Fifth Semester B.E. Degree Examination, CBCS - Dec 2017 / Jan 2018

Computer Networks

Time: 3 hrs. **Max. Marks: 80**

Note : *Answer any FIVE full questions, selecting ONE full question from each module.*

Module - 1

1. a. Compare client server and Perl-to-Peer architecture. **(05 Marks)**

Ans. In client server architecture, there is always on host called server, it services requests from many other hosts called clients. Ex : Web server server a find well known address called IP address.

In P2P architecture, there is minimal reliance on dedicated servers in data centers. The application exploits direct communication between pairs of intermittently connected hosts called peers. Because the peers communicate without passing through a dedicated server communicate without passing through a dedicated server the architecture is called peer to peer. Ex : Bit-torrent one of the feature of P2P is self - scalability.

In client server architecture, a data center housing a large no. of hosts, in often used to create a visual server.

b. Describe HTTP with persistent and non-persistent connections. **(08 Marks)**

Ans. All of the requests and their corresponding responses to be sent over same TCP connection is called HTTP persistent connection. If the requests are sent separate over TCP requests are called HTTP non-persistent connection.

With persistent connections, the server leaves the TCP connection open after sending a response subsequent requests and responses between the same client and server can be sent over the same connection. It uses pipelining concept. The HTTP server closes the connection when it is not used for a certain time.

For non-persistent : Refer Q.No. 2.a. of MQP - 2.

c. What are the services provided by DNS? **(03 Marks)**

Ans. Domain name system (DNS) translates hostname to IP address.

Refer Q.no 1(b) of MQP 2

OR

2. a. Demonstrate socket implementation using TCP. **(08 Marks)**

Ans. Three way handshake protocol is implemented in TCP. While the server process is running, the client can initiate a TCP connection to the server.

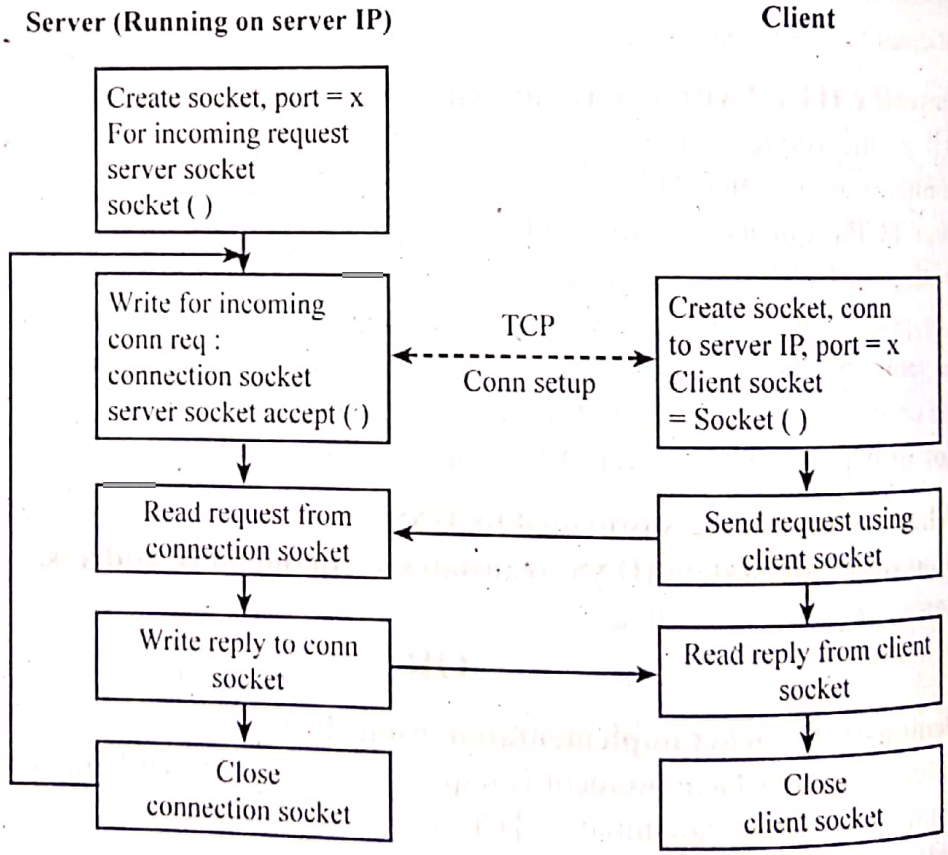
Below is the code for client side of application

```
from socket import *
ServerName = 'Servername'
Serverpost = 12000
ClientSocket = Socket (AF_INET, SOCK_STREAM)
```

```
ClientSocket.Connect((ServerName, ServerPost))
Sentence = raw_input('Input lowercase sentence:')
ClientSocket.send(Senctence)
modifiedSentence = ClientSocket.recv(1024)
Print 'From Server:' , modifiedSentence
ClientSocket.Close ( )
```

