What is a Computer Network?

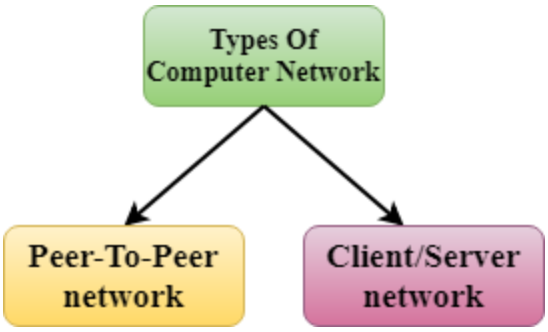
- **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
- The aim of the computer network is the sharing of resources among various devices.
- In the case of computer network technology, there are several types of networks that vary from simple to complex level.

Computer Network Architecture

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

The two types of network architectures are used:

- Peer-To-Peer network
- Client/Server network



Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.

- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

What are the different types of networks?

Networks can be divided on the basis of area of distribution. For example:

- **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.
- **LAN (Local Area Network)**: It is used for a small geographical location like office, hospital, school, etc.
- **HAN (House Area Network)**: It is actually a LAN that is used within a house and used to connect homely devices like personal computers, phones, printers, etc.

- **CAN (Campus Area Network)**: It is a connection of devices within a campus area which links to other departments of the organization within the same campus.
- **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.
- **GAN (Global Area Network)**: It uses satellites to connect devices over global are.

Transmission modes

- The way in which data is transmitted from one device to another device is known as **transmission mode**.
- The transmission mode is also known as the communication mode.
- Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The transmission mode is defined in the physical layer.

The Transmission mode is divided into three categories:

Differences b/w Simplex, Half-duplex and Full-duplex mode

Basis for comparison	Simplex mode	Half-duplex mode	Full-duplex mode
Direction of communication	In simplex mode, the communication is unidirectional.	In half-duplex mode, the communication is bidirectional, but one at a time.	In full-duplex mode, the communication is bidirectional.
Send/Receive	A device can only send the data but cannot receive it or it can only receive the data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
Performance	The performance of half-duplex mode is better than the simplex mode.	The performance of full-duplex mode is better than the half-duplex mode.	The Full-duplex mode has better performance among simplex and half-duplex mode as it doubles the utilization of the capacity of the communication channel.
Example	Examples of Simplex mode are radio, keyboard, and monitor.	Example of half-duplex is Walkie-Talkies.	Example of the Full-duplex mode is a telephone network.

Computer Network Components

Computer network components are the *major parts* which are needed to *install the software*. Some important network components are **NIC**, **switch**, **cable**, **hub**, **router**, and **modem**. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

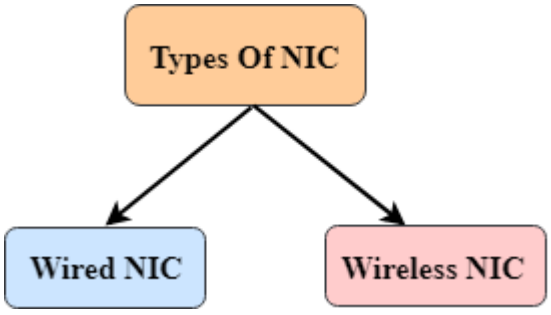
Following are the major components required to install a network:

NIC

- NIC stands for network interface card.
- NIC is a hardware component used to connect a computer with another computer onto a network
- It can support a transfer rate of 10,100 to 1000 Mb/s.
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

There are two types of NIC:

1. Wired NIC
2. Wireless NIC



Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

Wireless NIC: The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

Hub

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switch

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Router

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Advantages Of Router:

- **Security:** The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.
- **Reliability:** If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
- **Performance:** Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic. This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.

Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.

- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

- Standard PC modem or Dial-up modem
- Cellular Modem
- Cable modem

Cables and Connectors

Cable is a transmission media used for transmitting a signal.

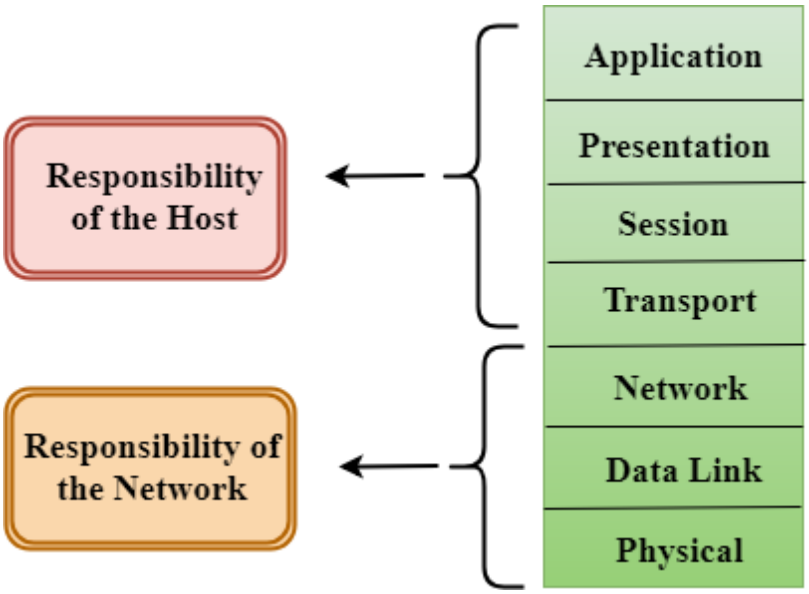
There are three types of cables used in transmission:

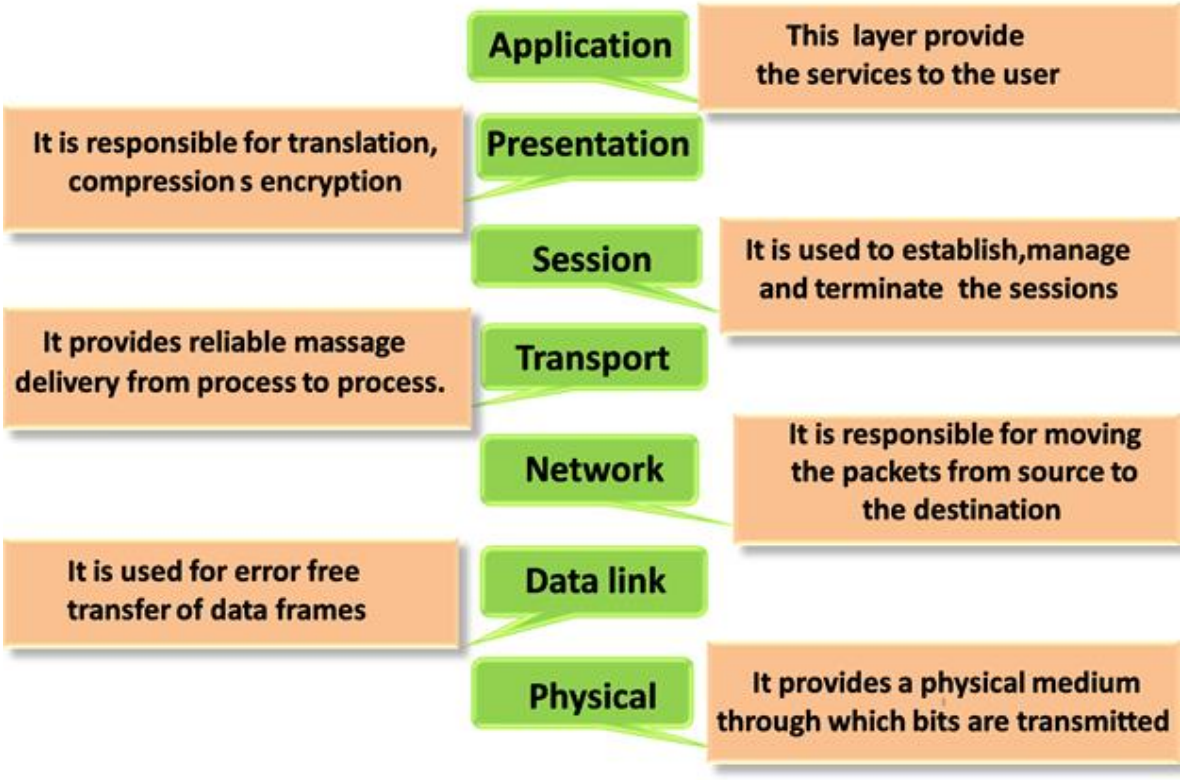
- Twisted pair cable
- Coaxial cable
- Fibre-optic cable

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.

