1. Define IP address. Write down characteristics of IPv4.

IP address stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information. An IP address allows information to be sent and received by the correct parties, which means it can also be used to track down a user's physical location in some instances. IP addresses are generated through a hierarchical system involving the IANA, RIRs and ISPs.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

2. Calculate class wise total number of networks and hosts for networks.

In class A, the network length is 8 bits, but since the first bit, which is 0, defines the class, we can have only seven bits as the network identifier. This means there are only 2^7 -2 = 126 networks and 16777214 hosts (2^{24}-2).

In class B, the network length is 16 bits, but since the first two bits, which are $(10)_2$, define the class, we can have only 14 bits as the network identifier. This means there are only 2^{14} = 16,384 networks and 65534 (2^{16}-2) Host addresses.

All addresses that start with (110)2 belong to class C. In class C, the network length is 24 bits, but since three bits define the class, we can have only 21 bits as the network identifier. This means there are 2^{21} = 2,097,152 networks and 254 (28-2) Host addresses.

Class D is not divided into prefix and suffix. It is used for multicast addresses. All addresses that start with 1110 in binary belong to class D.

As in Class D, Class E is not divided into prefix and suffix and is used as reserve.

3. **Differentiate between class full and class less IP.**

Parameter	Classful Addressing	Classless Addressing
Basics	In Classful addressing IP addresses are allocated according to the classes- A to E.	Classless addressing came to replace the classful addressing and to handle the issue of rapid exhaustion of IP addresses.
Practical	It is less practical.	It is more practical.
Network ID and Host ID	The changes in the Network ID and Host ID depend on the class.	There is no such restriction of class in classless addressing.
VLSM	It does not support the Variable Length Subnet Mask (VLSM).	It supports the Variable Length Subnet Mask (VLSM).
Bandwidth	Classful addressing requires more bandwidth. As a result, it becomes slower and more expensive as compared to classless addressing.	It requires less bandwidth. Thus, fast and less expensive as compared to classful addressing.
CIDR	It does not support Classless Inter-Domain Routing (CIDR).	It supports Classless Inter-Domain Routing (CIDR).
Updates	Regular or periodic updates	Triggered Updates
Troubleshooting and Problem detection	Troubleshooting and problem detection are easy than classless addressing because of the division of network, host and subnet parts in the address.	It is not as easy compared to classful addressing.
Division of Address	• Network • Host • Subnet	• Host • Subnet

4. Define public IP, private IP, Loopback address and broadcast address.

i. **Public IP Address**:

A public IP address is an address that is globally unique on the internet. It is assigned by an Internet Service Provider (ISP) or an organization's network administrator. Public IP addresses are used to identify devices on the public internet and are routable across the internet.

ii. **Private IP Address**:

A private IP address is an address that is used within a private network, such as a home or office network, and is not directly accessible from the internet. Private IP addresses are reserved for internal use and are typically assigned to devices within a network by a router or DHCP server. They are defined in RFC 1918 and include ranges such as 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.

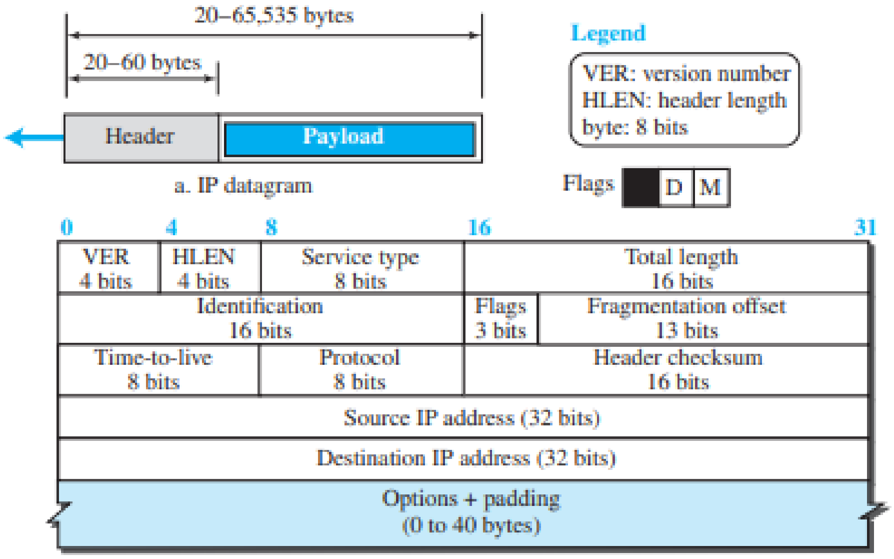
iii. **Loopback Address**:

The loopback address is a special IP address that represents the local device itself. It allows a device to send packets to itself for testing and diagnostic purposes. In IPv4, the loopback address is 127.0.0.1, and in IPv6, it is typically represented as ::1. It is often used for troubleshooting network configurations and testing network services running on the local machine.

iv. **Broadcast Address**:

The broadcast address is an address used to send data packets to all devices within a specific network segment. In IPv4, the broadcast address is typically the highest address in the network range, with all host bits set to 1 (e.g., 192.168.1.255 in a /24 network). In IPv6, the concept of broadcast addresses is replaced by multicast addresses. Broadcast addresses are used for tasks like network discovery, DHCP (Dynamic Host Configuration Protocol), and ARP (Address Resolution Protocol) resolution in IPv4 networks.

