3
UNIT

Network Layer

CONTENTS

PART-1

Network Layer : Point-to-Point Network.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.1. What are the duties of network layer ?

Answer

Duties of network layer are :

1. **Internetworking :** This is the main duty of network layer. It provides the logical connection between different types of networks.
2. **Addressing :**
   a. Addressing identify each device on the internet. This is similar to a telephone system.
   b. The addresses used in the network layer should be able to uniquely define the connection of a computer to the internet universally.
3. **Routing :**
   a. In a network, there are multiple roots available from a source to a destination and one of them is to be chosen.
   b. The network layer decides which root is to be taken. This is called as routing and it depends on various criterions.
4. **Packetizing :**
   a. The network layer receives the packets from upper layer protocol and encapsulates them to form new packets.
   b. This is called as packetizing. A network layer protocol called IP (Internetworking Protocol), does the job of packetizing.
5. **Fragmenting :** The sent datagram can travel through different networks. Each router decapsulates the IP datagram from the received frame. Then the datagram is processed and encapsulated in another frame.

Que 3.2. Describe design issues in network layer.

Answer

1. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are wired into the network and rarely changed. They can also be highly dynamic,

being determined as new for each packet, to reflect the current network load.

2. If too many packets are present in the subnet at the same time, they will get into one another's way, forming bottlenecks. The control of such congestion also belongs to the network layer.
3. Moreover, the quality of service provided (delay, transmit time, jitter, etc) is also a network layer issue.
4. When a packet has to travel from one network to another to get to its destination, many problems can arise such as:
   a. The addressing used by the second network may be different from the first one.
   b. The second one may not accept the packet at all because it is too large.
   c. The protocols may differ, and so on.
5. It is upto the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

PART-2

Routing.

CONCEPT OUTLINE

- Various types of routing algorithm :
  i. Dynamic/Adaptive routing
  ii. Static/Non-adaptive routing

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.3. Write down class of routing algorithms.

OR

What is adaptive routing algorithm ? Explain various types of adaptive routing algorithm.

Answer

Various types (class) of routing algorithm are :

1. **Dynamic / Adaptive algorithms :**
   a. Adaptive algorithms (dynamic routing) use such dynamic information as current topology, load, delay, etc., to select routes.

b. A dynamic algorithm can be run either periodically or in direct response to topology or link cost change.

c. While dynamic algorithms are more responsive to network changes, they are also more susceptible to problems such as routing loops and oscillation in routes.

d. Adaptive algorithms can be further divided in the following types :

i. **Isolated :** Each router makes its routing decisions using only the local information that it store. Specifically, routers do not even exchange information with their neighbours.

ii. **Centralized :** A centralized node makes all routing decisions. Specifically, the centralized node has access to global information.

iii. **Distributed :** Algorithms that uses a combination of local and global information.

2. **Static / Non-adaptive algorithms :**

a. In non-adaptive algorithms, routes never change, once initial routes have been selected, also called static routing.

b. In static routing algorithms, routes change very slowly over time, often as a result of human intervention (for example, a human manually editing a router's forwarding table).

c. Non-adaptive algorithms do not handle failed links.

Que 3.4. Differentiate between adaptive and non-adaptive routing algorithms.

Answer

S. No.	Adaptive routing algorithm	Non-adaptive routing algorithm
1.	In adaptive algorithm, routers exchange and update router table information.	In non-adaptive algorithm, network administrator manually enters routing paths into the router.
2.	In this algorithm, routers adjust automatically in response to changes in network topology.	In this algorithm, adjustments to changes in network topology require manual update.
3.	It prevents packet delivery failure and improves network performance.	It provides granular control over packet paths.
4.	It is dynamic routing.	It is static routing.
5.	It uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.	It manually sets up the optimal paths between the source and the destination computers.

Que 3.5. **What is meant by unicast and multicast routing with suitable diagrams ?** **AKTU 2013-14, Marks 05**

Answer

Unicast routing :

1. In unicast routing, there is one-to-one relation between the source and the destination. That means only one source sends packets to only one destination.
2. The type of source and destination addresses included in the IP datagram are unicast addresses assigned to the hosts as shown in Fig. 3.5.1.
3. In unicast routing, when a router receives a packet, it forwards that packet through only one of its ports which corresponds to the optimum path.

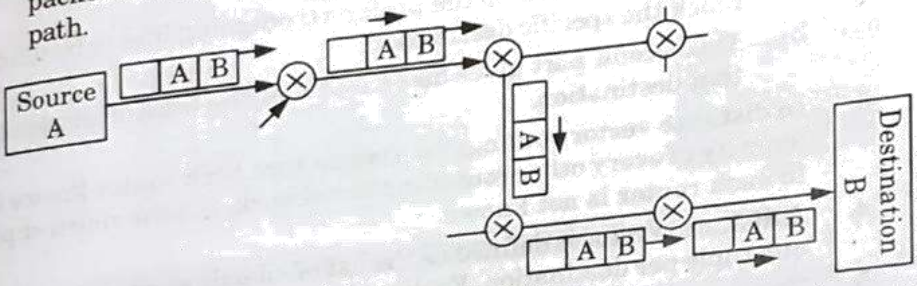

Fig. 3.5.1.

Multicast routing :

1. In multicasting, a message from a sender is to be sent to a group of destinations but not all the destinations in a network.
2. A process has to send a message to all other processes in the group. For a small group it is possible to send a point-to-point message.
3. But this is expensive if the group is large. So, we have to send messages to a well defined group which are small compared to the network size.
4. Sending message to such a group is called multicasting and the routing algorithm used for multicasting is multicast routing.
5. Multicast routing is a special class of broadcast routing as shown in Fig. 3.5.2.

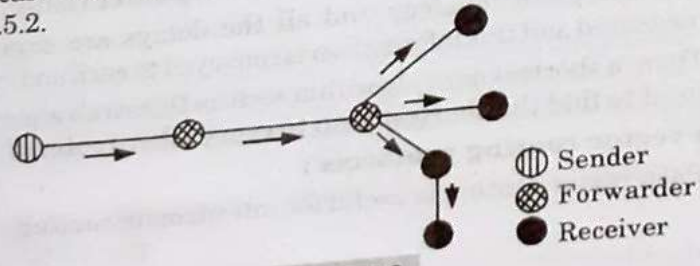

Fig. 3.5.2.

Que 3.6. **What is unicast routing ? Discuss unicast routing protocols.**

AKTU 2017-18, Marks 10

AKTU 2015-16, Marks 05

OR

Explain path vector routing protocol.

Answer

Unicast routing : Refer Q. 3.5, Page 3–5A, Unit-3.

Unicast routing protocols are :

i. Distance vector routing protocol :

1. In distance vector routing, each router maintains a routing table.
2. Routing table contains one entry for each router in the subnet. This entry has two parts :
   a. The first part shows the preferred outgoing line to be used to reach the specific destination.
   b. The second part gives an estimate of the time or distance to that destination.
3. In distance vector routing, we assume that each router knows the identity of every other router in the network, but the shortest part to each router is not known.
4. A distance vector is defined as the list of <destination, cost> tuples, one tuple per destination. Each router maintains a distance vector.
5. The cost in each tuple is equal to the sum of costs on the shortest path to the destination.

ii. Link state routing protocols :

1. The link state routing is simple and each router has to perform the following five operations :
   a. Discover its neighbours and learn their network address.
   b. Measure the delay or cost to each of its neighbours.
   c. Construct a packet containing the network addresses and the delays of neighbours.
   d. Send this packet to all other routers.
   e. Compute the shortest path to every other router.
2. The complete topology and all the delays are experimentally measured and this information is conveyed to each and every router.
3. Then, a shortest path algorithm such as Dijkstra's algorithm can be used to find the shortest path to every other router.

iii. Path vector routing protocols :

1. Path vector routing is useful for interdomain routing.

2. In path vector routing, there is one node in each Autonomous System (ASs) that acts on behalf of the entire ASs.
3. This single node is called the speaker node. The speaker node in an authentication server creates a routing table and advertises it to speaker nodes in the neighbouring ASs.