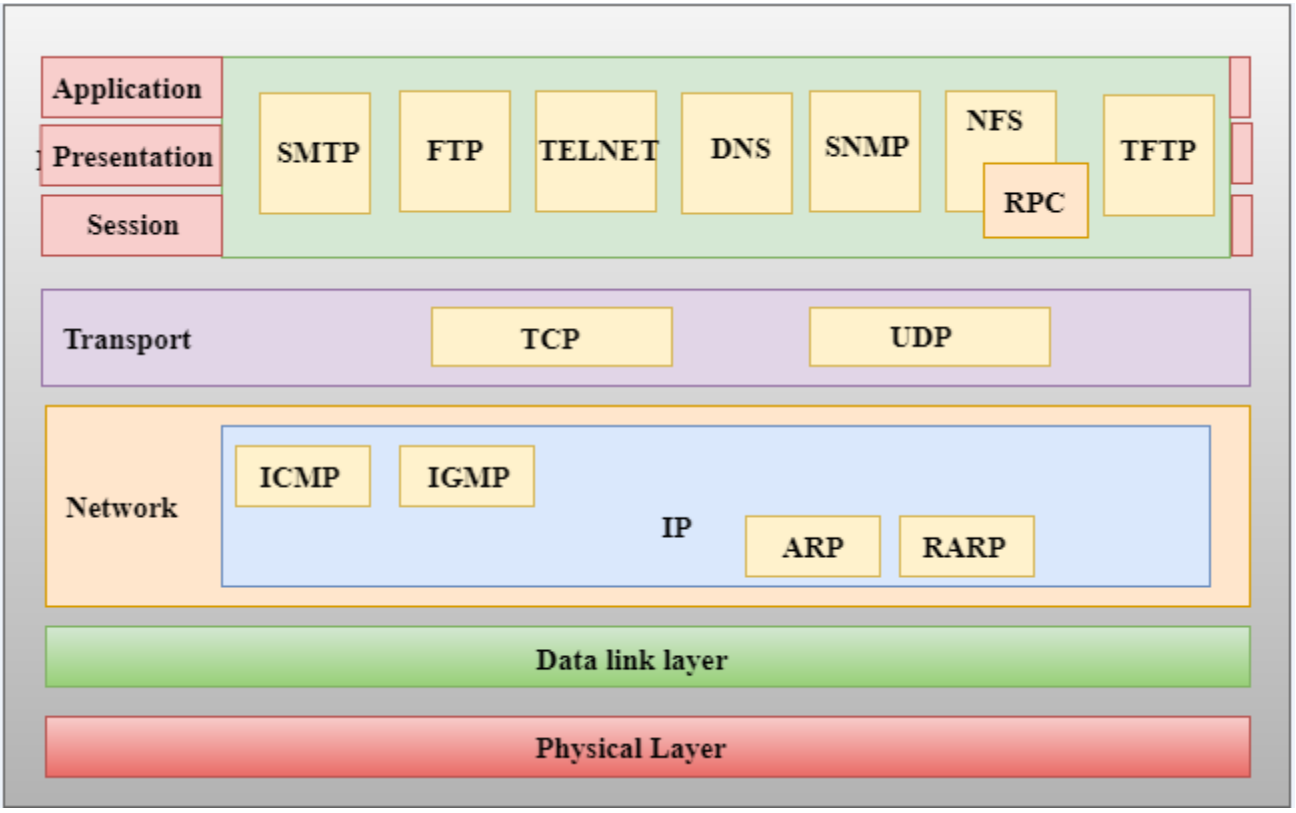




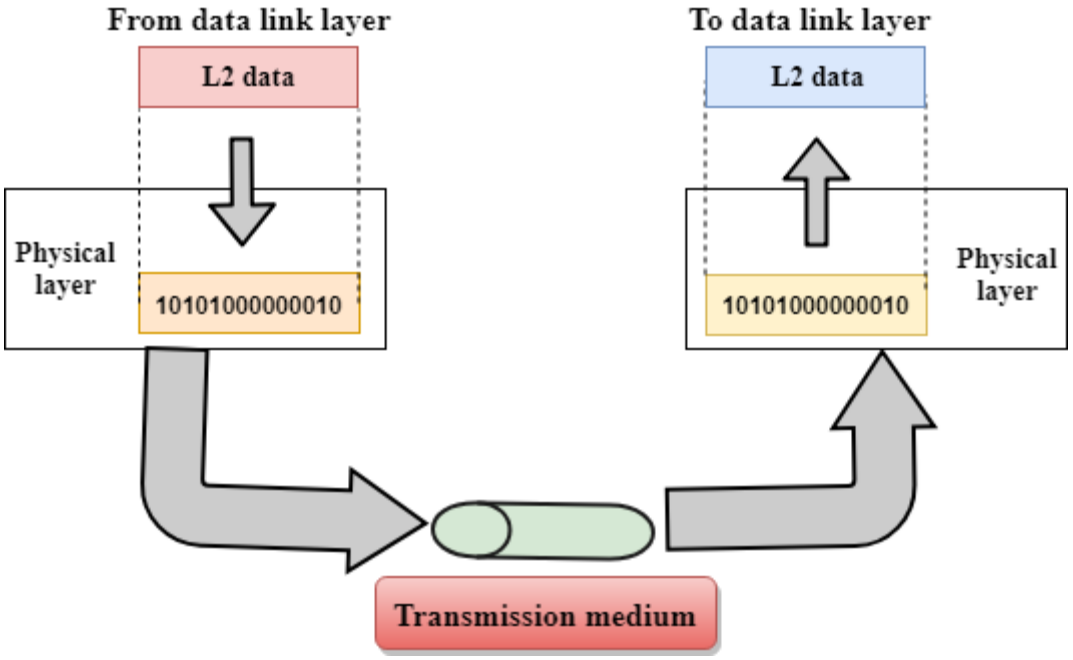
TCP/IP model

- 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.

Functions of TCP/IP layers:



Physical layer

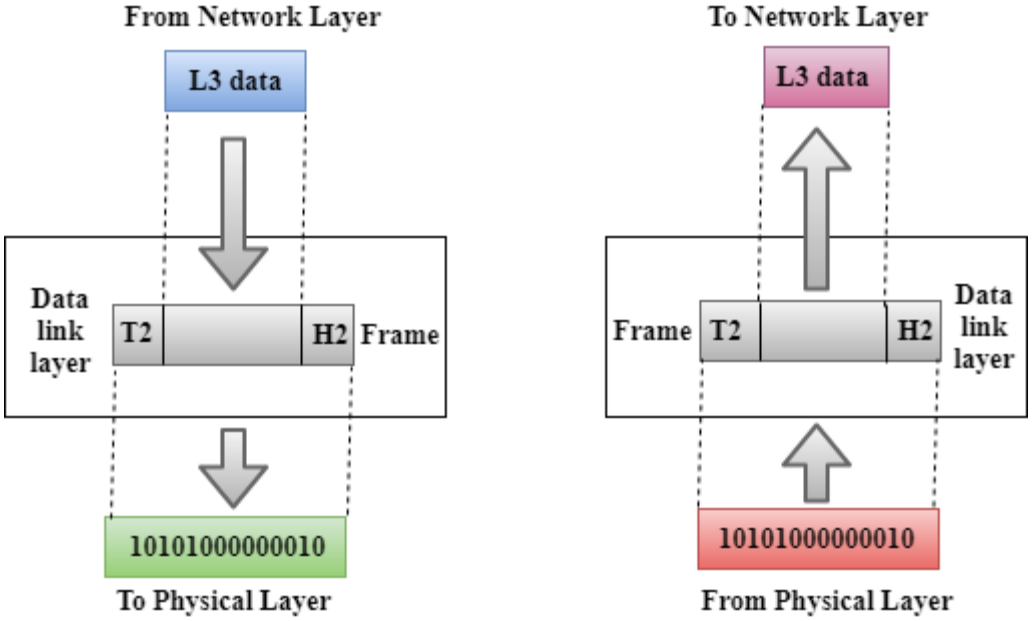


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

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.

