Syllabus:-**Unit-III**

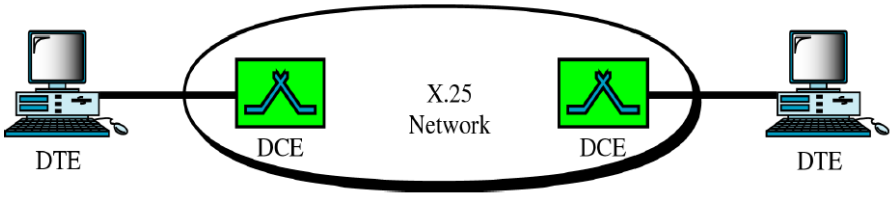
- Network Layer - Point-to-Point Networks,
- routing,
- congestion control
- Internetworking-
- TCP/IP-IP packet,
- IP address,
- IPv6.

Possible Conceptual Questions:-

Question No-(1): What are the responsibilities of Network Layer? What do you understand by Point-to-Point Networks?
Answer:- Responsibilities of Network Layer:-Network layer is responsible for following activities:-

a) Accepting Packets from Transport Layer at Sender Side.
b) Handing over the Packets to Transport Layer at Receiver Side.
c) Routing – i.e. to decide the optimized or best path from different alternate paths.
d) Congestion Control- i.e. to monitor and maintain the traffic over the link.

Point-to-point Network: - Point to point network refers to the network in a link is directly established between two devices. Link can be a dedicated media or it may be through public or wireless environment.



Examples of Point-Point Networks are:-

a) Direct link between two computers.
b) Direct link between two switches.
c) Direct Link between two Routers.
d) Virtual Link between two routers through public network.
e) Virtual Link between two satellite earth stations through public network.

Question No-(2): What do you understand by routing? Make a comparison between Adaptive & Non-Adaptive routing protocols?
Answer:- Routing:- Routing refers to selecting best or optimized path from different alternates available between source and destination. Routing is the main responsibility of Network Layer and is done by the router with the help of routing algorithms.

- Routing is an OSI Layer 3 function. Routing is a hierarchical organizational scheme that allows individual addresses to be grouped together. These individual addresses are

treated as a single unit until the destination address is needed for final delivery of the data.

- Routing is the process of finding the most efficient path from one device to another.
- The primary device that performs the routing process is the router.

- The following are the two key functions of a router:-
  (1) Routers maintain routing tables and make sure other routers know of changes in the network topology. This function is performed using a routing protocol to communicate network information with other routers. When packets arrive at an interface, the router must use the routing table to determine where to send them.

  (2) The router switches the packets to the appropriate interface, adds the necessary framing information for the interface, and then transmits the frame.

- Router uses one or more routing metrics to determine the optimal path along which network traffic should be forwarded.
- Routing metrics are values used in determining the advantage of one route over another.
- Routing protocols use various combinations of metrics for determining the best path for data.

Adaptive & Non-Adaptive Routing Algorithms:- Routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on. Routing Algorithms can be classified into two categories:-

a) **Non-Adaptive Routing Algorithms**: These routing algorithms do not base their routing decision on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from one end to other end is computed in advance, off-line, and downloaded to the routers when the network is booted. This procedure is also called as Static routing and is done by the administrator in advance.

b) **Adaptive Algorithms:** Adaptive routing algorithms, in contrast, change their decisions to reflect changes in the topology, and usually the traffic as well. Adaptive algorithms differ in where they get their information (e.g. locally, from adjacent routers, or from all routers), when they change the routes (e.g. ΔT sec, when the load changes or when the topology changes), and what metric is used for optimization. Adaptive routing can be classified mainly into two categories:-

   - Distance Vector Routing
   - Link State Routing.

Question No-(3): What is the different between Distance Vector & Link State Routing?
Answer: Adaptive Routing Algorithms can be categorized into two categories:-

- Distance Vector Routing
- Link State Routing.

