1. Explain different types of guided transmission media.

Ans.

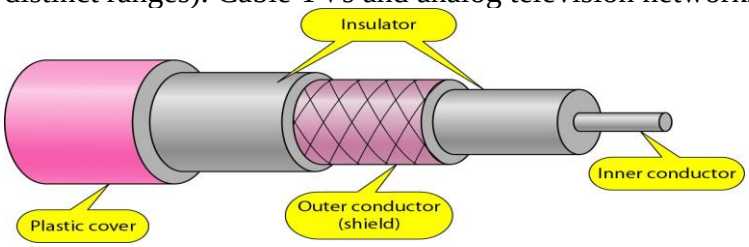
Guided Transmission Media, also known as Wired or Bounded transmission media, is the physical medium through which the signals are transmitted. The transmitted signals are directed and confined in a narrow pathway using physical links.

It provides us with features like higher speeds, and better security and is used preferably for comparatively shorter distances. A signal traveling along any such media is directed and contained by the physical limits of the medium.
There are three types of Guided Transmission Media:

Twisted Pair cable
Coaxial cable
Fibre Optic Cable

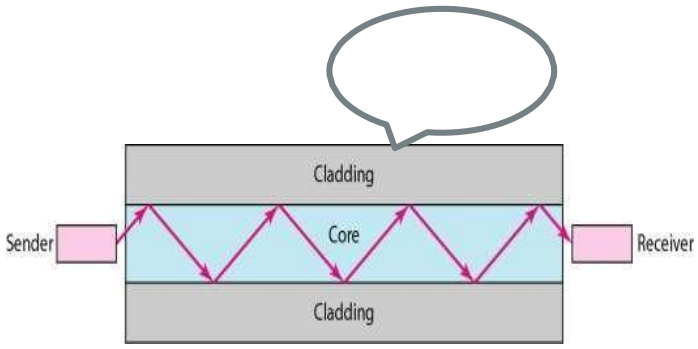
Twisted-Pair Cables are cables consisting of two insulated conductor wires (typically copper) wound and twisted together arranged in a regular spiral pattern. One wire carries the signal to the receiver, and the other is used as a ground reference. The receivers use the difference between the two to interpret signals. Generally, several such pairs are bundled together in a protective sheath. Twisting is done to make sure the noise will equally affect the wire from the external environment. They are the most popularly used Transmission Media and are also the least expensive, and they are lightweight and simple to install while supporting a wide range of network types. The frequency range for twisted pair cable ranges from 0 to 3.5KHz.The number of turns per foot determines the degree of reduction in noise interference. Increasing the number of turns per foot decreases the noise interference.

Coaxial cable, also known as coax, consists of an inner conductor surrounded by a concentric conducting shield. Coaxial Cables have an outer plastic covering containing an insulation layer made of PVC or Teflon and two parallel conductors, each having a separate insulated protection cover. The coaxial cable transmits information in baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into distinct ranges). Cable TVs and analog television networks widely use Coaxial cables.



A fiber optic cable is a cable that uses electrical signals for communication. A fiber optic is a cable that holds the optical fibers coated in plastic used to send the data by light pulses. The plastic coating protects the optical fibers from heat, cold, and electromagnetic interference from other types of wiring. Fiber optic cables provide faster data transmission

than copper wires.



2. Illustrate different types of topologies

Ans. Geometric representation of how the computers are connected to each other is known as topology.

• There are five types of topologies –

➢Mesh

➢Star

➢Bus

➢Ring

➢Hybrid

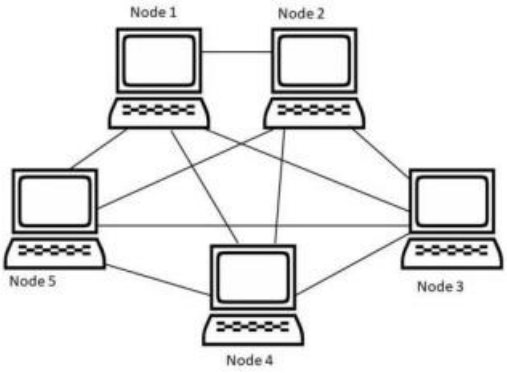
Mesh Topology

• In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link.

• The link only carries data for the two connected devices only.

Advantages of Mesh topology:

1. No data traffic issues as there is a dedicated link between two devices
2. Mesh topology is reliable and robust as failure of one link doesn't affect other links.
3. Fault detection is easy



Star Topology

• In star topology each device in the network is connected to a central device called hub.

• Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub.

Advantages of Star topology:

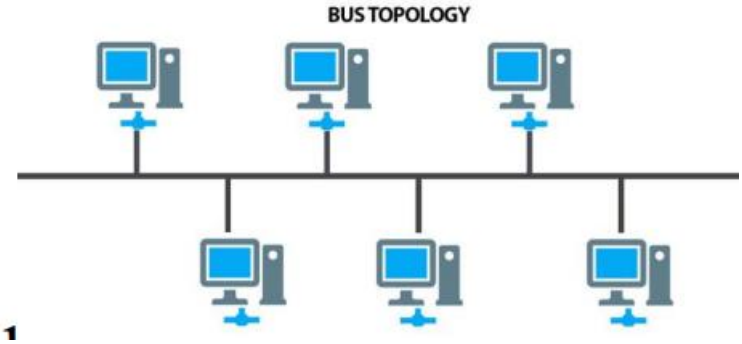
1. Less expensive because each device only needs one I/O port and needs to be connected with hub with one link.
2. Easier to install a smaller number of cables required because each device needs to be connected with the hub only.

Bus Topology

• In bus topology there is a main cable and all the devices are connected to this main cable through drop lines
• There is a device called tap that connects the drop line to the main cable.
• Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

Advantages of bus topology:

1. Easy installation, each cable needs to be connected with backbone cable.
2. Less cables required than Mesh and star topology



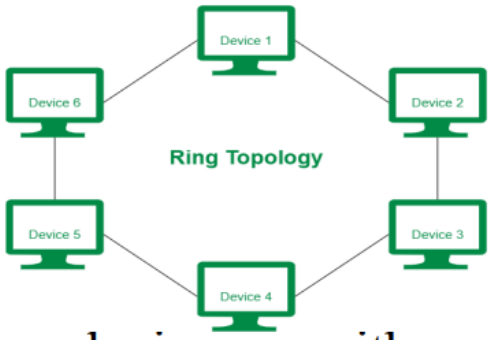
1

Ring Topology

• In ring topology each device is connected with the two devices on either side of it.
• This structure forms a ring thus it is known as ring topology.
• If a device wants to send data to another device, then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

Advantages of Ring Topology:

1. Easy to install.
2. Managing is easier as to add or remove a device from the topology only two links are



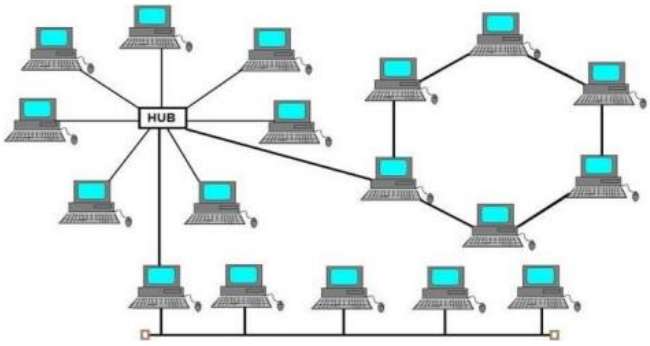
required to be changed.

Hybrid Topology

• A combination of two or more topology is known as hybrid topology. For example, a comb

Advantages of Hybrid topology:

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
2. Scalable as we can further connect other computer networks with the existing networks with different topologies



3. Compare and contrast circuit switching and packet switching.

Ans.

Similarities:

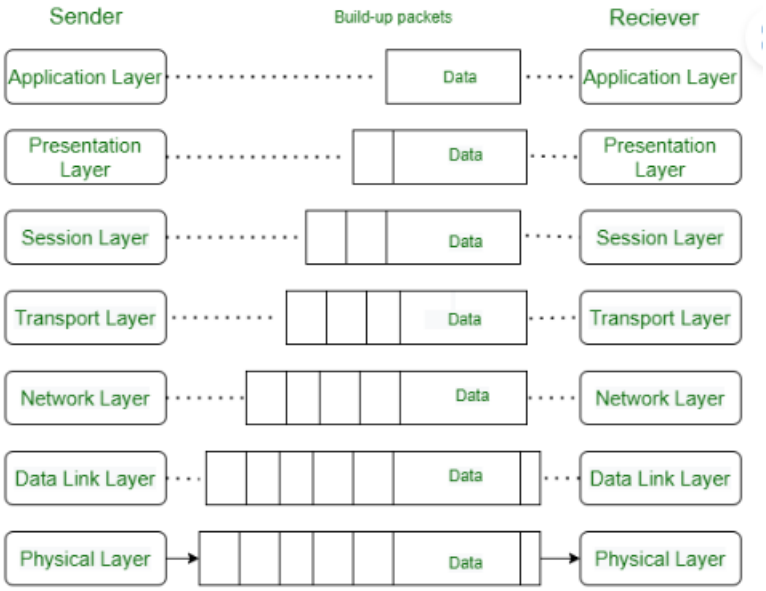
- Both methods involve the transmission of data over a network.
- Both methods use a physical layer of the OSI model for transmission of data.
- Both methods can be used to transmit voice, video, and data.
- Both methods can be used in the same network infrastructure.
- Both methods can be used for both wired and wireless networks.