Below is the code for server side of application

```
from Socket import *
ServerPort = 12000
ServerSocket = Socket (AF_INET,SOCK_STREAM)
ServerSocket.bind ('',ServerPost)
ServerSocket .listen(1)
print 'The server is ready to receive'
While 1 :
ConnectionSocket,addr = ServerSocket.accept ( );
Sentence = ConnectionSocket recv(1024)
Capitialized Sentence = Sentence.upper ( )
Connection Socket Send (CapitalizedSentence)
ConnectionSocket.Close ( )
```



b. Write a note on web caching. **(04 Marks)**

Ans. Web cache is also called Proxy server satisfies request on behalf of original web server. Ex : Suppose a browser is requesting the object http : //www.SomeSchool.edu/Campus.gif

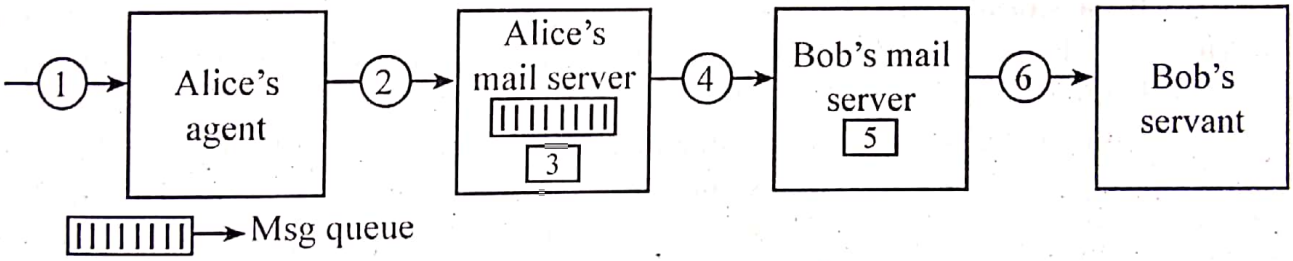
Below shows the steps of occurance

1. The browser establishes a TCP connection to the web cache and sends an HTTP request for the object to the web cache.
2. The web cache checks to see if it has a copy of the object stored locally. If it does, the web cache returns the object within an HTTP response message to the client browser.
3. If the web cache does not have the object, the web cache opens a TCP connection to the origin server i.e., www.someschool.edu. The web cache then sends an HTTP req for the object into the cache - to - server TCP connection. After receiving this request, the origin server sends the object within an HTTP response to the web cache.
4. When the web cache receives the object, it stores a copy in its local storage and sends a copy , within an HTTP response message , to the client browser.

c. Illustrate the basic operation of SMTP with an example. (04 Marks)

Ans. SMTP transfer messages from sender's mail server to the reception mail servers. Below ex illustrates the basic of SMTP suppose Alice wants to send a Bob a simple ASCII mesg

1. Alice invokes her user agent for e-mail provides Bob's e-mail address (en bob@ someschool.edu) composes a msg and instructs the user agent to send the msg.
2. Alice's user agent sends the msg to mail server, whose it is placed in a msg Queue
3. Client side of SMTP, running on Alice's mail server, sees the msg in msg Queue. It opens a TCP connection to an SMTP server, running on Bob's mail server.
4. After some initial SMTP handshaking , SMTP client sends Alice msg into TCP connection.
5. At Bob's mail server, server side of SMTP receives msg. Bob's mail server then places msg in Bob's mailbox.
6. Bob invokes his user agent to read the msg at his convenience.



