COMPUTER NETWORKS

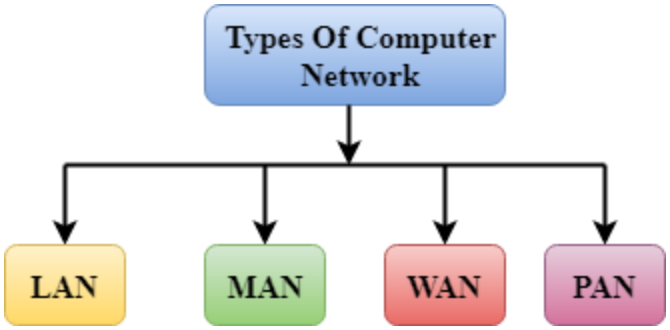
Define Network?

Ans:A network is a **set of devices** that are connected with **a physical media link.** In a network, **two or more nodes are connected** by a **physical link** or two or more networks are connected by one or more nodes. A network is a collection of devices **connected to each other to allow the sharing of data.**

A node can be a **computer, printer, or any other device capable of sending or receiving the data**. The links connecting the nodes are known as communication channels.

Types of Network?

- Networks can be divided on the basis of area of distribution.

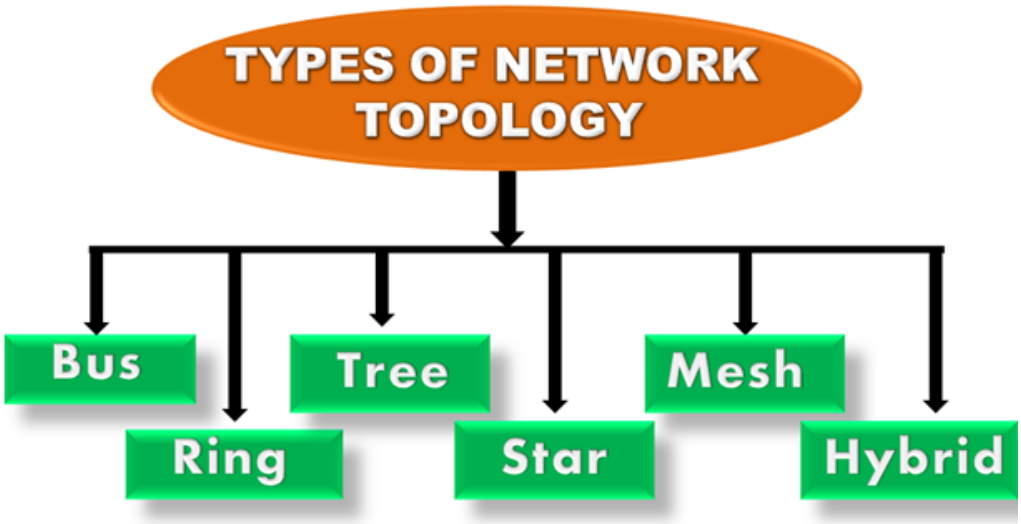


- **LAN (Local Area Network):** It is used for a small geographical location like office, hospital, school, etc.

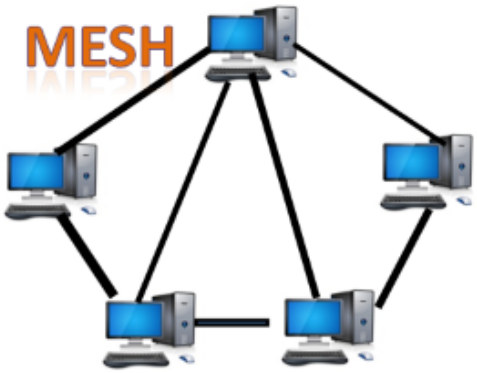
- **PAN (Personal Area Network):** Its range limit is up to 10 meters. It is created for personal use. Generally, personal devices are connected to this network. For example computers, telephones, fax, printers, etc.
- **MAN (Metropolitan Area Network):** It is used to connect the devices which span to large cities like metropolitan cities over a wide geographical area.
- **WAN (Wide Area Network):** It is used over a wide geographical location that may range to connect cities and countries.

