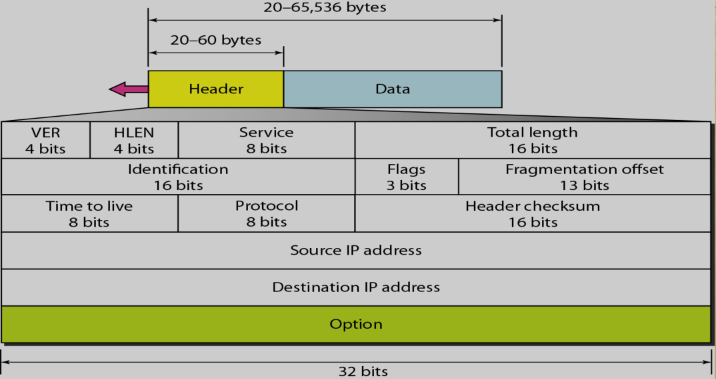
Module 3 QB

**1. Format of the IPv4 header. Describe the significance of each field.**



* Version(VER): 4-bit field defines the version [Version 4] of IP software running
* Header Length(HLEN): 4 bit field defines the total length of the datagram header
* Service Type: It define how the datagram should be handled.
* Total Length: This is a 16 bit field that defines the IP datagram's total length (header plus data).
* Identification, Flags, Fragmentation offset: used in fragmentation
* Time to Live: A datagram has a limited lifetime in its travel through an internet.
* Checksum : to detect corruption in Header
* Source Address: 32 bit field defines the IP address of the source.
* Destination Address: 32 bit field defines the IP address of the destination.

---------------------------------------------------------------------

2. Write about various classes of IP addresses.

IP Address:   
Identifier used in the IP layer to identify each device connected to the internet.

It is a 32-bit long address, unique and universal.

Address space- is the total number of addresses used by the protocol.

The address space of IPv4 is 2^32 or 4,294,967,296.

IP address space is divided into five classes: A, B, C, D and E.

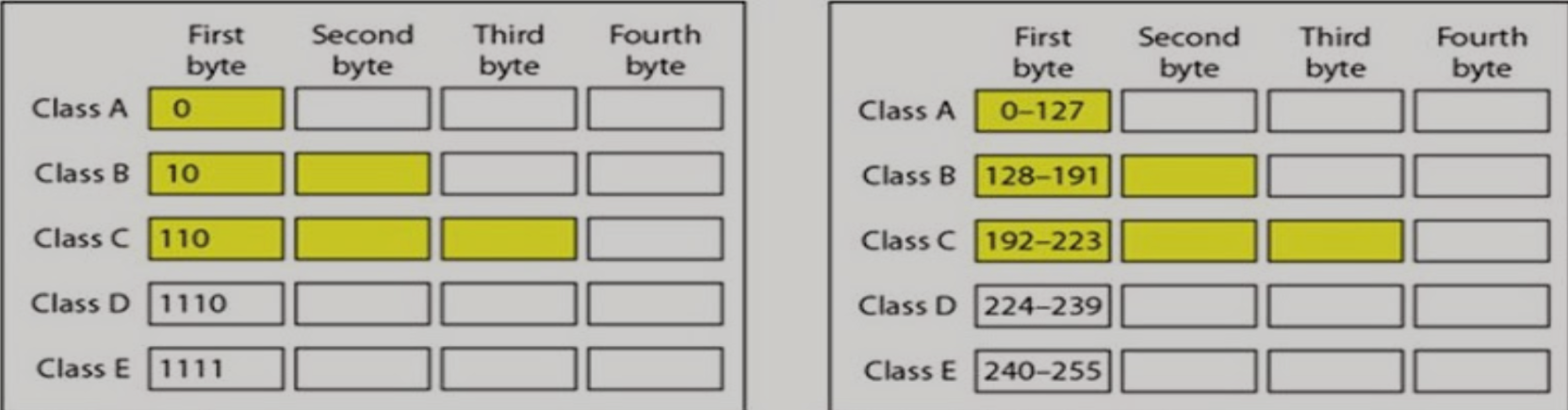
Class A: 2 31 = 2,147,483,648 addresses, 50%

