Chapter-4 Network Layer MIMP Questions

Q.1 What is routing loop? Discuss routing loop avoidance techniques. (May-2016)

Ans:

A routing loop is a serious network problem which happens when a data packet is continually routed through the same routers over and over. The data packets continue to be routed within the network in an endless circle. A routing loop can have a catastrophic impact on a network, and in some cases, completely disabling the network. Normally Routing Loop is a problem associated with Distance Vector Protocols.

How routing loops affect network performance?

- A major portion of the precious bandwidth which is available for normal user traffic of the affected routers will be consumed by looping IP datagram packets.
- The major portion of the processing power of the affected routers is used to process the looping IP datagram packets.
- Routing Loop can happen in large internetworks when a second topology change emerges before the network is able to converge on the first change. Convergence is the term used to describe the condition when all routers in an internetwork have agreed on a common topology.
- Link state protocols tend to converge very quickly, while distance vector protocols tend to converge slowly.

The following methods are used to avoid Routing Loops. Maximum hop Count

- Maximum hop count mechanism can be used to prevent Routing Loops.
- Distance Vector protocols use the TTL (Time- to- Live) value in the IP datagram header to avoid Routing Loops. When an IP datagram move from router to router, a router keeps track of the hops in the TTL field in the IP datagram header. For each hop a packet goes through, the packet's TTL field is decremented by one. If this value reaches 0, the packet is dropped by the router that decremented the value from 1 to 0.

Split Horizon

- A split horizon is a routing configuration that stops a route from being advertised back in the direction from which it came. Split Horizon mechanism states that if a neighbouring router sends a route to a router, the receiving router will not propagate this route back to the advertising router on the same interface.

Route Poisoning

- Route Poisoning is another method for avoiding routing loops. When a router detects that one of its connected routes has failed, the router will poison the route by assigning an infinite metric to it.

Hold- down Timers

- Hold- down timer is another mechanism used to prevent bad routes from being restored and propagated by mistake. When a route is placed in a hold- down state, routers will neither advertise the route nor accept advertisements about it for a specific interval called the hold- down period.

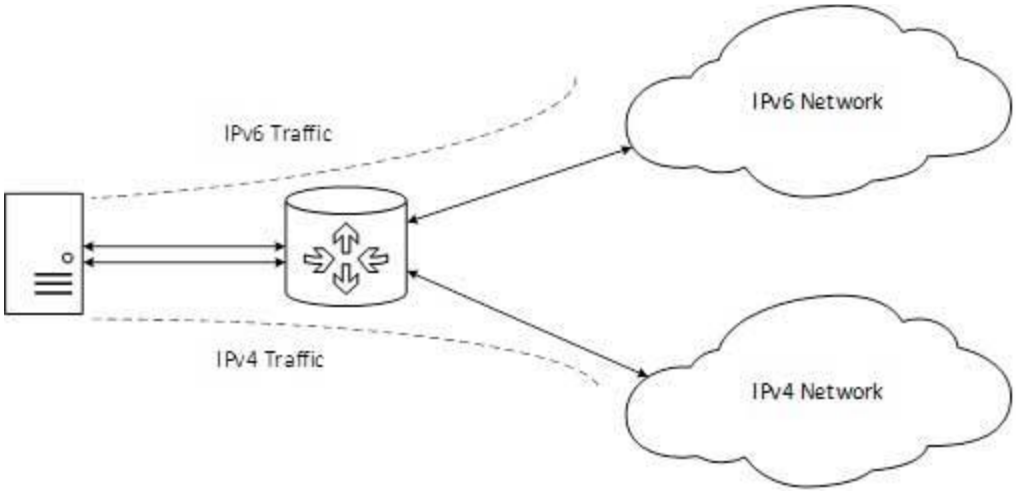
Q.2 Define Tunneling OR Show Tunneling of IP v6 packet over IP v4 router network. (June-2017, Nov-2017)

Ans:

- Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. It is unlike implementation of other new technologies where the newer one is backward compatible so the older system can still work with the newer version without any additional changes.
- To overcome this short-coming, we have a few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6.