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

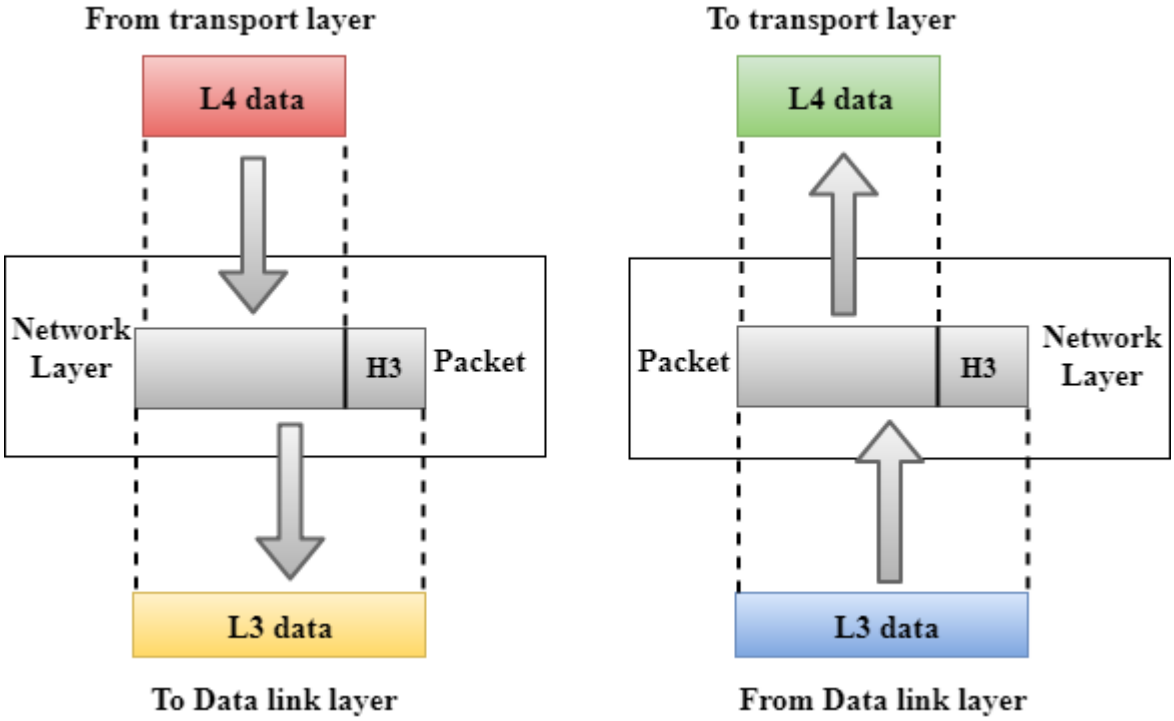
- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- **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.

- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **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 occurr, 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.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.

- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

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).

Forwarding & Routing

In Network layer, a router is used to forward the packets. Every router has a forwarding table. A router forwards a packet by examining a packet's header field and then using the header field value to index into the forwarding table. The value stored in the forwarding table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded.

Services Provided by the Network Layer

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.

- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Network Addressing

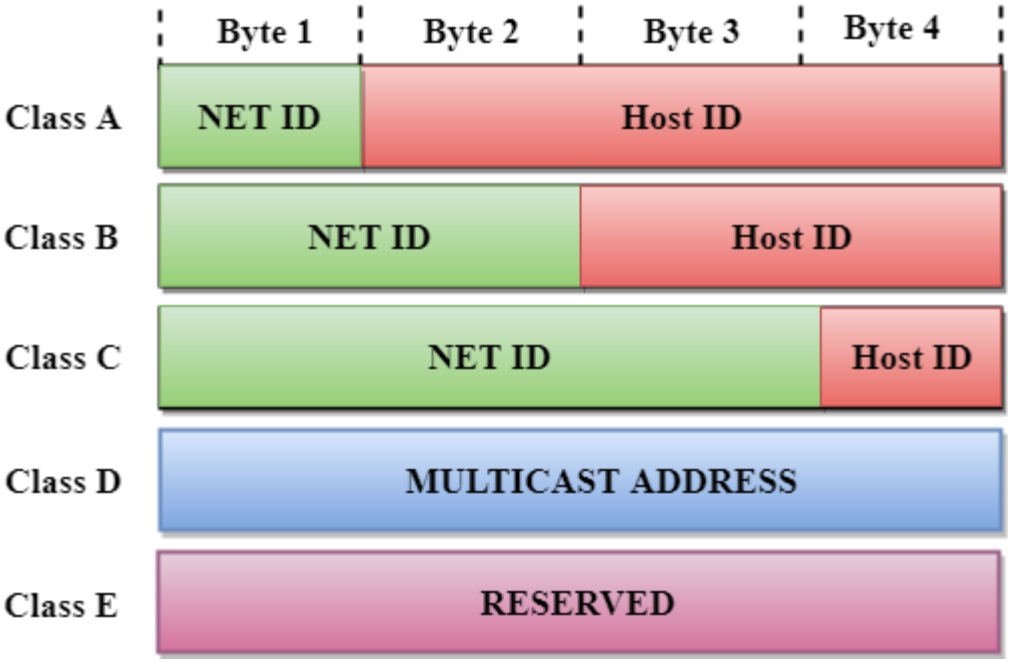
- Network Addressing is one of the major responsibilities of the network layer.
- Network addresses are always logical, i.e., software-based addresses.
- A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.

Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



next →← prev

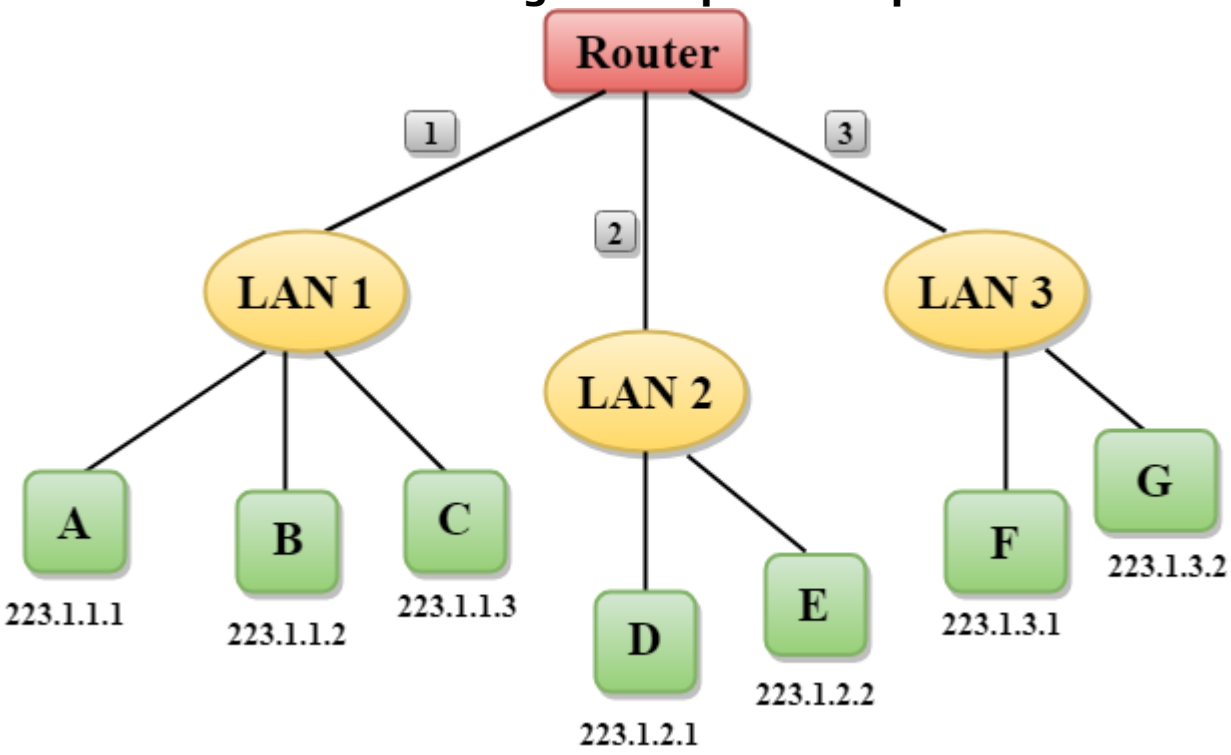
Network Addressing

- Network Addressing is one of the major responsibilities of the network layer.
- Network addresses are always logical, i.e., software-based addresses.
- A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
- A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the

router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.

- Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

- **Let's understand through a simple example.**



- In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
- Each host contains its own interface and IP address.
- All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2

and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.

- Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

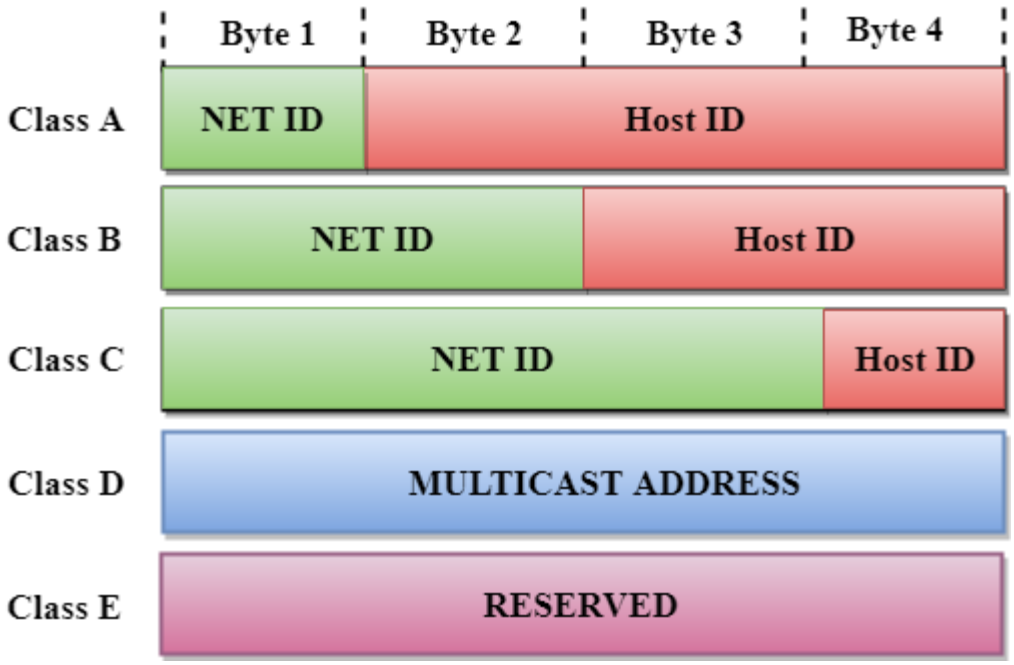
Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Classful Network Architecture

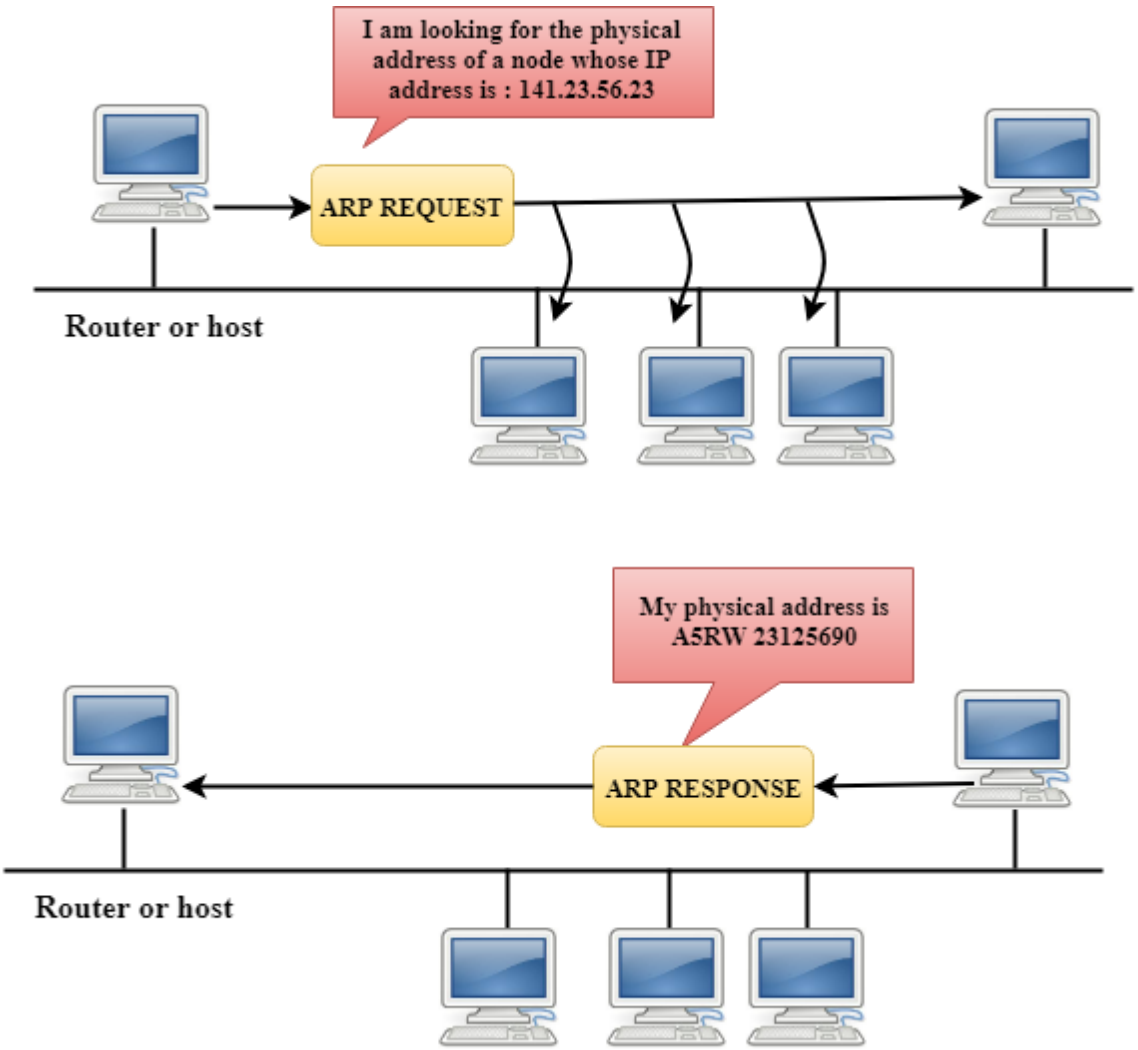
Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255

D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

Network Layer Protocols

ARP

- ARP stands for Address Resolution Protocol.
- It is used to associate an IP address with the MAC address.
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

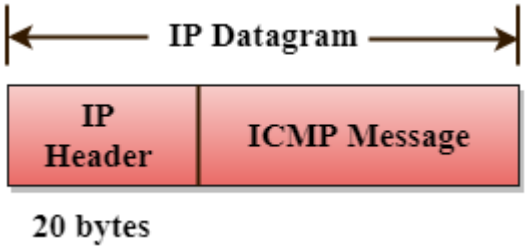


ICMP

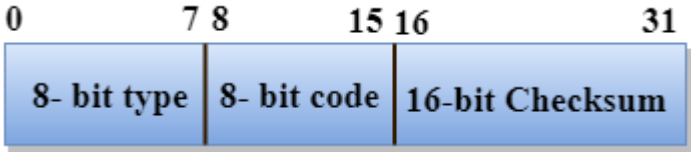
- ICMP stands for Internet Control Message Protocol.
- The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
- ICMP uses echo test/reply to check whether the destination is reachable and responding.
- ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
- An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which

it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.

- ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
- ICMP messages are transmitted within IP datagram.



The Format of an ICMP message



- The first field specifies the type of the message.
- The second field specifies the reason for a particular message type.
- The checksum field covers the entire ICMP message.

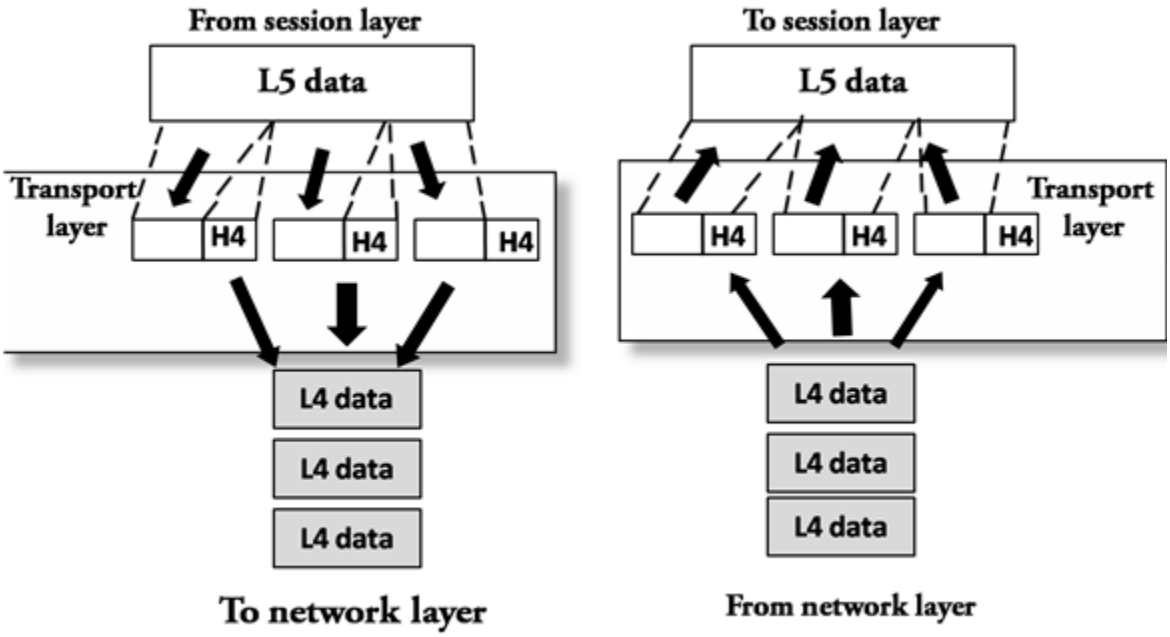
Error Reporting

ICMP protocol reports the error messages to the sender.

