mood-book

UNIT 3

The Network Layer

Syllabus

The Network Layer: Introduction, Forwarding and Routing, Network Service Models, Virtual Circuit and Datagram Networks – Virtual-circuit Networks, Datagram Networks, Origins of VC and Datagram Networks, Inside a Router – Input Processing, Switching, Output Processing, Queueing, The Routing Control Plane, The **Internet Protocol(IP):** Forwarding and Addressing in the Internet – Datagram Format, IPv4 Addressing, Internet Control Message Protocol(ICMP), IPv6.

Learning Objectives

- Network Layer Services
- Virtual Circuits and Datagram Networks
- Components and Processing of a Router
- Internet Protocol (IP)
- Various Versions of IP i.e., IPv4 and IPv6.

Introduction

Network layer offers various services like guaranteed delivery, on-time delivery, congestion control, quality of service, security and many more. One of the major devices that work on network layer is the router which is responsible for directing the data packets from one network to another. It carries four major components including input port, output port, routing processor and switching fabric. Each device in a network is assigned with a unique identity number called its IP address. This address is used by the router and other networking devices to identify the devices present on network. The two versions of IP address are IPv4 and IPv6.

PART-A SHORT QUESTIONS WITH SOLUTIONS

Q1. Define routing.

Answer : Model Paper-III, Q1(e)

Routing is defined as a process of transferring packets over a network from one host to another. This task is performed efficiently by making use of the devices called routers. In other words it is a process of finding a path/route in a network or group of networks. This process is used in various fields like Public Switched Telephone Network (PSTN), computer networks etc.

Q2. Differentiate between forwarding table and routing table.

Answer :

	Forwarding Table		Routing Table
1.	A table which implements the forwarding technique in a specialized hardware is known as forwarding table.	1.	A table which implements a Routing technique in specialized software is known as Routing table.
2.	Forwarding table holds less information when compared to routing table.	2.	Routing table holds the maximum information.
3.	It is optimized for searching a destination IP address.	3.	It is optimized for calculating changes in topology.
4.	Each entry in forwarding table maps an IP prefix to an outgoing interface.	4.	Each entry in Routing table maps an IP prefix to an next-hop interface.

Q3. How do routers differentiate the incoming unicast, multicast and broad cost IP packets?

Answer : Model Paper-I, Q1(e)

	Unicast Address		Multicast Address		Broadcast Address
1.	It is addressed to a single host.	1.	It is addressed to a group of hosts.	1.	It is addressed to all the hosts within a network.
2.	It has one-to-one relationship.	2.	It has one-to-many relationships.	2.	It has one-to-many relationships.
3.	The unicast destination address consists of both 1's and 0's.	3.	The multicast destination address consists of both 1's and 0's.	3.	The broadcast destination address consists of only 1's.
4.	Additional bandwidth is required.	4.	No additional bandwidth is required.	4.	No additional bandwidth is required.

Q4. List the advantages of connection oriented services over connection-less services.

Answer : Model Paper-II, Q1(e)

The advantages of connection-oriented services over connection-less services are as follows,

1. It is more reliable than connection-less services.
2. It guarantees the sequencing of messages.
3. It uses short header fields where as connection less services uses longer header fields.
4. It is capable of controlling the congestion that occurs in a network.

Q5. Highlight the characteristics of datagram networks.

Answer : Model Paper-III, Q1(f)

The characteristics of datagram networks are as follows,

1. The data packet is transmitted from a source to destination at any point of time. So, this data packet arrived at switch is forwarded at that instant. Because of this reason datagram networks are connectionless.
2. The data packet is forwarded from source to destination and the host does not guarantee about the delivery of packet to the destination.
3. Every single packet is routed independent of its predecessors which are also transmitted to the same destination. Therefore, the two sequential packet of different hosts have unique paths.
4. Occurrence of route or table updation of a failure will not effect the link failure or switch failure in the process of communication.

Q6. What is an IP?

Answer : Model Paper-I, Q1(f)

Internet protocol is the third layer in TCP/IP. The functionality of this layer is to transmit data over the Internet. The responsibility of this layer is to send IP packets from source to destination independently. This means that each packet should contain the full address of the desired destination. It is an connectionless protocol, where in no connection exists between the end points. The most widely used IP protocol is "IPV4", and "IPV6". Each packet which is transmitted through the "IP" is treated as an independent unit out data.

Q7. What is meant by IPv4 Addresses?

Answer :

IPv4 (IP-version 4) defines 32-bit IP address for hosts and routers connected to the Internet. Each host and router has a unique and universal IP address. This means that, no two hosts connected to the Internet can have same IP address at the same time. Any host that wants to establish connection on the Internet must accept the addressing system. Hence, IPv4 addresses are unique and universal.

Q8. Expand ICMP and write the function.

Answer : Model Paper-II, Q1(f)

ICMP stands for Internet Control Message Protocol. It is one of the core protocols of the Internet protocol suite. The main function of this protocol is to send the error messages to the IP packet sender and also to over come the problems that were raised by the IP protocols for example, error-reporting messages and query messages.

PART-B ESSAY QUESTIONS WITH SOLUTIONS

3.1 INTRODUCTION – FORWARDING AND ROUTING, NETWORK SERVICE MODELS

Q9. Discuss about forwarding and routing functions of network layer.

Answer : Model Paper-I, Q6(a)

Forwarding

Forwarding is a mechanism of sending packet from a source host to the destination via its route. A routing table is the essential requirement of forwarding, therefore a router or a host must maintain a routing table prior to forwarding the packet. If a host has a packet which is to be transmitted over the network, then the host must initially look into routing table so as to discover the route (path) of sending the packet to the desired destination. In the same way, if a router receives a packet which has to be forwarded then it initially look within the table so as to check the final destination route.

Routing

Routing is the key feature of Internet. It is a process of selecting a best path for a packet to reach the destination. Every intermediary computer performs routing of packets from one computer to another computer until it eventually reaches the destination. Its path is calculated using routing table.

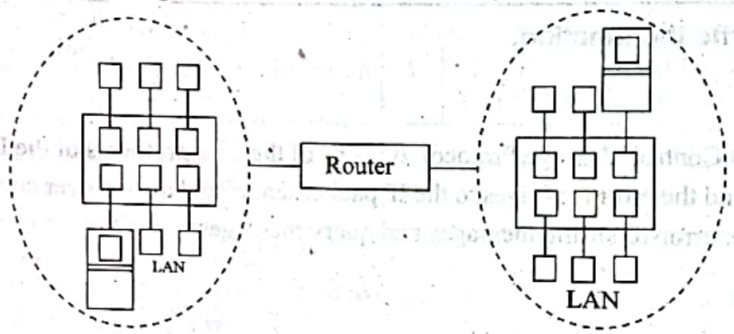


Figure: Routing

Generally, there exist many networks which many want to communicate with other networks. This also shows that there may be many routers too. For example consider different networks A to G which are connected to each other with the help of routers, irrespective of their size and topologies. Now one must focus on the following questions

(i) How these networks communicate with each other?

(ii) Which route datagrams should take to travel from source to destination?

The solution to the above questions is adaptation of routing algorithms which enables seamless integration of networks with the help of routers. As well as helps in identifying the paths which should be taken to forward a packet.

Routing/Forwarding Table

A routing table consists of various data field that holds path information according to which the data packets are transmitted to reach the destination. The destination can be a specific Internetwork or a node in an Internetwork. If the path information of a particular destination is not available then the table stores a default path for it. The process of routing a packet in the router using table is discussed below,

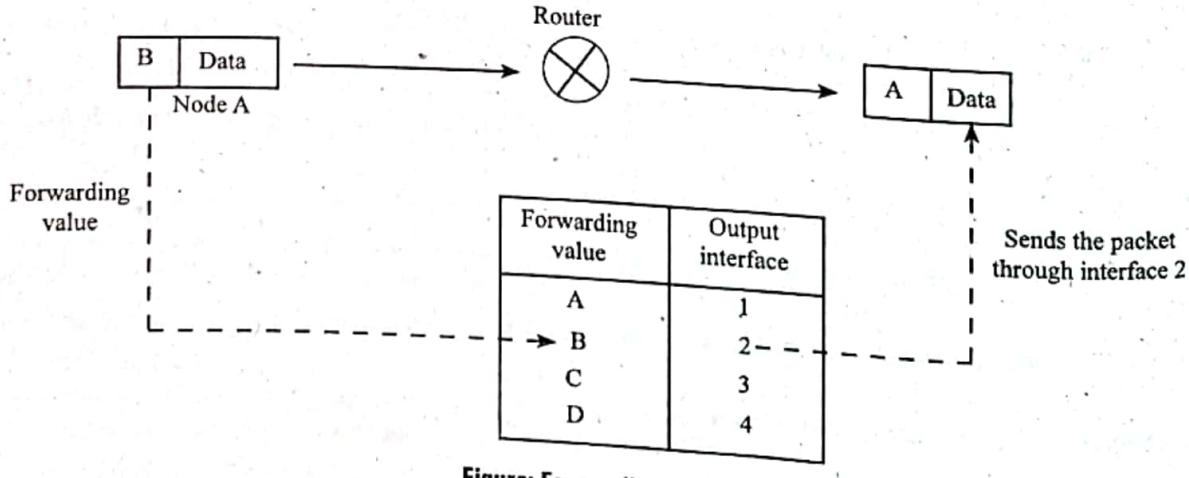


Figure: Forwarding Table

Q10. List the services provided by network layer. Discuss about network service model with an example.

