1.Explain different network layer functions. – 5marks

2. Explain different network layer services

Ans:

- **Internetworking:** An important function of the network layer is to provide a logical connection between different types of networks.
- **Addressing:** Each device on the internet must be uniquely identified. This is similar to a telephone system. The address used at the network layer should uniquely and universally describe a computer's connection.
- **Routing:** Multiple routes can be chosen from a source to a destination. The network layer determines what route to take based on various factors.
- **Packetizing:** Packetizing is the process by which a network layer protocol called IP (Internetworking Protocol) encapsulates packets received from the upper layer protocol.
- **Fragmenting:** The datagram can travel through different networks. Each router decapsulates IP datagram from received frame. Then datagram is processed and encapsulated in another frame.

3. Explain different network layer design issues. – 5marks

Ans:

- Routing packets is a major design decision at the network layer. It determines how each packet is sent from one location to another.
- A route can be based on static tables or highly dynamic; packets can have a predefined route or be changed regularly.
- At some point, if too many packets are available in the subnet, they will get in each other's way, causing bottlenecks.
- The service quality at the network layer is determined by delays, transmission times, and jitter.
- Packets can encounter many problems during their transit from one network to another, such as one network may use a different addressing scheme than another.
- Different protocols are needed for two networks to communicate.

4. Explain the concept of connectionless and connection-oriented services. – 5marks

Ans:

S.NO	Connection-oriented Service	Connection-less Service
1.	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.

3.	Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
4.	Connection-oriented Service is feasible.	Connection-less Service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
7.	In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
8.	Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.
9.	Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)
10.	Connection-oriented requires authentication.	Connection-less Service does not require authentication.

5. Explain the concept of connectionless and connection-oriented protocol with example. – 5marks

Ans:

Connection-oriented	Connectionless
Establishes a dedicated connection before sending data	Doesn't establish a dedicated connection before sending data
More reliable	Faster
Performs handshaking	Doesn't perform handshaking
Data is delivered in the same order the sender has sent them	No guarantee that the data is delivered in order
Performs flow control and error checking	Doesn't perform flow control or error checking

6.List and explain different types of addresses used in IPV4?– 5marks (repeated question)

7.Explain IPV4 classful addressing and state its disadvantages.

8.Explain classful addressing

- Ans: **Class A:** It uses an 8-bit network number whose first bit is always zero, as shown in the table. It is reserved for IP unicast addresses. If the number of hosts is huge on a network, this class is used. It uses only one octet to define prefix length. The numbers of the network, which can accommodate, are 2^8 or 128

- **Class B:** It facilitates 16 bits for both the network address and host address. The first two bits are continually 10. It is distant from IP unicast addresses. It uses 2 octets for a specific network, while the remaining two octets for host IDs. They are mainly used for medium to large-sized networks. The Class B addresses can be supported to 16,384 networks with up to 65,536 hosts per network.
- **Class C:** It is distant for IP unicast addresses. They are defined as small networks. The first 3 octets determine a specific network, and the last octet specifies host IDs. The Class C addresses can be used up to 2,097,152 networks with up to 254 hosts per network. Its first three bits are continually set to 110.
- **Class D:** It defines IP multicast addresses.
- **Class E:** These addresses were reserved for practical uses.

9.Explain in short subnetting – 5marks

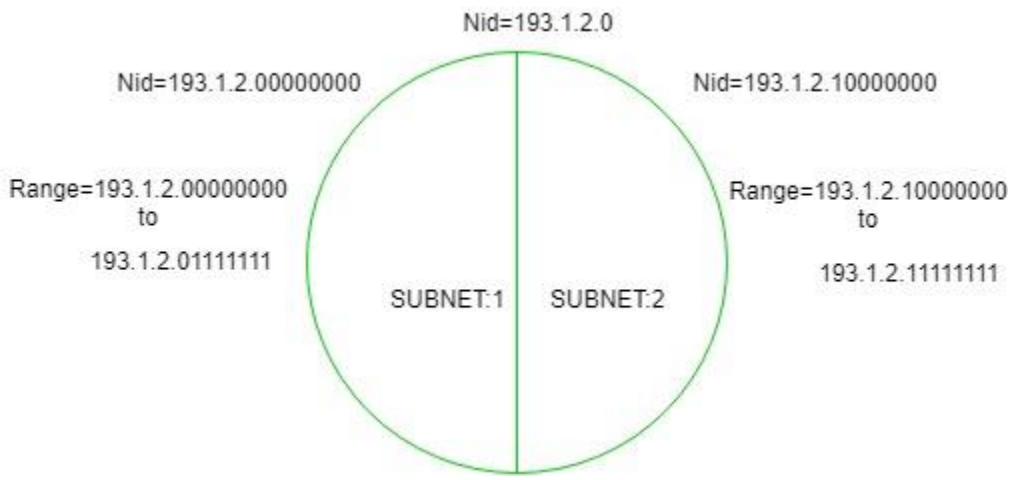
Ans:

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 2^{24} for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.

