MID 2 IMP QUESTIONS

UNIt-III

1. **Discuss in detail CSMA, CSMA/CD and CSMA/CA.**

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

CSMA access modes

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent
- **O- Persistent:** It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.

CSMA/CD:

- Collision detection is an analog process.
- The station's hardware must listen to the channel while it is transmitting. If the signal it reads back is different from the signal it is putting out, it knows that a collision is occurring.

HOW CSMA/CD WORKS:

- Check if the sender is ready for transmitting data packets.
- Check if the transmission link is idle?
- Transmit the data & check for collisions
- If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

CSMA/CA:

- In contrast to CSMA/CD (Carrier Sense Multiple Access/Collision Detection) that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their occurrence.

HOW CSMA/CA WORKS:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
- After sending the frame, it sets a timer.
- The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
- Otherwise, it waits for a back-off time period and restarts the algorithm.

2)What is Ethernet? And explain the following in detail

i)Fast ethernet ii) Gigabit ethernet iii) 10 Gigabit ethernet

ETHERNET:

- Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection.
- It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network.
- It offers a simple user interface that helps to connect various devices easily, such as switches, routers, and computers. A local area network (LAN) can be created with the help of a single router and a few Ethernet cables.

i)Fast ethernet:

This type of Ethernet is usually supported by a twisted pair or CAT5 cable, which has the potential to transfer or receive data at around100 Mbps. They function at 100Base and 10/100Base Ethernet on the fiber side of the link if any device such as a camera, laptop, or other is connected to a network. The fiber optic cable and twisted pair cable are used by fast Ethernet to create communication. The 100BASE-TX, 100BASE-FX, and 100BASE-T4 are the three categories of Fast Ethernet.

Its variants are:

1. 100Base-T4
2. 100Base-Tx
3. 100Base-Fx

The coverage limit of Fast Ethernet is up to 10 km and its round-trip delay in Fast Ethernet is 100 to 500 bit times.

ii) Gigabit ethernet

This type of Ethernet network is an upgrade from Fast Ethernet, which uses fiber optic cable and twisted pair cable to create communication. It can transfer data at a rate of 1000 Mbps or 1Gbps. In modern times, gigabit Ethernet is more common. This network type also uses CAT5e or other advanced cables, which can transfer data at a rate of 10 Gbps.

Gigabit Ethernet offers 1 Gbps speed.

coverage limit of Gigabit Ethernet is up to 70 km.

the round-trip delay in Gigabit Ethernet is 4000 bit times.

iii) 10 Gigabit ethernet

This type of network can transmit data at a rate of 10 Gigabit/second, considered a more advanced and high-speed network. It makes use of CAT6a or CAT7 twisted-pair cables and fiber optic cables as well. This network can be expended up to nearly 10,000 meters with the help of using a fiber optic cable.

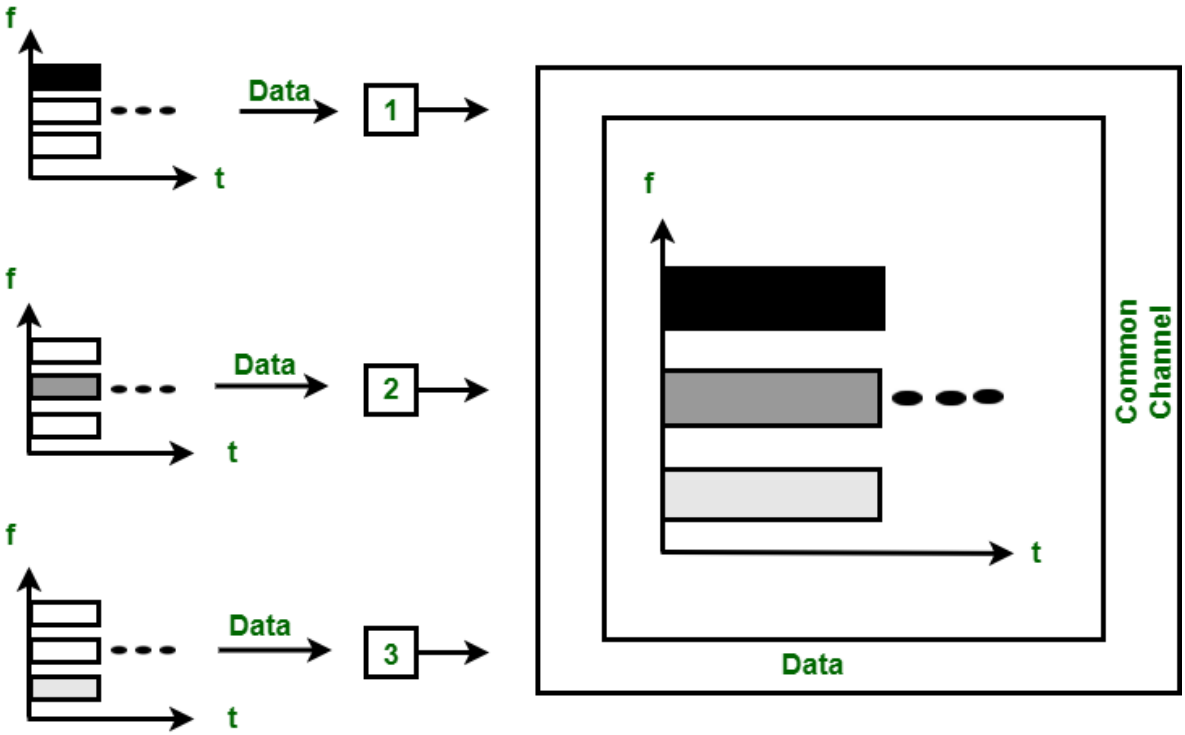
Advantages of 10G Ethernet:

1. Provides reliable superfast speed
2. Prevent data bottlenecks
3. Provides reliable security
4. Expands server capabilities
5. Provides greater scalability

3)Explain about channelization protocols(TDMA, FDMA &CDMA)

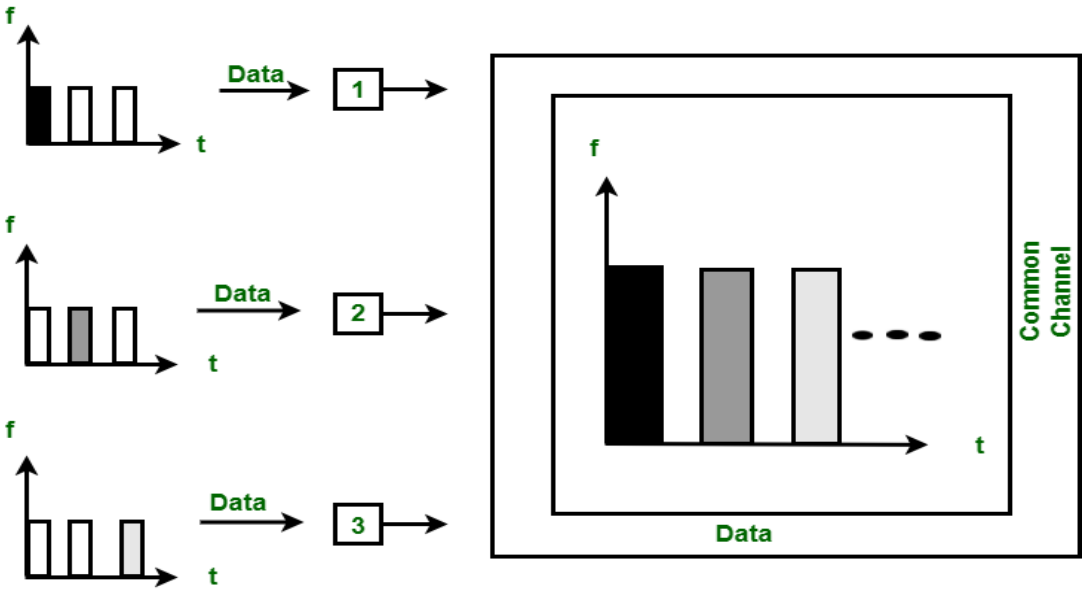
Frequency Division Multiple Access (FDMA) : FDMA is a type of channelization protocol. In this bandwidth is divided into various frequency bands. Each station is allocated with band to send data and that band is reserved for particular station for all the time.

The frequency bands of different stations are separated by small band of unused frequency and that unused frequency bands are called as guard bands that prevents the interference of stations. It is like access method in data link layer in which data link layer at each station tells its physical layer to make a band pass signal from the data passed to it. The signal is created in the allocated band and there is no physical multiplexer at the physical layer



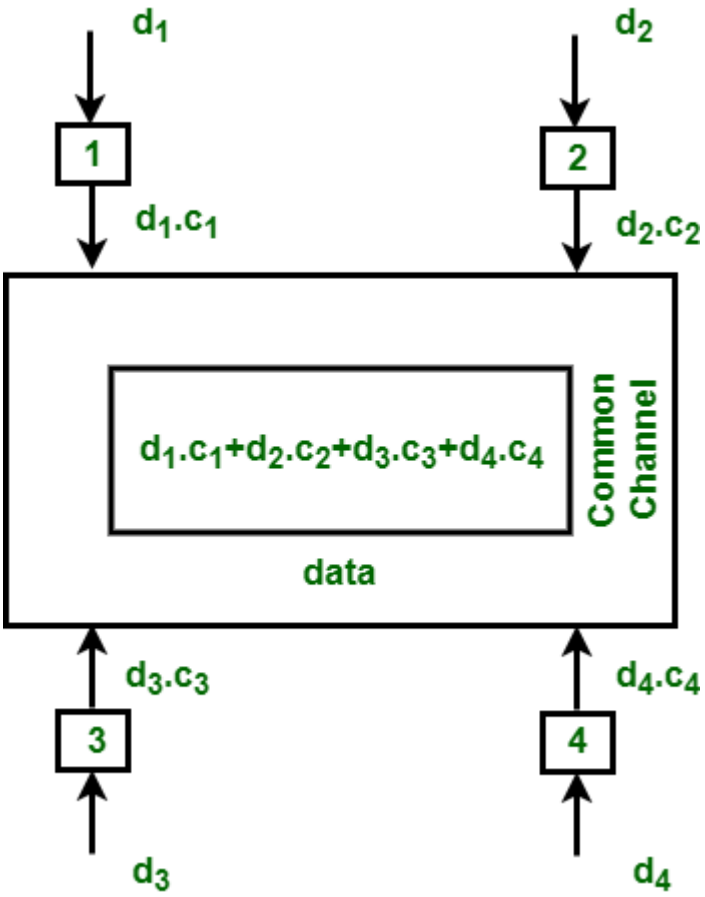
(TDMA) : TDMA is the channelization protocol in which bandwidth of channel is divided into various stations on the time basis. There is a time slot given to each station, the station can transmit data during that time slot only .

Each station must aware of its beginning of time slot and the location of the time slot. TDMA requires synchronization between different stations. It is type of access method in the data link layer. At each station data link layer tells the station to use the allocated time slot.