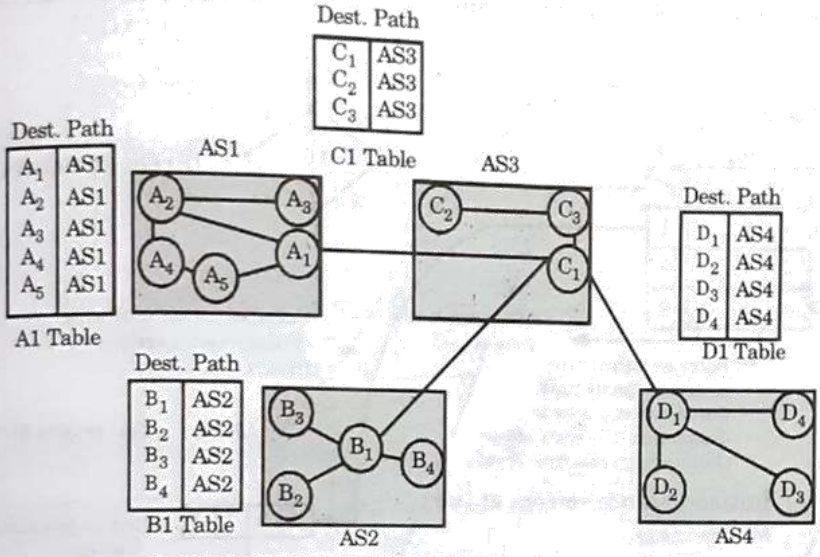

Fig. 3.6.1. Initial routing tables in path vector routing.

4. The principle of path vector routing is same as for distance vector routing except that only speaker nodes in each AS can communicate with each other.
5. A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems.

Que 3.7. Explain distance vector routing algorithm and how it updates the routing tables with the help of example.

Answer

Distance vector routing algorithm : Refer Q. 3.6, Page 3–6A, Unit-3.

Updation of router tables :

1. A router periodically sends a copy of its distance vector to all its neighbours.
2. When a router receives a distance vector from its neighbours, it tries to find out whether its cost to reach any destination would decrease if it routed packets to that destination through the particular neighbouring router.
3. Fig. 3.7.1 shows how the D.V. at *A* is automatically modified when a D.V. is received from *B*.
4. A similar calculation takes place at the other routers as well. So, the entries at every router can change. In Fig. 3.7.1 the initial distance

vector is shown. The entries in each source represent the shortest distance between the routers.

5. For example, $AC = 3$ indicates the cost corresponding to the shortest path in terms of number of hops from A to C.
6. Even if nodes asynchronously update their distance vectors the routing tables eventually converge.
7. Bellman-Ford algorithm is commonly used in distance vector routing.

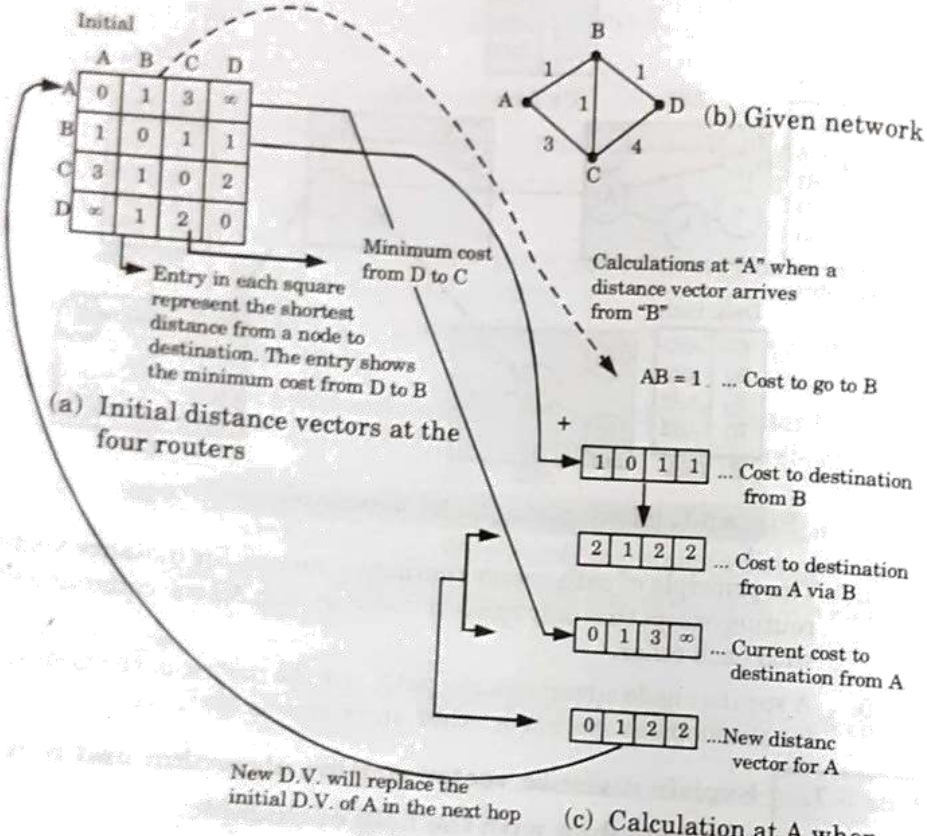

Fig. 3.7.1. Distance vector algorithm at router A.

Que 3.8. **Discuss link state routing. Compare distance vector routing with link state routing.**

Answer

Link state routing : Refer Q. 3.6, Page 3–6A, Unit-3.

Comparison :

S. No.	Distance vector routing	Link state routing
1.	Each router maintains routing table indexed by and containing one entry for each router in the subnet.	It is advanced version of distance vector routing.
2.	Algorithm is slower.	Algorithm is faster.
3.	Bandwidth is less.	Bandwidth is high.
4.	Router measure delay directly with special ECHO packets.	All delays measured and distributed to every router.
5.	It does not consider line bandwidth into account when choosing the routes.	It considers the line bandwidth into account when choosing the routes.

Que 3.9. Discuss Dijkstra algorithm.

Answer

1. The Dijkstra algorithm calculates the shortest path between two points on a network using a graph made up of nodes and arcs. Nodes in the graph may contain networks and routers.
2. Arcs are the connections between a router and a network (router to network and network to router). Cost is applied only to the arc from router to network.
3. The Dijkstra algorithm follows four steps to discover the shortest path tree (routing table) for each router :
   a. The algorithm begins to build the tree by identifying its root. The root of each router's tree is the router itself. The algorithm then attaches all nodes that can be reached from that root. Nodes and arcs are temporary at this step.
   b. The algorithm compares the tree's temporary arcs and identifies the arc with the lowest cumulative cost. This arc and the node to which it connects are now a permanent part of the shortest path tree.
   c. The algorithm examines the database and identifies every node that can be reached from its chosen node. These nodes and their arcs are added temporarily to the tree.
   d. The last two steps are repeated until every node in the network has become a permanent part of the tree. The only permanent arcs are those that represent the shortest (lowest-cost) route to every node.

Que 3.10. **Describe the problem of count-to-infinity associated with distance vector routing technique.** **AKTU 2016-17, Marks 7.5**

Answer

Count-to-infinity problem :

1. The main issue with Distance Vector Routing (DVR) protocols is routing loops.
2. This routing loops in DVR network causes count-to-infinity problem.
3. In distance vector routing, routing loops usually occur when an interface goes down.
4. Routing loops usually occur when any interface goes down or two routers send updates at the same time.