Uses of Subnetting

1. Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
2. Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
3. Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
4. Subnetting is used in increasing network security.

The network can be divided into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets.

10. An ISP is granted a block of addresses starting with 150.80.0.0/16. The ISP wants to distribute these blocks to 2600 customers as follows. – 10marks

Ans:

a. The first group has 200 medium-size businesses; each needs 128 addresses.

b. The second group has 400 small businesses; each needs 16 addresses.

c. The third group has 2000 households; each needs 4 addresses.

Design the sub-blocks and give the slash notation for each sub-block. Find out how many addresses are still available after these allocations.

Ans:

For 128 addresses we use /25 mask. 255.255.255.128Group 1 has 200 medium size businesses150.80.0.0 /25 Subnet 1

150.80.0.128 /25 Subnet 2

150.80.1.0 /25….150.80.1.128 /25 Subnet 3

……..Subnet 100

--->150.80.99.128 /25 upto 150.80.99.255

Next address is 150.80.100.0

b. Group 2 has 400 small businesses, each needs 16 addresses…..we use /28 mask or 255.255.255.240150.80.100.0 /28 Subnet 1

150.80.100.16 /28 Subnet 2

150.80.100.240 /28 Subnet 16

……150.80.124.240 /28 Subnet 400 [400/16=25]

Next address is 150.80.125.0

c. Group 3 has 2000 households each needs 4 addresses.For 4 addresses we use /30 mask or

255.255.255.252150.80.125.0 /30 Subnet 1

150.80.125.4 /30 Subnet 2

150.80.125.252 /30 Subnet 64

150.80.155.252 /30 Subnet 1984

31*64=1984

150.80.156.0 /30 Subnet 1985

150.80.156.60 /30 Subnet 2000

Next address available from 150.80.156.64

We have used 40000 addresses out of 65536 addresses. 25536 addresses remain available.

11.Explain classless inter domain routing (CIDR). – 10 marks

Ans: Classless Inter-Domain Routing (CIDR) is a method of IP address allocation and IP routing that allows for more efficient use of IP addresses. CIDR is based on the idea that IP addresses can be allocated and routed based on their network prefix rather than their class, which was the traditional way of IP address allocation.
CIDR addresses are represented using a slash notation, which specifies the number of bits in the network prefix. For example, an IP address of 192.168.1.0 with a prefix length of 24 would be represented as 192.168.1.0/24. This notation indicates that the first 24 bits of the IP address are the network prefix and the remaining 8 bits are the host identifier.
Advantages:

- Efficient use of IP addresses: CIDR allows for more efficient use of IP addresses, which is important as the pool of available IPv4 addresses continues to shrink.
- Flexibility: CIDR allows for more flexible allocation of IP addresses, which can be important for organizations with complex network requirements.
- Better routing: CIDR allows for more efficient routing of IP traffic, which can lead to better network performance.
  Reduced administrative overhead: CIDR reduces administrative overhead by allowing for easier management of IP addresses and routing.

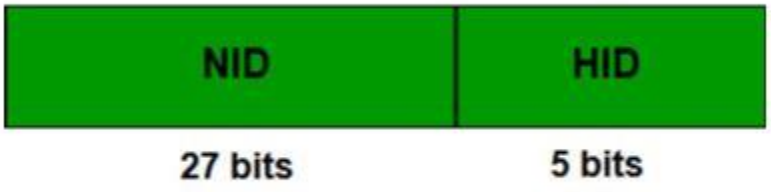
Disadvantages:

- Complexity: CIDR can be more complex to implement and manage than traditional class-based addressing, which can require additional training and expertise.
- Compatibility issues: Some older network devices may not be compatible with CIDR, which can make it difficult to transition to a CIDR-based network.
- Security concerns: CIDR can make it more difficult to implement security measures such as firewall rules and access control lists, which can increase security risks.
- Overall, CIDR is a useful and efficient method of IP address allocation and routing, but it may not be suitable for all organizations or networks. It is important to weigh the advantages and disadvantages of CIDR and consider the specific needs and requirements of your network before implementing CIDR