Dual Stack Routers

- A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.



- In the above diagram, a server having IPv4 as well as IPv6 address configured for it can now speak with all the hosts on both the IPv4 as well as the IPv6 networks with the help of a Dual Stack Router. The Dual Stack Router, can communicate with both the networks. It provides a medium for the hosts to access a server without changing their respective IP versions.

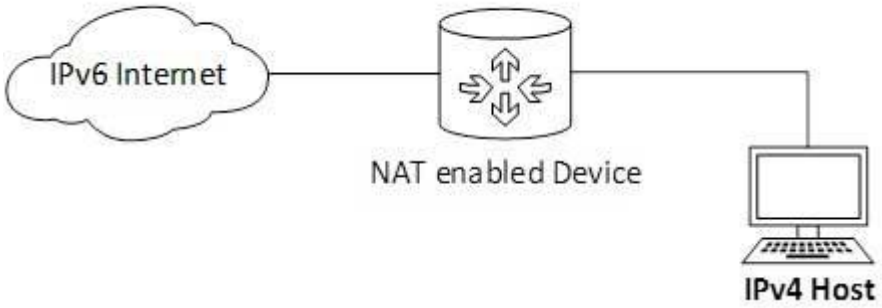
Tunneling

- In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through a non-supported IP version.

- The above diagram depicts how two remote IPv4 networks can communicate via a Tunnel, where the transit network was on IPv6. Vice versa is also possible where the transit network is on IPv6 and the remote sites that intend to communicate are on IPv4.

NAT Protocol Translation

- This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa. See the diagram below:



- A host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa.

Q.3 Differentiate broadcast and multicast with their functionalities. (Nov-2016)

BASIS FOR COMPARISON	BROADCAST	MULTICAST
Basic	The packet is transmitted to all the hosts connected to the network.	The packet is transmitted only to intended recipients in the network.
Transmission	One-to-all.	One-to-many.
Management	Broadcasting does not require any group management.	Multicasting requires group management to define the group of hosts/stations which will receive packets.
Bandwidth	Bandwidth is wasted.	Bandwidth is utilized efficiently.
Traffic	Unnecessarily huge amount traffic is generated in the network.	Traffic is under control.
Process	Slow.	Fast.

Q.4 What is a routing algorithm? List major types of it. (Nov-2016)
Ans:

- A routing algorithm is a set of step-by-step operations used to direct Internet traffic efficiently. When a packet of data leaves its source, there are many different paths it can take to its destination. The routing algorithm is used to determine mathematically the best path to take.

There are two main types of routing algoriths:

1) Distance Vector (distance-vector routing)
2) To link state (link state routing)

Q.5 What is IP address? What is Subnet? Explain different IP address in classes. (Nov-2017)
Ans:

IP address:

- IP address is short for Internet Protocol (IP) address. An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. Contrast with IP, which specifies the format of packets, also called datagrams, and the addressing scheme.

Subnet:

- A subnet is a logical partition of an IP network into multiple, smaller network segments. It is typically used to subdivide large networks into smaller, more efficient sub-networks.
- Subnet mask is used to separate the network address from the host address in IP address. As we discussed earlier an IP address is the combination of network address and host address, subnet mask helps us and programs which use IP address in identifying the network portion and the host portion.
- Just like IP address, subnet mask is also 32 bits in length and uses same notations which IP address uses to present itself.
- Subnet mask assigns an individual bit for each bit of IP address. If IP bit belongs to network portion, assigned subnet mask bit will be turned on. If IP bit belongs to host portion, assigned subnet mask bit will be turned off.

IP address classes:

a. IP address classes is divided in 5 categories:

   i. Class A (0-127)
   ii. Class B (128-191)
   iii. Class C (192-223)
   iv. Class D (224-239)
   v. Class E (240-255)

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

Q.6 Draw Router device architecture. (Nov-2016)

Ans:

A high-level view of generic router architecture is shown in Figure Four router components can be identified

Input ports:

- An input port performs several main functions. It performs the physical layer function of terminating an incoming physical link at a router; this is shown in the leftmost box of the input port and the rightmost box of the output port in Figure.
- An input port also performs link-layer functions needed to operate with the link layer at the other side of the incoming link; this is represented by the middle boxes in the input and output ports.