Explanation :

1. Consider a network connected with three routers as shown in Fig. 3.10.1.

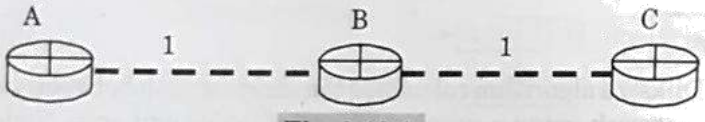

Fig. 3.10.1.

2. Let the matrices (weight or cost) between the routers is the number of jumps to reach the neighbour router.
3. In the Fig. 3.10.1 cost between B and C is 1 and cost between A and C is 2.
4. Now suppose the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from its table.
5. Before it can send any updates, it may be possible that it will receive an update from A which will be advertising that it can get to C at a cost of 2.
6. B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3.
7. A will then receive updates from B later and update its cost to 4.
8. This will slowly propagates through the network until it reaches infinity. This will cause count-to-infinity problem.

PART-3

Congestion Control.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.11. **What is congestion and congestion control ? Discuss open-loop congestion control techniques.**

OR

What is congestion ? Name the techniques that prevent congestion.

AKTU 2015-16, Marks 05

OR

What is congestion ? Briefly describe the techniques that prevent congestion.

AKTU 2017-18, Marks 10

Answer

Congestion : Congestion is a situation which may occur if users send data into the network at a rate greater than that allowed by network resources.

Congestion control : Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

Techniques to prevent congestion :

1. **Open-loop congestion control :** In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. Following are the policies that can prevent congestion :
   - i. **Retransmission policy :** The retransmission policy is designed to optimize efficiency and at the same time prevent congestion.
   - ii. **Window policy :** The type of window at the sender may also affect congestion. The selective repeat window is better than the Go-Back-N window for congestion control.
   - iii. **Acknowledgement policy :** The acknowledgement policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help to prevent congestion.
2. **Closed-loop congestion control :** Closed-loop congestion control mechanisms try to reduce congestion after it happens. Several mechanisms have been used by different protocols which are as follows :
   - i. **Backpressure :** The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.

ii. **Choke packet :** A choke packet is a packet sent by a node to the source to inform about congestion. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly.

iii. **Implicit signaling :** In implicit signaling, there is no communication between the congested node or nodes and the source.

iv. **Explicit signaling :** The node that experiences congestion can explicitly send a signal to the source or destination.

Que 3.12. What is the difference between open-loop congestion control and closed-loop congestion control ?

Answer

S. No.	Open-loop congestion control	Closed-loop congestion control
1.	Open-loop congestion control is based on prevention of congestion.	Closed-loop congestion control is based on the solution for removing the congestion.
2.	It prevents the congestion from happening.	It removes the congestion after it took place.
3.	It does not need end to end feedback.	It adjusts its data rate depending on some kind of feedback.
4.	Mechanisms are as follow : i. Retransmission policy ii. Window policy iii. Acknowledgement policy iv. Admission policy	Mechanisms are as follow : i. Backpressure ii. Choke packet iii. Implicit signaling iv. Explicit signaling

Que 3.13. Define traffic shaping. Elaborate leaky bucket algorithm used for congestion control.

OR

What is the congestion in network layer ? Discuss at least one algorithm used for congestion control.

OR

Write a short note on leaky bucket algorithm.

AKTU 2013-14, Marks 05

Answer

Traffic shaping : Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network.

Congestion in network layer : Refer Q. 3.11, Page 3–11A, Unit-3.

Leaky bucket algorithm :

1. If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket.
2. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty.
3. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket which can smooth out bursty traffic.
4. Bursty chunks are stored in the bucket and sent out at an average rate.
5. A simple leaky bucket implementation is shown in Fig. 3.13.1, a FIFO queue holds the packets. If the traffic consists of fixed size packets the process removes a fixed number of packets from the queue at each tick of the clock.

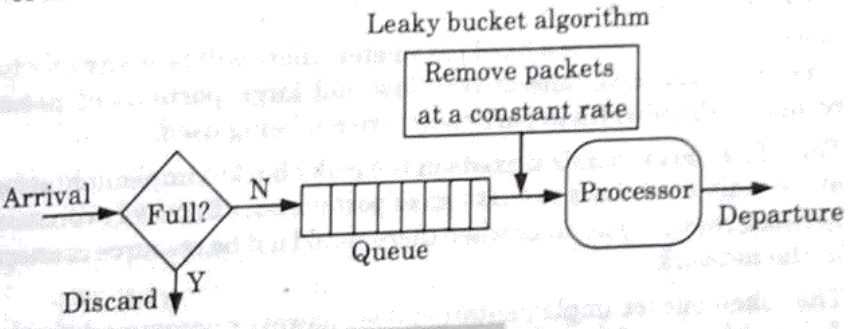

Fig. 3.13.1.

6. If the traffic consists of variable length packets, the fixed output rate must be based on the number of bytes or bits.
7. The following is an algorithm for variable length packets :
   i. Initialize a counter to n at the tick of the clock.
   ii. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
   iii. Reset the counter and go to step (i).

Que 3.14. Write a short note on token bucket algorithm. What are the limitations of leaky bucket algorithm ?

Answer

Token bucket :

1. Token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens.
2. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent.

3. In other words, the host can send bursty data as long as the bucket is not empty.
4. The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1.
5. Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.
6. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick.

Limitation of leaky bucket algorithm :

1. The leaky bucket implementation does not efficiently use available network resources.
2. Because its leak rate is a fixed parameter, there will be many instances when the traffic volume is very low and large portions of network resources (bandwidth in particular) are not being used.
3. Therefore, no mechanism exists in the leaky bucket implementation to allow individual flows to burst up to port speed, effectively consuming network resources at times when there would not be resource connection in the network.
4. The token bucket implementation does however accommodate traffic flows with bursty characteristics.
5. The leaky bucket and token bucket implementations can be combined to provide maximum efficiency and control of the traffic flow into a network.

Que 3.15. What do you mean by congestion control and QoS ? What are the parameters of QoS ? Explain.

Answer

Congestion control : Refer Q. 3.11, Page 3–11A, Unit-3.

Quality of Service : Quality of Service (QoS) refers to a network's ability to achieve maximum bandwidth and provide better service to selected network traffic.

There are four types of QoS parameters :

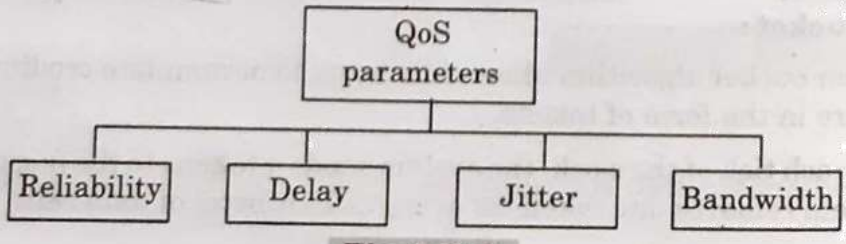

Fig. 3.15.1.

1. **Reliability :**
   a. Reliability is a characteristic that a flow needs.
   b. Lack of reliability means losing a packet or acknowledgement, which entails retransmission.
   c. However, the sensitivity of application programs to reliability is not the same.
   d. For example, it is more important that electronic mail, the transfer, and internet access have reliable transmission than telephony or audio conferencing.

2. **Delay :**
   a. Source to destination delay is another flow characteristic.
   b. Applications can tolerate delay in different degrees.
   c. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while delay in file transfer or e-mail is less important.

3. **Jitter :**
   a. Jitter is the variation in delay for packets belonging to the same flow.
   b. For example, if four packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23, all have the same delay, 20 units of time.
   c. On the other hand, if the above four packets arrive at 21, 23, 21 and 28, they will have different delays : 21, 22, 19 and 24.
   d. High jitter means that difference between delays is large; low jitter means that variation is small.

4. **Bandwidth :**
   a. Different applications need different bandwidths in video conferencing.
   b. We need to send millions of bits per second to refresh a colour screen while the total numbers of bits in an email not reach even a million.