5. **Explain IP datagram format with block diagram**.



a. IP datagram

b. Header

A datagram is a variable-length packet consisting of two parts: header and payload (data). The header is 20 to 60 bytes in length and contains information essential to routing and delivery. It is customary in TCP/IP to show the header in 4-byte sections.

Version Number. The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, obviously, has the value of 4.

Header Length. The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header. When a device receives a datagram, it needs to know when the header stops and the data, which is encapsulated in the packet, starts.

Service Type field is used to set priorities or precedence for data transmission. The size of the field is 8 bits. This field is also used to determine the type of service that is required for a particular application. The priority is set using the first three bits and the service type is set using the next three bits. The last two bits are reserved for future use.

Total Length: This 16-bit field defines the total length (header plus data) of the IP datagram in bytes. A 16-bit number can define a total length of up to 65,535 (when all bits are 1s). However, the size of the datagram is normally much less than this. This field helps the receiving device to know when the packet has completely arrived. Length of data = total length − (HLEN) × 4

Identification (16 bits): Used to uniquely identify each datagram within the current session. This field is primarily used for reassembly at the destination in case the datagram is fragmented during transmission.

Fl**ags (3 bits) and Fragment Offset (13 bits):** Flags are used to control fragmentation. The three flags are:

- Bit 0: Reserved, must be zero.
- Bit 1: Don't Fragment (DF)
- Bit 2: More Fragments (MF)

The Fragment Offset field indicates the offset of the fragment relative to the original unfragmented datagram.

Time-to-live. Due to some malfunctioning of routing protocols (discussed later) a datagram may be circulating in the Internet, visiting some networks over and over without reaching the destination. This may create extra traffic in the Internet. The time-to-live (TTL) field is used to control the maximum number of hops (routers) the packet is allowed to traverse before being discarded. It prevents packets from looping indefinitely in the network.

Protocol: It specifies the protocol used in the data portion of the datagram (e.g., TCP, UDP, ICMP). The Internet authority has given any protocol that uses the service of IP a unique 8-bit number which is inserted in the protocol field. When the payload is encapsulated in a datagram at the source IP, the corresponding protocol number is inserted in this field; when the datagram arrives at the destination, the value of this field helps to define to which protocol the payload should be delivered.

Header Checksum: The Header Checksum field contains the checksum, which is used by the destination to check for the integrity of the transmitted data by applying an algorithm on the IP header. The size of this field is 16 bits.
The Header Checksum value is calculated by the sender and is sent along with the IP header.

Source Address: The Source Address or the Source IP Address field is 32 bits long and is used to identify the sender of the data. This field is used to redirect error messages to the source in case the datagram is discarded before reaching the destination. The address that is specified in this field represents the originator of the message.

Destination Address: The Destination Address or the Destination IP Address field is 32 bits long. This field specifies the final destination of a data packet. However, this field does not provide information about the intermediate devices through which a data packet passes.

Options (if any): Optional field that may include additional information or control parameters, such as timestamp, record route, or security options.

Padding (if necessary): The IP header may be padded with zeros to ensure that the header length is a multiple of 32 bits.

6. Define IP routing. Explain routing algorithms.

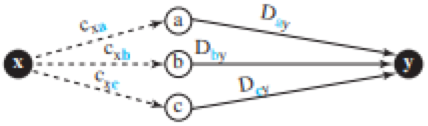
IP routing is the process of forwarding data packets from one network to another network based on their destination IP addresses. Routers are devices responsible for performing this task in computer networks. When a router receives a packet, it examines the destination IP address and consults its routing table to determine the best path or next-hop router to reach that destination. The router then forwards the packet to the appropriate interface for transmission towards its destination.

Routing algorithms are the algorithms used by routers to determine the best path for forwarding packets through a network. There are several routing algorithms such as:

a. Distance Vector Algorithm

The distance-vector (DV) routing uses the goal to find the best route. In distance-vector routing, the first thing each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbors. The incomplete trees are exchanged between immediate neighbors to make the trees more and more complete and to represent the whole internet.