Distance-Vector Protocol

- Routers using distance-vector algorithms send all or part of their complete routing table entries to adjacent routers on a periodic basis.
- This happens even if there are no changes in the network.
- By receiving a routing update, routes and make changes to its routing table.
- This process is known as "routing by rumor".
- The problem with Distance vector routing algorithm is of slow convergence about updates. As updates are communicated neighbor to neighbor, this process takes time

and delay sometime results in wrong decisions by distant router as updates are not known to that till long.

- Examples of Distance Vector protocols are (a) RIP(Routing Information Protocol) –It uses hop count as its only routing metric. (b) Interior Gateway Routing Protocol (IGRP) – The IGP developed by Cisco. (c) Enhanced IGRP (EIGRP) – The Cisco-proprietary IGP includes many of the features of a link-state routing protocol.

Link-state protocols

- Link-state routing protocols send trigger updates only when a network change occur.
- Link-state routing protocols send periodic updates, known as link-state refreshes, at longer time intervals, such as every 30 minutes.
- In addition to periodic updates when a route or link changes, the device that detected the change creates a link-state advertisement (LSA) concerning that link.
- The LSA is then transmitted to all devices.
- The advantage with link state routing algorithm is of fast convergence about updates. As updates are communicated to all at once, this process takes less time. But regular triggered updates overburden the routers and stop them to perform their normal duties.
- Examples of link-state protocols:
  - Open Shortest Path First (OSPF)
  - Intermediate System-to-Intermediate System (IS-IS)

(Students must also refer to the numerical problems based on distance vector routing as discussed in the classroom.)

Question No-(4): What do you understand by Congestion Control? What are various techniques of congestion control?

Answer:- **Congestion Control**:- Congestion Control is another important responsibility of the Network Layer. Congestion control refers to monitoring of outgoing traffic to a link and to maintain the traffic rate within the capacity of the link as well as to ensure the traffic rate upto a level so that link capacity may be utilized effectively.

Congestion control approaches are responsible basically for three tasks:-

- Monitor the system to detect when and where congestion occurs.
- Pass the information to place where action can be taken.
- Adjust system operation to correct the problem.

Congestion Control Techniques:- Congestion control techniques may be categorized into two categories:-

a) **Leaky Bucket Congestion Control Technique**:- This approach is based on the bucket that has a small hole in the bottom. No matter the rate at which water enters the bucket, the overflow is at a constant rate, when there is any water in the bucket and zero when the bucket is empty.

—

Once the bucket is full, any additional water entering it spills over the sides and is lost (i.e. does not appear in the output stream under the hole).

The same idea can be applied to packets. Conceptually, each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue. If a packet arrives at the queue when it is full, the packet is discarded. In fact, it is nothing other than a single-server queuing system with constant service time.

This mechanism turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion.

b) **Token Bucket Congestion Control Technique**:- The leaky bucket algorithm enforces a rigid output pattern at the average rate, no matter how bursty the traffic is. For many applications, it is better to allow the output to speed up somewhat when large bursts arrive, so a more flexible algorithm is needed, preferably one that never loses data. One such algorithm is token bucket.

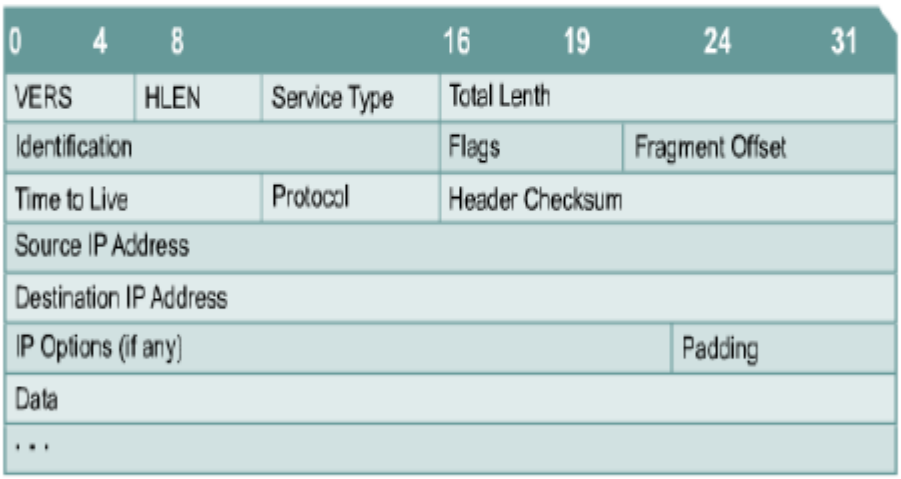
In this algorithm leaky bucket holds tokens, generated by a clock at the rate of one packet token every ΔT sec. More tokens are assigned to the traffic that is coming with more incoming rate; fewer tokens are assigned to the traffic that is coming with less incoming rate. Output rate variable and is decided based on the token hold.