Que 3.16. **Write short note on ARP. How it works ?**

Answer

Address Resolution Protocol (ARP) :

1. The address resolution protocol (ARP) is a protocol used by the internet protocol, specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.
2. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when IPv4 is used over Ethernet.

3. For two machines on a given network to communicate, they must know the other machine's physical addresses.
4. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically discover the MAC layer address corresponding to a particular IP network layer address.
5. The term address resolution refers to the process of finding an address of a computer in a network.
6. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer.
7. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address.
8. The address resolution procedure is completed when the client receives a response from the server containing the required address.
9. An ethernet network uses two hardware addresses, which identify the source and destination of each frame, sent by the Ethernet.

Working of Address Resolution Protocol (ARP) :

When a host *A* needs to find the MAC address of another host *B* the sequence of events taking place is as follows :

1. The host *A* who wants to find the MAC address of some other host, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender *A* and the IP address of the receiver *B*.
2. This request packet is broadcasted over the network as shown in Fig. 3.16.1.

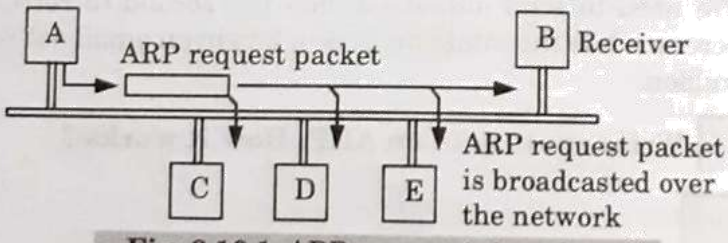

Fig. 3.16.1. ARP request is broadcast.

3. Every host on the network will receive the ARP request packet and process it. But only the intended receiver *B* will recognize its IP address in the request packet and will send an ARP response packet back to *A*.
4. The ARP response packet has the IP and MAC addresses of the receiver *B* in it. This packet is delivered only to *A* (unicast using *A*'s physical address in the ARP response packet). This is shown in Fig. 3.16.2. Thus host *A* has obtained the MAC address of *B* using ARP.

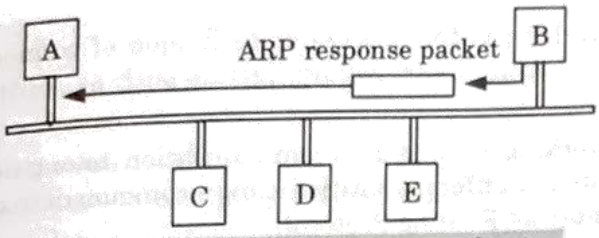

Fig. 3.16.2. ARP response unicast.

Que 3.17. **Write a short note on RARP.**

Answer

1. RARP (Reverse Address Resolution Protocol) is the logical inverse of ARP that resolves hardware address (MAC) to IP address.
2. RARP relies on the presence of a RARP server with table entries of MAC layer to IP address mappings.
3. RARP allows a physical machine in a local area network to request its IP address from a gateway server's address resolution protocol (ARP) table or cache.
4. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or media access control-MAC address) addresses to corresponding Internet Protocol addresses (IP address).
5. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address.
6. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine, which can store it for future use.
7. RARP is available for ethernet, fiber distributed data interface and token ring LANs.

PART-4

Internetworking – TCP/IP.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.18. **Write a short note on internetworking.**

Answer

1. Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.
2. Internetworking ensures data communication among networks owned and operated by different entities using a common data communication and the Internet Routing Protocol.
3. Internetworking is only possible when all the connected networks use the same protocol stack or communication methodologies.

Three units of internetworking :

1. **Extranet :** An extranet is a network of internetwork or internetworking that is limited in scope to a single organisation or entity.
2. **Intranet :** An intranet is a set of interconnected networks or internetworking, using the Internet Protocol and uses IP-based tools such as web browsers and FTP tools, that is under the control of a single administrative entity.
3. **Internet :** The internet is the largest pool of networks geographically located throughout the world and these networks are interconnected using the same protocol stack, TCP/IP.

PART-5

IP Packet, IP Address, IPv6.

CONCEPT OUTLINE

- Each TCP/IP host is identified by a logical IP address.
- Classification of IP address :
  - i. Class A
  - ii. Class B
  - iii. Class C
  - iv. Class D
  - v. Class E
- Various types of IP addresses :
  - i. IPv4 (Internet Protocol Version 4)
  - ii. IPv6 (Internet Protocol Version 6)

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.19. Explain IP addressing.

Answer

1. IP addressing is the process of finding unique IP address. A unique IP address is required for each host and network component that communicates using TCP/IP.
2. The IP address is a network layer address and has no dependence on the data link layer address (such as a MAC address of a network interface card).
3. Each TCP/IP host is identified by a logical IP address.
4. The IP address is a network layer address and has no dependence on the data link layer address (such as a MAC address of a network interface card).
5. A unique IP address is required for each host and network component that communicates using TCP/IP.
6. The IP address identifies a system's location on the network. An IP address must be globally unique and have a uniform format.
7. Each IP address includes a networkID and a hostID.
   i. The networkID (also known as a network address) identifies the systems that are located on the same physical networkID. The networkID must be unique to the internetwork.
   ii. The hostID (also known as a host address) identifies a workstation, server, router, or other TCP/IP host within a network. The address for each host must be unique to the networkID.
8. The use of the term networkID refers to any IP networkID, whether it is class-based, a subnet, or a supernet.

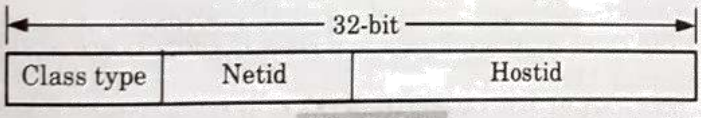

Fig. 3.19.1.

9. An IP address is 32-bits long. It is a common practice to segment the 32-bits of the IP address into four 8-bit fields called octets.
10. Each octet is converted to a decimal number (the base 10 numbering system) in the range 0-255 and separated by a period (a dot). This formal is called dotted decimal notation.

Que 3.20. Give the classification of different IP address.

OR

What is IP addressing? How it is classified? How is subnet addressing is performed? **AKTU 2015-16, 2017-18; Marks 10**

Answer

IP addressing : Refer Q. 3.19, Page 3–18A, Unit-3.

Classification of IP address :

1. **Class A :**
   i. Class A addresses are assigned to networks with a very large number of hosts.
   ii. The high-order bit in a class A address is always set to 0.
   iii. The next seven bits (completing the first octet) complete networkID. The remaining 24-bits (the last three octets) represent the hostID.
2. **Class B :**
   i. Class B addresses are assigned to medium-sized to large-sized networks.
   ii. The two high-order bit in a class B address are always set to binary 10.
   iii. The next 14-bits (completing the first two octets) complete the networkID. The remaining 16-bits (last two octets) represent the hostID.

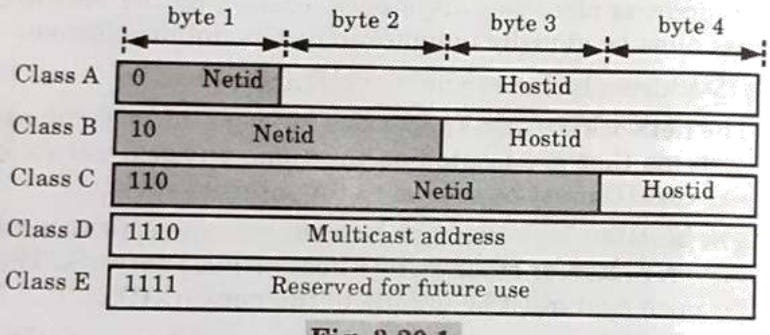

Fig. 3.20.1.

