Module 3 QB

[**What is the format of the IPv4 header? Describe the significance of each field. 2**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.nzdnu2dpwlmg)

[**With an example explain the Dynamic routing algorithms used in computer networks. 3**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.dhwf0gmk4jkx)

[Uses 3](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.7a7q3i9gremf)

[Advantages 3](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.dbgfqokgo2t)

[Disadvantages 4](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.dkvscpczqx8g)

[Working condition 4](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.l262e34oyqkg)

[**What is the difference between Broadcasting and Multicasting? 5**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.jbttsx97akhx)

[**Explain Distance Vector routing algorithm with an example. 6**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.h29u4btx44xf)

[How the DVR Protocol Works 6](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.6jmby2yzzax)

[Example − Distance Vector Router Protocol 6](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.k1n8me6icevc)

[Router A 8](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.b9k90xj5kt0e)

[Router B 9](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.y2ut7issie7c)

[Router C 9](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.snqjd0i9zsd4)

[**Explain the shortest path routing algorithm with an example. 9**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.2z7hmvlm57o7)

[Explanation 9](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.ckfnsrpd4vlv)

[**Discuss the internetworking of network layers on the internet. 10**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.2bi7snqqchvh)

[Tunneling 11](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.cfbe4kl2fglg)

[Packet Fragmentation 12](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.ogdunvico3to)

[Layer-3 Functionalities 13](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.mxyni9awtwei)

[Network Layer Features 14](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.ofw1z99fcxgq)

[**Describe Optimality Principle for Routing 14**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.ziibl3kvc9vw)

[Example 14](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.galdhzq8eorc)

[**Distinguish between IPV4 vs IPv6 Protocol. 17**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.58u6wounwvk7)

[**What is the format of the IPv6 header? Describe the significance of each field. 18**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.suqshet0i9io)

[**What is Subnetting? 19**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.gg3kg5etklrm)

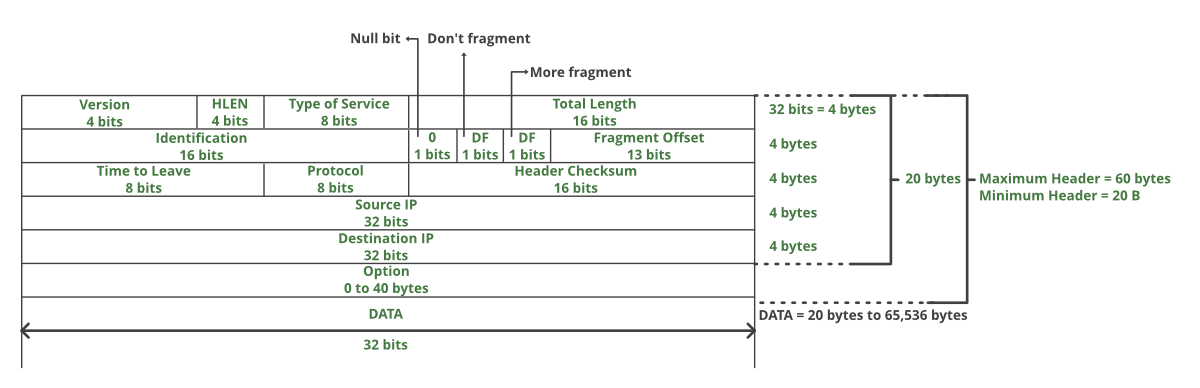
[**Explain Link state routing. 20**](https://docs.google.com/document/d/1MznlKXKUWLASik_LF8soUD2N7oFCF80mcdkOq7dy5lA/edit#heading=h.uvc9drqzg4oc)

1. **What is the format of the IPv4 header? Describe the significance of each field.**

* IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured.
* Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks.
* IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.
* IPv4 is defined and specified in IETF publication RFC 791.
* IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for military purposes, while class E addresses are reserved for future use.
* IPv4 uses 32-bit (4 byte) addressing, which gives 232 addresses. IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.

IPv4 Datagram Header

Size of the header is 20 to 60 bytes.



1. **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.