Another difference between the two algorithms is that the token bucket algorithm throws away tokens when the bucket fills up but never discards packets.

(Students must draw the diagrams of Leaky Bucket and Token Bucket as discussed in the class room. Also must refer to the numerical problems based on Congestion Control numerical problems as solved in the classroom).

Question No-(5) : What are various fields in the IP Version 4 Header?
Answer:- IP packets consist of the data from upper layers plus an IP header.

The IP-Header can be understood with the help of following diagram:-



The IP header consists of the following:

- **Version** – Indicates the version of IP currently used; Four bits are used in it. The version can be either IPV4 or IPV6. If the version field is different than the IP version of the receiving device, that device will reject the packets.

- **IP header length (HLEN)** – Indicates the datagram header points to the beginning of the data. 4 bits are used in it. HLEN represent length of header.

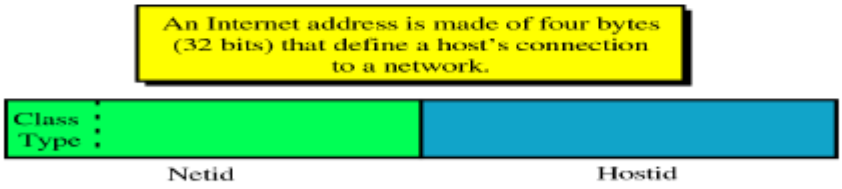
- **Type-of-service (TOS)** – 8 bits- that specify the level of importance that has been assigned by a particular upper-layer protocol.

- **Identification** – 16 bits that identify the current datagram. This is the sequence number.
- **Total length** – Specifies the length of the entire packet in bytes, including data and header.16 bits are used in it. To get the length of the data payload subtract the HLEN from the total length.
- **Time-to-live (TTL)** – A field that specifies the number of hops a packet may travel. Number is decreased by one as the packet travels through a router. When the counter reaches zero the packet is discarded. This prevents packets from looping endlessly.
- **Protocol** – indicates which upper-layer protocol, such as TCP or UDP, receives incoming packets after IP processing has been completed.8 bits are used in it.
- **Source address** – specifies the sending node IP address, 32 bits are used in it.
- **Destination address** – specifies the receiving node IP address, 32 bits are used in it.
- **Header checksum** – 16 bits that help ensure IP header integrity.
- **Padding** – extra zeros are added to this field to ensure that the IP header is always a multiple of 32 bits.
- **Data** – contains upper-layer information, variable length up to 64 Kb.

Question No-(6): What are various classes of IP Version 4 Addressing system? How many networks and hosts are possible in each class?

Answer:- **IP Addressing**:- To connect a node to a network as large as the Internet, an addressing system would have to be set in order to facilitate the information transactions.
This addressing system must ensure unique address to each machine as well as addressing system must be able to identify the group a node belongs to as well as the network the node is in.

The system to do this is via IP Addressing



The IP address serves to provide an address for nodes connected to the internet as well as giving information on the categories of networks they belong into. The number of hosts a network can support varies from network to network. Thus, a particular address is only assigned to organizations whose networks are large.

To facilitate these categorizations, the IP addressing system is divided into 5 classes.
All these classes cater to the different types of networks an organization might have.

Class A addresses are reserved for networks that have a lot of hosts. Class A uses 8-bits for network and remaining 24-bits for host-id. The supportable networks in class A will be 2^7 – 2.