CIDR, or Classless Inter-Domain Routing, is a networking technique introduced to overcome the limitations of the traditional IP addressing system, which was based on classes. CIDR allows more flexible allocation of IP addresses by eliminating the strict class-based divisions.
Rules for forming CIDR Blocks:

1. All IP addresses must be contiguous.
2. Block size must be the power of 2 (2n). If the size of the block is the power of 2, then it will be easy to divide the Network. Finding out the Block Id is very easy if the block size is of the power of 2. Example: If the Block size is 25 then, Host Id

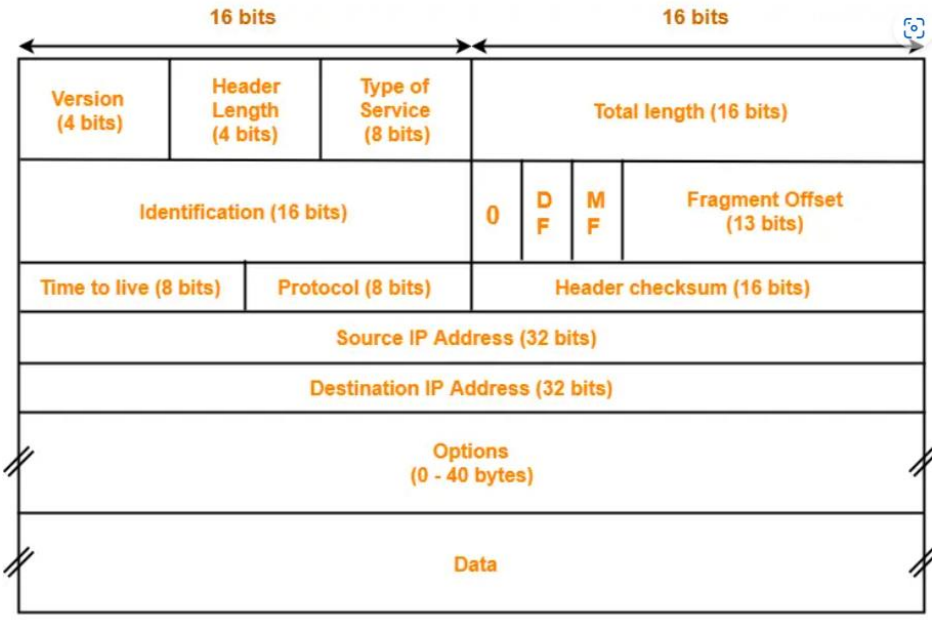
will contain 5 bits and Network will contain 32 – 5 = 27 bits.



3. First IP address of the Block must be evenly divisible by the size of the block. in simple words, the least significant part should always start with zeroes in Host Id. Since all the least significant bits of Host Id is zero, then we can use it as Block Id part.

12. Draw and explain ipv4 header. – 10 marks (repeated question)

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

4. **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

5. **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.

6. 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

7. 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-

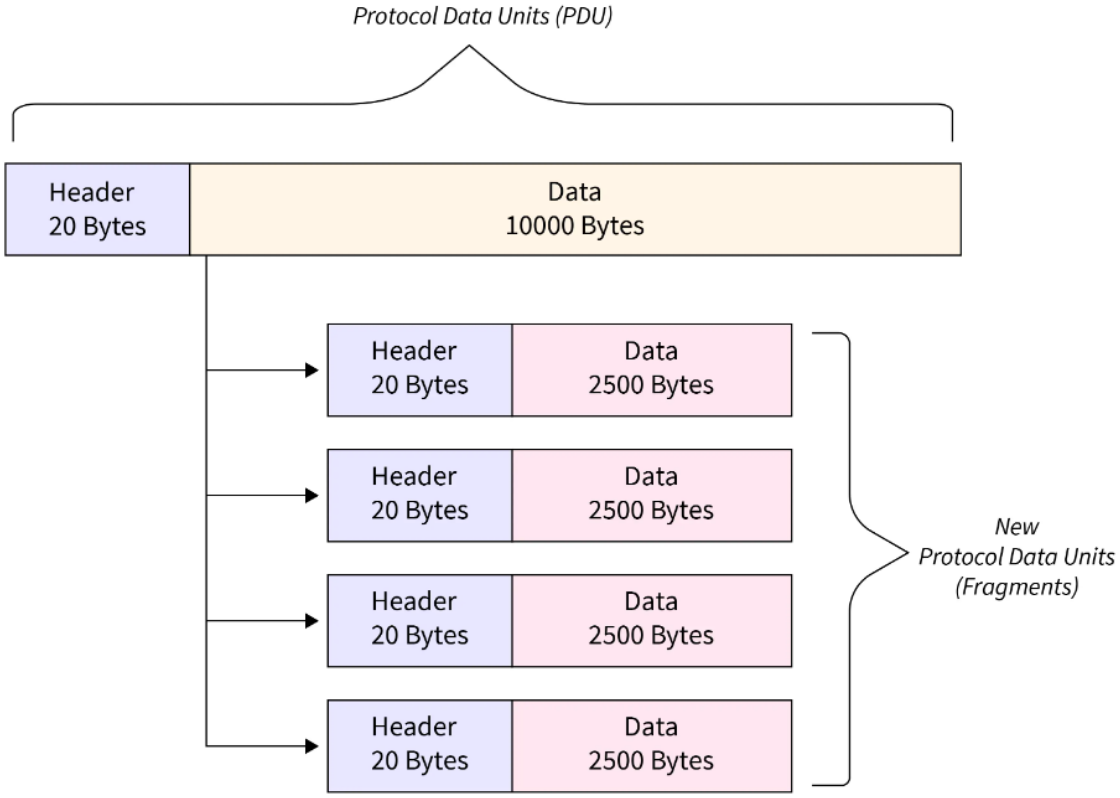
1. Record route
2. Source routing
3. Padding