4.Difference between Circuit Switching and Packet Switching:

Circuit Switching	Packet Switching
In-circuit switching has there are 3 phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
In-circuit switching, each data unit knows the entire path address which is provided by the source.	In Packet switching, each data unit just knows the final destination address intermediate path is decided by the routers.
In-Circuit switching, data is processed at the source system only	In Packet switching, data is processed at all intermediate nodes including the source system.
The delay between data units in circuit switching is uniform.	The delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because the path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources is more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source.	Transmission of the data is done not only by the source but also by the intermediate routers.
Congestion can occur during the connection establishment phase because there might be a case where a request is being made for a channel but the channel is already occupied.	Congestion can occur during the data transfer phase, a large number of packets comes in no time.
Circuit switching is not convenient for handling bilateral traffic.	Packet switching is suitable for handling bilateral traffic.
In-Circuit switching, the charge depends on time and distance, not on traffic in the network.	In Packet switching, the charge is based on the number of bytes and connection time.
Recording of packets is never possible in circuit switching.	Recording of packets is possible in packet switching.
In-Circuit Switching there is a physical path between the source and the destination	In Packet Switching there is no physical path between the source and the destination
Circuit Switching does not support store and forward transmission	Packet Switching supports store and forward transmission
Call setup is required in circuit switching.	No call setup is required in packet switching.
In-circuit switching each packet follows the same route.	In packet switching packets can follow any route.

The circuit switching network is implemented at the physical layer.	Packet switching is implemented at the datalink layer and network layer
Circuit switching requires simple protocols for delivery.	Packet switching requires complex protocols for delivery.

5. Describe ISO/OSI reference model with diagram.
Ans.



Physical Layer – Layer 1

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

Data Link Layer (DLL) – Layer 2

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.
The Data Link Layer is divided into two sublayers:

Logical Link Control (LLC)
Media Access Control (MAC)

Network Layer – Layer 3

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to

transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

Transport Layer – Layer 4

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the End-to-End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

Session Layer – Layer 5

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

Presentation Layer – Layer 6

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

Application Layer – Layer 7

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

6. Classify different framing methods and solve the below:

The following character encoding is used in a data link protocol: A: 01000111; B: 11100011;FLAG: 01111110; ESC: 11100000

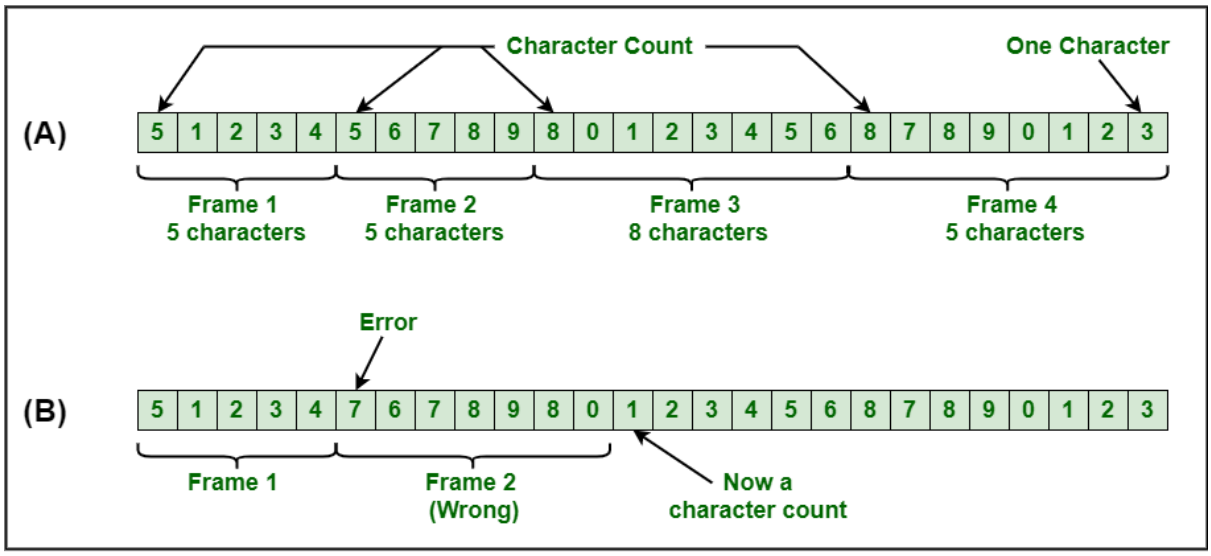
Show the bit sequence transmitted (in binary) for the four-character frame: A B ESC FLAG when each of the following framing methods are used: (a) Character count (b) Flag bytes with byte stuffing. (c) Starting and ending flag bytes, with bit stuffing.