Topology:

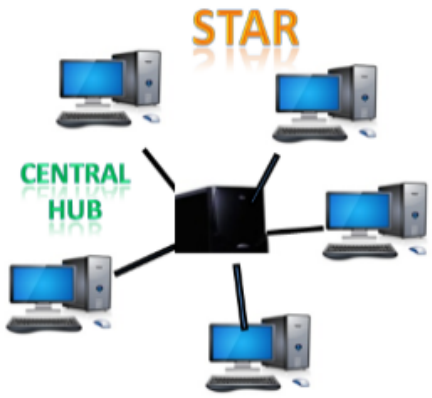
Topology defines the **structure of the network** of how **all the components are interconnected to each other.**



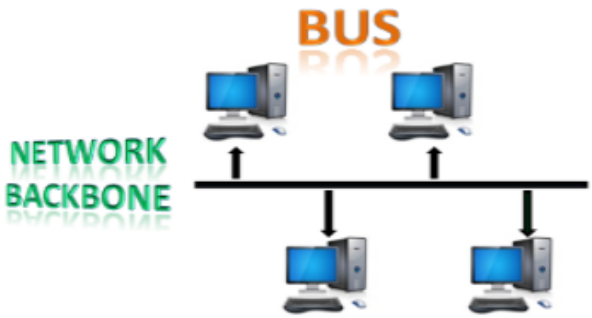
Mesh Topology:



Star Topology:

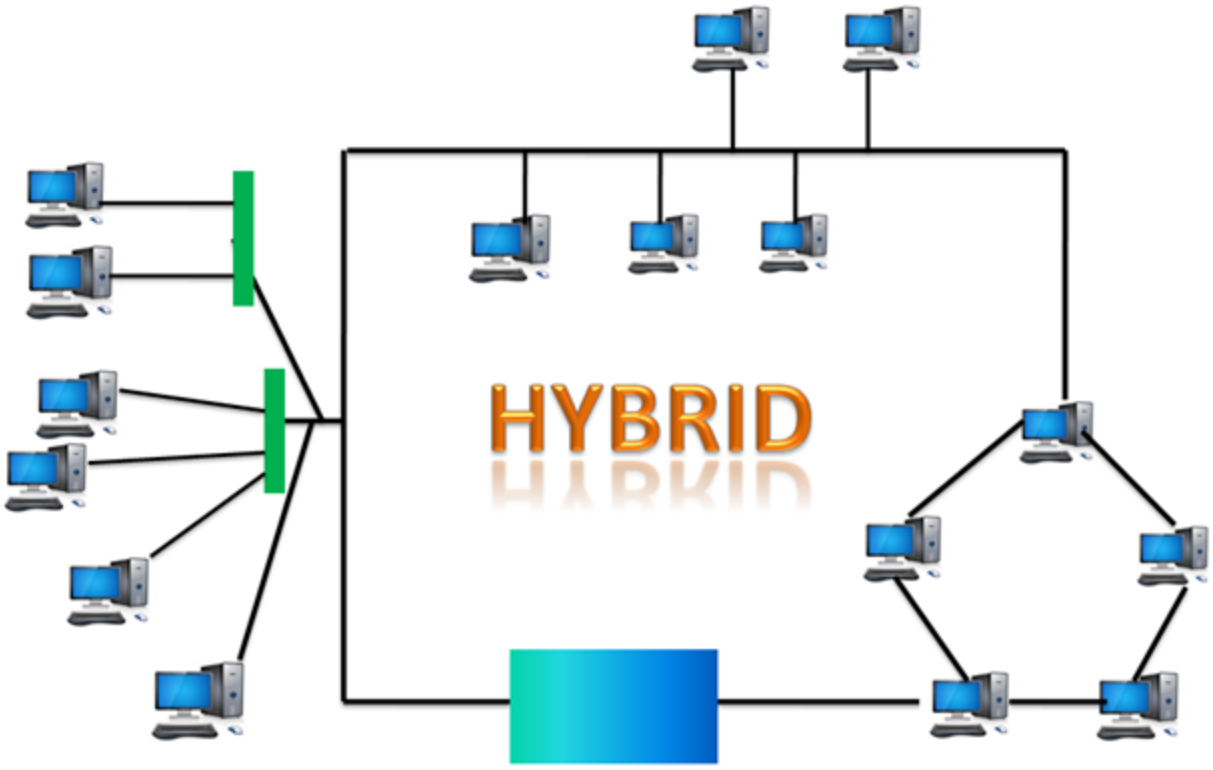


Bus Topology



Ring Topology:

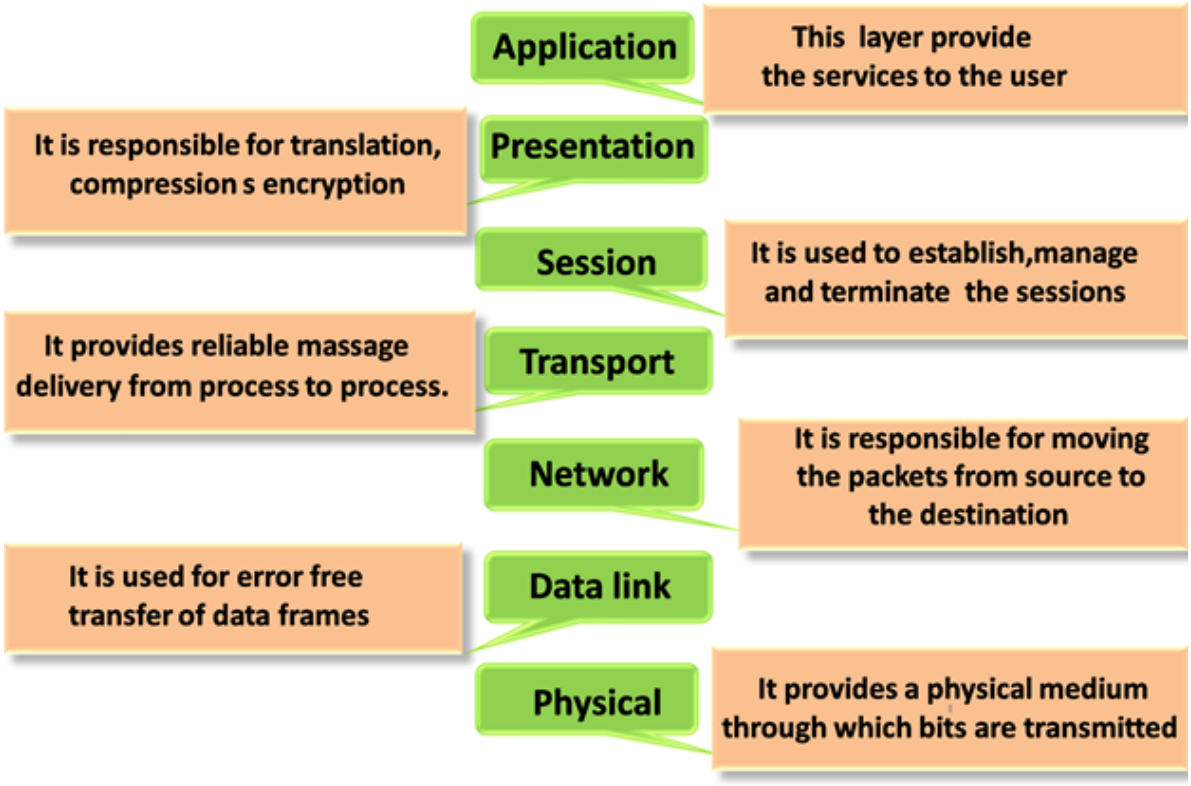
Hybrid Topology:



OSI Model(open system interconnection):

It is a **network architecture model** based on the ISO standards. It is called **the OSI model** as it deals with **connecting the systems that are open for communication with other systems.**
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**.

The **OSI model has seven layers.**



Physical Layer:

● It is the **lowest layer of the OSI** reference model.
●It is used for the **transmission of an unstructured raw bit stream over a physical medium.**
● Physical layer transmits the **data either in the form of electrical/optical or mechanical form.**
● The physical layer is mainly used for the **physical connection between the devices,** and such physical connection can be made by using **twisted-pair cable, fibre-optic or wireless transmission media.**
network hubs, cabling, repeaters, network adapters or modems.

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 i**t 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 t**he type of the signal used for transmitting the information.**

DataLink Layer:

- Last **Second Layer**,it is between **the network and physical layer.**
- It is used for **transferring the data** from **one node to another node.**
- It receives the **data from the network layer** and **converts the data into data frames** and then **attaches the physical address to these frames** which are **sent to the physical layer.**
- It enables the **error-free transfer of data from one node to another node.**

Functions of Data-link layer:

● **Frame synchronization:** Data-link layer **converts the data into frames**, and it ensures that the destination must **recognize the starting and ending of each frame.**

● **Flow control:** Data-link layer **controls the data flow** within the network.

● **Error control:** It **detects and corrects the error** occurred during the **transmission from source to destination**.

● **Addressing:** Data-link layers attach **the physical address with the data frames** so that the individual machines can be easily identified.

● **Link management:** Data-link layer manages **the initiation, maintenance and termination of the link between the source and destination** for the effective exchange of data.