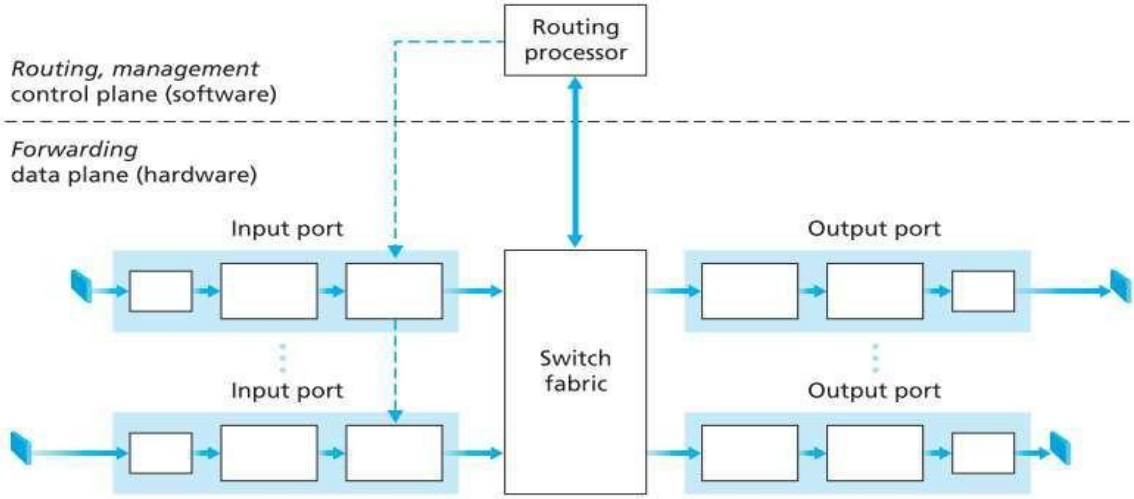


Figure : Router architecture

- The lookup function is also performed at the input port; this will occur in the rightmost box of the input port. Here the forwarding table is consulted to determine the router output port to which an arriving packet will be forwarded through the switching fabric.
- Control packets (for example, packets carrying routing protocol information) are forwarded from an input port to the routing processor. Note that the term port here referring to the physical input and output router interfaces—is different from the software ports associated with network applications and sockets discussed in application layer and transport layer.

Switching fabric:

- The switching fabric connects the router's input ports to its output ports. This switching fabric is within the router- a network inside a network router!

Output ports:

- An output port stores packet received from the switching fabric and transmits these packets on the outgoing link by performing the necessary link- layer and physical-layer functions.
- When a link is bidirectional (that is, carries traffic in both directions), an output port will typically be paired with the input port for that link on the same line card.

Routing processor:

- The routing processor executes the routing protocols, maintains routing tables and attached link state information, and computes the forwarding table for the router.
- It also performs the network management functions.

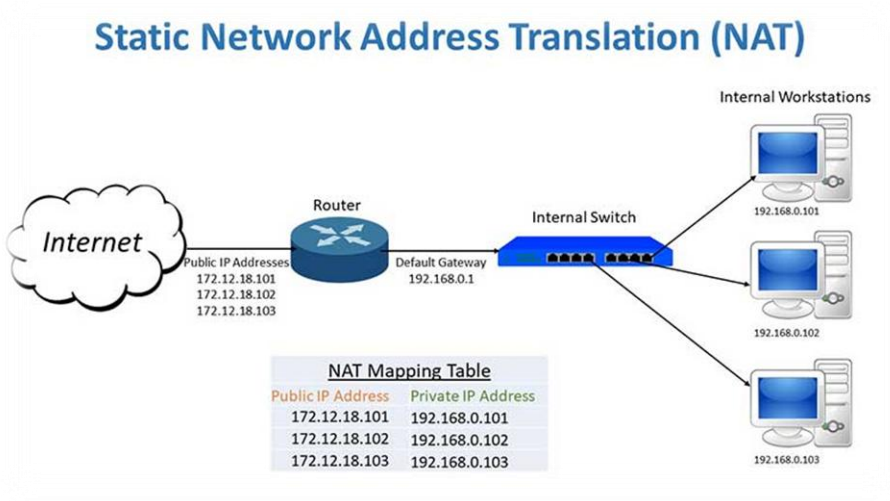
Q.7 How does NAT works? Explain. (June-2017, Nov-2017)

