Unit – I: Network Layer Protocols

Q.1 Explain Network Layer Protocol.

ANS.

- Network layer protocols are a vital part of the internet infrastructure, **responsible for routing and forwarding data packets** between devices on a network. These protocols are used to ensure that data is delivered to the correct destination and in a timely manner.

  - **There are several network layer protocols that are commonly used, each serving a specific purpose.**

- **Internet Protocol (IP):** This protocol is responsible for addressing and routing data packets across the internet. It works by assigning a unique numerical address, called an IP address, to each device on a network. This allows data packets to be forwarded to the correct device based on the IP address.
- **Internet Control Message Protocol (ICMP):** This protocol is used to transmit error messages and other information between devices on a network. It is often used to troubleshoot network issues or to send diagnostic information.
- **Address Resolution Protocol (ARP):** This protocol is used to map IP addresses to physical addresses, such as a device's media access control (MAC) address. This allows devices to communicate with each other on a network.
- **Routing Information Protocol (RIP):** The Routing Information Protocol (RIP) is another network layer protocol that is used to determine the best path for data packets to travel between devices on a network. It works by sending updates to other devices on the network, allowing them to update their routing tables and determine the best route for data packets.
- **Open Shortest Path First (OSPF) protocol:** This is a routing protocol that is used in large networks, such as enterprise networks or internet service providers. It works by using a link-state database to determine the best route for data packets and can quickly adapt to changes in the network.

Q.2 Explain IPV4 Addresses in detail.

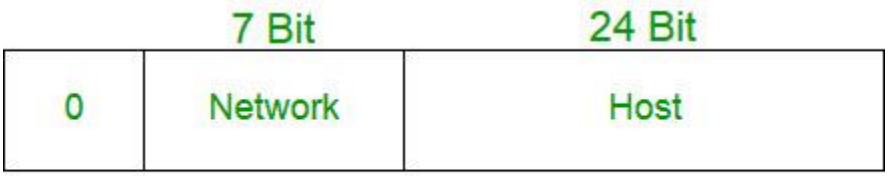
ANS.

- **These are:**

1. **Class A**
2. **Class B**
3. **Class C**
4. **Class D**
5. **Class E**

1. Class A

- IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.



Class A

2. Class B

- IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

Class B

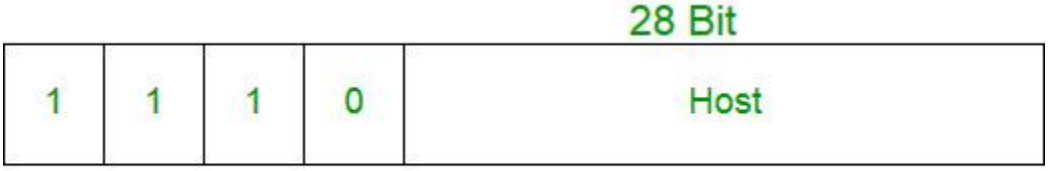
3. Class C

- IP addresses belonging to class C are assigned to small-sized networks.

Class C

4. Class D

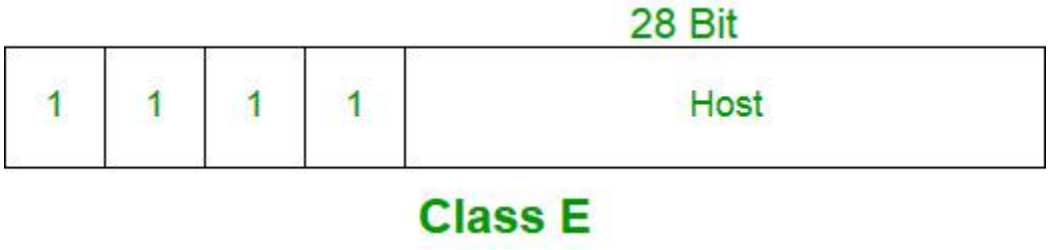
- IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.



Class D

5. Class E

- IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Range of Special IP Addresses

169.254.0.0 – 169.254.0.16: Link-local addresses
127.0.0.0 – 127.0.0.8: Loop-back addresses
0.0.0.0 – 0.0.0.8: used to communicate within the current network.

Q.3 Explain Forwarding of IP Packets.

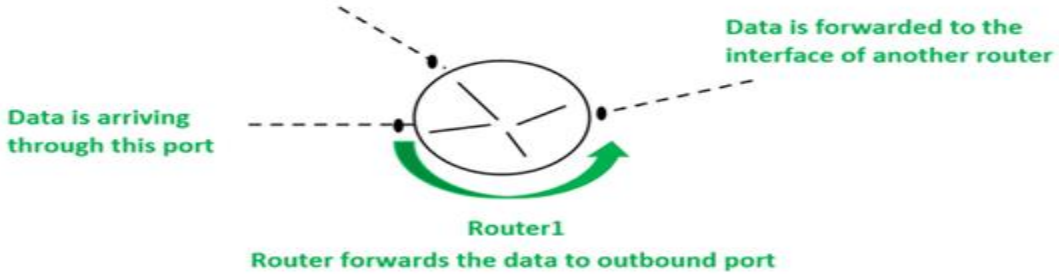
ANS.

Packet Forwarding in Router:

- Routers are used on the network for forwarding a packet from the local network to the remote network. So, the process of routing involves the packet forwarding from an entry interface out to an exit interface.

Working:

- The following steps are included in the packet forwarding in the router-
- The router takes the arriving packet from an entry interface and then forwards that packet to another interface.



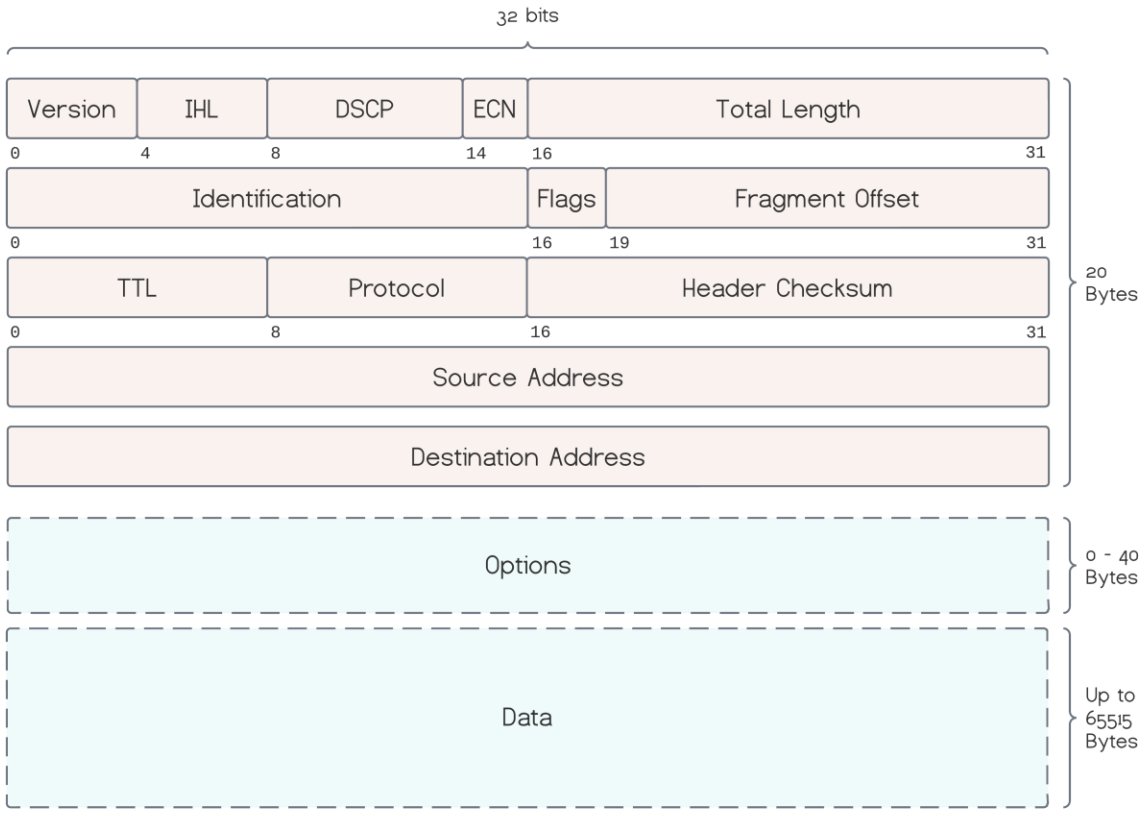
- **Forwarding based on destination address**

Following are the packet forwarding techniques based on the destination host:

- **Next-Hop Method:** By only maintaining the details of the next hop or next router in the packet's path, the next-hop approach reduces the size of the routing table. The routing table maintained using this method does not have the information regarding the whole route that the packet must take.
- **Network-Specific Method:** In this method, the entries are not made for all of the destination hosts in the router's network. Rather, the entry is made of the destination networks that are connected to the router.
- **Host-Specific Method:** In this method, the routing table has the entries for all of the destination hosts in the destination network. With the increase in the size of the routing table, the efficiency of the routing table decreases. It finds its application in the process of verification of route and security purposes.
- **Default Method:** Let's assume- A host in network N1 is connected to two routers, one of which (router R1) is connected to network N2 and the other router R2 to the rest of the internet. As a result, the routing table only has one default entry for the router R2.