Network Layer:

The Network Layer is the **third layer of the OSI model.**It handles the **service requests from the transport layer** and further **forwards the service request to the data link layer**.The network layer **translates the logical addresses into physical addresses**

It determines **the route from the source to the destination** and also **manages the traffic problems such as switching, routing and controls the congestion of data packets.**The main role of the network layer is **to move the packets from the sending host to the receiving host.**

Functions of Network Layer:

i)Internet Networking: An internetworking is the **main responsibility of the network layer**. It provides a **logical connection between different devices.**

ii)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.

iii)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.

iv)Packetizing: The process of **encapsulating the data received from upper layers of the network(also called as payload) in a network layer packet at the source** and **decapsulating the payload from the network layer packet at the destination** is known as packetizing.

Problems with classful addressing:

i) Wastage of IP addresses
ii) Maintenance is time consuming
iii)More prone to errors
iv)Flexibility issue

Classless Addressing:

Q)What is Bandwidth?

Ans: Every signal has a **limit of upper range frequency and lower range frequency.** The range of the limit of a network between **its upper and lower frequency is called bandwidth**.

Q)What is Node and Link?

Ans: A network is a **connection setup of two or more computers directly connected by some physical mediums like optical fiber or coaxial cable**. This **physical medium of connection is known as a link**, and **the computers that it is connected to** are known as nodes.

Q)Gateway and Difference between gateway and Routers?

Ans: **A node** that is **connected to two or more networks is** commonly **known as a gateway**. It is also known **as a router.** It is used to **forward messages from one network to another**. Both the gateway and router **regulate the traffic in the network**. A router is a networking device that **forwards the packet based on the information** available in the **packet header and forwarding table.**

Differences between gateway and router:

A r**outer sends the data between two similar networks** while **gateway sends the data between two dissimilar networks**.

Q)What is Routing?(physical,data link,network layer)

Ans: A Router is a process of **selecting a path along which the data can be transferred from source to the destination**. Routing is performed by a special device known as a **router**.A Router works at the **network layer in the OSI model and internet layer in TCP/IP model**

- The routing algorithms are used for **routing the packets**. The routing algorithm is nothing but a software responsible for **deciding the optimal path through which a packet can be transmitted.**
- The routing algorithm **initializes and maintains the routing table for the process** of path determination.

Things for optimal paths:Hop Count,Delay,Bandwidth,Load,Reliability.

Types of Routing:

i)Static Routing: It is a technique in which the **administrator manually adds the routes in a routing table.**

ii)Default Routing: Default Routing is a technique in **which a router is configured to send all the packets to the same hop device,** and **it doesn't matter whether it belongs to a particular network or not.** A Packet is transmitted to the device for which it is configured in default routing.

iii)Dynamic Routing: Dynamic protocols are used to **discover the new routes to reach the destination**.

Q)What Does Ping Command Do?

Ans: The "ping" is a utility program that **allows you to check the connectivity between the network devices**. You can **ping devices using its IP address or name.**

Q) What is a NIC(Network interface card)?

- NIC stands for **Network Interface Card.** It is a **peripheral card attached to the PC to connect to a network**. Every **NIC has its own MAC address** that identifies the PC on the network.
- It provides a **wireless connection to a local area network.**
- NICs were mainly used in **desktop computers.**

Q)What is an IP?

Ans: IP stands for **internet protocol.** It is a **protocol defined in the TCP/IP model used for sending the packets from source to destination**. The main task of IP is to deliver the **packets from source to the destination based on the IP addresses available in the packet headers**. IP defines **the packet structure that hides the data which is to be delivered as well as the addressing method** that labels the datagram with a source and destination information.

An IP protocol provides **the connectionless service,** which is accompanied by **two transport protocols, i.e., TCP/IP and UDP/IP**, so the internet protocol is also known as TCP/IP or UDP/IP.

Function: The **main function of the internet protocol** is to **provide addressing to the hosts,** e**ncapsulating the data into a packet structur**e, and **routing the data from source to the destination across one or more IP networks.** In order to achieve these functionalities, internet protocol provides two major things which are given below.

An internet protocol defines two things:

- **Format of IP packet**
- **IP Addressing system**

Q)What is IP Addressing?