3. **Class C :**
   i. Class C addresses are used for small networks.
   ii. The three high-order bits in a class C address are always set to binary 110.
   iii. The next 21-bits (completing the first three octets) complete the networkID. The remaining 8-bits (last octet) represent the hostID.

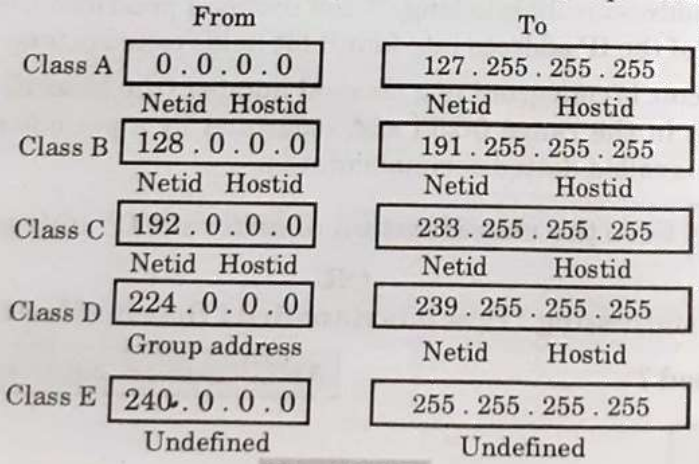

Fig. 3.20.2.

4. **Class D :**
   i. Class D addresses are reserved for IP multicast addresses.
   ii. The four high-order bits in a class D address are always set to binary 1110.
   iii. The remaining bits are for the addresses that interested hosts will recognize.
5. **Class E :**
   i. Class E addresses are experimental addresses reserved for future use.
   ii. The high-order bits in a class E address are set to 1111.

Steps for performing subnetting :

Step 1 : Check the IP address and the host's subnet mask.

Step 2 : Find the broadcast address.

Step 3 : Obtain the quantity of subnets : Find the number of subnets by using the following formula : 2^n, where, n is the number of subnet bits in the mask.

Step 4 : Acquire the number of hosts : Find the number of hosts by using the following formula : $2^n - 2$, where, n is the number of host bits in the mask.

Step 5 : Access the mask we need for the network : Find the number of sub-networks as well as the hosts for each network, by using formula $2^n - 2$.

Step 6 : Refer to the class C, mask to create sub-networks : To create sub-networks is to memorize class C masks. The default subnet mask is 255.255.255.0. There are other subnet masks that make up class C.

Step 7 : Decide which class mask to use for our sub-networks : Perform this step after we determined our networks and host.

Que 3.21. Explain the types of IP address.

Answer

There are two types of IP addresses :

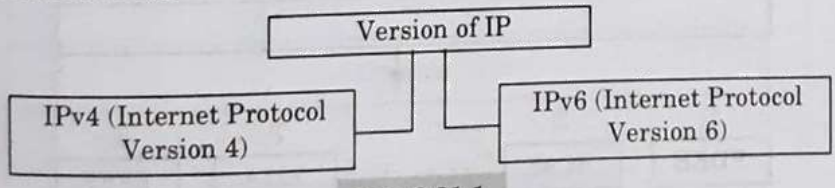

Fig. 3.21.1.

1. **IPv4 (Internet Protocol Version 4) :**
   i. IP addresses are 32-bit long and they are used in the source address and destination address fields of the IP header.

ii. Fig. 3.21.1 shows the IP address format. It consists of two fields called networkID and hostID. The IP numbers (addresses) for the hosts are assigned by the network administrator.

iii. An IP address consists of two parts. The first part of the address, called the network number, identifies a network on the internet, and the second part of address, called the hostID, identifies an individual host on that network.

iv. The IPv4 protocol has an address space. It is defined as the total number of addresses used by the protocol.

v. If N numbers of bits are used for defining an address then the address space will be 2^N addresses.

IPv4 address format :

i. The 32-bit IPv4 address is grouped into groups of 8-bits, separated by dots. Each 8-bit group is then converted into its equivalent binary number as shown in Fig. 3.21.2

ii Thus each octet (8-bit) can take value from (0 to 255). The IPv4 in the dotted decimal notation can range from 0.0.0.0 to 255.255.255. 255.

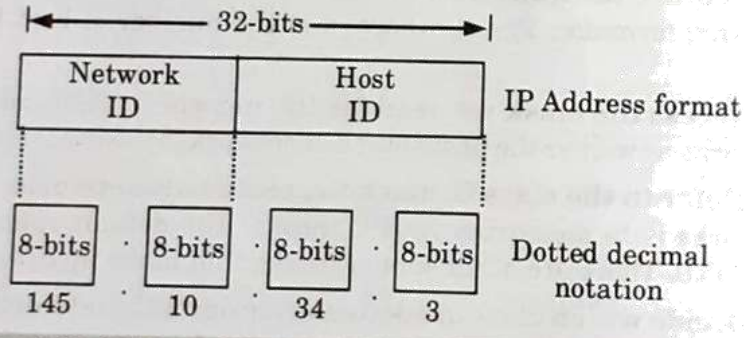

Fig. 3.21.2. IPv4 address format and dotted decimal format.

2. IPv6 (Internet Protocol Version 6) :

An IPv6 address is 128-bit long as shown in Fig. 3.21.3.

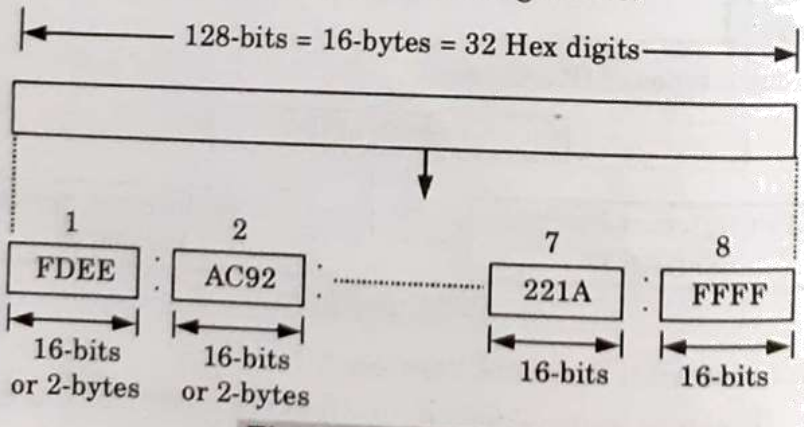

Fig. 3.21.3. IPv6 address.

Hexadecimal colon notation :

1. IPv6 uses a special notation called hexadecimal colon notation. In this, the total 128-bits are divided into 8 sections, each one 16-bits or 2-bytes long.
2. The 16-bits or 2-bytes in binary correspond to four hexadecimal digits of 4-bits each.
3. Hence, the 128-bits in hexadecimal form will have $8 \times 4 = 32$ hexadecimal digits. These are in groups of 4 digits and every group is separated by a colon as shown in Fig. 3.21.3.
4. In IPv6, about 15% of the address space is initially allocated, the remaining 85% being reserved for future use.

Que 3.22. Draw and explain the packet format of IPv4.

Answer

The IPv4 datagram format is shown in Fig. 3.22.1. The key fields in the IPv4 datagram are the following :

i. **Version number :** This 4-bits field is used to 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.

ii. **Header length :** In the IPv4 datagram header these 4-bits are needed to determine where in the IP datagram the data actually begins.

