Unit IV

4 Network Layer : Services and Addressing

4.1 : Network Layer Services

Q.1 Explain network layer services with example.

☞ [SPPU : May-19, Marks 4]

Ans. : • Main Task of the network layer is to move packets from the source host to the destination host.

- It transport packet from sending to receiving hosts via internet. Network layer protocols exist in every host and route. In order to provide this service, the transport layer relies on the services of the network layer, which provides a communication service between hosts. In particular, the network layer moves transport-layer segments from one host to another.
- At the sending host, the transport-layer segment is passed to the network layer. It is then the job of the network layer to get the segment to the destination host and pass the segment up the protocol stack to the transport layer.
- Three important functions of network layer :
  1. **Path determination :** Route taken by packets from source to destination. Routing algorithms is used for this.
  2. **Switching :** Move packets from router's input to appropriate router output.
  3. **Call setup :** Some network architectures require router call setup along path before data flows.
- The basic function of network layer is to provide an end-to-end communications capability to the transport layer which lies above it.

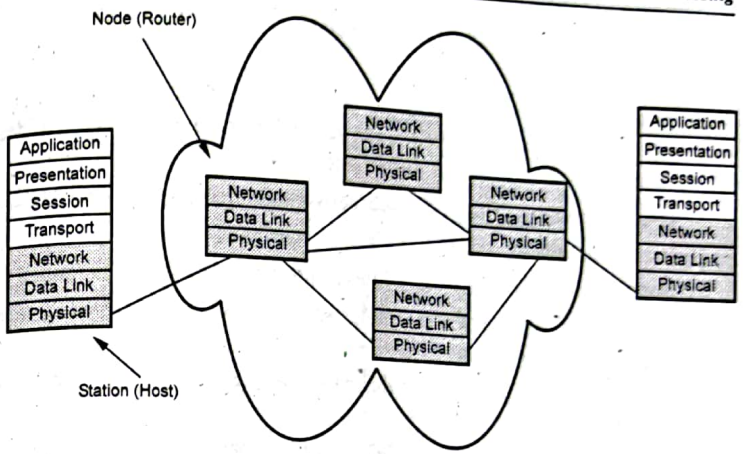

Fig. Q.1.1

Network layer is the lowest layer that deals with end-to-end transmission.

- To achieve the goal, the network layer must know about the topology of the communication subnet i.e. set of all routers and choose appropriate path through it. Network layer also takes care of loading of the chosen root.
- The network layer protocols are concerned with the exchange of packets of information between transport layer entities. A packet is a group of bits that includes data bits plus source and destination addresses. The service provided by the network layer to the transport layer is called network service.
- The functions carried out by a layer are different from its services. Functions are those activities which are carried out by a layer in order to provide the services. The network layer functions are carried out by adding a header to every Network Service Data Unit (NSDU) forming Network Protocol Data Unit (NPDU).

- The header contains all the information necessary for carrying out functions.
  1) It keeps track which MAC (Media Access Control), the unique number that each network card has address to send i.e. decides which system receives the information.
  2) It makes routing of data through network from source to destination.
  3) Virtual circuits are established in this layer.
  4) It translates logical network address into physical machine address.
  5) It breaks large packets into smaller so that it will be accepted by the frame of data link layer.
  6) Flow control of packetized information and congestion avoidance is concern of protocol.
  7) It determines the Quality Of Service (QOS) parameter.

4.2 : IPv4 Addresses

Q.2 What is classless addressing ? Explain.

☞ [SPPU : Dec.-15 (End Sem.) Marks 4]

Ans. : The IP address structure is divided into five address classes : Class A, Class B, Class C, Class D and Class E, identified by the most significant bits of the addresses.

- Fig. Q.2.1 shows the five classes of IP addresses.
- Class D addresses are used for multicast services that allow a host to send information to a group of hosts simultaneously. Class E addresses are reserved for future use.
- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size.