Q.4 Explain Internet Protocolin detail with diagram.

ANS.



1. Version

- IP version field set to 4 for IPv4.

2. Internet Header Length

- IHL is the number of 32-bit words making up the header field. As the first 20 bytes are mandatory, the minimum number is 5, and the maximum is 15.

3. Differentiated Services Code Point (DSCP)

- It specifies the type of service for differentiated services, such as voice-over IP.

4. Explicit Congestion Notification (ECN)

- ECN carries a network congestion notification without dropping packets or wasting bandwidth when supported.

5. Total Length

- It represents the total size of the datagram, including the header and the data segment.

6. Identification

- This field uniquely identifies the group of fragments of a single IP datagram.

7. Flags

- Different combinations of the flags control the fragmentation and indicate fragmented datagrams.
- For example, if the *don't fragment flag* (bit 1) is set to 1, and the destination host can't assemble the fragmented packets, it will drop them.

8. Fragment Offset

- It contains the offset of a fragmented packet.

9. Time to Live (TTL)

- The number of hops a packet lives. Each router decrements the TTL field and discards the packet when it reaches 0. This way, looping packets are eliminated.

10. Protocol

- It's the protocol for the data part.

11. Header Checksum

- It's a checksum for error detection, covering only the header field. Each router checks this value and discards the packet if an error is detected. Uncorrupted packets return 0 when summing the whole header, including the checksum itself.

12. Source Address

- Source host IPv4 address.

13. Destination Address

- Destination host IPv4 address.

14. Options

- Additional options are stored in this field when present.

Q.5 Explain ICMPv4 in detail.

ANS.

- ICMP is a network layer protocol.
- ICMP messages are not passed directly to the data link layer. The message is first encapsulated inside the IP datagram before going to the lower layer.

Types of ICMP messages

- **Information Messages** − In this message, the sender sends a query to the host or router and expects an answer. For example, A host wants to know if a router is alive or not.
- **Error-reporting message** − This message report problems that a router or a host (destination) may encounter when it processes an IP packet.

- **Query Message** − It helps a router or a network manager to get specific information from a router or another host.

Category	Type	Message
Error-Reporting Messages	3	Destination unreachable
	4	Source quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirection
Query Message	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router Solicitation or advertisement

- **Source Quench** − It requests to decrease the traffic rate of message sending from source to destination.
- **Time Exceeded** − When fragments are lost in a network the fragments hold by the router will be dropped and then ICMP will take the source IP from the discarded packet and inform the source, that datagram is discarded due to the time to live field reaches zero, by sending time exceeded message.
- **Fragmentation Required** − When a router is unable to forward a datagram because it exceeds the MTU of the next-hop network and the DF (Don't Fragment) bit is set, the router is required to return an ICMP Destination Unreachable message to the source of the datagram, with the Code indicating fragmentation is needed and DF (Don't Fragment) set.
- **Destination Unreachable** − This error message indicates that the destination host, network, or port number that is specified in the IP packet is unreachable
  - **Redirect Message** − A redirect error message is used when a router needs to tell a sender that it should use a different path for a specific destination. It occurs when the router knows a shorter path to the destination.

Unit-2: Next Generation IP

Q.1 Explain IPv6 Addressing.
Ans.

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

Components in Address format:

1. There are 8 groups and each group represents 2 Bytes (16-bits).
2. Each Hex-Digit is of 4 bits (1 nibble)
3. Delimiter used – colon (:)

IPv6 protocol responds to the above issues using the following main changes in the protocol:

1. Large address space
An IPv6 address is 128 bits long .compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.
2. Better header format
IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data . This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
3. New options
IPv6 has new options to allow for additional functionalities.
4. Allowance for extension
IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
5. Support for resource allocation
In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.
6. Support for more security
The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Q.2 Explain Address space allocation.
Ans.

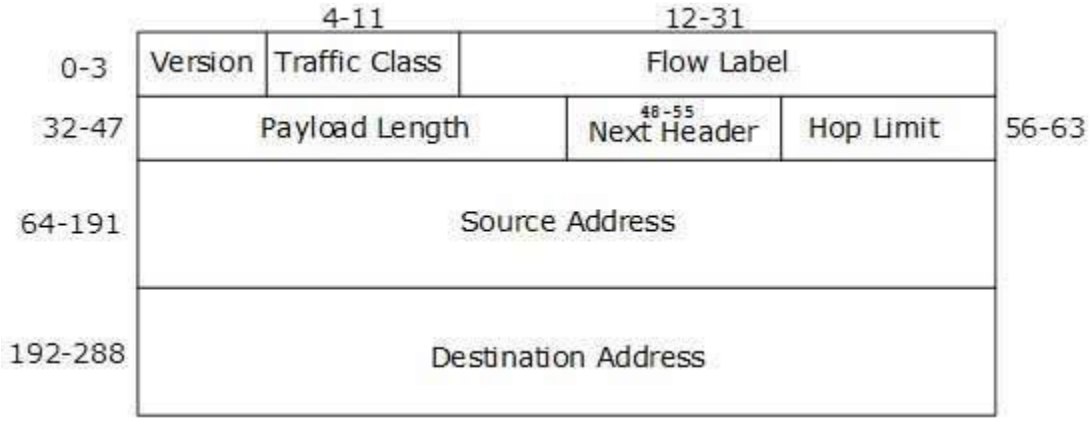
Prefix	Allocation	Fraction of Address Space
0000 0000	Reserved	1/256
0000 0001	Unassigned (UA)	1/256
0000 001	Reserved for NSAP	1/128
0000 01	UA	1/64
0000 1	UA	1/32
0001	UA	1/16
001	Global Unicast	1/8
010	UA	1/8
011	UA	1/8
100	UA	1/8
101	UA	1/8
110	UA	1/8
1110	UA	1/16
1111 0	UA	1/32
1111 10	UA	1/64
1111 110	UA	1/128

Prefix	Allocation	Fraction of Address Space
1111 1110 0	UA	1/512
1111 1110 10	Link-Local Unicast Addresses	1/1024
1111 1110 11	Site-Local Unicast Addresses	1/1024
1111 1111	Multicast Address	1/256

IPv6 addresses are assigned to organizations in much larger blocks as compared to IPv4 address assignments—the recommended allocation is a /48 block which contains 280 addresses, being 248 or about 2.8×1014 times larger than the entire IPv4 address space of 232 addresses and about 7.2×1016 times larger than the /8 .

Q.3 Explain The IPv6 Protocol Packet Format.

Ans.



The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

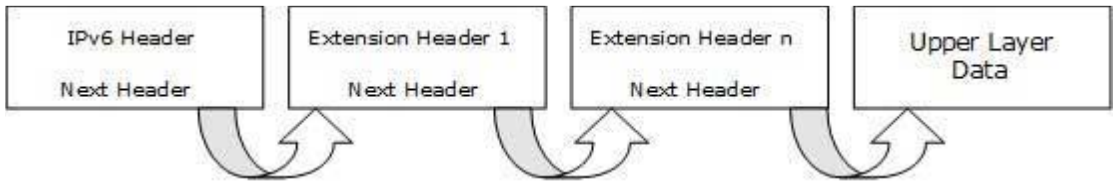
Q.4 Explain Extension Headers of IPv6.

In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required or is rarely used. All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers. Each Extension Header is identified by a distinct value.

Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

These headers:
1. should be processed by First and subsequent destinations.
2. should be processed by Final Destination.

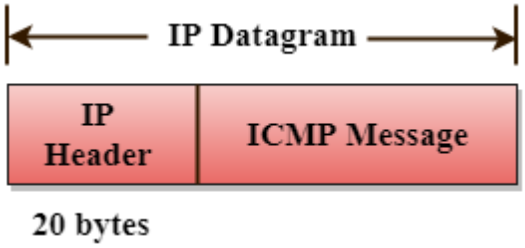
Extension Headers are arranged one after another in a linked list manner, as depicted in the following diagram:



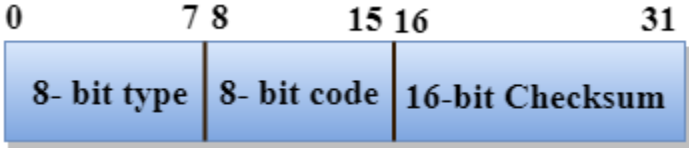
Q.5 Explain ICMPv6 Protocol.