Code Division Multiple Access (CDMA) : In CDMA, all the stations can transmit data simultaneously. It allows each station to transmit data over the

entire frequency all the time. Multiple simultaneous transmissions are separated by unique code sequence. Each user is assigned with a unique code sequence.



In the above figure, there are 4 stations marked as 1, 2, 3 and 4. Data assigned with respective stations as d_1, d_2, d_3 and d_4 and the code assigned with respective stations as c_1, c_2, c_3 and c_4.

Unit IV

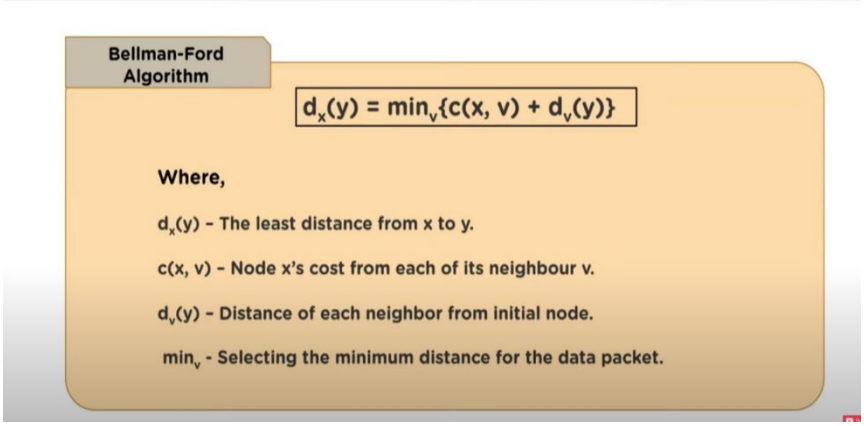
1. **Differentiate Virtual Circuit and Datagram Networks**

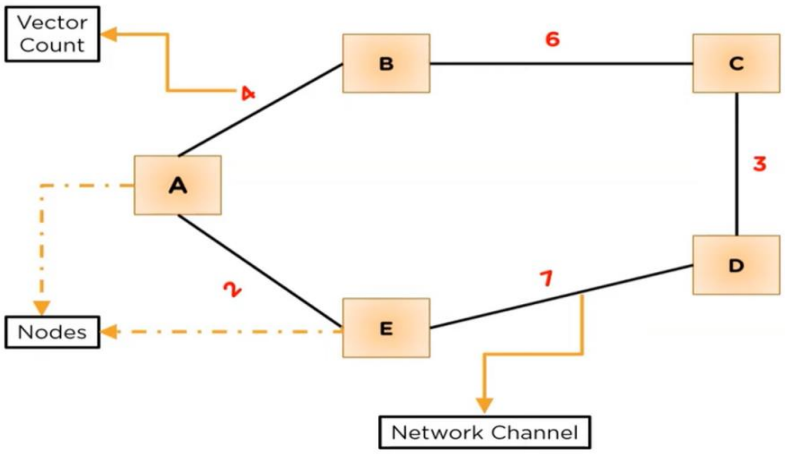
Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

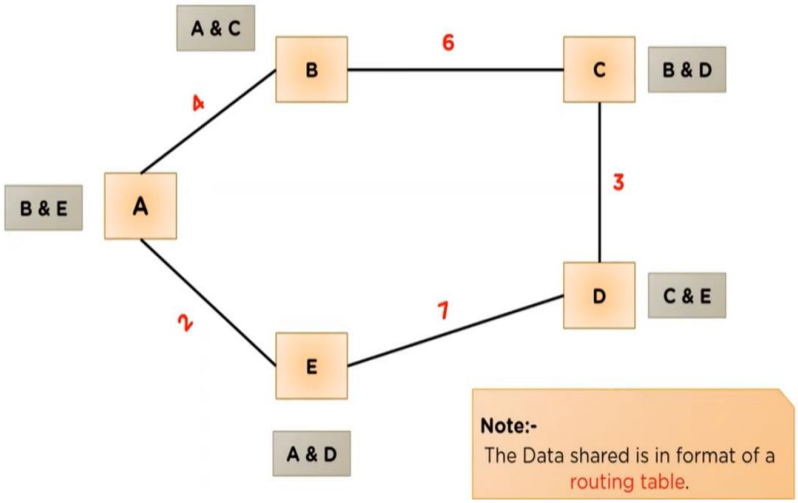
2)Apply Distance Vector Routing protocol to find minimum cost with an example

- Distance vector routing algorithm is also known as **Bellman-Ford routing algorithm.**
- A distance vector routing algorithm operates by having each router maintain a table (i.e., a vector) giving the best known distance to each destination and which link to use to get there. These tables are updated by exchanging information with the neighbors.
- Eventually, every router knows the best link to reach each destination.