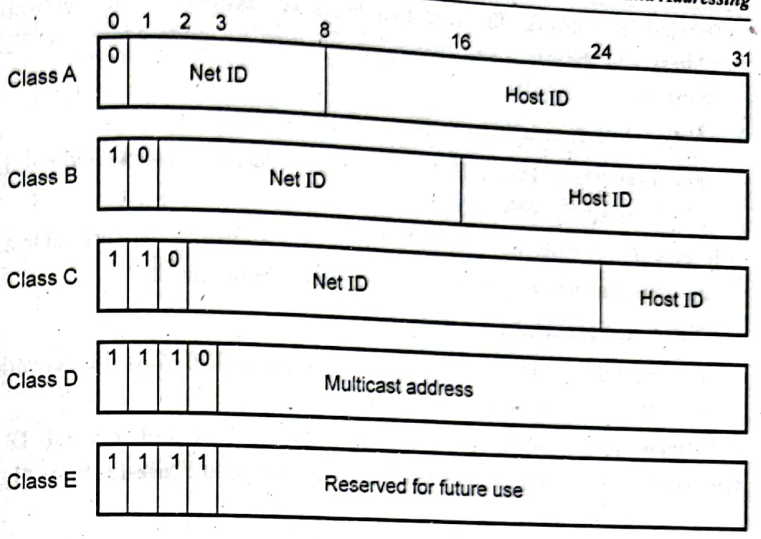

Fig. Q.2.1 Five classes of IP addresses

Class	Number of blocks	Block size
A	128	16777216
B	16384	65536
C	2097152	256
D	1	268435456
E	1	268435456

- In a class A network, the first byte is assigned to the network address and the remaining three bytes used for the node addresses. The class A format is

  Network.Node.Node.Node

  For example : 14.28.101.120 in this IP address 14 is the network address and 28.101.120 is the node address.

- In class B network, the first two bytes are assigned to the network address and the remaining two bytes are used for node addresses. The format is

  Network.Network.Node.Node

  For example : 150.51.30.40 in this IP address network address is 150.51 and node address is 30.40.

- In class C network, the first three bytes are assigned to network address and only one byte is used for node address. The format is

  Network.Network.Network.Node

  For example : 200.20.42.120 in this example 200.20.42 is the network address and 120 is the node address.

Q.3 Draw and explain IPv4 header format. List out special IP addresses and private IP addresses. ☞ **[SPPU : June-22, Marks 8]**

Or Draw and explain IPv4 header format.

☞ **[SPPU : May-16, End Sem, Marks 6]**

Ans. : • Packets in the IPv4 layer are called datagrams. A datagram is a variable length packet consisting of two parts : Header and data.

• Fig. Q.3.1 shows IPv4 header format

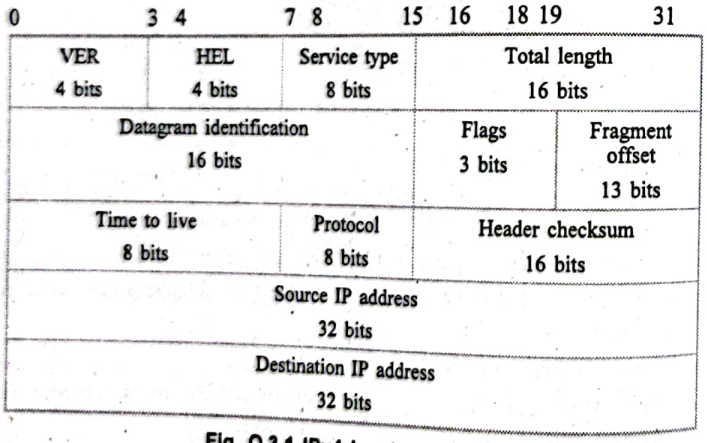

Fig. Q.3.1 IPv4 header format

1. **VER** is the field that contains the IP protocol version. The current version is 4.5 is an experimental version. 6 is the version for IPv6.
2. **HLEN** is the length of the IP header in multiples of 32 bits without the data field.The minimum value for a correct header is 5 (i.e. 20 bytes), the maximum value is 15 (i.e., 60 bytes).
3. **Service type** The service type is an indication of the quality of service requested for this IP datagram. It contains the following information.

Precedence	Types of service	R

Precedence specifies the nature / priority :

000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash override
101	Critical
110	Internetwork control
111	Internetwork control

TOS specifies the type of service value :

TOS bits	Description
1000	Minimize delay
0100	Maximum throughout
0010	Maximize reliability

0001	Minimize monetary cose
0000	Normal service

The last bit is reserved for future use.