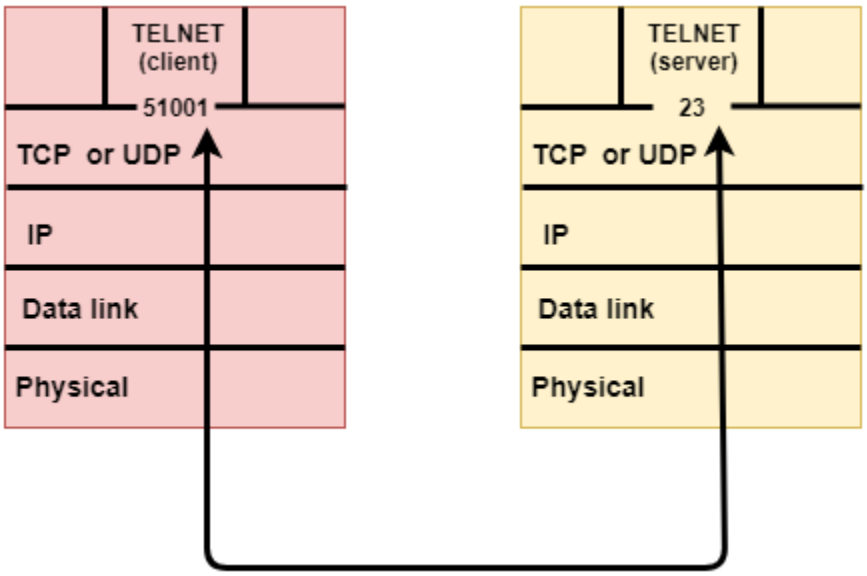
Five types of errors are handled by the ICMP protocol:

- Destination unreachable
- Source Quench
- Time Exceeded
- Parameter problems
- Redirection

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.

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

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.

Sequence Control

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the

lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

Loss Control

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

Duplication Control

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Multiplexing

The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.
- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

A port is a physical docking point using which an external device can be connected to the computer. It can also be programmatic docking point through which information flows from a program to the computer or over the Internet.

A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serving endpoint communication between two computers.

To determine what protocol incoming traffic should be directed to, different port numbers are used. They allow a single host with a single IP address to run network services. Each port number have a distinct service, and for each host can have 65535 ports per IP address. **Internet Assigned Numbers Authority (IANA)** is responsible for managing the uses of these ports. There are three categories for ports by IANA −

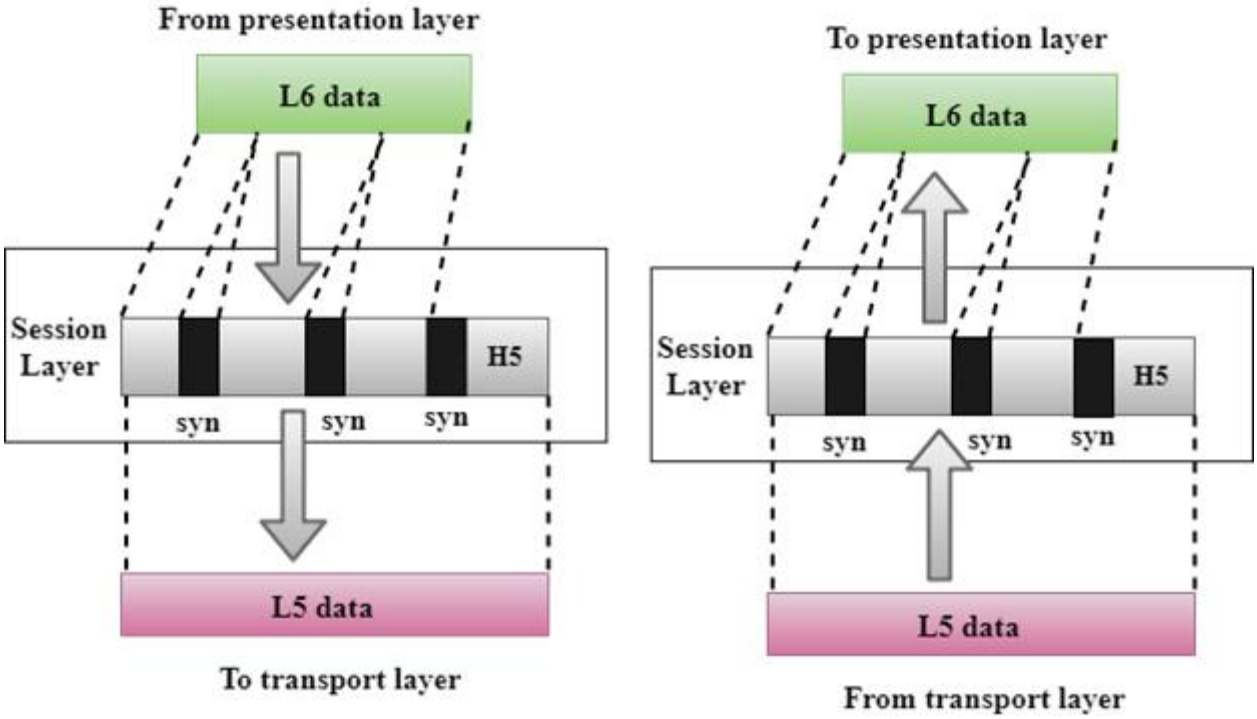
- 0 to 1023 – well known ports or system ports.

Some well-known ports are −

Port number	Transport protocol	Service name
20,21	TCP	File Transfer Protocol
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol(SMTP)
53	TCP and UDP	Domain Name System(DNS)
110	TCP	Post Office Protocol(POP3)
123	UDP	Network Time Protocol(NTP)

- **1024 to 49151** – registered ports assigned by IANA to a specific service upon application by a requesting entity.
- **49152 to 65 535** – dynamic (private, high) ports range from 49,152 to 65,535. Can be used by private or customer service or temporal purposes.

Session Layer

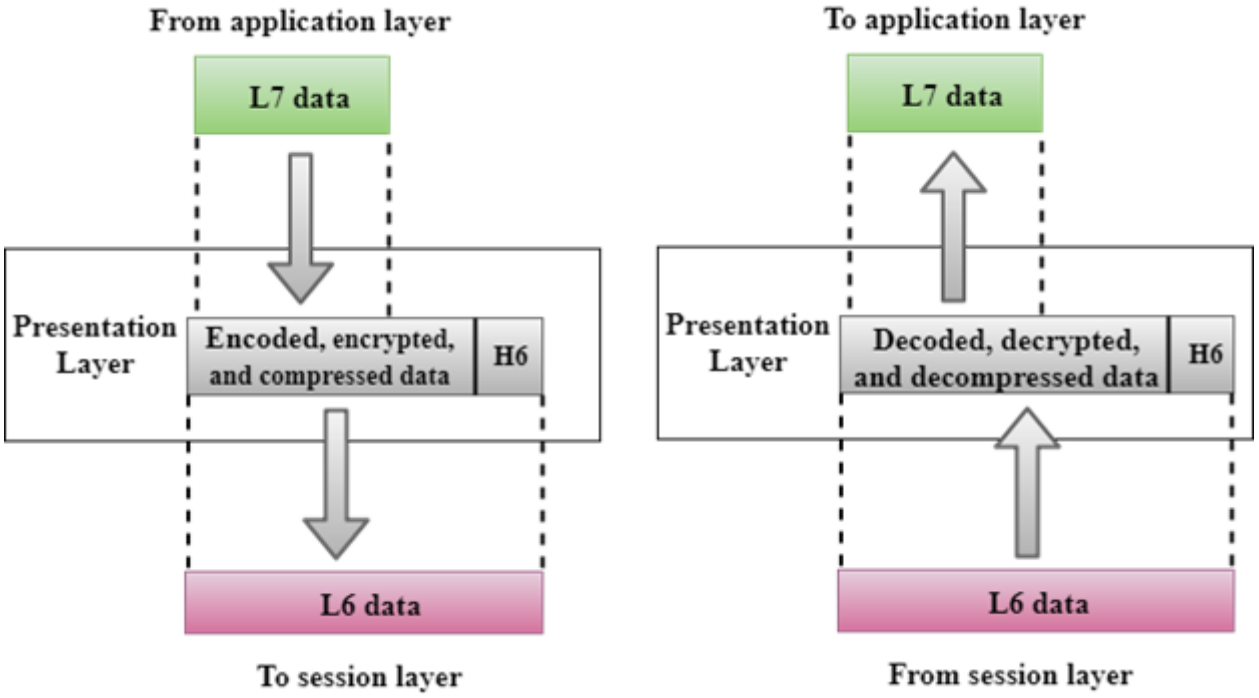


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

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.