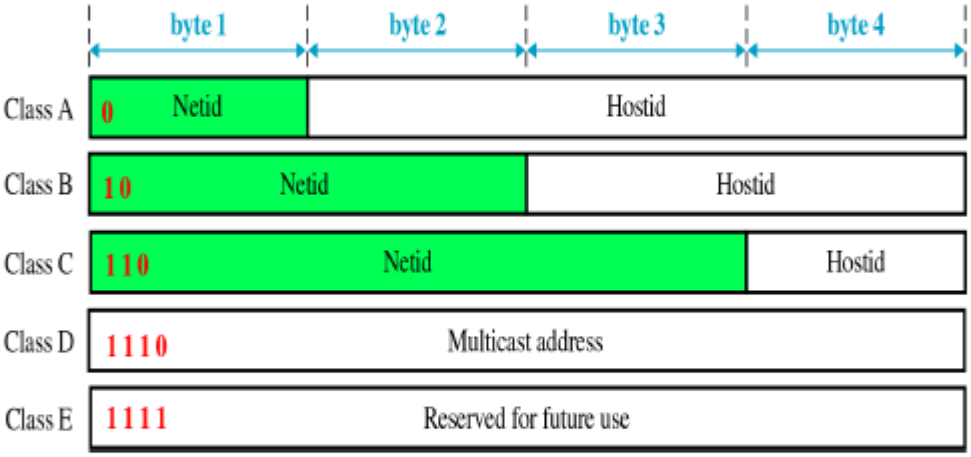
As all zeros are not allowed as first octet and 01111111 will result is 127 as first octet that is reserved for local loop back testing. The supportable number of hosts in a class A network is (2^24)-2, which equates to 16,777,214 hosts.

Class B addresses has a balance between network addresses and number of computers.Class B uses 16-bits for network and remaining 16-bits for host-id. The supportable networks in class B will be 2^14.The amount of hosts supported by a class B address is (2^16)-2, which equates to 65534 hosts.

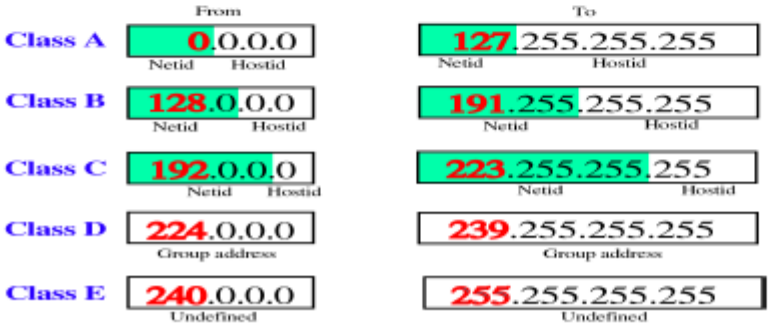
Class C addresses are usually used for public domain, having a high amount of network address but are able to support a low number of hosts. Class C uses 24-bits for network and remaining 8-bits for host-id. The supportable networks in class C will be 2^21. Class C supports (2^8)-2, which is 256 hosts.

Class D addresses are reserved for multicasting purposes. Multicasting uses a similar concept of broadcasting, but differs in which, multicasting can be directed a group of nodes, instead of the entire network.

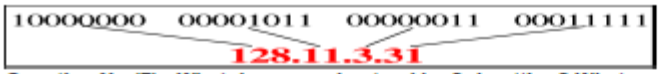
Class E addresses are being reserved for future use.



Thus Range of First Octet in different Classes may be given as below:-

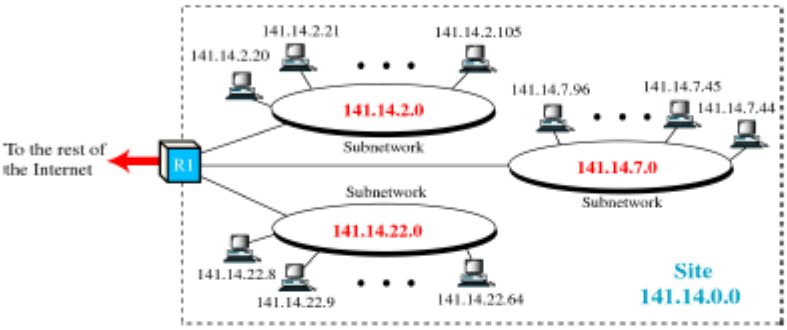


Naturally, the human mind finds it hard to memorize binary numerical. The dotted decimal notation system makes an IP address easier to read.