Answer :

Model Paper-III, Q6(a)

Services Provided by Network Layer

Some of the services provided by network layer are as follows,

1. **Guaranteed Delivery**

Network layer ensures that the data will reach its destination.

2. **Guaranteed Delivery within a Specified Time**

Network layer ensures that the data will reach its destination within a specified time.

3. **Flow Control**

Flow control means controlling the overflow of data on the receiver side. It is used when the receiver is not having the capacity to process the incoming data or when it does not have enough space in its memory to store the data.

4. **Congestion Control**

Congestion is the state in which network performance decreases. This happens when a network is holding too many packets which are much more than the network's capability. There are various reasons for congestion to occur. Few of them are listed below.

(i) If the traffic on the network is very high.

(ii) If the CPU's processing speed is slow.

(iii) If there is insufficient memory to hold the packets.

5. **Quality of Services**

Quality of Service (QoS) is defined as the ability to provide different priority to different applications, users or data flows or to guarantee a certain level of performance to a data flow.

The attributes that can be used to describe the data flow are as follows,

(i) Reliability

(ii) Jitter

(iii) Delay

(iv) Bandwidth.

6. **Security**

The Internet consists of tens of thousands of networks which are interconnected without any boundaries. Such environment requires high network security due to the fact that organizational network is accessible through any computer from any part of the world, therefore making it prone to threats.

According to the survey conducted by Computer Security Institute(CSI), 70% of the organizations network security policies has been violated and 60% of the misuse is performed from inside the organization itself. The most easy method to give protection to the network is securing it from outside attack by closing the network entirely from outside world. So, when the network is closed, it gives connectivity to the trusted parties only, not the public networks. The absence of outside connectivity makes the network secure from outside attacks.

One of the important issues to balance between two requirements is,

1. To open the networks inorder to establish emerging business requirements and freedom of information.
2. To secure private, personal and strategic business information.

With Internet, the organizations can maintain stronger relationship with customers, suppliers, partners and employees. Also the e-business has made the companies more competitive because many new applications were developed for e-commerce, supply chain management, customer care, work force optimization and e-learning. Apart from this, applications which organizes and improves the processes, decreases turn around time, lowering the cost were also developed.

Network Service Models

Network service model can be defined as a model which describes the characteristics of transfer of packets from source to destination in an end-to-end network.

Example

Consider ATM service models i.e., CBR (Constant Bit Rate) and ABR (Available Bit Rate).

1. CBR (Constant Bit Rate) ATM Service Model

CBR model is used to make the data packets flow at a constant bit-rate. It follows a criteria similar to the early telephone systems. The flow of packets is provided using virtual pipes which offer fixed bandwidth transmission.

2. ABR (Available Bit Rate) ATM Service Model

ABR model is used to offer best-effort service over Internet. It also offers an additional feature of sending feedback to the sender in the form of a notification.

The features/service comparison of CBR and ABR is tabulated below,

Feature/Service	CBR	ABR
Bandwidth	Guaranteed with constant bit-rate	Guaranteed Minimum
No-loss	Guaranteed	No Guaranteed
Ordering	Ordered	Ordered
Time based	Yes	No
Congestion	No Congestion	Notifies if occurs

3.2 VIRTUAL CIRCUIT AND DATAGRAM NETWORKS

3.2.1 Virtual Circuit Networks, Datagram Networks

Q11. Explain about virtual circuit network and datagram network.

Answer :

Model Paper-I, Q6(b)

Virtual Circuit Network

A connection in the context of connection-oriented organization of subnet is called as Virtual Circuit (VC). A virtual circuit packet network is analogous to the telephone networks.

With VC there are three phases,

(a) VC Setup

During this phase, the source machine requests the network layer to setup a virtual connection between it and the destination machine. The network layer finds and sets up a route between the sender and the receiver. The route consists of the set of transmission lines and packet switches that will be followed by all packets of the same VC. The network layer may also allocate resources such as bandwidth for the VC.

(b) Data Transmission

Once the VC is setup, the data transfer begins. All the data flows along the path of the VC.

(c) VC Termination

After all the data have been sent, the network layer terminates the VC on the desire from the sender (or receiver). It also updates routing tables at each of the packet switches along the path to indicate that the VC is terminated.

In VC subnets each VC is numbered and every router maintains a table with an entry for each of the currently open virtual circuits passing through it. This connection state information is needed to forward the packets on the correct VC since all the packets of a given virtual circuit always take the same route through the subnet. Each packet's header contains a VC number. The router uses this number to forward the packets on the correct output line.

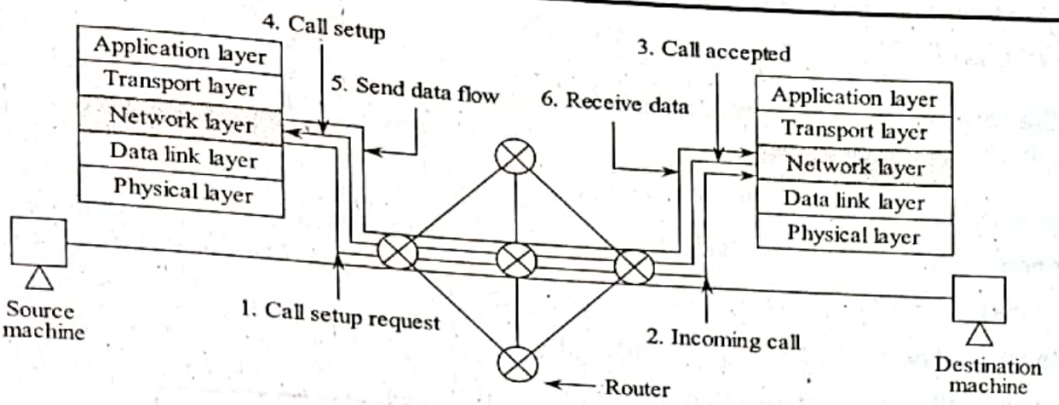


Figure (a): Virtual Circuit Network

Datagram Network

In datagram subnet, no routes are set up in advance even if the network layer service is connection-oriented. Each packet is routed independently of its predecessors, if any. Therefore, subsequent packets from the same source to same destination may follow different routes. The independent packets in the context of connectionless organization of subnet is called datagram and the corresponding subnet is called datagram subnet.

In datagram subnet the routers do not maintain any state information about VCs because no VCs are setup. Instead, they have a table with a pair of the destination router address and the outgoing time to be used for that destination.

Each time the source machine wants to send packets to destination machine, it puts the full destination address in the packet's header and then the packet is entered into the network. When the packet arrives at a router, the router examines the packet's destination address and uses its routing table to forward the packet in the direction of its destination. Since, the routing tables are updated, the series of packets from the same source to the same destination may follow different paths through the network. They may also arrive out of order at the receiver.

The destination address in a packet's header can be quite long for a large network. The datagram subnet are more robust and easily adapt to failures, the congestion control is also difficult.