Module-2

3. a. Elaborate the three way handshaking in TCP. (05 Marks)

Ans. TCP is connection oriented, because the two processes must first "handshake" with each other. The client application process first inform the client transport layer that it wants to establish TCP connection to a process in server.

Socket ClientSocket = new Socket ("host name", postNumber);

where hostname is the name of the server. Transport layer in the client then proceeds to establish TCP connection with TCP in the server. The server responds with a second special TCP segment and finally client responds again with a third segment. The first two segment carry no payload, third of these segment may carry payload. Because three segments are sent between two hosts , the connection establishment

procedure is called three way handshake. Once a TCP connection is established, the two application processes can send data to each other.

b. Discuss Go-Back N protocol. (06 Marks)

Ans. Refer Q.No. 3.a. of MQP - 3

c. Explain the connection-oriented multiplexing and de-multiplexing. (05 Marks)

Ans. Refer Q.No. 3.a. of MQP - 1

OR

4. a. State congestion and discuss the cause of congestion. (04 Marks)

Ans. Network congestion is too-many sources attempting to send data at too high rate. The causes of congestion are two senders, a router with infinite buffer, two senders and a router with finite buffers, four senders routers with finite buffers and multi hop paths. Congestion control techniques are available bit rate (ABR) service in asynchronous transfer mode (ATM). It also has per - connection throughput, offered load. Large queuing delays are experienced as the packet arrival rate nears the link capacity. Delays may cause a router to use its link capacity. Delays may cause a router to use its link bandwidth to forwarded unneeded copin of a packet.

b. With a neat diagram, explain the TCP segment structure. (08 Marks)

Ans. Refer Q.No. 3.a. of MQP - 2

c. Suppose that two measured sample RTT values are 106 ms and 120 ms. Compute:

i) Estimated RTT after each of these sample RTT value is obtained. Assume a = 0.125 and estimated RTT is 100 msec just before first of the samples obtained.

ii) Compute DevRTT. Assume p = 0.25 and DevRTT was 5 msec before first of these samples are obtained. (04 Marks)

Ans. i) TCP updates estimated RTT acc to the foll formula sample value is 106 ms.

EstimatedRTT = $(1 - \alpha)$. Estimated RTT + α. Sample RTT

EstimatedRTT = 0.875. Estimated RTT + 0.125. SampleRTT

= $0.875 \times 100 \times 10^3 + 0.125 \cdot 106(10^3)$

= 193.500.125 = 193 ms

Sampled value is 120 ms

Estimated RTT = $0.875 \times 100 \times 10^3 + 0.125 \times 120 \times 10^3$

= 2,07,500 = 2.07 m/sec

ii. DevRTT = $(1 - \beta)$. DevRTT + B./Sample RTT . Estimated RTT)

= $(1 - 0.25)$ .5 $\times 10^3 + 0.25 / 106 \times 10^3 - 193 \times 10^3)$

Module-3

5. a. Write the link-state routing algorithm. Solve the following graph using link-state algorithm with source node 'u'. Fig.Q5(a) (08 Marks)

Ans. Algorithm of link state routing is shown as below

1. Initialization
2. $N^1 = \{u\}$

3. For all nodes V
4. If v is a neighbour of u
5. then S(v) = c(u,v)
6. else D(v) = ∞
7. .
8. Loop
9. Find w not in N^1 such that D(w) is minimum
10. add W to N^1
11. Update D(v) for each neighbour v of W and not in N^1 =
12. D(v) = min(D(v), D(w) + C(w,v))
13. /* new cost to v is either old cost to v or known
14. path cost to W plus cost from W to v*/
15. Until N^1 = N

Running the also on the network in the fig.