Ans.

Character Count:

This method is rarely used and is generally required to count total number of characters that are present in frame. This is be done by using field in header. Character count method ensures data link layer at the receiver or destination about total number of characters that follow, and about where the frame ends.

There is disadvantage also of using this method i.e., if anyhow character count is disturbed or distorted by an error occurring during transmission, then destination or receiver might lose synchronization. The destination or receiver might also be not able to locate or identify beginning of next frame.



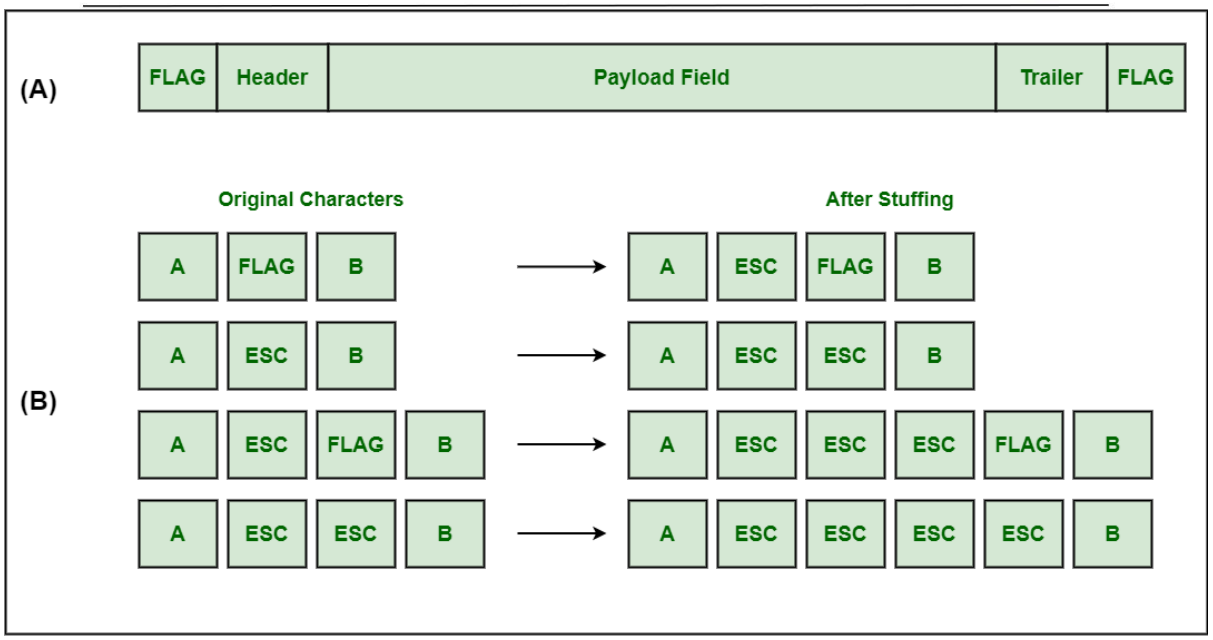
A Character Stream

(A) Without Errors
(B) With one Error

Character Stuffing :

Character stuffing is also known as byte stuffing or character-oriented framing and is same as that of bit stuffing but byte stuffing actually operates on bytes whereas bit stuffing operates on bits. In byte stuffing, special byte that is basically known as ESC (Escape Character) that has predefined pattern is generally added to data section of the data stream or frame when there is message or character that has same pattern as that of flag byte.