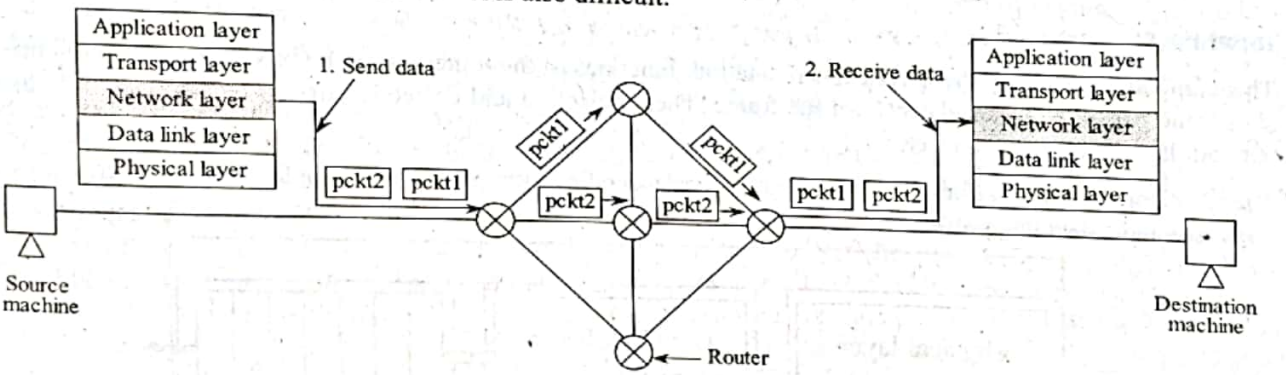


Figure (b): Datagram Network

3.2.2 Origins of VC and Datagram Networks

Q12. Discuss the evolution of virtual circuit and datagram networks.

Answer :

Model Paper-III, Q6(b)

The origin of virtual circuit networks is the traditional telephone systems which are based on real circuits. VC is complex than datagram because the responsibility of call set-up and per-call state is handed over to the routers. Datagram networks interconnect computers over the Internet and therefore, its origin lies in the Internet . The internet architects usually prefer to simplify the complexities existing end-system devices. The simplifications include the following,

1. The internet-based service model does not offer any service-level guarantees. This minimizes the network level requirements and simplifies the interconnection of networks over distinct link layer technologies. These technologies can differ in terms of physical properties, transmission rates and losses.
2. The servers in the network are responsible for handling infrastructure based services like DNS thereby simplifying the process of adding additional service or application layer protocol.

3.3 INSIDE A ROUTER

Q13. Discuss the four components present inside a router.

Answer : Model Paper-II, Q6(a)

The four components of a router are,

1. Input port
2. Output port
3. Routing processor
4. Switching fabric.

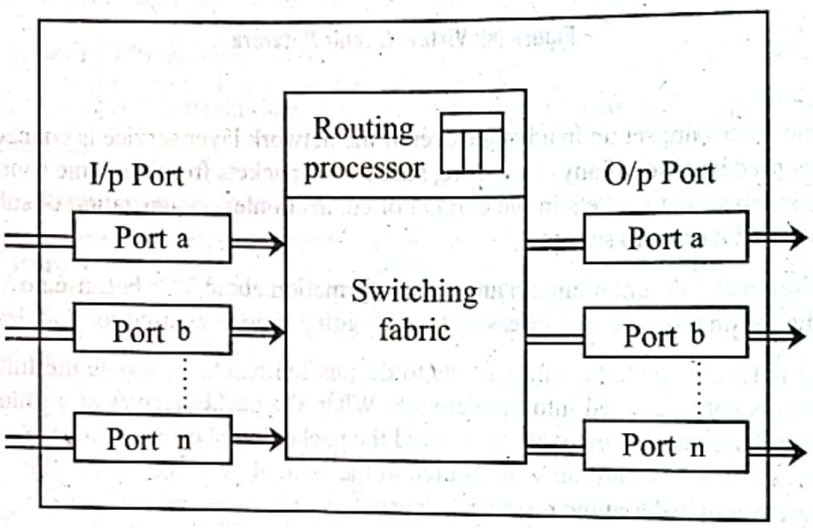


Figure (1): Architecture of Router

1. Input Port

This component performs the physical and data link functions of the router. Once the bits are created from the received signal, the packet is decapsulated from the frame. Then, detection and correction of errors is carried out allowing the network layer to route the packet.

The input port contains buffers to queue the packets prior sending them to the switching fabric along with a physical layer processor and a data link processor.

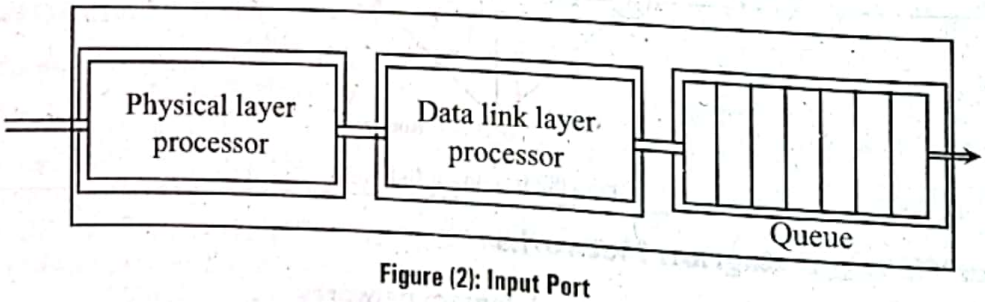


Figure (2): Input Port

2. Output Port

In output port, the packets are first queued. After that, the packets are encapsulated in a frame and then sent by implementing the functions of physical layer on frame. The functions performed by output port are reverse of the functions performed by the input port.

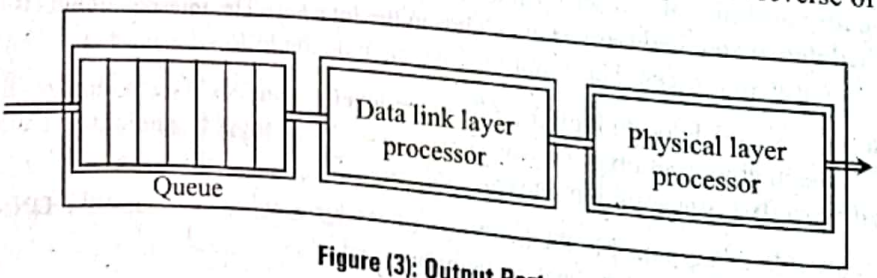


Figure (3): Output Port

3. **Routing Processor**

This component is responsible for carrying out the network layer functions. It simultaneously finds the address of the next hop as well as the output port number from which the packet arrived. This activity of choosing next hop for the packet is some times called **table lookup**. The functionality of routing processor in latest switches is handed over to input ports to make the process fast and efficient.

4. **Switching Fabric**

This component is responsible for moving the packets from the input queue to the output queue. The speed of this process not only impacts on the size of input/output queue but also on the total delay in packet delivery. The transfer of packets from input queue to the output queue is the most difficult task in the router. Earlier, the task of switching fabric was handled by computer memory or a bus where, the packets were stored in the memory by the input port and retrieved from the memory by the output port.

3.3.1 Input Processing

Q14. Explain in brief about input processing of a router.

Answer :

For answer refer Unit-III, Q13, Topic: Input Port.

Routers make use of forwarding table to forward a packet received from input port. This table is updated regularly by the routing processor where input port carry a copy of the table. The updated copies are sent to the input ports over an additional bus. With such an approach, routing decisions can be made without interacting with other ports within the local network. This helps in minimizing the overhead of centralized processing. For this, an efficient searching algorithm required especially in case of larger data transmissions. Moreover, it is also necessary to improve memory access times.

The data packet is forwarded to the switching fabric as soon as the entry of output port is identified in the lookup table. Some times when the switching fabric is in use, the other packets are blocked temporarily for entering into the fabric. The blocked packet is placed in a queue at input port. Apart from table lookup, the following actions are performed at the input port,

1. Processing of link layer and physical layer.
2. Checking and noting down the checksum, version number and time-to-live field.
3. Updating the counters such as data grams.

The same process can also be followed to block certain data packets based on the header value. A similar approach is followed by the network address (NAT) which discards every data packet whose port number value does not matches with a specific number/value.

3.3.2 Switching

Q15. Describe the three switching techniques.

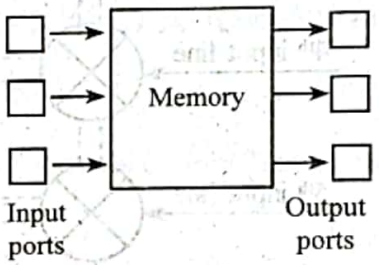
Answer : Model Paper-II, Q6(b)

The three switching techniques are,

1. Switching via memory
2. Switching via bus
3. Switching via crossbar switch.

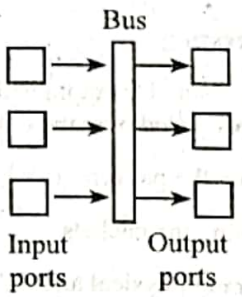
1. Switching via Memory

Traditional routers use routing processor as CPU for the purpose of switching among input and output ports. Here, input/output ports act as input/output devices for such routing processors. Modern routers use memory for the purpose of switching. These routers perform like a shared-memory multiprocessors in various aspects. These routers work by saving the packets in memory while using input line cards for processing. This process makes the modern routers different from traditional older routers. Some routers like Cisco 8500 series make use of shared-memory for forward packets.



