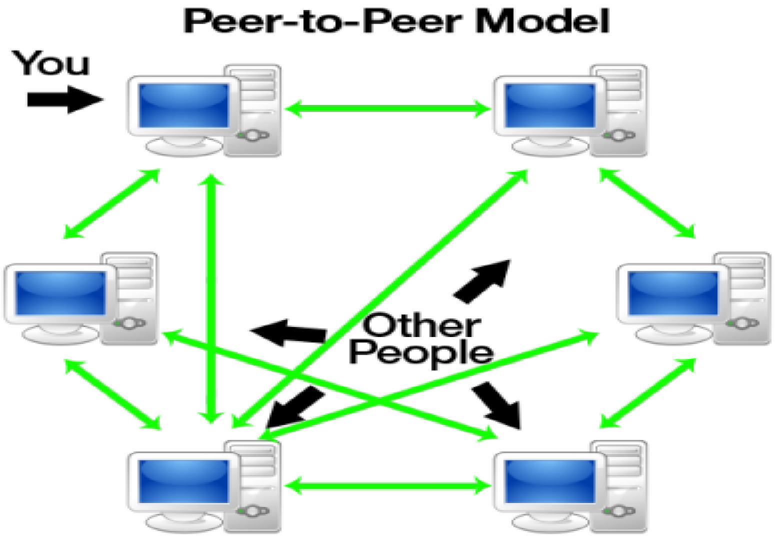


What is Peer to Peer architecture?

Client-server architecture is a computing model in which the server hosts, delivers, and manages most of the resources and services requested by the client. It is also known as the networking computing model or client-server network as all requests and services are delivered over a network. The client-server architecture or model has other systems connected over a network where resources are shared among the different computers.

Typically, client-server architecture is arranged in a way that clients are often situated at workstations or on personal computers, while servers are located elsewhere on the network, usually on more powerful machines. Such a model is especially beneficial when the clients and server perform routine tasks. For example, in hospital data processing, a client computer can be busy running an application program for entering patient information, meanwhile, the server computer can be running another program to fetch and manage the database in which the information is permanently stored.

f Peer to Peer Architecture In the common client-server architecture, multiple clients will communicate with a central server. A peer-to-peer (P2P) architecture consists of a decentralized network of peers - nodes that are both clients and servers. P2P networks distribute the workload between peers, and all peers contribute and consume resources within the network without the need for a centralized server. However, not all peers are necessarily equal. Super peers may have more resources and can contribute more than they consume. Edge peers do not contribute any resources, they only consume from the network. In its purest form, P2P architecture is completely decentralized. However, in application, sometimes there is a central tracking server layered on top of the P2P network to help peers find each other and manage the network. Here's a simple example of small P2P network.



Some uses of P2P architecture:

- File sharing
- Instant messaging
- Voice Communication
- Collaboration

- High Performance Computing

Some examples of P2P architecture:

- Napster - it was shut down in 2001 since they used a centralized tracking server

- BitTorrent - popular P2P file-sharing protocol, usually associated with piracy

- Skype - it used to use proprietary hybrid P2P protocol, now uses client-server model after Microsoft's acquisition

- Bitcoin - P2P cryptocurrency without a central monetary authority

What are Hybrid networks?

Hybrid networks are the networks that are based on both peer-to-peer & client-server relationships. Hybrid networks incorporate the best features of workgroups in peer-to-peer networks with the performance, security and reliability of server-based networks. Hybrid networks still provide all of the centralized services of servers, but they also allow users to share and manage their own resources within the workgroup.

Advantages of Hybrid Network

1. Client Server applications are still centrally located and managed.
2. Users can assign local access to resources in their computers.
3. Workgroups can manage resources without requiring assistance from network administrators.

Disadvantages of Hybrid Network

1. Users may need to remember multiple passwords.
2. Files can be duplicated and changes overwritten between the computers with the shared folder and the Server.

What is a network protocol?

In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless.

Standardized protocols are like a common language that computers can use, similar to how two people from different parts of the world may not understand each other's native languages, but they can communicate using a shared third language. If one computer uses the Internet Protocol (IP)and a second computer does as well, they will be able to communicate — just as the United Nations relies on its 6 official languages to communicate amongst representatives from all over the globe. But if one computer uses IP and the other does not know this protocol, they will be unable to communicate.

Network Layer Design Issues:

The network layer or layer 3 of the OSI (Open Systems Interconnection) model is concerned with delivery of data packets from the source to the destination across multiple hops or links. It is the lowest layer that is concerned with end − to − end transmission. The designers who are concerned with designing this layer need to cater to certain issues. These issues encompass the services provided to the upper layers as well as internal design of the layer.

The design issues can be elaborated under four heads −

- Store − and − Forward Packet Switching
- Services to Transport Layer
- Providing Connection Oriented Service
- Providing Connectionless Service

1. Store − and − Forward Packet Switching

The network layer operates in an environment that uses store and forward packet switching. The node which has a packet to send, delivers it to the nearest router. The packet is stored in the router until it has fully arrived and its checksum is verified for error detection. Once, this is done, the packet is forwarded to the next router. Since, each router needs to store the entire packet before it can forward it to the next hop, the mechanism is called store – and – forward switching.

2. Services to Transport Layer

The network layer provides service its immediate upper layer, namely transport layer, through the network – transport layer interface. The two types of services provided are –

Connection – Oriented Service – In this service, a path is setup between the source and the destination, and all the data packets belonging to a message are routed along this path.

Connectionless Service – In this service, each packet of the message is considered as an independent entity and is individually routed from the source to the destination.

The objectives of the network layer while providing these services are –

The services should not be dependent upon the router technology.

The router configuration details should not be of a concern to the transport layer.

A uniform addressing plan should be made available to the transport layer, whether the network is a LAN, MAN or WAN.

3. Providing Connection Oriented Service

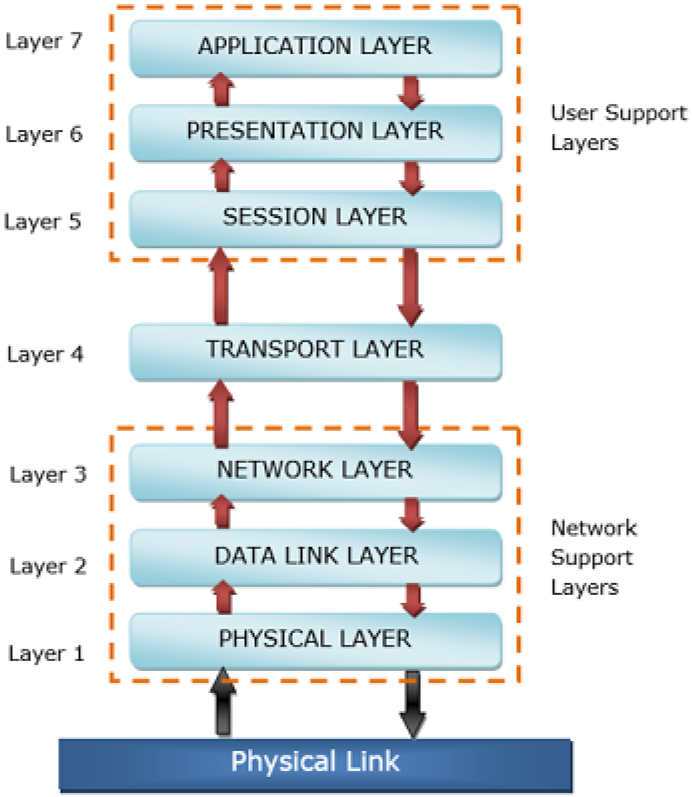
In connection – oriented services, a path or route called a virtual circuit is setup between the source and the destination nodes before the transmission starts. All the packets in the message are sent along this route. Each packet contains an identifier that denotes the virtual circuit to which it belongs to. When all the packets are transmitted, the virtual circuit is terminated and the connection is released. An example of connection – oriented service is MultiProtocol Label Switching (MPLS).