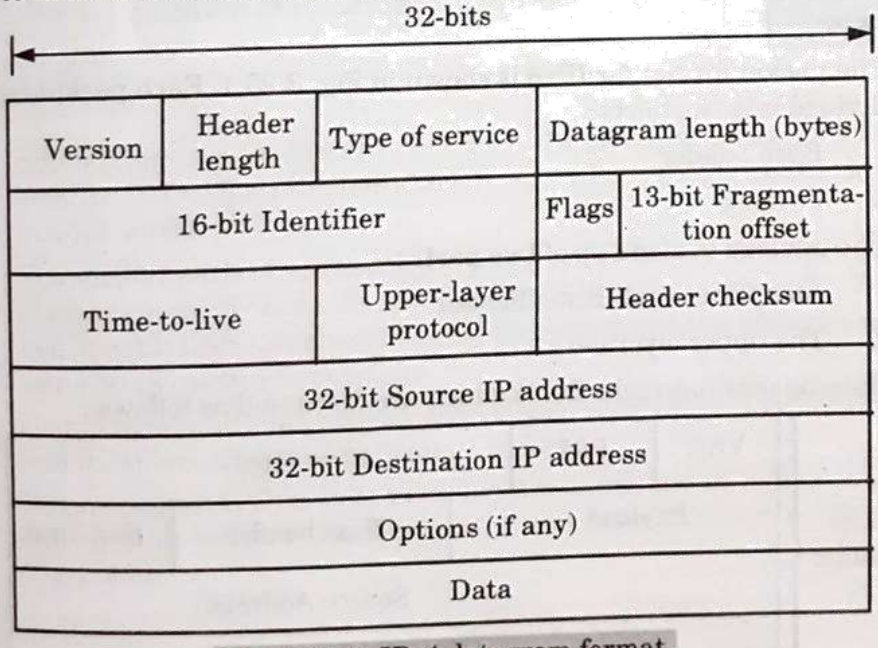

Fig. 3.22.1. IPv4 datagram format.

iii. **Type of service :** The type of service bits were included in the IPv4 header to allow different types of IP datagrams to be distinguished from each other.

iv. **Datagram length :** This is the total length of the IP datagram (header plus data) measured in bytes. This field is 16-bits long.

v. **Identifier, flags, fragmentation offset :** These three fields are used in IP fragmentation.

vi. **Time-to-live :** The time-to-live (TTL) field is included to ensure the datagrams do not circulate forever 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.

vii. **Protocol :** This field is used only when an IP datagram reaches its final destination.

viii. **Header checksum :** The header checksum is used by router for detecting errors in the received IP datagram. The header checksum is computed by treating each 2-bytes in the header as a number and summing these numbers using 1's complement arithmetic.

ix. **Source and destination IP addresses :** Source IP address field contain IP of source which create IP datagram. Destination IP address field contain IP of receiver to which IP datagram is received. The length of both fields is 32-bit.

x. **Options :** The options field allows an IP header to be extended.

xi. **Data (payload) :** In most circumstances, the data field of the IP datagram contains the transport layer segment (TCP or UDP) to be delivered to the destination.

Que 3.23. Explain the packet format for IPv6.

Answer

1. The packet format for IPv6 is shown in Fig. 3.23.1. Each packet can be divided into two parts :
   i. Base header
   ii. Payload
2. The payload is made up of two parts :
   i. An optional extension header
   ii. The upper layer data
3. Base header has eight fields which are discussed as follows :

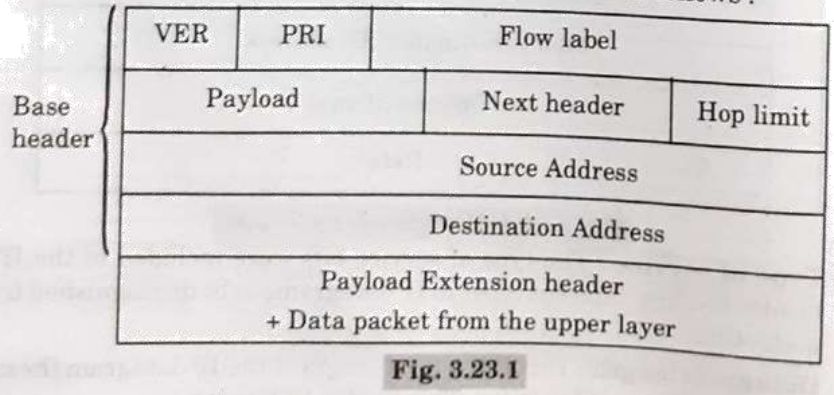

Fig. 3.23.1

i. **Version :** This is 4-bit field which defines the version number of IP. For IPv6, the value is 6.

ii. **Priority :** The 4-bit priority field defines the priority of the packet with respect to traffic congestion.

iii. **Flow label :** The flow label is a 3-byte field that is designed to provide special handling for a particular flow of data.

iv. **Payload length :** The 2-byte payload length field defines the total length of IP datagram excluding the base header.

v. **Next header :** The next header is an 8-bit field defines the header that follows the base header in the datagram.

vi. **Hop limit :** This 8-bit hop limit field serves the same purpose as TTL field in IPv4.

vii. **Source address :** The source address field is a 16-bytes internet address that identifies the original source of datagram.

viii. **Destination address :** The destination address field is a 16-byte internet address that usually identifies the final destination of the datagram.

ix. **Extension header :** Extension header field help in processing of data packets by appending different extension header. Each extension header has a length equal to multiple of 64-bits.

Que 3.24. Explain the concept of subnetting.

Answer

1. Subnetting is a mechanism in which the network splits into several smaller networks internally but it acts like a single network to the outside world.
2. The smaller parts of a network are called subnets. For example, a growing company initially has only one LAN but as the time passes by it might end up with LANs, each one having its own router and each one with its own class C network numbers.
3. Company should start up with class B address instead of class C address and it can number the host from 1 to 254.
4. When a second LAN is to be installed it can split the 16-bit host numbers into a 6-bit subnet number and 10-bit host number as shown in Fig. 3.24.1.

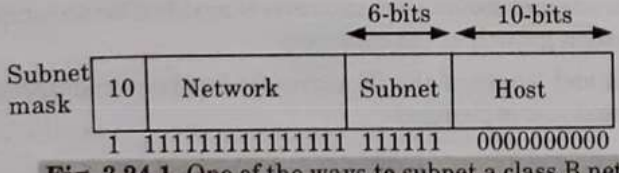

Fig. 3.24.1. One of the ways to subnet a class B network.

5. Due to this split it is possible to connect 62 LANs (0 and 1 are reserved) and each one can contain up to 1022 hosts.
6. The number of 1's in the subnet mask is more than the number of 1's in the corresponding default mask.
7. In a subnet mask, we change some of the leftmost 0's in the default mask to make it a subnet mask. Fig. 3.24.2 shows the difference between the class B default mask and subnet mask for the same block.
8. The number of subnets is determined by the number of extra 1's.
9. For three extra 1's, the number of subnets will be $2^3 = 8$. For n extra 1's, the number of subnets is 2^n.

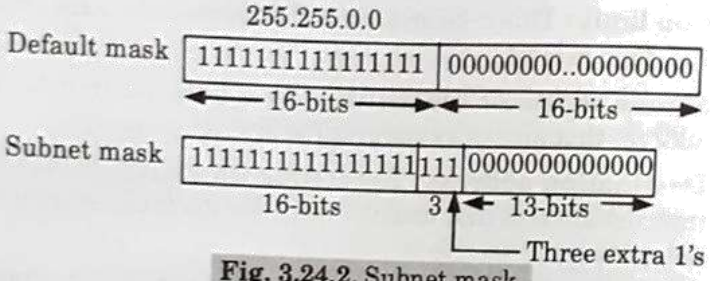

Fig. 3.24.2. Subnet mask.

Que 3.25. What are deficiencies of IPv4 ? How IPv6 was modified to overcome these deficiencies ?

Answer

1. The deficiency of IPv4 is its address field. IP relies on network layer addresses to identify end points on networks, and each networked device has a unique IP address.
2. Other identified deficiencies of the IPv4 protocol are :
   i. Complex host and router configuration
   ii. Non-hierarchical addressing
   iii. Large routing tables
   iv. Non-trivial implementations in providing security
   v. Multicasting

To overcome these deficiencies :

1. To overcome these problems/deficiencies the Internet Protocol Version 6 (IPv6) is used.
2. In IPv6, the internet protocol was extensively modified for accommodating the unforeseen growth of the internet.
3. The format and length of the IP addresses has been changed and the packet format also is changed.