2. Switching via a Bus

This type of processing makes use of a bus that directly forwards the packets received from input ports to the output ports. For this reason, it does not require assistance from routing processor. However, the bus need to be shared among all the available ports. Here, the input port includes a header value which indicates the output port to which the packet needs to be forwarded. The output ports receive the packets but the port whose associated value is included in the header keeps the packets while the remaining ports discard the packet. The label or header value is only used within the switch. The problem in these routers is that the arrived packets need to wait in a queue if a packet is already crossing the bus. This means that only one packet can cross the bus at a time. This makes the routing speed to completely depend on the bus. For this reason, this approach is preferred only for small local area/network.



3. Switching via Crossbar Switch

Crossbar switch consists of a series of points called cross points which handles inputs and outputs in the switch. Depending on the number of inputs given to the cross points, output will be given by the cross points. For example, if 5 inputs of data are given, then 5 outputs of data will be the result given by the cross points. Now, a question arises that how many cross points should be used. The answer is just multiply the total number of inputs and outputs to get the cross points. In this example, cross points required are $5 \times 5 = 25$ cross points.

The below figure shows a crossbar switch, which is built from two important entities, transistor or gates and switch which consists of 25 cross points. This switch is in the form of grid or a square,

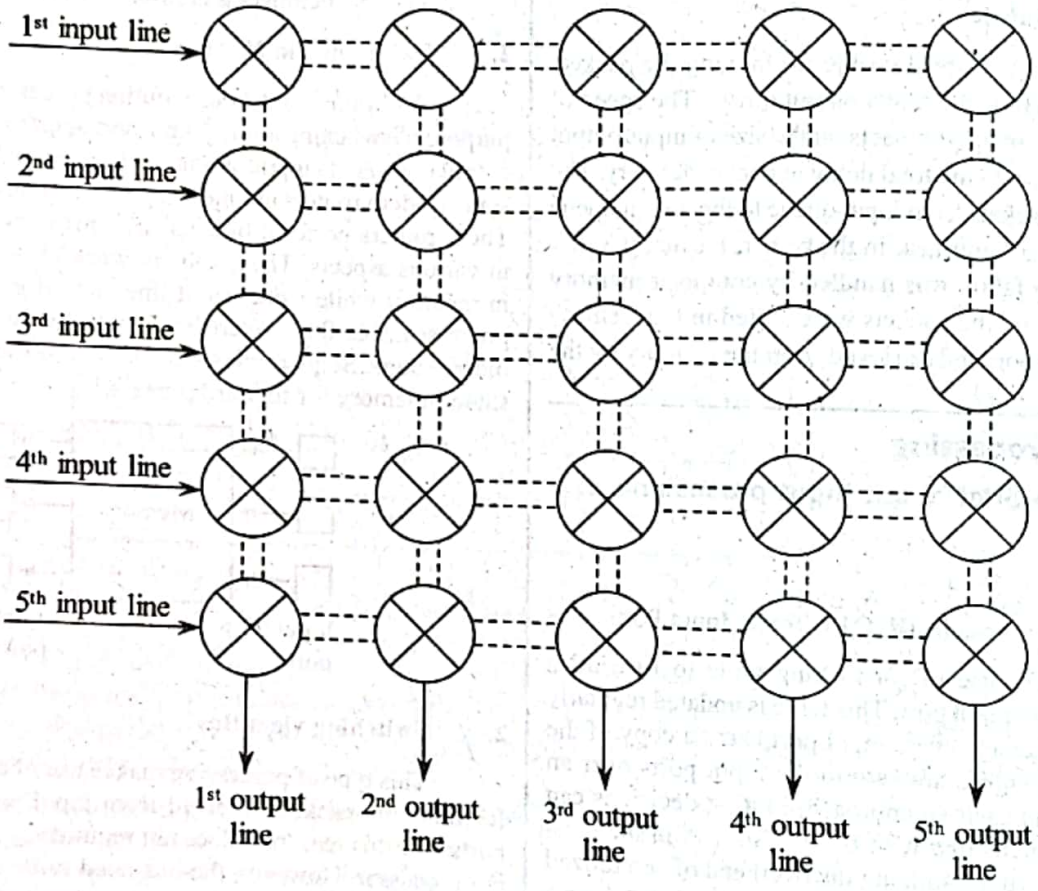


Figure: Crossbar Switch

3.3.3 Output Processing, Queueing, The Routing Control Plane

Q16. Write short notes on the following,

(i) Output processing

(ii) Queueing

(iii) Routing control plane.

Answer :

(i) Output Processing Model Paper-II, Q7(a)

The port processing for output in the process of switching starts by considering the data packets stored in the port memory. These packets are forwarded over the output link. The tasks performed during output processing are,

1. Selecting the packets
2. Dequeuing the packets
3. Performing physical and link-layer functions.

(ii) **Queueing**

Packet queueing is possible at both input and output ports similar to the cars weighting near round about for their turn to cross it. The weighting time and other attributes completely relay on the traffic load and speed of processing. With increase in the size of queue, the memory utilization increases thereby increasing the chances of packet loss in case if memory is completely in use. Such losses occur from router side as it starts dropping packets when memory is unavailable.

Similar situation can arise at output ports when multiple packets are sent simultaneously to a single port. This leads to the creation of queues as output port can forward only a single packet at a time. Moreover, the queued packets need to be forwarded based on certain criteria. This criterion is imposed using packet scheduler. Two of such criteria include FCFS (First-Comes First Served) and Weighted Fair Queueing (WFQ). In the former one, the packets are forwarded in the order of their arrival. In the latter one, the linked is shared among various connections on which the packets are destined.

The use of packet scheduler helps in ensuring quality of service.

Similarly on the input ports, various approaches like AQM (Active Queue Management) and RED (Random Early Detection) are adopted to make a decision regarding the packets arriving in the queue.

(iii) **Routing Control Plane**

The routing control plane exists near the location where the decisions are made by routing processor. This makes it decentralized as the routing process involves different aspects of entire network. However, modern routers integrate both hardware data plane and software control plane to generate an integrated product.

Moreover, research is under way to create an architecture in which the routing control plane can be internal as well as external to the routers. The internal part performs link state measurements, maintaining and installing routing tables etc., whereas the external part performs route calculations). To make these two parts work corroboratively, an API is used.

3.4 THE INTERNET PROTOCOL (IP): FORWARDING AND ADDRESSING IN THE INTERNET

3.4.1 Datagram Format

Q17. What is Internet Protocol (IP)? What are the two important components of IP? Discuss about the datagram format of IPv4.

Answer : **Model Paper-I, Q7(a)**

Internet Protocol (IP)

Internet protocol is the third layer in TCP/IP. The functionality of this layer is to transmit data over the Internet. The responsibility of this layer is to send IP packets from source to destination independently. This means that each packet should contain the full address of the desired destination. It is an connectionless protocol, where in no connection exists between the end points.

Components of IP

The two important components of IP are forwarding and routing.

For remaining answer refer Unit-III, Q9.

Datagram Format of IPv4

Datagram is nothing but the packets in IPv4. The datagram format of IPv4 is as follows,

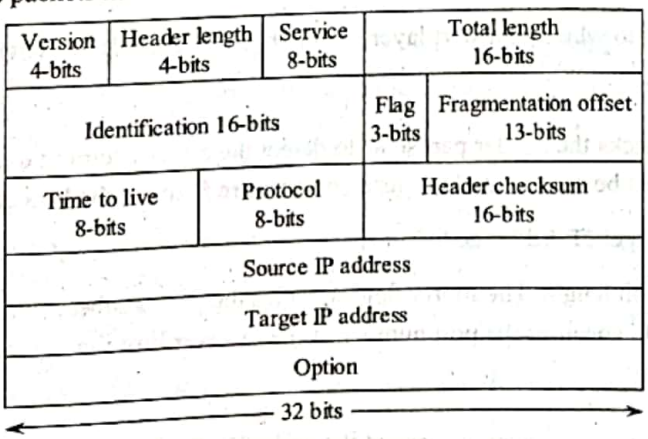


Figure: IPv4 Datagram Format

A datagram is a variable length packet having header and a data. Length of the header is about 20 to 60 bytes containing the information necessary for routing and forwarding. Usually, a 4-bytes header sections are shown in TCP/IP. The following are the fields of a datagram,

1. **Version (VER)**

   It is a 4-bit field defining the session of IPv4 protocol. Currently, the available version is 4. But in future, version 6 is supposed to replace version 4. Version (VER) field is responsible for informing the software in the processing machine about the version in use i.e., version 4. Interpretation of all the fields must be in accordance to fourth version of the protocol. If a different version of protocol used by the machine, then the datagram is eliminated so as not to interpret it wrongly.