EXAMPLE:

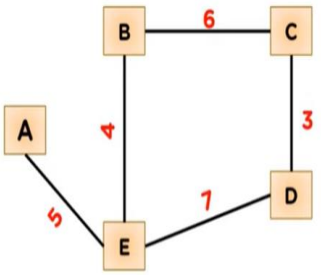






Node A

Destination	Vector	Hop
A	0	A
B	∞	-
C	∞	-
D	∞	-
E	5	E



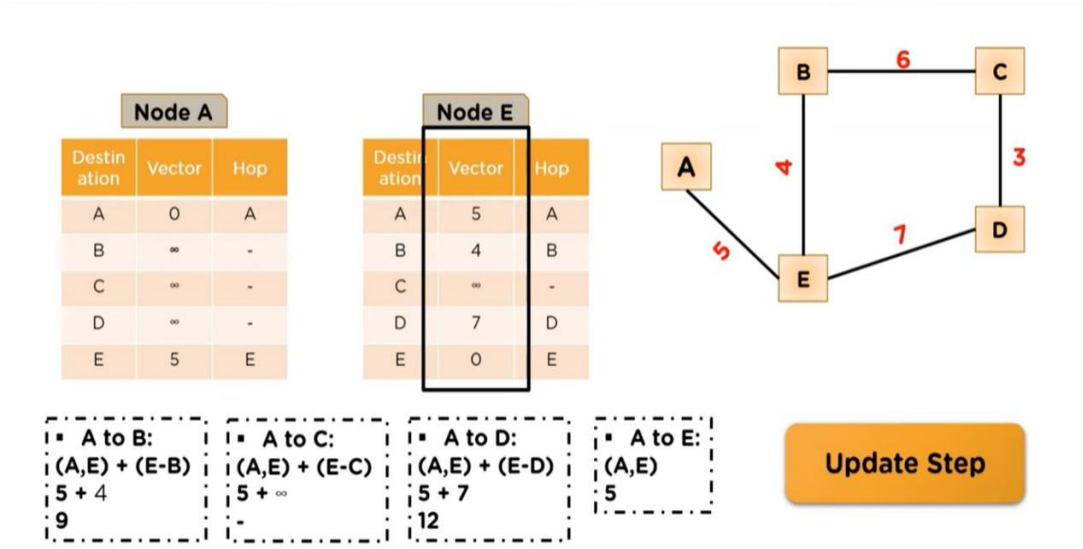
Destination	Vector	Hop
A	∞	-
B	6	B
C	0	C
D	3	D
E	∞	-

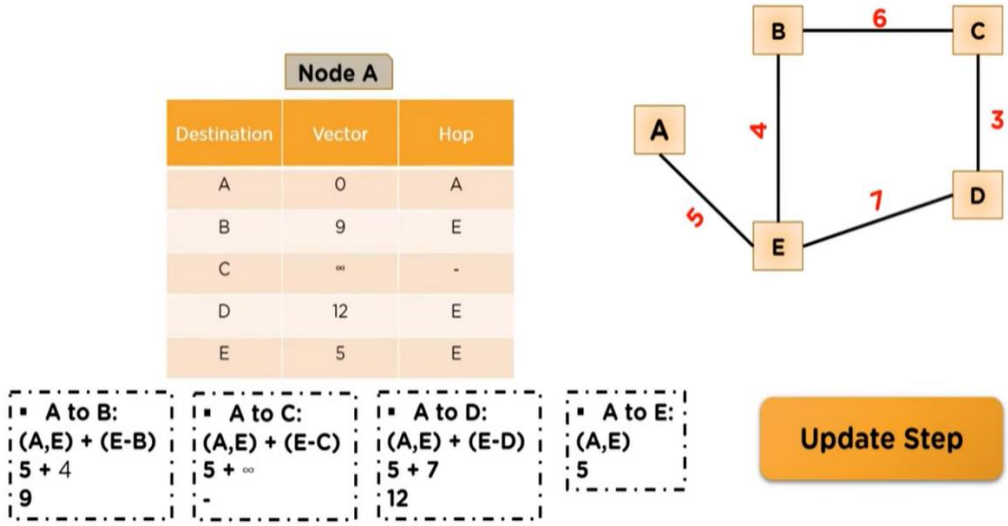
Node C

Destination	Vector	Hop
A	5	A
B	4	B
C	∞	-
D	7	D
E	0	E

Node E

Initial Step





3)Explain about link state and hierarchical routing algorithms

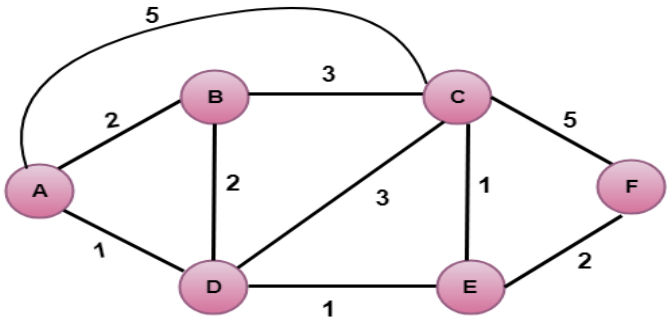
Link State Routing –

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding.
- **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

- **EXAMPLE:**



In the above figure, source vertex is A.

Step 1:

The first step is an initialization step. The currently known least cost path from A to its directly attached neighbors, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞

Step 2:

In the above table, we observe that vertex D contains the least cost path in step 1. Therefore, it is added in N. Now, we need to determine a least-cost path through D vertex.

a) Calculating shortest path from A to B

1. v = B, w = D
2. D(B) = min(D(B) , D(D) + c(D,B))
3. = min(2, 1+2)>
4. = min(2, 3)
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2 .

b) Calculating shortest path from A to C

1. v = C, w = D
2. D(B) = min(D(C) , D(D) + c(D,C))
3. = min(5, 1+3)
4. = min(5, 4)
5. The minimum value is 4. Therefore, the currently shortest path from A to C is 4 .</p>

c) Calculating shortest path from A to E

1. v = E, w = D
2. D(B) = min(D(E) , D(D) + c(D,E))
3. = min(∞, 1+1)
4. = min(∞, 2)
5. The minimum value is 2. Therefore, the currently shortest path from A to E is 2.