Que 3.26. **Perform the subnetting of the following IP address 160.11.X.X. Original subnet mask 255.255.0.0 and number of subnet 6 (six).** **AKTU 2014-15, Marks 10**

Answer

Given : Network IP address = 160.11.X.X

Subnet mask = 255.255.0.0

Number of subnet = 6

Let us consider a network. First we divide the network into four subnet as shown in Fig. 3.26.1, by using two bits of hostid part as

160.11.☐☐----------

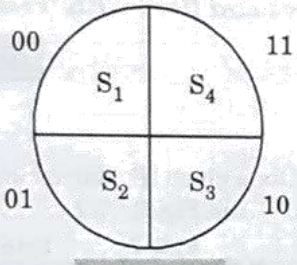

Fig. 3.26.1.

Range of subnet S_1 : 160. 11.0.0 – 160.11.63.0

Range of subnet S_2 : 160. 11.64.0 – 160.11.127.0

Range of subnet S_3 : 160. 11.128.0 – 160.11.191.0

Range of subnet S_4 : 160. 11.192.0 – 160.11.255.0

Now we divide the subnet S_3 into two more subnet as S_{31} and S_{32} as shown in Fig. 3.26.2 by using one bit from hostid part as

160.11.10☐00000--------

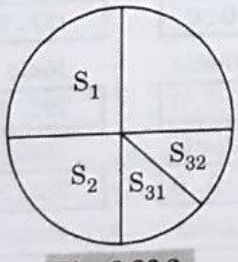

Fig. 3.26.2.

Range of subnet S_{31} : 160.11.128.0 – 160.11.159.0

Range of subnet S_{32} : 160.11.160.0 – 160.11.191.0

Again we divide subnet S_4 into two more subnet as S_{41} and S_{42} as shown in Fig. 3.26.3, by using one bit from hostid part as

160.11.11 0 00000.....

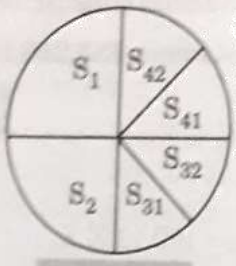

Fig. 3.26.3.

Range of subnet S_{41} :160.11.192.0 – 160.11.223.0
Range of subnet S_{42} :160.11.224.0 – 160.11.254.0
So, IP address 160.11.X.X has six subnets as $S_1, S_2, S_{31}, S_{32}, S_{41}, S_{42}$.

Que 3.27. **Give an IP address, how will you extract its netid and hostid and compare IPv4 and IPv6 with frame format.**

AKTU 2013-14, Marks 10

Answer

To extract netid and hostid for a given IP address we use internet class and its range as shown in Fig. 3.27.1 and Fig. 3.27.2.

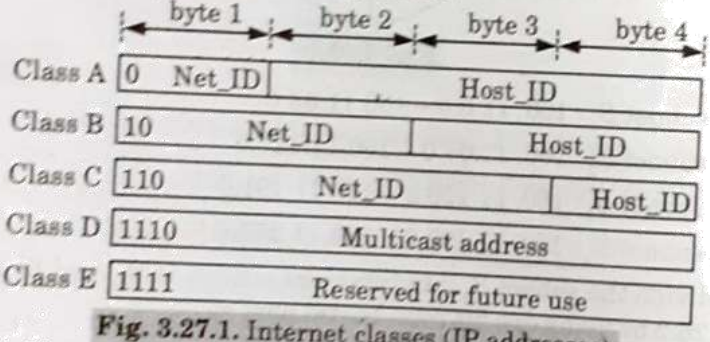

Fig. 3.27.1. Internet classes (IP addresses).

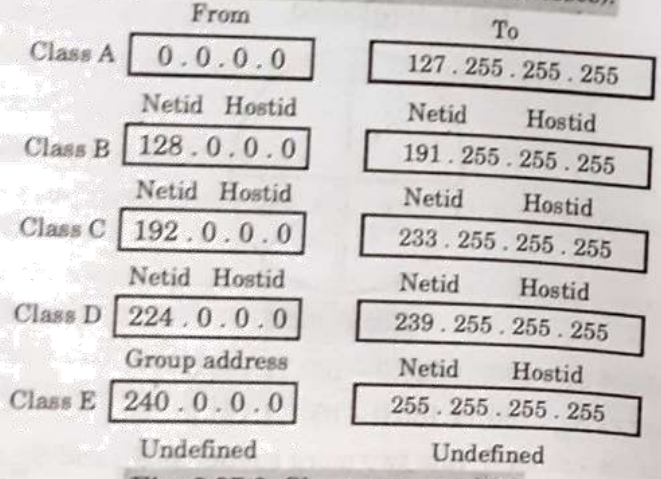

Fig. 3.27.2. Classes range of IP.

Comparison :

S. No.	IPv4	IPv6
1.	Source and destination addresses are 32-bits (4-bytes) in length.	Source and destination addresses are 128-bits (16-bytes) in length.
2.	IP Sec support is optional.	IP Sec support is required.
3.	No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the flow label field.
4.	Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host.
5.	Header includes a checksum.	Header does not include a checksum.
6.	Header includes options.	All optional data is moved to IPv6 extension headers.

IPv4 frame format : Refer Q. 3.22, Page 3–23A, Unit-3.
IPv6 frame format : Refer Q. 3.23, Page 3–24A, Unit-3.

Que 3.28. **What is meant by fragmentation ? Is fragmentation needed in concatenated virtual circuit internets, or in any datagram system ?** **AKTU 2013-14, Marks 10**

OR

Is fragmentation needed in concatenated virtual circuit internets or only in datagram systems ? Explain. **AKTU 2015-16, Marks 7.5**

Answer

1. Fragmentation is a technique in which the gateways break up large packets into smaller one called as fragments.
2. Then each fragment is sent as a separate internet packet.

Recombination of fragments : The recombination of fragments can be done by using one of the following two strategies :

Strategy - 1 for fragmentation (Transparent strategy) :

1. In this strategy, the fragmentation caused by a "small packet" network is made transparent to any subsequent network through which the packets will pass.
2. When a large packet arrives at a gateway G_1 in Fig. 3.28.1, it breaks the packet into fragments.

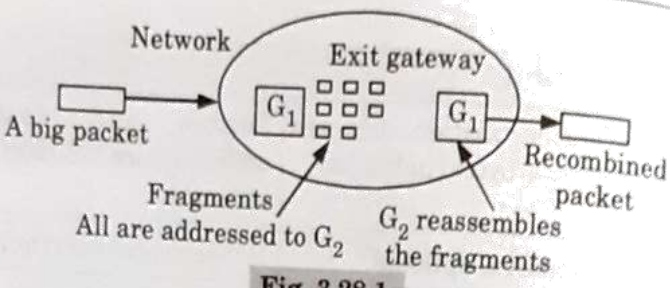

Fig. 3.28.1.

3. Each fragment is then addressed to the same exit gateway (G_2) that recombines all these fragments.

Strategy - 2 for fragmentation (Non-transparent strategy) :

1. In this strategy, the fragmented packets are not reassembled at any intermediate stage. That means the exit gateways will not reassemble the fragments.
2. Instead each fragment is treated as a separate original packet. All these packets are passed through the exit gateway or gateways and their recombination is carried out at the destination host as shown in Fig. 3.28.2.