2. **Header Length (HLEN)**

   It is a 4-bit field defining the entire length of the datagram header in 4-byte words. This field is required because header length is variable between 20 and 60 bytes. In the absence of options, header length is 20 bytes with value 5 (i.e., $5 \times 4 = 20$). The option field with maximum size has a value of 15 (i.e., $15 \times 4 = 60$).

3. **Services**

   It is a 8-bit field whose name and interpretation is changed by IETF from service type to differentiated services.

4. **Total Length**

   It is a 16-bit field that contains header as well as data. It has a maximum length of 65, 535 bytes. But, when larger datagrams are required, the field contains length greater than the maximum length.

5. **Identification Field**

   It is a 16-bit field, which specifies the identity of a fragment i.e., to which datagram it belongs to.

6. **Flag Bit**

   It is a 3 bit field which is used to control the fragment. Here, first bit is zero and it is reserved, second bit is 1 which represents. Don't fragment (DF). Third bit is '2' which represent More Fragment (MF).

7. **Fragment Offset**

   It is a 13-bit field, which specifies the location of the fragment in the datagram. The maximum length of fragment offset is one byte more than the total length field i.e., 65, 536 bytes.

8. **Time-to-live Field**

   It is a 8-bit field, which refers to a counter used for limiting the lifetime of a packet. The maximum lifetime of a packet is 255 sec. At each hop, the counter is decremented and when it becomes zero, the packet is removed and a warning packet is transmitted to the source.

9. **Protocol**

   It is a 8-bit field. It specifies to which transport layer protocol (TCP or UDP), the datagram is to be given.

10. **Header Checksum**

    It is a 16-bit field, which checks the header part so as to detect the errors occurred during the transmission of packets. At each hop, the checksum must be recomputed because one or more fields of the header changes regularly.

11. **Source IP Address and Target IP Address**

    Each of these fields is of 32-bit length. The source field specifies the port number of the sender host that sends the fragment whereas, the destination field specifies the port number of the receiver host that receives the fragment.

12. **Options Field**

    It is of variable length. Options may occupy space at the end of IP header and there lengths are multiple of four bytes. It is generally used to provide more information that wasn't covered in the IP header.

3.4.2 IPv4 Addressing

Q18. Discuss in brief about the IPv4 addresses.

Model Paper-II, Q7(b)

Answer :

IPv4 Address

IPv4 (IP-version 4) defines 32-bit IP address for hosts and routers connected to the Internet. Each host and router has a unique and universal IP address. This means that, no two hosts connected to the Internet can have same IP address at the same time. Any host that wants to establish connection on the Internet must accept the addressing system. Hence, IPv4 addresses are unique and universal.

Address Space

An address space is defined as the total number of addresses that are used by the protocol. IPv4 protocol uses 32-bit addresses. Hence, the address space of IPv4 is 2^{32} or 4, 294, 967, 296. (i.e., more than 4-billion). If limitation is not given then these large number of devices can be connected on the Internet. The IPv4 address makes use of three generated notations. They are,

1. **Binary Notation**

Binary notation is a popular notation to present an IPv4 address which is displayed as 32 bits. An IPv4 address can be defined as a 32-bit address or a 4 byte address where each octet (8-bits) refers to one byte.

Example

The example of IPv4 address in binary notation is,

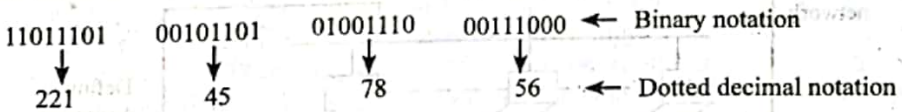
11011101 00101101 01001110 00111000

2. **Dotted Decimal Notation**

Dotted Decimal Notation is another notation that specifies the IPv4 addresses. Generally Internet addresses are written in decimal form which are more easier to look through. In decimal forms, each octet (byte) is separated by decimal point (dot), and its value ranges from 0 to 255.

Example

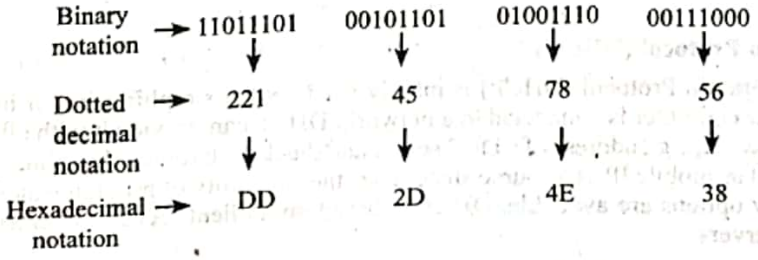
The dotted decimal notation for the IPv4 binary notation is given below.



3. **Hexadecimal Notation**

Hexadecimal notation is another notation which is used rarely to specify the IPv4 addresses. Here, every set of four bits is equal to a single hexadecimal digit. That is, in an address of 32-bit there are total 8-hexadecimal digits. This type of notations are mostly used in network programming.

Example



Hierarchy in Addressing

Every communication network requires hierarchy in addressing system. For example, a postal network or a postal addressing system involves the following hierarchy.

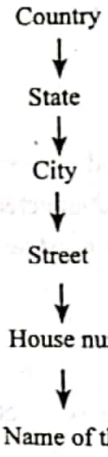


Figure (1): Hierarchy in Postal Network/postal Addressing System

Similarly a telephone network or a telephone addressing system involves the following hierarchy,

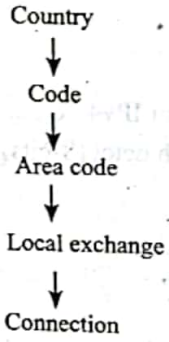
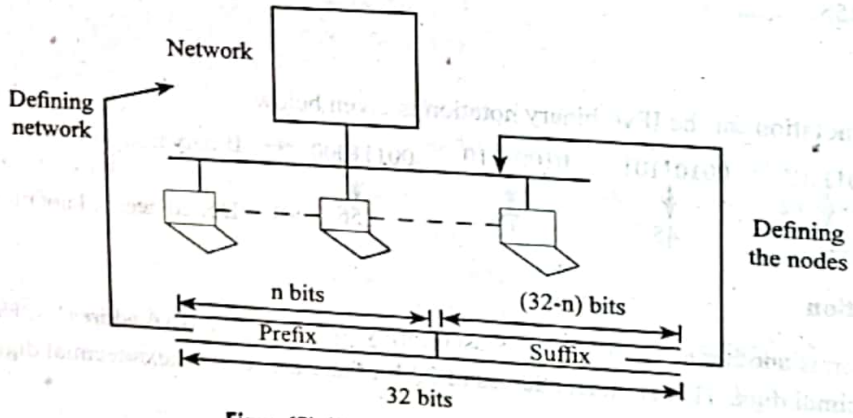


Figure (2): Hierarchy in Telephone Network/telephone Addressing System

The hierarchy of 32-bit IPv4 addressing is divided into two parts i.e., prefix and suffix. Prefix is the first part of the IPv4 address whose length is 'n' bits. It basically defines the network. The second part of the IPv4 address is suffix and the length of it is (32-n) bits. It basically defines the node. The length of prefix can be fixed or variable. The following figure shows the hierarchy in IPv4 addressing.



Figure(3): Hierarchy of IPv4 Addressing

Q19. Explain the working of DHCP protocol with its header format.

Answer :

Dynamic Host Configuration Protocol (DHCP)

Model Paper-I, Q7(b)

Dynamic Host Configuration Protocol (DHCP) is mainly used for the simplification of installation and maintenance of networked computers. If a new computer is connected to a network, DHCP can provide it with all necessary information for full system integration into the netwc.k, e.g., address of a DNS server and the default router, the subnet mask, the domain name and an IP address. DHCP mainly used as mobile IP as a source since it has the capability of providing an IP address. DHCP mechanisms are quite simple. Since, many options are available. DHCP is based on a client/server model as shown in figure (1) below. It contains one client and two servers.