Question No-(7) : What do you understand by Subnetting? What are the advantages of subnetting? Illustrate with suitable examples?

Answer:- Subnetting : Subnetting is a way to introduce another level of hierarchy within the same network. A subnet mask is applied to the IP address to filter the hostid and extract the subnet address. By doing this, we can segment our networks and still share the same internetworking resources.



Why Subnet:- Subnetting is required for following reasons:-

- To break the network down into pieces, each of which can be addressed separately.
- Controls network traffic.
- Reduces broadcasts.
- Can provide low level security with access lists on the router.
- Organization of IP addresses space.

Number of usable subnets & useable hosts:-

- **Number of usable subnets** = two to the power of the assigned subnet bits or borrowed bits, minus two. The minus two is for the reserved addresses of network ID and network broadcast. However all zero combination of subnet bits may be used as a subnet based on modern research. Thus number of usable subnets may be assumed as two to the power of the assigned subnet bits or borrowed bits, minus one.

- **Number of usable hosts** = two to the power of the bits remaining, minus two (reserved addresses for subnet id and subnet broadcast).

How the Router Determines the Subnet:-

The Subnet Mask: First step is to find out the subnet mask.

- **The subnet mask (in binary) has:**
  - all ones in the network and subnet portion of the address
  - all zeros in the host potion of the address
  - For example in class C if we are borrowing four bits for subnet.The subnet mask for this example will be: **255.255.255. 240**

Finding the subnet:- ANDing the subnet mask with any valid host address on the network will always yield the subnet address for that host.

Example:- Subnetting a Default Class C Network Address: e.g. 200.129.41.0

- Default Class C address is divided into network and host portions as follows:
  N . N . N . H
- To subnet we "borrow" bits from the host portion of the address (8 bits for Class C)
  N . N . N . x x x x x x x x
- Borrowing *n* bits yields $2n - 2$ subnets.
- Leaving *n* bits yields $2n - 2$ hosts.
- For a class C, we can borrow from 2 to 6 bits.
- Suppose we need 14 usable subnets
  - Remember, borrowing *n* bits give us:
    - $2n - 2$ subnets
  - Try borrowing 3 bits ($n = 3$):
    - $23 - 2 = 8 - 2$

    = 6 usable subnets (not enough)
  - Try borrowing 4 bits
    - $24 - 2 = 16 - 2$

    = 14 usable subnets (enough)
- Write it different combinations for borrowed four bits:

e.g.

200.129.41. 0000	0000	= 200.129.41.0
200.129.41. 0001	0000	= 200.129.41.16
200.129.41. 0010	0000	= 200.129.41.32
200.129.41. 0011	0000	= 200.129.41.48
200.129.41. 0100	0000	= 200.129.41.64
200.129.41. 0101	0000	= 200.129.41.80
200.129.41. 0110	0000	= 200.129.41.96
200.129.41. 0111	0000	= 200.129.41.112
200.129.41. 1000	0000	= 200.129.41.128
200.129.41. 1001	0000	= 200.129.41.154
200.129.41. 1010	0000	= 200.129.41.170
200.129.41. 1011	0000	= 200.129.41.186
200.129.41. 1100	0000	= 200.129.41.202

Above will be treated as subnet addresses:-

- Find out the subnet mask:- As we have borrowed 4-bits in class C.
  Thus subnet new mask will be 255.255.255.240.

- Now ANDing the subnet mask with any valid host address on the network will always yield the subnet address for that host.

Question No-(8) : **What do you understand by following kind of addressing?**

a) **Unicast Addressing.**
b) **Anycast Addressing.**
c) **Multicast Addressing.**

Answer:- **a) Unicast Addressing**:- Unicast address refers to the normal IP-Address that corresponds to some device, router port etc. If a packet is sent to unicast address it is forwarded to one and only one machine or port. Unicast address must have non-zero host as well as non-zero network address portion in its identification. As well as all host bits should not one.

e.g. 192.168.1.1 is a unicast address.