Class B: 2 30 = 1,073,741,824 addresses, 25%

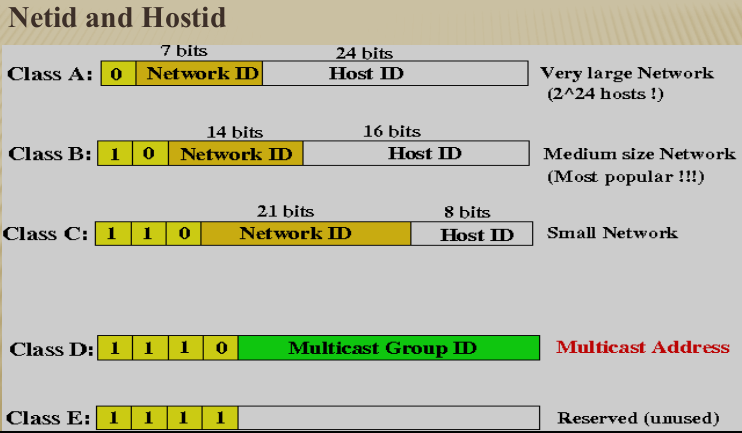
Class C: 2 29 = 536,870,912 addresses, 12.5%

Class D: 2 28 = 268,435,456 addresses, 6.25%

Class E: 2 28 = 268,435,456 addresses, 6.25%

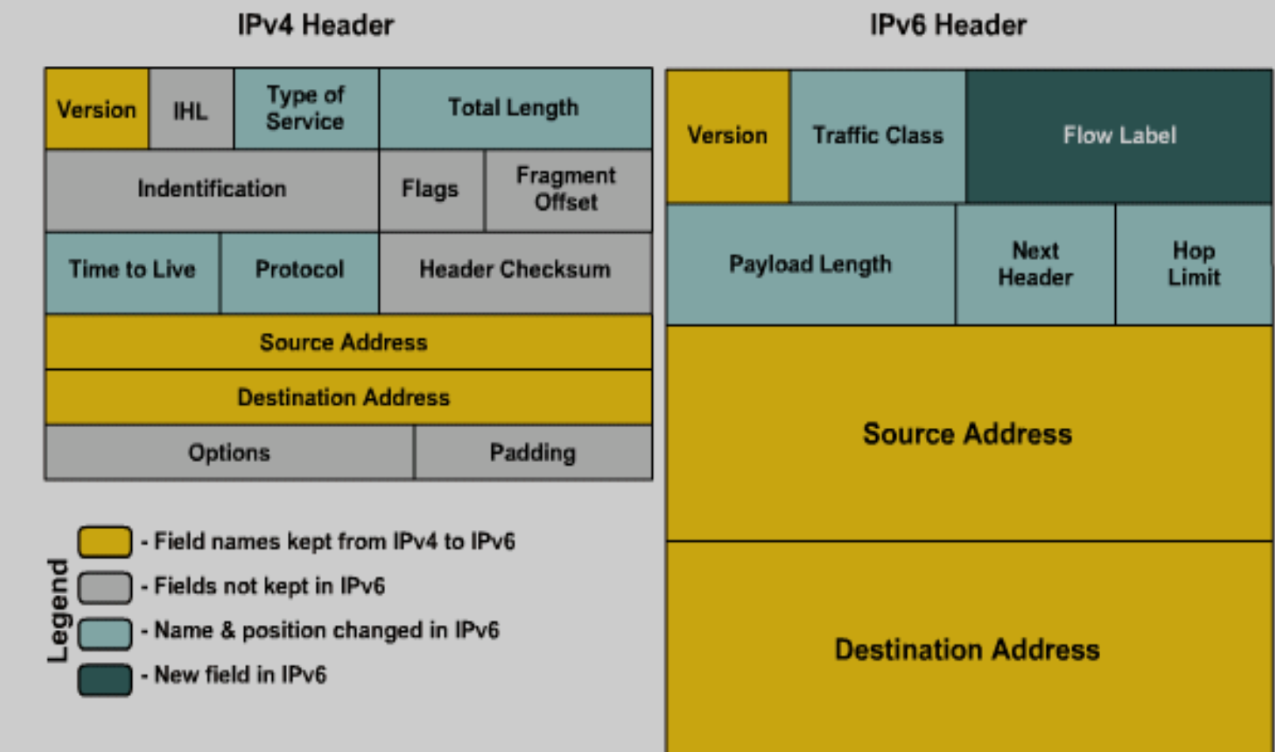


Netid and Hostid :



---------------------------------------------------------------------

**3. Format of the IPv6 header. Describe the significance of each field.**



Based on these rules, RFC 2460 defines the following IPv6 header fields:

header length fixed at 40 byte

Version: 4 bits are used to indicate the version of IP and is set to 6

Traffic Class (8 bits): the same function as the Type of Service field in the IPv4 header.