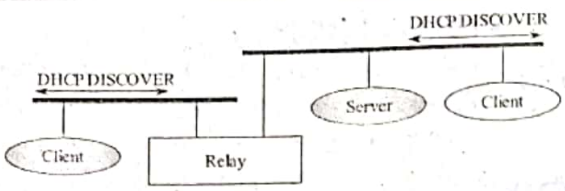


Figure (1): Basic DHCP Configuration

DHCP clients send a request to a server (DHCP DISCOVER) to which the server responds. A client sends requests using MAC broadcasts. A DHCP relay might be needed to forward requests to a DHCP server. Client initialization via DHCP is shown in figure (2).

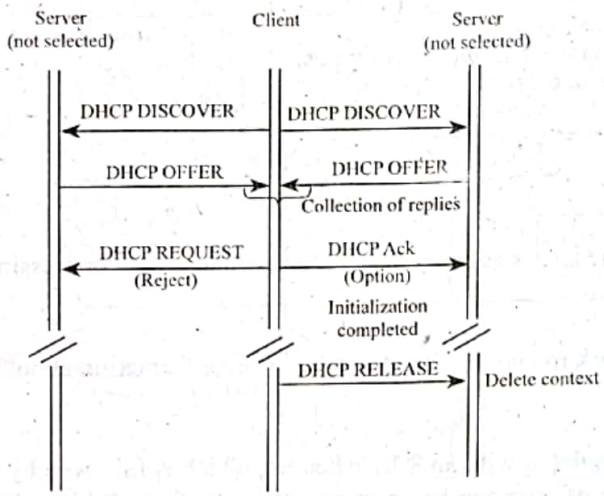


Figure (2): Client Initialization via DHCP

(i) In above figure there is one client and two servers. The client broadcasts a DHCP DISCOVER into the subnet. There might be a relay to forward this broadcast.

Two servers receive this broadcast and determine the configuration they can offer to the client. Servers reply to the client's request with DHCP OFFER and offer a list of configuration parameters. The client can choose one of the offered configurations.

(ii) The client then replies to the servers, accepting one of the configurations and rejecting the others using DHCP REQUEST. If a server receives a DHCP REQUEST with a rejection it can free the reserved configuration for other possible clients. The server with the configuration accepted by the client, confirm the configuration with DHC PACK this completes the initialization phase.

(iii) If a client leaves a subnet, it releases the configuration received by a server using DHCP RELEASE. The server free the context stored for the client and offer the configuration again. The configuration which a client gets from a server is only leased for a certain amount of time. Therefore, the client has to reconfirm the configuration from time to time otherwise, the server will free the configuration. This time out of configuration helps in case of crashed nodes or nodes moved away without releasing the context.

Advantage

(i) The DHCP is good for supporting the acquisition of Care-Of-Addresses (COA) for mobile nodes. The hosts for all other parameters needed, such as addresses of the default router, DNS servers, the time server etc.

(ii) A DHCP server should be located in the subnet of the access point of the mobile node or atleast a DHCP relay should provide forwarding of the messages.

Disadvantages

(i) Security Issue there is no authentication of DHCP messages specified. This means that the mobile node cannot trust a DHCP server and the DHCP server cannot trust the mobile node.

(ii) There is no protocol for server-server configuration i.e., one DHCP server cannot communicate with another DHCP server and exchange currently used configuration thus, configurations on servers have to be set up by hand.

(iii) An administrator has to take care that every DHCP server has its own address space for clients. This typically results in address space fragmentation.

3.4.3 Internet Control Message Protocol (ICMP)

Q20. Write a short notes on ICMP.

Answer : Model Paper-III, Q7(a)

Internet Control Message Protocol (ICMP)

ICMP has been designed to overcome the problems posed by IP protocol. It is used in IP network management and administration. Its importance is seen in IP implementations. It is said to be a control protocol because it does not hold the data instead it keeps the report of data. The latest version of ICMP is ICMP4.

Types of ICMP Messages

ICMP messages are categorized into following two types,

1. Error-reporting messages
2. Query messages.

1. Error Reporting Messages

These messages report about the issues encountered by host/ router while processing an IP packet.

2. Query Messages

These messages help the network manager in retrieving specific information about the network from host/router.

Format of ICMP Message

Every ICMP message is encapsulated with an 8-byte header, which is followed by variable length data field. The format of header vary depending on the type of message being transmitted, the first 32-bits of the header remains the same in every message. The general format of ICMP message is as follows.

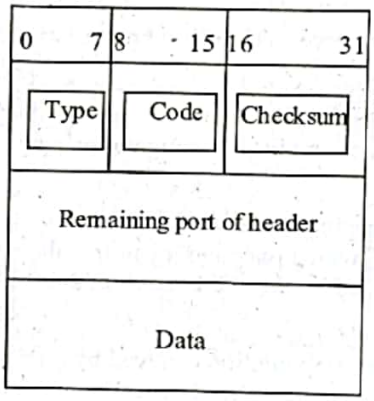


Figure (1): ICMP Message Format

1. Type

This is a 1-byte field that specifies the message type.

2. Code

This is a 1-byte field that specifies the reason for including a particular type of message.

3. Checksum

This is a 2-bytes field that is used for detecting the errors within the message.

4. Remaining Part of Header

This is a 4-byte field that contains information specific to the type of message specified in "type" field.

5. Data

This is a variable length field that contain data pertaining to respective message type. If "error messages" are specified in "type" field then the data part contain information for searching the actual erroneous packet. Moreover if "query messages" are specified in "type" field then data part contain additional information depending on the query type.

Message Format of ICMPv4

ICMPv4 is the integral part of IPv4 format (i.e., fourth version of IP protocols). This is included in the IPv4 header format. Its main purpose is to provide the information of error, loss of data packets and also it controls the data.

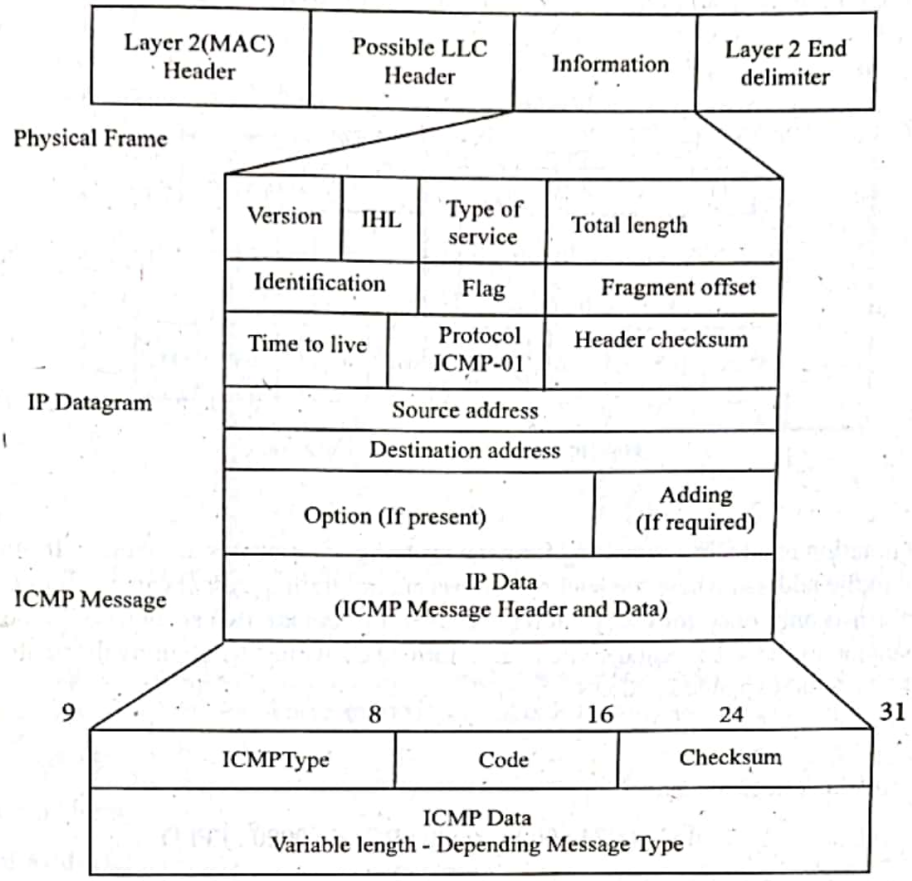


Figure (2): ICMPv4 Message Format

The above figure shows the basic ICMPv4 message format. It also shows the association between IP and physical frame. The ICMPv4 messages are transmitted in the data area of IPv4 datagram which uses protocol type of 1. In addition to this, it will follow all standard IPv4 datagram formatting rules. The ICMPv4 has a fixed format header wherein the first octet which is type field specifies the format of ICMPv4 message, the single octet code field specifies the type of message in use, and the 16 bit checksum field specifies the integrity check on the complete ICMPv4 message including header and data areas. The computation of actual value within the checksum field is performed by breaking the message into sequence of 16 bit words. Then it is added in 1's compliment arithmetic with any carry-the generated result in then added into the checksum field. However, the IP header is not significantly used in the computation of ICMPv4 checksum. Moreover, the variable length ICMPv4 data area specifies the actual message.