4. **Total length** specifies the total length of the datagram, header and data, in octets.
5. **Identification** is a unique number assigned by the sender used with fragmentation.
6. **Flags** contain control flags :
   a. The first bit is reserved and must be zero;
   b. The 2nd bit is DF (Do not Fragment), 0 means allow fragmentation;
   c. The third is MF (More Fragments), 0 means that this is the last fragment.
7. **Fragment offset** is used to reassemble the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.
8. **TTL** (Time To Live) specifies the time (in seconds) the datagram is allowed to travel. In practice, this is used as a hop counter to detect routing loops.
9. **Protocol number** indicates the higher level protocol to which IP should deliver the data in this datagram. E.g., ICMP = 1; TCP = 6; UDP = 17.
10. **Header checksum** is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.
11. **Source/Destination IP addresses** are the 32-bit source/destination IP addresses.
12. **IP options** is a variable-length field (there may be zero or more options) used for control or debugging and measurement. For instance :
    a. The **loose source routing** option provide a means for the source of an IP datagram to supply explicit routing information;
    b. The **timestamp** option tell the routers along the route to put timestamps in the option data.

13. **Padding** is used to ensure that the IP header ends on a 32 bit boundary. The padding is zero.

Q.4 For a given class C network 195.188.65.0. Design the equal subnets in such a way that each subnet has at least 50 nodes.

☞ [SPPU : May-19, Marks 6]

Ans. : For class-C IP address, 8-bit is used for subnet. Each subnet has atleast 60 nodes, so calculate subnet mask.

$2^2 - 2 = 2$ subnet

∴ Subnet mask is 255.255.255.11000000

255.255.255.192 subnet mask.

Calculate the subnet

255.255.255.0100000

255.255.255.64 First subnet

255.255.255.10000000

255.255.255.128 Second subnet

1st subnet = 255.255.255.64

2nd subnet = 255.255.255.128

Q.5 What is NAT ? Explain operation of NAT with suitable example.

☞ [SPPU : Oct.-16 (In Sem.), Marks 5]

Or Explain the operation of NAT with suitable example.

☞ [SPPU : May-18, Dec.-19, Marks 4]

Ans. : • Within the company, every machine has a unique address of the form 10.X.Y.Z. When a packet leaves the company premises, it passes through the NAT box that convert the internal IP source address 10.0.0.1.

- NAT box is often combined in a single device with a firewall. It is also possible to integrate the NAT box into the company router.
- Whenever an outgoing packet enters the NAT box, the 10.X.Y.Z. SA is replaced by the company true IP address. In, addition, TCP source port field is replaced by an index into the NAT box 65536 entry translation table. This table entry contains the original IP address and original

source port. Finally both the IP and TCP header checksums are recomputed and inserted into the packet.

- Fig. Q.5.1 shows the placement of NAT box.

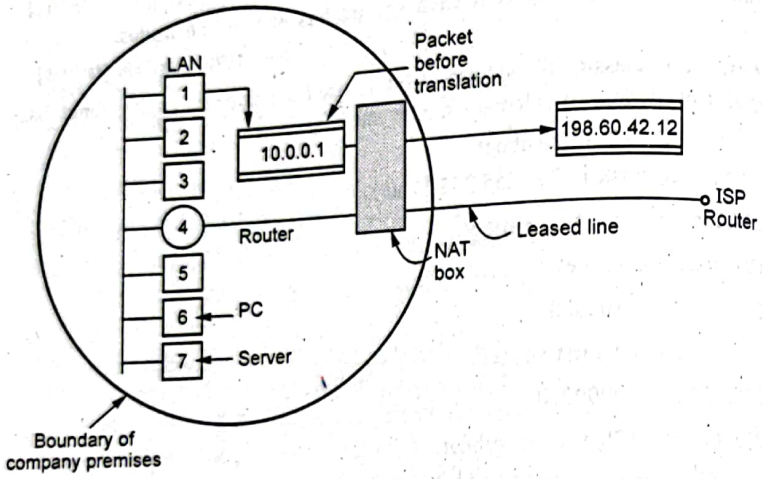

Fig. Q.5.1 NAT

- When process want to establish a TCP connection with a remote process, it attached itself to an unused TCP port on its own machine. This is called a source port and tells the TCP code where to send incoming packets belonging to this connection.
- The process also supplies a destination port to tell who to give the packet to on the remote side.

Q.6 Explain subnetting a network.

Ans. : • If a organization is large or if its computers are geographically dispersed, it makes good sense to divide network into smaller ones, connected together by routers. The benefits for doing things this way include.

1. Reduced network traffic
2. Optimized network performance
3. Simplified network management
4. Facilities spanning large geographical distances.

