Introduction to Computer Networks

A computer network is a group of interconnected computers that communicate with each other to share resources and information. The primary goal of a computer network is to allow computers to share data and resources efficiently. Networks can vary in size from small home networks to large global networks like the Internet.

Types of Computer Networks

1. Local Area Network (LAN):
    - Covers a small geographic area, like a single building or campus.
    - High-speed connections with low latency.
    - Commonly used in homes, offices, and schools.
2. Wide Area Network (WAN):
    - Covers a large geographic area, such as a city, country, or even multiple countries.
    - Lower speeds compared to LANs, often due to long-distance data transmission.
    - The Internet is the largest example of a WAN.
3. Metropolitan Area Network (MAN):
    - Spans a city or a large campus.
    - Larger than a LAN but smaller than a WAN.
    - Used to connect multiple LANs within a metropolitan area.
4. Personal Area Network (PAN):
    - Very small network, typically within the range of an individual person.
    - Used for connecting personal devices like smartphones, tablets, and laptops.
5. Virtual Private Network (VPN):
    - Extends a private network across a public network, allowing secure access to the private network.
    - Uses encryption to secure data transmission.

Network Applications

Network applications are software applications that utilize the capabilities of computer networks. They allow users to perform various tasks over a network, whether it's a local network or the Internet.

Common Network Applications

1. Email:
    - Allows users to send and receive messages over the Internet.
    - Examples: Gmail, Outlook.
2. Web Browsing:
    - Access and retrieve information from the World Wide Web.
    - Examples: Google Chrome, Mozilla Firefox.
3. File Sharing:
    - Transfer files between computers over a network.
    - Examples: Dropbox, Google Drive.
4. Instant Messaging:
    - Real-time text communication between users.
    - Examples: WhatsApp, Slack.
5. Voice over IP (VoIP):
    - Allows voice communication over the Internet.
    - Examples: Skype, Zoom.
6. Online Gaming:
    - Enables multiplayer gaming over a network.
    - Examples: Fortnite, League of Legends.
7. Remote Desktop:
    - Access and control a computer remotely over a network.
    - Examples: TeamViewer, Remote Desktop Protocol (RDP).
8. Streaming Media:
    - Allows real-time playback of audio and video over the Internet.
    - Examples: Netflix, Spotify.

Network Software Components

Network software components are essential for managing, monitoring, and operating computer networks. These software solutions facilitate communication between devices, ensure security, and optimize network performance.

Types of Network Software

1. Network Operating System (NOS):

- Manages network resources and provides services to connected devices.
- Examples: Windows Server, Linux, Unix.

2. Network Management Software:
   - Monitors and manages network performance, fault detection, and configuration.
   - Examples: SolarWinds, Nagios, PRTG Network Monitor.
3. Firewall Software:
   - Protects the network by controlling incoming and outgoing traffic based on predetermined security rules.
   - Examples: pfSense, Cisco ASA, ZoneAlarm.
4. Antivirus and Anti-malware Software:
   - Protects networked devices from malicious software and threats.
   - Examples: Norton, McAfee, Kaspersky.
5. Virtual Private Network (VPN) Software:
   - Creates a secure connection over a public network.
   - Examples: OpenVPN, NordVPN, Cisco AnyConnect.
6. Network Protocols:
   - Define rules and conventions for communication between network devices.
   - Examples: TCP/IP, HTTP, FTP, SMTP.
7. Remote Access Software:
   - Allows users to access a computer or network remotely.
   - Examples: TeamViewer, AnyDesk, Remote Desktop Protocol (RDP).

Network Hardware Components (Interconnection Networking Devices)

Network hardware components are the physical devices that connect and enable communication between different devices in a network. These devices facilitate data transfer, network management, and ensure smooth network operation.

Types of Network Hardware Components

1. Router:
   - Connects different networks and directs data packets between them.
   - Determines the best path for data to travel from source to destination.
2. Switch:

- Connects multiple devices within the same network (LAN).
- Uses MAC addresses to forward data to the correct device.

3. Hub:
    - Connects multiple Ethernet devices, making them act as a single network segment.
    - Broadcasts data to all connected devices, less efficient than switches.
4. Modem:
    - Modulates and demodulates analog signals for digital data transmission over telephone lines or cable systems.
    - Used for Internet access in homes and offices.
5. Access Point (AP):
    - Provides wireless connectivity to devices within a network.
    - Extends the reach of a wired network to wireless devices.
6. Network Interface Card (NIC):
    - Allows a computer to connect to a network.
    - Can be wired (Ethernet NIC) or wireless (Wi-Fi NIC).
7. Firewall (Hardware):
    - Protects the network by filtering traffic based on security rules.
    - Can be standalone devices or integrated into routers.
8. Repeater:
    - Amplifies and retransmits signals to extend the range of a network.
    - Used in both wired and wireless networks.
9. Bridge:
    - Connects two or more network segments, improving communication and reducing traffic.
    - Operates at the data link layer (Layer 2) of the OSI model.
10. Gateway:
    - Acts as a bridge between different networks using different protocols.
    - Translates data between different network formats.
11. Load Balancer:

- Distributes incoming network traffic across multiple servers to ensure no single server becomes overwhelmed.
- Enhances the performance and reliability of applications.

12. Proxy Server:
    - Acts as an intermediary for requests from clients seeking resources from other servers.
    - Provides anonymity, content filtering, and load balancing.

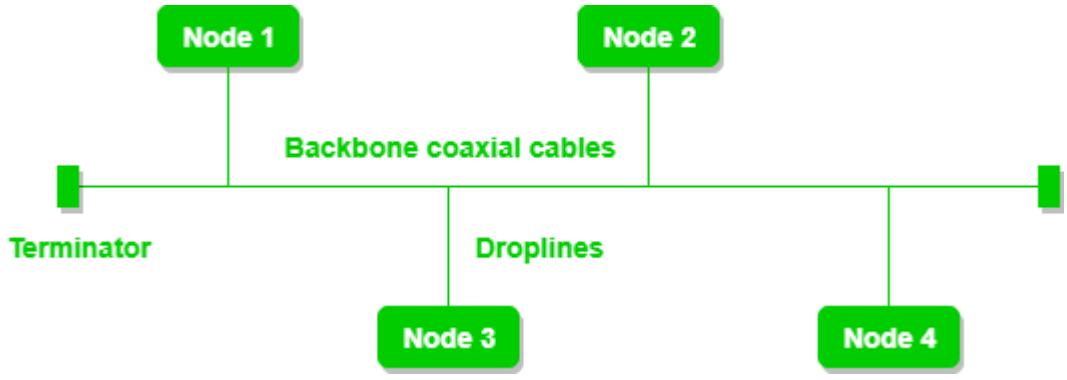
Network Topology

Network topology refers to the arrangement of different elements like nodes, links, and devices in a computer network. It defines how these components are connected and interact with each other. Understanding various types of network topologies helps in designing efficient and robust networks. Common types include bus, star, ring, mesh, and tree topologies, each with its own advantages and disadvantages. In this article, we are going to discuss different types of network topology their advantages and disadvantages in detail.

Types of Network Topology

What is Bus Topology?

