COMPUTER NETWORKS

Unit 1

Introduction to Computer Networks

WHAT IS COMPUTER NETWORK?

- A computer network is a set of interconnected computers and other devices that are capable of sharing resources and information.
- These interconnected devices can communicate with each other through various means such as wired or wireless connections.
- The primary purpose of a computer network is to enable the exchange of data and resources among different devices.
- A computer network can be as small as two laptops connected through an Ethernet cable or as complex as the internet, which is a global system of computer networks.
- Computer networks facilitate communication and resource sharing among users, devices, and applications. They enable data transfer, access to shared resources such as printers and storage devices, and provide connectivity to the internet and other networks.

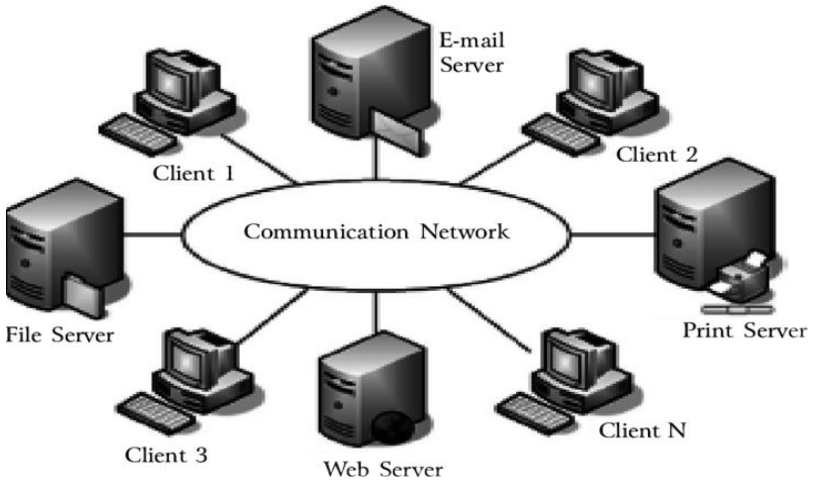


Fig. A Simple Computer Network

ADVANTAGES OF COMPUTER NETWORK

1. Resource Sharing:
    - Hardware Resources: Networks allow the sharing of hardware resources such as printers, scanners, and storage devices, reducing costs and improving utilization.
    - Software Resources: Users can access and use software applications installed on network servers, promoting efficiency and consistency.
2. Data Sharing:

- Networks enable the seamless sharing of data and information among connected devices.
- This facilitates collaboration and improves decision-making processes.

3. Communication:
   - Networks provide various communication tools, including email, instant messaging, video conferencing, enhancing real-time communication irrespective of geographical distances.

4. Remote Access:
   - Users can access network resources and data remotely, which is especially valuable for telecommuting or when employees need to work from different locations.
5. Centralized Management:
   - Network administrators can centrally manage and control resources, user access, and security policies, simplifying administration tasks and ensuring consistency.
6. Cost Efficiency:
   - Shared resources, centralized management, and the ability to power existing infrastructure contribute to cost savings compared to standalone systems.
7. Scalability:
   - Networks can be easily scaled. New devices can be added to the network without significant disruption.
8. Reliability and Redundancy:
   - Network redundancy and failover mechanisms enhance reliability by ensuring continuous operation even in the event of hardware failures or network issues.
9. Data Security:
   - Networks provide tools and protocols for implementing security measures, including firewalls, encryption, and access controls, to protect sensitive data from unauthorized access or malicious attacks.
10. Information Backup and Recovery:
    - Centralized storage on network servers allows for efficient data backup and recovery processes, reducing the risk of data loss due to hardware failures

DISADVANTAGES OF COMPUTER NETWORK

1. Security Concerns:
   - Networks are susceptible to security breaches, unauthorized access, and cyber attacks. Hackers may attempt to steal sensitive information or disrupt operations.
2. Virus and Malware Spread:
   - Computer networks can facilitate the rapid spread of viruses and malware. Once a device is infected, it can easily transmit the malicious software to other connected devices.
3. Complexity and Cost:

- Setting up and maintaining a computer network can be complex and expensive. It requires specialized knowledge, equipment, and ongoing maintenance.

4. Dependency:
   - Businesses and individuals become heavily reliant on networks. If the network fails or experiences downtime, it can disrupt operations and lead to productivity losses.
5. Privacy Issues:
   - With information being shared over networks, there is a potential risk to privacy. Unauthorized access or data interception can compromise sensitive information.
6. Data Loss:
   - In the event of a network failure or a technical glitch, there is a risk of data loss. Without proper backup measures, important information may be unrecoverable.
7. Maintenance Challenges:
   - Networks require regular maintenance, updates, and troubleshooting. If not properly managed, performance issues or unexpected downtime may occur.
8. Compatibility Issues:
   - Different devices and software may not always be compatible with each other within a network. This can lead to communication problems and reduced efficiency.
9. Overload and Congestion:
   - As the number of users and devices on a network increases, there's a risk of congestion. This can result in slower data transfer speeds and decreased overall performance.
10. Limited Physical Security:
    - Physical access to the network infrastructure (servers, routers, etc.) needs to be restricted. If someone gains unauthorized physical access, it can pose a significant security threat.

APPLICATIONS OF COMPUTER NETWORK

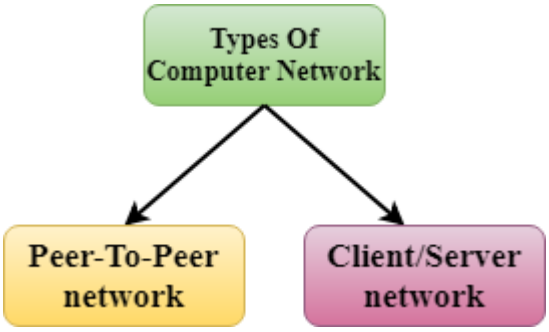
1. Business applications:
   - Computer networks are widely used in businesses to improve communication, share resources, and enable remote access.

2. Educational applications:
   - Computer networks are used extensively in educational institutions to facilitate distance learning, provide access to educational resources, and enable collaboration among students and teachers.
3. Healthcare applications:
   - Computer networks are used in healthcare to store and share patient information, enabling healthcare professionals to provide more personalized care.
4. Entertainment applications:
   - Computer networks are used for entertainment purposes such as online gaming, streaming movies and music, and social media.

5. Military applications:
    - Computer networks are used in military applications to provide secure communication and information sharing among military personnel.
6. Scientific applications:
    - Computer networks are used in scientific research to facilitate collaboration among researchers and share data and information.
7. Transportation applications:
    - Computer networks are used in transportation to manage traffic, track vehicles, and improve transportation efficiency.
8. Banking and finance applications:
    - Computer networks are used in banking and finance to process transactions, share information, and provide secure access to financial services.

COMPUTER NETWORK ARCHITECTURE

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



PEER-TO-PEER NETWORK

- In the P2P (Peer-to-Peer) network, “peers” generally represent computer system.
- Peer-To-Peer network is a network in which these peers are connected to each other with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Files might be shared directly without requirement of central server among these systems on the network.
- It can be said that each of computers on P2P network usually becomes server and client also.
- In this network, tasks are allocated at each and every device available on network.

- There is also no separate division as clients and servers.
- Each and every computer in this network are treated same and equally and might send even receive message directly.
- This P2P network is generally useful in various fields such as business, education, military, etc.

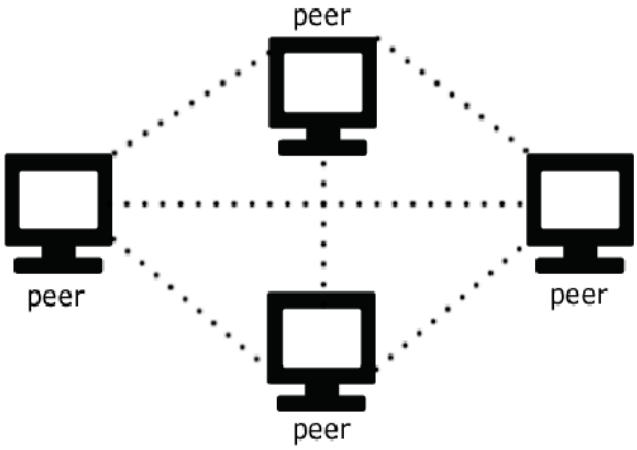


Fig. Peer-To-Peer Network

Advantages:

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

Disadvantages:

- Files and folders cannot be centrally backed up
- It has a security issue as the device is managed itself.
- Because each computer might be being accessed by others it can slow down the performance for the user

CLIENT/SERVER ARCHITECTURE

- Client/Server network is a network model designed for the end users to access the resources from a central computer.
- The central controller is known as a server while all other computers in the network are called clients.
- The clients in this model don't share resources, but request the central server, as all the resources are installed on it.
- The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource, called servers, and service requesters called clients.
- In the client-server architecture, when the client computer sends a request for data to the server,

the server accepts the requested process and delivers the data packets back to the client.

- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server.
- For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.
- Examples of Client-Server Model are Email, World Wide Web, etc.

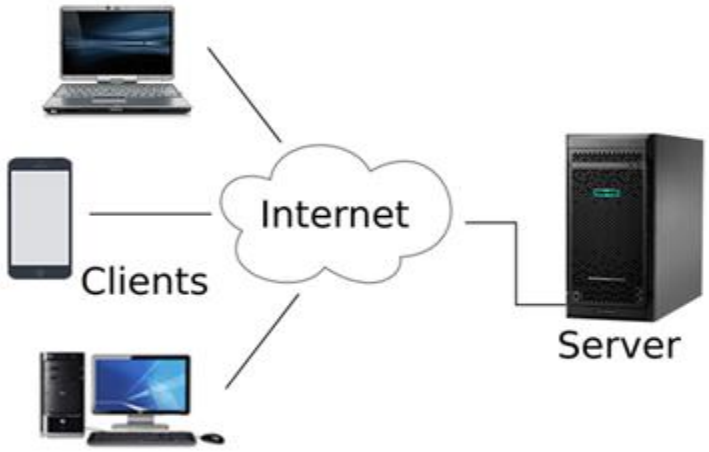


Fig. Client Server Network

Advantages:

- All files are stored in a central location
- Network peripherals are controlled centrally
- A Client/Server network contains the centralized system. Therefore data can be back up easily.
- Improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.

Disadvantages:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- The server is expensive to purchase
- It requires a dedicated network administrator to manage all the resources.
- Specialist staff such as a network manager is needed
- If any part of the network fails a lot of disruption can occur

CONNECTION-ORIENTED SERVICE

- Connection-oriented refers to a type of communication protocol used in computer networks

where a dedicated connection is established between two devices before they can exchange data.

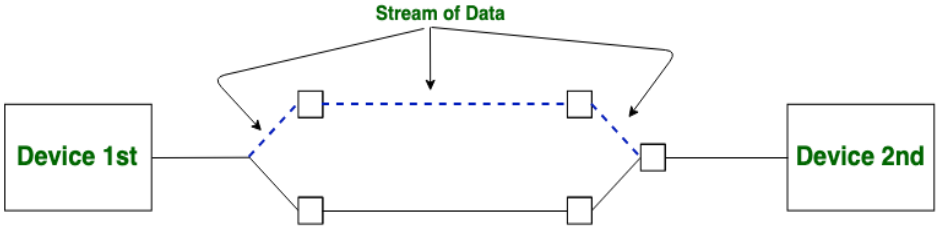
- This dedicated connection ensures a reliable and ordered transfer of information.
- Connection-oriented service is related to the telephone system. It includes connection establishment and connection termination.
- In a connection-oriented service, the Handshake method is used to establish the connection between sender and receiver.
- Operations: There is a sequence of operations that are needed to be followed by users. These operations are given below :
    - Establishing Connection – It generally requires a session connection to be established just before any data is transported or sent with a direct physical connection among sessions.
    - Transferring Data or Message – When this session connection is established, then we transfer or send message or data.
    - Releasing the Connection – After sending or transferring data, we release connection.
- An example of connection-oriented is TCP (Transmission Control Protocol) protocol.