- If Network Information Center (NIC) assign only one network address to an organization which having multiple network, that organization has a problem. A single network address can be used to refer to multiple physical networks.
- An organization can request individual network **address** for each one of its physical networks. If these were granted, there wouldn't be enough to go around for everyone.
- Another problem is, if each router on the internet needed to know about each existing physical network, routing tables would be impossibly huge. This is physical overhead on the router. To solve this type of problem, the subnet addressing method is used.
- To allow a single network address to span multiple physical networks is called **subnet addressing** or **subnet routing** or **subnetting**. Subnetting is a required part of IP addressing.
- To understand subnet addressing, consider the next example. Consider the site has a single class B IP network address assigned to it, but the organization has two or more physical networks.

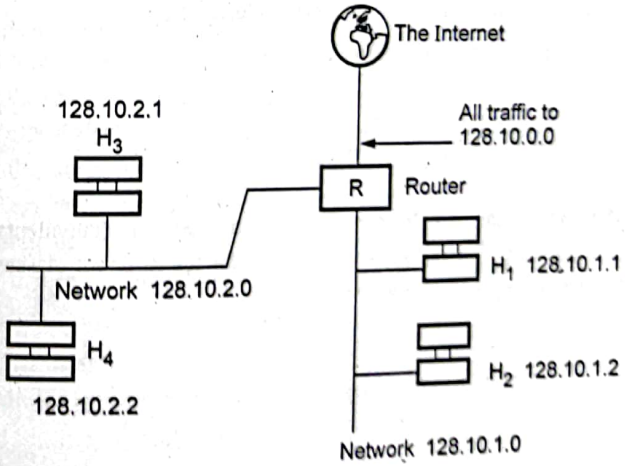

Fig. Q.6.1 Multiple network

- Only local routers know that there are multiple physical networks and how to route traffic among them.
- In the example, the organization is using the single class B network address for two networks. For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning each machine a subnet mask.
- The network administrator creates a 32-bit subnet mask comprised of ones and zeros. The ones in the subnet mask represent the positions that refer to the network or subnet addresses.
- The zeros represent the positions that refer to the host part of the address. Class B address format is Net.Net.Node.Node. The third byte, normally assigned as part of the host address is now used to represent the subnet address. Hence, these bit positions are represented with ones in the subnet mask.
- The fourth byte is the only part in example that represents the unique host address.

Subnet mask code

1 = Positions representing network or subnet addresses.

0 = Positions representing the host address.

Subnet mask format

1111 1111 1111 1111 1111 1111 0000 0000

Network address positions *Subnet positions* *Host positions*

- The subnet mask can also be denoted using the decimal equivalents of the binary patterns. The default subnet masks for the different classes of networks are as below in Table Q.6.1.

Class	Format	Defult subnet mask
A	Net.Node.Node.Node	255.0.0.0
B	Net.Net.Node.Node	255.255.0.0
C	Net.Net.Net.Node	255.255.255.0

Table Q.6.1 Default subnet mask of IP address

Masking

- A process that extracts the address of the physical network from an IP address is called Masking. If we done the subnetting, then masking extracts the subnetwork address from an IP address.
- To find the subnetwork address, two method are used. There are boundary level masking and non-boundary level masking, we take one by one.
- In boundary level masking, two masking numbers are consider (i.e. 0 or 255). In non-boundary level masking other value of masking is used Apart from 0 and 255.

A. Rules for boundary level masking

1. In this mask number is either 0 or 255.
2. If the mask number is 255 in the mask IP address, then the IP address is repeated in subnetwork address.
3. If the mask number is 0 (zero) in the mask IP address, then the 0 is repeated in subnetwork address.

B. Rules for non-boundary level masking

1. In this mask numbers are not 0 or 255 mask number is greater than 0 or less than 255.
2. If the mask number is 255 in the mask IP address, then the original IP address (byte) is repeated in subnetwork address.
3. If the mask number is 0 in the mask IP address, then the 0 is repeated in the subnetwork address.

4. For any other mask numbers, bit-wise AND operator is used. Bit-wise ANDing is done in between mask number (byte) and IP address (byte).

- The first address in the block is used to identify the organization to rest of the Internet. This address is called the **network address.**

1. How many subnets ?

- Number of subnet is calculated as follows :

Number of subnet = 2^x

where x is the number of masked bits or the 1s (ones).

- For example 11100000, the number of 1s gives us 2^3 subnets. In this example there are 8 subnets.