4. Providing Connectionless Service

In connectionless service, since each packet is transmitted independently, each packet contains its routing information and is termed as datagram. The network using datagrams for transmission is called datagram networks or datagram subnets. No prior setup of routes are needed before transmitting a message. Each datagram belong to the message follows its own individual route from the source to the destination. An example of connectionless service is Internet Protocol or IP.

The OSI Reference Model

OSI or Open System Interconnection model was developed by International Standards Organization (ISO). It gives a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. It has seven interconnected layers. The seven layers of the OSI Model are a physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer, as shown in the following diagram −



The physical layer, data link layer and the network layer are the network support layers. The layers manage a physical transfer of data from one device to another. Session layer, presentation layer, and application layer are the user support layers. These layers allow communication among unrelated software in dissimilar environments. Transport layer links the two groups.

The main functions of each of the layers are as follows –

Physical Layer – Its function is to transmit individual bits from one node to another over a physical medium.

Data Link Layer – It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.

Network Layer – It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.

Transport Layer –It is responsible for delivery of the entire message from the source host to destination host.

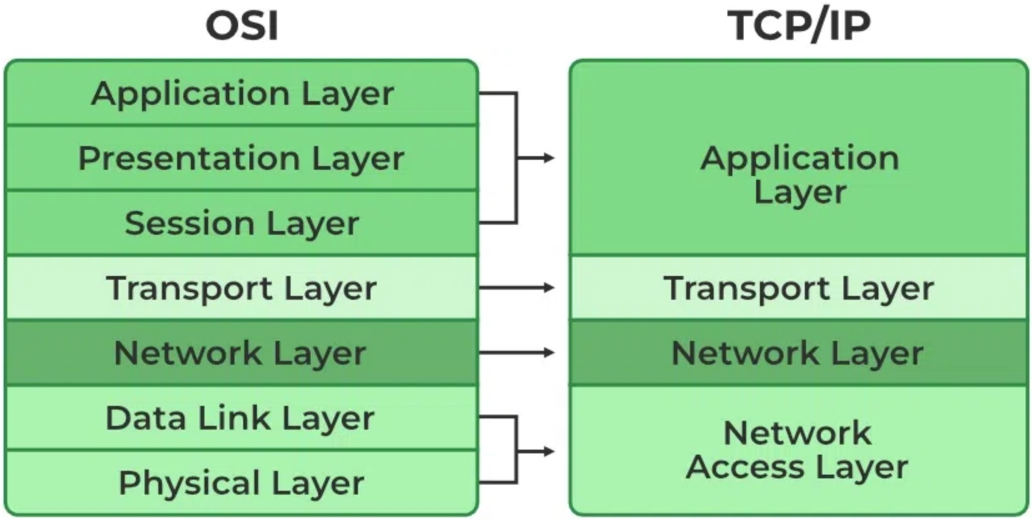
Session Layer – It establishes sessions between users and offers services like dialog control and synchronization.

Presentation Layer – It monitors syntax and semantics of transmitted information through translation, compression, and encryption.

Application Layer – It provides high-level APIs (application program interface) to the users.

TCP/IP Model

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.



1. Physical Layer
It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

2. Data Link Layer
The packet's network protocol type, in this case, TCP/IP, is identified by the data-link layer. Error prevention and "framing" are also provided by the data-link layer. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

3. Internet Layer
This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:

IP: IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.

4. Transport Layer
The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error.

End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

TCP: Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.

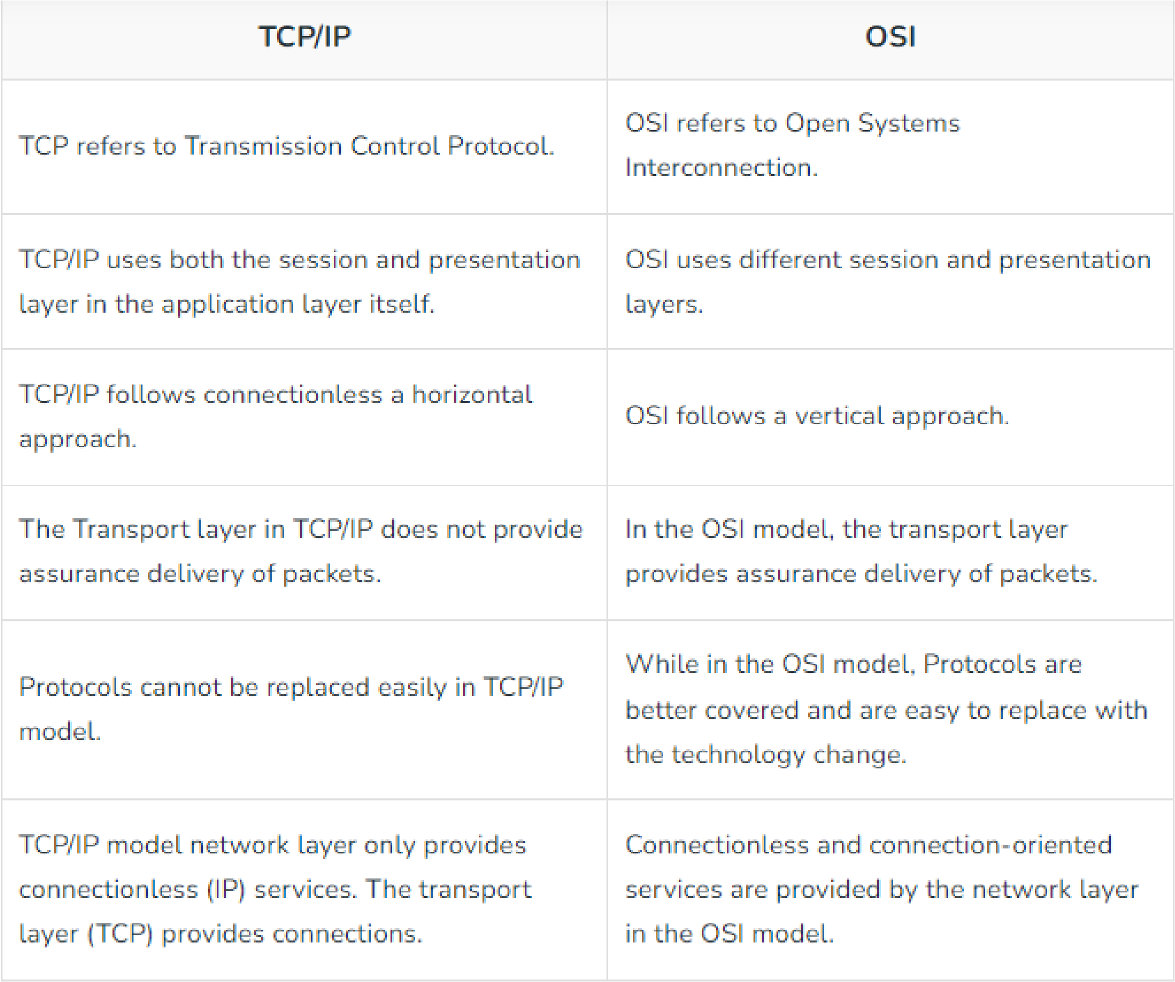
UDP: The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

5. Application Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:

HTTP and HTTPS: HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.

Difference between TCP/IP and OSI Model



TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP uses both the session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP follows connectionless a horizontal approach.	OSI follows a vertical approach.
The Transport layer in TCP/IP does not provide assurance delivery of packets.	In the OSI model, the transport layer provides assurance delivery of packets.
Protocols cannot be replaced easily in TCP/IP model.	While in the OSI model, Protocols are better covered and are easy to replace with the technology change.
TCP/IP model network layer only provides connectionless (IP) services. The transport layer (TCP) provides connections.	Connectionless and connection-oriented services are provided by the network layer in the OSI model.