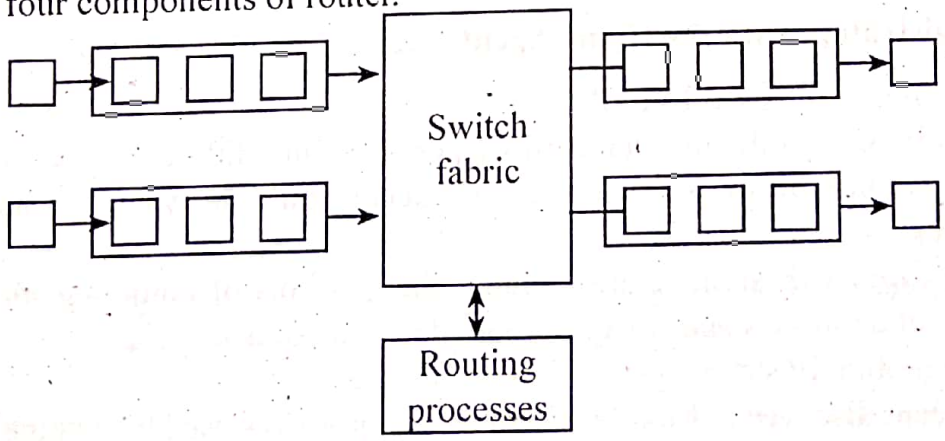
Step	N^1	D(v), p(v)	D(W), p(W)	D(x), p(s)	D(y), p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	u x	2,u	4,x		2,x	∞
2	u x y	2,u	3,y			4,y
3	u x yv					4,y
4	u x yvw					4,y
5	u x yvwz					4,y

1. In the initialization step, currently known least cost paths from u to its directly attached neighbours v,x & w are initialized to 2,1 & 5 respectively. The costs to y & z are set to infinity became they are not directly connected to u.
2. In the second iteration, nodes v & y are found to have the least cost path (2) & we break the tie arbitrarily and add y to the set N^1 now contains u,x & y. The costs to the remaining nodes not yet in N^1 i.e., nodes v,w and z are updated via line 12 of the LS also, yielding the results shown in the third row.

b. What is routing? Explain the structure of a router. **(08 Marks)**

Ans. Router is a networking device that forwards data packets between computer networks.

There are four components of router.



1. Input ports : It performs physical layer functions of terminating an incoming physical link to a router. It perform the data link layer functions needed to interoperate with the data link layer functions at the remote side of the link. Multiple ports are gathered together on a single line card within a router.

2. Switching fabric connects the router's input ports to its output ports. Switching fabric is contained within the router - a network inside of a network router.

3. Output ports : An output port stores the packets that have been forwarded to it through the switching fabric and then transmits the packets on the outgoing link. The output port performs the reverse data link and physical layer functionality of the input port.

4. Routing processor - Executes the routing protocols maintains the routing info and forwarding tables and performs network management functions, within the router.

OR

6. a. Discuss the IPV6 packet format. (05 Marks)

Ans. Refer Q.No. 5.b. of MQP - 3

b. Elaborate the path attributes in BGP and steps to select the BGP routes. (05 Marks)

Ans. Refer Q.No. 6.b. of MQP - 1

c. List the broadcast routing algorithms. Explain any one of them. (06 Marks)

Ans. The broadcast routing algorithms are

1. Uncontrolled flooding
2. Controlled flooding
3. Spanning tree broadcast

For spanning tree broadcast routing also explanation refer 6(B) MQP 3.

Module - 4

7. a. Show the components of GSM 2G cellular network architecture with a diagram. (07 Marks)

Ans. Refer Q.No. 7.b. of MQP - 2

b. Illustrate the steps involved in mobile IP registration with home agent. (05 Marks)

Ans. Registration with the Home Agent : Refer Q.No. 8.a. of MQP - 1

c. Write a note on mobile IP. (04 Marks)

Ans. Mobile IP, is a flexible standard supporting many different modes of operation. Ex: Operation with or without a foreign agent, multiple ways for agents and mobile nodes.

The mobile IP architecture includes the concepts of home agents, foreign agents, case of addresses and encapsulation/ decapsulation.