The heart of distance-vector routing is the famous **Bellman-Ford equation**. This equation is used to find the least cost (shortest distance) between a source node, x, and a destination node, y, through some intermediary nodes (a, b, c, . . .) when the costs between the source and the intermediary nodes and the least costs between the intermediary nodes and the destination are given. The following shows the general case in which Dij is the shortest distance and cij is the cost between nodes i and j.



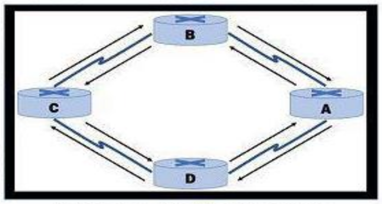
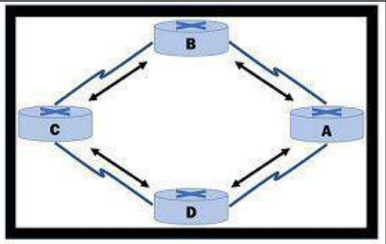
a. General case with three intermediate nodes

Dxy = min{(cxa + Day), (cxb + Dby), (cxc + Dcy), …}

b. Linked-State Routing

Link-state routing algorithms involve routers exchanging information about the state of their links with all other routers in the network. Each router constructs a complete topological map of the network, called a Link-State Database (LSDB). Using this map, routers compute the shortest path to each destination using algorithms like Dijkstra's shortest path algorithm. A routing algorithm that directly follows our discussion for creating least-cost trees and forwarding tables is link-state (LS) routing. This method uses the term link-state to define the characteristic of a link (an edge) that represents a network in the internet. Examples include the Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) protocols. Benefits include faster convergence and loop-free paths.

7. Differentiate between Link-State routing and Distance Vector Routing.

S.No.	Distance Vector Routing	Link State Routing
1.	Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
2.	Based on local knowledge, since it updates table based on information from neighbours.	Based on global knowledge, it have knowledge about entire network.
3.	Make use of Bellman Ford Algorithm.	Make use of Dijakstra's algorithm.
4.	Traffic is less.	Traffic is more.
5.	Converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.
6.	Count of infinity problem.	No count of infinity problem.
7.	Persistent looping problem i.e, loop will be there forever.	No persistent loops, only transient loops.
8.	Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.
	 Distance Vector Routing	 Link State Routing

8. **List and explain routing protocols.**
Routing protocols are sets of rules used by routers to determine the best paths for forwarding packets through a network. These protocols enable routers to exchange routing information, update routing tables, and make dynamic decisions about packet forwarding. Here are some common routing protocols along with brief explanations:

i. Routing Information Protocol (RIP):

RIP is one of the oldest distance-vector routing protocols. It uses hop count as the metric to measure the distance to a destination. RIP routers broadcast their entire routing tables to their neighboring routers every 30 seconds. RIP is simple to configure and deploy but is limited in scalability and convergence speed.

ii. Open Shortest Path First (OSPF):

OSPF is a link-state routing protocol designed for IP networks. It uses Dijkstra's shortest path first algorithm to calculate the best path to each destination. OSPF routers exchange link-state advertisements (LSAs) to build a complete map of the network topology. OSPF supports hierarchical design and route summarization, making it scalable and efficient in large networks.

iii. Border Gateway Protocol (BGP):

BGP is the primary routing protocol used on the Internet for interdomain routing. It is a path vector protocol that considers policies and path attributes when selecting routes. BGP routers exchange routing information, known as network reachability information (NLRI), with their neighboring routers. BGP allows for complex routing policies, traffic engineering, and route aggregation.

9. **Write short note on ARP, RARP, NAT.**

Sure, here's a brief overview of ARP, RARP, and NAT:

a. Address Resolution Protocol (ARP):

ARP is a protocol used to map IP addresses to MAC addresses on a local network. When a device needs to communicate with another device on the same network, it first checks its ARP cache (a table of IP-MAC address mappings). If the destination IP address is not in the ARP cache, the device sends out an ARP request broadcast asking "Who has this IP address?" The device with the corresponding IP address responds with its MAC address, and the sender updates its ARP cache with this mapping. ARP helps devices on the same network communicate efficiently by ensuring they have the necessary MAC address information for packet delivery.

b. Reverse Address Resolution Protocol (RARP)

RARP is the opposite of ARP; it's used to map MAC addresses to IP addresses. RARP was primarily used in diskless workstations to obtain their IP addresses from a server. A RARP request is sent by a device with only its MAC address to request its IP address from a RARP server. The RARP server responds with the corresponding IP address, allowing the device to configure its network settings. RARP has largely been replaced by more modern methods like DHCP (Dynamic Host Configuration Protocol) for dynamic IP address assignment.

c. Network Address Translation (NAT)