Flow Label (20 bits): identifies a flow and it is intended to enable the router to identify packets that should be treated in a similar way without the need for deep lookups

within those packets.

Payload Length (16 bits):

Indicate the length of the payload (length of the entire packet)

Next Header (8 bits):

Indicates either the first extension header (if present) or the protocol in the

upper layer PDU (such as TCP, UDP, or ICMPv6).

Hop Limit (8 bits):

In IPv6, the IPv4 TTL was appropriately renamed Hop Limit because it is a

variable that is decremented at each hop, and it does not have a temporal

dimension.

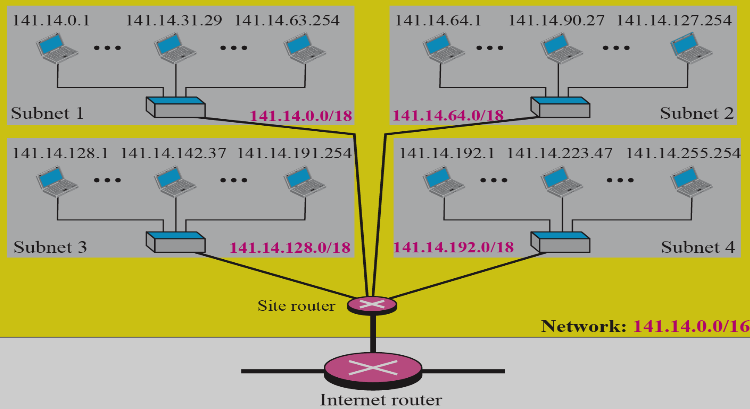
Source IPv6 Address (128 bits): Stores the IPv6 address of the originating host.

Destination IPv6 Address (128 bits): Stores the IPv6 address of the current destination host.

---------------------------------------------------------------------**4. What is Subnetting?**

* Splitting a block to smaller blocks is subnetting
* In Subnetting, a network is divided into several smaller subnetworks (subnets) with each subnetworking having its own subnetwork address.

* It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.
* It also helps you to reduce the size of the routing tables, which is stored in routers.
* This method also helps you to extend the existing IP address base & restructures the IP address.



---------------------------------------------------------------------

5. Distinguish between IPV4 vs IPv6 Protocol.

| Sr. No. | IPv4 | IPv6 |
| --- | --- | --- |
| 1 | IPv4 has a 32-bit address length | IPv6 has 128-bit address length |
| 2 | It Supports Manual and DHCP address configuration. | It supports Auto and Renumbering address configuration. |
| 3 | Address space: 2^32 | Address space : 2^128 |
| 4 | Address representation of IPv4 is in decimal | Address representation of IPv6 is in hexadecimal |
| 5 | In IPv4 Packet flow identification isn’t available | In IPv6 Packet flow identification are  availablwe |
| 6 | In IPv4 checksum field is available | In IPv6 checksum field isn’t available |
| 71 | In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication facility are provided |
| 8 | IPv4 has a header of 20-60 bytes | IPv6 has a header of 40 bytes |
| 9 | IPv4 consists of 4 fields which are separated by a dot (.) | IPv6 consists of 8 fields which are separated by a colon (:) |
| 10 | IPv4’s IP addresses are divided into 5 different classes: Class A, Class B, Class C, Class D, and Class E | IPv6 doesn’t have any classes of IP addresses |
| 11 | Example of IPv4:  66.94.29.13 | Example of IPv6:  ::/0 |

---------------------------------------------------------------------6. What is Network Address Translation (NAT)?  
  
 To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required.

Network Address Translation (NAT) is a process in which one or more local IP addresses are translated into one or more Global IP addresses 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 has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverses outside the local (inside) network, 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.

---------------------------------------------------------------------7. What is the difference between Broadcasting and Multicasting?

| S.No. | Broadcast | Multicast |
| --- | --- | --- |
| 1 | It has one sender and multiple receivers. | It has one or more senders and multiple receivers. |
| 2 | It sends data from one device to all the other devices in a network. | It sends data from one device to multiple devices. |
| 3 | It works on star and bus topology. | It worlds on star, mesh, tree and hybrid topology. |
| 4 | It scales well across LAN. | It doesn’t scale well across LAN. |
| 5 | Its bandwidth is wasted. | It utilizes bandwidth efficiently. |
| 6 | It has one-to-all mapping. | It has one-to-many mapping. |
| 7 | Device Eg. Hub | Device Eg. Switch |

---------------------------------------------------------------------

8. Explain Link state routing.

Link state routing is a method in which each router shares its neighborhood’s knowledge with every other router in the internetwork. In this algorithm, each router in the network understands the network topology and then makes a routing table depending on this topology.