Whereas 192.168.1.0 and 192.168.1.255 are not unicast addresses because All host bits in first are zero and all host bits are one in second address.

(b) Anycast Addressing:-Anycast address or broadcast refers to the IP-Address that corresponds to all devices and router ports in that network. If a packet is sent to anycast address it is forwarded to all machines and ports of that network. Anycast address must have all-one host bits as well as non-zero network address portion in its identification.

e.g. 192.168.1.255 is an anycast or broadcast address as all host bits are one in it.

(c) Multicast Addressing:-Multicast address refers to the IP-Address that corresponds to all devices and router ports in a subnetwork. If a packet is sent to multicast address it is forwarded to all machines and ports of that subnetwork. Multicast address must have all-one hostbits as well as non-zero subnetwork address portion in its identification.
Thus muticast is an intermediate choice between unicast and anycast addressing.

e.g. if 192.168.1.0 network is further divided into three subnets and subnet addresses are:-
192.168.1.000 00000 ---- Subnet 1
192.168.1.001 00000 -----Subnet 2
192.168.1.010 00000 ------Subnet 3

The address 192.168.1.000 11111 = 192.168.1.31 will be the multicast address. As packet will be sent to all hosts of subnet one. Not to other subnets.

Question No-(9): How router decides the path? What do you understand by Routing tables and routing parameters? Illustrate with suitable examples?
Answer:- **Process to find out the path**:-

The following process is used to determine the path for every packet that is routed.

- The router compares the IP address of the packet that it received to the IP tables that it has.
- The destination address is obtained from the packet.
- The mask of the first entry in the routing table is applied to the destination address.
- The masked destination and the routing table entry are compared.
- If there is a match, the packet is forwarded to the port that is associated with that table entry.
- If there is not a match, the next entry in the table is checked.
- If the packet does not match any entries in the table, the router checks to see if a default route has been set.
- If a default route has been set, the packet is forwarded to the associated port. A default route is a route that is configured by the network administrator as the route to use if there are no matches in the routing table.
- If there is no default route, the packet is discarded. A message is often sent back to the device that sent the data to indicate that the destination was unreachable.

Routing tables

- Contain route information.
- Used for process of path determination.
- Routing protocols fill routing tables with a variety of route information.
- This information varies depending on the routing protocol used eg..

Learned	N/W address	Hop	Interface

C	192.168.1.0	0	E1
C	192.168.2.0	0	E0
R	192.168.5.0	1	S0
R	192.168.6.0	1	S0

C – Refers to Directly connected interfaces
R - Refers to the entry made by RIP in routing table
Hop count – refers to the distance or number of routers till those networks,
Interface – refers to the port through which the data must be sent out to get to the destination network

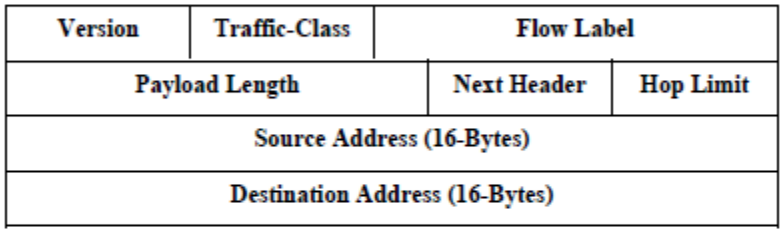
Routing Protocol Metrics : Following are the important routing parameters that may be used in combination to decided the best path by router.

- **Bandwidth** – The data capacity of a link. Normally, a 10-Mbps Ethernet link is preferable to a 64-kbps leased line.
- **Delay** – The length of time required to move a packet along each link from source to destination. Delay depends on the bandwidth of intermediate links, network congestion, and physical distance.
- **Load** – The amount of activity on a network resource such as a router or a link.
- **Reliability** – Usually a reference to the error rate of each network link
- **Hop count** – The number of routers that a packet must travel through before reaching its destination. If multiple paths are available to a destination, the path with the least number of hops is preferred.
- **Ticks** –One tick is approximately 1/18 second.
- **Cost** – An arbitrary value, usually based on bandwidth monetary expense, or other measurement, that is assigned by a network administrator.

