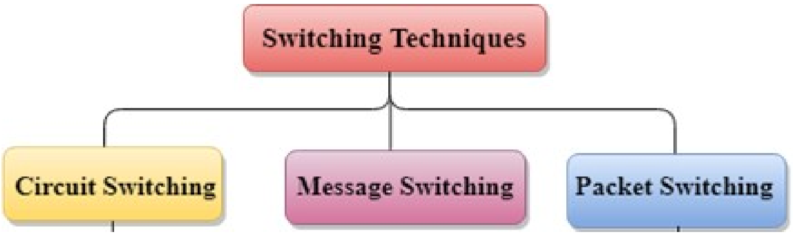
Que : 1 what is switching techniques? Explain types of switching techniques.

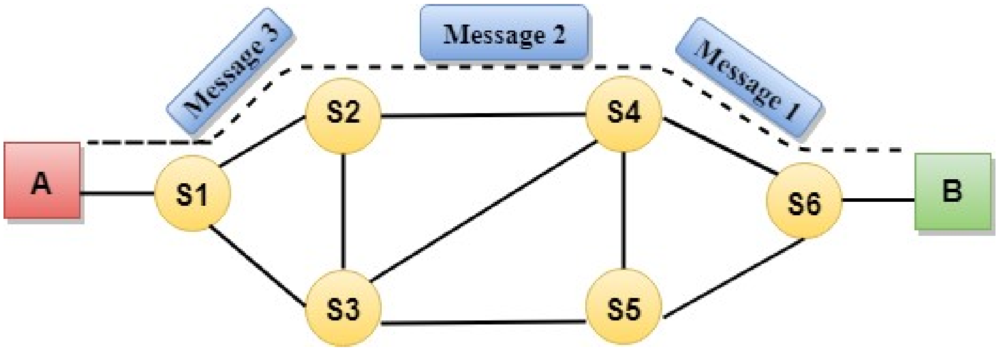
In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.



Circuit Switching

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



Advantages Of Circuit Switching:

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

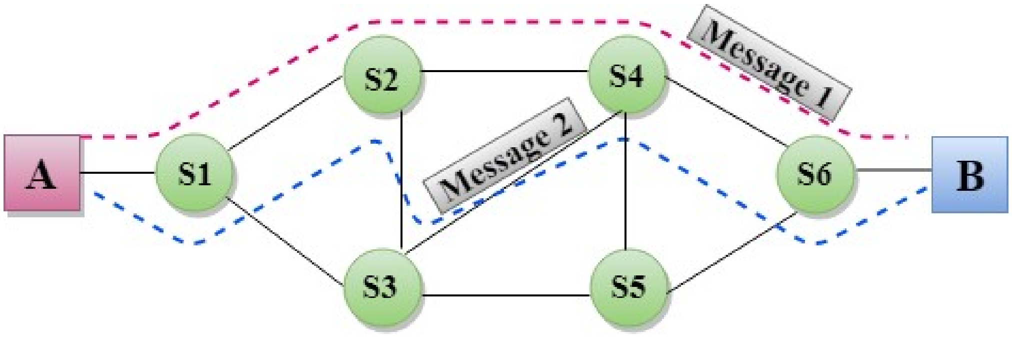
Disadvantages Of Circuit Switching:

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

Message Switching

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

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



Advantages Of Message Switching

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

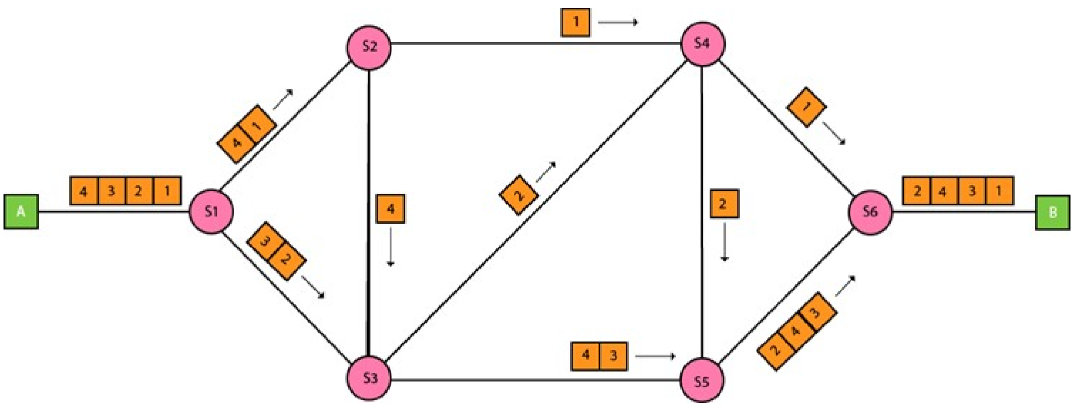
Disadvantages Of Message Switching

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

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.

- ○ Every packet contains some information in its headers such as source address, destination address and sequence number.
- ○ Packets will travel across the network, taking the shortest path as possible.
- ○ All the packets are reassembled at the receiving end in correct order.
- ○ If any packet is missing or corrupted, then the message will be sent to resend the message.
- ○ If the correct order of the packets is reached, then the acknowledgment message will be sent.