Advantages:

- This connection is more reliable than connectionless service.
- There is no duplication of data packets.
- There are no chances of Congestion.

Disadvantages:

- In this connection, cost is fixed no matter how traffic is.
- If any route or path failures or network congestions arise, there is no alternative way available to continue communication.
- This allocation of resources is mandatory before communication.

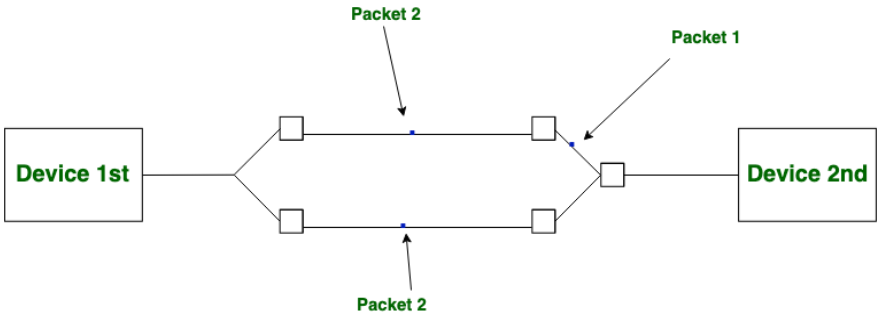


CONNECTION-ORIENTED SERVICE

CONNECTION LESS SERVICES

- Connectionless communication refers to a type of communication protocol in which data is transmitted from one system to another without establishing a dedicated connection beforehand.
- Unlike connection-oriented communication, there is no setup phase, and each data packet is treated independently.

- It is similar to the postal services, as it carries the full address where the letter is to be carried.
- Each message is routed independently from source to destination.
- The order of messages sent can be different from the order received.
- In connectionless the data is transferred in one direction from source to destination without checking the destination is still there or not or if it prepared to accept the message. Authentication is not needed in this.
- An example of a Connectionless service is UDP (User Datagram Protocol) protocol.



CONNECTIONIESS SERVICE

Advantages

- There are usually low overheads.
- Connection-Oriented services help to broadcast or multicast messages to multiple recipients.
- In this, there is no circuit setup. Thus it takes a fraction of a minute in order to establish a connection.
- In the case of Network congestion or router failures, it has an alternative path of data transmission.

Disadvantages

- These are susceptible to congestion in the network.
- It is not reliable as there is the possibility of a loss of data packets, wrong delivery of packets or duplication is high.
- In this, each data packet needs lengthy fields because these are supposed to hold all the destination addresses and the routing information.

CONNECTION-ORIENTED VS CONNECTIONLESS SERVICE

S. No	Comparison Parameter	Connection-oriented Service	Connection Less Service
1.	Related System	It is designed and developed based on the telephone system.	It is service based on the postal system.
2.	Definition	It is used to create an end to end connection between the senders to the	It is used to transfer the data packets between senders to the

		receiver before transmitting the data over the same or different network.	receiver without creating any connection.
3.	Virtual path	It creates a virtual path between the sender and the receiver.	It does not create any virtual connection or path between the sender and the receiver.
4.	Authentication	It requires authentication before transmitting the data packets to the receiver.	It does not require authentication before transferring data packets.
5.	Data Packets Path	All data packets are received in the same order as those sent by the sender.	Not all data packets are received in the same order as those sent by the sender.
6.	Bandwidth Requirement	It requires a higher bandwidth to transfer the data packets.	It requires low bandwidth to transfer the data packets.
7.	Data Reliability	It is a more reliable connection service because it guarantees data packets transfer from one end to the other end with a connection.	It is not a reliable connection service because it does not guarantee the transfer of data packets from one end to another for establishing a connection.
8.	Congestion	There is no congestion as it provides an end-to-end connection between sender and receiver during transmission of data.	There may be congestion due to not providing an end-to-end connection between the source and receiver to transmit of data packets.

WIRED NETWORK

- "Wired" refers to any physical medium made up of cables.
- A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.
- Wired networks are networks where devices such as computers, printers, and routers are physically connected to each other and to the internet or another network using cables.
- The most common type of cable used for wired networks is called an Ethernet cable and coaxial cables.
- This allows the computer to access the internet and communicate with other devices on the network.
- Wired networks can be more expensive to set up and lack mobility since computers must be physically connected via cables.
- Examples of wired networks in use include –

- Ethernet connections between computers in an office, or coaxial cables providing internet access to a home.
- Fiber optic networks using fiber optic cables to transmit data at high speeds.

Fig. Wired Network

Advantages

1. **Speed:** Wired networks often provide faster data transfer speeds compared to their wireless counterparts. Especially with modern Ethernet and fiber-optic cables, high-speed data transfer is achievable.
2. **Reliability:** Wired networks offer a high level of reliability due to the stable physical connection.
3. **Security:** Wired networks tend to be more secure as they're harder to intercept compared to wireless networks. A wired network is very well-protected from illegal and unwanted access.
4. **No Unexpected Traffic:** A wired network rarely experiences unexpected traffic. Thus, it is easy to maintain fast speeds at all times. This is because only a few users can connect to it at any given time.
5. **Stability:** Wired connections are less prone to fluctuations and signal degradation. This stability ensures a consistent and reliable connection, making wired networks preferable.

Disadvantages

1. **Limited Mobility:** Since devices need to be physically connected to the network, moving around can be a challenge in wired networks. This can limit flexibility, especially in larger or more dynamic environments.
2. **Installation Complexity and Cost:** Wired networks can be complex to install, especially in large buildings. Running cables through walls and ceilings, and managing the physical infrastructure can require significant time and resources.
3. **Aesthetics:** From a design perspective, visible network cables may not always be desirable in certain settings.
4. **Cost:** The cost of installation, maintenance, and cable management can also add up over time, especially for larger networks spanning multiple locations.
5. **Vulnerability to Physical Damage:** Since wired networks rely on physical cables, they are susceptible to damage caused by factors such as accidental cuts, environmental conditions, or

equipment failure. Any disruption in the cable infrastructure can result in loss of connectivity and downtime.

6. **Scalability Challenges:** Expanding or modifying a wired network can be more challenging compared to wireless networks.

WIRELESS NETWORK

- "Wireless" means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves.
- Antennas or sensors will be present on all wireless devices.
- This allows all of your devices to access the internet and communicate with each other without the need for cables.
- For data or voice communication, a wireless network uses radiofrequency waves rather than wires.
- A wireless network allows devices to stay connected to the network but roam untethered to any wires.
- Access points amplify Wi-Fi signals, so a device can be far from a router but still be connected to the network.
- When you connect to a Wi-Fi hotspot at a cafe, a hotel, an airport lounge, or another public place, you're connecting to that business's wireless network.
- Examples of wireless networks in use include -
    - Wi-Fi connections between laptops, smartphones, and routers in a home or office.
    - Bluetooth's connections between a smartphone and wireless headphones.
- Wireless networks are more convenient than wired networks because you can connect to them from anywhere within range of the signal.

Fig. Wireless Network

Advantages

1. **Convenience:** Wireless networks enable seamless connectivity without the need for physical connections or cables.

2. **Mobility:** User is not tied to the desk. For example employees can go online in conference room meetings.
3. **Productivity:** Wireless access to the Internet and to company's key applications and resources helps staff get the job done and encourages collaboration.
4. **Easy setup:** You don't have to string cables, so installation can be quick and cost effective.
5. **Expandability**: wireless networks can easily expand with existing equipment, whereas a wired network might require additional wiring.
6. **Security:** Advances in wireless networks provide robust security protections.
7. **Reduced cost:** Because wireless networks eliminate or reduce wiring expenses, they can cost less to operate than wired networks.
8. **Ease of Installation:** Setting up a wireless network is relatively easier compared to wired networks as it eliminates the need for extensive cable installations.
9. **Flexibility and Scalability:** Wireless networks offer greater flexibility in terms of adding or removing devices.

Disadvantages

1. **Signal Range Limitations:** The coverage area of wireless networks is limited by the signal range of the access points. Thick walls, long distances, or environmental factors can affect the signal strength and coverage, leading to poor network connectivity.
2. **Speed and Bandwidth Constraints:** Wireless networks may experience reduced speeds and limited bandwidth, especially when multiple devices are connected simultaneously.
3. **Reliability Challenges:** Wireless networks are more prone to reliability issues due to the potential for signal interference or signal loss caused by environmental factors.
4. **Interference:** Wireless signals can be subject to interference from other electronic devices or physical obstacles, potentially causing a drop in connection quality or speed.
5. **Security:** While wireless networks can be secured, they are inherently more open to potential security threats than wired networks. Extra precautions are necessary to keep them secure.

WIRED NETWORK VERSES WIRELESS NETWORK

Sr. No.	Factors	Wired Networks	Wireless Networks
1	Connectivity	Wired networks use physical cables to connect devices together.	Wireless networks use radio waves or infrared signals to connect devices.
2	Security	Wired networks are more secure as physical cables are used, which does not allow easy interference of signals.	Wireless networks are considered to be less secure as the radio wave used for data transmission can be interrupted or interfered
3	Speed	Wired networks offer faster and more stable speeds as cables provide a	Speed of wireless networks are typically slow and less stable

		direct and dedicated connection between devices.	
4	Mobility	Wired networks provide less mobility as devices must be connected to cables.	Wireless networks provide greater mobility as devices can connect from anywhere within range of the wireless signal.
5	Cost	Wired networks can be more expensive to set up initially, as they require cables and other physical infrastructure.	Wireless networks may have lower initial costs, but may require additional equipment such as routers or access points to ensure coverage throughout an area.
6	Setup and maintenance	Wired networks generally require more time and effort to set up and maintain, as cables need to be run and devices need to be physically connected to the network.	Wireless networks are typically easier to set up, but may require more maintenance due to potential signal interference or connectivity issues.
7	Network range	Wired networks have a greater range. Copper cables can carry signals up to 100 m, while fiber optic cables can carry signals over 100 km or more.	Wireless networks have a shorter range. Typically, the range of a wireless network is a few hundred feet to several hundred yards or meters, depending on the setup and conditions.
8	Interference	Wired networks are less susceptible to interference because wired networks use a dedicated connection between devices	Wireless networks are more susceptible to interference from other wireless signals. As it uses a shared medium.
9	Example	Ethernet cable and coaxial cable	(Wi-Fi) (Bluetooth

TYPES OF COMPUTER NETWORK

1. LAN
2. MAN
3. WAN

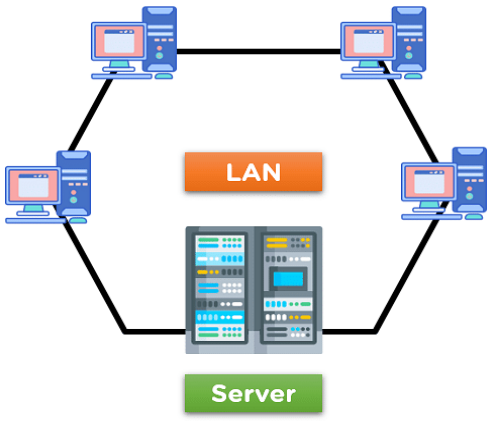
LOCAL AREA NETWORK (LAN)

- The Local Area Network (LAN) is designed to connect multiple network devices and systems within a limited geographical distance.
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- A local area network (LAN) is a group of computers and peripheral devices that share a common communications line or wireless link to a server within a distinct geographic area.