Bus topology carries transmitted data through the cable because data reaches each node, the node checks the destination address (MAC/IP address) to determine if it matches their address. If the address does not match with the node, the node does nothing more. But if the addresses of nodes match to addresses contained within the data then they process knowledge. In the bus, communication between nodes is done through a foremost network cable.



Bus Topology

Key Features of Bus Topology

- An efficient bus architecture is established, and each station is connected by a single backbone cable.
- There are two requirements: Initially, the nodes are connected to the backbone cable directly, or they use a drop cable to help them connect.
- The well-known access method for bus topologies is called CSMA (Carrier Sense Multiple Access).

Best Practice for Designing Bus Topology

1. Plan for Scalability: Plan for the network's future growth and expansion. Ensure that the bus topology can accommodate extra devices with out extensively affecting overall performance.
2. Use Good Quality Cabling: Create a good cabling setup for the bus backbone. Ensure that the cable is properly shielded to minimize sign interference and degradation. Use cable with suitable bandwidth and make certain that it meets the necessities of the network.
3. Implement Redundancy: Think about adding redundancy to decrease the risk of a single point of failure (SPoF).
4. Terminate the Bus Properly: Terminate both ends of the bus with terminators to prevent signal reflection and ensure signal integrity. Improper termination can result in signal degradation and performance issues.

Advantages of Bus Topology

- It is the easiest network topology for linearly connecting peripherals or computers.
- It works very efficiently well when there is a small network.
- The length of cable required is less than a star topology.
- It is easy to connect or remove devices in this network without affecting any other device.
- Very cost-effective as compared to other network topology i.e. mesh and star
- It is easy to understand topology.
- Easy to expand by joining the two cables together.

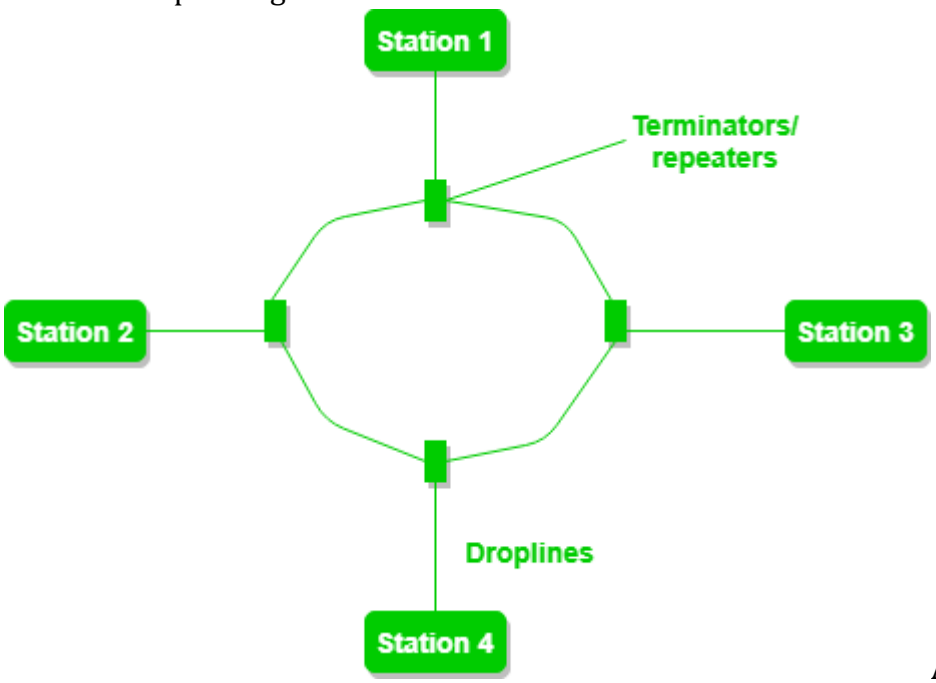
Disadvantages of Bus Topology

- Bus topology is not good for large networks.
- Identification of problems becomes difficult if the whole network goes down.
- Troubleshooting individual device issues is very hard.
- Need terminators are required at both ends of the main cable.

- Additional devices slow the network down.
- If the main cable is damaged, the whole network fails or splits into two.
- Packet loss is high.
- This network topology is very slow as compared to other topologies.

Ring Topology

Ring Topology may be a network configuration where device connections create a circular data path. In this each device is connected to with its exactly two neighboring devices, like points on a circle which forms like a ring structure. A number of repeaters are used for Ring topology with a large number of nodes to send data and to prevent data loss repeaters are used in this network. Together, devices during a ring topology are mentioned as a hoop network. In this packets travels from one device to another until they reach the desired destination. In this data travels in unidirectional forms means in only one direction but it can also do bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. It is used in LANs and WANs depending on the card of network in the computer.



Advantages of Ring topology :

- In this data flows in one direction which reduces the chance of packet collisions.
- In this topology additional workstations can be added after without impacting performance of the network.
- Equal access to the resources.
- There is no need of server to control the connectivity among the nodes in the topology.

- It is cheap to install and expand.
- Minimum collision.
- Speed to transfer the data is very high in this type of topology.
- Due to the presence of token passing the performance of ring topology becomes better than bus topology under heavy traffic.
- Easy to manage.
- Ring network is extremely orderly organized where every device has access to the token and therefore the opportunity to transmit.

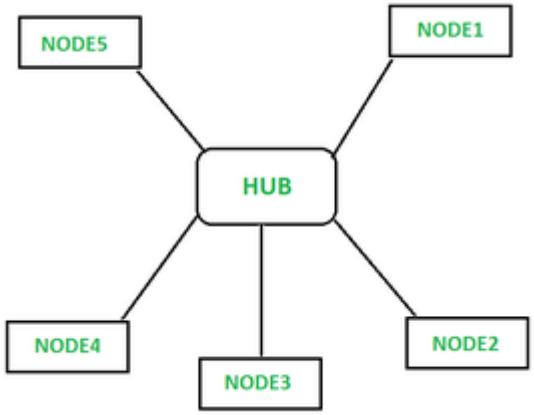
Disadvantages of Ring topology :

- Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes.
- If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.
- It is slower in performance as compared to the bus topology
- It is Expensive.
- Addition and removal of any node during a network is difficult and may cause issue in network activity.
- Difficult to troubleshoot the ring.
- In order for all the computer to communicate with each other, all computer must be turned on.
- Total dependence in on one cable.
- They were not Scalable.

Star Topology

A star may be a topology for a Local Area Network (LAN) during which all nodes are individually connected to a central connection point, sort of a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, just one node is going to be brought down. Each device within the network is connected to a central device called a hub. If one device wants to send data to another device, it's first to send the info to the hub then the hub transmits that data to the designated device. The number of links required to connect nodes in the star topology is N where N is the

number of nodes. The hub, switch, or concentrator manages and controls all functions of



the network.

How Does Star Topology Works in Computer Networks?

As we know, all the nodes in a star topology are connected to the Hub, which star topology are connected to the central node called the Hub is responsible for the transmission of the data. For example- when any node wants to transmit data to another node it first transmits data to the central node which then transfers the data to all the nodes on the network. Once the node receives the data then it checks for the destination address if the address matches the data is accepted otherwise data is rejected.