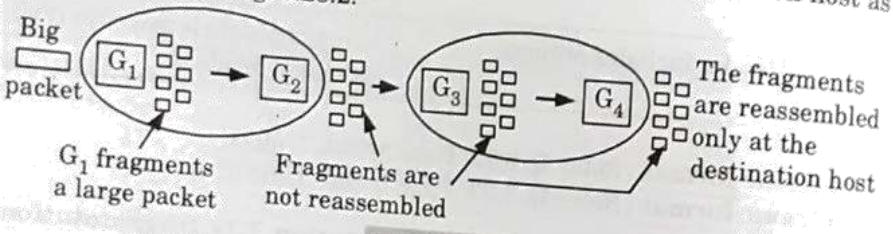

Fig. 3.28.2.

Need of fragmentation in internet :

Yes, fragmentation is needed in concatenated virtual circuit internet due to following reasons :

1. To break the packets into smallest maximum size Packet Data Unit (DDU).
2. To support the packet for different network.

Que 3.29. What is the transmission time of a packet sent by a station if the length of the packet is 2 million bytes and the bandwidth of the channel is 300 kbps. **AKTU 2014-15, Marks 10**

Answer

Given :

$B = 300$ kbps

Size of packet = 2000000 byte

$$T = \frac{\text{Data size}}{\text{Bandwidth}} = \frac{2000000 \times 8}{300 \times 1000} = 53.33 \text{ sec}$$

Que 3.30.

i. Find the class of each address

a. 140.213.10.80 b. 52.15.150.11

ii. What is the type of the following address ?

a. 4F : : A234 : 2 b. 52F : : 1234 : 2222

Answer AKTU 2015-16, Marks 10

i. a. **Given address :** 140. 213. 10. 80

The binary equivalent of 140 will be,

2	140	
2	70	0
2	35	0
2	17	1
2	8	1
2	4	0
2	2	0
	1	0

$(140)_2 = \underline{10}001100$

10 belongs to the class B.

b. **Given address :** 52.15.150.11

Binary equivalent of 52 will be

2	52	
2	26	0
2	13	0
2	6	1
2	3	0
	1	1

$(52)_2 = \underline{110}100$

110 belongs to class C.

ii. a. **Given address :** 4F : : A234 : 2

It could be expanded as follows :

004F : 0 : 0 : 0 : 0 : 0 : A234 : 2

Now, consider the leftmost byte *i.e.*, 4F

004F Hex = $\underbrace{0000\ \ 0000}_{\text{Type prefix}}$ 0100 1111

Leftmost 8-bits correspond to type prefix. All 8 zeros correspond to reserved address.

Thus, the type of 4F : : A234 : 2 is a reserved address.

b. **Given address :** 52F : : 1234 : 2222

It could be expanded as follows :

052F : 0 : 0 : 0 : 0 : 0 : 1234 : 2

Now, consider the leftmost byte *i.e.*, 52F

052F Hex = $\underbrace{0000\ \ 0101}_{\text{Type prefix}}$ 0010 1111

Thus, the type of 52F : : 1234 : 2222 is a network address.

Que 3.31. What is an interconnecting device in the internet ? Explain various interconnecting device used in the internet with suitable example.

Answer

Interconnecting devices are those devices which are used for sharing data over the network.

Different types of interconnecting devices are :

1. **Repeaters :**
   a. A repeater is a connecting device which can operate only in the physical layer.
   b. Repeater amplifies signals to ensure data transmission.
   c. A repeater receives a signal and before it get attenuated or corrupted, regenerates the original signal.

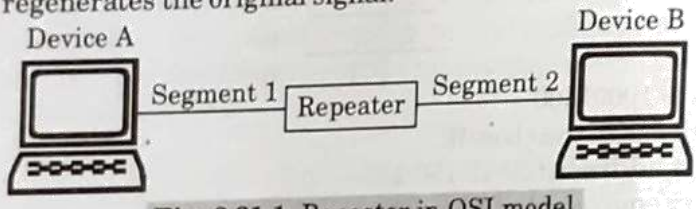

Fig. 3.31.1. Repeater in OSI model.

2. **Hubs :**
   a. Hub is a central location to connect various segments of media coming from various nodes.
   b. It is normally used for connecting stations in a physical star topology.
   c. A hub organizes the cables and relays signal to the other media segments as shown in Fig. 3.31.1.

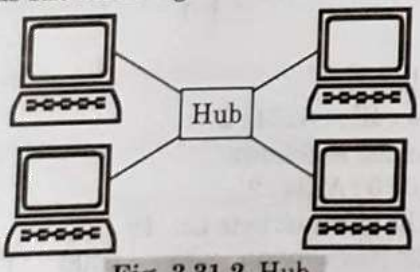

Fig. 3.31.2. Hub.

3. **Bridges :**
   a. A bridge can operate the physical as well as in the data link layer of the OSI model.
   b. It can regenerate the signal that it receives and it can check the physical (MAC) addresses of source and destination mentioned in the header of a frame.

4. **Routers :**
   a. Routers are devices that connect two or more networks as by using IP addresses.
   b. Various types of network can be interconnected through routers as shown in Fig. 3.31.3.

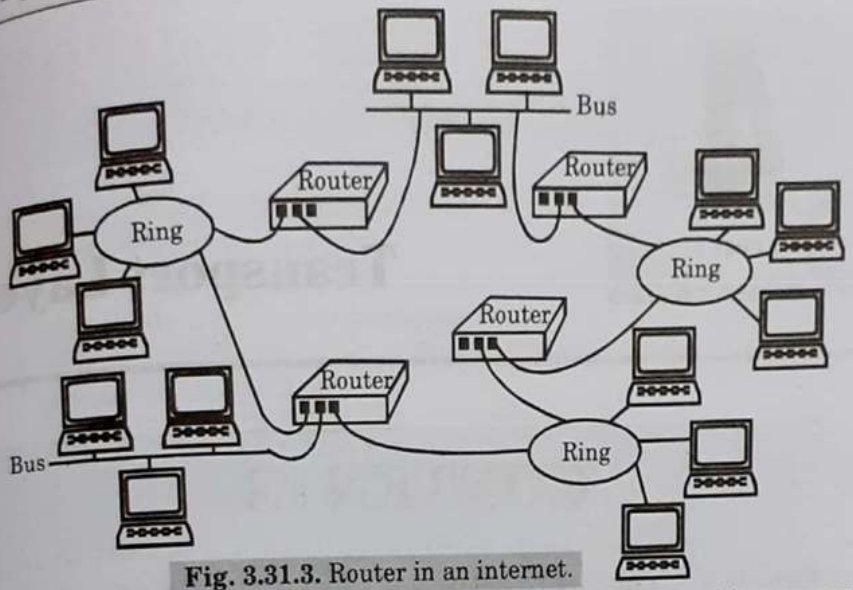

Fig. 3.31.3. Router in an internet.

c. Routers use logical and physical addressing to connect two or more logically separate networks.

5. **Gateways :**
   a. A gateway is a device that can interpret and translate the different protocols that are used on two distinct networks as shown in Fig. 3.31.4.
   b. Gateway comprise of software, dedicated hardware or a combination of both.
   c. Gateway operates through all the seven layers of the OSI model and all five layers of the internet model.

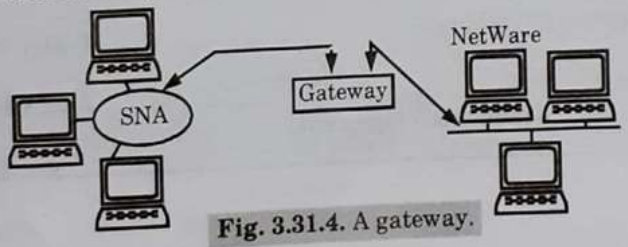

Fig. 3.31.4. A gateway.

6. **Switches :**
   a. A switch is a device which provides bridging functionality with greater efficiency.
   b. A switch acts as a multiport bridge to connect devices or segments in a LAN.
   c. The switch acts as a buffer for each link to which it is connected.
   d. When it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link.
   e. If the outgoing link is free, the switch sends the frame to that particular link.

☺☺☺