- A local area network may serve as few as two or three users in a home office or thousands of users in a corporation's central office.
- Homeowners and information technology (IT) administrators set up LANs so that network nodes can communicate and share resources such as printers or network storage.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

Example

- Home WiFi networks
- Small business networks.



Advantages

- **Simple and reasonable cost:** immediate and easy to set up and also its price is minimum.
- **Accessing of software program:** With the help of LAN, software programs are also shared. You can incorporate a single licensed program that can be used by any device on a network.
- **Data protection:** Data protection is a safe and secure way to keep information on the server. To update or eliminate any data, you can do on a single server computer and other devices are obtain to new information.
- **Fast communication:** LAN-connected system to communicate directly at very high speed. The most prevalent enabled speed is 10Mbps, 100Mbps, and 1000Mbps.

Disadvantages

- **Limited distance:** Local area networks are used only in buildings or apartment complexes; it cannot be occupied in bigger areas.
- **Installing LAN is expensive:** It is expensive to establish a LAN. Here specialized software is essential to install a server. Communication hardware such as hubs, switches, routers, and cables are expensive to buy.

- **Data sharing via outside source:** It is difficult and time-consuming to send files from outside the network since transportable media like pen drives and CDs cannot be easily performed on all devices on the network.
- **Limited scalability**: LANs are limited in terms of the number of devices that can be connected to them. As the number of devices increases, the network can become slow and congested.
- **Single point of failure:** LANs typically have a single point of failure, such as a central server. If this server fails, the entire network can go down.
- **Maintenance and management**: LANs require regular maintenance and management to ensure optimal performance. This can be time-consuming and costly.

METROPOLITAN AREA NETWORK (MAN)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- It has a higher range than Local Area Network (LAN).
- The Metropolitan Area Network (MAN) is a network type that covers the network connection of an entire city or connection of a small area. The area covered by the network is connected using a wired network, like data cables.

Example

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

Advantages

- **Security:** MAN provides more security as compared to WAN and it is easy to implement.
- **Distance occupies:** MAN is occupied more distance as compared to LAN i.e. It is wider than LAN.
- **Less expensive:** MAN implementation cost is less than WAN because MAN requires fewer resources as compared to WAN. It saves implementation costs.
- **High speed:** Man has a high speed of data transfer because MAN often uses fiber optics cables that are capable of offering speeds up to 1000Mbps.
- **Centralized management:** MANs can be centrally managed, making it easier to monitor and control network traffic.
- **Cost-effective**: Compared to WANs, MANs are more cost-effective to implement and maintain.
- **Scalability**: MANs can be easily scaled up or down to meet changing business needs.
- **Improved communication**: MANs can improve communication within organizations by allowing for faster and more efficient sharing of data and resources.

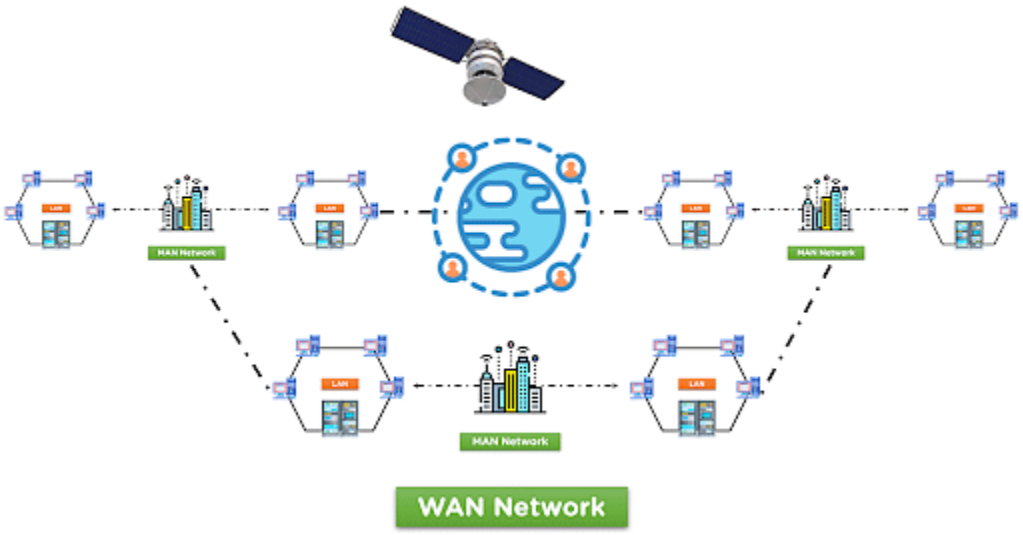
Disadvantages

- **The problem of less security:** It is difficult to secure the system from hackers because of the large area. This is mainly due to safety issues.
- **Wire required:** more cables are required to connect MAN from one place to another. MAN requires fiber optics cables which are quite expensive.
- **Technical assistance:** Here, skilled technicians and administrators are required. This can overall increase the installation cost.
- **Difficult to manage:** MAN consumes a large area then there is difficult to manage a large network, here is a chance of attacking hackers on the network. Data can be secured but it needs experienced staff and security tools.

WIDE AREA NETWORK (WAN)

- The Wide Area Network (WAN) is designed to connect devices over large distances like states or between countries.
- The connection is wireless in most cases and uses radio towers for communication.
- The WAN network can be made up of multiple LAN and MAN networks.
- The speed of the WAN data transfer is lower than in comparison to LAN and MAN networks due to the large distance covered.
- The WAN network uses a satellite medium to transmit data between multiple locations and network towers.
- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.

- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples

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

Advantages

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

- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages

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

NETWORK DEVICES

- Network devices are physical devices that allow hardware on a computer network to interact and communicate with one another.
- Network devices in computer networks as the devices that connect fax machines, computers, printers, and other electronic devices to the network.
- Various network devices are explained below:

1. Hub

- Hub is a hardware device that allows multiple devices or connections to connect to a computer.
- Hubs are intermediary devices that usually operate at the physical layer (Layer I) of the OSI model that connect multiple devices on a local network.
- Hubs function by broadcasting data to all the devices that are connected to it, regardless of their destination.
- Hubs can help in simplifying the wiring and installation of a LAN by providing a central point of connection.
- A USB hub, for example, allows multiple USB devices to connect with one computer, even if that computer only has one USB connection.
- Depending on the hub, the number of ports on a USB hub can range from 4 to over 100

Advantages

- Easy to install
- Inexpensive
- It does not affect the performance of the network seriously

Disadvantages

- Cannot filter information
- It cannot reduce the network traffic
- Broadcast of the data happens to all the port

2. Switch

- Switches serve as networking devices that function at the data link layer (layer 2) of the OSI model.
- The main purpose of switches is to connect end devices within a network and allow the forwarding of data packets utilizing their MAC addresses.
- A switch is a physical circuitry part that controls the flow of signals in networking
- A switch enables you to open or close a connection. When the switch is opened, a signal or power can pass through the connection. When the switch is closed, the flow is stopped, and the circuit connection is broken.

Advantages

- Increases the available bandwidth of the network.
- It helps in reducing the workload on individual host PCs
- Increases the performance of the network

Disadvantages

- They are more costly than network bridges.
- Broadcast traffic can be problematic.

3. Router

- Routers are networking devices that operate at the network layer (layer 3) of the OSI model.
- The main function of the router is to connect networks and allow the forwarding of data packets based on their respective IP addresses.
- Router is a piece of hardware that receives, analyses, and forwards incoming packets to another network.
- Routers examine incoming packets to determine the correct target IP address and send the packet to that address.
- Routers typically connect LANs and WANs and use a rapidly updating routing table to make routing decisions for data packets.

Advantages

- Connects various network architectures such as ethernet and token ring, among others.
- Reduces network traffic by establishing collision domains as well as broadcast domains.
- Chooses the best path across the internetwork using dynamic routing algorithms.

Disadvantages

- They work with routable network protocols.
- More expensive than other network devices.
- They are slower because they must analyze data from layer 1 to layer 3.

4. Bridge

- A bridge is a device that connects two LANs or two segments of the same LAN.
- Networking bridges are also known as network bridges and bridging.
- Bridges, unlike routers, are protocol independent in that they can forward packets without analyzing and re-routing messages.
- Bridging, in a nutshell, connects two smaller networks to form a more extensive network.
- Bridges' primary function in network architecture is to store and forward frames between the various segments that the bridge connects.
- They transfer frames using hardware Media Access Control (MAC) addresses.
- Bridges can forward or prevent data crossing by analyzing the MAC addresses.
- A bridge operates at the OSI model's Data Link layer (Layer 2).

Advantages

- Reduces collisions
- Reduces network traffic with minor segmentation
- Connects similar network types with different cabling

Disadvantages

- Does not filter broadcasts
- More expensive compared to repeaters
- Slower compare to repeaters due to the filtering process

5. Gateway

- A gateway is a networked device that serves as an entry point into another network.
- A wireless router, for example, is frequently used as the default gateway in a home network.
- In short, a gateway acts as a messenger agent, taking data from one network, interpreting it, and transferring it to another.
- Gateways, also known as protocol converters, can operate at any OSI model layer.

Advantages

- Allows to broaden the network
- Handles traffic issues effectively
- Permits to link two different kinds of networks

Disadvantages

- Never filter data
- Costly and difficult to manage
- Protocol conversion is performed, thus resulting in a slower transmission rate.

6. Modem

- A modem is a piece of hardware that enables a computer to transmit and receive data over telephone lines.
- A modem is a piece of hardware that connects a computer or router to a broadband network.
- When a signal is sent, the device converts digital data to an analog audio signal and sends it over a phone line. Similarly, when an analog signal is received, it is converted back to a digital signal by the modem.
- A modem operates at the OSI model's physical layer (Layer 1) or Data link layer (Layer 2), depending on the type.

Advantages

- Easily allows connecting LAN to internet
- Converts digital signal into an analog signal
- When compared to the hub, the speed is slow

Disadvantages

- It only serves as a bridge between the LAN and the internet.
- It cannot maintain its network traffic.
- The modem is unaware of its destination path.

7. Repeater

- A repeater is an item that boosts the strength of a signal so that it can travel longer distances without losing quality.
- These devices are commonly used in networks to help data reach further destinations.
- A range extender or wireless repeater, for example, is a repeater that extends the range and strength of a Wi-Fi signal.
- A repeater is effective in office buildings, schools, and factories where a single wireless router cannot reach all areas.
- A repeater operates at the OSI model's physical layer (Layer 1).

Advantages

- Repeaters are simple to set up and inexpensive.

- Repeaters do not necessitate any additional processing.
- They can connect signals with various types of cables.

Disadvantages

- Repeaters are unable to connect disparate networks.
- They are unable to distinguish between actual signals and noise.
- They will not be able to reduce network traffic.

COMPUTER NETWORKS

UNIT 2

Network Topology

and

Layered Architecture

WHAT IS NETWORK TOPOLOGY?

- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology.
- A network topology refers to the physical or logical arrangement of devices and connections in a computer network.
- It defines how different devices and components in the network are interconnected and how data flows between them.
- Network topologies can be physical, where the devices and connections are physically laid out, or logical, where the topology is represented conceptually, regardless of the physical arrangement.
- Types of Network Topology
  1. Bus Topology

2. Star Topology
3. Ring Topology
4. Tree topology
5. Mesh topology
6. Hybrid Topology

BUS TOPOLOGY

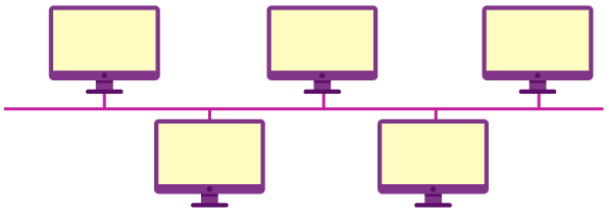


Fig. Bus Topology

- In bus network topology, every node is connected in series along a single cable, known as bus.
- The bus acts as a shared communication medium, where devices take turns transmitting data.
- The data is broadcasted to all devices on the network, but only the intended recipient accepts and processes it.
- When a node wants to send a message over the network, it puts a message over the network.
- Each device on the network listens to the bus for incoming data and only accepts data addressed specifically to it.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- While bus topology was widely used in the past, it is less common in modern networks.
- However, it is still used in small-scale environments or as a backbone for some network architectures.