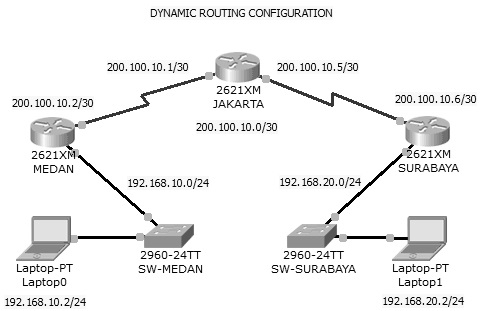
Step 3 − Routers exchange their routing information so that if the internetwork is reconfigured or it goes down, the routing tables of each router are modified accordingly.

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 −



1. **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 utilises bandwidth efficiently. |
| **6** | It has one-to-all mapping. | It has one-to-many mapping. |
| **7** | Device eg. Hub | Device Eg. Switch |

1. **Explain 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.

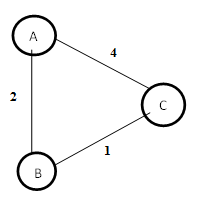
How the DVR Protocol Works

* 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

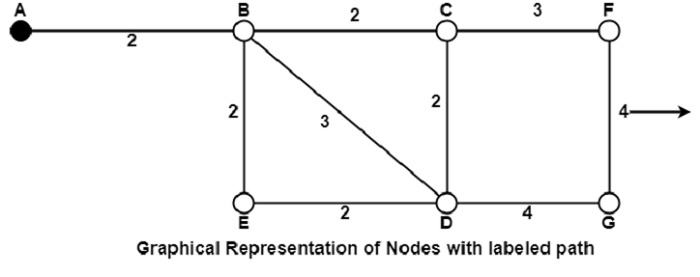
|  |  |  |  |
| --- | --- | --- | --- |
| Form C | A | B | C |
| A | 0 | 2 | 3 |
| B | 2 | 0 | 1 |
| C | 3 | 1 | 0 |

1. **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, Dijikstra uses the nodes labelling with its distance from the source node along the better-known route. Initially, all nodes are labelled with infinity, and as the algorithm proceeds, the label may change. The labelling graph is displayed in the figure.



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

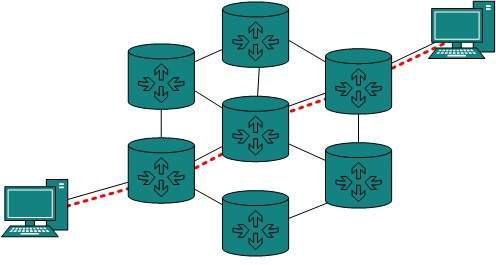
* Pass 1. B (2, A), C(∞,−), F(∞,−), e(∞,−), d(∞,−), G 60
* Pass 2. B (2, A), C(4, B), D(5, B), E(4, B), F(∞,−),G(∞,−)
* Pass 3. B(2, A), C(4, B), D(5, B), E(4, B), F(7, C), G(9, D)

1. **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 address and addresses beyond them. They can be statically configured to go on different networks or they can learn by using internetworking routing protocol.

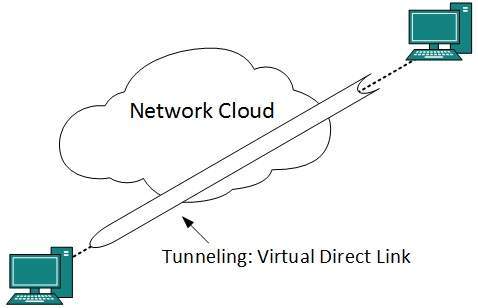


Routing protocols which are used within an organization or administration are called Interior Gateway Protocols or IGP. RIP, OSPF are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.

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.

1. **What is the significance of The Network layer in the internet**

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

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. 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 design over the physical network design.
* L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

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

1. **Describe Optimality Principle for Routing**

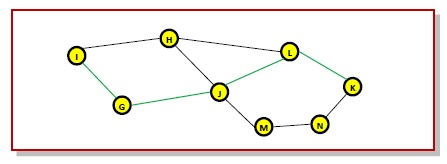
The purpose of a routing algorithm at a router is to decide which output line an incoming packet should go. The optimal path from a particular router to another may be the least cost path, the least distance path, the least time path, the least hop path or a combination of any of the above.

The optimality principle can be logically proved as follows −

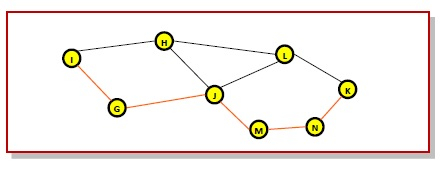
* If a better route could be found between router J and router K, the path from router I to router K via J would be updated via this route. Thus, the optimal path from J to K will again lie on the optimal path from I to K.