Advantages of Star Topology

- It is very reliable – if one cable or device fails then all the others will still work.
- It is high-performing as no data collisions can occur.
- It is less expensive because each device only needs one I/O port and wishes to be connected to the hub with one link.
- Easier to put in.
- Robust in nature.
- Easy fault detection because the links are often easily identified.
- No disruptions to the network when connecting or removing devices.
- Each device requires just one port i.e. to attach to the hub.
- If N devices are connected to each other in star, then the amount of cables required to attach them is N. So, it's easy to line up.

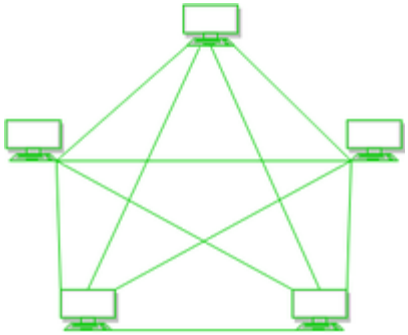
Disadvantages of Star Topology

- Requires more cable than a linear bus.
- If the connecting network device (network switch) fails, the nodes attached are disabled and can't participate in network communication.
- More expensive than linear bus topology due to the value of the connecting devices (network switches).

- If the hub goes down everything goes down, none of the devices can work without the hub.
- Hub requires more resources and regular maintenance because it's the central system of Star.
- Extra hardware is required (hubs or switches) which adds to the cost.
- Performance is predicated on the one concentrator i.e. hub.

Mesh Topology :

In mesh, all the computers are interconnected to every other during a network. Each computer not only sends its own signals but also relays data from other computers. The nodes are connected to every other completely via a dedicated link during which information is travel from nodes to nodes and there are N(N-1)/2 links in mesh if there are N nodes. Every node features a point-to-point connection to the opposite node. The connections within the mesh are often wired or wireless.



There are two types of Mesh topologies –

1. Fully-connected Mesh Topology
2. Partially-connected Mesh Topology

1. Full Mesh Topology :

All the nodes within the network are connected with every other If there are n number of nodes during a network, each node will have an n-1 number of connections. A full mesh provides an excellent deal of redundancy, but because it is prohibitively expensive to implement, it's usually reserved for network backbones.

Total number of links required for the mesh topology is [n(n-1)]/2.

2. Partial Mesh Topology :

The partial mesh is more practical as compared to the full mesh. In a partially connected mesh, all the nodes aren't necessary to be connected with one another during a network. Peripheral networks are connected using partial mesh and work with a full-mesh backbone in tandem.

Advantages of Mesh Topology :

- 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 of Mesh Topology :

- 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.

Tree Topology

Network topology is the systematic arrangement of the elements (links, nodes, etc.) of a communication network. Network topology can be used to make understand that it is the arrangement of various types of telecommunication networks which includes command and control radio networks, industrial field busses, and other essential network. Tree Topology: Tree Topology is a topology which is having a tree structure in which all the computers are connected like the branches which are connected with the tree. In Computer Network, tree topology is called a combination of a Bus and Star network topology. The main advantages of this topology are that is very flexible and also has better scalability. Tree network topology is considered to be the simplest topology in all the topologies which is having only one route between any two nodes on the

network. The pattern of connection resembles a tree in which all branches spring from one root hence (Tree Topology). Tree topology is one of the most popular among the five network topologies.

Advantages of Tree Topology :

- This topology is the combination of bus and star topology.
- This topology provides a hierarchical as well as central data arrangement of the nodes.
- As the leaf nodes can add one or more nodes in the hierarchical chain, this topology provides high scalability.
- The other nodes in a network are not affected if one of their nodes gets damaged or does not work.
- Tree topology provides easy maintenance and easy fault identification can be done.
- A callable topology. Leaf nodes can hold more nodes.
- Supported by several hardware and software vendors.
- Point-to-point wiring for individual segments.
- Tree Topology is highly secure.
- It is used in WAN.
- Tree Topology is reliable.

Disadvantages of Tree Topology :

- This network is very difficult to configure as compared to the other network topologies.
- The length of a segment is limited & the limit of the segment depends on the type of cabling used.
- Due to the presence of a large number of nodes, the network performance of tree topology becomes a bit slow.
- If the computer on the first level is erroneous, the next-level computer will also go under problems.
- Requires a large number of cables compared to star and ring topology.
- As the data needs to travel from the central cable this creates dense network traffic.
- The Backbone appears as the failure point of the entire segment of the network.
- Treatment of the topology is pretty complex.
- The establishment cost increases as well.

- If the bulk of nodes is added to this network, then the maintenance will become complicated.

A hybrid topology

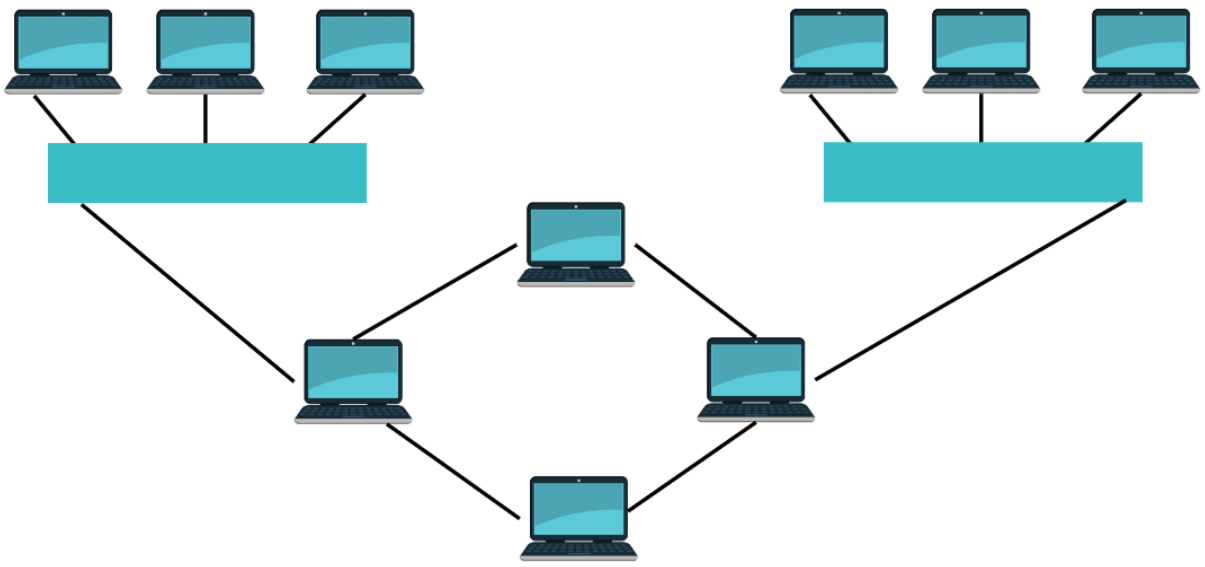
A hybrid topology is defined as a network topology that combines two or more different network topologies. A hybrid topology can be a combination of bus topology, ring topology and mesh topology. The selection of different types of network topologies combined together depends upon the number of computers, their location, and the required performance. In the hybrid topology network sections consist of a configuration of different types of network topologies. The structure of hybrid topology is more complex but offers various advantages such as flexibility and fault tolerance.