Advantages:

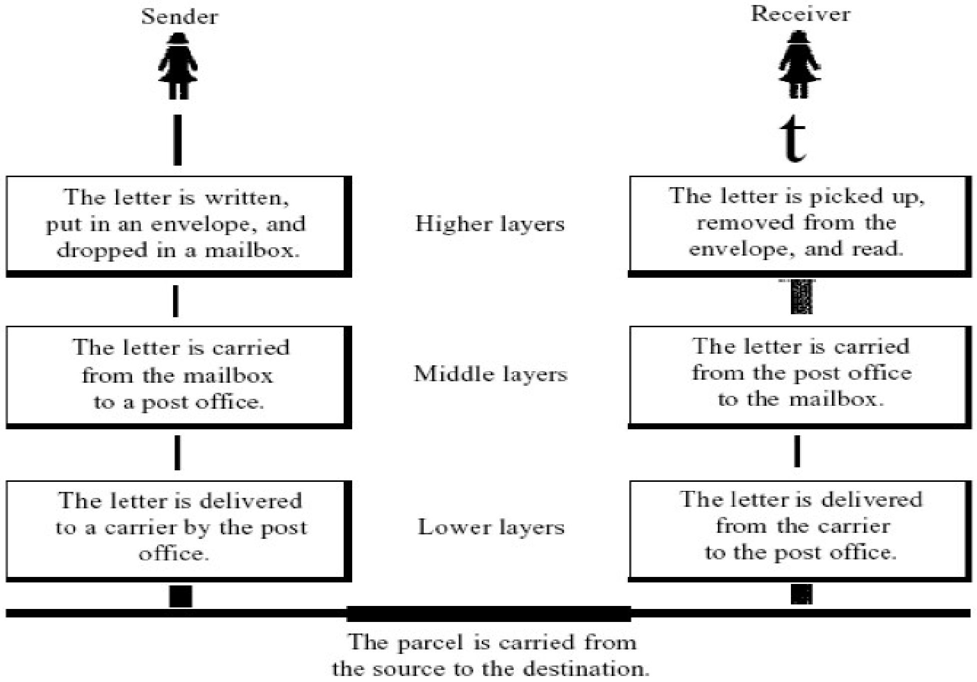
- Packet switching is cost effective.
- Offers improved delay characteristics.
- Packet can be rerouted if any problem occurs.

Disadvantages:

- Packet switching protocols are typically more complex.
- If packet gets lost sender needs to resend the data.

Que : 2 Explain layered taks

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail The process of sending a letter to a friend would be complex if there were no services available from the post office. Below Figure shows the steps in this task.


Sender
Receiver
The letter is written, put in an envelope, and dropped in a mailbox.
Higher layers
The letter is picked up, removed from the envelope, and read.
The letter is carried from the mailbox to a post office.
Middle layers
The letter is carried from the post office to the mailbox.
The letter is delivered to a carrier by the post office.
Lower layers
The letter is delivered from the carrier to the post office.
The parcel is carried from the source to the destination.

In Figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site

The activities that take place at the sender site :
» **Higher layer** : The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.
» **Middle layer** : The letter is picked up by a letter carrier and delivered to the post office.
» **Lower layer** : The letter is sorted at the post office; a carrier transports the letter

0n the Way

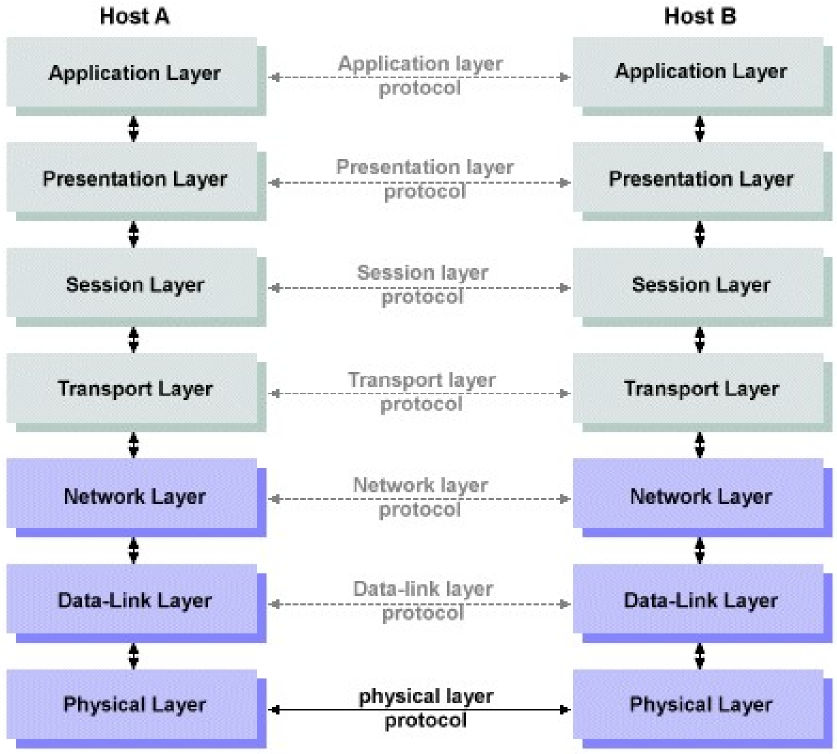
The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