Ans: An IP address is a **unique identifier assigned to the computer which is connected to the internet**. Each IP address consists of a series of characters like 192.168.1.2. **Users cannot access the domain name of each website with the help of these characters**, so DNS resolvers are used to convert the human-readable domain names into a series of characters. **Each IP packet contains two addresses**, i.e., the **IP address of the device,** which is sending the packet, and the **IP address of the device which is receiving the packet.**

Types of IP Addressing:

1)Public Address: The public address is also known **as an external address as they are grouped under the WAN addresses**. We can also define the **public address as a way to communicate outside the network**. This address is used to **access the internet.** The public address available on our computer provides remote access to our computer. With the help of a **public address, we can set up the home server to access the internet.** This address is generally assigned by the ISP (Internet Service Provider).

Key points related to public address are:

- The scope of the **public address is global**, which means **that we can communicate outside the network.**
- This address is assigned by the **ISP (Internet Service Provider).**
- It is **not available at free of cost.**

2) Private Address: A private address is also known **as an internal address, as it is grouped under the LAN addresses.** It is used to **communicate within the network.** These addresses are **not routed on the internet so that no traffic can come from the internet to this private address.** The address space for the private address is a**llocated using InterNIC to create our own network**. The private addresses are a**ssigned mainly to those computers, printers, smartphones, which are kept inside the home** or the computers that are kept within the organization.

Key points related to private addresses are:

- Its scope is local, as **we can communicate within the network only.**
- It is generally used for **creating a local area network.**
- It is available at **free of cost.**
- We can get to know the **private IP address by simply typing the "ipconfig"** on the command prompt.

Q)What is a MAC Address?

Ans: Part of the **data link layer** stands for **multiple access protocol**.

- MAC address is **the physical address,** which **uniquely identifies each device on a given network**. To make **communication between two networked devices**, we need two addresses: **IP address and MAC address.** It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.
- It is **globally unique;** it means **two devices cannot have the same MAC address.** It is represented in a **hexadecimal format** on each device, such as **00:0a:95:9d:67:16.**
- It is provided **by the device's vendor at the time** of manufacturing and **embedded in its NIC**, which ideally cannot be changed.

Types of MAC Address:

1)Unicast Mac address: If the LSB (least significant bit) of the **first octet of an address is set to zero**, the frame is meant to reach **only one destination NIC**.

2)Multicast Mac address: LSB (least significant bit) or **first 3 bytes of the first octet of an address** is set to **one and reserved for the multicast addresses.**

3)Broadcast Mac address: Ethernet frames with **ones in all bits of the destination address (FF-FF-FF-FF-FF-FF)** are known as a broadcast address

MAC address	IP address
It stands for Media Access Control.	It stands for Internet Protocol.
It is the unique address provided by the manufacturer.	It is the logical address provided by the ISP or Internet Service Provider.
It is the physical address of the device's NIC that is used to identify a device within a network.	It is the logical address that identifies a network or device on the internet.
It operates on the data link layer.	It operates on a network Layer.
It is the 6 -bytes hexadecimal address.	It is of 4 bytes for IPv4 and 8 bytes for IPv6 addresses.

The main difference between MAC and IP address: MAC Address is used to ensure the **physical address of a computer**. It uniquely **identifies the devices on a network**. While IP addresses are used to **uniquely identify the connection of a network** with that device taking part in a network.

Difference between IPv4 vs IPv6?

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.

Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

Q)What is a subnet?

Ans: **Dividing the big network** into the **small network**.A subnet is **a network inside a network** achieved by the **process called subnetting** which helps divide a **network into subnets.**
It is used for getting a **higher routing efficiency** and **enhances the security of the network.**
It **reduces the time to extract the host address from the routing table**.

Q)What is Supernet?

Ans: Supernetting is the **opposite of Subnetting.** In subnetting, **a single big network is divided into multiple smaller subnetworks**. In Supernetting, multiple networks are **combined into a bigger network termed as a Supernetwork or Supernet.**

There are some points which should be kept in mind while supernetting:

- **All the Networks should be contiguous.**
- The block size of **every network should be equal** and **must be in the form of 2^n.**
- **First Network id should be exactly divisible by the whole size of the supernet.**

Advantages of Supernetting –Control and reduce network traffic,**Minimize the routing table**

Q)What is a firewall?