But receiver removes this ESC and keeps data part that causes some problems or issues. In simple words, we can say that character stuffing is addition of 1 additional byte if there is presence of ESC or flag in text.



A Character Stuffing
(A) A frame delimited by flag bytes
(B) Four examples of byte sequences before and after byte stuffing

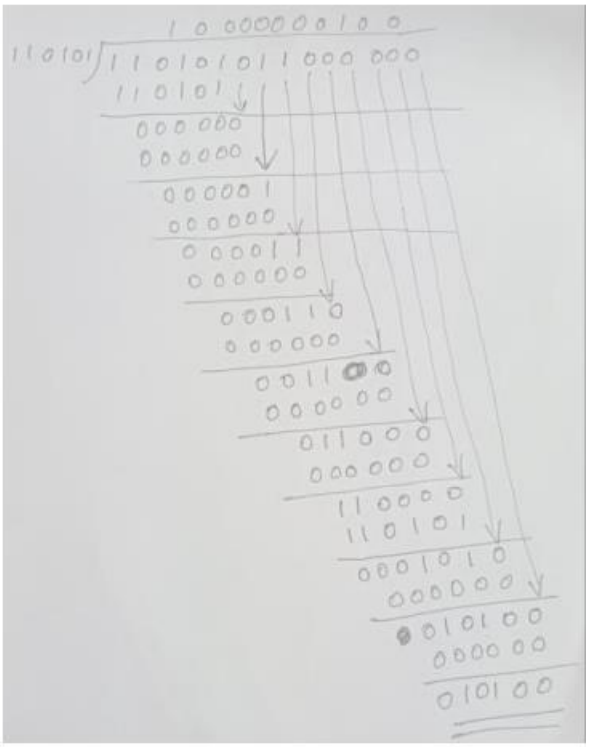
Bit Stuffing:
Bit stuffing is also known as bit-oriented framing or bit-oriented approach. In bit stuffing, extra bits are being added by network protocol designers to data streams. It is generally insertion or addition of extra bits into transmission unit or message to be transmitted as simple way to provide and give signaling information and data to receiver and to avoid or ignore appearance of unintended or unnecessary control sequences.
It is type of protocol management simply performed to break up bit pattern that results in transmission to go out of synchronization. Bit stuffing is very essential part of transmission process in network and communication protocol. It is also required in USB.

a) 00000100 01000111 11100011 11100000 01111110
b) 01111110 01000111 11100011 11100000 11100000 11100000 01111110 01111110
c) 01111110 01000111 110100011 11100000 011111010 0111110

7. Identify why Data link protocols always put theCRC in a trailer rather than in a header. Given the data words 1101010110, show generation of CRC at sender site by using the devisor
110101.
Ans.
It is more efficient. Only one pass needs to be made over the packet as it computes the CRC while scanning the packet, and then outputs it at the end (trailer). If the CRC were in the header, then two passes would be necessary - one to compute the CRC, and one more to append it to the front of the packet.
placing the CRC at the end of a frame reduces packet latency and reduces hardware buffering requirements. On the transmit side, hardware can read and transmit bytes of the frame

immediately. The transmitter calculates the CRC on the fly as data passes through, then simply appends the CRC the tail of the frame.

Consider the alternative where the CRC comes somewhere in the Ethernet header. Hardware must read and store the entire frame in order to calculate the CRC. This amounts to a large look-ahead operation and adds significantly to transmit latency and hardware cost. The situation also becomes more complex for the receiver as well



8.In SR protocol, suppose frames through 0 to 4have been transmitted. Now, imagine that frame:0 times-out, 5 (a new frame) is transmitted, frame:1 times-out, frame:2 times-out and 6 (another new frame) is transmitted.

At this point, what will be the outstandingpackets in sender's window?
On the basis of above example Justify selective repeat (SR) is better than Go BackN.
Ans.

Step-01:

Frames through 0 to 4 have been transmitted-

4 , 3 , 2 , 1 , 0

Step-02:

0 times out. So, sender retransmits it-

0 , 4 , 3 , 2 , 1

Step-03:

5 (a new frame) is transmitted-

5 , 0 , 4 , 3 , 2 , 1

Step-04:

1 times out. So, sender retransmits it-

1 , 5 , 0 , 4 , 3 , 2

Step-05:

2 times out. So, sender retransmits it-

2 , 1 , 5 , 0 , 4 , 3

Step-06:

6 (another new frame) is transmitted-

6 , 2 , 1 , 5 , 0 , 4 , 3

Ans. 3405126

9. Summarize in detail about Classful addressing anduse of subnetting. Find the class of each address.

i. 00000001 00001011 00001011 11101111
ii. 11000001 10000011 00011011 11111111
iii. 14.23.120.8
iv. 252.5.15.111

Ans.