2. How many host per subnet ?

Number of host per subnet = $2^y - 2$

Where y is the number of unmasked bits or the 0s (zeros).

- For example 11100000, the number of 0s gives us $2^5 - 2$ hosts. In this example there are 30 hosts per subnet. You need to subtract 2 for subnet address and the broadcast address.

3. What are the valid subnets ?

For valid subnet = 256 – Subnet mask = Block size. An example would be 256 – 224 = 32. The block size of a 224 mask is always 32.

Start counting at zero in block of 32 until you reach the subnet mask value and these are your subnets. 0, 32, 64, 96, 128, 160, 192, 224.

4. What is the broadcast address for each subnet ?

- Our subnets are 0, 32, 64, 96, 128, 160, 192, 224, the broadcast address is always the number right before the next subnet. For example, the subnet 0 has a broadcast address of 31 because next subnet is 32. the subnet 32 has a broadcast address of 63 because next subnet is 64.

5. What are the valid hosts ?

- Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s. For example, if 32 is the subnet number and 63 is the

broadcast address, then 32 to 63 is the valid host range. It is always between the subnet address and the broadcast address.

Q.7 What is subnetting ? A company is granted a site address 172.16.10.33/19 design the subnets and answer following questions :
i) How many subnets does the chosen subnet mask produce ?
ii) How many valid hosts per subnet are available ?
iii) What are the valid subnets ?
iv) What's the broadcast address of each subnet ?
v) What are the valid hosts in each subnet ?

☞ [SPPU : June-22, Marks 8]

Ans. : Subnetting : Refer Q.6.

Subnet mask : 255.255.224.0

Network Address : 172.16.0.0

Broadcast address : 172.16.31.255

Host IP range : 172.16.0.1 to 172.16.31.254

Valid number of hosts : 8192

Number of usable host : 8190

Q.8 Explain supernetting.

Ans. :

- Although class A and B addresses are almost depleted, class C addresses are still available. In super netting, an organization can combine several class C blocks to create a larger range of addresses.
- Several networks are combined to create a super network. For example : Organization needs 1000 address can be granted 4 contiguous class C blocks to create one super network.
- Supernet is a block of contiguous sub-networks addressed as a single subnet in the larger network. Supernets always have a subnet mask that is smaller than the masks of the component networks.
- The size of routing tables has been rapidly increasing during the expansion of the Internet. Supernetting is the process of aggregating routes to multiple smaller networks, thus saving storage space in the

routing table and simplifying routing decisions. Routing advertisements to neighboring gateways are reduced.

- An organization has been allocating a block of class C address in 2n with contiguous address space. It archive by using bits which belongs to the network address as hosts bits.
- An organization with 4 class C

193.0.32.0 , 193.0.33.0 , 193.0.34.0 , 193.0.35.0

11111111 11111111 11111100 00000000 mask 255.255.252.0

11000001 00000000 00100000 00000000 net 193.0.32.0

11000001 00000000 00100001 00000000 net 193.0.33.0

11000001 00000000 00100010 00000000 net 193.0.34.0

11000001 00000000 00100011 00000000 net 193.0.35.0

11000001 00000000 00100000 00000000

- Bit wise AND results 193.0.32.0 : 11000001 00000000 00100000 00000000
- This organization's network has changed from 4 net to a single net with 1,022 hosts.
- Supernetting requires the use of routing protocols that support Classless Inter-Domain Routing (CIDR). Interior Gateway Routing Protocol, Exterior Gateway Protocol and version 1 of the Routing Information Protocol (RIPv1) are based on classful addressing, and therefore cannot transmit subnet mask information.

Q.9 List the network layer services and define subnetting, supernetting, classful addressing, classless addressing.

☞ [SPPU : June-22, Marks 9]

Ans. : Refer Q.1,2,6 and 8.

4.3 : Delivery and Forwarding of IP Packet

Q.10 Explain delivery and forwarding IP packets.

Ans. :

- Forwarding refers to the way a packet is delivered to the next node. It requires a host or router to have a routing table.
- Forwarding refers to the router local action of transferring a datagram from an input link interface to the appropriate output link interface.
- When host has a packet to send, it looks at routing table to find the route to the final destination.

Types of forwarding techniques

1. Next hop versus route method.
2. Network specific versus host specific method.
3. Default method.

1) Next hop versus route method

- Fig. Q.10.1 shows network with routing table for this method. This method reduce the content of rounting table. Routing table stores only the address of the next hop.