The mobile IP std consists of three main pieces.

i. Agent discovery - Mobile IP defines the protocols used by a home or foreign agent to advertise its services to mobile nodes and protocols for mobile nodes to solicit the services of a foreign or home agent.

ii. Regitration with home agen - Mobile IP defines the protocols used by the mobile node and / or foreign agent to register and deregister COA with a mobile node's home agent.

iii. Indirect routing of datagrams - The std also defines the manner in which datagrams are forwarded to mobile nodes by a home agent, including rules for forwarding datagram, rules for handling error conditions.

OR

8. a. Define Handoff. Explain the steps accomplishing a handoff. (07 Marks)

Ans. Refer Q.No. 7.a. of MQP - 3

b. Bring out the mechanism of direct routing to mobile node in mobility management. (06 Marks)

Ans. Refer Q.No. 8.b. of MQP - 1

c. Compare the 4G LTE standard to 3G systems. (03 Marks)

Ans. 4G means long term evolution (LE) and is the dominant framework of cellular system.

3G cellular systems are required to provide telephone service as well as data communications at significantly higher speed than their 2G counterparts.

These are two major stds in 3G UMTS (universal mobile telecommunication service and CDMA 2000.

In 4G, in heterogenous environment access technology is switched from one to another automatically and transparently.

Module-5

9. a. Elaborate the features of streaming stored video. (03 Marks)

Ans. Refer Q.No. 10.b. of MQP - 2

b. With a neat diagram, explain the CDN operation. (08 Marks)

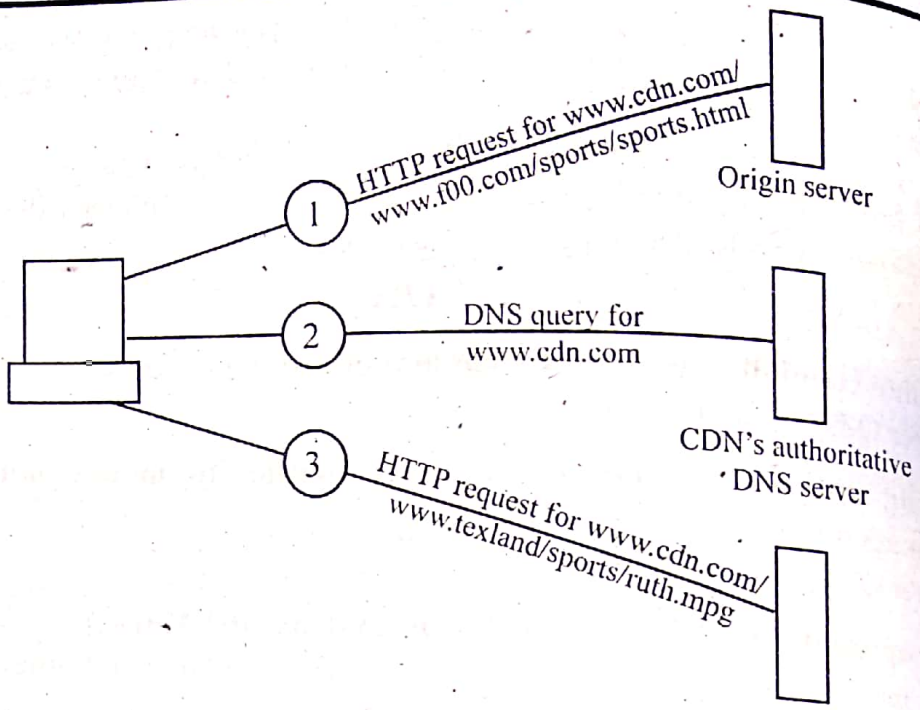
Ans. If the client can't come to the content, the content should be brought to the client. The CDN company typically places the CDN servers in data center. The CDN replicates its customers content in the CDM server. CDN pushes content provider's tagged object to its CDN servers.

When a browser requests a web page containing the image ruth. mpg following actions occur.

1. The browser sends its request for the base HTML object to the origin server, www.foo.com which sends the requested HTML objects to the browser. The browser parses the HTML file and finds reference to
http : //www.cdn.com/www.too.com/sports/ruth.mpg.