13. Explain the purpose of fragmentation of packet and how it is done. – 10 marks

Ans: The datagram generated by the network layer at the source computer must traverse many networks before arriving at the destination computer. Typically, the source computer favors sending large datagrams. This is because if the datagram is broken up into smaller pieces, the header will be repeated for each datagram unit. The header is repeated for every fragmented datagram, wasting network bandwidth.

However, each network has a cap on the largest packet size it can send during this occurrence. Even worse, the source computer is unaware of the packet's route to get to its destination. It cannot, therefore, determine how small each fragmented datagram must be. The reasons for fragmenting a large datagram into a small fragmented datagram are listed below:

The capacity of data is limited by the hardware and operating system employed.
Conformity with national and international norms.
Each network's protocols allow for different packet sizes.
Large packets occupy the network for a longer time than small packets.
Reduce the mistakes caused by retransmission.



An IP packet cannot be larger than the maximum size allowed by that local network when sent over the network by a host. The network's data link and IP Maximum Transmission Units (MTUs), which are typically the same, determine its size. 1500 byte MTUs are standard for modern Ethernet-based office, campus, or data center networks.

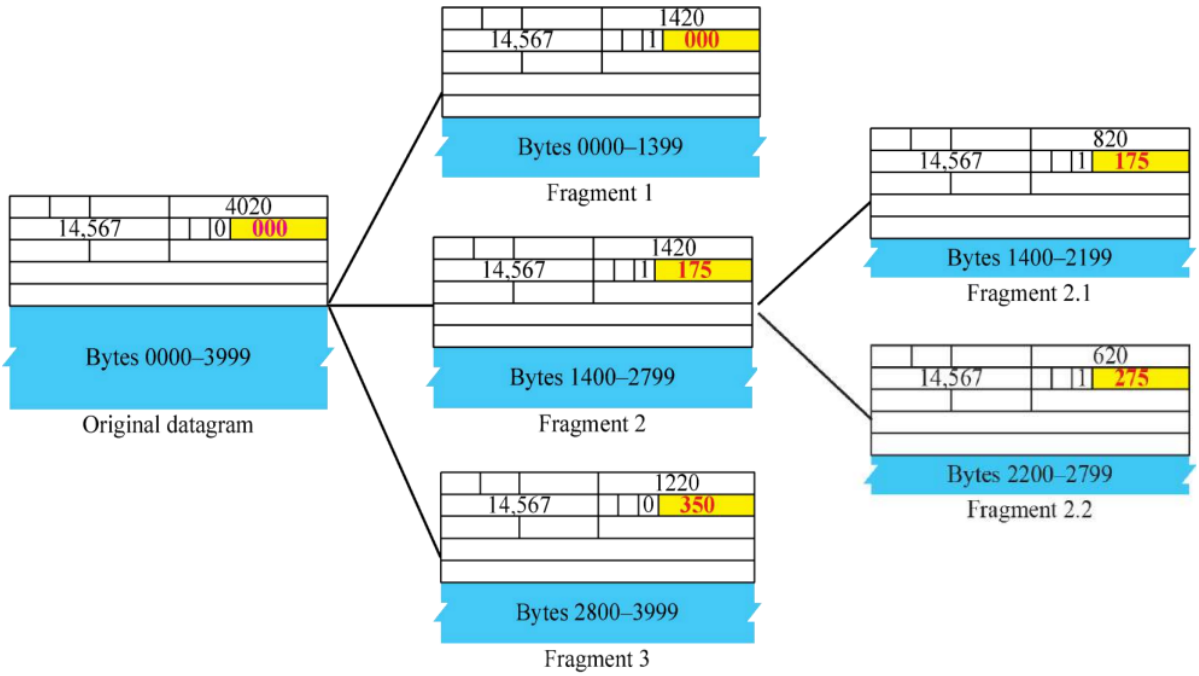
However, packets initially delivered across a network with one MTU may need to be routed over networks with a smaller MTU (such as a WAN or VPN tunnel). If the packet size in these circumstances is greater than the lower MTU, the data in the packet must be fragmented (if possible). This indicates that it is divided into fragments carried in brand-new packets (fragments) that are equal to or less than the lower MTU. This is known as fragmentation, and when the fragments arrive at their destination, the data is usually put back together.