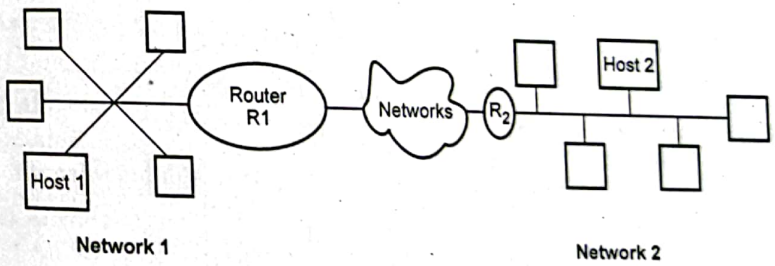

Fig. Q.10.1

Routing table for next hop

hkhdskjandm,

For host 1

Destination address	Next hop
Host 2	R1

For router R2

Destination Address	Next hop
Host 2	R2

For Router R2

Destination Address	Next hop
Host 2	-

2) Network specific versus host specific method

- It simplify the searching process and also reduce the routing table size.
- Routing table contains only the address of the destination network.
- It provides good security.

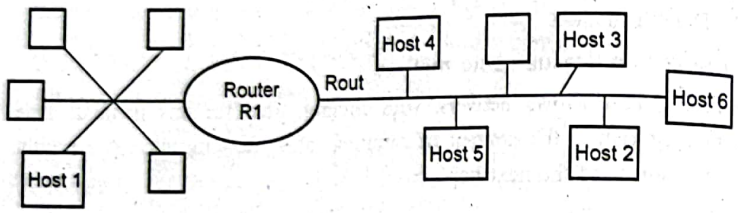

Fig. Q.10.2

Routing table for host 1

Destination address	Next hop
Network 2	R1

3) Default method

- Host is connected with more than one routers.
- A router is assigned to receive all packets with no match in the routing table.
- Default router is used for communication with outside world.

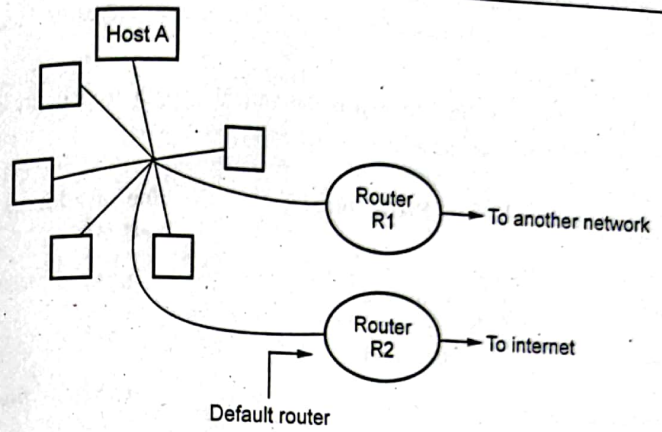

Fig. Q.10.3

4.4 : IPv6

Q.11 What is the need of IPv6 ? Explain types of IPv6 address.

☞ [SPPU : June-22, Marks 9]

Ans. : IPv6 allows three types of addresses.

1) Unicast 2) Anycast 3) Multicast

1) Unicast

An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

2) Anycast

An identifier for a set of interfaces. A packet sent to an anycast address is delivered to one of the interfaces identified by the address.

3) Multicast

An identifier for a set of interfaces. A packet sent to a multicast address is delivered to all interfaces identified by that address.

- Following Table Q.11.1 shows the current allocation of addresses based on the format prefix.
- The first field of any IPv6 address is the variable-length fromat prefix, which identifies various categories of addresses.

Allocation space	Prefix (binary)	Fraction of address space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reversed for NSAP allocation	0000 001	1/128
Reversed for IPX allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider-Based Unicast Address	010	1/8
Unassigned	011	1/8
Reserved for Geographic-Based Unicast Addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16

Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

Table Q.11.1 Address allocation

Q.12 Draw neatly IPv6 header format.

☞ [SPPU : Aug.-15, In Sem, Marks 6]

Ans. : • The IPv6 packet is shown in Fig. Q.12.1. Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts : Optional and data

• Fig. Q.12.2 shows the IPv6 datagram header format.