Types of Network Topology

In Computer Network ,there are various ways through which different components are connected to one another. **Network Topology** is the way that defines the structure, and how these components are connected to each other.

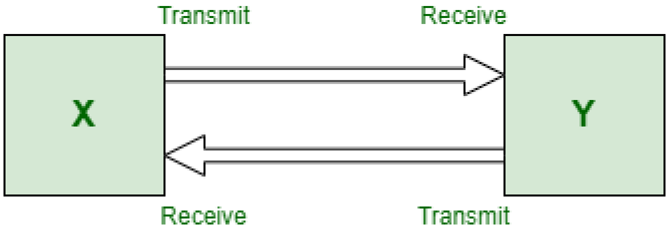
Types of Network Topology

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**. The various network topologies are:

- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Tree Topology
- Hybrid Topology

1. Point to Point Topology

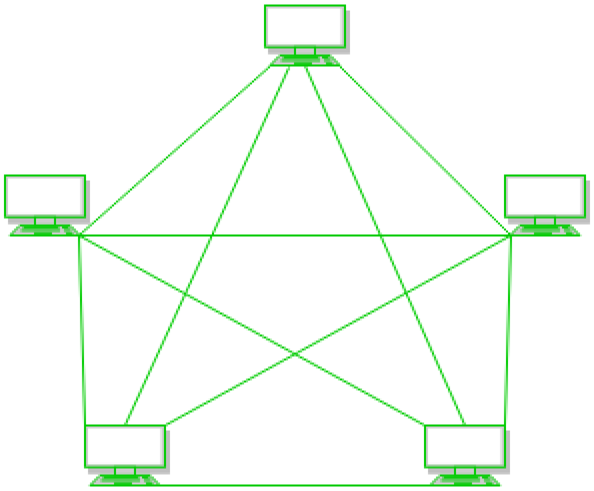
Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Point to Point Topology

2. Mesh Topology

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.



- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is $_{N}C_{2}$ i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.

- Provides security and privacy.

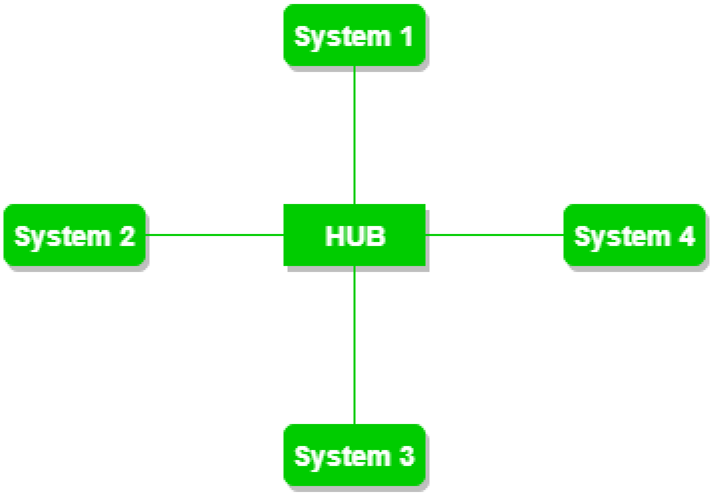
Drawbacks of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

3. Star Topology

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.



Star Topology

A star topology having four systems connected to a single point of connection i.e. hub.

Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Drawbacks of Star Topology

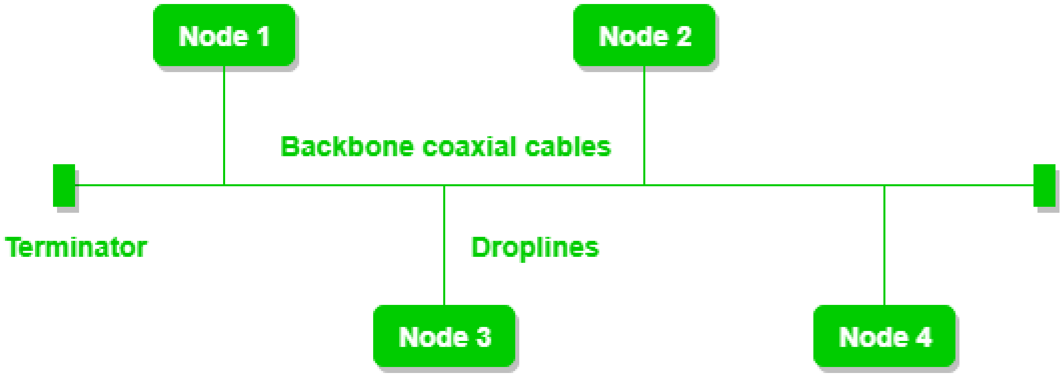
- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.

- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

4. Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Bus Topology

Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Drawbacks of Bus Topology

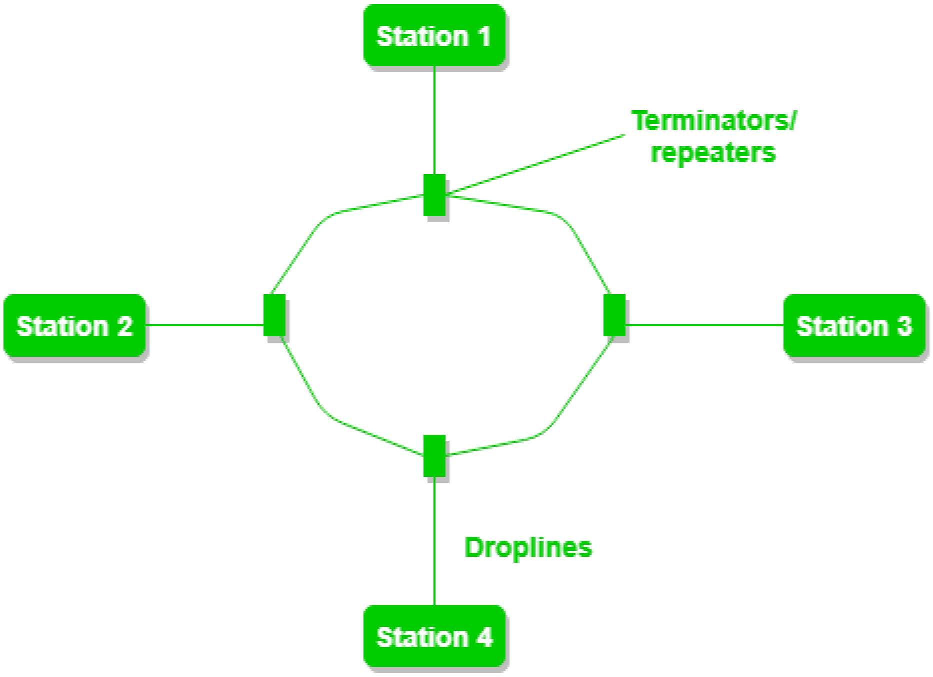
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

5. Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Ring Topology

Figure 4: A ring topology comprises 4 stations connected with each forming a ring.

The most common access method of ring topology is token passing.