Question No-( ):What are various fields in the IPV6? How addressing scheme is different here than that of IPv4?

Answer:( ):- IPV6:- IP Version 6 is being developed to deal with the problem of IPV4-Address shortage and address wastage. It is just under research and could not be implemented till now. Once implemented all network hardware will require to be replaced.

Following are the fields in IPV6.



Version: Version field is same and represent the version of the IP. Obviously it will be Six in case of IPV6 headers.

Traffic Class:- Traffic class filed is used to distinguish between packets with different real-time delivery requirements. It can inform the router about the importance and priority of the packet.

Flow Label:- The flow label field will be used to allow a source and destination to set up a pseudo connection with particular properties and requirements. Flow label field can identify that particular connection and can inform the router that this packet belongs to that connection with specified properties.

Payload Length:- This field tells how many bytes follows the 40-byte header. The 40-byte header bytes are no longer counted as part of the length.

Next Header:- The next header field lets the cat out of the bag. This field tells which of the(currently) six extension headers, if any follow this one. If this header is the last IP header, the Next header filed tells which transport protocol handler (e.g. TCP, UDP) to pass the packet to.

Hop-Limit:- This field is used to keep packets from living forever. This represents the number of routers after which packet will be discarded if could reach the destination.

Source Address:- Source Address filed identifies the address of the source machine from where the packet was generated. This is of 16-bytes.

Destination Address:- Destination Address filed identifies the address of the destination machine where the packet has to sent. This is of 16-bytes.

Addressing Scheme of IPV6 is different than that of IPV4:-

- IPV4 addressing was of 32-bits, IPV6 addressing uses 128-bits.
- IPV4 addressing uses decimal dotted notation. IPV6 uses hexadecimal notations.
- IPV4 used net-id and host-id concept. Whereas in IPV6 address is not divided into host and network portions.
- In IPV4 8-bits are grouped as a single group. Dots are used between two groups.
  In IPV6 32-bits are grouped as a single group. Colons are used between two groups.
- Example:
  IPV4 IP Address: - 192.168.1.1
  IPV6 IP Address: - 8000 : AACF: 5563 : B3B5 : 1112 : 1121 : 1123 : AAAB

Question No-( ): What is count to infinity problem? How it can be avoided by split horizon?

Answer:- **Count to Infinity Problem**:- Distance Vector routing algorithm works in theory but has a serious drawback in practice: Although it converges to the correct answer, it may do it so slowly. In practice it, it reacts rapidly to good news, but leisurely to bad news.

Assume there are five nodes in a subnet, where the delay metric is the number of hops, Suppose A is down initially and router knows this. They have all recorded the delay to A as infinity.

A	B	C	D	E	
-	-	-	-	-	Initially
1	_	_	_		After 1 exchange
1	2	_	_		After 2 exchange
1	2	3	_		After 3 exchange
1	2	3	4		After 4 exchange

When A comes up, the other routers learn about it via the vector exchanges. Let us assume that there is gigantic gong somewhere that is stuck periodically to initiate a vector exchange at all routers simultaneously.

Now let us assume the different situation in which all the lines and routers are up initially. Suddenly A goes down. At the first packet exchange, B does not hear anything from A. Fortunately C says : Don't worry I have a path to A of length 2, due to this entire scenario will get confused and will try a path to A through B or other routers.

A	B	C	D	E	
1	2	3	4		After 1 exchange
-	2	3	4		After 2 exchange

3 2 3 4 After 3 exchange

.....

.....

Therefore due to the delay in communication all routers may continue to change their routing tables through wrong paths and metrics will continue to increase.

Split Horizon can limit the problem of count to infinity problem.

Split Horizon is a mechanism used to avoid routing loops. Information about routes is prevented from being advertised out the router interface through which the information was received.

1. Router A advertises route to Network A
2. Router B updates its routing table
3. Router B does not include Network A in update to A