Ans.

ICMP stands for Internet Control Message Protocol. The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender. ICMP uses echo test/reply to check whether the destination is reachable and responding. ICMP handles both control and error messages, but its main function is to report the error but not to correct them.



The Format of an ICMP message



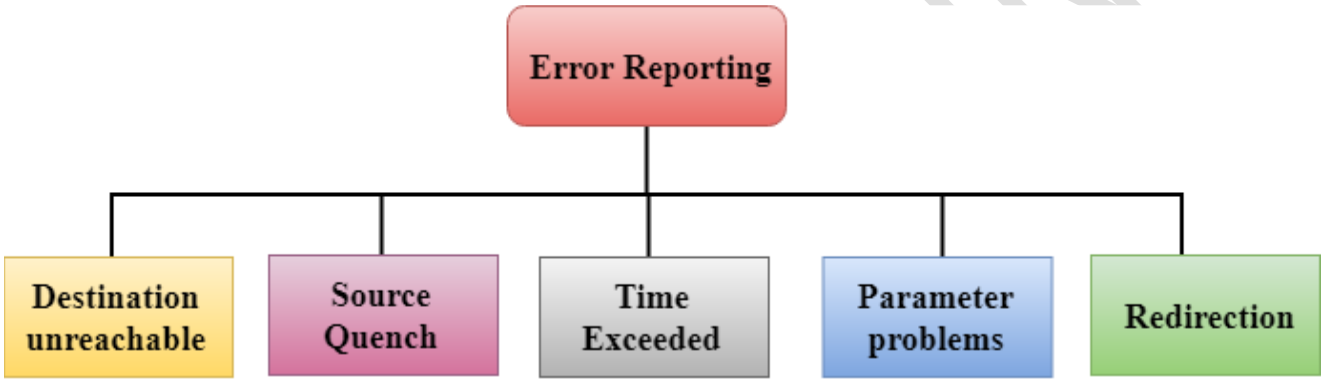
Q.6 Explain Error Reporting in ICMPv6 Protocol.

Ans.

ICMP protocol reports the error messages to the sender.

Five types of errors are handled by the ICMP protocol:

1. Destination unreachable
2. Source Quench
3. Time Exceeded
4. Parameter problems
5. Redirection



Destination unreachable: The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable.

Source Quench: The purpose of the source quench message is congestion control. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate so that the router will be free from congestion.

Time Exceeded: Time Exceeded is also known as "Time-To-Live". It is a parameter that defines how long a packet should live before it would be discarded.

Parameter problems: When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.

Redirection: Redirection message is generated when host consists of a small routing table. When the host consists of a limited number of entries due to which it sends the datagram to a wrong router. The router that receives a datagram will forward a datagram to a correct router and also sends the "Redirection message" to the host to update its routing table.

Q.7 Write short note on: ICMPv6 informational messages, Neighbor-Discovery Messages& Group Membership Messages.

Ans.

ICMPv6 informational messages: ICMPv6 informational messages are used for network diagnostic functions and additional critical network functions like Neighbor Discovery, Router Solicitation & Router. Advertisements, Multicast Memberships. Echo Request and Echo Reply (used by many commands and utilities like "ping" for network diagnostics and communication trouble shooting) are also ICMPv6 informational

messages. The ICMPv6 informational messages have values for the Type field (8 bit binary number) between 128 and 255.

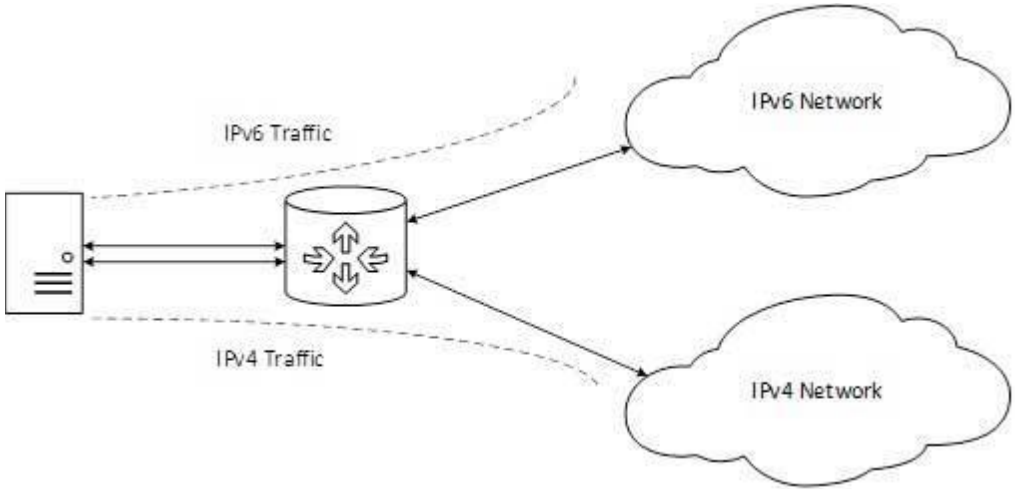
. Neighbor-Discovery Messages: ICMPv6 ND (Neighbor Discovery) Messages are used for the Neighbor Discovery Protocol (NDP). ND (Neighbor Discovery) Messages includes Router Solicitation & Router Advertisement, Neighbor Solicitation and Neighbor Advertisement.

Group Membership Messages: ICMPv6 MLD (Multicast Listener Discovery) Messages are used by an IPv6 enabled router to discover hosts who are interested in multicast packets, and the multicast addresses they are interested. MLD (Multicast Listener Discovery) messages are used by MLD (Multicast Listener Discovery) Protocol. MLD (Multicast Listener Discovery) Protocol is the IPv6 equivalent of IGMP (Internet Group Management) Protocol in IPv4.

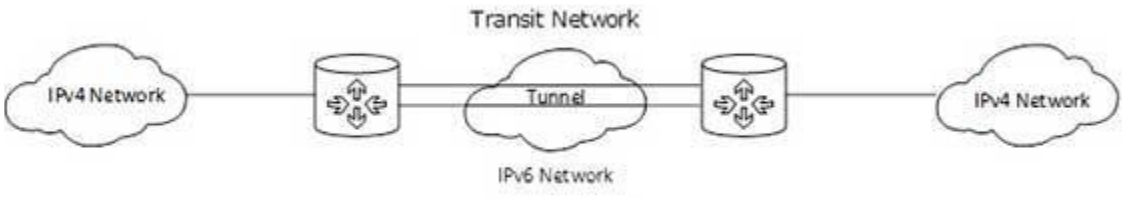
Q.8 ExplainTransition from IPv4 to IPv6.

Ans.

Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. It is unlike implementation of other new technologies where the newer one is backward compatible so the older system can still work with the newer version without any additional changes.



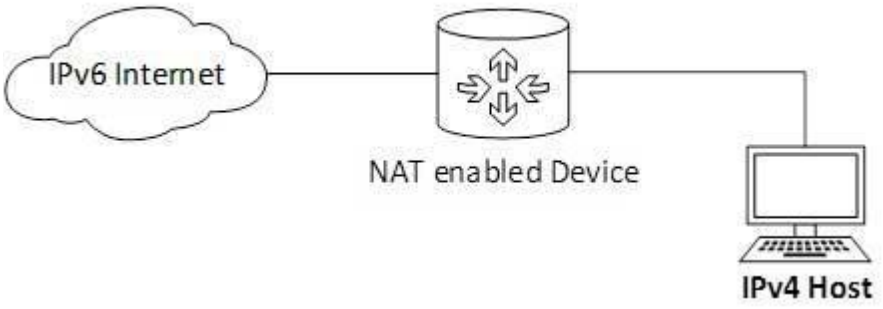
Tunneling



In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user‟s data can pass through a non-supported IP version.

NAT Protocol Translation

This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa. See the diagram below:



Unit-3Unicast Routing

Q.1 ExplainRouting.
Ans.

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. Thesoftware based routers have limited functionality and limited scope. A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination, router can make decision based on the following information:

- Hop Count
- Bandwidth
- Metric
- Prefix-length
- Delay

Routes can be statically configured or dynamically learnt. One route can be configured to be preferred over others.

Q.2 Explain difference Intra- and Inter-domain Routing.
Ans.

Basis	Interdomain Routing	Intradomain Routing
Definition	The interdomain routing algorithms are used for routing within as well as with other domains.	The intradomain routing algorithms are used for routing within domains.
Router information	It requires information about the routers in the current domain as well as other domains.	It requires information only about the routers in the current domain.
Protocols	For interdomain routing, the protocols used are known as exterior-gateway protocols as they route traffic outside as well as inside a domain.	For intradomain routing, the protocols used are known as interior-gateway protocols as they route traffic within a domain.
Types	Interdomain routing is done using Path Vector Routing which uses the Border Gateway Protocol (BGP).	Intradomain Routing is of two types: Distance Vector Routing (uses Routing Information Protocol (RIP) and Link State Routing (uses Open Shortest Path First (OSPF).
Internet	The Internet is assumed to be a collection of interconnected autonomous systems by the interdomain routing protocol.	The internet outside the autonomous system is ignored by intradomain routing protocols.