Ans:

- As internet grew and IP address became scarce a mechanism discovered called NAT.
- The basic idea behind NAT is to provide an illusion, because a single IP address cannot be assigned to multiple computers-as conflict arises.
- Some IP addresses are reserved for sole purpose of private & intra-enterprise communications. These addresses are known as private IP addresses defined in RFC 1918.
- Each end system in organization is been assigned IP Address from a private IP Pool.
- When any of the end system requests a communication to internet with source IP of it, but private IP cannot be used for global communication.
- So a NAT enable router is installed which acts as an interface between home network and internet, Router has its own unique IP over internet.
- So every request from organization gets transferred to NAT Router. NAT enabled maintains a table of source IP & destination IP of each and every request.
- NAT router eliminates private IP as source IP and its own IP as source IP address whereas, destination IP remains untouched.
- The request gets transferred to destination IP address and the response generated is

received by NAT router which examines the table and forwards the response to end system.

- Figure shows the operation of a NAT-enabled router.



- The NAT-enabled router, residing in the home, has an interface that is part of the home network on the right.
- Addressing within the home network is exactly as we have seen above—all four interfaces in the home network have the same subnet address of 10.0.0/24.
- The address space 10.0.0.0/8 is one of three portions of the IP address space that is reserved in for a private network or a realm with private addresses, such as the home network in Figure.
- A realm with private addresses refers to a network whose addresses only have meaning to devices within that network.
- To see why this is important, consider the fact that there are hundreds of thousands of home networks, many using the same address space, 10.0.0.0/24.
- Devices within a given home network can send packets to each other using 10.0.0.0/24 addressing.
- However, packets forwarded beyond the home network into the larger global Internet clearly cannot use these addresses (as either a source or a destination address) because there are hundreds of thousands of networks using this block of addresses.
- That is, the 10.0.0.0/24 addresses can only have meaning within the given home network.
- But if private addresses only have meaning within a given network, how is addressing handled when packets are sent to or received from the global Internet, **where addresses are necessarily unique?**
- The answer lies in understanding NAT.
- The NAT-enabled router does not look like a router to the outside world.
- Instead the NAT router behaves to the outside world as a single device with a single

IP address.

- In Figure, all traffic leaving the home router for the larger Internet has a source IP address of 172.12.18.101, and all traffic entering the home router must have a destination address of 172.12.18.101.
- In essence, the NAT-enabled router is hiding the details of the home network from the outside world.
- But where the home network computers get their addresses and where the router gets its single IP address. Often, the answer is the same—DHCP!
- When datagrams arrives at the NAT router from the WAN have the same destination IP address (specifically, that of the WAN-side interface of the NAT router), then router uses a NAT translation table at the NAT router, and to include port numbers as well as IP addresses in the table entries to determine internal host to which it should forward a given datagram.
- Consider the example in Figure.
- Following sequence of steps are going to execute, Suppose a user sitting in a home network behind host 10.0.0.1 requests a Web page on some Web server (port 80) with IP address 192.168.0.101.
- The host 10.0.0.1 assigns the (arbitrary) source port number 3345 and sends the datagram into the LAN.
- The NAT router receives the datagram, generates a new source port number 5001 for the datagram, replaces the source IP address with its WAN-side IP address 172.12.18.101, and replaces the original source port number 3345 with the new source port number 5001.
- When generating a new source port number, the NAT router can select any source port number that is not currently in the NAT translation table. (Note that because a port number field is 16 bits long, the NAT protocol can support over 60,000 simultaneous connections with a single WAN-side IP address for the router!)
- NAT in the router also adds an entry to its NAT translation table.
- The Web server, unaware that the arriving datagram containing the HTTP request has been manipulated by the NAT router, responds with a datagram whose destination address is the IP address of the NAT router, and whose destination port number is 5001.
- When this datagram arrives at the NAT router, the router indexes the NAT translation table using the destination IP address and destination port number to obtain the appropriate IP address (10.0.0.1) and destination port number (3345) for the browser in the home network.
- The router then rewrites the datagram destination address and destination port number and forward the datagram into the home network.