- The maximum size of an IP datagram is $216-1=65,535_{216}-1=65,535$ bytes, as the IP header has a total length of 16 bits.
- It is performed by the network layer at the destination side, typically at routers.

- Due to intelligent (*excellent*) segmentation by the transport layer, the source side does not require fragmentation. Specifically, the transport layer looks at the datagram and frame data limits and segments the data so that it can easily fit in a frame without the need for fragmentation.
- The receiver uses the identification (16 bits) field in the IP header to identify the packet. The identification number for each frame fragment is the same.
- The receiver uses the fragment offset(13 bits) field in the IP header to identify the series of frames.
- The extra header created by fragmentation results in overhead at the network layer.

Fields in IP Header for Fragmentation

- Identification Field (16 bits):- It is used to recognize fragments of the same frame.
- Fragment Offset Field (13 bits):- It is used to determine the sequence of pieces in the frame. It often denotes the number of data bytes preceding or preceding the fragment. Maximum fragment offset possible = (65535−20)=65515(65535−20)=65515, where 65535 is the maximum datagram size, and 20 is the minimum IP header size. As a result, a fragment offset requires ciel(log265515)=16ceil(log265515)=16 bits, yet the fragment offset field only has 13 bits. So, to efficiently represent the fragment offset field, we must scale it down by 216/213=8216/213=8, which functions as a scaling factor. As a result, all fragments except the last should have data in multiples of 8, so that fragment offset belongs to N.
- More Fragments Field (MF):- This field tells if there are more fragments ahead of this fragment, i.e., if MF = 1, there are more fragments ahead of this fragment, and if MF = 0, it is the last fragment.
- Don’t Fragment Field (DF):- If we don't want the packet to be fragmented, we set DF to 1.



13. Write a short note on NAT. -10 marks (repeated question)

Ans.

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working –

Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.

- Inside local address – An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.

- Inside global address – IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

- Outside local address – This is the actual IP address of the destination host in the local network after translation.

- Outside global address – This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

1.Static NAT – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

2.Dynamic NAT – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool

is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.
Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

3.Port Address Translation (PAT) – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.
Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunnelling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

14.Explain IPv6 protocol?
Ans. Internet protocol version 6 (IPv6) is a network layer protocol that allows communication to take place over the network. Each device on the internet has a unique IP address used to identify it and figure out where it is. The IPv6 packet is built with 40 extended octets so that users can scale the protocol for the future without disrupting its core structure. The packet has two parts: the header and the payload. IPv6 introduced jumbograms that enabled the packet to handle over 2^32. Jumbograms enhance performance over high maximum transmission unit (MTU) links and tackle the payload.

IPv6 has a 128-bit address and has a larger address space available for future allocation. The 128-bit address is broken into 8 groups, each containing 16 bits. Four hexadecimal numbers represent each group, and colons are used to divide each group from the others. IPv6 provides a host connected to the network with a unique identifier specific to the subnet.