Each router will share data about its connection to its neighbor, who will, consecutively, reproduce the data to its neighbors, etc. This appears just before all routers have constructed a topology of the network.

In LSP, each node transmits its IP address and the MAC to its neighbor with its signature. Neighbors determine the signature and maintain a record of the combined IP address and the MAC. The Neighbour Lookup Protocol (NLP) of LSP derives and maintains the MAC and IP address of every network frame accepted by a node. The extracted data can support the mapping of MACs and IP addresses. The link-state flooding algorithm prevents the general issues of broadcast in the existence of loops by having every node maintain a database of all LSP messages. The creator of each LSP contains its identity, data about the connection that has changed status, and also a sequence number.

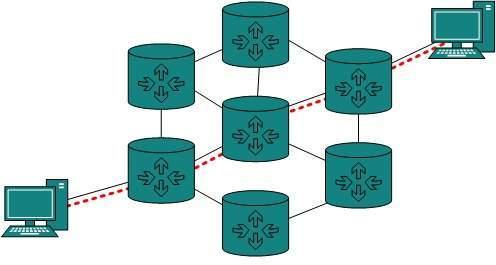
---------------------------------------------------------------------

9. Discuss the internetworking of network layers on the internet.

Routing between two networks is called internetworking.

Networks can be considered different based on various parameters such as Protocol, topology, Layer-2 network, and addressing scheme.

In internetworking, routers have knowledge of each other’s addresses and addresses beyond them. They can be statically configured to go on different networks or they can learn by using an internetworking routing protocol.

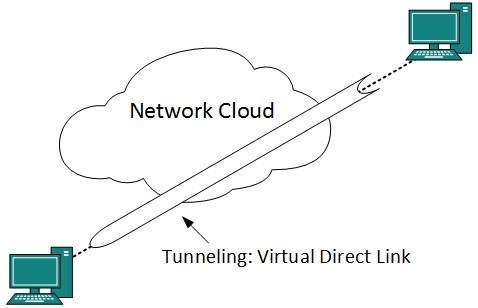


Routing protocols that are used within an organization or administration are called Interior Gateway Protocols or IGPs. RIP and OSPF are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.

Tunneling

If they are two geographically separate networks, which want to communicate with each other, they may deploy a dedicated line between or they have to pass their data through intermediate networks.

Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends.



When the data enters from one end of the Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists in the Tunnel its tag is removed and delivered to the other part of the network.

Both ends seem as if they are directly connected and tagging makes data travel through the transit network without any modifications.

Packet Fragmentation

Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.

If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.

If a packet with DF (don’t fragment) bit set to 1 comes to a router which can not handle the packet because of its length, the packet is dropped.

When a packet is received by a router that has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet are on the way.

If the packet is fragmented too small, the overhead increases. If the packet is fragmented too large, the intermediate router may not be able to process it and it might get dropped.

---------------------------------------------------------------------

10. With an example explain the Dynamic routing algorithms used in computer networks.

Dynamic routing is an adaptive routing algorithm, and it is a process where a router can forward data through a different route.

The term is most associated with data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so if other path choices are available. Dynamic routing allows many routes to remain valid in response to the change.

Systems that do not implement dynamic routing are usually preferred to static routing, because static routes through a network are described by fixed paths. If anything, those that take an affected path will either have to wait for the failure to be repaired before restarting its journey or will have to fail to reach its destination and give up the journey.

Uses

The benefits of using a dynamic routing protocol are as follows −

* The routers can exchange routing information whenever there is a topology change.
* This exchange allows routers to automatically learn about new networks and to find alternate paths if there is a link failure to a current network.

Advantages

The advantages of dynamic routing algorithm are as follows −

* Dynamic routing is simpler to configure on larger networks.
* If a link goes down this technique can choose a better router dynamically.
* It has the ability to load balance between multiple links.

Disadvantages

The disadvantages of dynamic routing algorithm are as follows −

* Dynamic routing consumes more bandwidth because updates are shared between routers.
* In dynamic routing, the routing protocols keep an additional load on the router.