Q.8 What is the main difference between forwarding and routing? (May-2015, Dec-2015)

Ans:

- Forwarding and Routing are the two most important network-layer functions.
- Both of these terms are different, but is often used interchangeably. Forwarding refers to the router-local action of transferring the packet from an input link interface to the appropriate output link interface.
- Routing refers to the network-wide process that determines end-to-end paths that packets take from source to destination.
- Using driving analogy, consider a trip from RAJKOT to MAHUVA, To differentiate between the two, Routing is the process of planning the whole trip from RAJKOT to MAHUVA, i.e. the best route from RAJKOT to MAHUVA.
- Forwarding on the other hand, can be considered as a process of getting through a single intersection. A car enters the interchange from one road and determines which road it should take to leave the interchange.
- Forwarding is the process of moving packets from input to output using
    - The forwarding table
    - Information in the packet
- Routing is the process by which the forwarding table is built and maintained using
- One or more routing protocols (link state routing or distance vector routing)
- Procedures (algorithms) to convert routing info to forwarding table.

Explain at least two forwarding techniques used by the router to switching to packets from input port to output port of the router.

a. Next-Hop Method versus Route Method:

- One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method). The entries of a routing table must be consistent with one another.

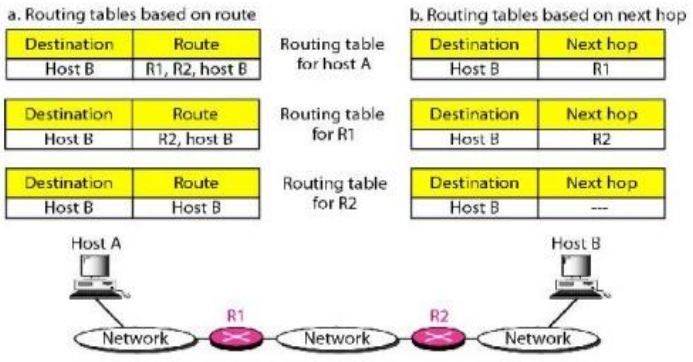


Figure 3.40 Route method versus next-hop method

b. Network-Specific Method versus Host-Specific Method:

- A second technique to reduce the routing table and simplify the searching process is called the network-specific method. Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself.
- Host-specific routing is used for purposes such as checking the route or providing security measures