Working of Hybrid Topology

- Hybrid topology in computer networks is a combination of more than one topology.
- This hybrid topology makes use of standards such as Wi-Fi and Ethernet for performing its different operations.
- The functioning of hybrid topology depends upon various types of hybrid routers used such as switches and hubs as they can easily connect the devices that are connected over wired or wireless networks.
- The hybrid topology has different network branches and each branch as its own unique design.
- The functioning takes place by gaining various benefits of the both of the different topologies used.

Types of Hybrid Topologies

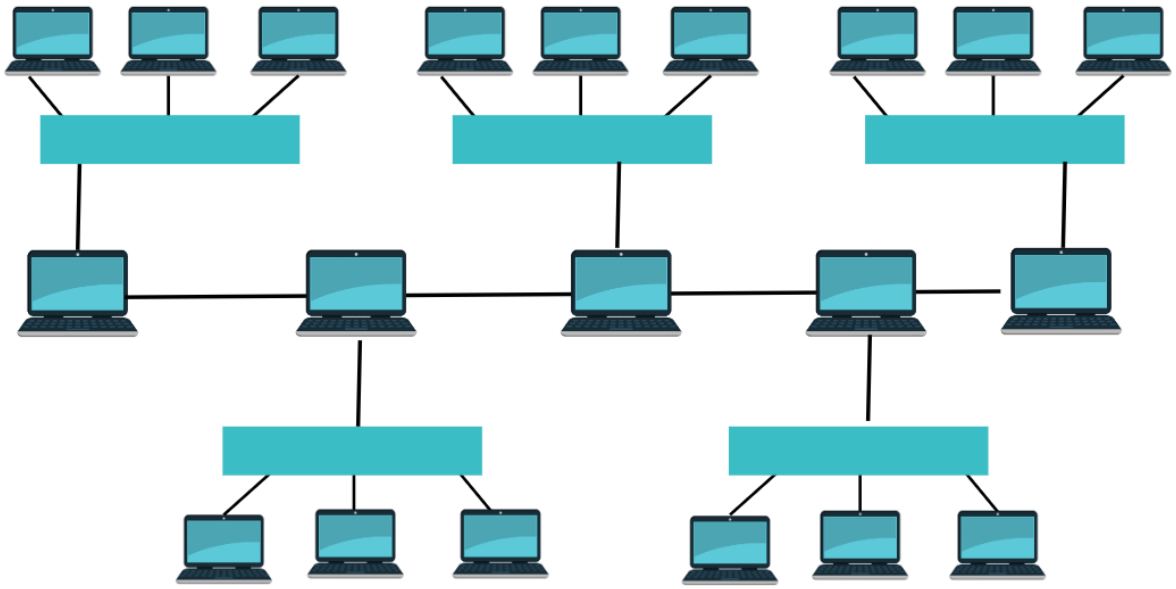
1. Star-Ring Hybrid Topology



Star-Ring Hybrid Topology

The combination of star and ring topology forms a star-ring topology. Two or more than two star topologies are connected together through a ring topology using a wired connection. The flow of data in star-ring topology is bidirectional or unidirectional. If any node of the original ring topology gets fail the bidirectional data flow provides with the surety that there will be no effect on the rest of the data in network flow.

2. Star-Bus Hybrid Topology



Star-Bus Hybrid Topology

The combination of star and bus topology is known as star-bus hybrid topology. Two or more star topologies are connected together with the help of bus topology through a wired connection. The bus topology can interrelate different star topologies and offers with a backbone structure. The entire network is not affected in case of any node failure. The failed node can be then easily replaced and offers with a easy way for adding or deleting the nodes. The overall network can be easily modified according to the need.

3. Hierarchical Network Topology

Hierarchical network topology is designed like a hierarchical tree and also known as network tree topology. Hierarchical network topology is a combination of star-ring hybrid topology and star-bus hybrid topology. The maximum level of hierarchical network topology is known as root node or parent node. The sub-nodes of parent node are known as child nodes. The last nodes that does does not have any child are known as leaf nodes.

Advantages of Hybrid Topology

Below are the advantages of hybrid topology:

- Adding a new node or deleting the existing node is easy in hybrid topologies.

- Hybrid topology is more secure, reliable, and scalable as compared to individual star, ring and mesh topology.
- Error detection and troubleshooting is easier in hybrid topology.
- When an organization has a large geographical area utilizing hybrid topology is considered as better option.
- Traffic with large volume is handled easily by the hybrid topology.
- The overall performance and speed is greater in hybrid topology.

Protocol Hierarchies

Protocol hierarchies, also known as protocol stacks or layers, are a structured set of protocols that work together to facilitate communication between devices in a network. Each layer in the hierarchy has a specific function and interacts with the layers directly above and below it. This layered approach helps in managing the complexity of network communication and ensures that protocols can be developed and updated independently.

OSI Model (Open Systems Interconnection Model)

The OSI model is a conceptual framework used to understand and implement network protocols in seven distinct layers. Each layer serves a specific function and communicates with the layers directly above and below it.

1. **Layer 1: Physical Layer**
    - Deals with the physical connection between devices and the transmission of raw binary data.
    - Includes hardware components like cables, switches, and network interface cards.
    - Examples: Ethernet, USB, Bluetooth.
2. **Layer 2: Data Link Layer**
    - Responsible for node-to-node data transfer and error detection/correction.
    - Divided into two sublayers: Media Access Control (MAC) and Logical Link Control (LLC).
    - Examples: Ethernet, Wi-Fi, PPP.
3. **Layer 3: Network Layer**
    - Manages logical addressing and routing of data packets between devices across different networks.

- Responsible for packet forwarding, including routing through intermediate routers.
- Examples: IP (Internet Protocol), ICMP, ARP.

4. **Layer 4: Transport Layer**
   - Ensures end-to-end communication, error recovery, and flow control.
   - Segments and reassembles data for transport.
   - Examples: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
5. **Layer 5: Session Layer**
   - Manages sessions or connections between applications.
   - Responsible for establishing, maintaining, and terminating connections.
   - Examples: NetBIOS, RPC.
6. **Layer 6: Presentation Layer**
   - Translates data between the application layer and the network.
   - Handles data encryption, decryption, compression, and translation.
   - Examples: SSL/TLS, JPEG, MPEG.
7. **Layer 7: Application Layer**
   - Provides network services directly to end-user applications.
   - Handles high-level APIs, resource sharing, and remote file access.
   - Examples: HTTP, FTP, SMTP, DNS.

TCP/IP Model (Transmission Control Protocol/Internet Protocol Model)

The TCP/IP model is a more practical and widely used framework compared to the OSI model. It has four layers, each corresponding to one or more layers in the OSI model.

1. **Layer 1: Link Layer (Network Interface Layer)**
   - Corresponds to the OSI's Physical and Data Link layers.
   - Handles the physical connection and data framing.
   - Examples: Ethernet, Wi-Fi.
2. **Layer 2: Internet Layer**
   - Corresponds to the OSI's Network layer.
   - Manages logical addressing and routing of data packets.
   - Examples: IP, ICMP, ARP.

3. **Layer 3: Transport Layer**
    - Corresponds to the OSI's Transport layer.
    - Ensures reliable data transfer and error recovery.
    - Examples: TCP, UDP.
4. **Layer 4: Application Layer**
    - Corresponds to the OSI's Session, Presentation, and Application layers.
    - Provides application-level services and protocols.
    - Examples: HTTP, FTP, SMTP, DNS.