Q.3 ExplainDistance Vector Routing.

Ans.

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node.

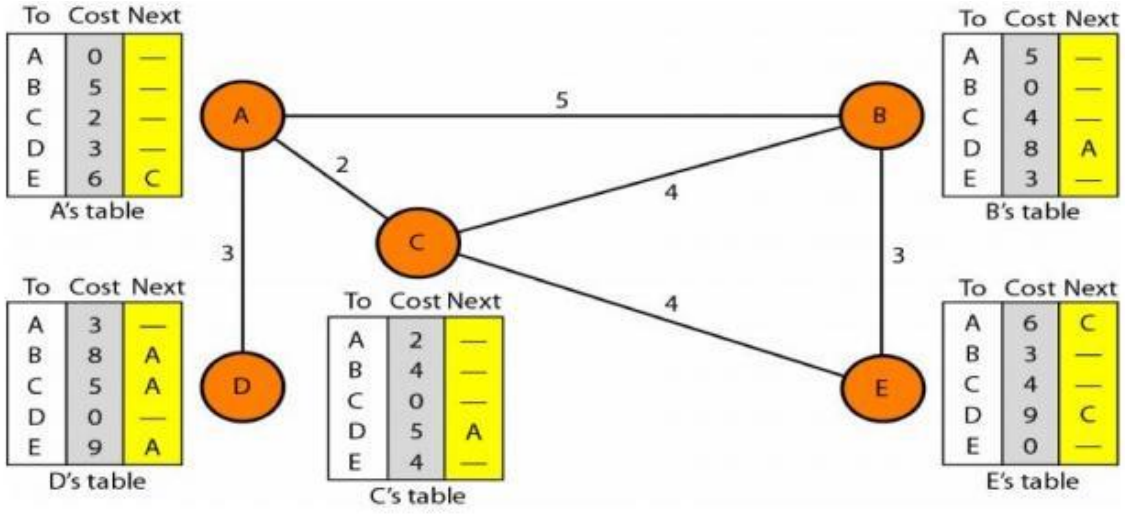


Figure 3.45 Distance vector routing tables

Initialization

The tables in above Figure are stable; each node knows how to reach any other node and the cost.

Sharing

The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E.

Updating

When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is *x* mi, and the distance between A and C is *y* mi, then the distance between A and that destination, via C, is $x + y$ mi.
2. The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.
3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

Q.4 ExplainLink State Routing.

Ans.

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected

including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.

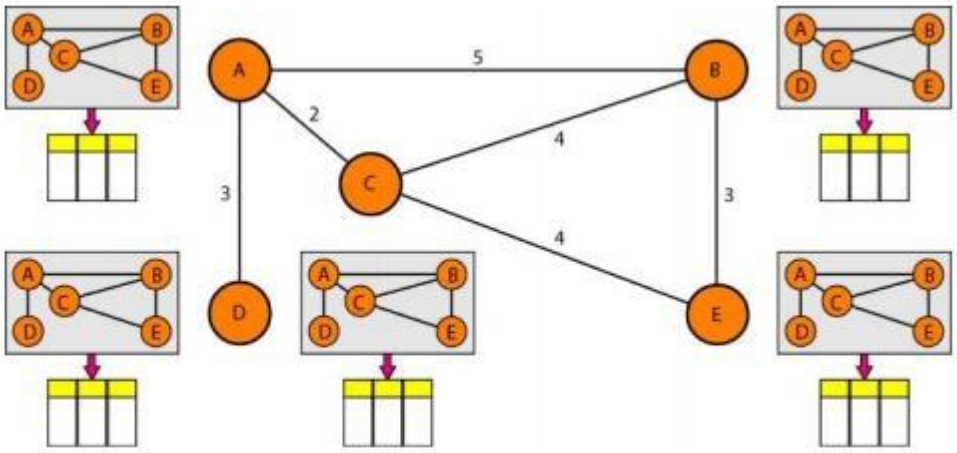
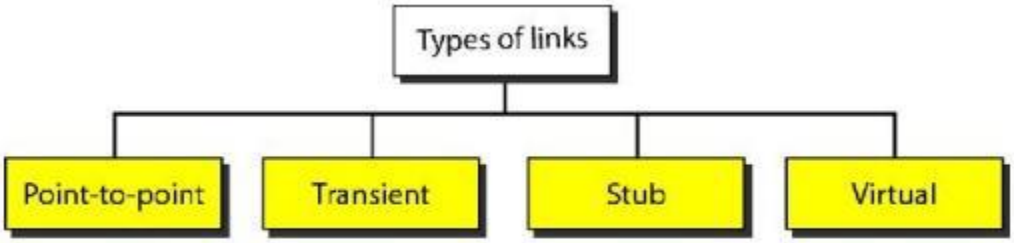


Figure 3.50 Concept of link state routing

Types of Links



Q.5 ExplainRIP Protocol& Message format.

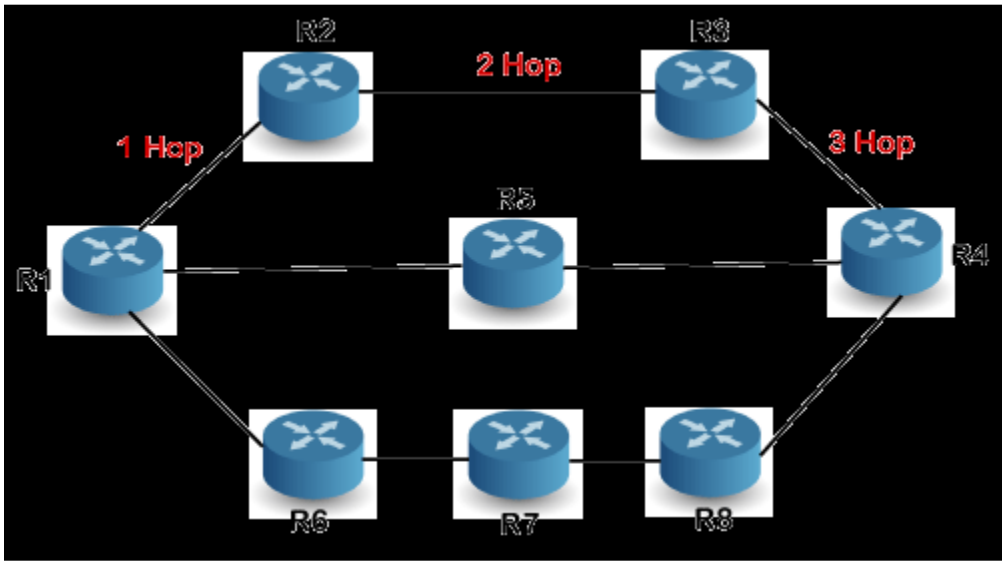
Ans.

RIP stands for Routing Information Protocol.

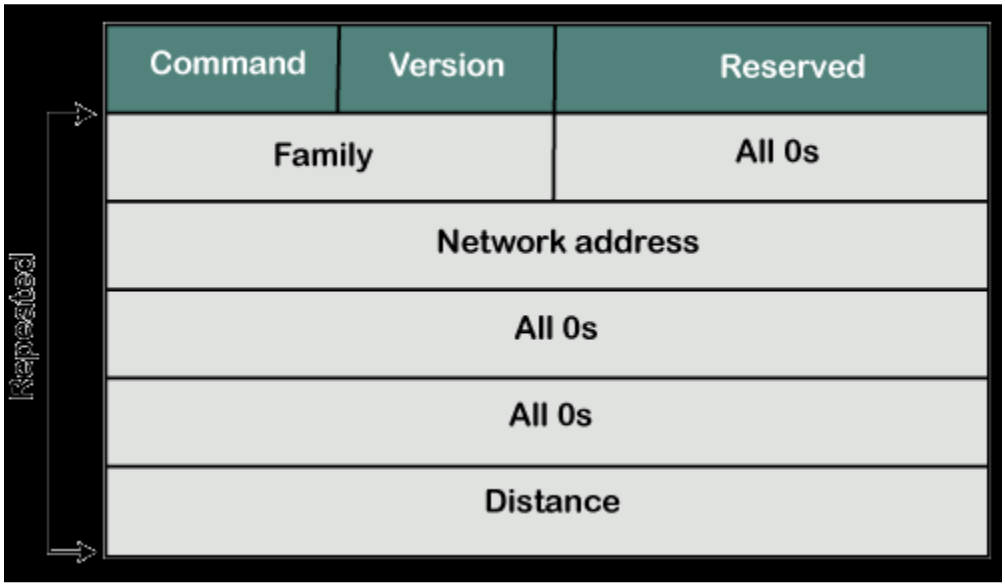
RIP is an intra-domain routing protocol used within an autonomous system.

Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area.

To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.



RIP Message Format



Command: It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.

- Version: Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.
- Reserved: This is a reserved field, so it is filled with zeroes.
- Family: It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.
- Network Address: It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.
- Distance: The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

Q.6 ExplainOSPF Protocol & Message format.

Ans.

The OSPF stands for **Open Shortest Path First**. It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network.
It is an interior gateway protocol that has been designed within a single autonomous system.

There are four types of links in OSPF:

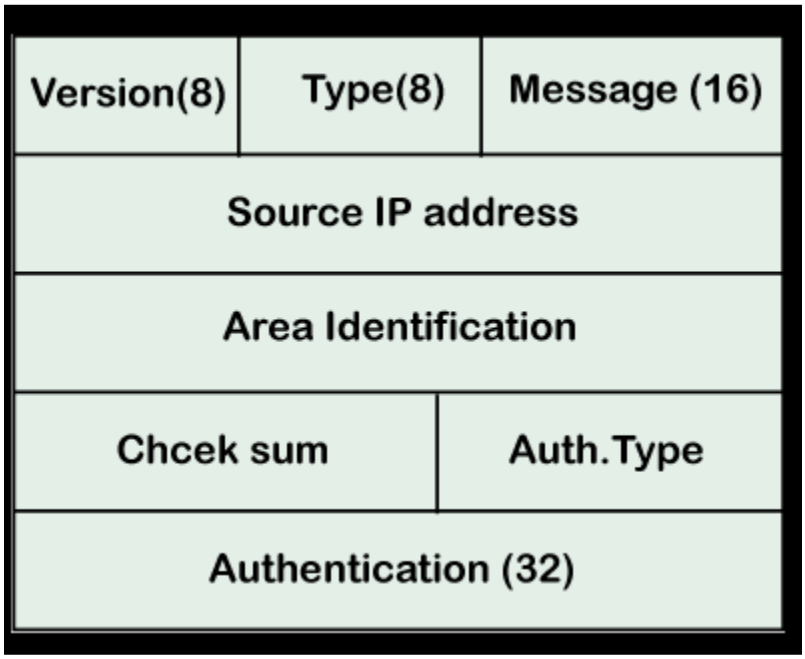
1. **Point-to-point link:** The point-to-point link directly connects the two routers without any host or router in between.

2. **Transient link:** When several routers are attached in a network, they are known as a transient link. The transient link has two different implementations: Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology.
Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.

3. **Stub link:** It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.

4. **Virtual link:** If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.

The following are the fields in an OSPF message format:



Q.7 ExplainBorder Gateway Protocol.

Ans.

. It is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet. As we know that Border Gateway Protocol works on different autonomous systems, so we should know the history of BGP, types of autonomous systems, etc.

BGP Features The following are the features of a BGP protocol:

Open standard It is a standard protocol which can run on any window device.

Exterior Gateway Protocol It is an exterior gateway protocol that is used to exchange the routing information between two or more autonomous system numbers.

Inter AS-domain routing It is specially designed for inter-domain routing, where inter AS-domain routing means exchanging the routing information between two or more autonomous number system.

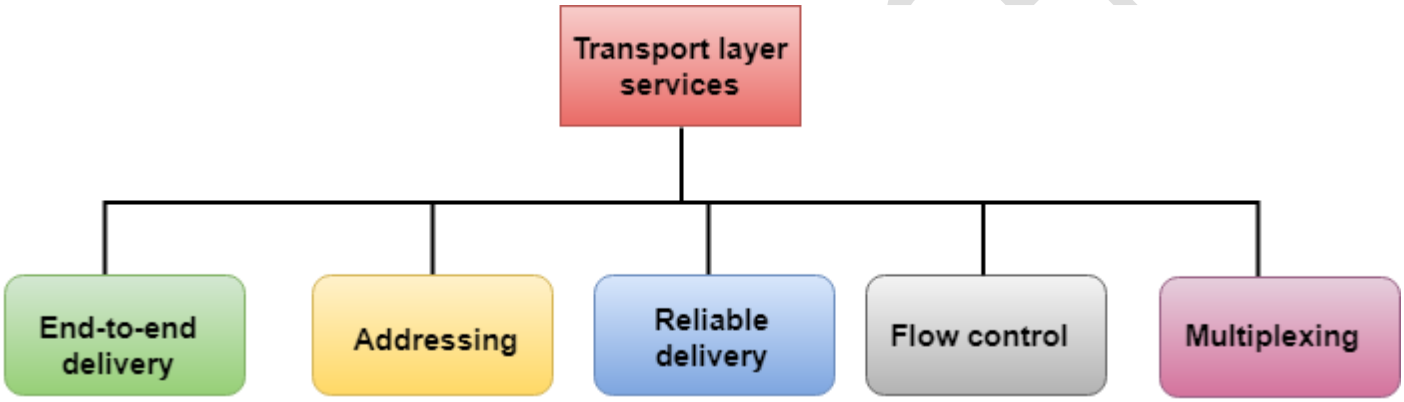
Supports internet It is the only protocol that operates on the internet backbone.

Unit-4: Transport Layer Protocols.

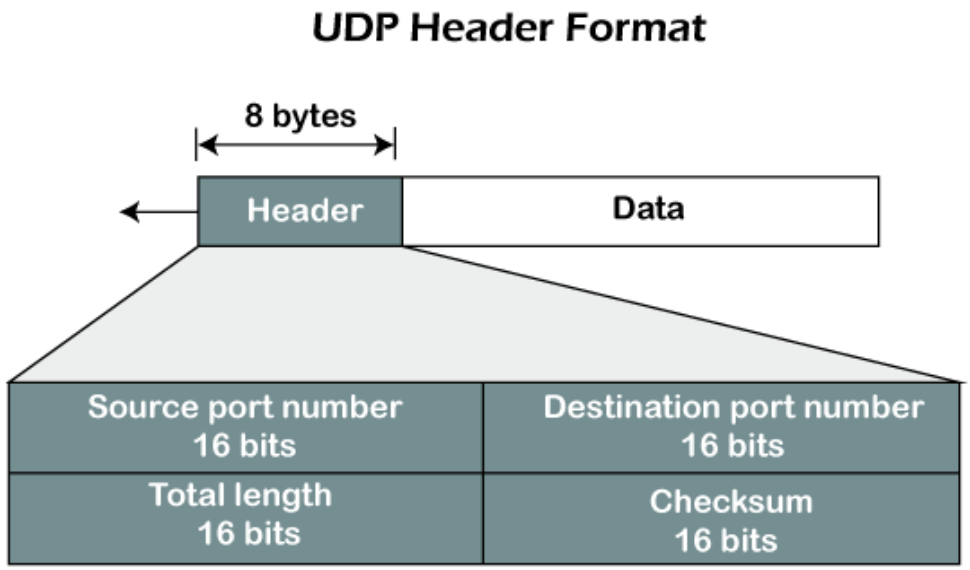
Q.1 Explain Services provided by the Transport Layer.
Ans.

The services provided by the transport layer protocols can be divided into five categories:

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- Multiplexing



Q.2 ExplainUDP Header Format.
Ans.

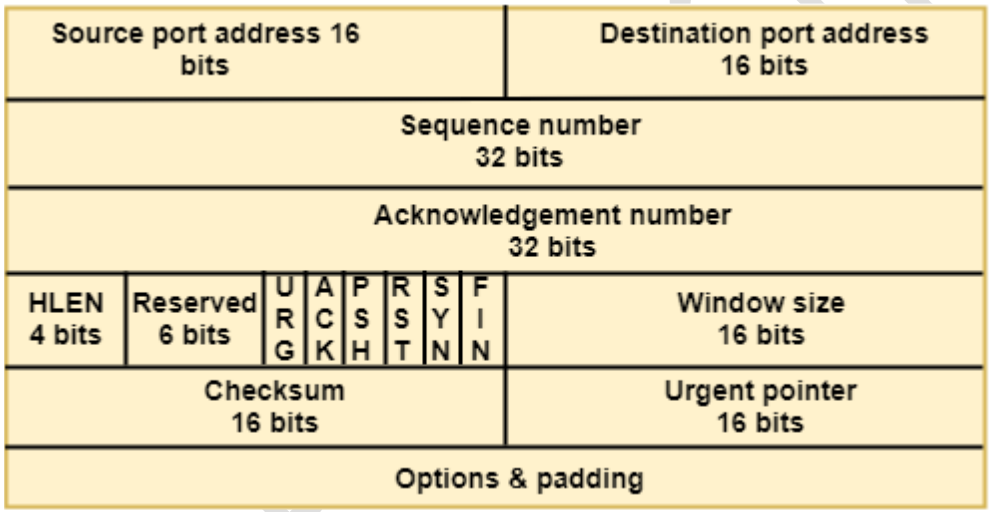


The UDP header contains four fields:

- **Source port number:** It is 16-bit information that identifies which port is going t send the packet.
- **Destination port number:** It identifies which port is going to accept the information. It is 16-bit information which is used to identify application-level service on the destination machine.
- **Length:** It is 16-bit field that specifies the entire length of the UDP packet that includes the header also. The minimum value would be 8-byte as the size of the header is 8 bytes.
- **Checksum:** It is a 16-bits field, and it is an optional field. This checksum field checks whether the information is accurate or not as there is the possibility that the information can be corrupted while transmission.