Ans: The firewall is **a network security system** that is used to **monitor the incoming and outgoing traffic** and **blocks the same based on the firewall security policies**.
It acts as a **wall between the internet (public network)** and the **networking devices (a private network).**
It is either a hardware device, software program, or a combination of both.
It **adds a layer of security to the network**.its acts as a boundary

Q)Packet filtering firewall?(layer-4)

Ans: check IP header,TCP header,
works on the network and transport layer.
can block Ip address,full networks.
Can block a service(http,ftp)

Q)What is the Application Gateway(Proxy firewall)?(layer-5)

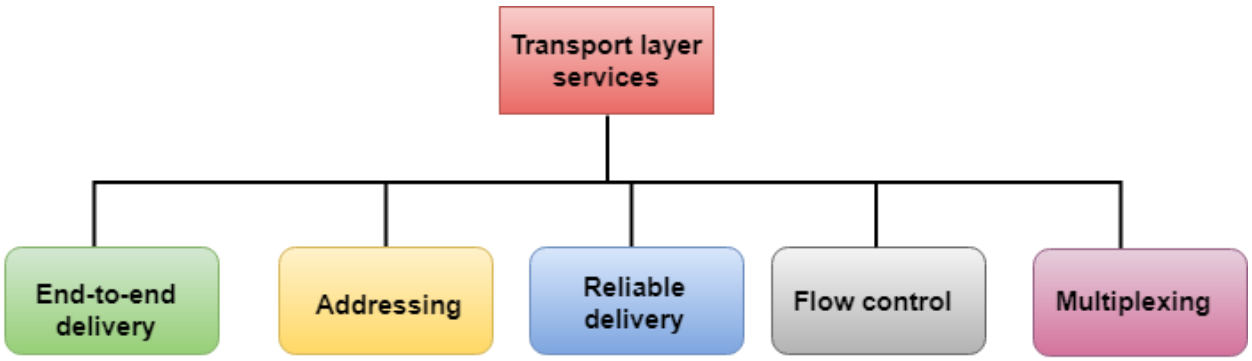
Ans: User authentication

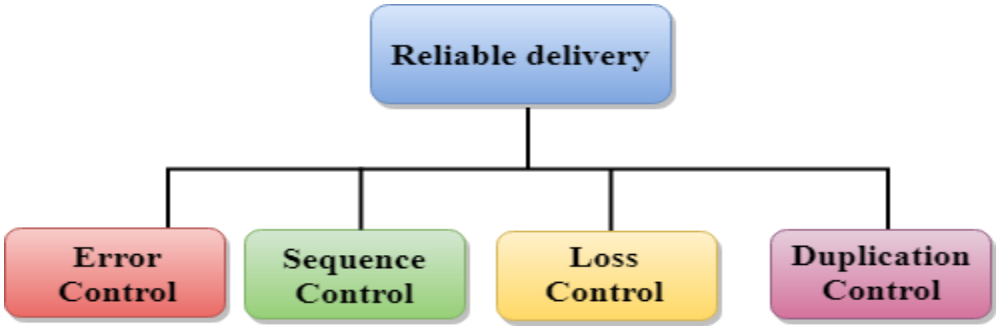
Q) What is a proxy server?

Ans:

Transport Layer:

The transport layer is a **4th layer from the top**.The main role of the transport layer is to **provide the communication services directly to the application processes running on different host**.A computer network provides more than **one protocol to the network applications. For example, TCP and UDP** are two transport layer protocols **that provide a different set of services to the network laye**r.All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as **reliable data transfer, bandwidth guarantees, and delay guarantees.**





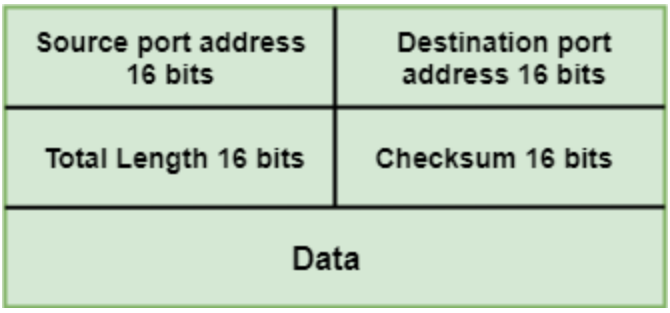
Multiplexing: The transport layer uses the **multiplexing to improve transmission efficiency.**

i) Upward Multiplexing: Upward multiplexing means **multiple transport layer connections use the same network connection**.

ii)Downward Multiplexing: Downward multiplexing means **one transport layer connection uses multiple network connections**.

Transport Layer protocol: TCP and UDP

UDP(User datagram protocol): UDP stands for **User Datagram Protocol**.UDP is a **simple protocol and it provides nonsequenced transport** functionality.UDP is a c**onnectionless protocol.**This type of protocol is used **when reliability and security are less important than speed and size.**



Disadvantage: UDP can discover **that an error has occurred,** but it d**oes not specify which packet has been lost** as **it does not contain an ID or sequencing number** of a particular data segment.