Presentation Layer



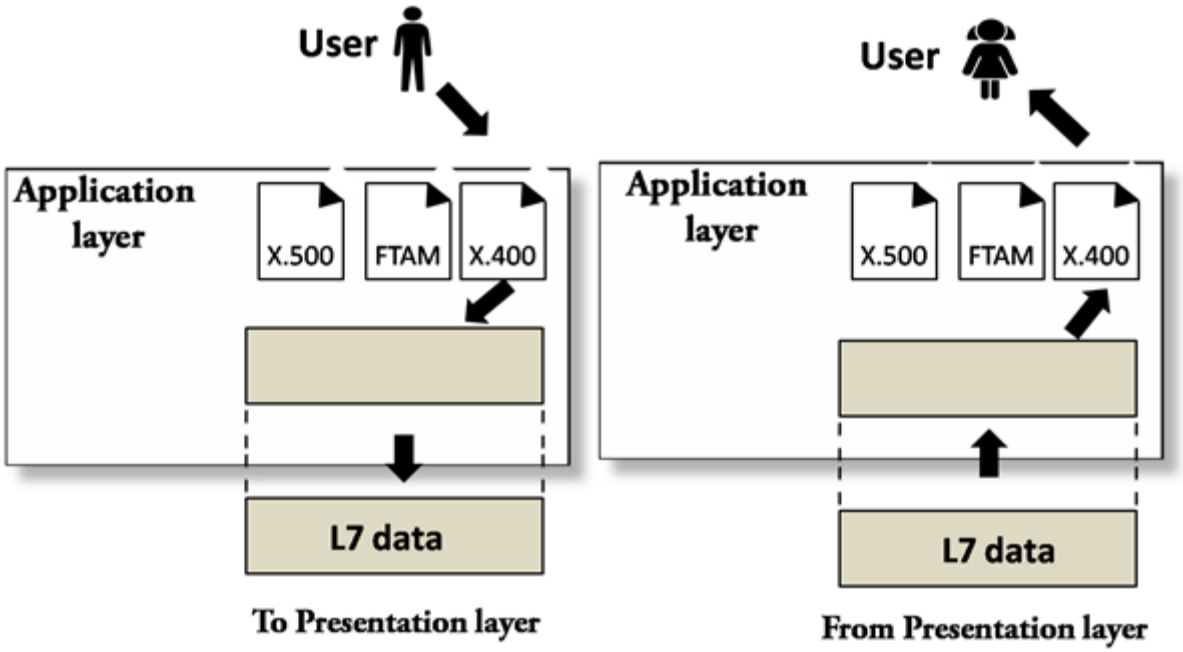
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation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

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:

- **Network Virtual terminal:** An application layer allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allows the user to log on.
- **File Transfer, Access, and Management (FTAM):** An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer. FTAM defines a hierarchical virtual file in terms of file structure, file attributes and the kind of operations performed on the files and their attributes.
- **Addressing:** To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.
- **Mail Services:** An application layer provides Email forwarding and storage.
- **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.

Authentication: It authenticates the sender or receiver's message or both.

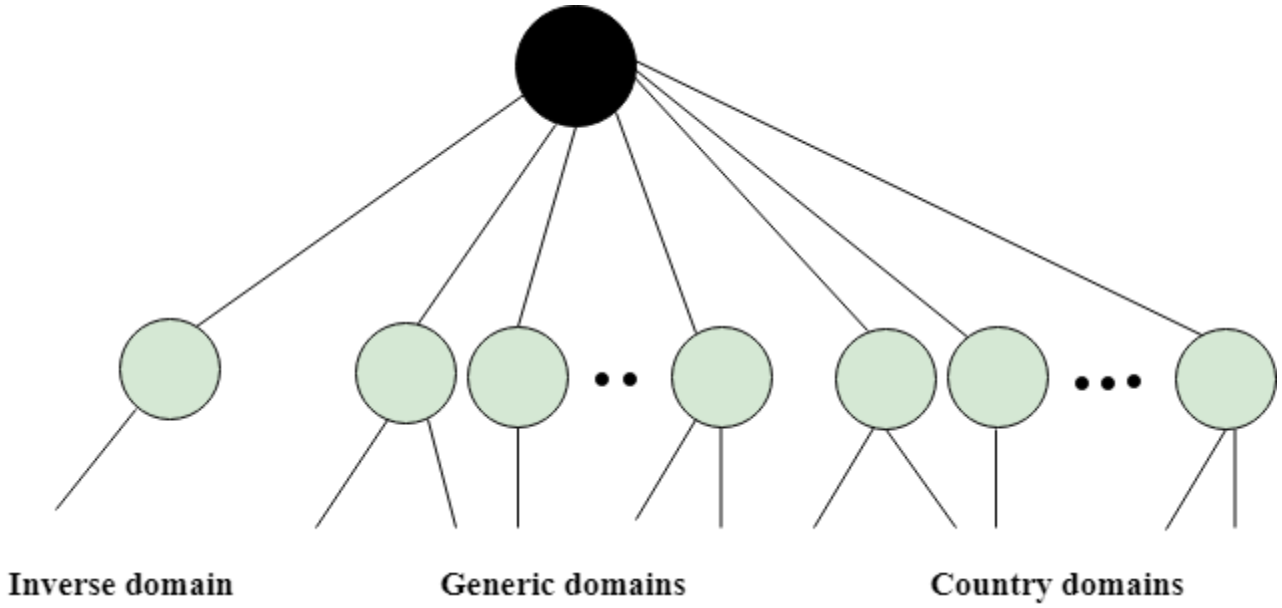
Application Layer Protocols

DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type

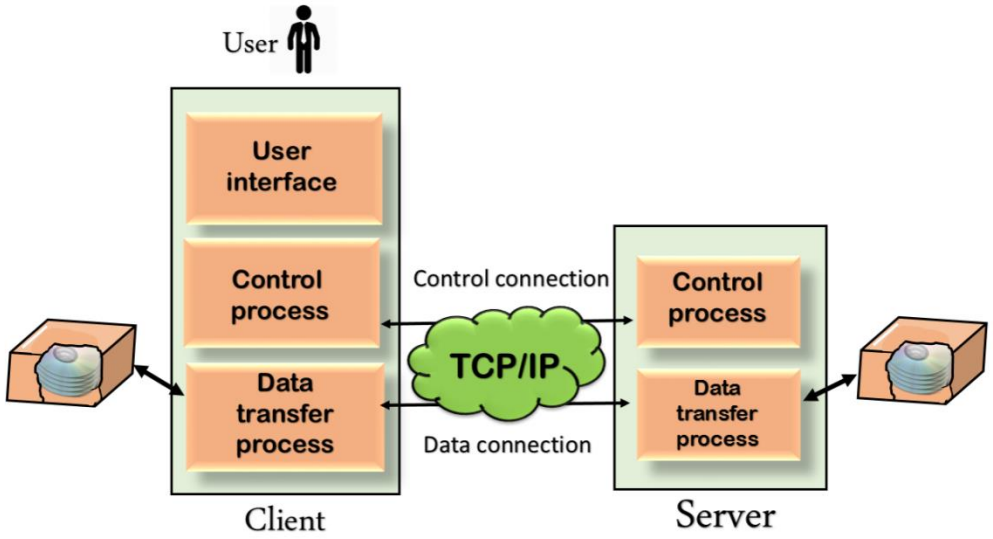
Working of DNS

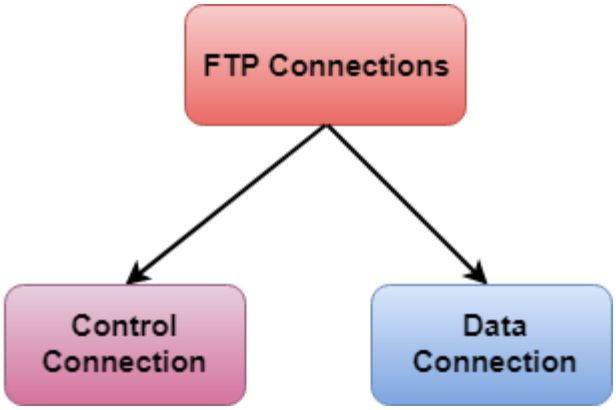
- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.

- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

FTP

- FTP stands for File transfer protocol.
- FTP 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 computer from other servers.





- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

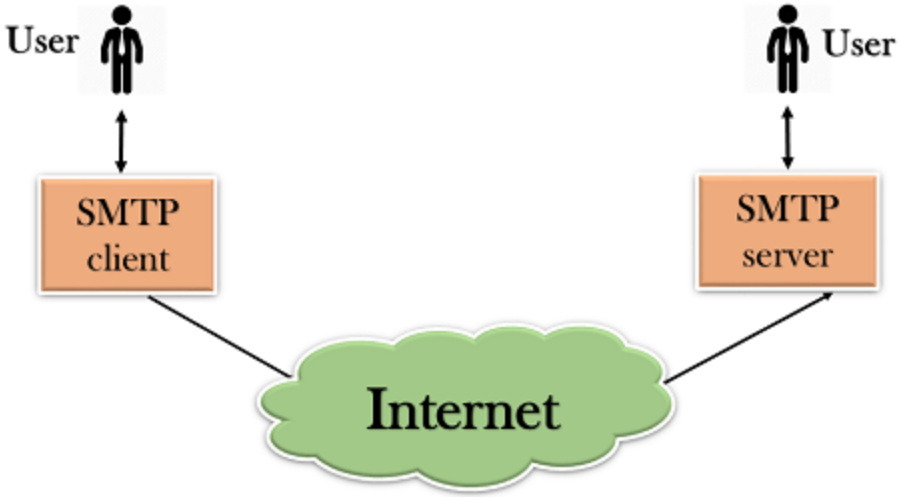
SMTP

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:

- It can send a single message to one or more recipients.
- Sending message can include text, voice, video or graphics.
- It can also send the messages on networks outside the internet.

- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

Components of SMTP

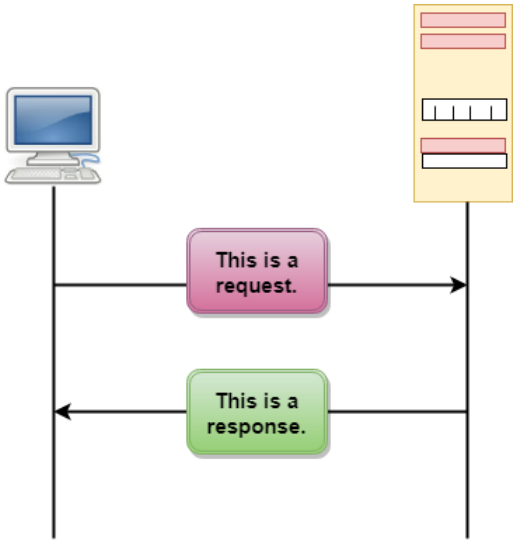


- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.

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.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

HTTP Transactions

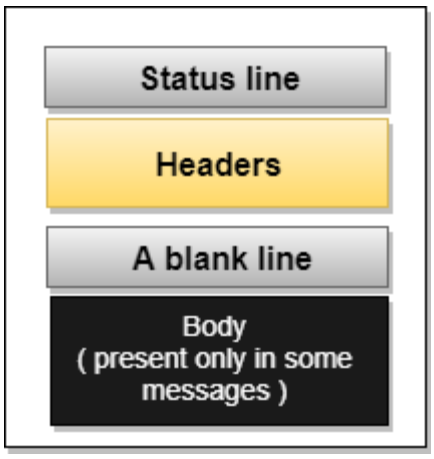


Messages

HTTP messages are of two types: request and response. Both the message types follow the same message format.

Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.

Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



Uniform Resource Locator (URL)

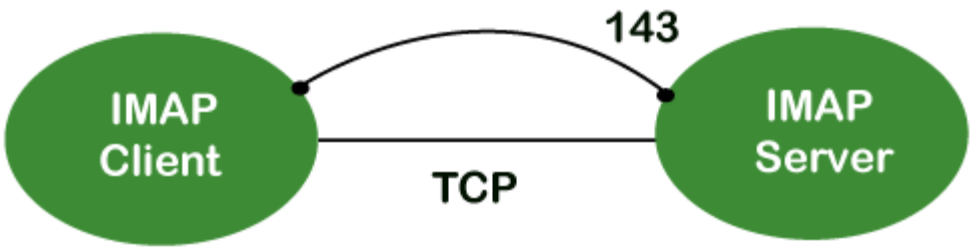
- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.

- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

IMAP Protocol

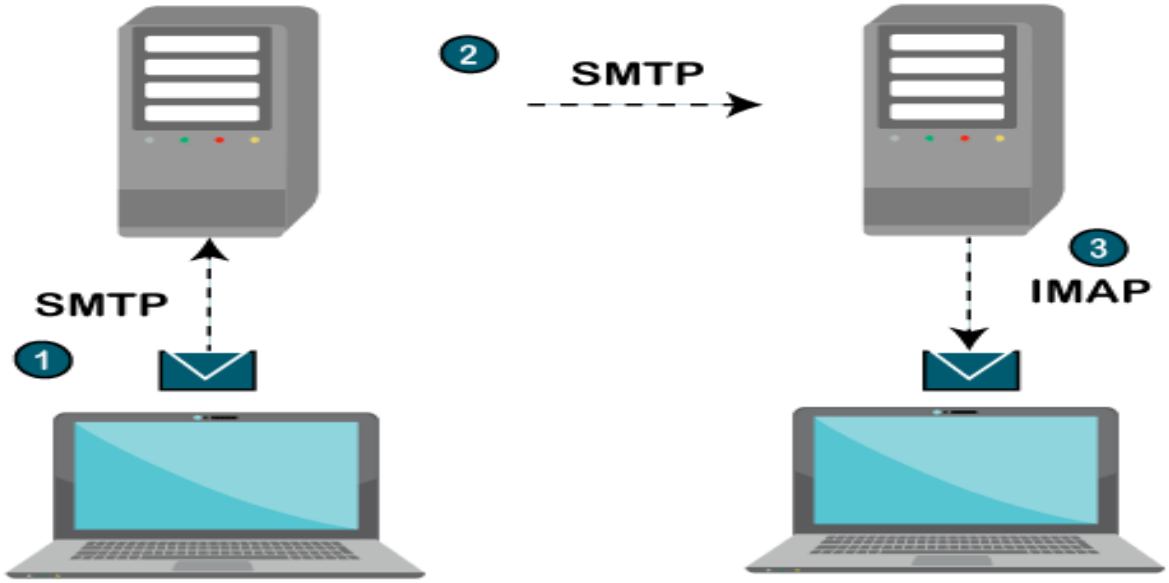
IMAP stands for **Internet Message Access Protocol**. It is an application layer protocol which is used to receive the emails from the mail server. It is the most commonly used protocols like POP3 for retrieving the emails.

It also follows the client/server model. On one side, we have an IMAP client, which is a process running on a computer. On the other side, we have an IMAP server, which is also a process running on another computer. Both computers are connected through a network.



The IMAP protocol resides on the TCP/IP transport layer which means that it implicitly uses the reliability of the protocol. Once the TCP connection is established between the IMAP client and IMAP server, the IMAP server listens to the port 143 by default, but this port number can also be changed.

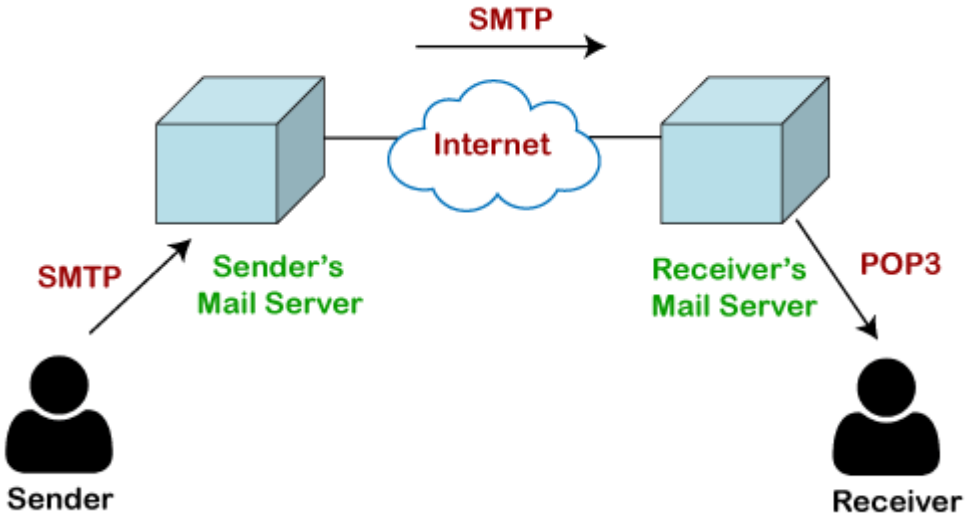
IMAP General Operation



POP Protocol

The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent. When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.

How is mail transmitted?



Suppose sender wants to send the mail to receiver. First mail is transmitted to the sender's mail server. Then, the mail is transmitted from the sender's mail server to the receiver's mail server over the internet. On receiving the mail at the receiver's mail server, the mail is then sent to the user. The whole process is done with the help of Email protocols. The transmission of mail from the sender to the sender's mail server and then to the receiver's mail server is done with the help of the SMTP protocol. At the receiver's mail server, the POP or IMAP protocol takes the data and transmits to the actual user

.

What is the maximum length allowed for a UTP cable?

The maximum length of UTP cable is 90 to 100 meters.

What is RIP?

- RIP stands for Routing Information Protocol. It is accessed by the routers to send data from one network to another.
- RIP is a dynamic protocol which is used to find the best route from source to the destination over a network by using the hop count algorithm.

- Routers use this protocol to exchange the network topology information.
- This protocol can be used by small or medium-sized networks.

What is netstat?

The "netstat" is a command line utility program. It gives useful information about the current TCP/IP setting of a connection.