Comparison of OSI and TCP/IP Models

- **Layer Count:**
    - OSI Model: 7 layers.
    - TCP/IP Model: 4 layers.
- **Development:**
    - OSI Model: Developed as a theoretical framework by ISO.
    - TCP/IP Model: Developed by the Department of Defense (DoD) as part of the ARPANET project.
- **Usage:**
    - OSI Model: Primarily used as a teaching tool and for conceptual understanding.
    - TCP/IP Model: Widely used in practical implementations and the Internet.

Design Issues for the Layers

The following are the design issues for the layers:

1. **Reliability:** It is a design issue of making a network that operates correctly even when it is made up of unreliable components.
2. **Addressing:** There are multiple processes running on one machine. Every layer needs a mechanism to identify senders and receivers.
3. **Error Control**: It is an important issue because physical communication circuits are not perfect. Many error detecting and error correcting codes are available. Both sending and receiving ends must agree to use any one code.
4. **Flow Control:** If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers. There are several mechanisms used for flow control such as increasing buffer size at receivers, slow down the fast sender, and so on. Some process will

not be in position to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting and the reassembling messages.

5. **Multiplexing and De-multiplexing:** If the data has to be transmitted on transmission media separately, it is inconvenient or expensive to setup separate connection for each pair of communicating processes. So, multiplexing is needed in the physical layer at sender end and de-multiplexing is need at the receiver end.
6. **Scalability**: When network gets large, new problem arises. Thus scalability is important so that network can continue to work well when it gets large.
7. **Routing:** When there are multiple paths between source and destination, only one route must be chosen. This decision is made on the basis of several routing algorithms, which chooses optimized route to the destination.
8. **Confidentiality and Integrity:** Network security is the most important factor. Mechanisms that provide confidentiality defend against threats like eavesdropping. Mechanisms for integrity prevent faulty changes to messages.

Difference between Connection-oriented and Connection-less Services:

S.NO	Connection-oriented Service	Connection-less Service
1.	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
3.	Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
4.	Connection-oriented Service is feasible.	Connection-less Service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.

S.NO	Connection-oriented Service	Connection-less Service
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
7.	In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
8.	Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.
9.	Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)
10.	Connection-oriented requires authentication.	Connection-less Service does not require authentication.

OSI Model

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

Characteristics of OSI Model:

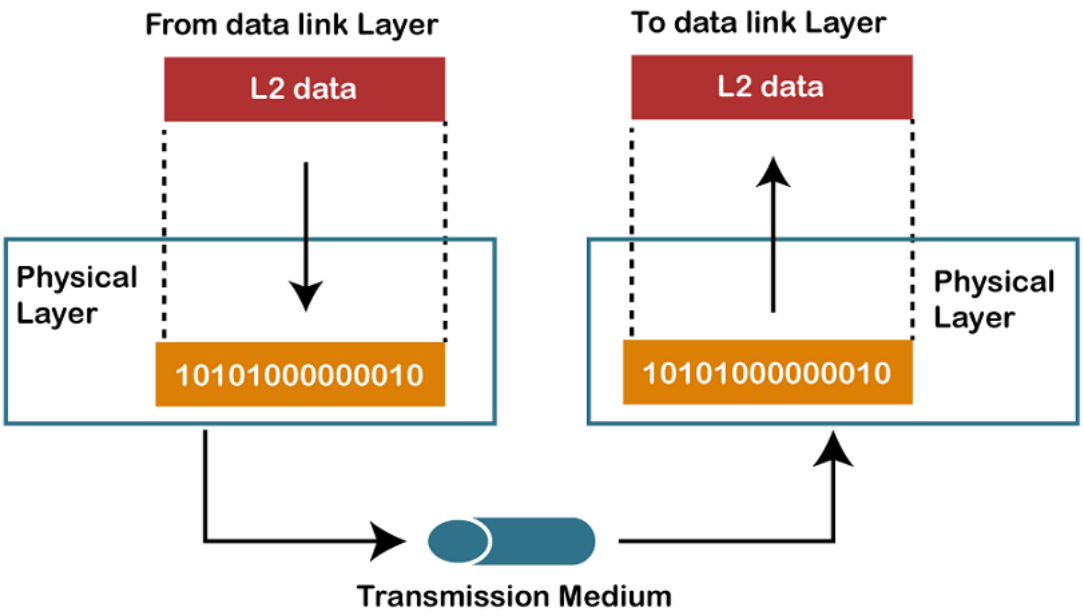
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer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