TCP(Transmission control protocol)

Session Layer:

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

Functions:

1)Authentication

2)Authorization

3)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.

4)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 t**ake place again from the checkpoint.** This process is known as **Synchronization and recovery.**

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:

i)Translation: **Different computers use 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.

ii)Encryption: Encryption is needed to **maintain privacy.** Encryption is a process of **converting the sender-transmitted information into another form** and **sending the resulting message over the network**.

iii)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, and video.**

Application Layer:

The **application layer in the OSI mode**l is the **closest layer to the end user** which means that **the application layer and end user can interact directly with the software application.** The application layer is **present at the top of the OSI model**. It is the **layer through which users interact.**

Functions:

i)Identifying Communication partners.
ii)determine resource availability.
iii)Synchronizing Communication.

Application architecture is of two types:

i)Client-Server Architecture: An application program running on the **local machine sends a request to another application program is known as a clien**t, and a program that **serves a request is known as a server.**In Client-server architecture, **clients do not directly communicate with each other**.

ii)P2P(Peer to peer) Architecture: The peers **communicate with each other without passing the information through a dedicated server**, this architecture is known as peer-to-peer architecture. The applications based on P2P architecture includes file sharing and internet telephony.

Application Layer Protocol:

1)TELNET: TELecommunications NETwork. A program that allows a **user to log on to a remote computer.** A popular client-server program Telnet is used to meet such demands.

2)FTP : File Transfer protocol is a **standard internet protocol provided by TCP/IP** used for **transmitting the files from one host to another**.It is mainly used for transferring the **web page files from their creator to the computer that acts as a server for other computers on the internet**.It is also used for **downloading the files** to the computer from other servers.

3)SMTP(Simple mail transfer protocol):

SMTP is a set of **communication guidelines that allow software to transmit an electronic mail** over the internet.It is a program used for **sending messages to other computer users based on e-mail addresses.**

4)SNMP : It stands for **Simple Network Management Protocol**.SNMP is a framework **used for managing devices on the internet**.It provides a set of operations for **monitoring and managing the internet.**

5) HTTP : HTTP stands for **HyperText Transfer Protocol.**It is a protocol used to **access the data on the World Wide Web (www)**.The HTTP protocol can be used to **transfer the data in the form of plain text, hypertext, audio, video,** and so on.

Features of HTTP:

i)Connectionless Protocol
ii)Media independent
iii)Stateless

6)DNS(Domain Name System): It is a **naming system** for **all the resources over the internet which includes physical nodes and applications**. It is used to locate **resources easily over a network**.

- DNS is an internet which **maps the domain names to their associated IP addresses.**
- **Without DNS,** users must know **the IP address of the web page that you wanted to access. Works on UDP Protocol.**

Working DNS:If you want to visit the website of "javaTpoint", then the user will type "https://www.javatpoint.com" into the **address bar of the web**

browser. Once the domain **name is entered**, then the **domain name system will translate the domain name into the IP address** which can be easily interpreted by the computer. **Using the IP address, the computer can locate the web page requested by the user**.

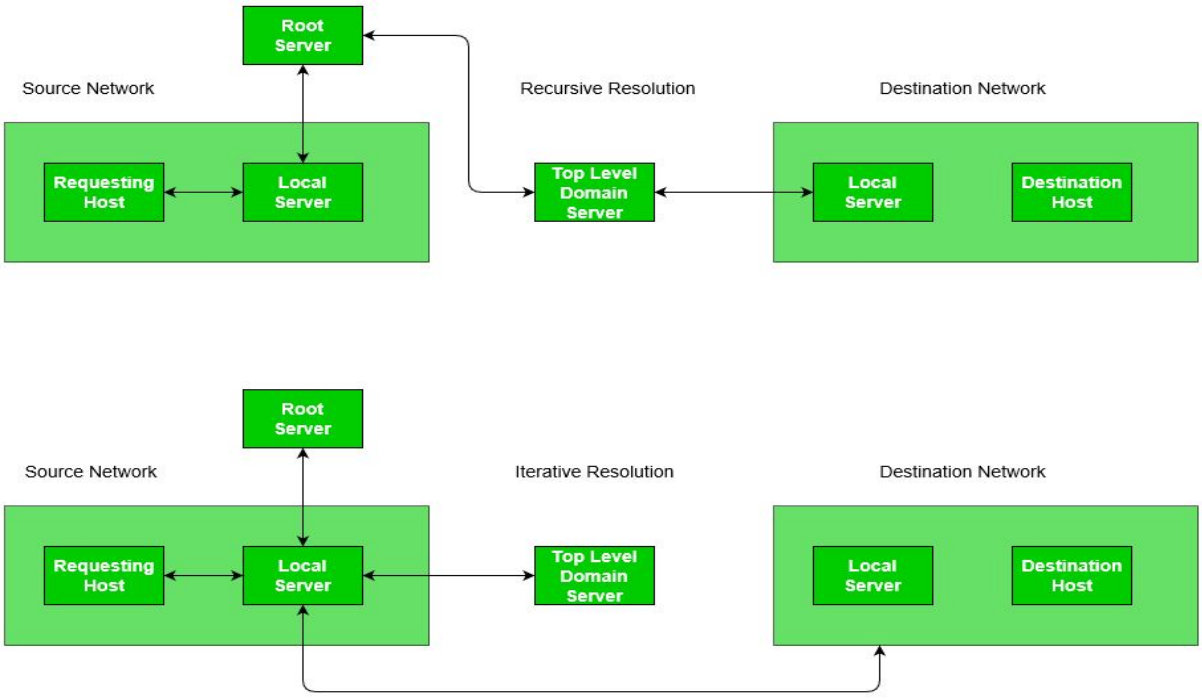
Q)Why does DNS use UDP and not TCP?