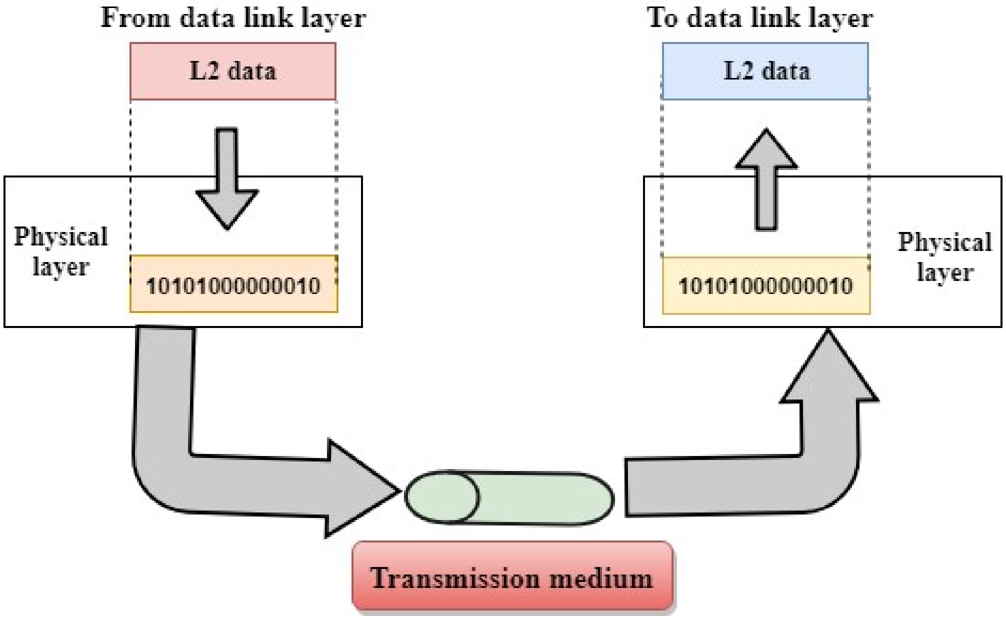
» **Lower layer** : The carrier transports the letter to the post office.
» **Middle layer** : The letter is sorted and delivered to the recipient's mailbox.
» **Higher layer** : The receiver picks up the letter, opens the envelope, and reads it.

Que : 3 What is OSI Reference Model? Explain it.

- 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.



Physical layer

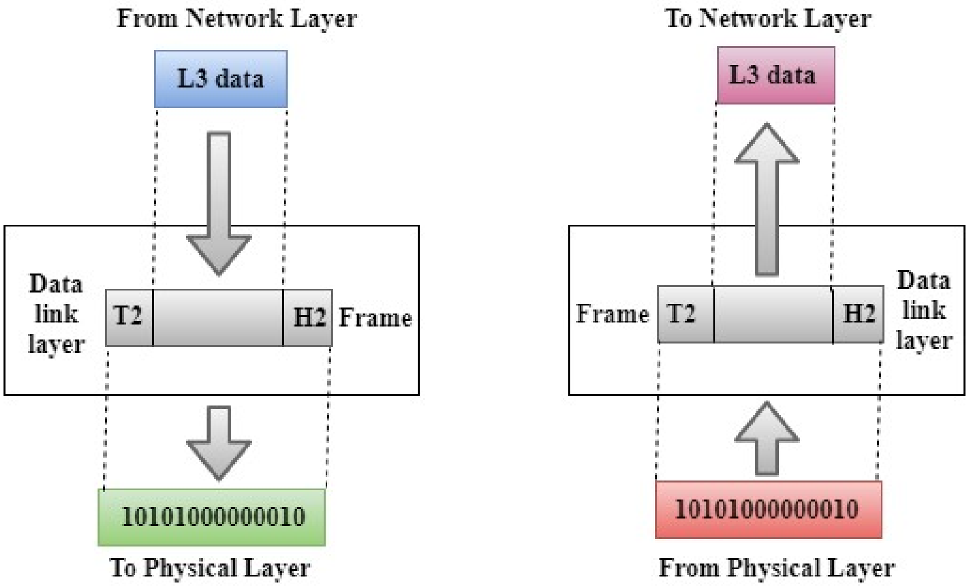


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

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.

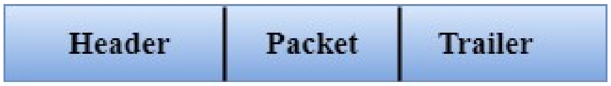
Data-Link Layer



- 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.