2. Browser then does a DNS lookup on www.cdn.com which is the host name for referenced URL. When the authoriative DNS server receives the query, it extracts the IP address of requesting browser.

3. DNS in the requesting client receives a DNS reply with IP address. The browser then sends its HTTP request to the CDN server with that IP address.



c. Summarize the limitations of Best-effort IP service. (05 Marks)

Ans. The limitations are

1. Packet loss - The UDP segment in encapsulated in an IP datagram. As the datagra wanders through the network, it passes through buffers in the routers in order t access outbound links. In this case, the IP datagram is discarded never to arrive the receiving application.
2. End to end delay is the accumulation of transmission, processing and queuin delay in routers, propagation delays in links and system processing delays. Thu packets that are delayed by more than the threshold are effectively lost.
3. Packet jitter - End to End delay is the random queuing delays in the routers. Th time from when a packet is generated at the source until it is received at the receive can fluctuate from packet to packet. This phenomenon is called jitter. Jitter can b removed by using sequence nos, timestamps and a payout delay.

OR

10. a. Explain the diffserv internet architecture.

Ans. Refer Q.No. 10.b. of MQP - 3 **(05 Mark**

b. Describe the leaky bucket policing mechanism.

Ans. Refer Q.No. 10.a. of MQP - 1 **(06 Mark**

c. Discuss the round-robin and waited fair queuing scheduling mechanism.

Ans. Refer Q.No. 9.b. of MQP - 2 **(05 Mark**

Fifth Semester B.E. Degree Examination, CBCS - June/July 2018

Computer Networks

Time: 3 hrs. **Max. Marks: 80**

Note : *Answer any FIVE full questions, selecting ONE full question from each module.*

Module - 1

1. a. **What are the different types of transport services provided by internet.** **(08 Marks)**

Ans. Refer Q.no.1(b) of MQP - I.

b. **Compose logical note on proxy - server with suitable diagram.** **(08 Marks)**

Ans. Refer Q.no.2(b) of Dec 17/ Jan 18.

OR

2. a. **Discuss how files are distributed in peer-peer application**

Ans. Let us consider a simple quantiative model for distributing a file to a fixed set of peers. The upload rate of the server's access in denoted by u_s, upload rate of ith link by u and download rate of ith peer access links by di. the size of the file to be distributed is F bits and no. of peers that want to obtain a copy of the file by N. Distribution time is the time it takes a copy of file to all N peers.

Following observations are made

i. At the beginning of file distribution, only the server has the file. To get this file into the community of peers, the server send each bit of the file atleast once access link. Minimum distribution time is atleast F/us.

ii. The peer with the lowest download rate cannot obtain all F bits of the file in less F/d_{min} seconds. Thus, minimum distribution is atleast F/d_{min}.