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

Operations of Ring Topology

1. One station is known as a **monitor** station which takes all the responsibility for performing the operations.
2. To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

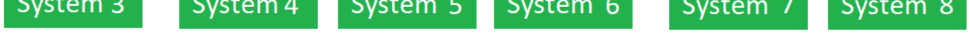
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Drawbacks of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

6. Tree Topology

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



Tree Topology

Figure 5: In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

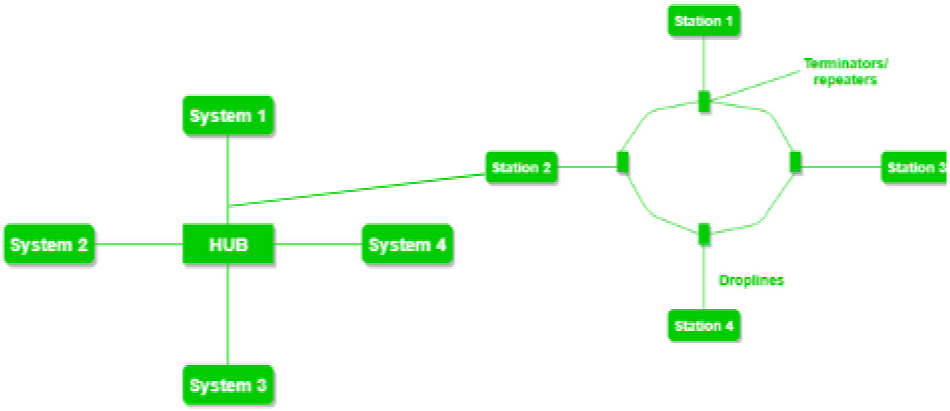
Drawbacks of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

7. Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Hybrid Topology

Figure 6: The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Advantages of Hybrid Topology

- This topology is **very flexible**.
- The size of the network can be easily expanded by **adding new devices.**

Drawbacks of Hybrid Topology

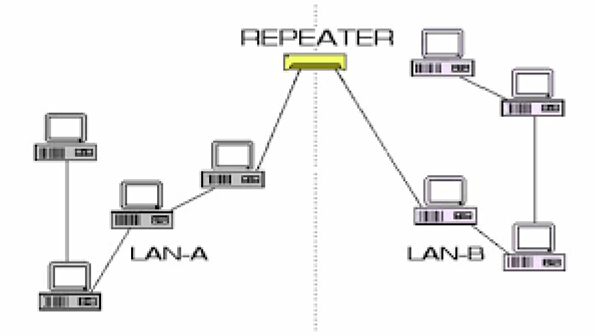
- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**.

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

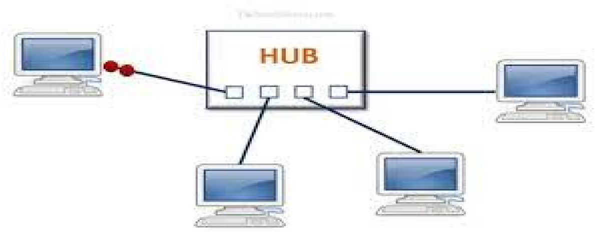
Network Hardware Devices:

Network Devices: Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway etc

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.



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

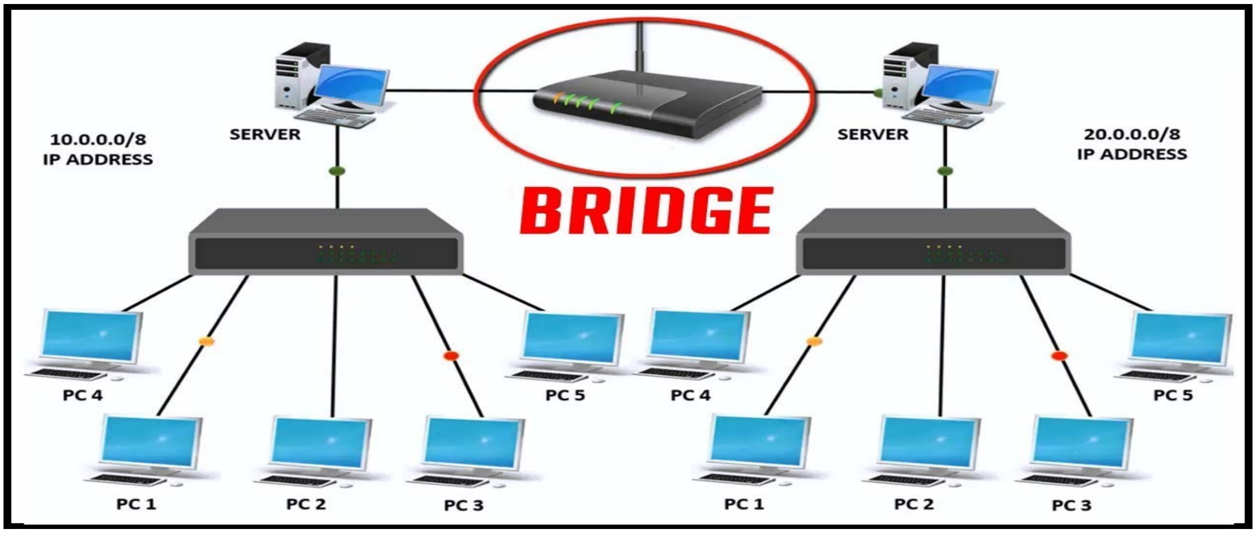


Types of Hub

- Active Hub:- These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- Passive Hub:- These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- Intelligent Hub:- It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single

output port, thus making it a 2 port device.

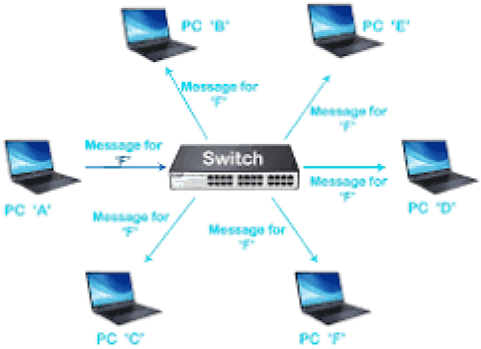


Types of Bridges

- Transparent Bridges:- These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- Source Routing Bridges:- In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform

error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

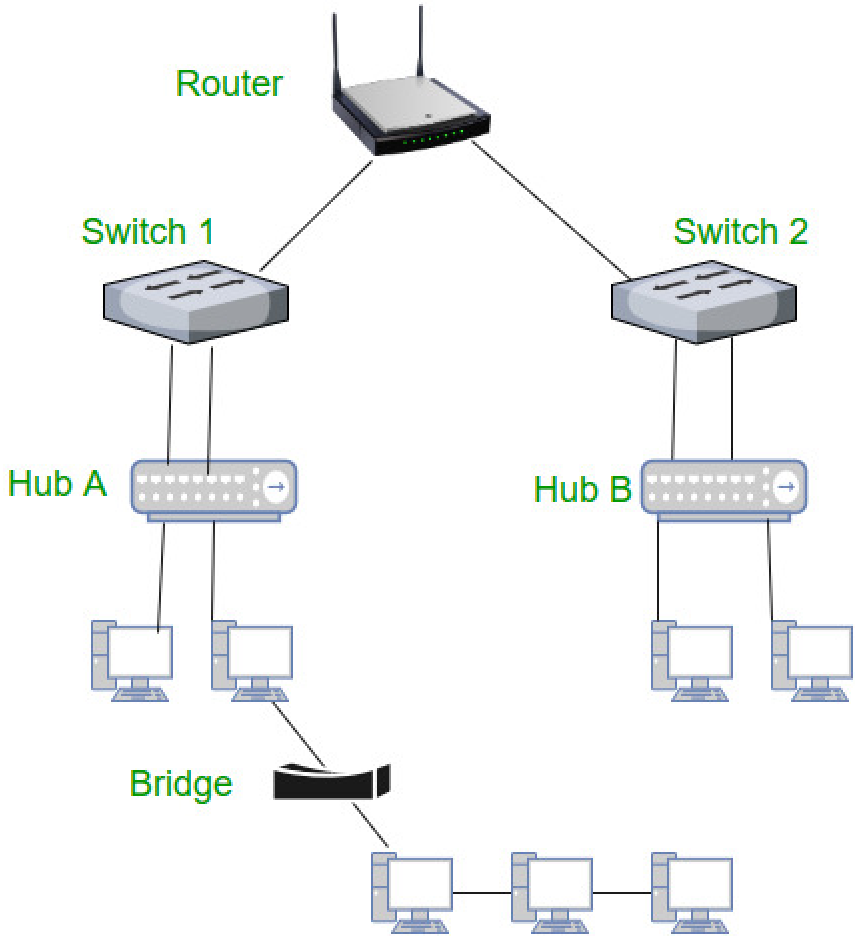


Types of Switch

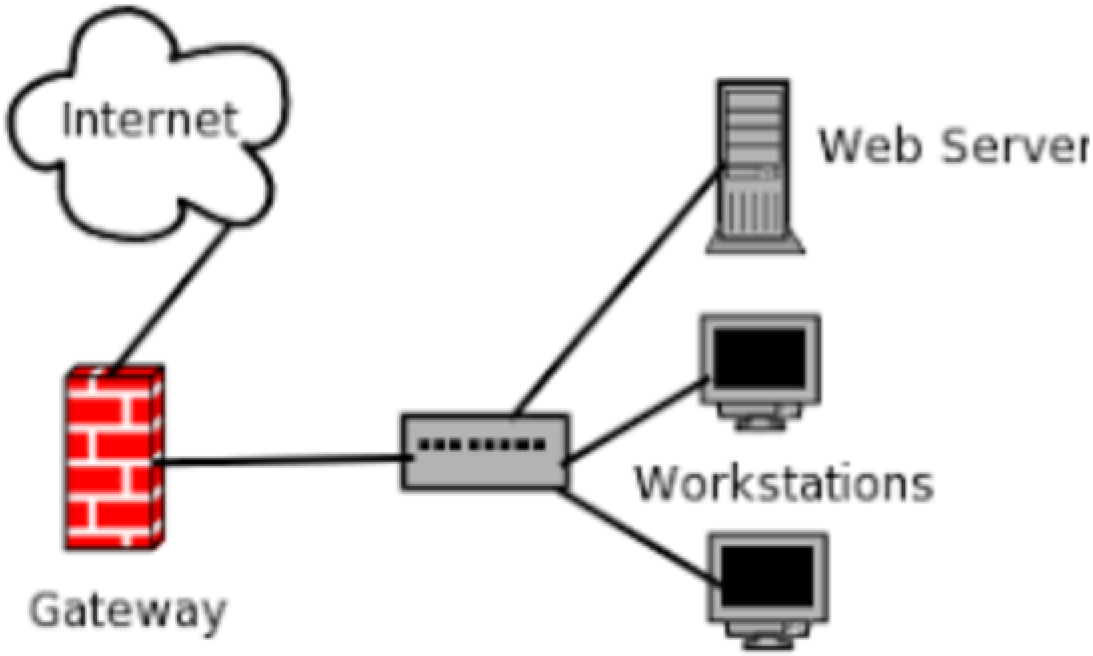
1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.

4. Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
5. Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.



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



Line coding scheme:

A line code is the code used for data transmission of a digital signal over a transmission line. This process of coding is chosen so as to avoid overlap and distortion of signals such as inter-symbol interference.

Following are the properties of line coding –

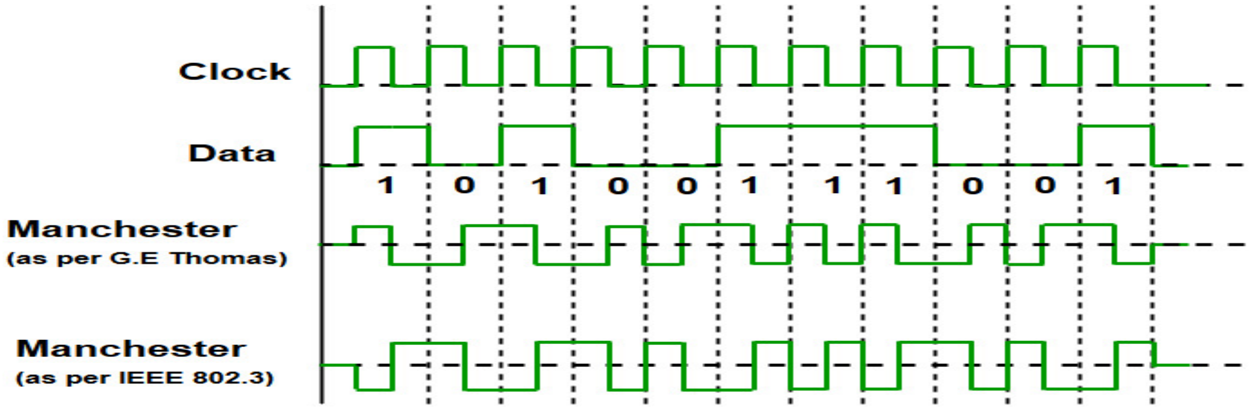
1. As the coding is done to make more bits transmit on a single signal, the bandwidth used is much reduced.
2. For a given bandwidth, the power is efficiently used.
3. The probability of error is much reduced.
4. Error detection is done and the bipolar too has a correction capability.
5. Power density is very favorable.
6. The timing content is adequate.
7. Long strings of **1s** and **0s** are avoided to maintain transparency.

Manchester Encoding in Computer Network

Manchester encoding is a synchronous clock encoding technique used by the physical layer of the Open System Interconnection [OSI] to encode the clock and data of a synchronous bit stream. The idea of RZ and the idea of-L are combined in manchester

Different encoding techniques are used in data communication to ensure data security and transmission speed. Manchester encoding is an example of digital encoding. Because each data bit length is defined by default, it differs from other digital encoding schemes. The bit state is defined by the direction of the transition. Bit status is represented in various ways by different systems, although most systems use 1 bit for low to high transitions and 0 bit for high to low transitions.

In Manchester the duration of a bit is divided into two halves. The voltage remains the same at one level during the first half & moves to the other level.The transition at the middle of the bit provides synchronization.Differential Manchester,on the other hand,combines the idea of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. if next bit is zero there is transition, if the next bit is 1 there is none.



The binary data to be transmitted over the cable are not sent as NRZ [Non-return-to-zero].

Non-return-to-zero [NRZ] –

NRZ code’s voltage level is constant during a bit interval. When there is a long

sequence of 0s and 1s, there is a problem at the receiving end. The problem is that the synchronization is lost due to a lack of transmissions.
It is of 2 types:

1. **NRZ-level encoding –**

   The polarity of signals changes when the incoming signal changes from '1' to '0' or from '0' to '1'. It considers the first bit of data as polarity change.
2. **NRZ-Inverted/ Differential encoding –**

   In this, the transitions at the beginning of the bit interval are equal to 1 and if there is no transition at the beginning of the bit interval is equal to 0.

Characteristics of Manchester Encoding –

- A logic 0 is indicated by a 0 to 1 transition at the center of the bit and logic 1 by 1 to 0 transition.
- The signal transitions do not always occur at the 'bit boundary' but there is always a transition at the center of each bit.
- The **Differential Physical Layer Transmission** does not employ an inverting line driver to convert the binary digits into an electrical signal. And therefore the signal on the wire is not opposite the output by the encoder.
- The following are the properties of Manchester encoding:
- Each bit is sent at a predetermined rate.
- When a high to low transition happens, a '1' is recorded; when a low to high transition occurs, a '0' is recorded.
- At the mid-point of a period, the transition that is utilized to precisely note 1 or 0 happens.