1. **Versions :** This 4 bits field defines the version number of the IP. The value is 6 for IPv6.
2. **Priority :** The 4 bits priority field defines the priority of the packet with respect to traffic congestion.
3. **Flow label :** It is 24 bits field that is designed to provide special handling for a particular flow of data.
4. **Payload length :** The 16 bits payload length field defines the length of the IP datagram excluding the base header.
5. **Next header :** It is an 8 bits field defining the header that follows the base header in the datagram.
6. **Hop limit :** This 8 bits hop limit field serves the same purpose as the TTL field in IPv4.
7. **Source address :** The source address field is a 128 bits internet address that identifies the original.

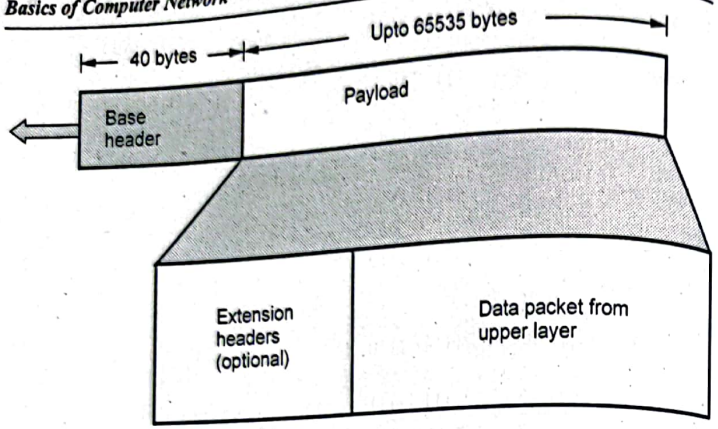

Fig. Q.12.1 IPv6 datagram header of payload

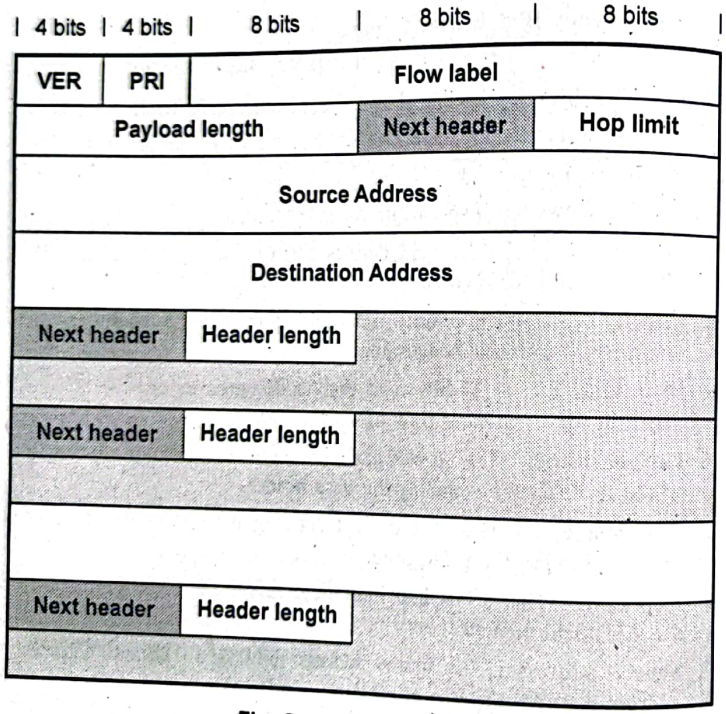

Fig. Q.12.2 IPv6 header

8. **Destination address :** It is 128 bits Internet address that usually identifies the final destination of the datagram.

- Next header codes for IPv6

Code	Next header
0	Hop by hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null
60	Destination option

Priority

- The priority field defines the priority of each packet with respect to other packets from the same source. IPv6 divides traffic into two broad categories
  1. Congestion controlled
  2. Noncongestion controlled
- If a source adapts itself to traffic slowdown when there is congestion, the traffic is referred to as congestion controlled traffic. Congestion controlled data are assigned priorities from 0 to 7.

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

- A priority of 0 is the lowest; a priority of 7 is the highest.
- Noncongestion controlled traffic refers to a type of traffic that excepts minimum delay. Discarding of packets is not desirable. Retransmission in most cases is impossible. Real time audio and video are examples of this type of traffic.
- Priority numbers from 8 to 15 are assigned to noncongestion controlled traffic.

4.5 : Transition from IPv4 to IPv6

Q.13 Explain Dual stack and tuneling.