3.4.4 IPv6

Q21. Explain about IPv6 addresses.

Answer : **Model Paper-III, Q7(b)**

IPv6 Addresses

The IPv6 addresses were introduced to overcome the problems related to,

(i) Address depletion for the Internet

(ii) Lack of accommodation for real time audio and video transmission

(iii) Data encryption and authentication.

Structure

An IPv6 address is 128 bits long (i.e. 16 bytes). The structure of IPv6 addresses is based on hexadecimal colon notation and abbreviation that enables the IPv6 address to be more readable and abbreviated.

(a) Hexadecimal Colon Notation

Hexadecimal colon notation of IPv6 address makes them more readable. In hexadecimal colon notation 128 bits are divided into eight sections where each section is of 2 bytes, which requires four hexadecimal digits. This implies that IPv6 addresses comprises of 32 hexadecimal digits. The arrangement of these digits is made in such a way that a colon is placed as a separator between every four digits.

Example

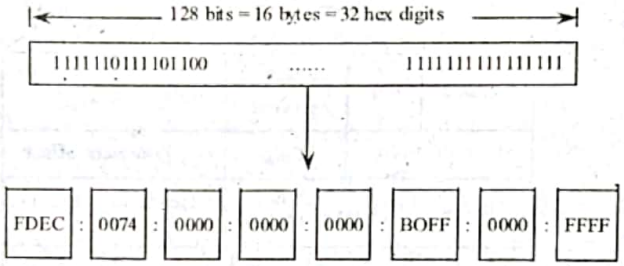


Figure: Hexadecimal Colon Notation

(b) Abbreviation

The hexadecimal notation results in a very long format consisting of numerous zero digits. In such cases, the abbreviation technique can be applied to the address where the leading zeroes (but not trailing zeros) can be eliminated from the section. The abbreviation can be performed only once for every address. That is, if there are two sections of zeroes, only one of them is abbreviated. The re-expansion of the abbreviated address is performed easily just by aligning the unabbreviated parts and inserting zeroes so as to get the original expanded address.

Example

Consider the hexadecimal notation as,

FDEC : 0074 : 0000 : 0000 : BOFF : 0000 : FFFO

After Abbreviation,

FDEC : 74 : 0 : 0 : BOFF : 0 : FFFO

More Abbreviation,

FDEC : 74 : : BOFF : 0 : FFFO

Address Space

The IPv6 addresses consists of much larger address space with the availability of storing maximum of 2^{128} address. The address of IPv6 is divided into various categories, which are defined by the left most bits called "type prefix" of each address. This prefix is of variable length and is used so as to ensure that the first part of a code is different from other code, thereby avoiding ambiguity issue. The following table shows the prefix of every address type,

	Type Prefix	Type of Address
1.	0000 0000	Reserved
2.	0000 0001	Unassigned
3.	0000 001	ISO network addresses
4.	0000 010	IPX (Novell) network address
5.	0000 011	Unassigned
6.	0000 1	Unassigned
7.	0001	Reserved
8.	001	Reserved
9.	010	Provider based unicast addresses
10.	011	Unassigned

11.	100	Geographic based unicast addresses
12.	101	Unassigned
13.	110	Unassigned
14.	1110	Unassigned
15.	11110	Unassigned
16.	111110	Unassigned
17.	1111 110	Unassigned
18.	1111 11100	Unassigned
19.	1111 1110 10	Link local addresses
20.	1111 1110 11	Site local addresses
21.	1111 1111	Multicast addresses

Table: Address of IPv6

Type of Addresses

IPv6 defines the following different type of addresses,

1. **Unicast Addresses**

The unicast address defines a single host. Therefore, if the packet is supposed to be forwarded using unicast address, then it should be delivered to that particular destination. There are two types of unicast addresses defined by IPv6.

(a) Geographic based address

(b) Provider based address.

(a) **Geographic Based Address**

Geographic based address was introduced as an alternative for Simple Internet Protocol (SIP). These addresses are based on geographic location and once assigned they cannot be changed. The geographic based addresses are significantly complicated and are highly expensive. The geographic address allocation is used in developing improved automatic and dynamic host configuration in IPv6.

(b) **Provider Based Address**

Provider based address is generally used as a unicast address by a normal host.

The address format of provider based address is as follows,

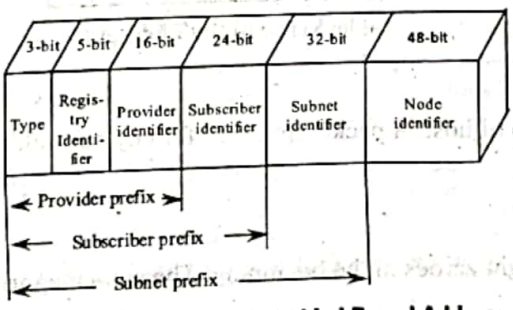


Figure: Address Format of Provided Based Address

(i) **Type Identifier**

The type identifier is a 32-bit field that defines the address as a "provider-based address".

(ii) **Registry Identifier**

The registry identifier is a 5-bit field that specifies the agency that has registered the address.

(iii) **Provider Identifier**

The provider identifier is a 16-bit field that specifies the provider for Internet access.

(iv) Subscriber Identifier

The subscriber identifier is a 24-bits field that is assigned if the organization subscribe to the Internet via provider.

(v) Subnet Identifier

A subnet identifier is a 32-bit field that defines a particular subnetwork that belongs to a subscriber.

(vi) Node Identifier

A node identifier is a 48-bit field that specifies the identity of the node which is connected to a subnet.

2. Multicast Address

Multicast address defines a group of hosts rather than a specific host if a packet is supposed to be forwarded, then it is delivered to each and every member of a group. The address format of multicast address is as follows,

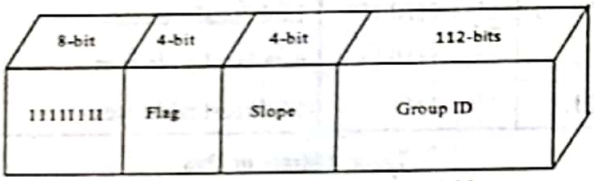


Figure: Address Format of Multicast Address

(i) Flag

The flag field is a 4-bit field that specifies whether the group address is a permanent address (0000) or transient address (0001).

(ii) Scope

The scope field is a 4-bit field that defines the scope of the group address. The following table shows different scopes.

Type Perfix	Address Type
0000	Reserved
0001	Node local
0010	Link local
0101	Site local
1000	Organizational
1110	Global
1111	Reserved

Table: Scope of IPv6 Address

3. Any Cast Address

Any cast address defines a group of host. A packet intended for any cast address is delivered to only a single member of any cast group that have shortest route.

4. Reserved addresses

Reserved addresses consist of eight zeroes in the beginning. The sub-categories of reserved addresses are as follows,

(a) Unspecified Address

It is used when the host is unaware of its own address and requests other host to determine its address.

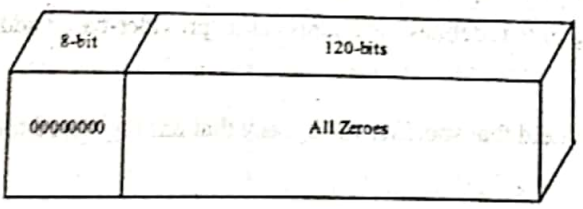


Figure: Unspecified Address

(b) **Loop Back Address**

It is used by the host inorder to test itself without traversing the network.

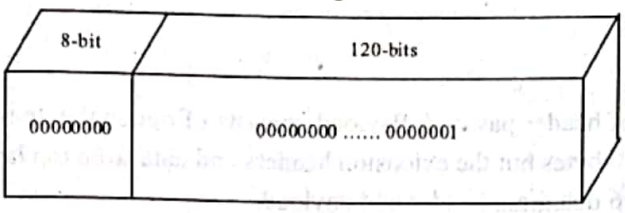


Figure: Loop-back Address

(c) **Compatible Address**

It is used by the host that wants to perform transition from IPv4 to IPv6.