So on as we continue the process we get:

Step-2:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞

Step-3:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E

Step-4:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E

Step-5:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E

FINAL STEP:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E
6	ADEBCF					

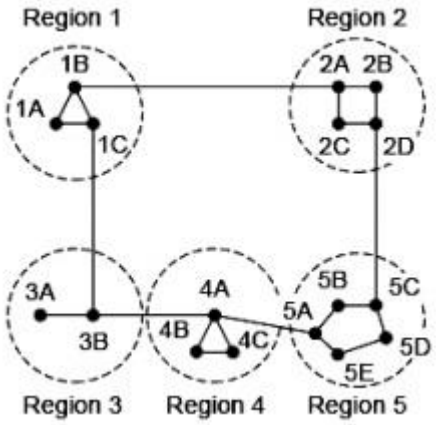
Hierarchical routing algorithm:

In hierarchical routing, the routers are divided into regions. Each router has complete details about how to route packets to destinations within its own region. But it does not have any idea about the internal structure of other regions.

In hierarchical routing, routers are classified in groups called regions. Each router has information about the routers in its own region and it has no information about routers in other regions. So, routers save one record in their table for every other region.

Example

Consider an example of two-level hierarchy with five regions as shown in figure –



Let see the full routing table for router 1A which has 17 entries, as shown below –

Full Table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4

Dest.	Line	Hops
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

. When routing is done hierarchically then there will be only 7 entries as shown below –

Hierarchical Table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Unfortunately, this reduction in table space comes with the increased path length.

4)Define congestion and demonstrate leaky bucket algorithm with neat sketch.

Congestion

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

- Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.

Congestion control algorithms:

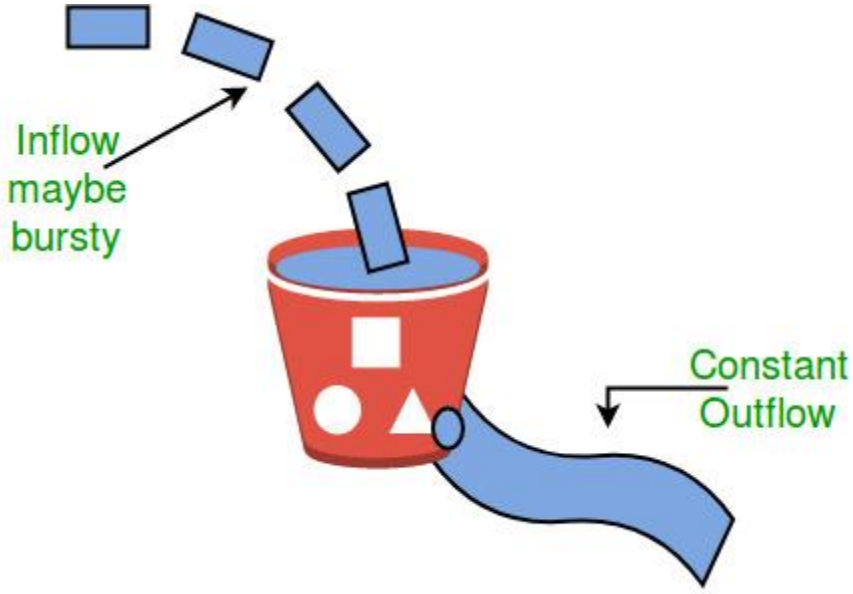
- **Leaky Bucket Algorithm**
- **Token bucket Algorithm**

Leaky Bucket Algorithm

- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
- This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.

The large area of network resources such as bandwidth is not being used effectively.

EXAMPLE:
Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

5)Compare Internet Protocol (IPv4 and IPv6).

IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end to end, connection integrity is Achievable
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided

IPv4 has a header of 20-60 bytes.	IPv6 has header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consist of 4 fields which are separated by dot (.)	IPv6 consist of 8 fields, which are separated by colon (:)
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

6)Explain various messages of ICMP protocol.

The ICMP messages are usually divided into two categories:

- **Error-reporting messages**

The error-reporting message means that the router encounters a problem when it processes an IP packet then it reports a message.

- **Query messages**

The query messages are those messages that help the host to get the specific information of another host. For example, suppose there are a client and a server, and the client wants to know whether the server is live or not, then it sends the ICMP message to the server.

TYPES OF ERROR REPORTING MESSAGES:

Destination un-reachable

This message is generated by the host to inform the client that the destination is unreachable for some reason.

Time exceeded message :

When some fragments are lost in a network then the holding fragment by the router will be droped then ICMP will take source IP from discarded packet and informs to the source.

Parameter problem :

Whenever packets come to the router then calculated header checksum should be equal to received header checksum then only packet is accepted by the router.

Source quench: It is a message request to decrease traffic rate for messages sending to the host(destination).

Redirection message :

Redirect requests data packets be sent on an alternate route.

Echo-request and echo-reply message

A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive".

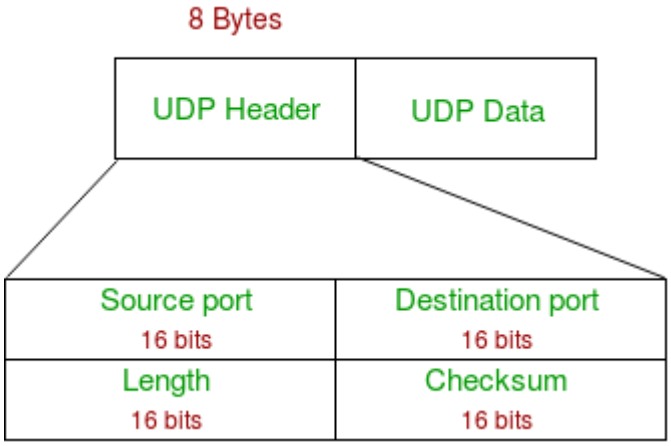
Timestamp-request and timestamp-reply message

The timestamp-request and timestamp-reply messages are also a type of query messages. Suppose the computer A wants to know the time on computer B, so it sends the timestamp-request message to computer B. The computer B responds with a timestamp-reply message.