Advantages:

- Additional devices can be connected to the bus without disrupting the network.
- Devices can be added or removed without affecting other devices on the network.
- It works excellently in a tiny network and is cost-effective for small networks
- require fewer cables, It is easy to set up
- It demands a shorter cable length as compared to the star topology.
- Nodes are directly linked to the cable, therefore, the starting cost of installation is quite low.

Disadvantages:

- If the main cable, bus, fails, the entire network can be disrupted.
- It is very tough to determine the issues if the entire network goes down.
- Bandwidth is shared among all devices, so network performance can be adversely affected if many devices are transmitting simultaneously.

- The length of the bus cable is limited, which may impact network size and reach.
- If new devices are added, it would affect the network and slow down.
- It is not suitable for large networks.
- Though the concept of bus topology is pretty easy, it still demands a lot of cabling.

STAR TOPOLOGY

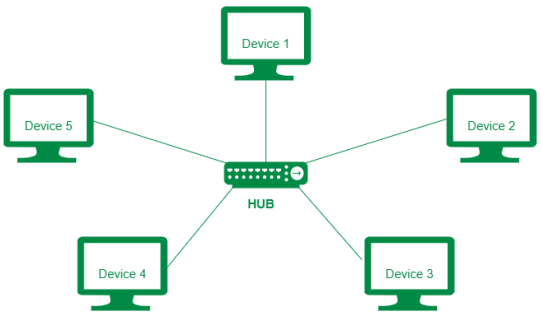


Fig. Star Topology

- In star topology all devices are connected to a central device, often referred as hub or switch.
- In this topology, each device has its own dedicated connection to the central device, forming a star-like structure with the central device at the center.
- Devices are connected to the central device using point-to-point connections, typically Ethernet cables.
- Every communication between hosts, takes place through only the hub.
- All data transmitted between devices in the network passes through the hub.
- Communication between devices is achieved by sending data from the source device to the central device, which then forwards the data to the destination device.
- Hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails.
- Local area networks based on Ethernet switches
- Most wired home and office networks have a physical star topology.

Advantages:

- The central hub allows for easy management and troubleshooting of the network.
- Issues with individual device connections can be isolated and addressed without affecting the entire network.
- It is relatively easy to add or remove devices from the network without disrupting the other devices.
- If a device or connection fails, it only affects the device connected to it, while the rest of the network remains operational.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages:

- If the central hub fails, the entire network can be disrupted.
- Each device requires its own connection to the central hub, resulting in more cables
- The central hub requires more resources and can be more expensive
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

RING TOPOLOGY

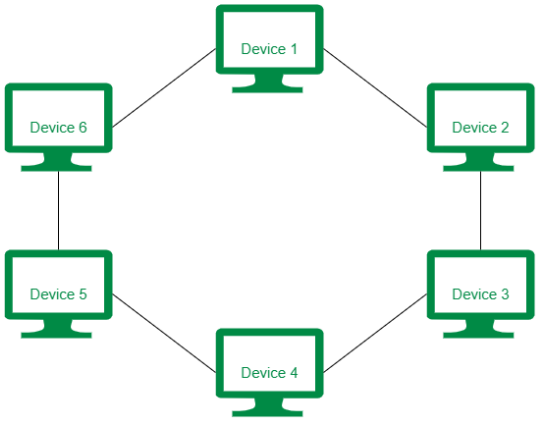


Fig. Ring Topology

- Each device has a dedicated connection to two neighboring devices, forming a continuous loop.
- A ring topology is a network configuration in which devices are connected in a closed loop, forming a ring.
- Data is transmitted in a sequential manner, passing through each device in the ring.
- Each device is connected to two neighboring devices, and data travels in one direction around the ring.
- When a device receives data, it processes and forwards it to the next device until it reaches its intended destination.
- When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.
- To connect one more host in the existing structure, the administrator may need only one more extra cable.
- Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure.

Advantages:

- Data flows in a circular path, leading to efficient network performance.
- Each device gets an equal chance to transmit data, as token-based access control ensures fairness.

- The ring structure is relatively easy to set up and maintain.
- 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.

Disadvantages:

- The failure of a single node in the network can cause the entire network to fail.
- Adding or removing devices to the network can be challenging
- The overall length of the ring is limited, which can impact the size and reach of the network.
- Troubleshooting is difficult in this topology.
- Less secure.

TREE TOPOLOGY

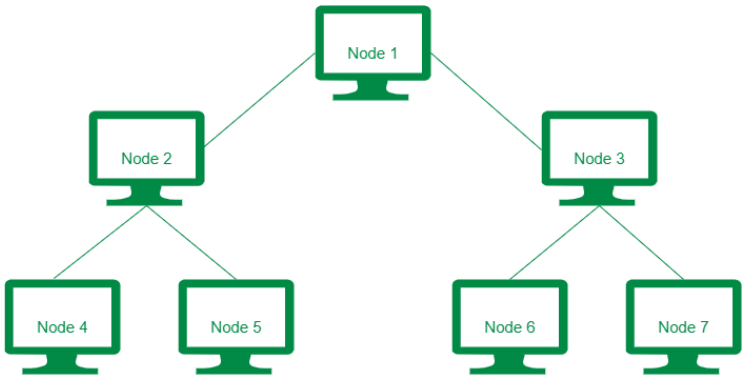


Fig. Tree Topology

- A tree topology, also known as a hierarchical topology
- This is the most common form of network topology in use presently.
- This topology imitates as extended Star topology and inherits properties of bus topology.
- This topology divides the network in to multiple levels/layers of network.
- Mainly in LANs, a network is bifurcated into three types of network devices, is a network configuration in which devices are arranged in a hierarchical structure, resembling a tree.
- It combines characteristics of both bus and star topologies.
- Devices are connected in a hierarchical manner, where a central device acts as the root of the tree.
- The central device, usually a switch or a router, connects to multiple branches of devices.
- Each branch of devices can have its own sub-branches, forming multiple levels of hierarchy.
- Communication between devices is achieved by sending data from a source device to the central device, which then determines the appropriate path to forward the data to the destination device.
- Tree topologies are commonly used in larger networks, such as wide area networks (WANs) or campus networks, that require scalability and organization.

Advantages:

- Tree topologies allow for easy expansion by adding new devices or branches without impacting the entire network.
- Devices can be added, removed, or reorganized with minimal disruption to the network.
- Devices in the same branch can communicate directly with each other, reducing network traffic.
- 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.
- Error detection and error correction are very easy in a tree topology.

Disadvantages:

- If the central hub gets fails the entire system fails.
- The hierarchical structure can lead to increased complexity in network management and troubleshooting.
- Implementing and maintaining can require more resources and infrastructure
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

MESH TOPOLOGY

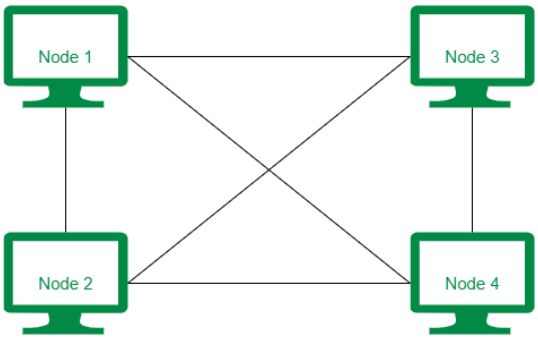


Fig. Mesh Topology

- In mesh topology, each device is connected to every other device in the network.
- This creates a fully interconnected network, where data can take multiple paths to reach its destination.
- Each device is directly connected to every other device, forming a web-like structure.
- Communication between devices can happen directly, without the need for a central device.
- Data can travel through multiple paths in the network, increasing redundancy and improving fault tolerance.
- Mesh topologies are commonly used in mission-critical networks, such as telecommunications networks and data centers, where high reliability and fault tolerance are essential.
- Mesh topologies can be categorized into two types
    - Full mesh: every device is connected to every other device in the network.

- Partial mesh: only certain devices are directly connected to each other.

Advantages:

- The direct connections between devices allow for efficient communication and data transfer.
- Failure during a single device won't break the network.
- There is no traffic problem as there is a dedicated point to point links for every computer.
- Fault identification is straightforward.
- This topology provides multiple paths to succeed in the destination and tons of redundancy.
- It provides high privacy and security.
- Data transmission is more consistent because failure doesn't disrupt its processes.
- Adding new devices won't disrupt data transmissions.
- This topology has robust features to beat any situation.
- A mesh doesn't have a centralized authority.

Disadvantages:

- It's costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
- Installation is extremely difficult in the mesh.
- Power requirement is higher as all the nodes will need to remain active all the time and share the load.
- Complex process.
- The cost to implement mesh is above other selections.
- There is a high risk of redundant connections.
- Each node requires a further utility cost to think about.
- Maintenance needs are challenging with a mesh.

HYBRID TOPOLOGY

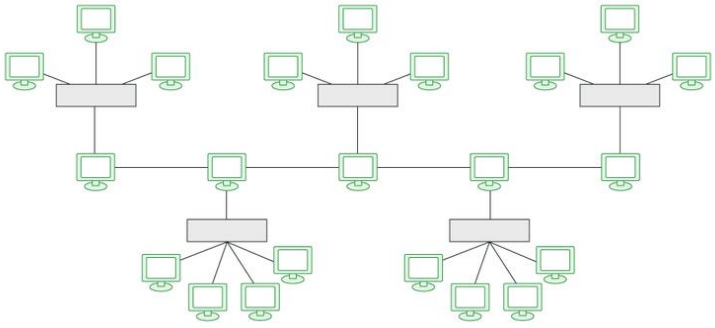


Fig. Hybrid Topology

- A network structure whose design contains more than one topology is said to be hybrid topology.

- Hybrid topology inherits merits and demerits of all the incorporating topologies.
- 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.
- A common example of a hybrid topology is a university campus network.

Advantages:

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is extremely flexible.
- It is very reliable.
- It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.
- Error detecting and troubleshooting are easy.
- Handles a large volume of traffic.
- It is used to create large networks.
- The speed of the topology becomes fast when two topologies are put together.

Disadvantages:

- It is a type of network expensive.
- The design of a hybrid network is very complex.
- There is a change in the hardware to connect one topology with another topology.
- Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.
- Hubs which are used to connect two distinct networks are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
- Installation is a difficult process.

LAYERED ARCHITECTURE

- Layered Architecture in a computer network is defined as a model where a whole network process is divided into various smaller sub-tasks.
- These divided sub-tasks are then assigned to a specific layer
- A single layer performs only specific type of task.
- To run the application and provide all types of services to clients a lower layer adds its services to the higher layer present above it.

OSI MODEL

- The open systems interconnection (OSI) model refers to a standard model used to describe the

flow of information from one computing device to another operating in a networking environment.

- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks.
- OSI consists of seven layers, and each layer performs a particular network function.
- Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.
- The model defines a set of rules and requirements for data communication and interoperability between different devices, products, and software in a network infrastructure.
- Until OSI emerged, network architecture lacked the standard protocols necessary for effective data communication and design infrastructure.