Working condition

The working condition of dynamic routing is explained below in a stepwise manner −

Step 1 − In dynamic routing a routing protocol must be installed on every router in the internetwork.

Step 2 − Starting manually to enter the first hop of the routing table of one router with routing information, and then the routing protocol takes over and dynamically builds the routing table for each router.

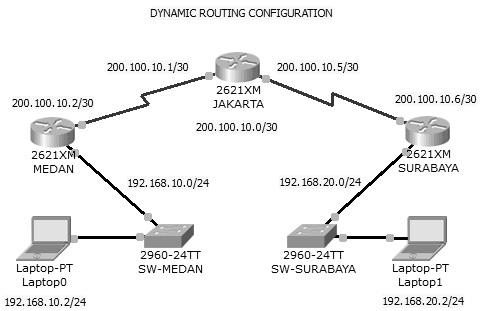
Step 3 − Routers exchange their routing information so that if the internetwork is reconfigured or it goes down, the routing tables of each router are modified accordingly.

Step 4 − Hosts on a network need only be configured so that their default gateway address matches the IP address of the local router interface.

Step 5 − Dynamic routers are simpler to administer than static routers, but they are sometimes less secure.

Step 6 − If the network is reconfigured or a router goes down, it takes time for this information to propagate between the various routers on the network.

The diagram given below depicts the dynamic routing algorithm −



---------------------------------------------------------------------

11. Explain the Distance Vector routing algorithm with an example.

In distance-vector routing (DVR), each router is required to inform the topology changes to its neighboring routers periodically. Historically it is known as the old ARPANET routing algorithm or Bellman-Ford algorithm.

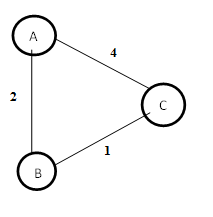
How the DVR Protocol Works

* In DVR, each router maintains a routing table. It contains only one entry for each router. It contains two parts − a preferred outgoing line to use for that destination and an estimate of time (delay). Tables are updated by exchanging the information with the neighbor’s nodes.
* Each router knows the delay in reaching its neighbors (Ex − send echo request).
* Routers periodically exchange routing tables with each of their neighbors.
* It compares the delay in its local table with the delay in the neighbor’s table and the cost of reaching that neighbor.
* If the path via the neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor.

Example − Distance Vector Router Protocol

In the network shown below, there are three routers, A, B, and C, with the following weights − AB =2, BC =3 and CA =5.

Step 1 − In this DVR network, each router shares its routing table with every neighbor. For example, A will share its routing table with neighbors B and C and neighbors B and C will share their routing table with A.



| Form A | A | B | C |
| --- | --- | --- | --- |
| A | 0 | 2 | 3 |
| B |  |  |  |
| C |  |  |  |

| Form B | A | B | C |
| --- | --- | --- | --- |
| A |  |  |  |
| B | 2 | 0 | 1 |
| C |  |  |  |

| Form C | A | B | C |
| --- | --- | --- | --- |
| A |  |  |  |
| B |  |  |  |
| C | 3 | 1 | 0 |

Step 2 − If the path via a neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor. In this table, the router updates the lower cost for A and C by updating the new weight from 4 to 3 in router A and from 4 to 3 in router C.

| Form A | A | B | C |
| --- | --- | --- | --- |
| A | 0 | 2 | 3 |
| B |  |  |  |
| C |  |  |  |

| Form B | A | B | C |
| --- | --- | --- | --- |
| A |  |  |  |
| B | 2 | 0 | 1 |
| C |  |  |  |

| Form C | A | B | C |
| --- | --- | --- | --- |
| A |  |  |  |
| B |  |  |  |
| C | 3 | 1 | 0 |

Step 3 − The final updated routing table with lower cost distance vector routing protocol for all routers A, B, and C is given below −

Router A

| Form A | A | B | C |
| --- | --- | --- | --- |
| A | 0 | 2 | 3 |
| B | 2 | 0 | 1 |
| C | 3 | 1 | 0 |

Router B

| Form B | A | B | C |
| --- | --- | --- | --- |
| A | 0 | 2 | 3 |
| B | 2 | 0 | 1 |
| C | 3 | 1 | 0 |

Router C

| Form C | A | B | C |
| --- | --- | --- | --- |
| A | 0 | 2 | 3 |
| B | 2 | 0 | 1 |
| C | 3 | 1 | 0 |