Ans:

1) **UDP is much faster.** TCP is slow as **it requires a 3-way handshake**. The load on DNS servers is also an important factor. **DNS servers (since they use UDP) don't have to keep connections**.
2) DNS requests are g**enerally very small and fit well within UDP segments.**

Q) Address Resolution in DNS?

Ans: Iterative and Recursive



Q)Difference b/w http: & https:?

Ans:

- **I**n HTTP, the **URL begins with “http://”** whereas the URL starts with **“https://”**.
- **HTTP uses port number 80** for communication and **HTTPS uses 443**
- HTTP is considered to be **insecure and HTTPS is secure**
- HTTP Works at **Application Layer** and **HTTPS works at Transport Laye**r
- in **HTTP, Encryption is absent** and **Encryption is present in HTTPS**.
- HTTP does not **require any certificates** and HTTPS needs **SSL Certificates**

Q) What happens when you enter “Google.com”?

Ans:

Steps :

● Check the browser cache first if the content is fresh and present in the cache display the same.

● If not, the browser checks if the IP of the URL is present in the cache (browser and OS) if not then requests the OS to do a DNS lookup using UDP to get the corresponding IP address of the URL from the DNS server to establish a new TCP connection.

● A new TCP connection is set between the browser and the server using three-way handshaking.
● An HTTP request is sent to the server using the TCP connection.
● The web servers running on the Servers handle the incoming HTTP request and send the HTTP response.
● The browser processes the HTTP response sent by the server and may close the TCP connection or reuse the same for future requests.
● If the response data is cacheable then browsers cache the same.
● Browser decodes the response and renders the content.

Q)Hub vs Switch?

Ans:

Hub: Hub is a **networking device which is used to transmit the signal to each port (except one port) to respond from which the signal was received**. Hub is operated on a Physical layer. In this packet filtering is not available.

It is of two types: **Active Hub, Passive Hub**.

Switch: Switch is a **network device which is used to enable the connection establishment and connection termination on the basis of need**. Switch is operated on the Data link layer. In this packet filtering is

available. It is a type of full duplex transmission mode and it is also called an efficient bridge.

Q)Different Types of delay?

Ans: The delays, here, means the **time for which the processing of a particular packet takes place.**

1. Transmission Delay:

The time taken to transmit a **packet from the host to the transmission medium** is called Transmission delay.

Let B bps is the bandwidth and L bit is the size of the data then transmission delay is, **`Tt = L/B`**

2.Propagation delay:

After the **packet is transmitted to the transmission medium**, it has to go through the **medium to reach the destination**. Hence the **time taken by the last bit of the packet to reach the destination** is called propagation delay.

```
Tp = Distance / Velocity
```

3 . Queueing delay:

If the packet is **received by the destination**, the **packet will not be processed by the destination immediately**. It has **to wait in a queue in something called a buffer.** So the **amount of time it waits in queue before being processed** is called queueing delay.

4. Processing delay:

Now the **packet will be taken for processing** which is **called processing delay.** Time taken to process the data packet by processor is time required by intermediate routers to decide where to forward the packet, update TTL, perform header checksum calculations.

```
Total = Tt + Tp + Tq + Tpro

Total = Tt+Tp(when taking Tq and Tpro equals to 0)
```