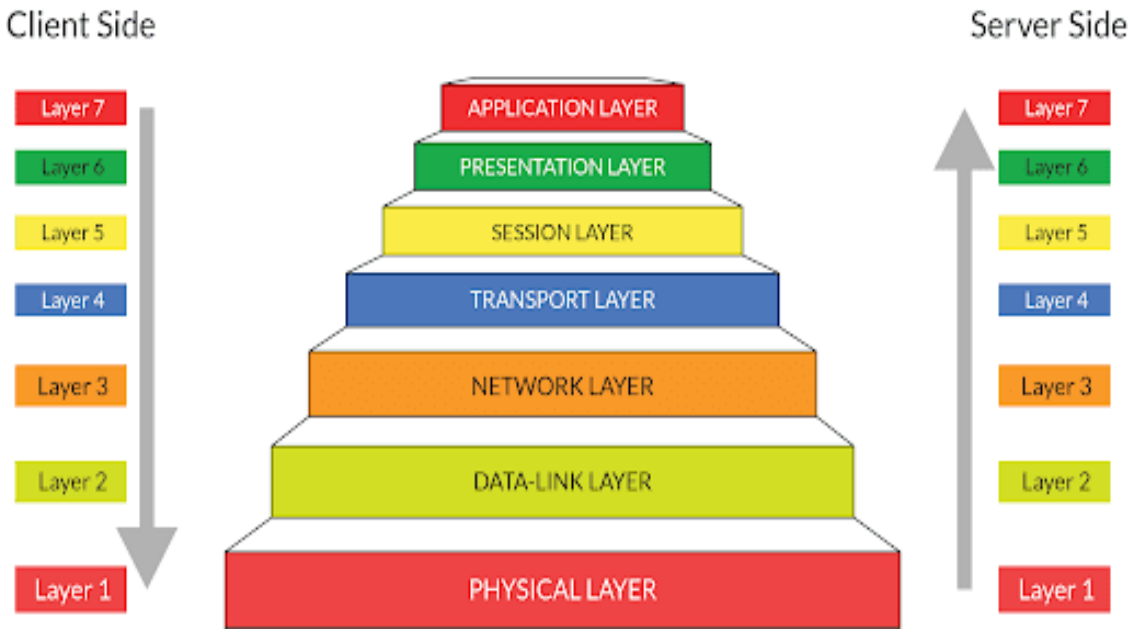


Fig. OSI Model

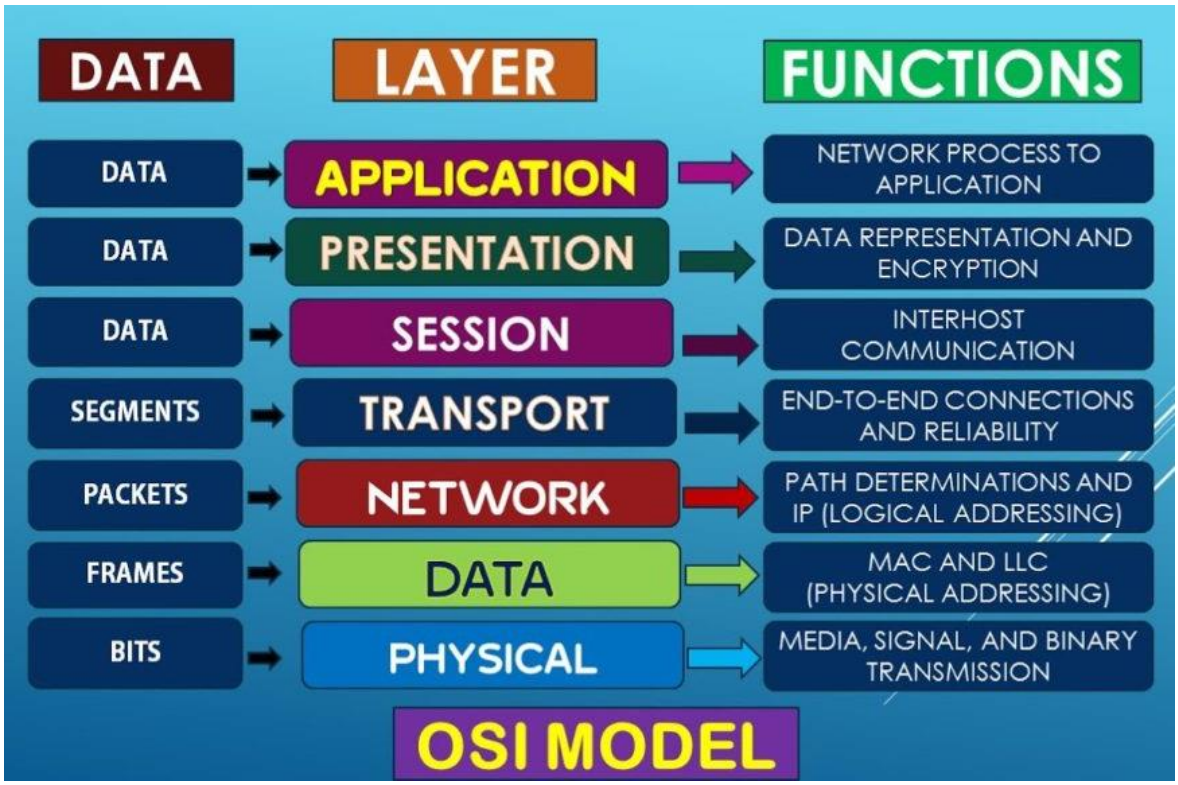
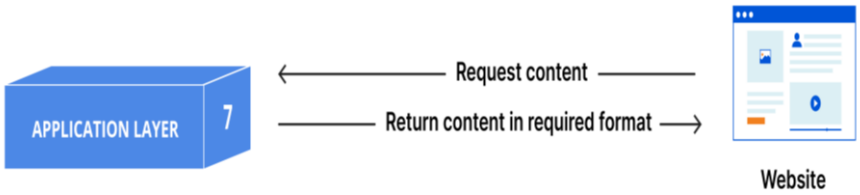


Fig. Concept of OSI Model

7. Application layer



- The application layer is the topmost layer in the OSI model.
- Application layer protocols allow the software to direct data flow and present it to the user.
- Software applications like web browsers and email clients rely on the application layer to initiate communications.
- This is the only layer that directly interacts with data from the user.
- The layer establishes communication between the application on the network and the end user using it by defining the protocols for successful user interaction.
- Client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.

- Application layer protocols include Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP).

Key functions:

- The application layer provides user interfaces (UI) that are key to user interaction
- Supports a variety of applications such as e-mail and remote file transfer
- Layer 7 ensures effective communication between applications on different computing systems and networks.

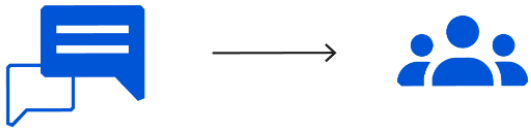
6. Presentation layer

- The presentation layer is often referred to as syntax or translation layer as it translates the application data into a network format.
- The presentation layer is responsible for translation, encryption, and compression of data.
- This layer also encrypts and decrypts data before transmitting it over the network.
- Layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.
- Moreover, this layer is known to compress data received from layer 7 to reduce the overall size of the data transferred.
- Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5.
- This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

Key functions:

- Performs data translation based on the application's data semantics
- Encrypts and decrypts sensitive data transferred over communication channels
- Performs data compression to reduce the number of bits in exchanged data
- layer 6 ensures that the communicated information is in the desired format as required by the receiving application.

5. The session layer



- The session layer establishes a communication session between communicating entities.
- The time between when the communication is opened and closed is known as the session.
- This is the layer responsible for opening and closing communication between the two devices.
- The session is maintained at a sufficient time interval to ensure efficient data transmission and avoid wasting computing resources.
- In situations where large volumes of data are sent at once, layer 5 can break down the data into smaller chunks by adding checkpoints.
- The session layer also synchronizes data transfer with checkpoints.
- For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

Key functions:

- Opens maintains, and closes communication sessions
- Enables data synchronization by adding checkpoints to data streams
- Layer 5 establishes, maintains, synchronizes, and terminates sessions between end-user applications.

4. Transport layer

- Layer 4 is responsible for end-to-end communication between the two devices.
- This includes taking data from the session layer and breaking it up into chunks called segments
- The transport layer allows safe message transfer between the sender and the receiver.
- It divides the data received from the layer 5 into smaller segments. It also reassembles the data at the receiver side to allow the session layer to read it.
- Layer 4 performs two critical functions: flow control and error control.

- Flow control implies regulating data transfer speeds. It ensures that the communicating device with a good network connection does not send data at higher rates, which is difficult for devices with slower connections to handle.
- Error control refers to the error-checking functionality to ensure the completeness of data. In incomplete data cases, this layer requests the system to resend the incomplete data.
- Examples of transport layer protocols include transmission control protocol (TCP) and user datagram protocol (UDP).

Key functions:

- Ensures completeness of each message exchanged between source and destination
- Maintains proper data transmission through flow control and error control
- Performs data segmentation and reassembling of data
- Layer 4 is responsible for transmitting an entire message from a sender application to a receiver application.

3. Network layer

- The network layer enables the communication between multiple networks.
- The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary.
- The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device.
- The network layer also finds the best physical path for the data to reach its destination; this is known as routing.
- This network layer uses internet protocol (IP) for data delivery.

Key functions:

- Handles routing to recognize suitable routes from sender to receiver
- Performs logical addressing that assigns unique names to each device operating over the network
- Layer 3 is responsible for dividing segmented data into network packets, reassembling them at the recipient's side, and identifying the shortest yet most suitable and secure path for transmitting data packets.

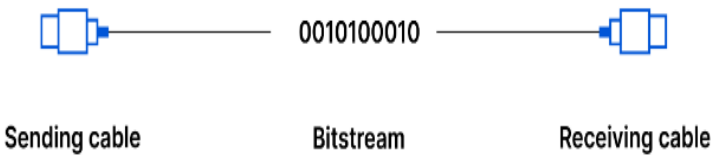
2. Data link layer

- The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the same network.
- The data link layer transmits data between two nodes that are directly connected or are operating over the same network architecture.
- The data link layer takes packets from the network layer and breaks them into smaller pieces called frames.
- Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication.
- The transport layer only does flow control and error control for inter-network communications.
- Layer 2 is divided into two sub-layers: media access control (MAC) and logical link control (LLC). The MAC layer encapsulates data frames transmitted through the network connecting media such as wires or cables. In situations where such data transmission fails, LLC helps manage packet retransmission.

Key functions:

- Detects damaged or lost frames and retransmits them
- Performs framing where data received from layer 3 is further subdivided into smaller units called frames
- Updates headers of created frames by adding the MAC address of the sending device and receiving device
- Layer 2 is responsible for setting up and terminating physical connections between participating network nodes.

1. Physical layer



- The last OSI layer is the physical layer.
- This layer manages physical hardware and network components such as cables, switches, or routers that transmit data.

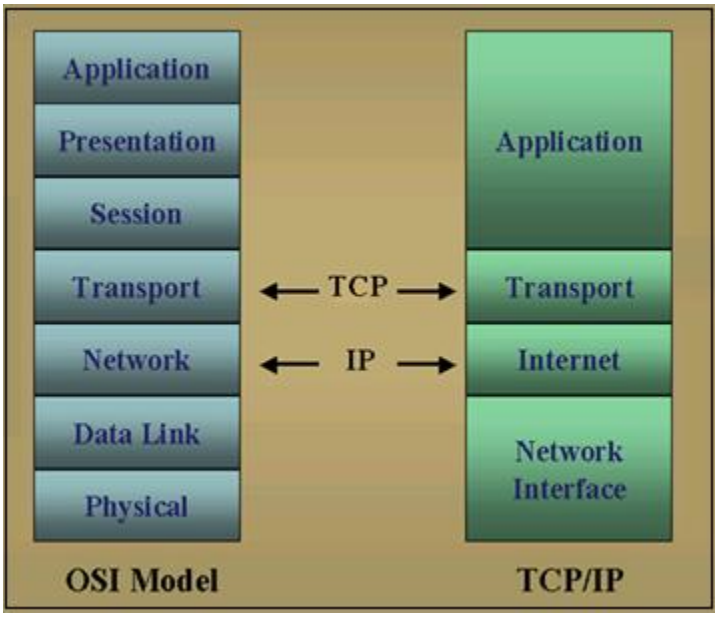
- This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s.
- The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

- Technically, this layer picks up bits from the sender end, encodes them into a signal, sends the signal over the network, and decodes the signal at the receiver end.
- Thus, without layer 1, communicating data bits across network devices through physical media is not possible.