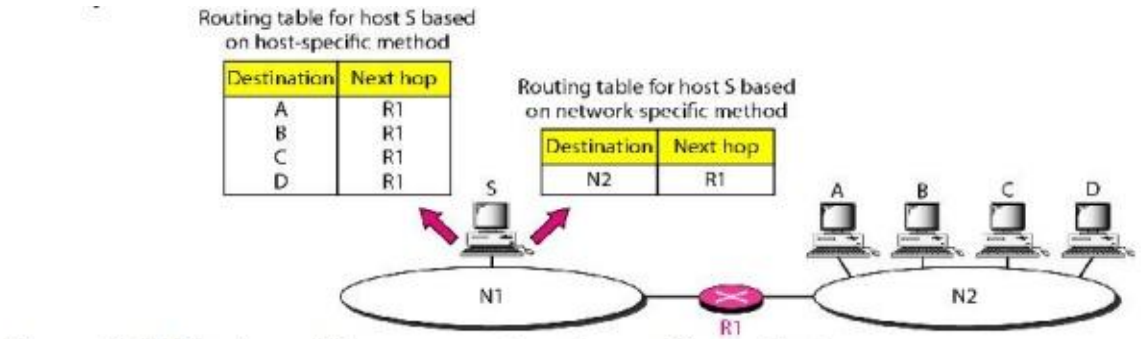
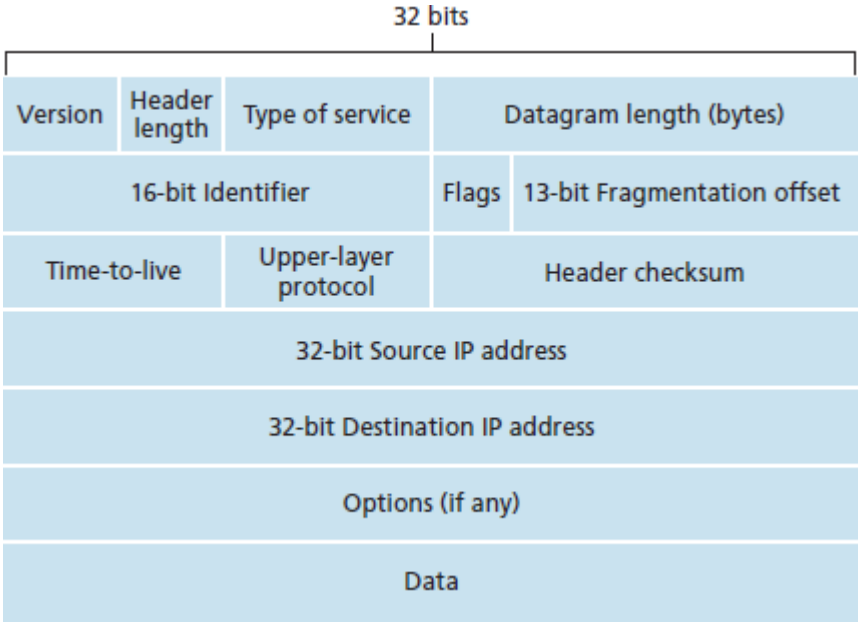


Figure 3.41 Host-specific versus network-specific method

Q.9 IPv4 Datagram Format with each Field. (May-2015, May-2016, Nov-2016, June-2017)

Ans:

The IPv4 datagram format is shown in the figure below.



Version Number: These 4 bits specify the IP protocol version of the datagram. By looking at the version number, the router can determine how to interpret the remainder of the IP datagram. Different versions of IP use different datagram formats. The datagram format for

the current version of IP, IPv4 is shown in the figure above. The datagram format for the new version of IP (IPv6) will be discussed later.

Header Length: An IPv4 datagram can contain these 4 bits are needed to determine where in the IP datagram the data actually begins. Most IP datagrams do not contain options, so the typical IP datagram has a 20-byte header.

Type of Service: The type of service (TOS) bits were included in the IPv4 header to allow different types to be distinguished from each other. For example, it might be useful to distinguish real-time datagrams by an IP telephony application from non-real-time traffic (for example, FTP). The specific level of service to be provided is a policy issue determined by the router's administrator.

Datagram Length: This is the total length of the IP datagram (header plus data), measured in bytes. Since this filed is 16 bits long, the theoretical maximum size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 1,500 bytes.

Identifier, Flags, Fragmentation Offset: These three fields have to do with so-called IP fragmentation, a topic we will consider in depth shortly. Interestingly, the new version of IP, IPv6, does not allow fragmentation at routers.

Time-to-live: The time-to-live (TTL) field is included to ensure that datagrams do n I'mot circulate forever (due to, for example, a long-lived routing loop) in the network. This field is decremented by one each time the datagram is processed by a router. If the TTL field reaches 0, the datagram must be dropped.

Protocol: This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport- layer protocol to which the data portion of this IP datagram should be passed. For example, a value of 6 indicates that the data portion is passed to TCP, while a value of 17 indicates that the data is passed to UDP.