7 Layers of OSI Model

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

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

1) Physical layer

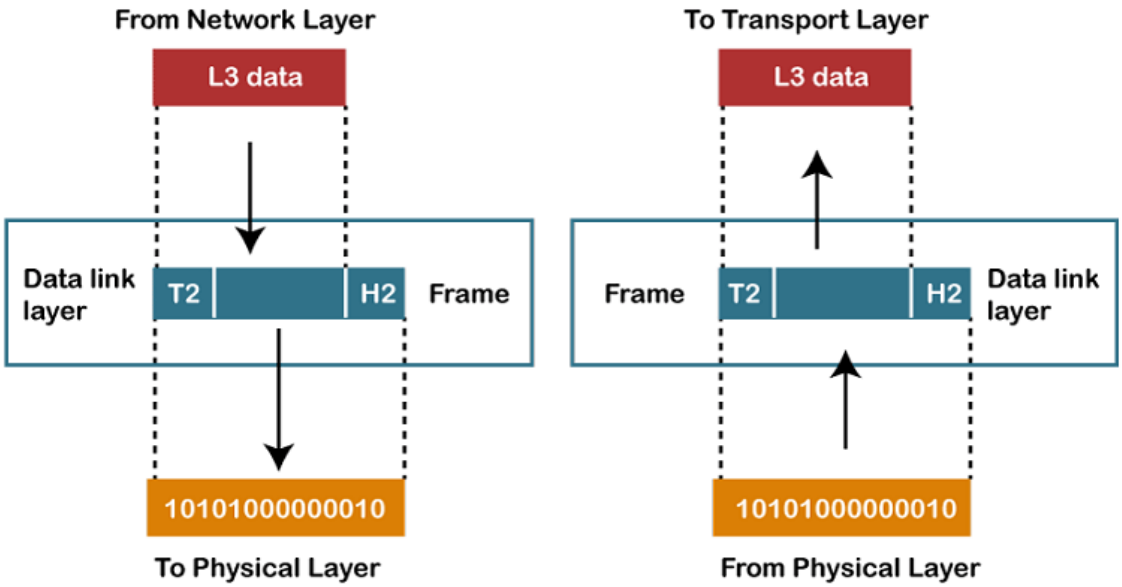


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

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

2) Data-Link Layer



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

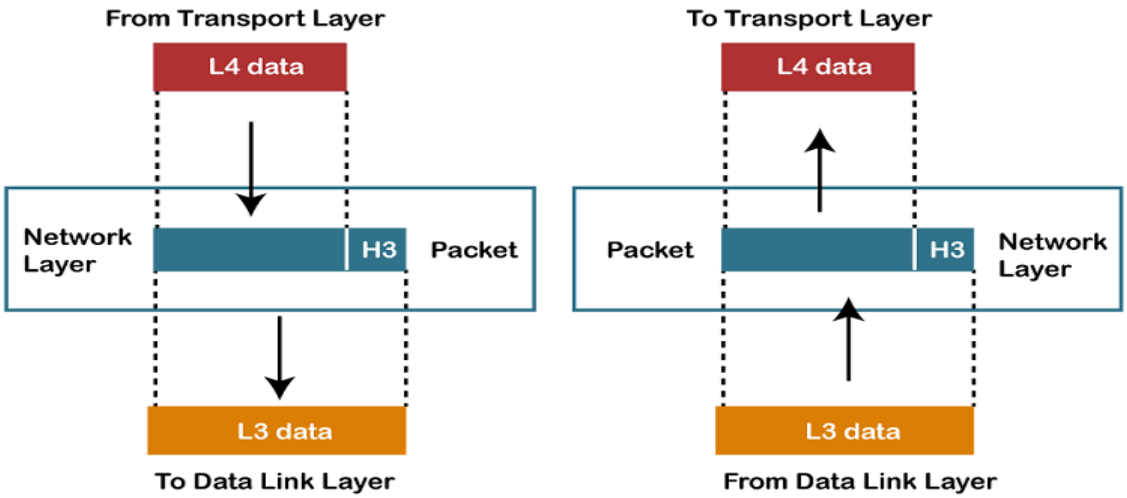
Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame.

The header which is added to the frame contains the hardware destination and source address.

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

3) Network Layer

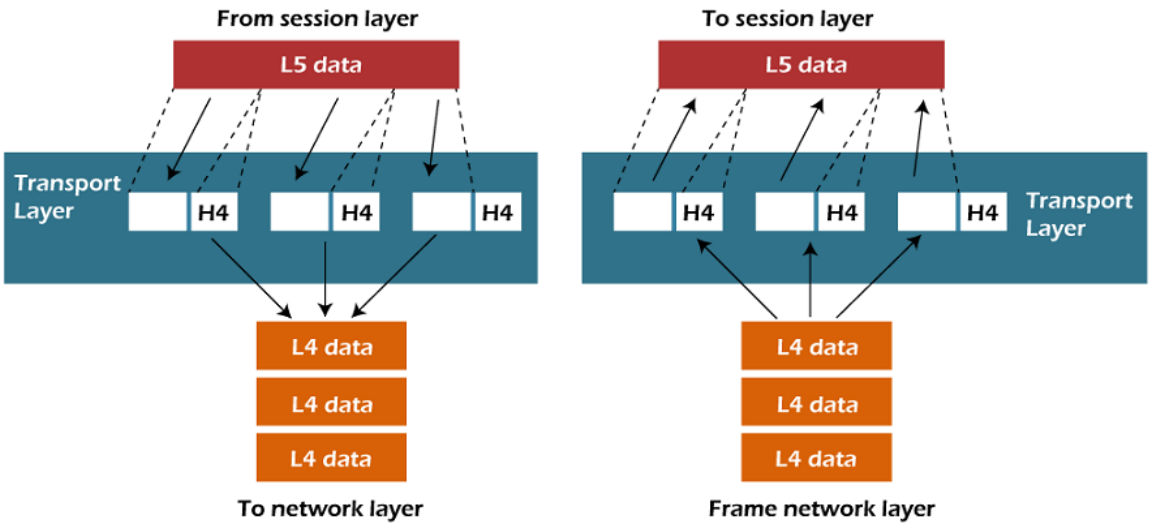


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and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

Functions of Network Layer:

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

4) Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.

- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

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

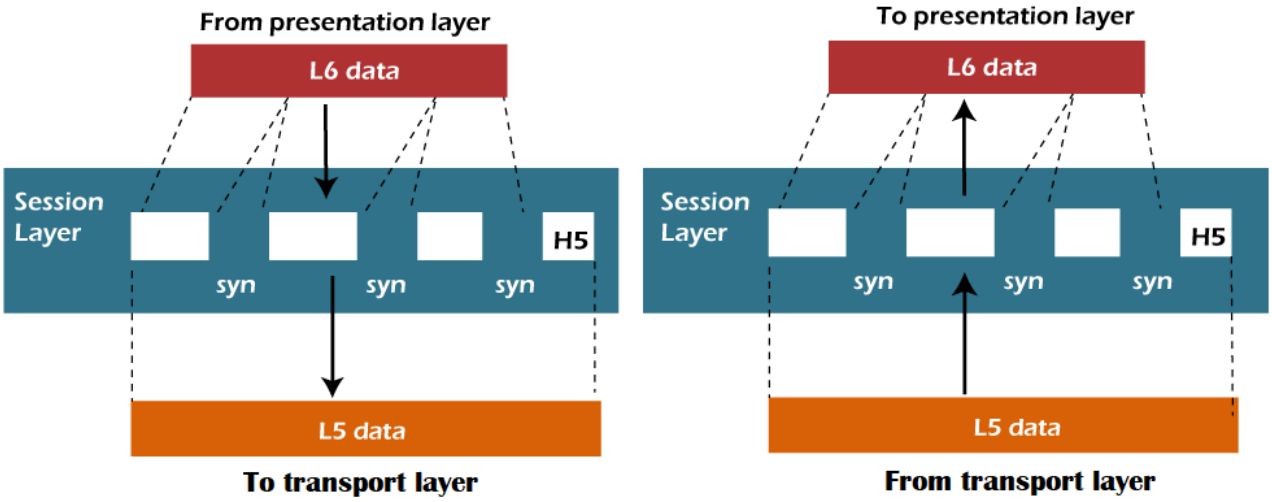
Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each

segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5) Session Layer



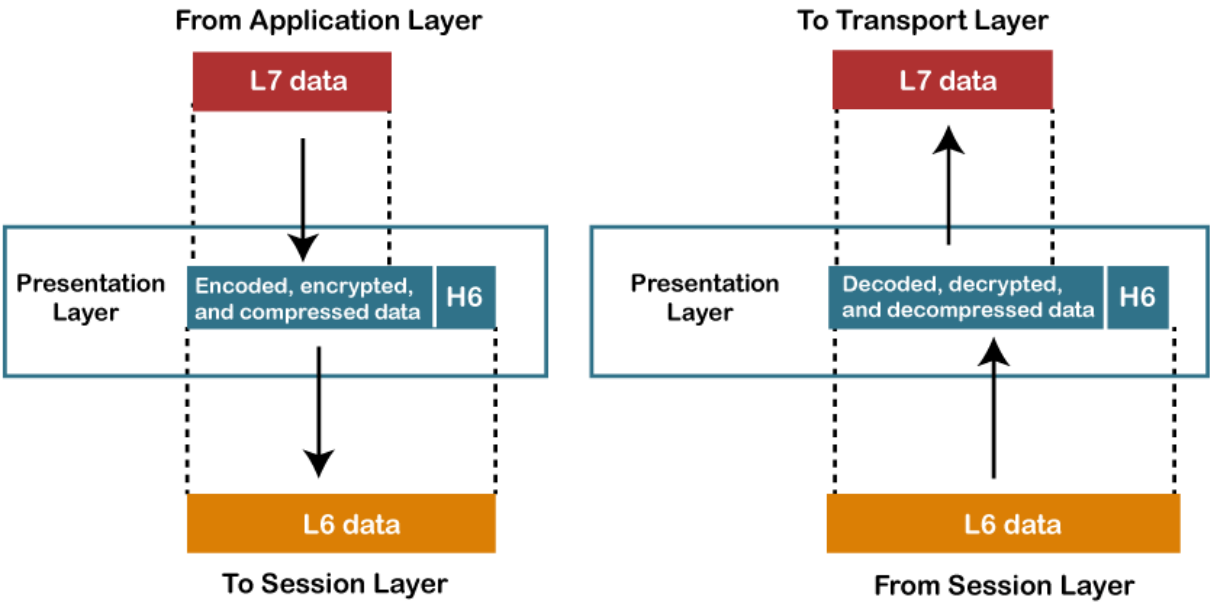
- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6) Presentation Layer