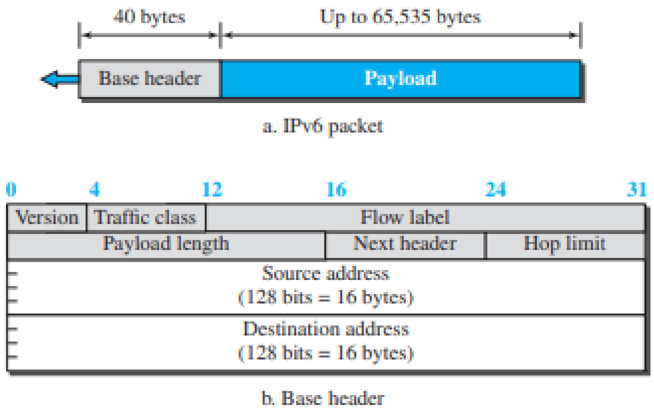
NAT is a technique used to modify network address information in IP packet headers while in transit across a router or firewall. NAT allows multiple devices within a private network to share a single public IP address for internet connectivity. When a device with a private IP address sends a packet to the internet, the router/firewall performing NAT replaces the private source IP address with its public IP address before forwarding the packet. The router maintains a NAT translation table to keep track of the mappings between private and public IP addresses. NAT helps conserve public IP address space and adds a layer of security by hiding the internal network structure from external entities. There are various types of NAT, including Static NAT, Dynamic NAT, and PAT (Port Address Translation), each serving different purposes in network address translation.

10.Write characteristics of IPv6 with its header format.

Characteristics of IPv6 are:

- **Expanded routing and addressing capabilities** – IPv6 increases the IP address size from 32 bits to 128 bits to support more levels of addressing hierarchy. In addition, IPv6 provides a greater number of addressable nodes.
- **Header format simplification** – Some IPv4 header fields have been dropped or have been made optional. This change reduces the common-case processing cost of packet handling. This change also keeps the bandwidth cost of the IPv6 header as low as possible, despite the increased size of the addresses.
- **Quality-of-service capabilities** – This capability enables the labeling of packets that belong to particular traffic **flows** for which the sender requests special handling. For example, the sender can request non-default quality of service or **real-time** service.
- **Authentication and privacy capabilities** – IPv6 includes the definition of extensions that provide support for authentication, data integrity, and confidentiality.

- **Auto-configuration** – IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.
- **Faster Forwarding/Routing** – Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.



a. IPv6 packet

b. Base header

- **Version**. The 4-bit version field defines the version number of the IP. For IPv6, the value is 6.
- **Traffic class**. The 8-bit traffic class field is used to distinguish different payloads with different delivery requirements. It replaces the type-of-service field in IPv4.
- **Flow label**. The flow label is a 20-bit field that is designed to provide special handling for a particular flow of data. We will discuss this field later.
- **Payload length**. The 2-byte payload length field defines the length of the IP datagram excluding the header. Note that IPv4 defines two fields related to the length: header length and total length. In IPv6, the length of the base header is fixed (40 bytes); only the length of the payload needs to be defined.
- **Next header**. The next header is an 8-bit field defining the type of the first extension header (if present) or the type of the data that follows the base header in the datagram. This field is similar to the protocol field in IPv4, but we talk more about it when we discuss the payload.
- **Hop limit**. The 8-bit hop limit field serves the same purpose as the TTL field in IPv4.
- **Source and destination addresses**. The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram. The destination address field is a 16-byte (128-bit) Internet address that identifies the destination of the datagram.

11. Differentiate between IPv4 and IPv6.

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
It can generate 4.29×109 address space	The address space of IPv6 is quite large it can produce 3.4×1038 address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
IPv4 supports VLSM(Variable Length subnet mask).	IPv6 does not support VLSM.
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

12.Explain types of IPv6.

a) **Unicast Address**: A unicast address defines a single interface (computer or router). The packet sent to a unicast address will be routed to the intended recipient.

b) **Anycast Address**: An anycast address defines a group of computers that all share a single address. A packet with an anycast address is delivered to only one member of the group, the most reachable one. An anycast communication is used, for example, when there are several servers that can respond to an inquiry. The request is sent to the one that is most reachable. The hardware and software generate only one copy of the request; the copy reaches only one of the servers. IPv6 does not designate a block for anycasting; the addresses are assigned from the unicast block.

c) **Multicast Address**: A multicast address also defines a group of computers. However, there is a difference between anycasting and multicasting. In anycasting, only one copy of the packet is sent to one of the members of the group; in multicasting each member of the group receives a copy. As we will see shortly, IPv6 has designated a block for multicasting from which the same address is assigned to the members of the group. It is interesting that IPv6 does not define broadcasting, even in a limited version. IPv6 considers broadcasting as a special case of multicasting.