Advantages of using IPv6

The technology provides internet users with several advantages:

- IPv6 provides a solution to address the global issue of depleting address spaces due to increased demand for IP addresses due to technological advancements.
- It offers reliability and faster speeds. IPv6 supports multicast addresses, meaning bandwidth-intensive packet flows like media streams can reach many destinations simultaneously.
- It enforces more robust network security than IPv4. IPv6 has IPSecurity, which ensures data privacy and data integrity. It also reinforces routing efficiency.
- It supports stateless and stateful address configuration regardless of the presence or absence of a Dynamic Host Configuration Protocol (DHCP) server.
- It has a larger address space and can handle packets more efficiently.

FEATURES OF IPV6

- Better header format
- New options
- Allowance for extension
- Support for resource allocation

ADDRESS SPACE ALLOCATION OF IPV6

- IPv6 provides a 128-bit address space to handle up to 3.4×10^{38} nodes.
- IPv6 uses *classless* addressing, but classification is based on MSBs.
- The address space is subdivided in various ways based on the leading bits.
- The current assignment of prefixes is listed in Table

Prefix	Use
00…0 (128 bits)	Unspecified
00…1 (128 bits)	Loopback
1111 1111	Multicast addresses
1111 1110 10	Link-local unicast
Everything else	Global Unicast Addresses

- A node may be assigned an "IPv4-compatible IPv6 address" by zero-extending a 32-bit IPv4 addressto128 bits.

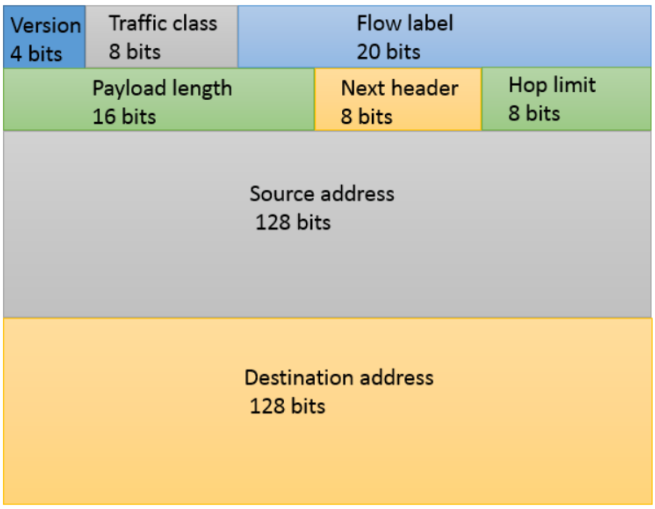
- Standard representation of IPv6 address is ***x*** **:** ***x*** **:** ***x*** **:** ***x*** **:** ***x*** **:** ***x*** **:** ***x*** **:** ***x*** where *x* is a 16-bit hexadecimal address separated by colon (:).
  For example,
  47CD **:** 1234 **:** 4422 **:** ACO2 **:** 0022 **:** 1234 **:** A456 **:** 0124

- IPv6 address with contiguous 0 bytes can be written compactly.
  For example,
  47CD **:** 0000 **:** 0000 **:** 0000 **:** 0000 **:** 0000 **:** A456 **:** 0124 → 47CD **: :** A456 **:** 0124

- IPv4 address is mapped to IPv6 address by prefixing the 32-bit IPv4 address with 2 bytes of 1s and then zero-extending the result to 128 bits.
  For example,
  128.96.33.81 → : : FFFF : 128.96.33.81
  This notation is called as CIDR notation or slash notation.

15. Draw and explain IPv6 header

Ans.



Version (4-bits): Indicates version of Internet Protocol which contains bit sequence 0110.

Traffic Class (8-bits): The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.

As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.
Priority assignment of Congestion controlled traffic:

Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic.

The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

Flow Label (20-bits): Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.

Payload Length (16-bits): It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.

Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.

Hop Limit (8-bits): Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.

Source Address (128-bits): Source Address is the 128-bit IPv6 address of the original source of the packet.

Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

Extension Headers: In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

1. Any extension header can appear at most once except Destination Header because Destination Header is present two times in the above list itself.
2. If Destination Header is present before Routing Header then it will be examined by all intermediate nodes specified in the routing header.
3. If Destination Header is present just above the Upper layer then it will be examined only by the Destination node.

Ext. Header	Description
Hop-by-Hop Options	Examined by all devices on the path
Destination Options (with routing options)	Examined by destination of the packet
Routing Header	Methods to take routing decision
Fragment Header	Contains parameters of fragmented datagram done by source
Authentication Header	verify authenticity
Encapsulating Security Payload	Carries Encrypted data

16. Compare IPv4 and IPv6

Ans.

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 2^32 address space	The address space of IPv6 is quite large it can produce 2^128 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

IPv4	IPv6
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