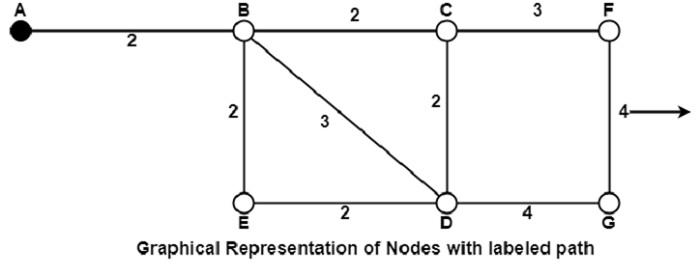
---------------------------------------------------------------------

12. Explain the shortest path routing algorithm with an example.

In computer networks, the shortest path algorithms aim to find the optimal paths between the network nodes so that routing cost is minimized. They are direct applications of the shortest path algorithms proposed in graph theory.

Explanation

Consider that a network comprises N vertices (nodes or network devices) that are connected by M edges (transmission lines). Each edge is associated with a weight, representing the physical distance or the transmission delay of the transmission line. The target of shortest path algorithms is to find a route between any pair of vertices along the edges, so the sum of weights of edges is minimum. If the edges are of equal weights, the shortest path algorithm aims to find a route having a minimum number of hops.  
For example, Djikstra uses node labeling with its distance from the source node along the better-known route. Initially, all nodes are labeled with infinity, and as the algorithm proceeds, the label may change. The labeling graph is displayed in the figure.



It can be done in various passes as follows, with A as the source.

* Pass 1. B (2, A), C(∞,−), F(∞,−), e(∞,−), d(∞,−), G 60
* Pass 2. B (2, A), C(4, B), D(5, B), E(4, B), F(∞,−),G(∞,−)
* Pass 3. B(2, A), C(4, B), D(5, B), E(4, B), F(7, C), G(9, D)

---------------------------------------------------------------------

13. What is the significance of The Network layer on the internet?

Layer 3 in the OSI model is called the Network layer. The network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

The network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnets may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnets may be operating on different protocols which are not compatible with each other. The network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Layer-3 Functionalities

Devices which work on Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:

* Addressing devices and networks.
* Populating routing tables or static routes.
* Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
* Internetworking between two different subnets.
* Delivering packets to destination with best efforts.
* Provides connection oriented and connection less mechanism.

Network Layer Features

With its standard functionalities, Layer 3 can provide various features as:

* Quality of service management
* Load balancing and link management
* Security
* Interrelation of different protocols and subnets with different schema.
* Different logical network designs over the physical network design.
* L3 VPN and tunnels can be used to provide end-to-end dedicated connectivity.

Internet protocol is a widely respected and deployed Network Layer protocol that helps to communicate end-to-end devices over the internet. It comes in two flavors. IPv4 has ruled the world for decades but now is running out of address space. IPv6 is created to replace IPv4 and hopefully mitigates the limitations of IPv4 too.  
---------------------------------------------------------------------

14. Describe the Optimality Principle for Routing.

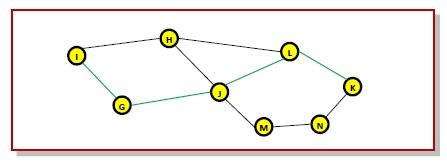
The purpose of a routing algorithm at a router is to decide which output line an incoming packet should go. The optimal path from a particular router to another may be the least cost path, the least distance path, the least time path, the least hop path or a combination of any of the above.

The optimality principle can be logically proved as follows −

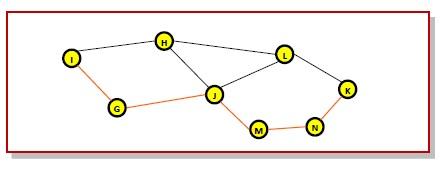
* If a better route could be found between router J and router K, the path from the router I to router K via J would be updated via this route. Thus, the optimal path from J to K will again lie on the optimal path from I to K.

Example

Consider a network of routers, {G, H, I, J, K, L, M, N} as shown in the figure. Let the optimal route from I to K be as shown via the green path, i.e. via the route I-G-J-L-K. According to the optimality principle, the optimal path from J to K with be along the same route, i.e. J-L-K.



Now, suppose we find a better route from J to K is found, say along J-M-N-K. Consequently, we will also need to update the optimal route from I to K as I-GJ- M-N-K, since the previous route ceases to be optimal in this situation. This new optimal path is shown line orange lines in the following figure −



---------------------------------------------------------------------