Q.3 Explain TCP Segment Format.

Ans.



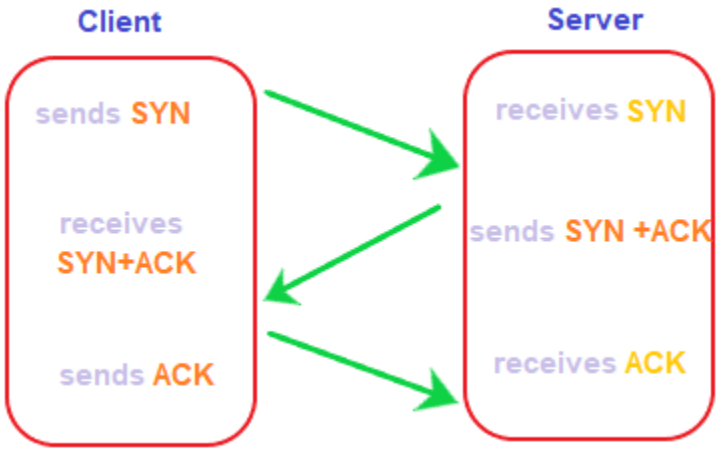
Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.

- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

Q.4 Explain TCP Connection (A 3-way handshake).

Ans.



The three handshakes are discussed in the below steps:

Step 1: SYN

SYN is a segment sent by the client to the server. It acts as a **connection request** between the client and server. It informs the server that the client wants to establish a connection. Synchronizing sequence numbers also helps synchronize sequence numbers sent between any two devices, where the same SYN segment asks for the sequence number with the connection request.

Step 2: SYN-ACK

It is an SYN-ACK segment or an SYN + ACK segment sent by the server. The ACK segment informs the client that the server has received the connection request and it is ready to build the connection. The SYN segment informs the sequence number with which the server is ready to start with the segments.

Step 3: ACK

ACK (Acknowledgment) is the last step before establishing a successful TCP connection between the client and server. The ACK segment is sent by the client as the response of the received ACK and SN from the server. It results in the establishment of a reliable data connection. After these three steps, the client and server are ready for the data communication process. TCP connection and termination are full-duplex, which means that the data can travel in both the directions simultaneously.

Q.5 Explain SCTP Packet Format.

Source port		Destination port	
32	Verification tag		
64	Checksum		
96	Chunk 1 type	Chunk 1 flags	Chunk 1 length
128	Chunk 1 data		
...	...		
...	Chunk *N* type	Chunk *N* flags	Chunk *N* length
...	Chunk *N* data		

The **Stream Control Transmission Protocol (SCTP)** has a simpler basic packet structure than TCP. Each consists of two basic sections:
1. The common header, which occupies the first 12 bytes. In the adjacent diagram, this header is highlighted in blue.
2. The data chunks, which form the remaining portion of the packet. In the diagram, the first chunk is highlighted in green and the last of N chunks (Chunk N) is highlighted in red. There are several types, including payload data and different control messages.

All SCTP packets require the common header section (shown with a blue background).
Source port This field identifies the sending port.
Destination port This field identifies the receiving port that hosts use to route the packet to the appropriate endpoint/application.
Verification tag
A 32-bit random value created during initialization to distinguish stale packets from a previous connection.
Checksum
SCTP's original design catered for Adler-32; but RFC 3309 changed the protocol to use the CRC32c algorithm.

Unit-5 Application Layer Protocols

Q.1 Explain Application Layer Protocols in detail.

ANS.

- **Application Layer Protocol in Computer Network**

1. TELNET

- Telnet stands for the **Tel**etype **Net**work. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. Port number of telnet is 23.

2. FTP

- FTP stands for File Transfer Protocol. It is the protocol that actually lets us transfer files. It can facilitate this between any two machines using it.

3. TFTP

- The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it.The Port number for TFTP is 69.

4. NFS

- It stands for a Network File System.

5. SMTP

- It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol.

6. LPD

- It stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A "daemon" is a server or agent. The Port number for LPD is 515.

7. X window

- It defines a protocol for the writing of graphical user interface–based client/server applications.

8. SNMP

- It stands for Simple Network Management Protocol. The Port number of SNMP is 161(TCP) and 162(UDP).

9. DNS

- It stands for Domain Name System.

10. DHCP

- It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts.

11. HTTP/HTTPS

- HTTP stands for Hypertext Transfer Protocol and HTTPS is the more secured version of HTTP, that's why HTTPS stands for Hypertext Transfer Protocol Secure.

12. POP

- POP stands for Post Office Protocol and the latest version is known as POP3 (Post Office Protocol version 3). This is a simple protocol used by User agents for message retrieval from mail servers.

13. IRC

- IRC stands for Internet Relay Chat. It is a text-based instant messaging/chatting system. IRC is used for group or one-to-one communication.

14. MIME

- MIME stands for Multipurpose Internet Mail Extension. This protocol is designed to extend the capabilities of the existing Internet email protocol like SMTP

Q.2 Explain FTP in detail.

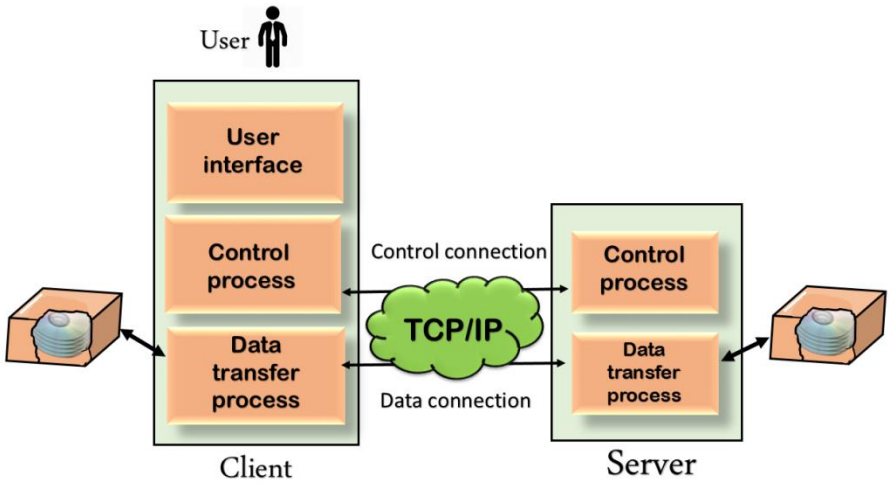
ANS.

- FTP stands for File transfer protocol.
- It is also used for downloading the files to computer from other servers.

Objectives of FTP

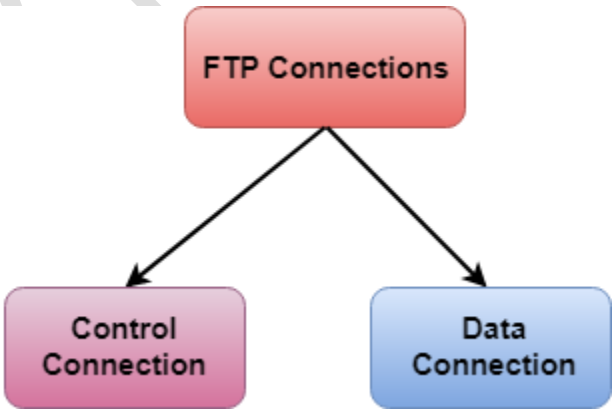
- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Mechanism of FTP



- The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is

made between the control processes. The control connection remains connected during the entire interactive FTP session.