Router Advertisement-find a nearby router.

Unit V

1. **Discuss User Datagram Protocol (UDP) in Transport layer.**
   User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.**



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.

2)Explain about Transmission Control Protocol (TCP) in Transport layer.

- **TCP (Transmission Control Protocol)** was specifically designed to provide a reliable end-to-end byte stream over an unreliable internetwork.
- TCP was formally defined in RFC 793 in September 1981.
- A port is the TCP name for a TSAP
- All TCP connections are full duplex and point-to-point.
- Full duplex means that traffic can go in both directions at the same time. Point-to-point means that each connection has exactly two end points.

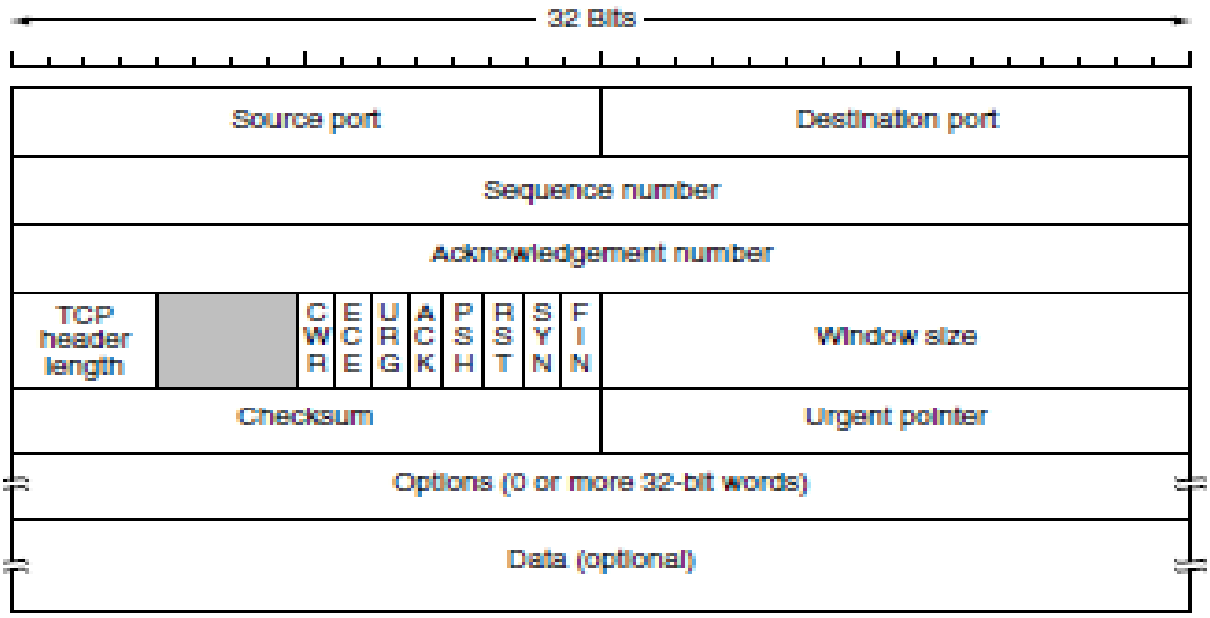
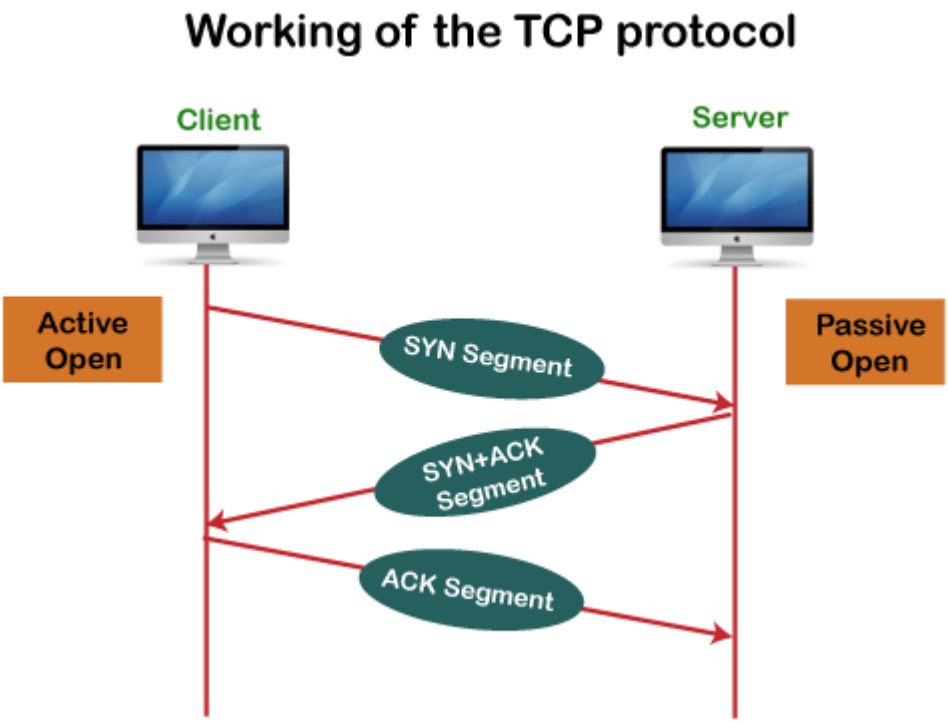


Figure 6-36. The TCP header.

- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.

.



CHARECTERISTICS:

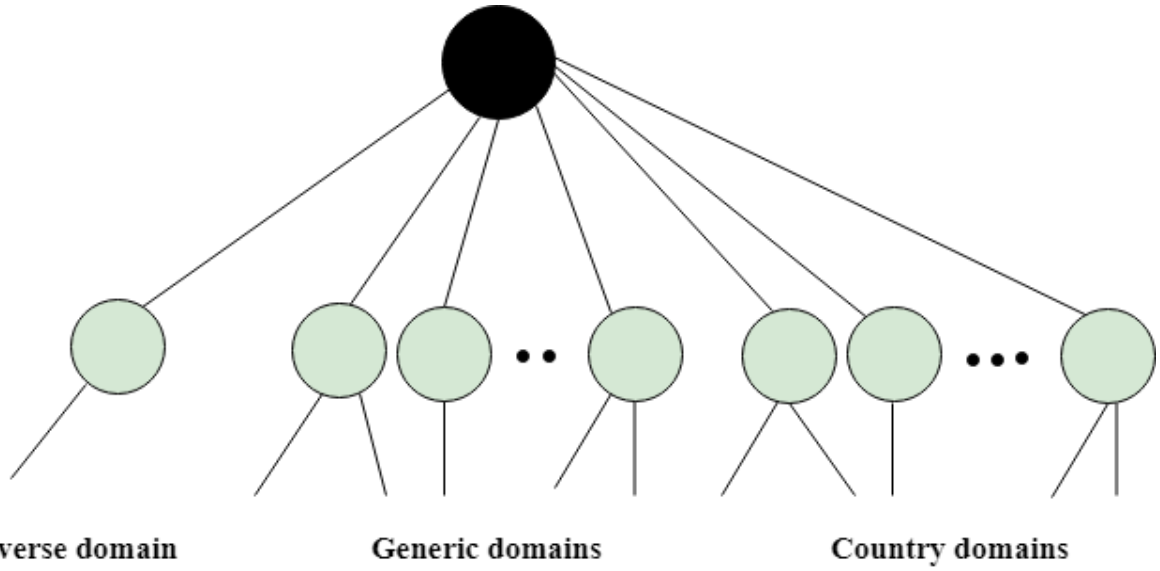
- . **Reliable**
- **Order of the data is maintained**
- **Connection-oriented**
- **Full duplex**
- **Stream-oriented**

3)Write a short note on WWW and DNS.

DNS

- 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.

- DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



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.

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.

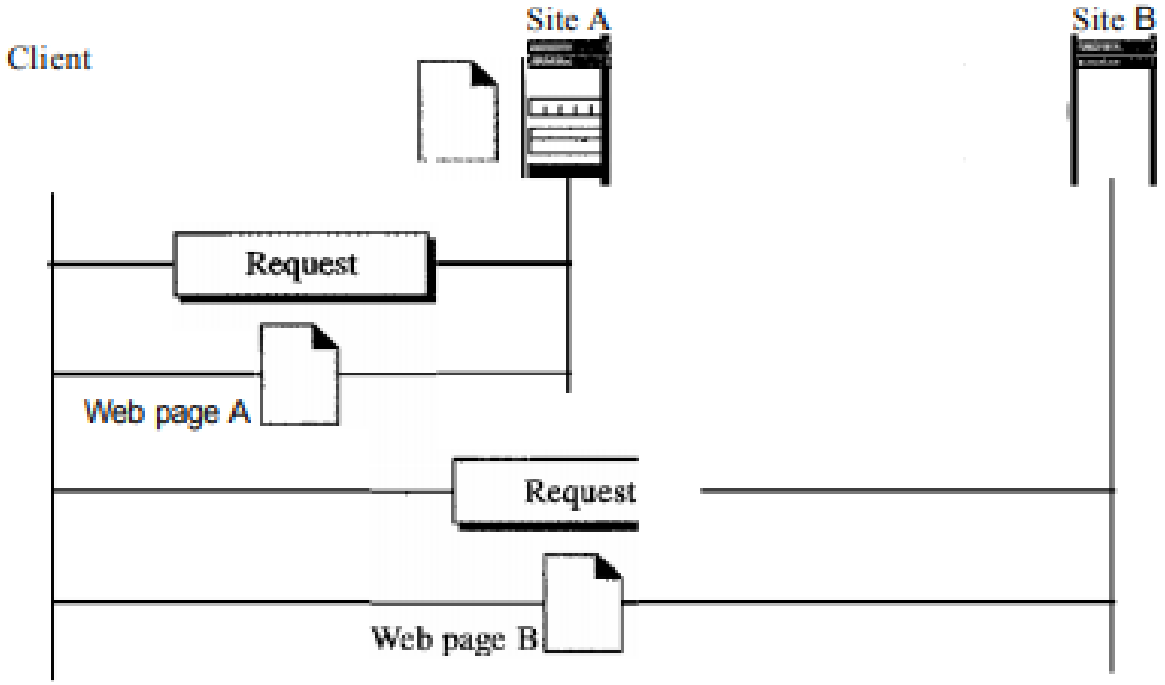
World wide Web:

- The World Wide Web (WWW) is a repository of information linked together from points all over the world.
- The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.