Source and Destination IP Addresses: When a source creates a datagram, it inserts its IP address into the source IP address field and inserts the address of the ultimate destination into the destination IP address field.

Q. 10 One the address in a block is 17.63.1.114/24, find the first address and last address in block. (MAY 2016)

Ans:

- First address is 17.63.110.0/24
- Last address is 17.63.110.255/24

Q.11 Explain packet Fragmentation with example. (Nov-2017)

Ans:

- A Breaking the large packet into smaller size called as packet fragmentation. An packet fragmentation can be handled at many different protocol layers.

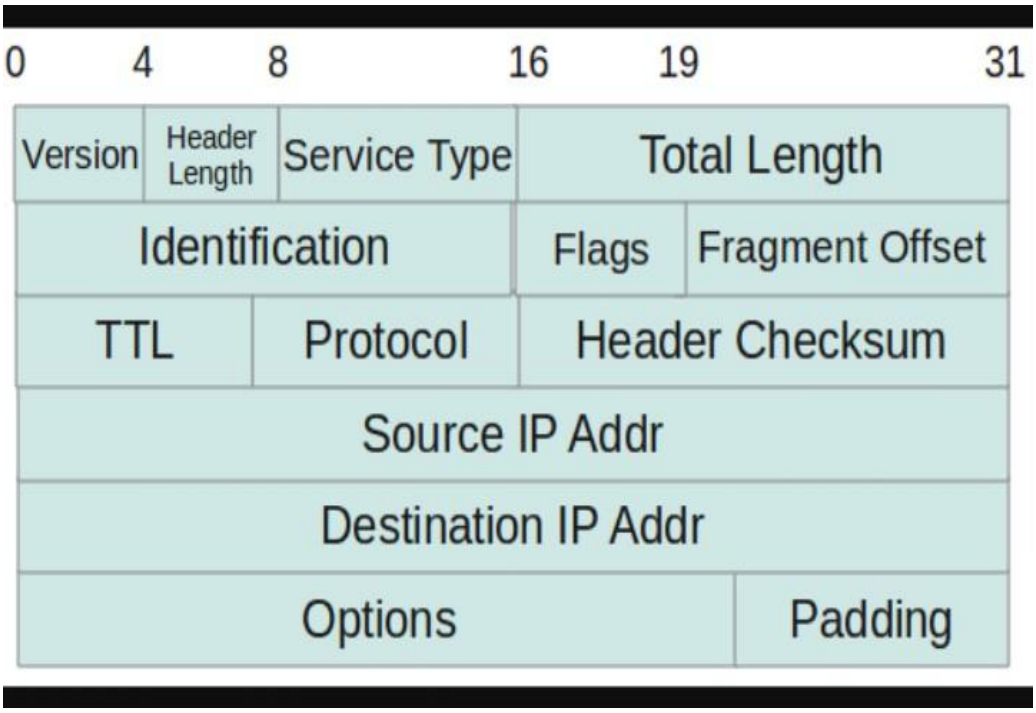
Fragmentation Needed:

- Fragmentation at Network layer. Fragmentation is done by the network layer when the maximum size of Datagram is greater than Maximum size of data that can be held a frame. i.e, its Maximum Transmission Unit (MTU) an Overhead at network

layer is present due to extra header introduced due to fragmentation.

Packet Header:

- Every IP packet an IP(internet protocol)header that stores information about the packet ,including:
    - Version
    - IHL
    - Type of service
    - Total Length
    - Identification
    - Flags
    - Fragment Offset
    - Protocol
    - Header Checksum
    - Source Address
    - Destination Address



A Packet Fragmentation Example

If a 2,366 byte packet enters an Ethernet network with a default MTU size, it must be fragmented into two packets.

The first packet will:

- Be 1,500 bytes in length. 20 bytes will be the IP header, 24 bytes will be the TCP header, and 1,456 bytes will be data.
- Have a DF bit equal to 0 to mean "May Fragment" and an MF bit equal to 1 to mean "More Fragments."
- Have a Fragmentation Offset of 0.