---

38) What do you understand by ping command?

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.

---

39) What is Sneakernet?

Sneakernet is the earliest form of networking where the data is physically transported using removable media.

---

40) Explain the peer-peer process.

The processes on each machine that communicate at a given layer are called peer-peer process.

---

41) What is a congested switch?

A switch receives packets faster than the shared link. It can accommodate and stores in its memory, for an extended period of time, then the switch will eventually run out of buffer space, and some packets will have to be dropped. This state is called a congested state.

What is multiplexing in networking?

In Networking, multiplexing is the set of techniques that is used to allow the simultaneous transmission of multiple signals across a single data link.

What are the advantages of address sharing?

Address sharing provides security benefit instead of routing. That's because host PCs on the Internet can only see the public IP address of the external interface on the computer that provides address translation and not the private IP addresses on the internal network.

What is RSA Algorithm?

RSA is short for Rivest-Shamir-Adleman algorithm. It is mostly used for public key encryption.

What is the difference between TCP/IP model and the OSI model?

Following are the differences between the TCP/IP model and OSI model:

TCP/IP model	OSI model
Full form of TCP is transmission control protocol.	Full form of OSI is Open System Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable than the OSI model.	OSI model is less reliable as compared to the TCP/IP model.

TCP/IP model uses horizontal approach.	OSI model uses vertical approach.
TCP/IP model uses both session and presentation layer in the application layer.	OSI Reference model uses separate session and presentation layers.
TCP/IP model developed the protocols first and then model.	OSI model developed the model first and then protocols.
In Network layer, TCP/IP model supports only connectionless communication.	In the Network layer, the OSI model supports both connection-oriented and connectionless communication.
TCP/IP model is a protocol dependent.	OSI model is a protocol independent.

What is the difference between domain and workgroup?

Workgroup	Domain
A workgroup is a peer-to-peer computer network.	A domain is a Client/Server network.
A Workgroup can consist of maximum 10 computers.	A domain can consist up to 2000 computers.
Every user can manage the resources individually on their PCs.	There is one administrator to administer the domain and its resources.
All the computers must be on the same local area network.	The computer can be on any network or anywhere in the world.

Each computer must be changed manually.	Any change made to the computer will reflect the changes to all the computers.

What is bandwidth?

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

What is a gateway? Is there any difference between a gateway and router?

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**.

Differences between gateway and router:

A router sends the data between two similar networks while gateway sends the data between two dissimilar networks.

What is DNS forwarder?

- A forwarder is used with DNS server when it receives DNS queries that cannot be resolved quickly. So it forwards those requests to external DNS servers for resolution.
- A DNS server which is configured as a forwarder will behave differently than the DNS server which is not configured as a forwarder.
- **Following are the ways that the DNS server behaves when it is configured as a forwarder**:
  - When the DNS server receives the query, then it resolves the query by using a cache.
  - If the DNS server is not able to resolve the query, then it forwards the query to another DNS server.

- If the forwarder is not available, then it will try to resolve the query by using root hint.

What is the meaning of 10Base-T?

It is used to specify data transfer rate. In 10Base-T, 10 specify the data transfer rate, i.e., 10Mbps. The word Base specifies the baseband as opposed to broadband. T specifies the type of the cable which is a twisted pair.

What is NOS in computer networking?

- NOS stands for Network Operating System. It is specialized software which is used to provide network connectivity to a computer to make communication possible with other computers and connected devices.
- NOS is the software which allows the device to communicate, share files with other devices.
- The first network operating system was Novel NetWare released in 1983. Some other examples of NOS are Windows 2000, Windows XP, Linux, etc.

What is IP address?

IP address is a unique 32 bit software address of a computer in a network system.

What is private IP address?

There are three ranges of IP addresses that have been reserved for IP addresses. They are not valid for use on the internet. If you want to access internet on these private IPs, you must have to use proxy server or NAT server.

What is public IP address?

A public IP address is an address taken by the Internet Service Provider which facilitates you to communication on the internet.

What is APIPA?

APIPA is an acronym stands for Automatic Private IP Addressing. This feature is generally found in Microsoft operating system.

What is the full form of ADS?

- ADS stands for Active Directory Structure.
- ADS is a microsoft technology used to manage the computers and other devices.
- ADS allows the network administrators to manage the domains, users and objects within the network.
- ADS consists of three main tiers:
  - **Domain**: Users that use the same database will be grouped into a single domain.
  - **Tree**: Multiple domains can be grouped into a single tree.
  - **Forest**: Multiple trees can be grouped into a single forest.

What is RAID?

RAID is a method to provide Fault Tolerance by using multiple Hard Disc Drives.

What is anonymous FTP?

Anonymous FTP is used to grant users access to files in public servers. Users which are allowed access to data in these servers do not need to identify themselves, but instead log in as an anonymous guest.

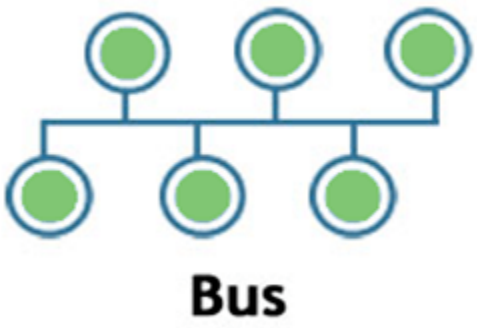
What is protocol?

A protocol is a set of rules which is used to govern all the aspects of information communication.

What do you mean by network topology?

Network topology specifies the layout of a computer network. It shows how devices and cables are connected to each other. The types of topologies are:

Bus:

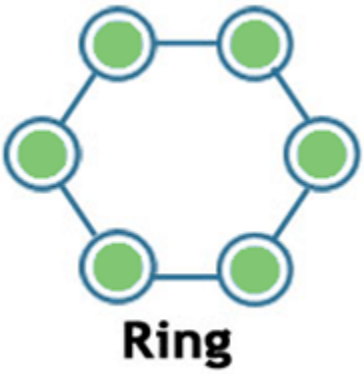


- Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.
- It acts as a shared communication medium, i.e., if any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all the attached devices.
- Bus topology is useful for a small number of devices. As if the bus is damaged then the whole network fails.

Star:

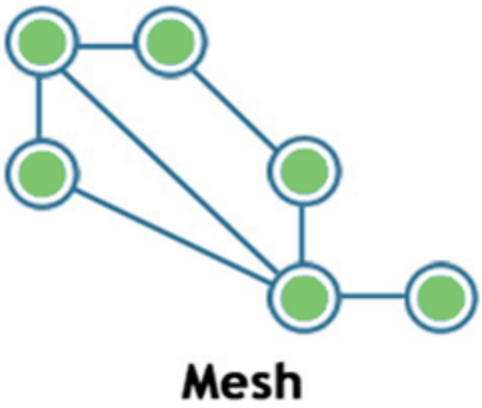
- Star topology is a network topology in which all the nodes are connected to a single device known as a central device.
- Star topology requires more cable compared to other topologies. Therefore, it is more robust as a failure in one cable will only disconnect a specific computer connected to this cable.
- If the central device is damaged, then the whole network fails.
- Star topology is very easy to install, manage and troubleshoot.
- Star topology is commonly used in office and home networks.

Ring



- Ring topology is a network topology in which nodes are exactly connected to two or more nodes and thus, forming a single continuous path for the transmission.
- It does not need any central server to control the connectivity among the nodes.
- If the single node is damaged, then the whole network fails.
- Ring topology is very rarely used as it is expensive, difficult to install and manage.
- Examples of Ring topology are SONET network, SDH network, etc.

Mesh



- Mesh topology is a network topology in which all the nodes are individually connected to other nodes.
- It does not need any central switch or hub to control the connectivity among the nodes.
- Mesh topology is categorized into two parts:
    - **Fully connected mesh topology**: In this topology, all the nodes are connected to each other.
    - **Partially connected mesh topology**: In this topology, all the nodes are not connected to each other.
- It is a robust as a failure in one cable will only disconnect the specified computer connected to this cable.
- Mesh topology is rarely used as installation and configuration are difficult when connectivity gets more.
- Cabling cost is high as it requires bulk wiring.

Tree

- Tree topology is a combination of star and bus topology. It is also known as the expanded star topology.
- In tree topology, all the star networks are connected to a single bus.

- Ethernet protocol is used in this topology.
- In this, the whole network is divided into segments known as star networks which can be easily maintained. If one segment is damaged, but there is no effect on other segments.
- Tree topology depends on the "main bus," and if it breaks, then the whole network gets damaged.

Hybrid

- A hybrid topology is a combination of different topologies to form a resulting topology.
- If star topology is connected with another star topology, then it remains star topology. If star topology is connected with different topology, then it becomes a Hybrid topology.
- It provides flexibility as it can be implemented in a different network environment.
- The weakness of a topology is ignored, and only strength will be taken into consideration.