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 −



1. Write about various classes of IP addresses.  
   IP Address: identifier used in IP layer to identify each device connected to the internet

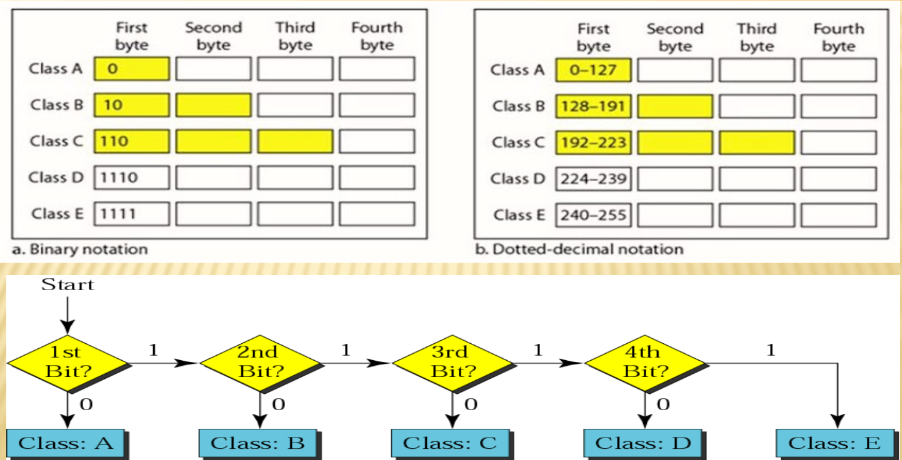
It is a 32 bit long address ,unique and universal.

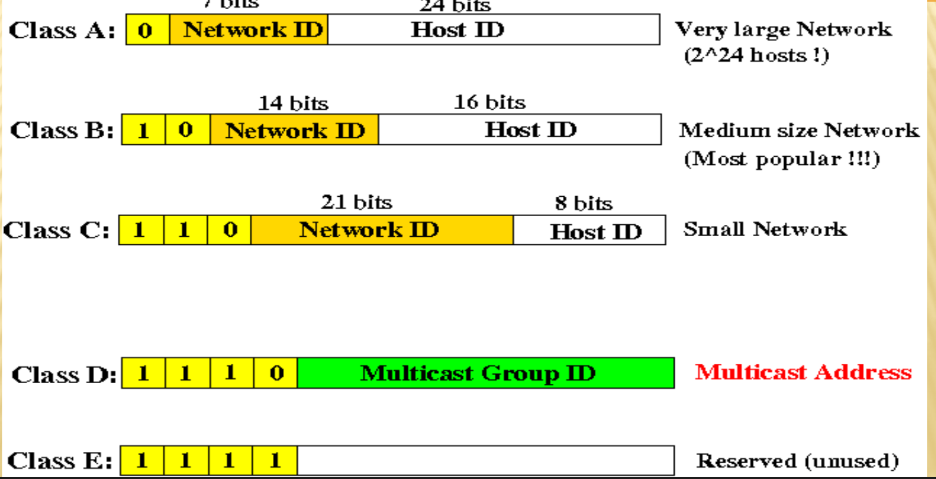
IPv4 addresses have address space.

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

If a protocol uses N bits to define an address, the address space is 2N because each bit can have two different values (0 and 1) and N bits can have 2N values.

The address space of IPv4 is 232 or 4,294,967,296.