The second packet will:

- Be 910 bytes in length. 20 bytes will be the IP header, 24 bytes will be the TCP header, and 866 bytes will be data.
- Have the DF bit equal to 0 to mean "May Fragment" and the MF bit equal to 0 to mean "Last Fragment."
- Have a Fragmentation Offset of 182

Q.12 Compare distance vector routing and link state routing algorithm. (June-2017)
Ans:

- **distance vector routing algorithm :**

```
1   Initialization:
2   for all destinations y in N:
3   Dx(y)=c(x,y) /*if y is not a neighbor then cx,y=∞*/
4   for each neighbor w
5   Dw(y)=? for all destinations y in N
6   for each neighbor w
7   send distance vector Dx=[Dx(y):y in N] to w 8
9   loop
10  wait(until I see a link cost change to some neighbor w
11  or until I receive a distance vector from some  neighborw)
12  for each y in N:
13  Dx(y) = minv{c(x,v) + Dv(y)} 14
15  if Dx(y) changed for any destination y
16  send distance vector D x= [Dx(y): y in N] to all neighbors 17
18  Forever
```

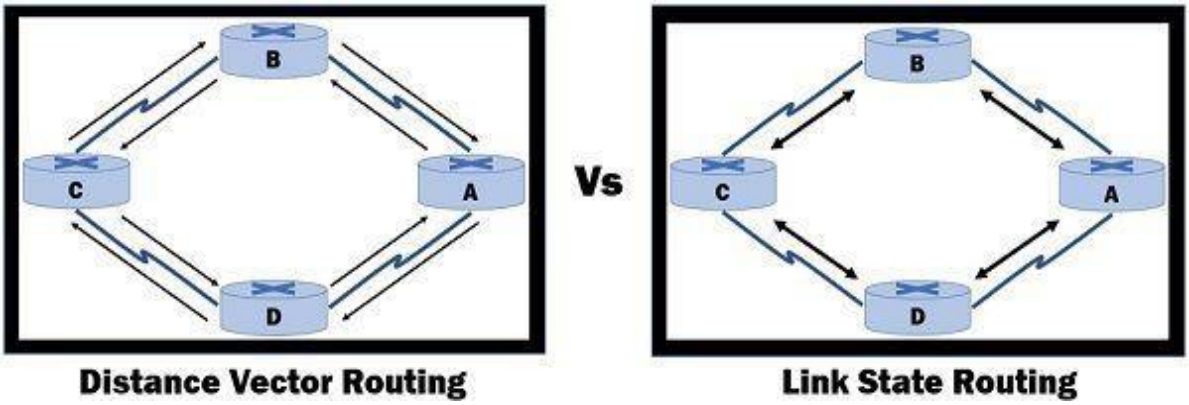
- **link state routing algorithm**.

1 Initialization:
2 N' = {u}
3 for all nodes v
4 if v is a neighbor of u
5 then D(v) = c(u,v)
6 else
Dv = ∞ 7
8 Loop
9 find w not in N' such that Dw is a minimum
10 add w to N'
11 update Dv for each neighbor v of w and not in N':
12 12 D(v) = min(D(v), D(w) + c(w,v))
13 /* new cost to v is either old cost to v or known
14 least path cost to w plus cost from w to v */
15 until N'= N

- **comparison** :

BASIS FOR COMPARISON	DISTANCE VECTOR ROUTING	LINK STATE ROUTING
Algorithm	Bellman ford	Dijsktra
Network view	Topology information from the neighbour point of view	Complete information on the network topology
Best path calculation	Based on the least number of hops	Based on the cost
Updates	Full routing table	Link state updates
Updates frequency	Periodic updates	Triggered updates
CPU and memory	Low utilization	Intensive
Simplicity	High simplicity	Requires a trained network administrator
Convergence time	Moderate	Fast
Updates	On broadcast	On multicast

Hierarchical structure	No	Yes
Intermediate Nodes	No	Yes



Distance Vector Routing **Link State Routing**