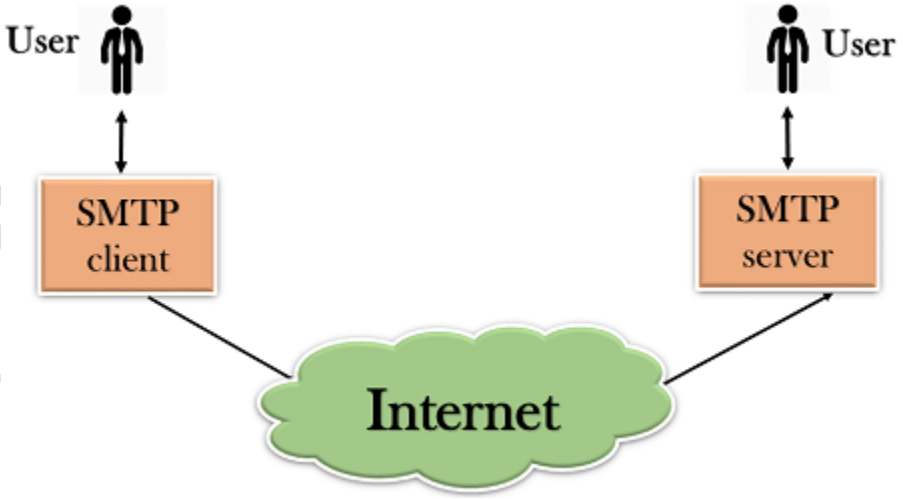
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

Q.3 Explain SMTP in detail.

ANS.

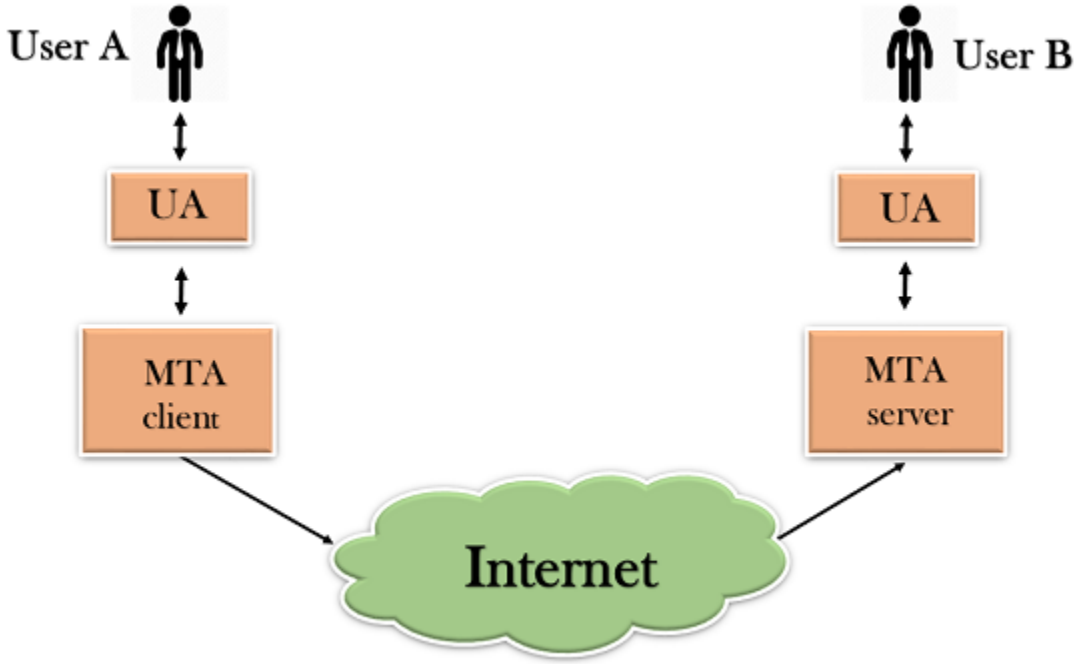
- SMTP stands for **Simple Mail Transfer Protocol.**
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
    - It can send a single message to one or more recipients.
    - Sending message can include text, voice, video or graphics.
    - It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

Components of SMTP

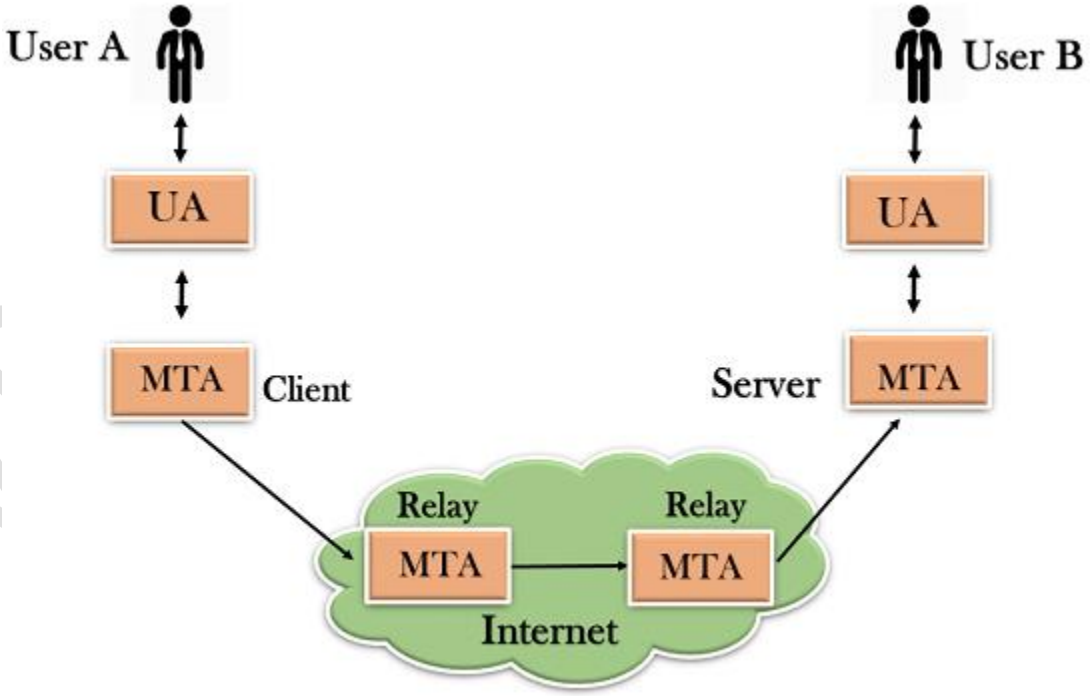


- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and

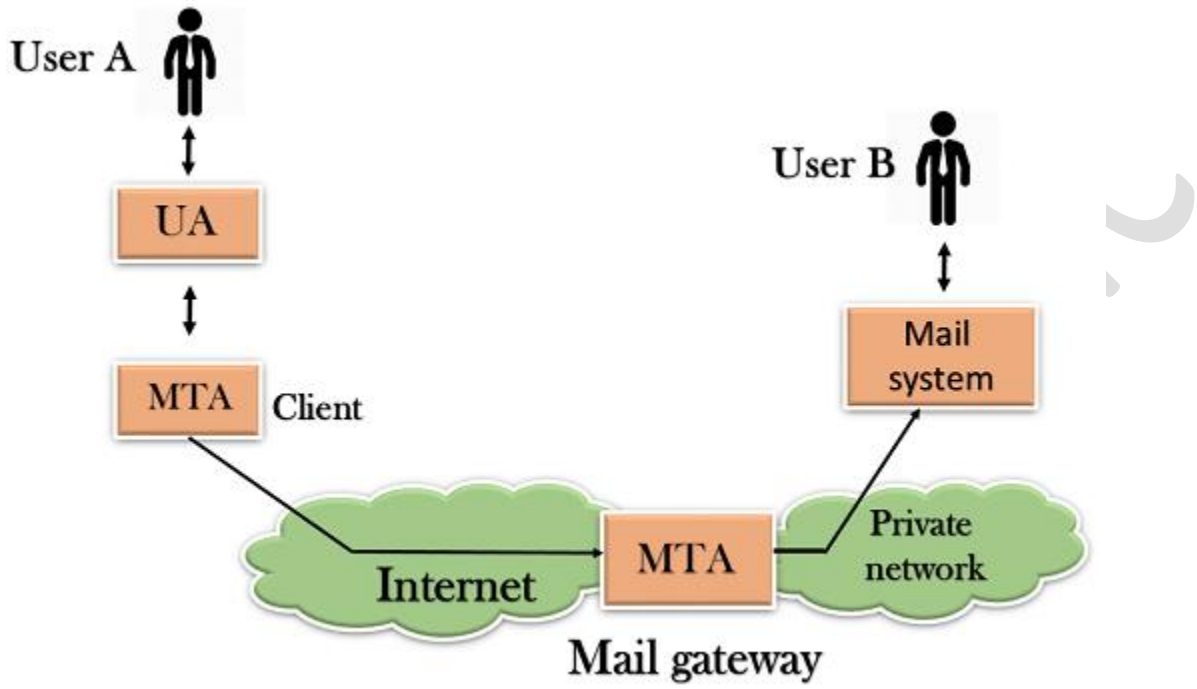
then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.



- SMTP allows a more complex system by adding a relaying system. Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.



- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.



Advantages of SMTP

- If necessary, the users can have a dedicated server.
- It allows for bulk mailing.
- Low cost and wide coverage area.
- Offer choices for email tracking.
- Reliable and prompt email delivery.