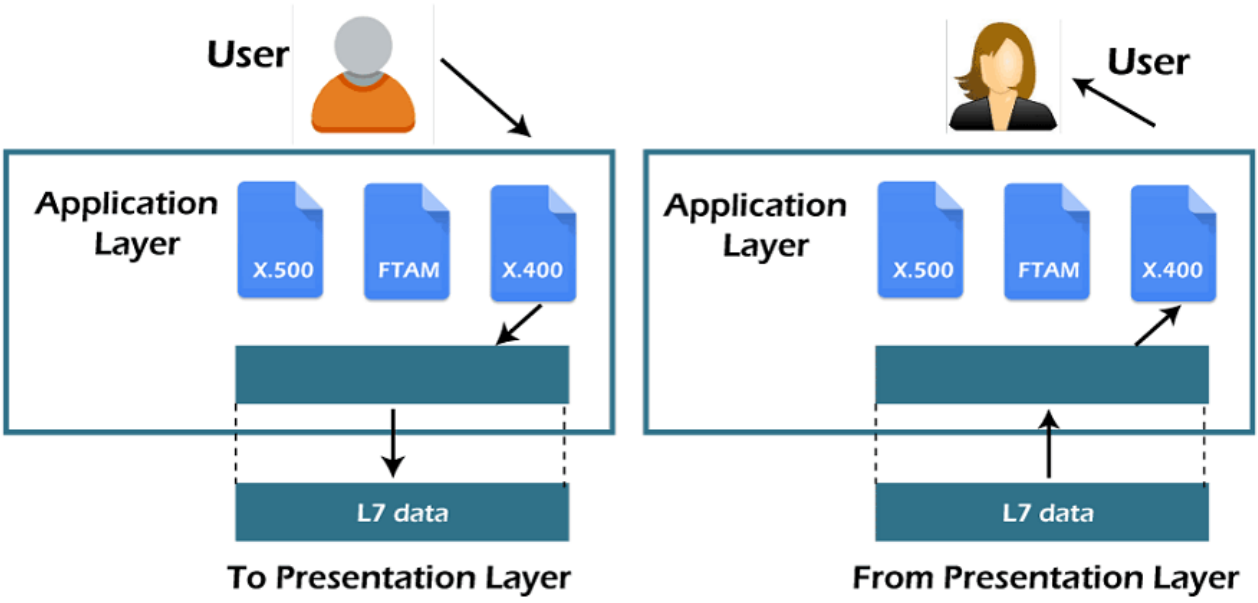
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation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

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

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

7) Application Layer



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

Functions of Application layer:

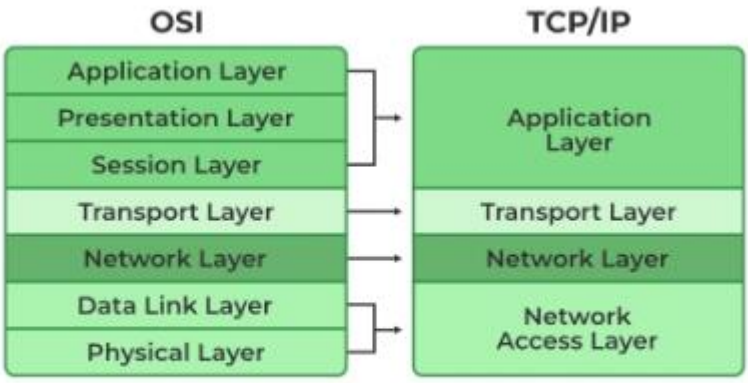
- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.

- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP model

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

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



TCP/IP and OSI

1. Network Access Layer

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

The packet's network protocol type, in this case, TCP/IP, is identified by network access layer. Error prevention and "framing" are also provided by this layer. Point-to-

Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

2. Internet Layer

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

- **IP:** IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
- **ICMP:** ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP:** ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.

The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet. The Internet Layer is responsible for routing packets of data from one device to another across a network. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.

Example: Imagine that you are using a computer to send an email to a friend. When you click "send," the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend's computer can reassemble them into the original email message.

In this example, the Internet Layer plays a crucial role in delivering the email from your computer to your friend's computer. It uses IP addresses and routing tables to determine the best route for the packets to take, and it ensures that the packets are delivered to the correct destination. Without the Internet Layer, it would not be possible to send data across the Internet.

3. Transport Layer

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

- **TCP:** Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.
- **UDP:** The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

4. Application Layer

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

- **HTTP and HTTPS:** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
- **SSH:** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
- **NTP:** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

Overview of 5G Technology

5G (Fifth Generation) is the latest generation of mobile network technology, designed to significantly enhance the speed, coverage, and responsiveness of wireless networks. It is set to enable a new kind of network that is designed to connect virtually everyone and everything together, including machines, objects, and devices.

Key Features of 5G

1. **Faster Speeds**:
    - 5G networks are expected to be up to 100 times faster than 4G.
    - Download speeds can reach up to 10 Gbps.
2. **Lower Latency**:
    - Latency refers to the delay before a transfer of data begins following an instruction.
    - 5G aims to reduce latency to as low as 1 millisecond, making real-time communication possible.
3. **Increased Capacity**:
    - 5G networks can handle a significantly larger number of devices simultaneously compared to previous generations.
    - This is crucial for the Internet of Things (IoT), where numerous devices need to communicate with each other.
4. **Improved Reliability**:
    - Enhanced reliability and reduced packet loss.
    - Essential for critical applications like remote surgery or autonomous driving.

5. **Energy Efficiency**:
    - More efficient use of the spectrum and lower energy consumption per bit.

Evolution from Previous Generations

1G (First Generation)

- **Introduction**: Launched in the 1980s.
- **Technology**: Analog signal.
- **Features**: Basic voice communication.
- **Limitations**: Poor quality, lack of security, and no data services.

2G (Second Generation)

- **Introduction**: Launched in the early 1990s.
- **Technology**: Digital signal (GSM, CDMA).
- **Features**: Enhanced voice quality, SMS, and basic data services (MMS).
- **Improvements**: Improved security and reduced eavesdropping.

3G (Third Generation)

- **Introduction**: Early 2000s.
- **Technology**: WCDMA, HSPA.
- **Features**: Higher data speeds (up to 2 Mbps), video calling, and mobile internet.
- **Improvements**: Enhanced mobile browsing and streaming.

4G (Fourth Generation)

- **Introduction**: Late 2000s.
- **Technology**: LTE (Long Term Evolution).
- **Features**: High-speed internet (up to 1 Gbps), HD streaming, online gaming, and VoIP.
- **Improvements**: Significant improvement in data speeds and network efficiency.