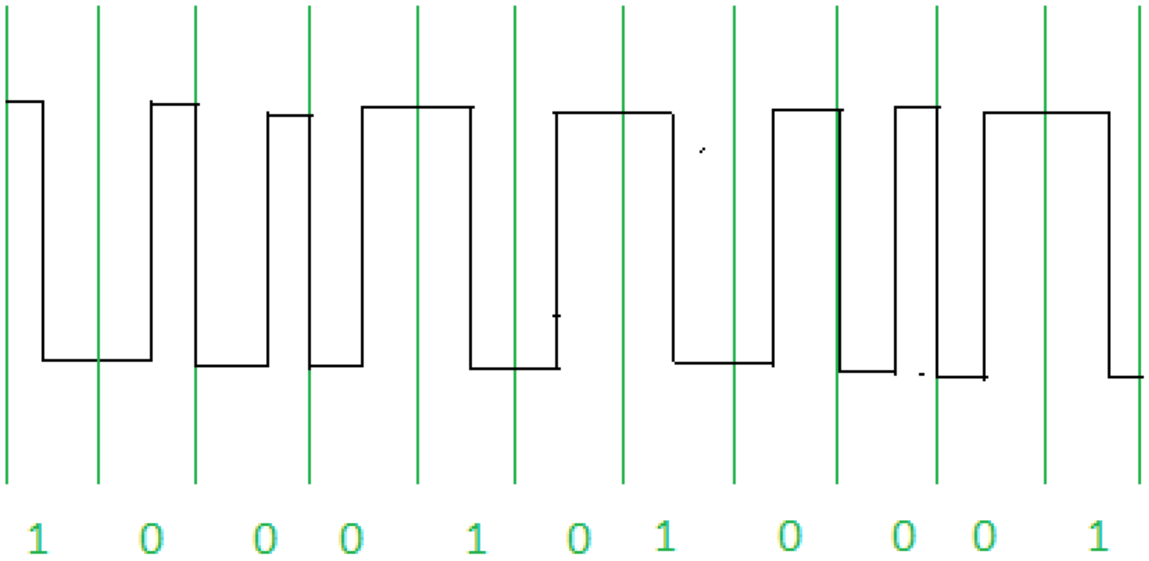
  The Manchester Encoding is also called **Biphase code** as each bit is encoded by a positive 90 degrees phase transition or by negative 90 degrees phase transition.

- The **Digital Phase Locked Loop (DPLL)** extracts the clock signal and deallocates the value and timing of each bit. The transmitted bitstream must contain a high density of bit transitions.
- The Manchester Encoding consumes twice the bandwidth of the original signal.
- The advantage of the Manchester code is that the DC component of the signal carries no information. This makes it possible that standards that usually do not carry power can transmit this information.
- It is a self-clocking protocol, meaning that the receiver can determine the clock frequency from the incoming data.
- The Manchester encoding ensures a constant transition density, making it easier to detect the start and end of a data frame.
- It provides a simple and reliable way to detect errors in the data transmission by checking for a violation of the encoding rules.
- The encoding process adds a redundant bit to the data, enabling error correction in some applications.
- Manchester encoding can also be used for multi-level signaling, where multiple voltage levels are used to represent different data states.

Only drawback is the signal rate.The signal rate is manchester and differential is double that for NRZ. The reason is that there is always one transition at the middle of the bit and maybe one transition at the end of each bit.

Eg: For 10Mbps LAN the signal spectrum lies between 5 and 20

- Another example to find out the bits by seeing the transitions.



Advantages of Manchester Encoding:

Self-clocking: Manchester encoding is self-clocking, which means that the receiver can synchronize its clock with the transmitter’s clock. This ensures that the data is transmitted and received at the same rate, and there is no need for a separate clock signal.

Reduced DC component: Manchester encoding eliminates the DC component in the transmitted signal, which reduces the risk of errors due to interference from external sources.

Error detection: Manchester encoding provides a mechanism for detecting errors in the transmitted data. Any change in the voltage level within a time interval indicates a bit error, which can be detected and corrected.

Simplicity: Manchester encoding is a relatively simple encoding scheme that can be implemented using simple digital circuits.

Disadvantages of Manchester Encoding:

Lower data rate: Manchester encoding has a lower data rate than other encoding schemes, such as non-return-to-zero (NRZ) encoding, which means that it takes more time to transmit the same amount of data.

Higher bandwidth requirement: Manchester encoding requires a higher bandwidth than other encoding schemes, as each bit requires two voltage transitions within each time interval.

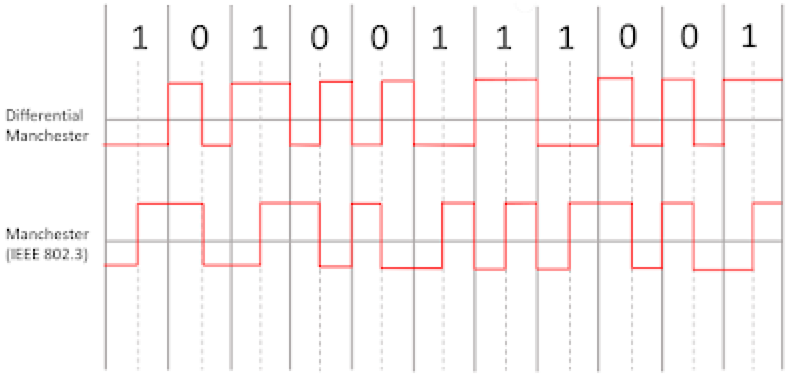
Clock synchronization: Although Manchester encoding is self-clocking, it still requires the receiver to synchronize its clock with the transmitter’s clock, which can be a challenge in some situations.

Reduced transmission distance: Manchester encoding has a reduced transmission distance compared to other encoding schemes, as the signal loses strength over long distances due to the need for frequent voltage transitions.

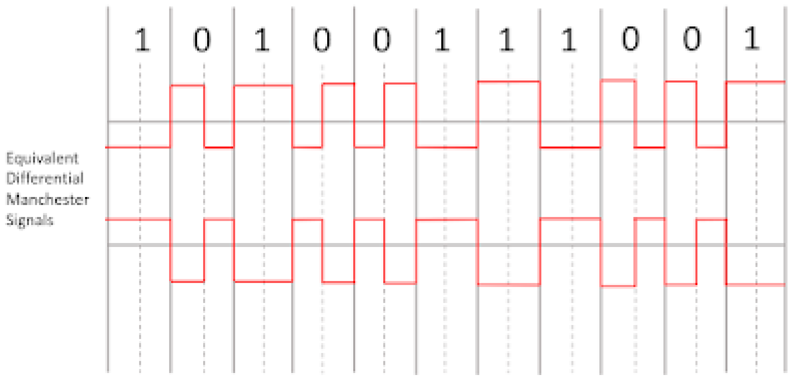
What Is Differential Manchester Encoding?

Differential Manchester Encoding (DME) is an example of a differential, bi-phase encoding technology. DME is specified in the IEEE 802.5 standard for Token Ring local area network (LAN) topology.

Manchester is categorized as bi-phase encoding because the signal is checked twice every bit interval, also called self-clocking. Each check is one “tick”, each bit interval equals two ticks of the clock. This removes the need for the separate clock signal that is required for Non-Return to Zero (NRZ) encoding. Instead, data and clock signals are combined into a single, two-level, self-synchronizing data stream. The clock can be "extracted" by measuring the timing of the edges.



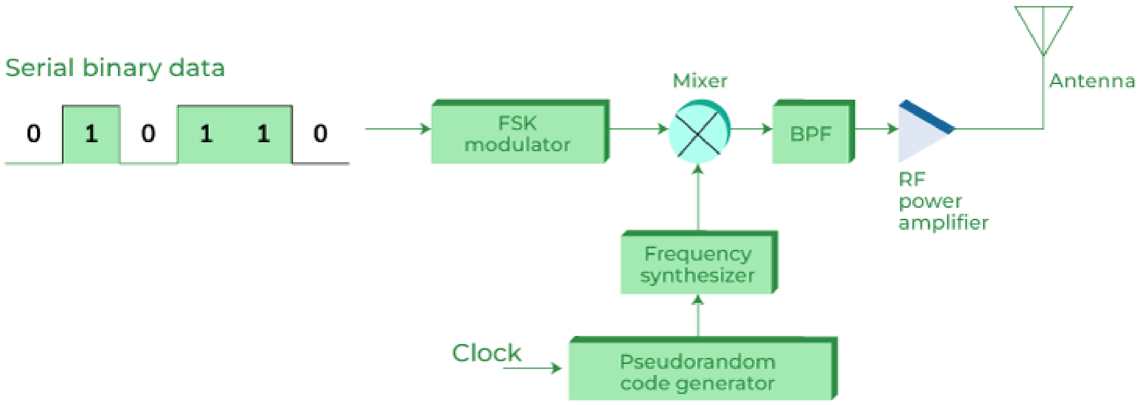
In Manchester encoding, we see a digital modulation scheme where voltage *transitions* rather than voltage *levels* are used to represent 1s and 0s. In IEEE 802.3 Manchester, a low-to-high transition occurring in the middle of the bit interval represents logical 0, while a high-to-low transition represents logical 1 (the Thomas variant reverses this logic). Significant transitions always occur in the middle of the bit interval to ensure clock synchronization. Transitions at the start of a period are only used to reset the polarity to achieve the proper transition for the next bit. This increases error detection capabilities, compared to NRZ, but also increases the bandwidth needed to transmit the signal at the same data rate, making it a better candidate for short-distance applications.