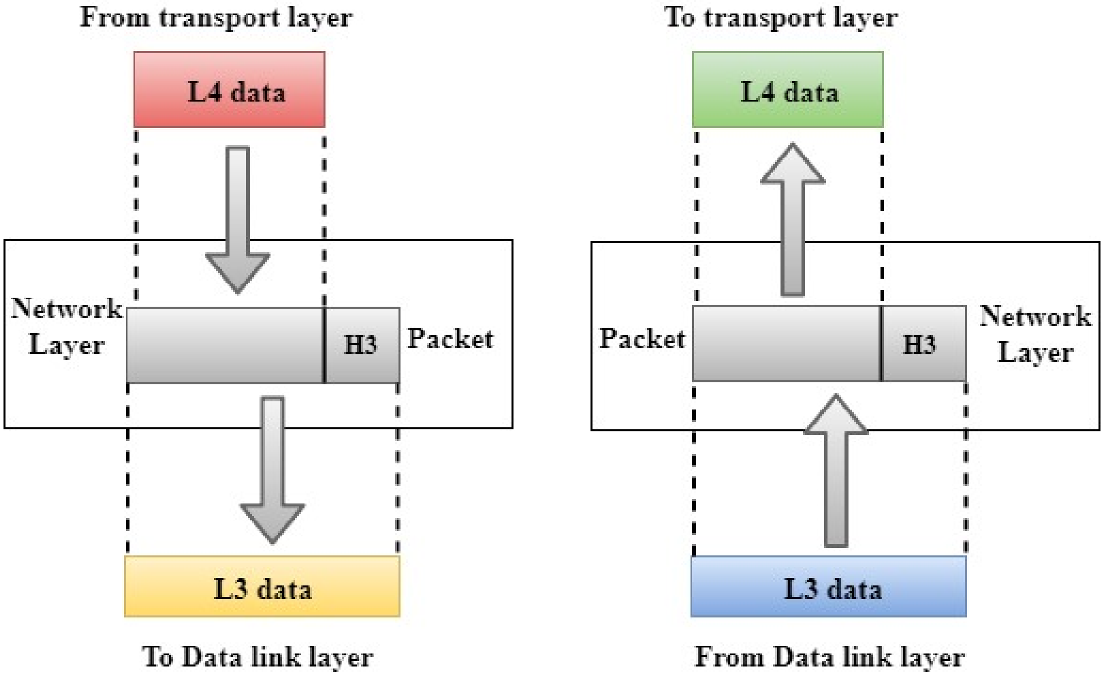
Functions of the Data-link layer

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

Network Layer

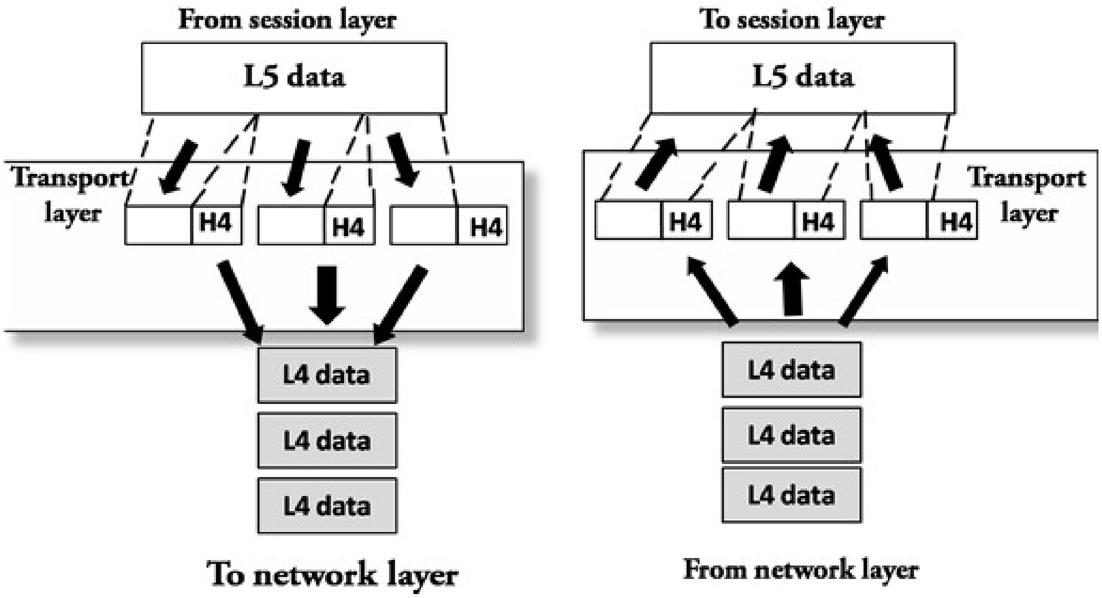


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and 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).

Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

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

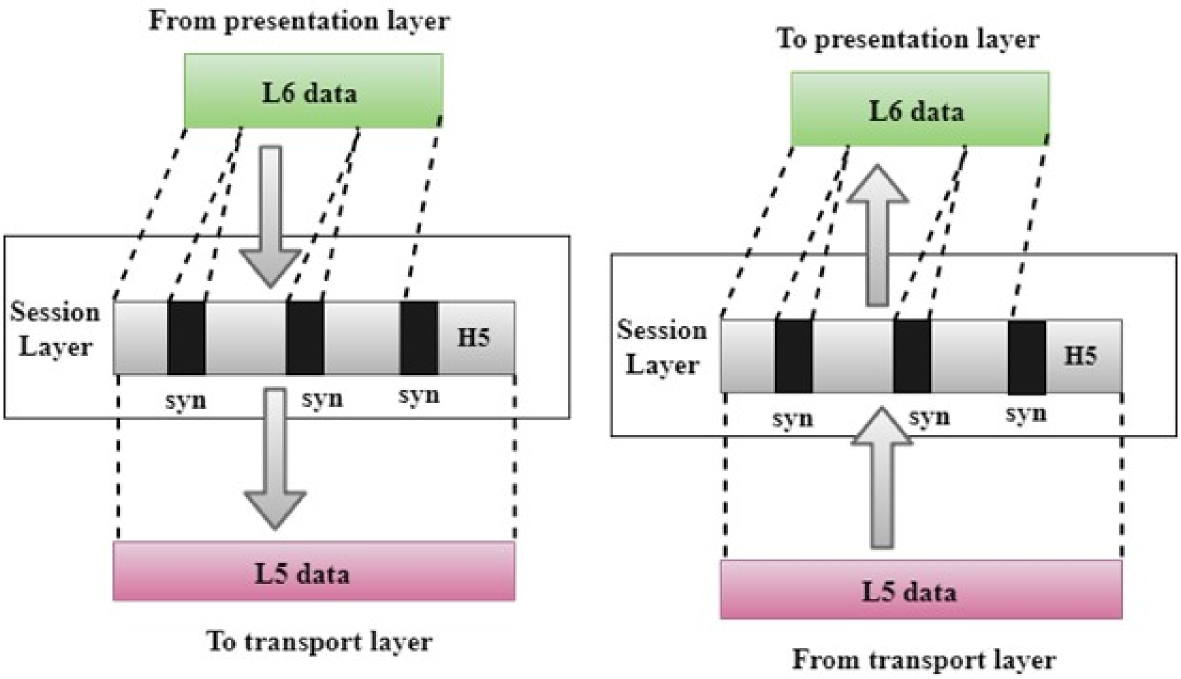
Functions of Transport Layer:

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

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

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

Session Layer

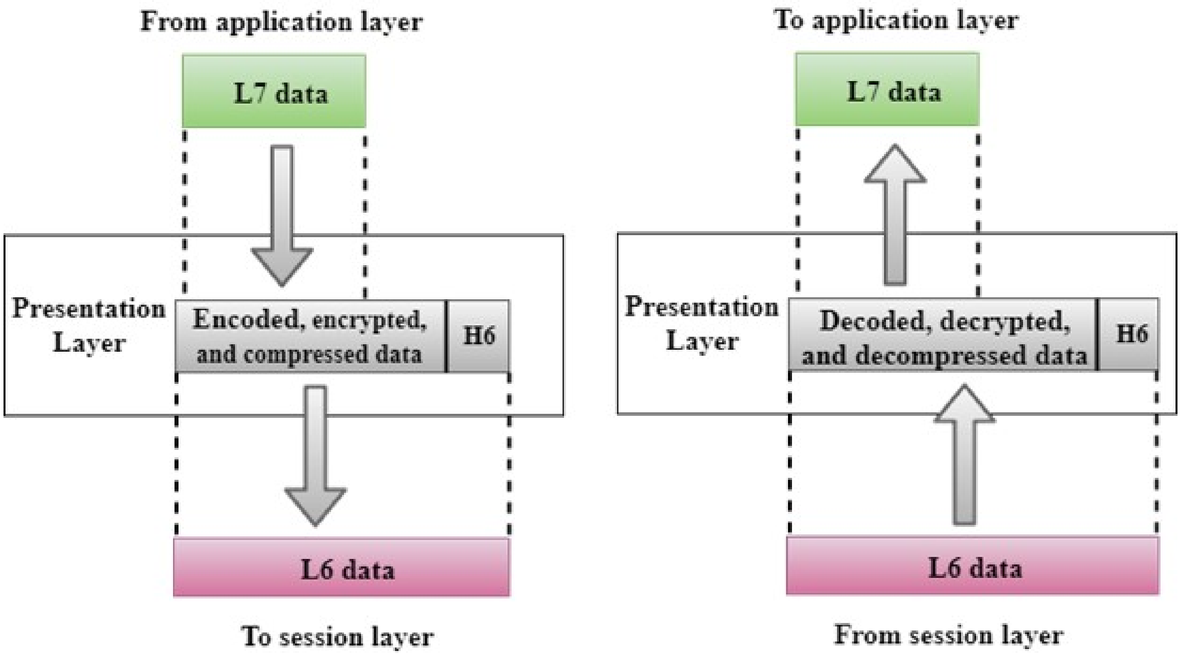


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

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



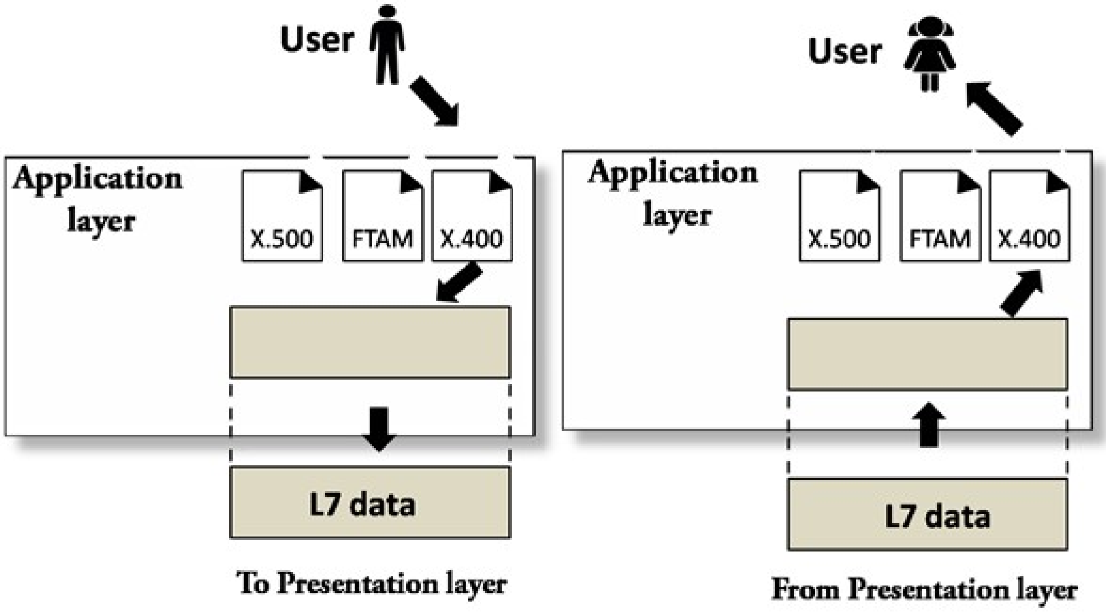
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation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

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

Que :4 Explain IP format and IP Adressing(IPV4)