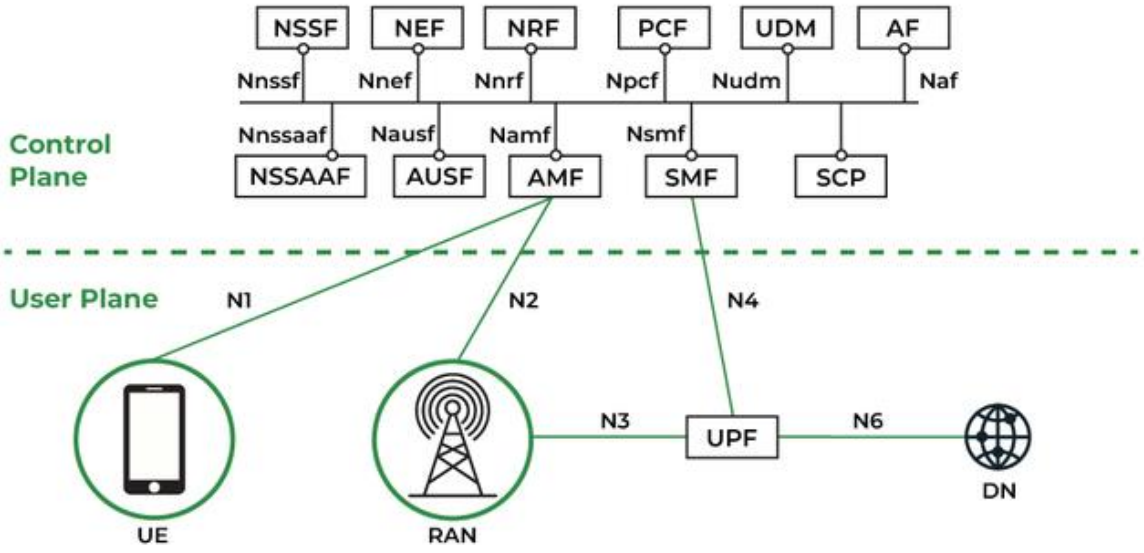
5G Compared to 4G

1. **Speed**: 5G is significantly faster than 4G, enabling quicker downloads and smoother streaming.
2. **Latency**: 5G offers much lower latency, which is critical for applications requiring real-time feedback.
3. **Capacity**: 5G supports more connected devices per unit area than 4G, which is vital for the IoT.
4. **Reliability**: 5G provides more reliable connections, making it suitable for mission-critical services.

Potential Applications of 5G

1. **Enhanced Mobile Broadband (eMBB)**: Ultra-fast internet for mobile devices.
2. **Massive IoT**: Connecting billions of devices efficiently.
3. **Ultra-Reliable Low-Latency Communication (URLLC)**: Critical applications like autonomous vehicles, remote surgery, and industrial automation.
4. **Smart Cities**: Improved connectivity for public services, traffic management, and utilities.
5. **Virtual and Augmented Reality (VR/AR)**: Immersive experiences with low latency and high bandwidth.

Core network architecture in 5G.



Functions of 5G network:

1. **NRF(Network Repository Function):** All of the 5G network functions (NFs) in the operator's network are stored centrally in the Network Repository Function (NRF). The NRF provides a standards-based API that enables 5G NFs to register and find one another. A crucial element needed to execute the new service-based architecture (SBA) in the 5G core is NRF.
2. **PCF (Policy Control Function):** Policy Control Function makes it simple to develop and implement policies in a 5G network. PCF will help you monetize and reap the rewards of 5G because it was created and designed using cloud-native principles to address the demands of 5G services.
3. **BSF (Binding Support Function):** The Session Binding Function on the Diameter Routing Agent (DRA) used in 4G is comparable to the 5G Binding Support Function (BSF). When numerous Policy Control Function (PCF) systems are installed in the network, it becomes a necessary necessity.
4. **SCP (Service Communication Proxy):** By granting routing control, resiliency, and observability to the core network, Service Communication Proxy (SCP) enable operators to securely and effectively operate their 5G network. To address many of

the issues brought on by the new service-based architecture (SBA) in the 5G core, SCP makes advantage of IT service mesh (ISTIO) and adds crucial capabilities to make it 5G-aware.

5. **NSSF (Network Slicing Selection Function):** In the 5G environment, where a variety of services are offered, the NSSF (Network Slicing Selection Function) system is a solution to choose the best network slice available for the service requested by the user.
6. **UDM (Unified Data Management) & UDR (User Data Repository):** UDM is cloud-native and created for 5G, similar to Home Subscriber Server (HSS) in LTE. It is in charge of creating the credentials needed for authentication, granting access depending on user subscription, and sending those credentials to the other network functions. It retrieves the credentials from the User Data Repository (UDR). Different key 5G features are supported by the UDM network function. In order to complete the authentication process, it creates authentication credentials. Based on user subscriptions, it approves network access and roaming.
7. **AUSF (Authentication Server Function):** 5G authentication and Key Agreement method 5G AKA are carried out via the authentication server function. In order to manage hidden or privacy-protected subscription identifiers, AUSF also provides additional functionality. During the registration process, AMF(Access and Mobility Function) is in charge of choosing the proper Authentication Server Function (AUSF).
8. **NWDAF (Network Data Analytics Function):** The 5G Network Data Analytics Function (NWDAF) is intended to improve the end-user experience by streamlining the production and consumption of key network data as well as generating insights and taking appropriate action. By expediting the production and consumption of core network data, creating insights, and acting on these insights, NWDAF is intended to address market fragmentation and proprietary solutions in the field of network analytics.

Functions of 5G Network Explained Simply

1. **NRF (Network Repository Function)**
   - **What It Does:** Stores information about all the 5G network functions (NFs) in one central place.
   - **Why It's Important:** Helps different parts of the network find and communicate with each other.
2. **PCF (Policy Control Function)**
   - **What It Does:** Manages and enforces policies in the 5G network.
   - **Why It's Important:** Ensures efficient and effective use of the network, and helps monetize 5G services.
3. **BSF (Binding Support Function)**
   - **What It Does:** Supports session management by linking multiple Policy Control Functions (PCFs).
   - **Why It's Important:** Essential when there are several PCFs in the network to ensure smooth operation.
4. **SCP (Service Communication Proxy)**
   - **What It Does:** Controls routing, provides resiliency, and offers visibility into the network.

- **Why It's Important:** Helps operators manage and secure the 5G network more effectively.

5. **NSSF (Network Slicing Selection Function)**
   - **What It Does:** Chooses the best network slice for a specific service request.
   - **Why It's Important:** Ensures that each service gets the optimal resources it needs.
6. **UDM (Unified Data Management) & UDR (User Data Repository)**
   - **What They Do:** Manage user credentials and subscription information.
   - **Why They're Important:** Control network access and authenticate users, ensuring only authorized users can connect.
7. **AUSF (Authentication Server Function)**
   - **What It Does:** Handles user authentication and security.
   - **Why It's Important:** Ensures secure access to the network and protects user identity.
8. **NWDAF (Network Data Analytics Function)**
   - **What It Does:** Analyzes network data to improve performance and user experience.
   - **Why It's Important:** Helps operators make informed decisions based on insights from network data.