Classful Addressing

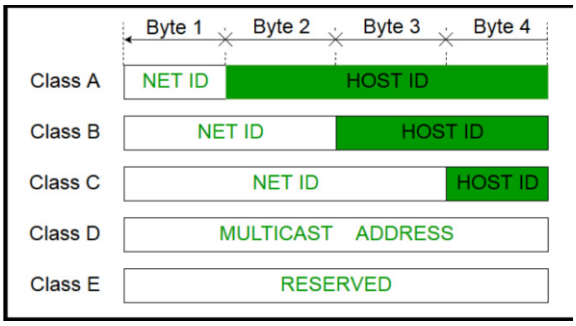
The 32-bit IP address is divided into five sub-classes. These are:

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

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the classes of the IP address.
The IPv4 address is divided into two parts:

- Network ID
- Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns an IP address to each device that is connected to its network.



Class A

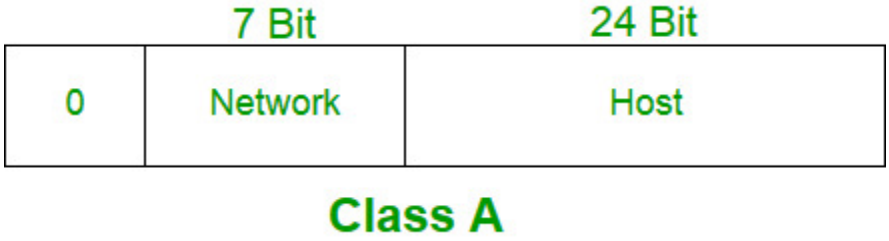
IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

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

The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for Class A is 255.x.x.x. Therefore, class A has a total of:

- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.0.0.0 – 126.255.255.255.



Class A

Class B

IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.0.0 – 191.255.255.255.

Class B

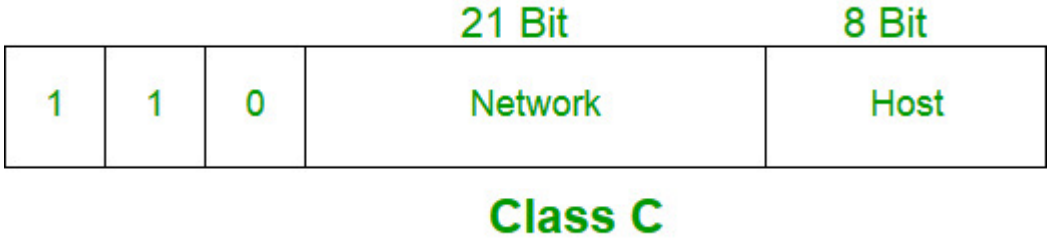
Class C

IP addresses belonging to class C are assigned to small-sized networks.

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

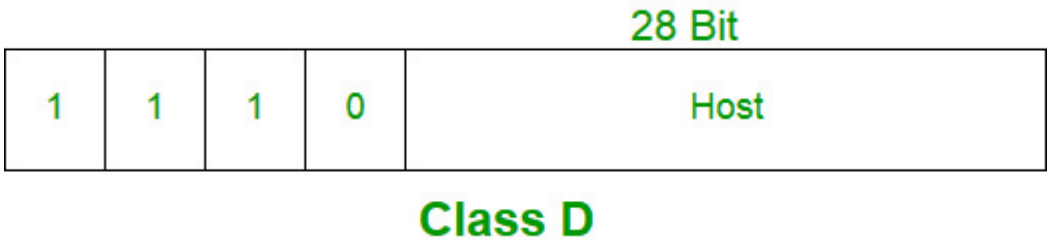
The higher-order bits of the first octet of IP addresses of class C is always set to 110. The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address



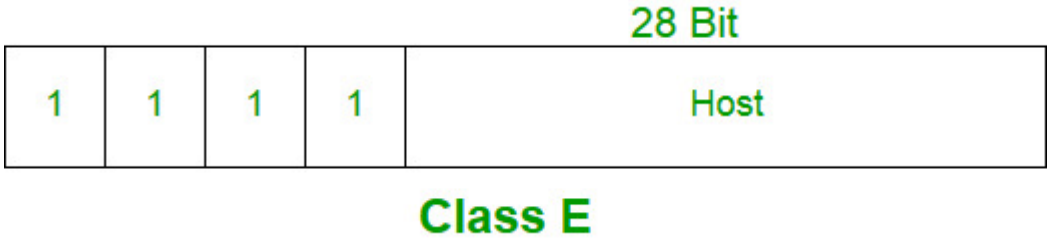
Class D

- IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.
- Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.