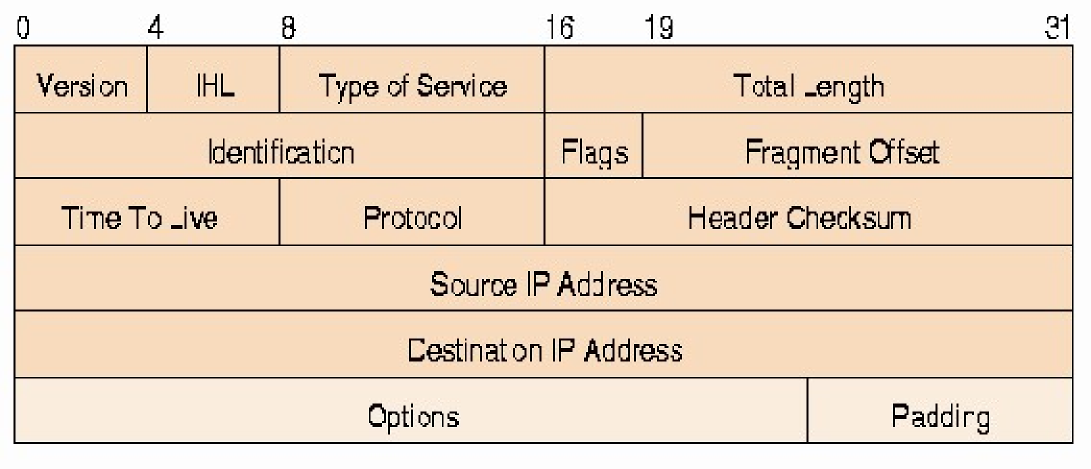
IP Format

On the massive network known as the Internet, computing devices send all kinds of messages to other computing devices. A message might be a tiny ping to check if another device is online or a message could be an entire webpage.

But there's a limit to how large a message can be, since there's a limit to how much data can be reasonably transmitted at once by the physical network connections between devices.

That's why many networking protocols split each message into multiple small **packets**. The Internet Protocol (IP) describes the structure of the packets that whizz around the Internet.

Each IP packet contains both a header (20 or 24 bytes long) and data (variable length). The header includes the IP addresses of the source and destination, plus other fields that help to route the packet. The data is the actual content, such as a string of letters or part of a webpage.



0	4	8	16	19 31
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding

A diagram of an IP packet. The header is 24 bytes long and contains 15 fields, including 4 bytes for source IP address and 4 bytes for destination IP address. The payload is variable length.

You can think of IP packets like postal letters: the header is the envelope with all the routing information that's needed by the post office, and the payload is the letter that's read only by the recipient.

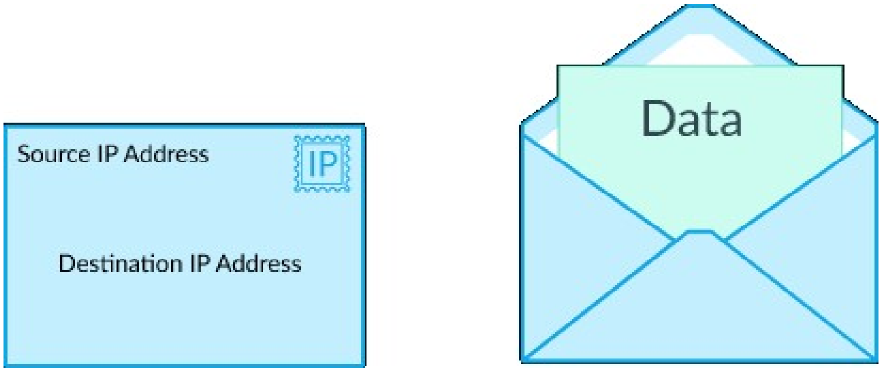


Diagram of an IP packet as a postal letter. An envelope is shown with "Source IP address" as the return address and "Destination IP address" as the mailing address. The envelope is then shown in an open state, with a letter that says "Data" poking out.

Just like the postal system routes postal letters around the world, the Internet Protocol routes IP packets around the Internet.

Following are various components/fields of IP packet header

- **Version:** The first IP header field is a 4-bit version indicator. In IPv4, the value of its four bits is set to 0100, which indicates 4 in binary. However, if the router does not support the specified version, this packet will be dropped.
- **Internet Header Length:** Internet header length, shortly known as IHL, is 4 bits in size. It is also called HELEN (Header Length). This IP component is used to show how many 32-bit words are present in the header.
- **Type of Service:** Type of Service is also called Differentiated Services Code Point or DSCP. This field is provided features related to the quality of service for data streaming or VoIP calls. The first 3 bits are the priority bits. It is also used for specifying how you can handle Datagram.
- **Total length:** The total length is measured in bytes. The minimum size of an IP datagram is 20 bytes and the maximum, it can be 65535 bytes . HELEN and Total length can be used to calculate the dimension of the payload.

  All hosts are required to be able to read 576-byte datagrams. However, if a datagram is too large for the hosts in the network, the fragmentation method is widely used.

- **Identification:** Identification is a packet that is used to identify fragments of an IP datagram uniquely. Some have recommended using this field for other things like adding information for packet tracing, etc.
- **Flags:** Flag is a three-bit field that helps you to control and identify fragments.

  The following can be their possible configuration:

  Bit 0: is reserved and has to be set to zero

  Bit 1: means do not fragment

  Bit 2: means more fragments.

- **Fragment Offset:** Fragment Offset represents the number of Data Bytes ahead of the particular fragment in the specific Datagram. It is specified in terms of the number of 8 bytes, which has a maximum value of 65,528 bytes.
- **Time to live:** It is an 8-bit field that indicates the maximum time the Datagram will be live in the internet system. The time duration is measured in seconds, and when the value of TTL is zero, the Datagram will be erased.