The most prominent feature that distinguishes DME from classic Manchester encoding is that, in DME only the *presence or absence of a transition* during the bit interval is important, not the polarity. The presence of a transition represents a logical 0, while the absence of a transition represents a logical 1. Whether the signal goes line-high or line-low depends simply on its state the previous bit interval. This increases bit rate at lower bandwidths, because one bit is guaranteed to occur every interval. It also helps with data recovery in noisy environments, like automotive, because DME allows for a data stream to be inverted, yet still be properly decoded, unlike classic Manchester where the polarity is significant.

frequency-hopping spread spectrum (FHSS)

Frequency-hopping spread spectrum is designed for robust operation in noisy environments by transmitting short packets at different frequencies across wide portions of channel bandwidth. The receiver correlates these "near" signals against each other and selects the best signal for demodulation, which typically gives better performance compared with non-frequency hopping receivers operating under similar conditions.



In the spread spectrum, the information is transmitted in short breaks of data at different carrier frequencies. In the frequency-hopping spread spectrum (FHSS), each component is transmitted at a different carrier frequency. Conversely, multi-carrier systems (such as OFDM) transmit multiple signals on a single carrier frequency. The spread spectrum can be used to send independent digital data streams across a noisy channel by assigning different 'slots' to each signal.

In FHSS systems, the transmitted power is concentrated on one or a few carriers at a time. The carrier frequencies are chosen in accordance with a pseudo-random sequence or hopping sequence that changes periodically, so as to prevent long-term predictability of the carrier frequencies used. The receiver correlates received signals against the sequence of the received signals to determine which doesn't interfere from noise and interference.

Advantages of FHSS:

Some of the major advantages are as follows:

- The processing gain PG is higher than that of DSSS system.
- The synchronization is not greatly dependent on the distance.
- The serial search system with FHSS needs shorter time for acquisition.

Direct Sequence Spread Spectrum in Wireless Networks (DSSS):

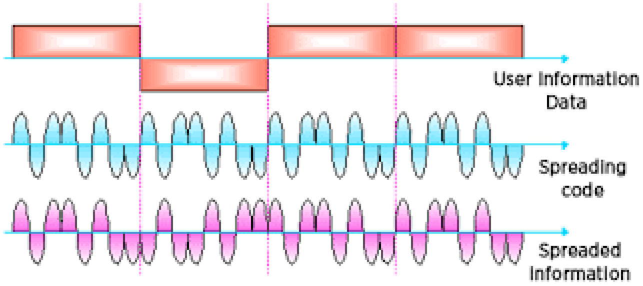
Direct-sequence spread spectrum in Wireless Networks is a technique that transmits a data signal over a range of frequencies, spreading it uniformly across the allocated spectrum. Direct-sequence spread spectrum is used to ensure that a particular frequency band (and its corresponding range of frequencies) is kept free from interference. This technique can be related to escaping the problem of co-channel interference (like two different wireless networks transmitting on the same frequency band) and cross-talk interference. Direct-sequence spread spectrum can also be used as an alternative approach to orthogonal frequency division multiplexing, where the baseband signal is encoded and transmitted across a quantity of fixed, predetermined channels. In this situation, each channel may carry different information, data signals, or time slots for different applications within the same network. Direct-sequence spread spectrum has also been used to transmit data that is encrypted and, in some processes, it is used to transmit non-data signals like power signaling or control signals.

Direct Sequence Spread Spectrum (DSSS) is a communication system that was developed in the 1980s. It divides the bandwidth of a radio channel into wide frequency bands and transmits these signals over separate frequencies. In this frequency-hopping process, each signal is assigned a different orthogonal sequence of frequencies.

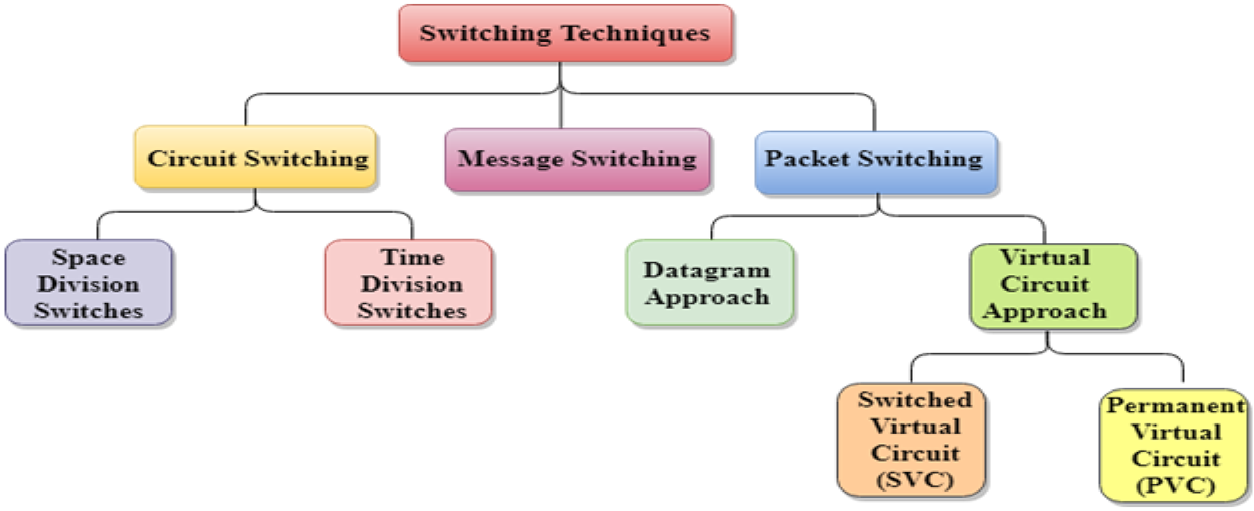
All other radios in the range must gain each signal sequentially and then transmit it, which significantly reduces the risk of interference from outside sources or jamming.

The time required for this process is proportional to the number of frequencies used for transmission. When security agencies need to be ready to communicate secretly, DSSS can be implemented so that their transmissions cannot be spied upon by other parties who are monitoring broadcasts on a shorter wavelength or through tapping devices.

For Example, the NIST specification for the Advanced Encryption Standard used in the Secure Electronic Transaction program defines a system that uses eight bits of data per transmitted symbol in an eight-bit wire transmission to transmit a 128-bit cryptographic key. A receiver would need to correlate eight different symbols to calculate a hash value. If only one of these symbols were encoded with a source-synchronous code, then the receiver would need to acquire each of eight signals in order, which would take time proportional to the number of signals. By using DSSS, however, a single signal can be transmitted that is available for correlation and decryption at any moment.