Key functions:

- Synchronizes data bits
- Enables modulation, that is, conversion of a signal from one form to another for data transmission
- Defines data transmission rate (bits/sec)
- Defines transmission modes such as simple or half-duplex mode
- Layer 1 is responsible for transmitting data bits of 0s and 1s between network systems via electrical, mechanical, or procedural interfaces.

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.
- The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a conceptual framework used for designing and understanding how network protocols and communication work within computer networks.
- It is a suite of communication protocols used to interconnect network devices on the internet.
- TCP and IP are the two main protocols, though others are included in the suite.

The 4 layers of the TCP/IP model

4. Application Layer:

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- The Application Layer enables communication between software applications and services running on different devices within a network.
- For example: web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- It defines the formats and conventions for data exchange between applications. This includes specifying how data is formatted, encoded, and structured.
- The Application Layer includes protocols
    - HTTP (Hypertext Transfer Protocol) for web browsing.
    - FTP (File Transfer Protocol) for file transfers.
    - SMTP (Simple Mail Transfer Protocol) for email communication.
    - DNS (Domain Name System) for translating domain names to IP addresses.

3. Transport Layer

- This is third layer in the TCP/IP model.
- The Transport Layer is responsible for maintaining reliable, end-to-end communication between devices across a network.
- It manages the flow control, error checking, and data integrity during the exchange of information.
- The Transport Layer breaks down large messages into smaller units called segments for transmission. This process is known as segmentation.
- At the receiving end, the Transport Layer reassembles the segments into the original message.
- It includes mechanisms for error detection, acknowledgment, and retransmission of lost or corrupted segments.

- This ensures that data is delivered accurately and completely, and any errors during transmission are corrected.
- The two primary protocols operating at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- TCP establishes and terminates connections between devices to facilitate reliable communication. A three-way handshake is used for connection establishment, and a four-way handshake is used for connection termination.
- UDP operates as a connectionless protocol without the overhead of establishing and maintaining a connection.

2. Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Its primary functions include logical addressing, routing, and fragmentation
- The Internet layer assigns logical address known as IP address to devices. IP addresses are used to uniquely identify devices in the network.
- The Internet Layer is also responsible for fragmentation, in which large packets breaks down into smaller fragments if the network has a smaller maximum packet size. At the receiving end, the fragments are reassembled into the original complete packet.
- The Internet layer ensures that the packet is forwarded to the correct destination. It uses routing algorithms to determine the best path for a packet to reach its destination.
- The Internet Layer handles error detection

1. Network Access Layer

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

DIFFERENCE BETWEEN TCP/IP AND OSI MODEL

TCP/IP MODEL	OSI MODEL
TCP/IP refers to Transmission Control	OSI refers to Open Systems Interconnection.

Protocol/ Internet Protocol.	
It is a communication protocol that is based on standard protocols and allows the connection of hosts over a network.	It is a structured model which deals which the functioning of a network.
In 1982, It was developed by ARPANET (Advanced Research Project Agency Network).	In 1984, OSI model has been developed by ISO (International Standard Organization).
It comprises of four layers: • Network Interface • Internet • Transport • Application	It comprises seven layers: • Physical • Data Link • Network • Transport • Session • Presentation • Application
It follows a horizontal approach.	It follows a vertical approach.
The TCP/IP is the implementation of the OSI Model.	An OSI Model is a reference model, based on which a network is created.
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.
It is protocol dependent.	It is protocol independent.
This model is highly used.	The usage of this model is very low.
In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.	In this model, the session and presentation layers are separated, i.e., both the layers are different.
The network layer provides only connectionless service.	In this model, the network layer provides both connection-oriented and connectionless service.
In this model, the protocol cannot be easily replaced.	Protocols in the OSI model are hidden and can be easily replaced when the technology changes.
It does not provide the standardization to the devices. It provides a connection between various computers.	It provides standardization to the devices like router, motherboard, switches, and other hardware devices.

SIMILARITIES BETWEEN OSI MODEL AND TCP/IP MODEL

- Share common architecture
  - Both the models are the logical models and having similar architectures as both the models are constructed with the layers.
- Define standards

  - Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.

- Simplified troubleshooting process
  - Both models have simplified the troubleshooting process by breaking the complex function into simpler components.
- Pre-defined standards
  - The standards and protocols are already pre-defined; these models do not redefine them. For example, the Ethernet standards were already defined by the IEEE before the development of these models; instead of recreating them, models have used these pre-defined standards.
- Both have similar functionality of 'transport' and 'network' layers
  - The function which is performed between the 'presentation' and the 'network' layer is similar to the function performed at the transport layer.

UNIT 2

Network Topology

and

Layered Architecture

WHAT IS NETWORK TOPOLOGY?

- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology.
- A network topology refers to the physical or logical arrangement of devices and connections in a computer network.
- It defines how different devices and components in the network are interconnected and how data flows between them.
- Network topologies can be physical, where the devices and connections are physically laid out, or logical, where the topology is represented conceptually, regardless of the physical arrangement.
- Types of Network Topology
  7. Bus Topology
  8. Star Topology
  9. Ring Topology
  10. Tree topology
  11. Mesh topology
  12. Hybrid Topology

BUS TOPOLOGY

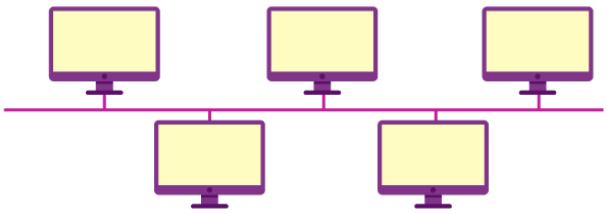


Fig. Bus Topology

- In bus network topology, every node is connected in series along a single cable, known as bus.
- The bus acts as a shared communication medium, where devices take turns transmitting data.
- The data is broadcasted to all devices on the network, but only the intended recipient accepts and processes it.
- When a node wants to send a message over the network, it puts a message over the network.
- Each device on the network listens to the bus for incoming data and only accepts data addressed specifically to it.
- The configuration of a bus topology is quite simpler as compared to other topologies.

- While bus topology was widely used in the past, it is less common in modern networks.
- However, it is still used in small-scale environments or as a backbone for some network architectures.

Advantages:

- Additional devices can be connected to the bus without disrupting the network.
- Devices can be added or removed without affecting other devices on the network.
- It works excellently in a tiny network and is cost-effective for small networks
- require fewer cables, It is easy to set up
- It demands a shorter cable length as compared to the star topology.
- Nodes are directly linked to the cable, therefore, the starting cost of installation is quite low.

Disadvantages:

- If the main cable, bus, fails, the entire network can be disrupted.
- It is very tough to determine the issues if the entire network goes down.
- Bandwidth is shared among all devices, so network performance can be adversely affected if many devices are transmitting simultaneously.
- The length of the bus cable is limited, which may impact network size and reach.
- If new devices are added, it would affect the network and slow down.
- It is not suitable for large networks.
- Though the concept of bus topology is pretty easy, it still demands a lot of cabling.

STAR TOPOLOGY

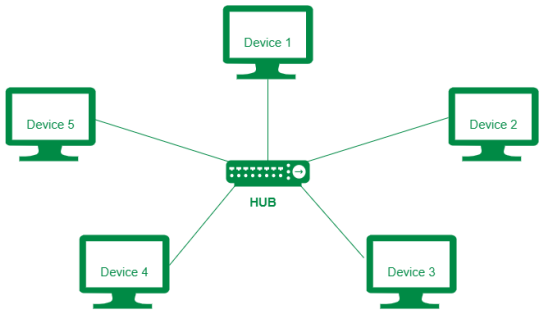


Fig. Star Topology

- In star topology all devices are connected to a central device, often referred as hub or switch.
- In this topology, each device has its own dedicated connection to the central device, forming a star-like structure with the central device at the center.
- Devices are connected to the central device using point-to-point connections, typically Ethernet cables.
- Every communication between hosts, takes place through only the hub.
- All data transmitted between devices in the network passes through the hub.

- Communication between devices is achieved by sending data from the source device to the central device, which then forwards the data to the destination device.
- Hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails.
- Local area networks based on Ethernet switches
- Most wired home and office networks have a physical star topology.

Advantages:

- The central hub allows for easy management and troubleshooting of the network.
- Issues with individual device connections can be isolated and addressed without affecting the entire network.
- It is relatively easy to add or remove devices from the network without disrupting the other devices.
- If a device or connection fails, it only affects the device connected to it, while the rest of the network remains operational.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages:

- If the central hub fails, the entire network can be disrupted.
- Each device requires its own connection to the central hub, resulting in more cables
- The central hub requires more resources and can be more expensive
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

RING TOPOLOGY

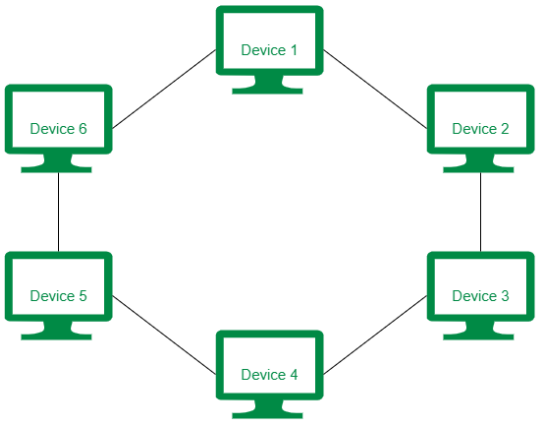


Fig. Ring Topology

- Each device has a dedicated connection to two neighboring devices, forming a continuous loop.
- A ring topology is a network configuration in which devices are connected in a closed loop,

forming a ring.

- Data is transmitted in a sequential manner, passing through each device in the ring.
- Each device is connected to two neighboring devices, and data travels in one direction around the ring.
- When a device receives data, it processes and forwards it to the next device until it reaches its intended destination.
- When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.
- To connect one more host in the existing structure, the administrator may need only one more extra cable.
- Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure.

Advantages:

- Data flows in a circular path, leading to efficient network performance.
- Each device gets an equal chance to transmit data, as token-based access control ensures fairness.
- The ring structure is relatively easy to set up and maintain.
- 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.

Disadvantages:

- The failure of a single node in the network can cause the entire network to fail.
- Adding or removing devices to the network can be challenging
- The overall length of the ring is limited, which can impact the size and reach of the network.
- Troubleshooting is difficult in this topology.
- Less secure.