  Every time a datagram is processed its TTL value is decreased by one second. TTL are used so that datagrams are not delivered and discarded automatically. The value of TTL can be 0 to 255.

- **Protocol:** This IPv4 header is reserved to denote that internet protocol is used in the latter portion of the Datagram. For Example, 6 number digit is mostly used to indicate TCP, and 17 is used to denote the UDP protocol.
- **Header Checksum:** The next component is a 16 bits header checksum field, which is used to check the header for any errors. The IP header is compared to the value of its checksum. When the header checksum is not matching, then the packet will be discarded.

- **Source Address:** The source address is a 32-bit address of the source used for the IPv4 packet.
- **Destination address:** The destination address is also 32 bit in size stores the address of the receiver.
- **Options:** It is an optional field of IPv4 header used when the value of IHL (Internet Header Length) is set to greater than 5. It contains values and settings related with security, record route and time stamp, etc. You can see that list of options component ends with an End of Options or EOL in most cases.
- **Data/padding:** This field stores the data from the protocol layer, which has handed over the data to the IP layer.

IP Adressing(IPV4)

IP address is a short form of "Internet Protocol Address." It is a unique number provided to every device connected to the internet network, such as Android phone, laptop, Mac, etc. An IP address is represented in an integer number separated by a dot (.), for example, 192.167.12.46.

Types of IP Address

An IP address is categorized into two different types based on the number of IP address it contains. These are:

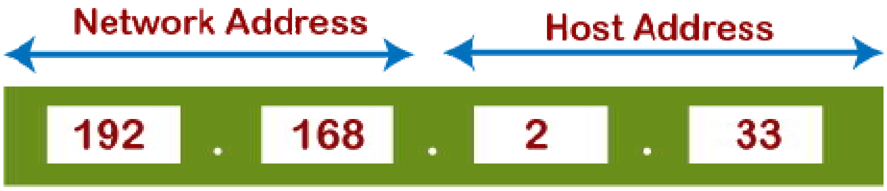
- IPv4 (Internet Protocol version 4)
- IPv6 (Internet Protocol version 6)

What is IPv4?

IPv4 is version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by a dot (.), i.e., periods. This address is unique for each device. For example, 66.94.29.13

IP Address Format

Originally IP addresses were divided into five different categories called **classes**. These divided IP classes are class A, class B, class C, class D, and class E. Out of these, classes A, B, and C are most important. Each address class defines a different number of bits for its **network prefix (network address)** and **host number (host address)**. The starting address bits decide from which class an address belongs.

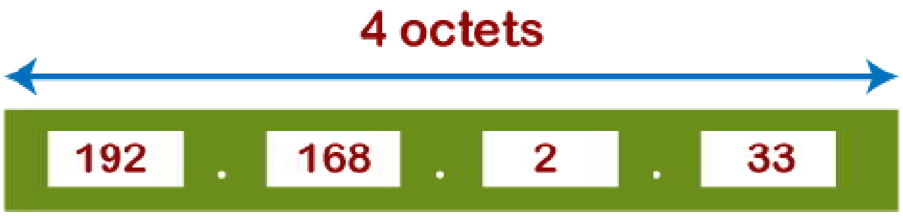


Network Address: The network address specifies the unique number which is assigned to your network. In the above figure, the network address takes two bytes of IP address.

Host Address: A host address is a specific address number assigned to each host machine. With the help of the host address, each machine is identified in your network. The network address will be the same for each host in a network, but they must vary in host address.

Address Format IPv4

The address format of IPv4 is represented into **4-octets** (32-bit), which is divided into three different classes, namely class A, class B, and class C.



The above diagram shows the address format of IPv4. An IPv4 is a 32-bit decimal address. It contains four octets or fields separated by 'dot,' and each field is 8-bit in size. The number that each field contains should be in the range of 0-255.

Class A

Class A address uses only first higher order octet (byte) to identify the network prefix, and remaining three octets (bytes) are used to define the individual host addresses. The class A address ranges between 0.0.0.0 to 127.255.255.255. The first bit of the first octet is always set to 0 (zero), and next 7 bits determine network address, and the remaining 24 bits determine host address. So the first octet ranges from 0 to 127 (00000000 to 01111111).

Class B

Class B addresses use the initial two octets (two bytes) to identify the network prefix, and the remaining two octets (two bytes) define host addresses. The class B addresses are range between 128.0.0.0 to 191.255.255.255. The first two bits of the first higher octet is always set to 10 (one and zero bit), and next 14 bits determines the network address and remaining

16 bits determines the host address. So the first octet ranges from 128 to 191 (10000000 to 10111111).