Class E

- IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



use of subnetting

•Reducing traffic and improving network performance by dividing broadcast domains and routing traffic efficiently.

•Increasing network security by isolating different subnets from each other and preventing unauthorized access.

•Providing different network priorities to different subnets based on their needs and functions.

•Simplifying network maintenance and administration for small networks.

Large enterprises looking to expand technologically need to know how to organize a network efficiently. IP addresses can be kept geographically confined, allowing a subnet to be used to preserve efficiency and order. Let's look at some of the major motivations for using subnetting.

1.**Reallocating IP Addresses:** - A limited number of host allocations are available for each class; for example, networks with more than 254 devices require a Class B allocation. Suppose a network administrator works with a Class B or C network and needs to allocate 150 hosts across three physical networks in three different cities. In that case, they must either request more address blocks for each network or divide the network into subnets that allow administrators to use one block of addresses across multiple physical networks.

2.**Improves Network Speed**: - Subnetting divides the large network into small subnets, and the purpose of these subnets is to divide a huge network into a collection of smaller, interconnected networks to reduce traffic. Subnets eliminate the need for traffic to pass through extraneous routs, resulting in faster network speeds.

3.**Improving Network Security**: - Subnetting helps network administrators to reduce network-wide threats by quarantining compromised areas of the network and making it more complex for trespassers to travel throughout an organization's network.

4.**Reliving Network Congestion**: - If a large portion of an organization's traffic is intended to be shared regularly across a group of computers, putting them all on the same subnet can help reduce network traffic. Without a subnet, data packets from every other computer on the network would be visible to all computers and servers.

5.**Efficiency**: - Subnetting is used to simplify network traffic by eliminating the need for additional routers. This ensures that the data being sent can move as quickly as possible to its destination, avoiding any potential detours that can slow it down**.**

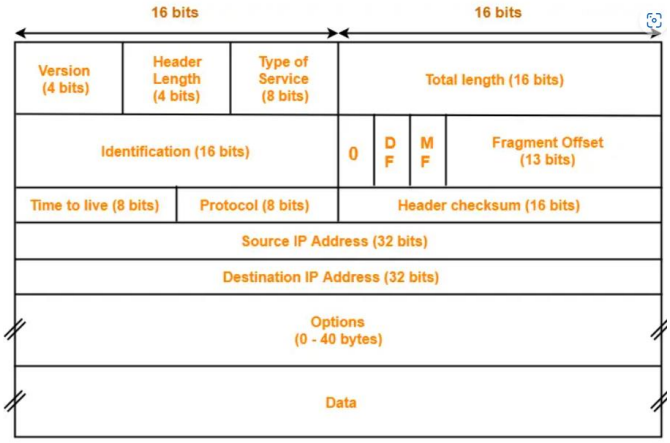
i. The first bit is 0. This is a class A address.
ii. The first 2 bits are 1, third bit is 0..This is a class C address
iii. The first byte is 14, the class is A.
iv. The first byte is 252, the class is E.

10.Demonstrate IPV4 header format and solve thequestions below.

i. An IP packet has arrived with the first 8bits as shown: 01000010.The receiver discards the packet. Why?

ii. A packet has arrived in which the offsetvalue is 100. What is the number of the first byte? Do we know the number of the last byte? Justify your answer.

Ans.



IPv4 Header

- IPv4 short for Internet Protocol Version 4 is the fourth version of the **Internet Protocol** (IP).
- IP is responsible to deliver data packets from the source host to the destination host.
- This delivery is solely based on the **IP Addresses** in the packet headers.
- IPv4 is the first major version of IP.
- IPv4 is a connectionless protocol for use on **packet-switched networks**.

1.**Version**-

- Version is a 4 bit field that indicates the IP version used.
- The most popularly used IP versions are version-4 (IPv4) and version-6 (IPv6).
- Only IPv4 uses the above header.
- So, this field always contains the decimal value 4

2.Header Length

- Header length is a 4 bit field that contains the length of the IP header.
- It helps in knowing from where the actual data begins

Minimum And Maximum Header Length

- The initial 5 rows of the IP header are always used.
- So, minimum length of IP header = 5 x 4 bytes = 20 bytes.
- The size of the 6th row representing the Options field vary.
- The size of Options field can go up to 40 bytes.
- So, maximum length of IP header = 20 bytes + 40 bytes = 60 bytes.