TREE TOPOLOGY

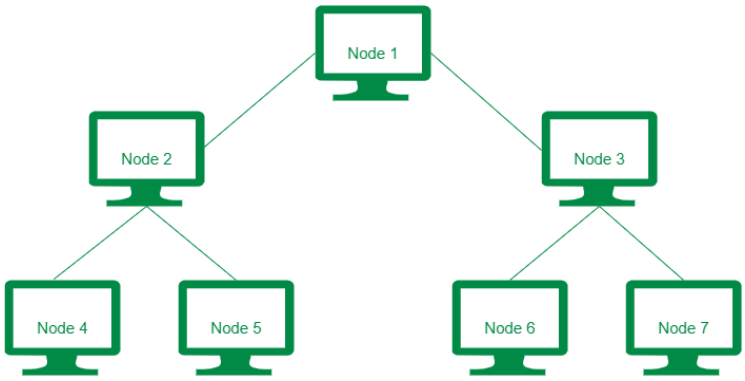


Fig. Tree Topology

- A tree topology, also known as a hierarchical topology
- This is the most common form of network topology in use presently.
- This topology imitates as extended Star topology and inherits properties of bus topology.
- This topology divides the network in to multiple levels/layers of network.
- Mainly in LANs, a network is bifurcated into three types of network devices, is a network configuration in which devices are arranged in a hierarchical structure, resembling a tree.
- It combines characteristics of both bus and star topologies.
- Devices are connected in a hierarchical manner, where a central device acts as the root of the tree.
- The central device, usually a switch or a router, connects to multiple branches of devices.
- Each branch of devices can have its own sub-branches, forming multiple levels of hierarchy.
- Communication between devices is achieved by sending data from a source device to the central device, which then determines the appropriate path to forward the data to the destination device.
- Tree topologies are commonly used in larger networks, such as wide area networks (WANs) or campus networks, that require scalability and organization.

Advantages:

- Tree topologies allow for easy expansion by adding new devices or branches without impacting the entire network.
- Devices can be added, removed, or reorganized with minimal disruption to the network.
- Devices in the same branch can communicate directly with each other, reducing network traffic.
- 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.
- Error detection and error correction are very easy in a tree topology.

Disadvantages:

- If the central hub gets fails the entire system fails.
- The hierarchical structure can lead to increased complexity in network management and troubleshooting.
- Implementing and maintaining can require more resources and infrastructure

- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

MESH TOPOLOGY

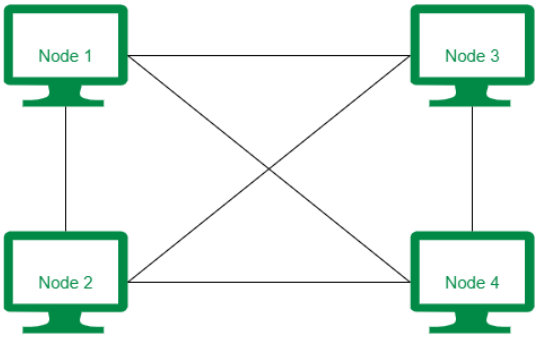


Fig. Mesh Topology

- In mesh topology, each device is connected to every other device in the network.
- This creates a fully interconnected network, where data can take multiple paths to reach its destination.
- Each device is directly connected to every other device, forming a web-like structure.
- Communication between devices can happen directly, without the need for a central device.
- Data can travel through multiple paths in the network, increasing redundancy and improving fault tolerance.
- Mesh topologies are commonly used in mission-critical networks, such as telecommunications networks and data centers, where high reliability and fault tolerance are essential.
- Mesh topologies can be categorized into two types
    - Full mesh: every device is connected to every other device in the network.
    - Partial mesh: only certain devices are directly connected to each other.

Advantages:

- The direct connections between devices allow for efficient communication and data transfer.
- Failure during a single device won't break the network.
- There is no traffic problem as there is a dedicated point to point links for every computer.
- Fault identification is straightforward.
- This topology provides multiple paths to succeed in the destination and tons of redundancy.
- It provides high privacy and security.
- Data transmission is more consistent because failure doesn't disrupt its processes.
- Adding new devices won't disrupt data transmissions.
- This topology has robust features to beat any situation.
- A mesh doesn't have a centralized authority.

Disadvantages:

- It's costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
- Installation is extremely difficult in the mesh.
- Power requirement is higher as all the nodes will need to remain active all the time and share the load.
- Complex process.
- The cost to implement mesh is above other selections.
- There is a high risk of redundant connections.
- Each node requires a further utility cost to think about.
- Maintenance needs are challenging with a mesh.

HYBRID TOPOLOGY

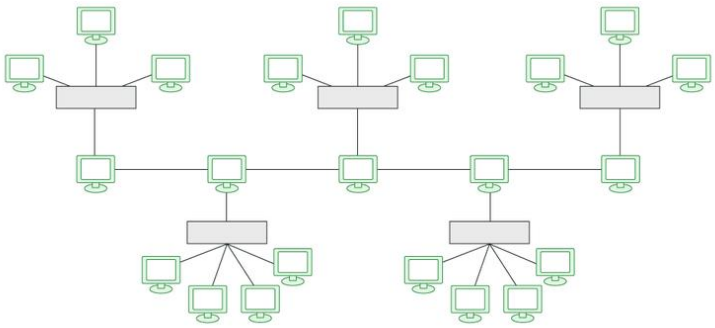


Fig. Hybrid Topology

- A network structure whose design contains more than one topology is said to be hybrid topology.
- Hybrid topology inherits merits and demerits of all the incorporating topologies.
- 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.
- A common example of a hybrid topology is a university campus network.

Advantages:

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is extremely flexible.
- It is very reliable.
- It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.

- Error detecting and troubleshooting are easy.
- Handles a large volume of traffic.
- It is used to create large networks.
- The speed of the topology becomes fast when two topologies are put together.

Disadvantages:

- It is a type of network expensive.
- The design of a hybrid network is very complex.
- There is a change in the hardware to connect one topology with another topology.
- Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.
- Hubs which are used to connect two distinct networks are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
- Installation is a difficult process.

LAYERED ARCHITECTURE

- Layered Architecture in a computer network is defined as a model where a whole network process is divided into various smaller sub-tasks.
- These divided sub-tasks are then assigned to a specific layer
- A single layer performs only specific type of task.
- To run the application and provide all types of services to clients a lower layer adds its services to the higher layer present above it.

OSI MODEL

- The open systems interconnection (OSI) model refers to a standard model used to describe the flow of information from one computing device to another operating in a networking environment.
- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks.
- OSI consists of seven layers, and each layer performs a particular network function.
- Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.
- The model defines a set of rules and requirements for data communication and interoperability between different devices, products, and software in a network infrastructure.

- Until OSI emerged, network architecture lacked the standard protocols necessary for effective data communication and design infrastructure.

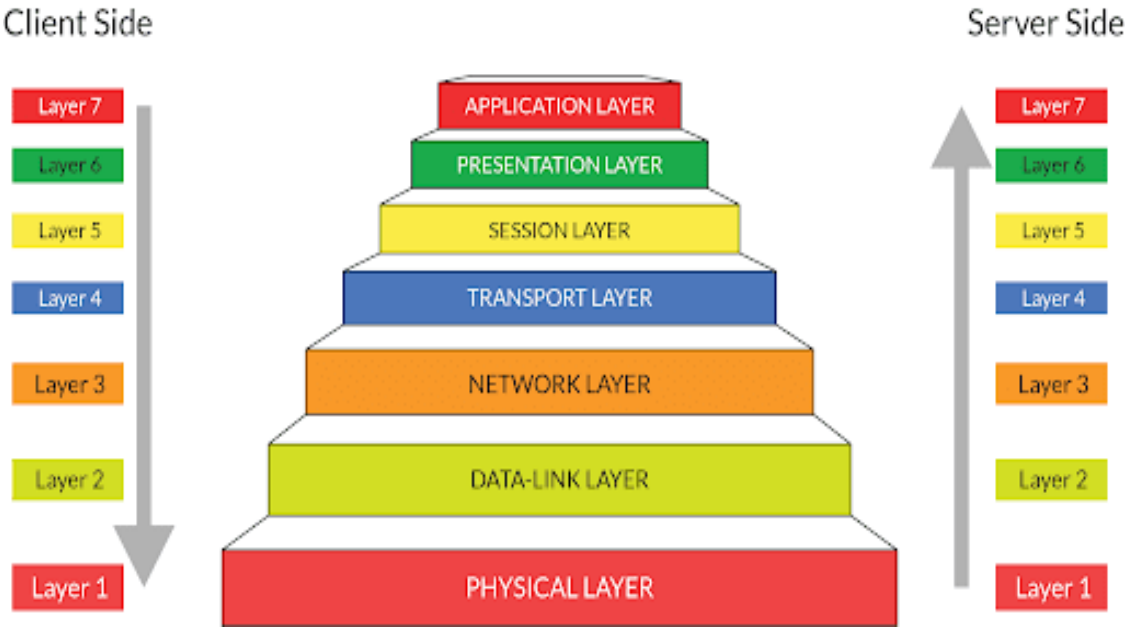


Fig. OSI Model

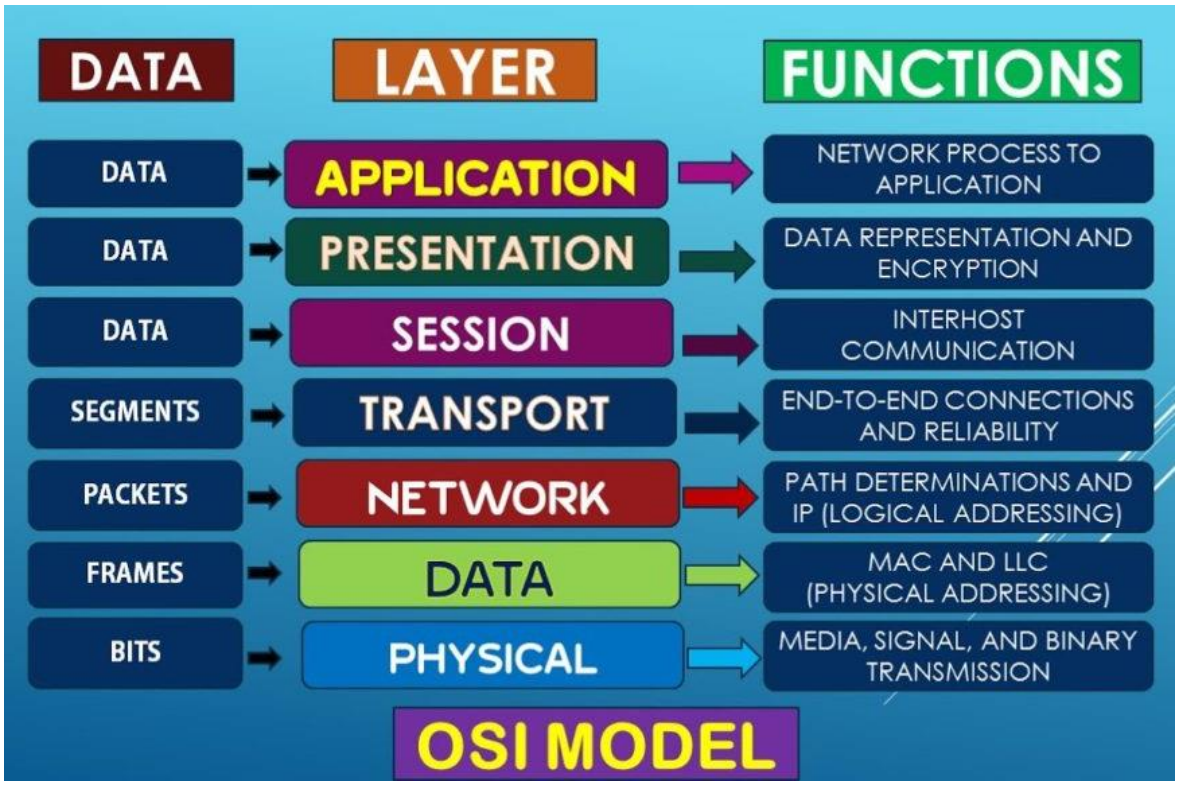
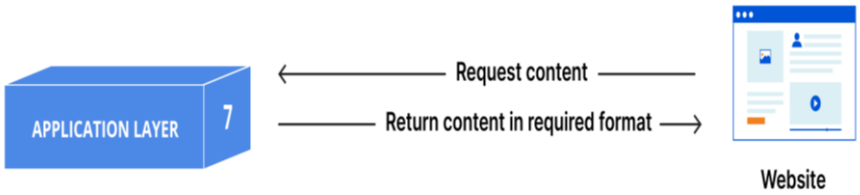


Fig. Concept of OSI Model

7. Application layer



- The application layer is the topmost layer in the OSI model.
- Application layer protocols allow the software to direct data flow and present it to the user.
- Software applications like web browsers and email clients rely on the application layer to initiate communications.
- This is the only layer that directly interacts with data from the user.
- The layer establishes communication between the application on the network and the end user using it by defining the protocols for successful user interaction.
- Client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.