Disadvantages of SMTP

- SMTP's common port can be blocked by several firewalls.
- SMTP security is a bigger problem.
- Its simplicity restricts how useful it can be.
- Just 7-bit ASCII characters can be used.
- If a message is longer than a certain length, SMTP servers may reject the entire message.

Q.4Explain MIME in detail.
ANS.

- MIME stands for **Multipurpose Internet Mail Extensions**.
- It is used to extend the capabilities of Internet e-mail protocols such as SMTP.

- The MIME protocol allows the users to exchange various types of digital content such as pictures, audio, video, and various types of documents and files in the e-mail.
- MIME was created in 1991 by a computer scientist named Nathan Borenstein at a company called Bell Communications.

Need of MIME Protocol

MIME protocol is used to transfer e-mail in the computer network for the following reasons:

1. The MIME protocol supports multiple languages in e-mail, such as Hindi, French, Japanese, Chinese, etc.
2. Simple protocols can reject mail that exceeds a certain size, but there is no word limit in MIME.
3. Images, audio, and video cannot be sent using simple e-mail protocols such as SMTP. These require MIME protocol.
4. Many times, emails are designed using code such as HTML and CSS, they are mainly used by companies for marketing their product. This type of code uses MIME to send email created from HTML and CSS.

MIME Header

MIME adds five additional fields to the header portion of the actual e-mail to extend the properties of the simple email protocol. These fields are as follows:

1. MIME Version
2. Content Type
3. Content Type Encoding
4. Content Id
5. Content description

1. MIME Version

It defines the version of the MIME protocol. This header usually has a parameter value 1.0, indicating that the message is formatted using MIME.

2. Content Type

It describes the type and subtype of information to be sent in the message. These messages can be of many types such as Text, Image, Audio, Video, and they also have many subtypes such that the subtype of the image can be png or jpeg. Similarly, the subtype of Video can be WEBM, MP4 etc.

3. Content Type Encoding

In this field, it is told which method has been used to convert mail information into ASCII or Binary number, such as 7-bit encoding, 8-bit encoding, etc.

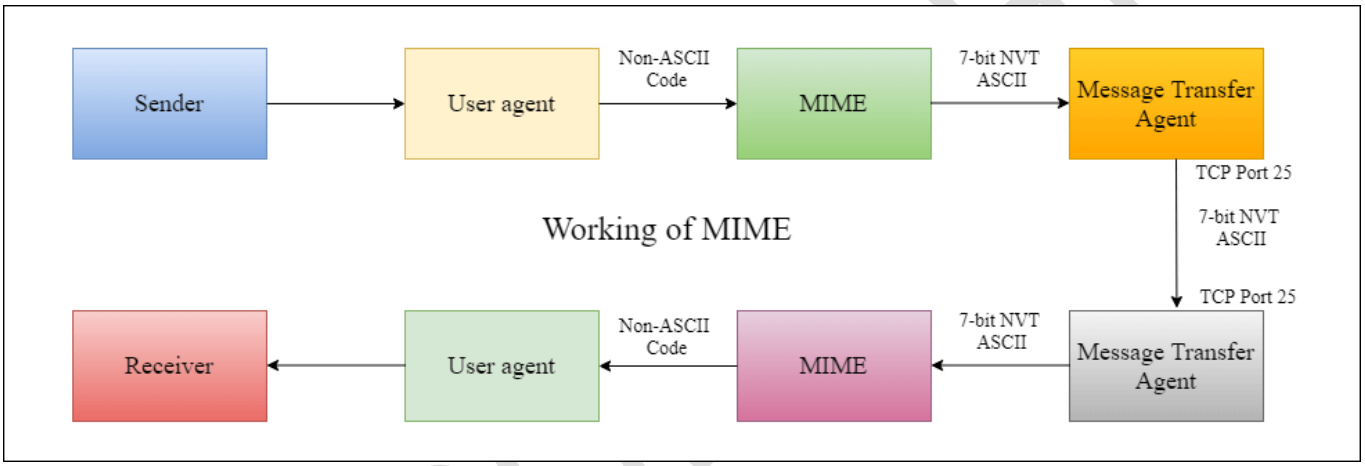
4. Content Id

In this field, a unique "Content Id" number is appended to all email messages so that they can be uniquely identified.

5. Content description

This field contains a brief description of the content within the email. This means that information about whatever is being sent in the mail is clearly in the "Content Description". This field also provides the information of name, creation date, and modification date of the file.

- **Working diagram of MIME Protocol**

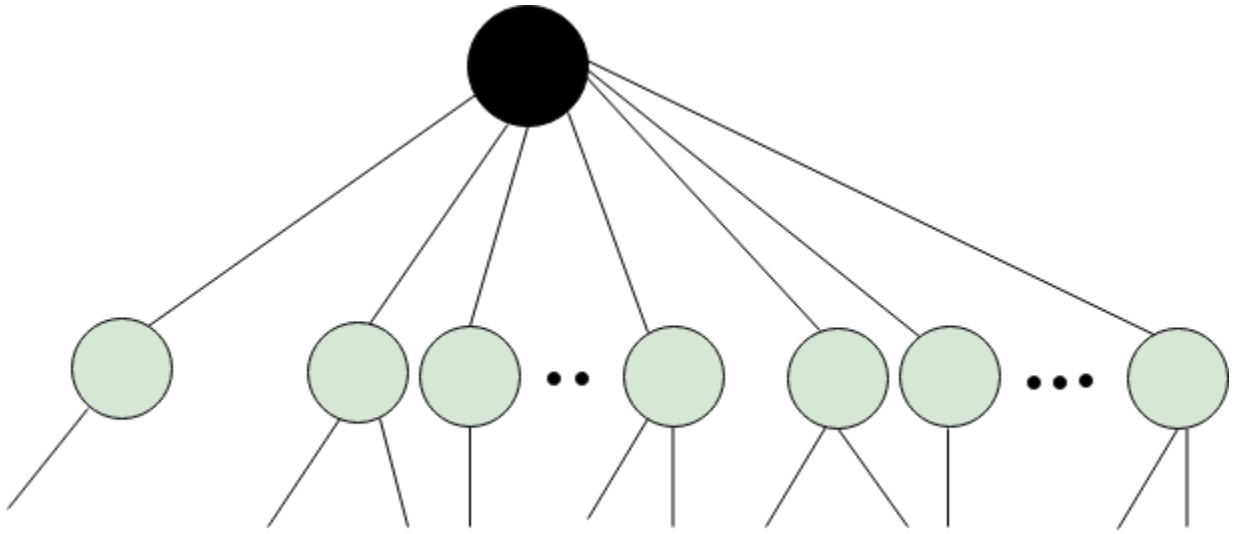


Q.5 Explain Domain Name System with example.

ANS.

- DNS stands for **Domain Name System.**
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.

- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

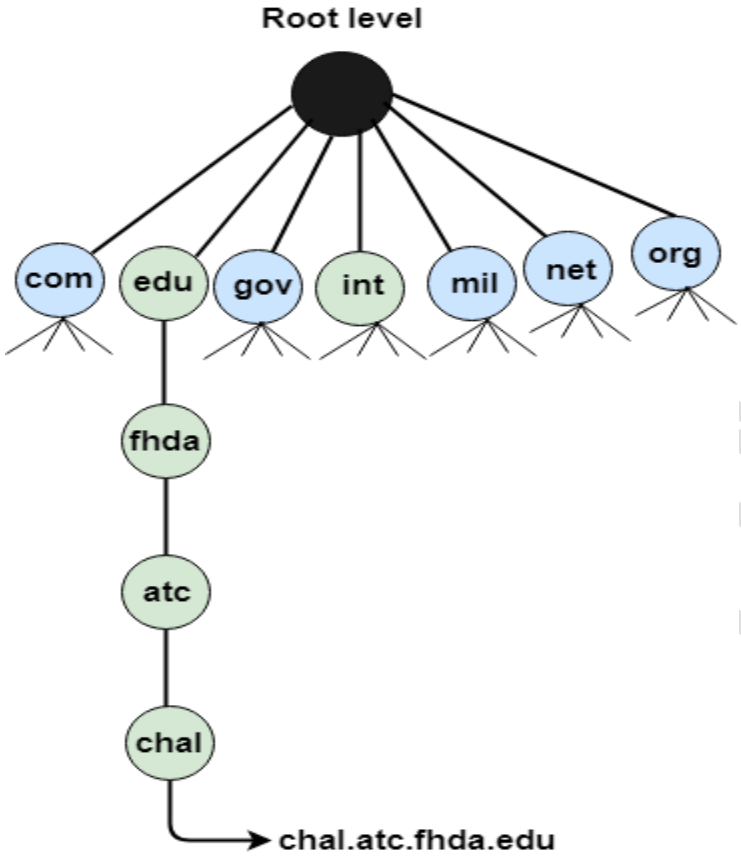


Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions

gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

- The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

- The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.