Concept of Scaling Factor-

- Header length is a 4 bit field.
- So, the range of decimal values that can be represented is [0, 15].
- But the range of header length is [20, 60].
- So, to represent the header length, we use a scaling factor of 4.

In general,

Header length = Header length field value x 4 bytes

3. Type Of Service

- Type of service is a 8 bit field that is used for Quality of Service (QoS).
- The datagram is marked for giving a certain treatment using this field

3. **Total Length-**

- Total length is a 16 bit field that contains the total length of the datagram (in bytes).

Total length = Header length + Payload length

- Minimum total length of datagram = 20 bytes (20 bytes header + 0 bytes data)
- Maximum total length of datagram = Maximum value of 16 bit word = 65535 bytes

4. **Identification-**

- Identification is a 16 bit field.
- It is used for the identification of the fragments of an original IP datagram.

When an IP datagram is fragmented,

- Each fragmented datagram is assigned the same identification number.
- This number is useful during the re assembly of fragmented datagrams.
- It helps to identify to which IP datagram, the fragmented datagram belongs to.

5. DF Bit-

- DF bit stands for Do Not Fragment bit.
- Its value may be 0 or 1.

When DF bit is set to 0,

- It grants the permission to the intermediate devices to fragment the datagram if required.

When DF bit is set to 1,

- It indicates the intermediate devices not to fragment the IP datagram at any cost.
- If network requires the datagram to be fragmented to travel further but settings does not allow its fragmentation, then it is discarded.

- An error message is sent to the sender saying that the datagram has been discarded due to its settings

6. MF Bit-

- MF bit stands for More Fragments bit.
- Its value may be 0 or 1.

When MF bit is set to 0,

- It indicates to the receiver that the current datagram is either the last fragment in the set or that it is the only fragment.

When MF bit is set to 1,

- It indicates to the receiver that the current datagram is a fragment of some larger datagram.
- More fragments are following.
- MF bit is set to 1 on all the fragments except the last one.

8.Fragment Offset-

- Fragment Offset is a 13 bit field.
- It indicates the position of a fragmented datagram in the original unfragmented IP datagram.
- The first fragmented datagram has a fragment offset of zero.

Fragment offset for a given fragmented datagram
= Number of data bytes ahead of it in the original unfragmented datagram

9.Time To Live-

- Time to live (TTL) is a 8 bit field.
- It indicates the maximum number of hops a datagram can take to reach the destination.
- The main purpose of TTL is to prevent the IP datagrams from looping around forever in a routing loop.

The value of TTL is decremented by 1 when-

- Datagram takes a hop to any intermediate device having network layer.
- Datagram takes a hop to the destination.

If the value of TTL becomes zero before reaching the destination, then datagram is discarded.

10. Protocol-

Protocol is a 8 bit field.

It tells the network layer at the destination host to which protocol the IP datagram belongs to.

In other words, it tells the next level protocol to the network layer at the destination side.

Protocol number of ICMP is 1, IGMP is 2, TCP is 6 and UDP is 17.

11. Header Checksum-

- Header checksum is a 16 bit field.
- It contains the checksum value of the entire header.
- The checksum value is used for error checking of the header.

At each hop,

- The header checksum is compared with the value contained in this field.
- If header checksum is found to be mismatched, then the datagram is discarded.
- Router updates the checksum field whenever it modifies the datagram header.

The fields that may be modified are-

1. TTL
2. Options
3. Datagram Length
4. Header Length
5. Fragment Offset

12. Source IP Address-

- Source IP Address is a 32 bit field.
- It contains the logical address of the sender of the datagram.

13. Destination IP Address-

- Destination IP Address is a 32 bit field.
- It contains the logical address of the receiver of the datagram.

14. Options-

- Options is a field whose size vary from 0 bytes to 40 bytes.
- This field is used for several purposes such as-

1. Record route
2. Source routing
3. Padding

i. There is an error in this packet. The 4 left-most bits (0100) show the version, which is correct. The next 4 bits (0010) show the wrong header length ($2 \times 4 = 8$). The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

ii. To find the number of the first byte, we multiply the offset value by 8. This means that the first byte number is 800. We cannot determine the number of the last byte unless we know the length of the data