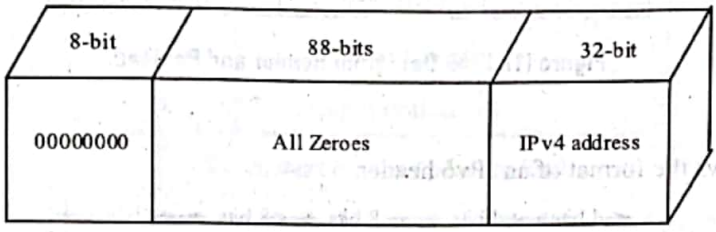


Figure: Compatible Address

(d) **Mapped Address**

It is used by a host that wants to perform transition from IPv6 to IPv4.

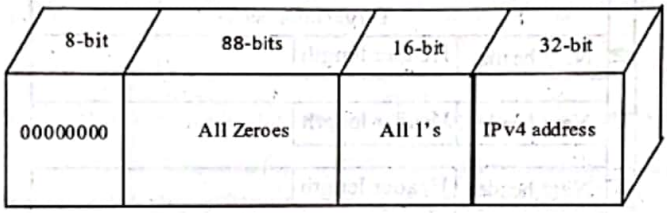


Figure: Mapped Address

5. **Local Addresses**

If an organization is in need of IPv6 protocol without connecting itself to the global Internet, then it uses local addresses. Alternatively, local addresses are the addresses provided to private networks. An organization using this address cannot send beyond its boundary network.

The two types of addresses defined by local addresses are as follows,

(a) **Link Local Address**

It is used in an isolated subnet.

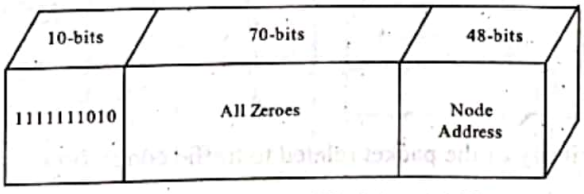


Figure: Address Format of Link Local Address

(b) **Site Local Address**

It is used in an isolated site consisting of many subnets.

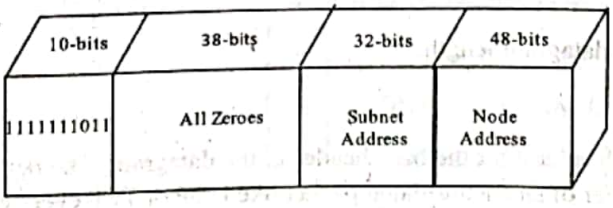


Figure: Address Format of Site Local Address

Q22. Draw the IPv6 packet header format.

Answer :

IPv6 Header Format

The IPv6 packet is made up of header payload. Payload consists of optional extension headers and data from top layer. The base header has fixed length of 40 bytes but the extension headers and data from top layer has approximately 65,535 byte of data. The following figure shows IPv6 datagram header and payload.

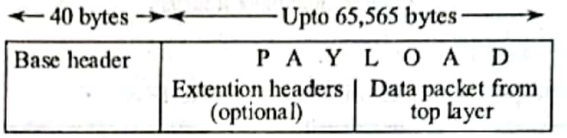


Figure (1): IPv6 Datagram Header and Payload

Base Header

The following figure shows the format of an IPv6 header.

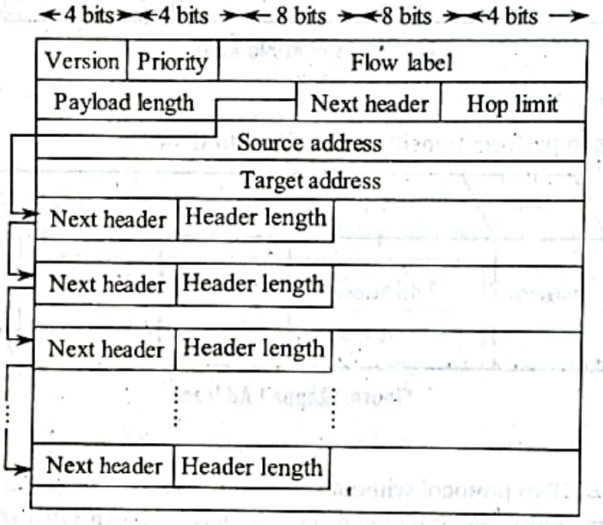


Figure (2): Format of an IPv6 Header

The base header of an IPv6 header has the following fields,

(i) Version

It is a 4-bit field defining the version number of the Internet protocol.

Example: IPv6 has the value 6.

(ii) Priority

It is a 4-bit field defining the priority of the packet related to traffic congestion.

(iii) Flow Label

It is a 3-byte field used for handling flow of data.

(iv) Payload Length

It is a 2-byte field defining IP datagram length.

(v) Next Header

It is a 8-bit field defining the header after the base header in the datagram. The next header can be an optional extension headers used by IP or the header of an encapsulated packet like UDP or TCP every extension header includes this field. In version 4, this field is called the protocol. The values of the next headers are tabulated below,

Code	Next Header
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	No next header
60	Target option

Table: Next Header Codes for IPv6

(vi) **Hop Limit**

It is 8-bit field, which has the same function as that of TTL field in IPv4.

(vii) **Source Address**

It is 16-byte Internet address field identifying the actual source of the datagram.

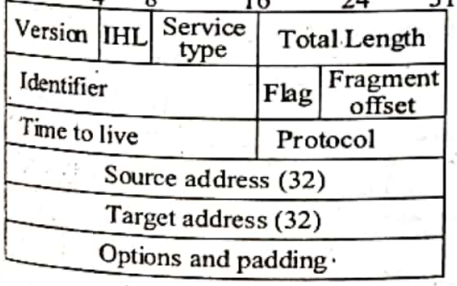
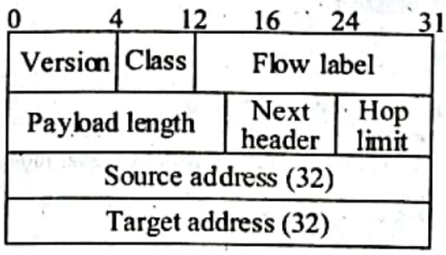
(viii) **Target Address**

It is a 16-byte Internet address field identifying the final target of the datagram. In case of source routing, this field includes the address of the next router.

Q23. Compare IPv4 and IPv6. Also write the advantages of IPv6 over IPv4.

Answer :

Comparison of IPv4 and IPV6

IPv4 Headers	IPv6 Headers
1. IPv4 is the fourth version of Internet protocol.	1. IPv6 is the sixth version of Internet protocol.
2. 	2. 
Figure: IPv4 Header	**Figure: IPv6 Header**
3. IPv4 allows 32-bit source and target addresses.	3. IPv6 allows 128-bit source and target addresses.
4. IPv4 has service type field which represents priority of the packet.	4. IPv6 do not have service type field. Its functionality is handled by priority and flow label fields.
5. In IPv4, fields are not renamed.	5. In IPv6, some of the fields are renamed. **Example:** Type of service to traffic class and total length to payload length etc.

6.	In IPv4, identification, flag and offset fields are present.	6.	In IPv6, identification, flag and offset fields are removed from the base header and added in the fragmentation extension header.
7.	IPv4 has a TTL field and protocol field.	7.	In IPv6, TTL field is replaced by hop limit and protocol field is replaced by next header field.
8.	IPv4 has a header checksum field.	8.	In IPv6, header checksum field is removed because checksum is carried out by its upper layer protocols.
9.	IPv4 has an options field.	9.	In IPv6, options field is moved under extension header.

Advantages of IPv6 Over IPv4

IPv6 has the following advantages over IPv4,

1. IPv6 has a larger address space. It is 128-bits long. It has 296 increase in its address space compared with that of 32-bit address of IPv4.
2. It has a better header format wherein the options are separated from the base header and if required they are placed in between the base header and the upper-layer data. Routing process is simplified and speeded up because most options do not require to be checked by the routers.
3. It has new options which adds additional functionalists.
4. If necessary, the protocol can be intended by new technologies or applications.
5. It supports resource allocation. The type-of-service field is removed and a method called flow label is introduced which allows the source to request packet handling. This method can handle traffic like real-time audio and video can be supported.
6. It provides greater security. Confidentiality and integrity of the packet is provided by encryption and authentication options in IPv6.

IMPORTANT QUESTIONS

1. Discuss about forwarding and routing functions of network layer. **Refer Q9**
2. Explain about virtual circuit network and datagram network. **Refer Q11**
3. Write short notes on the following,
   (i) Output processing
   (ii) Queueing
   (iii) Routing control plane. **Refer Q16**
4. Explain the working of DHCP protocol with its header format. **Refer Q19**
5. Explain about IPv6 addresses. **Refer Q21**
6. Compare IPv4 and IPv6. Also write the advantages of IPv6 over IPv4. **Refer Q23**