- Application layer protocols include Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP).

Key functions:

- The application layer provides user interfaces (UI) that are key to user interaction
- Supports a variety of applications such as e-mail and remote file transfer
- Layer 7 ensures effective communication between applications on different computing systems and networks.

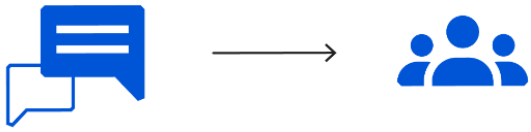
6. Presentation layer

- The presentation layer is often referred to as syntax or translation layer as it translates the application data into a network format.
- The presentation layer is responsible for translation, encryption, and compression of data.
- This layer also encrypts and decrypts data before transmitting it over the network.
- Layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.
- Moreover, this layer is known to compress data received from layer 7 to reduce the overall size of the data transferred.
- Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5.
- This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

Key functions:

- Performs data translation based on the application's data semantics
- Encrypts and decrypts sensitive data transferred over communication channels
- Performs data compression to reduce the number of bits in exchanged data
- layer 6 ensures that the communicated information is in the desired format as required by the receiving application.

5. The session layer



- The session layer establishes a communication session between communicating entities.
- The time between when the communication is opened and closed is known as the session.
- This is the layer responsible for opening and closing communication between the two devices.
- The session is maintained at a sufficient time interval to ensure efficient data transmission and avoid wasting computing resources.
- In situations where large volumes of data are sent at once, layer 5 can break down the data into smaller chunks by adding checkpoints.
- The session layer also synchronizes data transfer with checkpoints.
- For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

Key functions:

- Opens maintains, and closes communication sessions
- Enables data synchronization by adding checkpoints to data streams
- Layer 5 establishes, maintains, synchronizes, and terminates sessions between end-user applications.

4. Transport layer

- Layer 4 is responsible for end-to-end communication between the two devices.
- This includes taking data from the session layer and breaking it up into chunks called segments
- The transport layer allows safe message transfer between the sender and the receiver.
- It divides the data received from the layer 5 into smaller segments. It also reassembles the data at the receiver side to allow the session layer to read it.
- Layer 4 performs two critical functions: flow control and error control.

- Flow control implies regulating data transfer speeds. It ensures that the communicating device with a good network connection does not send data at higher rates, which is difficult for devices with slower connections to handle.
- Error control refers to the error-checking functionality to ensure the completeness of data. In incomplete data cases, this layer requests the system to resend the incomplete data.
- Examples of transport layer protocols include transmission control protocol (TCP) and user datagram protocol (UDP).

Key functions:

- Ensures completeness of each message exchanged between source and destination
- Maintains proper data transmission through flow control and error control
- Performs data segmentation and reassembling of data
- Layer 4 is responsible for transmitting an entire message from a sender application to a receiver application.

3. Network layer

- The network layer enables the communication between multiple networks.
- The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary.
- The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device.
- The network layer also finds the best physical path for the data to reach its destination; this is known as routing.
- This network layer uses internet protocol (IP) for data delivery.

Key functions:

- Handles routing to recognize suitable routes from sender to receiver
- Performs logical addressing that assigns unique names to each device operating over the network
- Layer 3 is responsible for dividing segmented data into network packets, reassembling them at the recipient's side, and identifying the shortest yet most suitable and secure path for transmitting data packets.

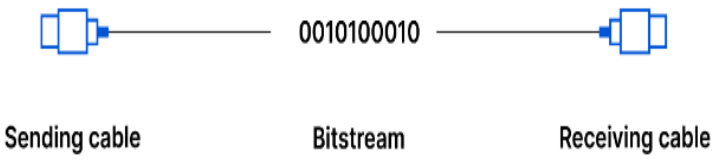
2. Data link layer

- The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the same network.
- The data link layer transmits data between two nodes that are directly connected or are operating over the same network architecture.
- The data link layer takes packets from the network layer and breaks them into smaller pieces called frames.
- Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication.
- The transport layer only does flow control and error control for inter-network communications.
- Layer 2 is divided into two sub-layers: media access control (MAC) and logical link control (LLC). The MAC layer encapsulates data frames transmitted through the network connecting media such as wires or cables. In situations where such data transmission fails, LLC helps manage packet retransmission.

Key functions:

- Detects damaged or lost frames and retransmits them
- Performs framing where data received from layer 3 is further subdivided into smaller units called frames
- Updates headers of created frames by adding the MAC address of the sending device and receiving device
- Layer 2 is responsible for setting up and terminating physical connections between participating network nodes.

1. Physical layer



- The last OSI layer is the physical layer.
- This layer manages physical hardware and network components such as cables, switches, or routers that transmit data.

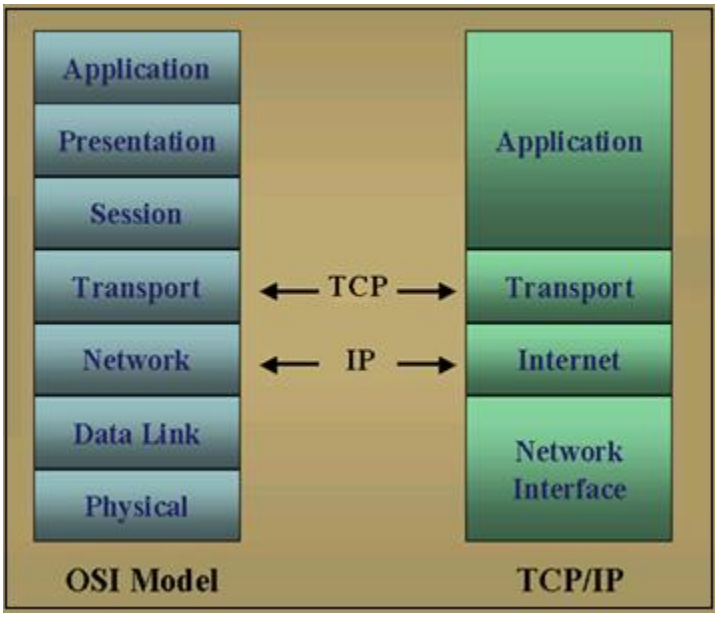
- This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s.
- The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

- Technically, this layer picks up bits from the sender end, encodes them into a signal, sends the signal over the network, and decodes the signal at the receiver end.
- Thus, without layer 1, communicating data bits across network devices through physical media is not possible.

Key functions:

- Synchronizes data bits
- Enables modulation, that is, conversion of a signal from one form to another for data transmission
- Defines data transmission rate (bits/sec)
- Defines transmission modes such as simple or half-duplex mode
- Layer 1 is responsible for transmitting data bits of 0s and 1s between network systems via electrical, mechanical, or procedural interfaces.

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.
- The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a conceptual framework used for designing and understanding how network protocols and communication work within computer networks.
- It is a suite of communication protocols used to interconnect network devices on the internet.
- TCP and IP are the two main protocols, though others are included in the suite.

The 4 layers of the TCP/IP model

5. Application Layer:

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- The Application Layer enables communication between software applications and services running on different devices within a network.
- For example: web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- It defines the formats and conventions for data exchange between applications. This includes specifying how data is formatted, encoded, and structured.
- The Application Layer includes protocols
    - HTTP (Hypertext Transfer Protocol) for web browsing.
    - FTP (File Transfer Protocol) for file transfers.
    - SMTP (Simple Mail Transfer Protocol) for email communication.
    - DNS (Domain Name System) for translating domain names to IP addresses.

4. Transport Layer

- This is third layer in the TCP/IP model.
- The Transport Layer is responsible for maintaining reliable, end-to-end communication between devices across a network.
- It manages the flow control, error checking, and data integrity during the exchange of information.
- The Transport Layer breaks down large messages into smaller units called segments for transmission. This process is known as segmentation.
- At the receiving end, the Transport Layer reassembles the segments into the original message.
- It includes mechanisms for error detection, acknowledgment, and retransmission of lost or corrupted segments.

- This ensures that data is delivered accurately and completely, and any errors during transmission are corrected.
- The two primary protocols operating at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- TCP establishes and terminates connections between devices to facilitate reliable communication. A three-way handshake is used for connection establishment, and a four-way handshake is used for connection termination.
- UDP operates as a connectionless protocol without the overhead of establishing and maintaining a connection.

2. Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Its primary functions include logical addressing, routing, and fragmentation
- The Internet layer assigns logical address known as IP address to devices. IP addresses are used to uniquely identify devices in the network.
- The Internet Layer is also responsible for fragmentation, in which large packets breaks down into smaller fragments if the network has a smaller maximum packet size. At the receiving end, the fragments are reassembled into the original complete packet.
- The Internet layer ensures that the packet is forwarded to the correct destination. It uses routing algorithms to determine the best path for a packet to reach its destination.
- The Internet Layer handles error detection

1. Network Access Layer

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

DIFFERENCE BETWEEN TCP/IP AND OSI MODEL

TCP/IP MODEL	OSI MODEL
TCP/IP refers to Transmission Control	OSI refers to Open Systems Interconnection.

Protocol/ Internet Protocol.	
It is a communication protocol that is based on standard protocols and allows the connection of hosts over a network.	It is a structured model which deals which the functioning of a network.
In 1982, It was developed by ARPANET (Advanced Research Project Agency Network).	In 1984, OSI model has been developed by ISO (International Standard Organization).
It comprises of four layers: • Network Interface • Internet • Transport • Application	It comprises seven layers: • Physical • Data Link • Network • Transport • Session • Presentation • Application
It follows a horizontal approach.	It follows a vertical approach.
The TCP/IP is the implementation of the OSI Model.	An OSI Model is a reference model, based on which a network is created.
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.
It is protocol dependent.	It is protocol independent.
This model is highly used.	The usage of this model is very low.
In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.	In this model, the session and presentation layers are separated, i.e., both the layers are different.
The network layer provides only connectionless service.	In this model, the network layer provides both connection-oriented and connectionless service.
In this model, the protocol cannot be easily replaced.	Protocols in the OSI model are hidden and can be easily replaced when the technology changes.
It does not provide the standardization to the devices. It provides a connection between various computers.	It provides standardization to the devices like router, motherboard, switches, and other hardware devices.

SIMILARITIES BETWEEN OSI MODEL AND TCP/IP MODEL

- Share common architecture
  - Both the models are the logical models and having similar architectures as both the models are constructed with the layers.
- Define standards

  - Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.

- Simplified troubleshooting process
  - Both models have simplified the troubleshooting process by breaking the complex function into simpler components.
- Pre-defined standards
  - The standards and protocols are already pre-defined; these models do not redefine them. For example, the Ethernet standards were already defined by the IEEE before the development of these models; instead of recreating them, models have used these pre-defined standards.
- Both have similar functionality of 'transport' and 'network' layers
  - The function which is performed between the 'presentation' and the 'network' layer is similar to the function performed at the transport layer.