Class C

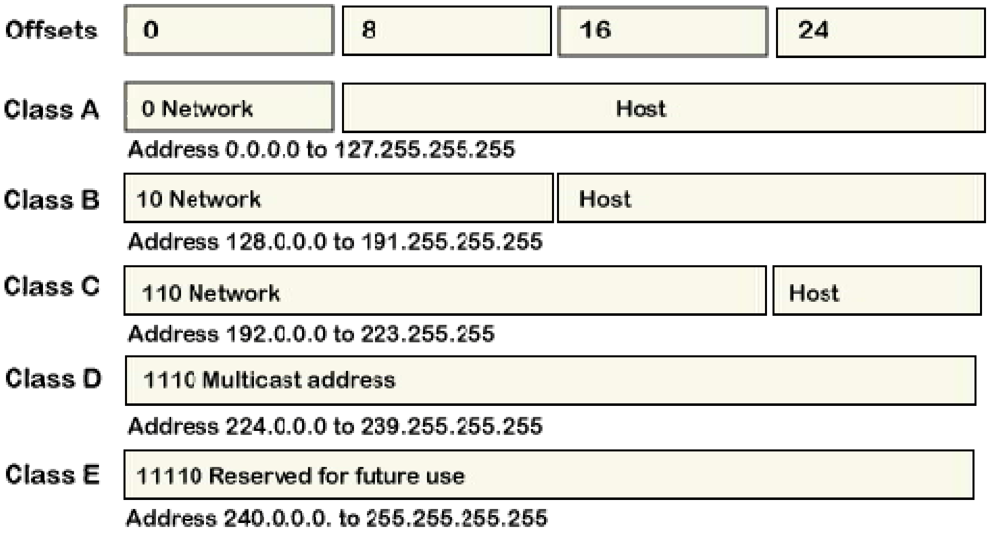
Class C addresses use the first three octets (three bytes) to identify the network prefix, and the remaining last octet (one byte) defines the host address. The class C address ranges between 192.0.0.0 to 223.255.255.255. The first three bit of the first octet is always set to 110, and next 21 bits specify network address and remaining 8 bits specify the host address. Its first octet ranges from 192 to 223 (11000000 to 11011111).

Class D

Class D IP address is reserved for multicast addresses. Its first four bits of the first octet are always set to 1110, and the remaining bits determine the host address in any IP address. The first higher octet bits are always set to 1110, and the remaining bits specify the host address. The class D address ranges between 224.0.0.0 to 239.255.255.255. In multicasting, data is not assigned to any particular host machine, so it is not require to find the host address from the IP address, and also, there is no subnet mask present in class D.

Class E

Class E IP address is reserved for experimental purposes and future use. It does not contain any subnet mask in it. The first higher octet bits are always set to 1111, and next remaining bits specify the host address. Class E address ranges between 240.0.0.0 to 255.255.255.255.


Offsets
0
8
16
24
Class A
0 Network
Host
Address 0.0.0.0 to 127.255.255.255
Class B
10 Network
Host
Address 128.0.0.0 to 191.255.255.255
Class C
110 Network
Host
Address 192.0.0.0 to 223.255.255
Class D
1110 Multicast address
Address 224.0.0.0 to 239.255.255.255
Class E
11110 Reserved for future use
Address 240.0.0.0. to 255.255.255.255

In every IP address class, all host-number bits are specified by a power of 2 that indicates the total numbers of the host's address that can create for a particular network address. Class A address can contain the maximum number of 2^{24} (16,777,216) host numbers. Class B addresses contain the maximum number of 2^{16} (65, 536) host numbers. And class C contains a maximum number of 2^{8} (256) host numbers.

Que : 5 Give difference between connectionless and connection oriented

S. No	Comparison Parameter	Connection-oriented Service	Connection Less Service
1.	Related System	It is designed and developed based on the telephone system.	It is service based on the postal system.
2.	Definition	It is used to create an end to end connection between the senders to the receiver before transmitting the data over the same or different network.	It is used to transfer the data packets between senders to the receiver without creating any connection.
3.	Virtual path	It creates a virtual path between the sender and the receiver.	It does not create any virtual connection or path between the sender and the receiver.
4.	Authentication	It requires authentication before transmitting the data packets to the receiver.	It does not require authentication before transferring data packets.
5.	Data Packets Path	All data packets are received in the same order as those sent by the sender.	Not all data packets are received in the same order as those sent by the sender.
6.	Bandwidth Requirement	It requires a higher bandwidth to transfer the data packets.	It requires low bandwidth to transfer the data packets.
7.	Data Reliability	It is a more reliable connection service because it guarantees data packets transfer from one end to the other end with a connection.	It is not a reliable connection service because it does not guarantee the transfer of data packets from one end to another for establishing a connection.
8.	Congestion	There is no congestion as it provides an end-to-end connection between sender and receiver during transmission of data.	There may be congestion due to not providing an end-to-end connection between the source and receiver to transmit of data packets.
9.	Examples	Transmission Control Protocol (TCP) is an example of a connection-oriented service.	User Datagram Protocol (UDP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP) are examples of connectionless service.

Que : 6 Reliable connection vs. unreliable connection

RELIABLE

End stations running reliable protocols will work together to verify the transmission of data to ensure accuracy and integrity of the data. A reliable system will set up a connection and verify that: all data transmitted is controlled in an orderly fashion, is received in the correct order and is intact. Reliable protocols work best over physical medium that loses data, and is prone to errors. The error correction, ordering and verification mechanisms require overhead in the data packets and increase the total amount of bandwidth required to transmit data. Transmission Control Protocol (TCP) is a typical reliable protocol. TCPoften usually adds an average of 42-63 bytes of overhead to datagrams. For a Telnet connection which transmits each keystroke individually, this is horribly inefficient because up to 64 bytes of data are transmitted to communicate just 1 byte of useful information.

UNRELIABLE

Unreliable protocols make no effort to set up a connection, they don't check to see if the data was received and usually don't make any provisions for recovering from errors or lost data. Unreliable protocols work best over physical medium with low loss and low error rates. User Datagram Protocol (UDP) is an example of an unreliable protocol. UDP makes no provisions for verifying whether data arrived or is intact. However, UDPadds a minimum of overhead when compared to TCPand is thus much faster for data transfers over high quality physical links that are high speed and exhibit little or no errors in communication.