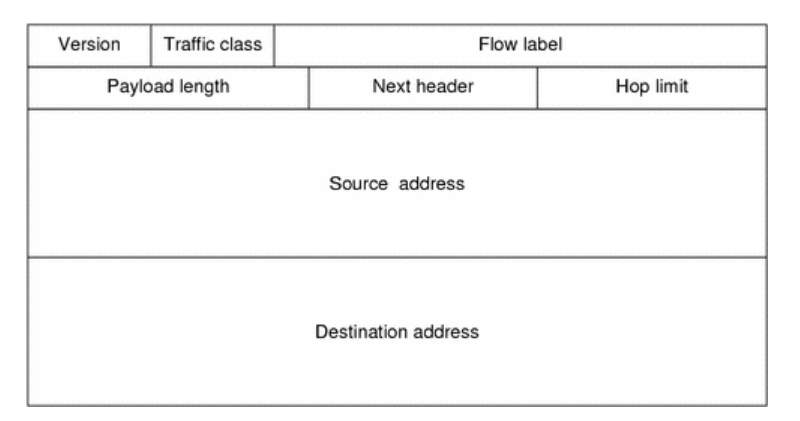




1. Distinguish between IPV4 vs IPv6 Protocol.

|  |  |  |
| --- | --- | --- |
| **S. 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** | In IPv4 end to end, connection integrity is unachievable | In IPv6 end to end, connection integrity is achievable |
| **4** | It can generate 4.29 x 109 address space. | Address space of IPv6 is quite large, it can produce 3.4 x 1038 address space |
| **5** | The security feature is dependant on application. | IPSEC is an inbuilt security feature in the IPv6 protocol |
| **6** | Address representation of IPv4 is in decimal | Address representation of IPv6 is in hexadecimal |
| **7** | Fragmentation performed by Sender and forwarding Routers | In IPv6 fragmentation is performed only by the sender |
| **8** | In IPv4 Packet flow identification isn’t available | In IPv6 Packet flow identification are  availablw, and uses the flow label field in the header |
| **9** | In IPv4 checksum field is available | In IPv6 checksum field isn’t available |
| **10** | It has broadcast message transmission scheme | In IPv6, multicast and anycast message transmission scheme is available |
| **11** | In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication facility are provided |
| **12** | IPv4 has a header of 20-60 bytes | IPv6 has a header of 20-60 bytes |
| **13** | IPv4 consists of 4 fields which are separated by dot (.) | IPv6 consists of 8 fields which are separated by colon (:) |
| **14** | IPv4’s IP addresses are divided into 5 different classes: Class A,Class B, Class C, Class D, Class E | IPv6 doesn’t have any classes of IP addresses |
| **15** | IPv4 supports VLSM (Variable Length subnet mask). | IPv6 doesn’t support VLSM |
| **16** | Example of IPv4:  66.94.29.13 | Example of IPv6:  2001:0000:3238:DFE1:0063:0000:0000:FEFB |

1. **What is the format of the IPv6 header? Describe the significance of each field.**



* Traffic Class
* This field represents the class or priority of the IPv6 packet.
* Its size is eight bits.
* The Traffic Class field has the same functionality as the Service field of IPv4.
* There is need of IPv6 implementation for the purpose of providing a means for an application layer protocol to mention the Traffic
* Class field value to test.

* Flow Label
* This field point outs that the respective packet is concerned with a particular order of packets between a source and destination,

having special handling by intermediate IPv6 routers.

* This field has a size of 20 bits.
* The use of Flow Label is for non-default quality of service connections, for example those required by real-time data (voice and video).
* For the purpose of default router handling, the value of Flow Label is set as 0. There is a possibility of multiple flows between a source and destination, as differentiated by individual non-zero Flow Label.

* Payload Length
* This field represents the length of the IPv6 payload. (ii) This field has a size of 16 bits.
* This field contains the extension headers as well as the upper layer PDU (Protocol Data Unit). (iv) Using 16 bits, it is possible to indicate an IPv6 payload of up to 65,535 bytes.
* For payload greater than 65.535 bytes, payload field is set to 0 and Jumbo payload option is used in Hop-by-Hop Options extension header.

* Next Header (8 bits)
* Specifies the type of the next header.
* This field usually specifies the transport layer protocol used by a packet's payload.

* Hop Limit(8 bits)
* Replaces the time to live field of IPv4.
* This value is decremented by one at each forwarding node and the packet discarded if it becomes 0.
* However, the destination node should process the packet normally even if the hop limit becomes 0.
* Source Address (128 bits) : The IPv6 address of the sending node.
* Destination Address (128 bits) : The IPv6 address of the destination node(s).

1. **What is Subnetting?**

* Subnetting is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.
* IP Subnetting designates high-order bits from the host as part of the network prefix. This method divides a network into smaller subnets.
* 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.

1. **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 which 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.

1. **Explain Link state routing.**

Link state routing is a method in which each router shares its neighbourhood’s knowledge with every other router in the internetwork. In this algorithm, each router in the network understands the network topology then makes a routing table depend on this topology.  
Each router will share data about its connection to its neighbour, who will, consecutively, reproduce the data to its neighbours, 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 neighbour with its signature. Neighbours determine the signature and maintain a record of the combining 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.