Architecture:

- The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server.
- The service provided is distributed over many locations called sites.

Each site holds one or more documents, referred to as Web pages. Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browsers



4)Explain about HTTP

HTTP:

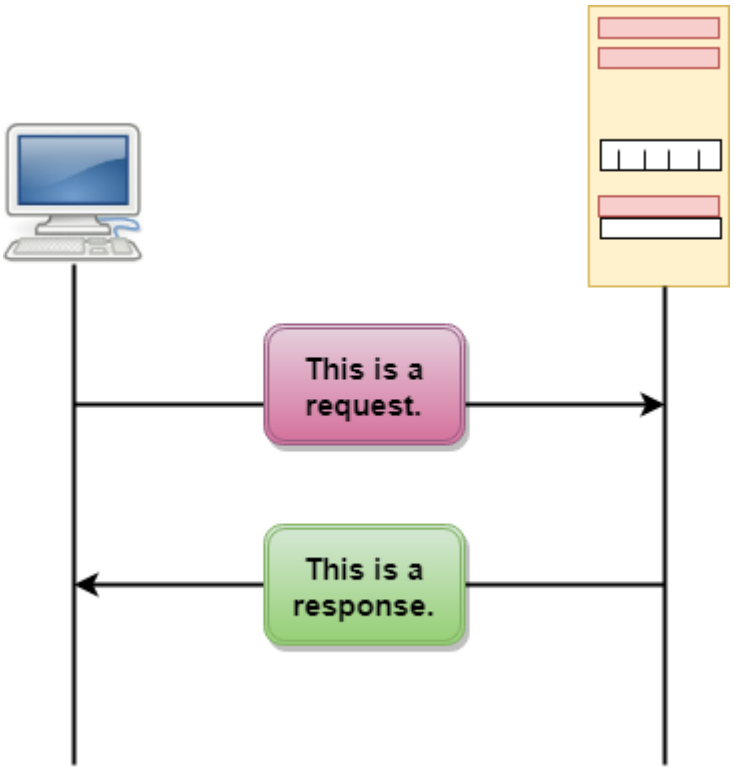
- Hypertext Transfer Protocol (HTTP) is an application-level protocol.
- HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well.
- The most current version of HTTP is 1.1.

Features:

HTTP is connectionless.

HTTP is media independent.

HTTP is stateless



The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

HTTP messages are of two types: request and response. Both the message types follow the same message format.

Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.

Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

HTTP Connections:

Non-persistent connection is known as HTTP 1.0 and Persistent connection is known as HTTP 1.1.

- **Non-Persistent Connection**: It requires connection setup again and again for each object to send.

Persistent connection: It does not require connection setup again and again. Multiple objects can use connection.

5)Discuss in detail about SNMP protocol.

Simple Network Management Protocol:

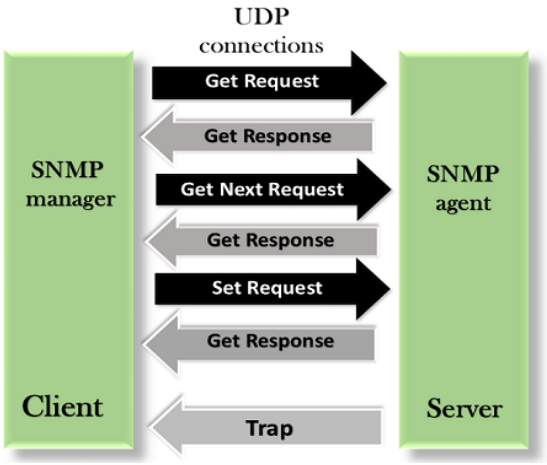
- The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite.
- It provides a set of fundamental operations for monitoring and maintaining an internet.
- A manager, usually a host, controls and monitors a set of agents, usually routers.
- The manager is a host that runs the SNMP client program.
- The agent is a router or host that runs the SNMP server program.

SNMP functions in three ways:

- 1. A manager can retrieve the value of an object defined in an agent.
- 2. A manager can store a value in an object defined in an agent.
- 3. An agent can send an alarm message to the manager.

SNMP defines five types of messages

GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.



GetRequest: The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.

GetNextRequest: The GetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table.

GetResponse: The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.

SetRequest: The SetRequest message is sent from a manager to the agent to set a value in a variable.

Trap: The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

6)Illustrate electronic mail and its architecture.

Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world.

Components of E-Mail System : The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. **User Agent (UA) :** The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.
2. **Message Transfer Agent (MTA) :** MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA.

3. Mailbox : It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement.

4.Spool file : This file contains mails that are to be sent.User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery.

Email Architecture and Services

An e-mail system includes two subsystems as under:

- User agents
- Message transfer agents

User agents

They allow people to read message transfer agents.

They transfer the messages from the source to the destination.

Basic Functions

The E-mail system supports five basic systems, which are as follows:

Composition

The process of generating messages and answering them is called composition. The system can also support assistance with addressing and several header fields attached to each message.

Transfer

It is the process of moving messages from the sender to the recipient. This includes establishing a connection from the sender to a destination or some intermediate machine, outputting the message and releasing the connection.

Reporting

This is to tell the sender whether the message was delivered or rejected, or lost.

Displaying

It is the process of displaying incoming messages. For this purpose, simple conversation and formatting are required to be done.

Disposition

This is concerned with what the recipient does with the messages after receiving them. Some of the possibilities are as follows –

- Throw after reading
- Throw before reading
- Save messages
- Forward messages
- Process messages in some other way