Switching techniques:

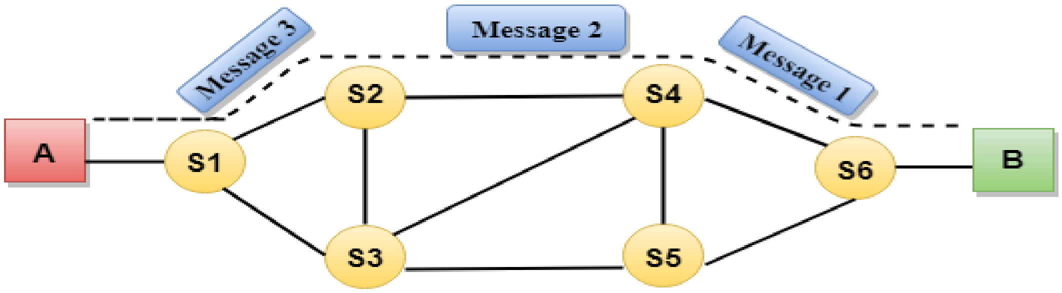


Circuit Switching:-

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgement to ensure the availability of the dedicated path. After receiving the acknowledgment, a dedicated path transfers the data.
- Circuit switching is used in public telephone networks. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- **Circuit establishment**
- **Data transfer**
- **Circuit Disconnect**



Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

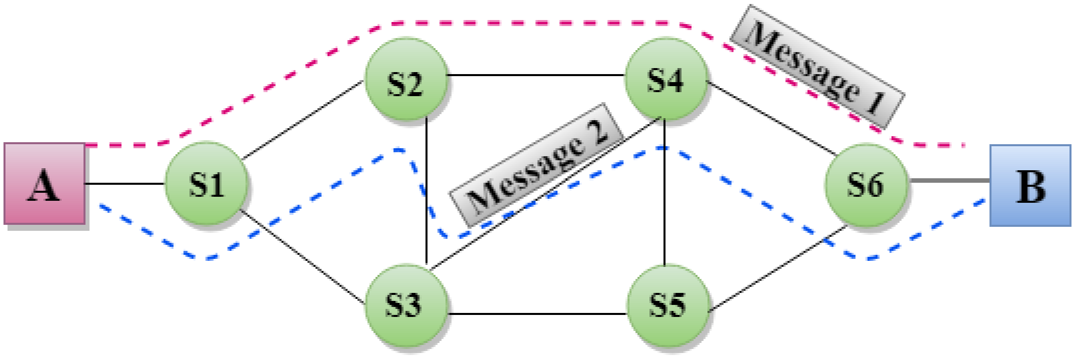
Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.

- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forwards it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

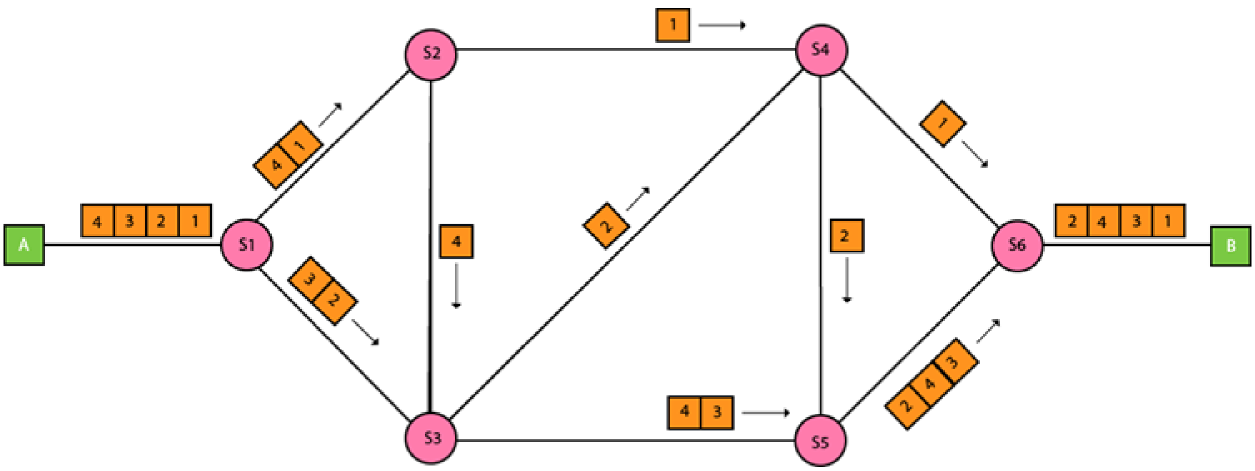
- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports unlimited size.

Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching:

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.

- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

How do you measure Network Performance?

Parameters Used to Measure Network Performance

The following parameters are used to measure Network Performance –

- Bandwidth
- Throughput
- Latency
- Packet Loss
- Jitter

Let us discuss each of these parameters in detail.

Bandwidth

The quantity of bandwidth allocated to the network is one of the most important conditions of a website's performance. The web server's bandwidth controls how quickly it can transfer the requested data. While there are many elements to consider regarding a site's speed, bandwidth is frequently the limiting issue.

The amount of data or information that can be transmitted in a given amount of time is referred to as bandwidth. The phrase can be applied in two ways, each having its own set of estimating values. The bandwidth of digital devices is measured in bits per second (bps) or bytes per second (bps). The bandwidth of analog devices is measured in cycles per second, or Hertz (Hz).

Throughput

The number of messages successfully delivered per unit time is referred to as throughput. Throughput is influenced by the available bandwidth, as well as the available signal-to-noise ratio and device limitations.

To separate the concepts of throughput and latency, throughput will be calculated from the arrival of the first bit of data reaching the receiver for this article. The terms 'throughput' and 'bandwidth' are frequently interchanged in discussions of this nature.

The Time Window refers to the time frame in which the throughput is calculated. The selection of a suitable time window will frequently determine whether or not latency affects throughput. Likewise, whether or not latency is taken into account will determine whether or not latency impacts throughput.

Latency

Latency is simply the time it takes for data to travel from one designated location to another regarding network performance evaluation. The term "delay" is sometimes used to describe this attribute. The latency of a network should be as low as possible.

Speed of light is the fundamental factor for latency, but packet queuing and refractive index of fiber optic cable are also two factors that can be used to reduce latency.

Packet Loss

Packet loss refers to the number of packets that fail to transfer from one destination to another regarding network performance measurement. This statistic can be measured by recording traffic data on both ends and then identifying lost packets and packet retransmission.

Network congestion, router performance, and software difficulties, among other things, can cause packet loss.

Jitter

The variance in time delay for data packets carried over a network is known as jitter. This variable denotes an interruption in data packet sequencing that has been identified. Jitter and latency are linked because jitter generates increased or uneven latency between data packets, which can damage network performance and cause packet loss and congestion.

While some jitter is to be expected and can typically be tolerated, quantifying network jitter is an integral part of measuring overall network performance.

Factors Affecting Network Performance

The following factors affect the performance of a network –

- Network Infrastructure
- Applications Used in the Network
- Network Issues
- Network Security

Network Infrastructure

Network hardware, such as routers, switches, and cables, networking software, security and operating systems, and network services, such as IP addressing and wireless protocols, are all part of the entire network infrastructure. Therefore, it is critical to characterize the network's overall traffic and bandwidth patterns from an infrastructure standpoint.

This network performance evaluation will reveal which flows are the most congested over time, perhaps posing an issue.

Instead of just responding to any performance crisis that may develop, identifying the over-capacity aspects of the infrastructure might lead to pre-emptive fixes or upgrades that can minimize future downtime.

Applications Used in the Network

While network hardware and infrastructure difficulties can directly impact a specific application's user experience, it's also crucial to consider the impact of applications as essential cogs in the overall network architecture. For example, poorly performing programs can eat up a lot of bandwidth and make the user experience poor.

As applications become more complicated, diagnosing and monitoring their performance becomes increasingly important. In addition, application characteristics like window sizes and keep-alive have an impact on network speed and capacity.

Network Issues

The network's intrinsic performance constraints are frequently the focus of attention. Several aspects of the network influence performance and flaws in any of these areas can lead to systemic issues. Because hardware requirements are so crucial incapacity planning, these components should be built to meet all expected system demands.

Network Security

Privacy, intellectual property, and data integrity are all protected by network security. As a result, the importance of solid cybersecurity is never in doubt. Device scanning, data encryption, virus prevention, authentication, and intrusion detection are all required for managing and mitigating network security challenges, all of which take valuable network bandwidth and can negatively influence performance.