Ans. : • All the host must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.

- Fig. Q.13.1 shows the dual stack.
- To determine which version to use when sending a packet to destination, the source host queries the DNS. If the DNS returns an

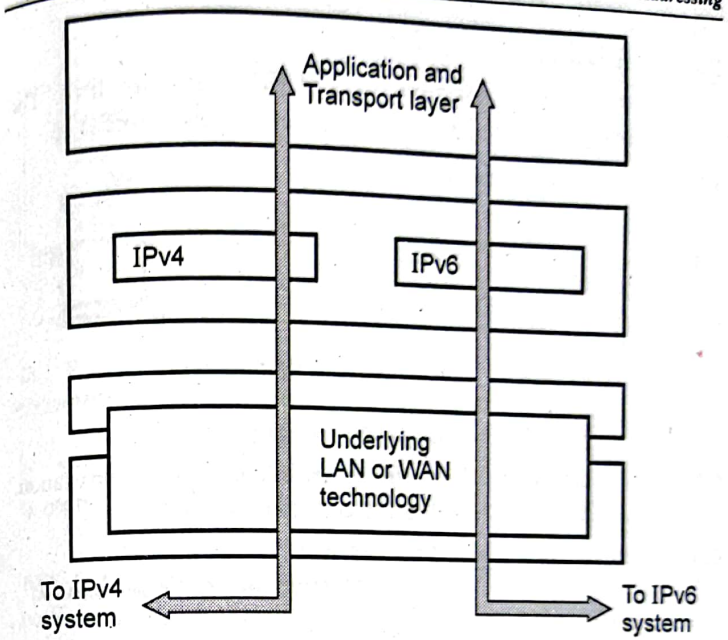

Fig. Q.13.1 Dual stack

IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

Tunneling

- When two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. The IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.
- Fig. Q.13.2 shows the tunneling.

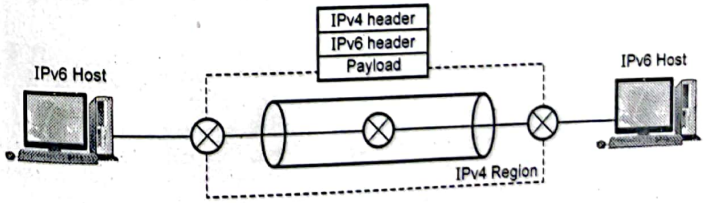

Fig. Q.13.2 Tunneling

Header Translation

- Header translation is used when some of the system uses IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6.
- Fig. Q.13.3 shows the header translation.

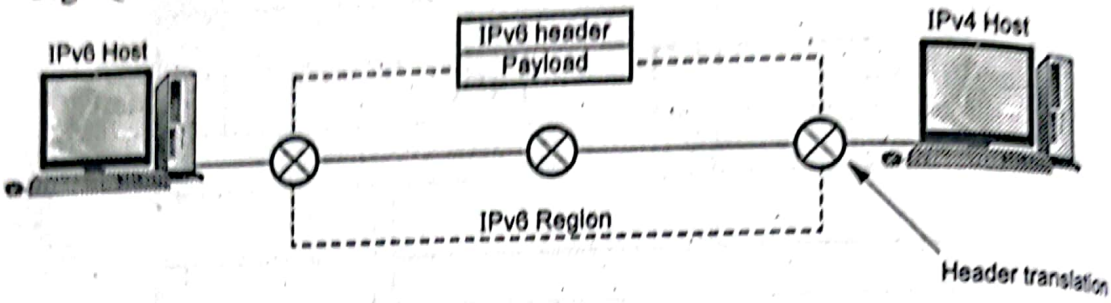

Fig. Q.13.3 Header translation

- The header format must be totally changed through header translation. The header of the IPv6 parket is converted to IPv4 header.

Q.14 1.Differentiate between IPv4 and IPv6.

☞ [SPPU : Dec.-15, End Sem, Marks 4]

Or Compare between IPv4 and IPv6.

☞ [SPPU : April-18, In Sem, Marks 6]

Ans. :

Sr. No.	IPv4	IPv6
1.	Header size is 32 bits.	Header size is 128 bits.
2.	It cannot support autoconfiguration	Supprots autoconfiguration
3.	Cannot support real time application.	Supports real time application.
4.	No security at network layer.	Provides security at network layer.
5.	Throughput and delay is more.	Throughput and delay is less.

END...