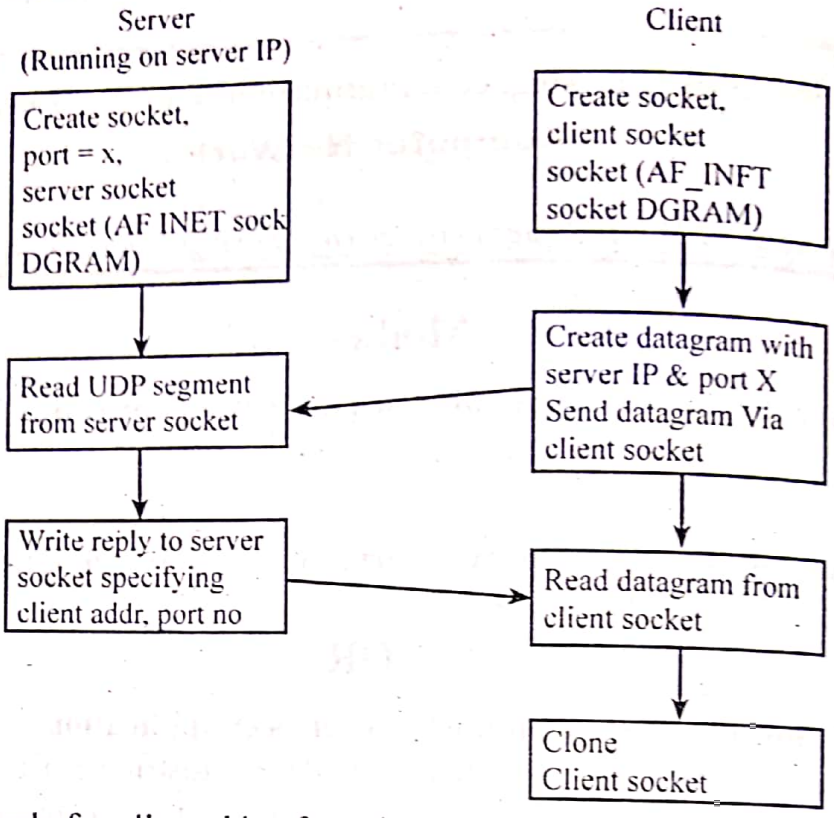
iii. The total upload capacity of the system as a whole is equal to the upload rate of server plus upload rates of each of the individual peers i.e., $u_{total} = u_s + u_1 + ... + u_N$. System must deliver (upload) F bits to each of the N peers, thus delivering a total of NF bits. This cannot be done at a rate faster than u_{total}. Thus, min distribution is also at least $NF/ (u_s + u_1 + ... + u_N)$

The minimum distribution time for P2P, denoted by D_{P2P}.

$$D_{P2P} \geq \max\left\{\frac{F}{u_s}, \frac{F}{d_{min}}, \frac{NF}{u_s + \sum_{i=1}^{N} u_i}\right.$$

b. **Design network application using socket programming with UDP.** **(08 Marks)**

Ans. When a socket is created, an identifier called port number is assigned.



Below is the code for client side of application

```
from socket import *;
ServerName = 'hostname'
Server Port = 12000
ClientSocket = Socket(Socket, AF_INET,Socket, SOCK_DGRAM)
message = raw _input (Input lowercase sentence:')
ClientSocket.Sendto (message(ServerName, Serverport))
modified message, Server Address=ClientSocket. recvfrom (2048)
print modified message
ClientSocket. Close( )
```

Here is the code for server side of application

```
from Socket import *
Serverport = 12000
ServerSocket = Socket (AF_INET, SOCK_DGRAM)
ServerSocket bind(' ',ServerPort)
print " The server is ready to receive"
While 1 :
message, ClientAddress = ServerSocket, recv from (2048)
modifie Message = message. upper( )
ServerSocket, Sendto (modifiedMessage,ClientAddress)
ClientSocket = Socket(Socket.AF_INFT,Socket.Sock_DGRAM)
```

This line creates the clients socket called clientsocket. First parameter indicates address family. AF_INFT indicates underlying network in IPv4.Second parameter indicates socket is of type

SOCK_DGRAM meaning it is a UDP socket raw_input( ) is a built in function in

python. When this command is executed, user at the client is prompted with words " Input data".

Module - 2

3. a. Describe the various fields of UDP segment. Explain how checksum is calculated. (08 Marks)

Ans. UDP segment structure is defined in RFC 768.

Source port #	Dest port #
Length	Checksum
Application data (message)	

Application data occupies the data field of UDP segment. Ex DNS data field contains either a query or response message. UDP header has four fields, each consisting of two bytes. The port # header has four fields, each consisting of two bytes. The port # allows the destination to the application data to the correct process running on the destination end system. Checksum is used by the receiving host to check whether errors have been introduced into the segment.

UDP Checksum :

UDP checksum provides error detection. Checksum is used to determine whether bits within the UDP segment have been altered as it moved from source to destination. UDP at the sender side performs 1's complement of the sum of all 16 bit words in segment, with anyoverflow encounter the sum being wrapped around.

Ex : Suppose following three 16 bit words are there

0110011001100000
0101010101010101
1000111100001100

Sum of the first two of these 16 bit words is

0110011001100000
0101010101010101
1011101110110101

Adding the third word to the above sum gives

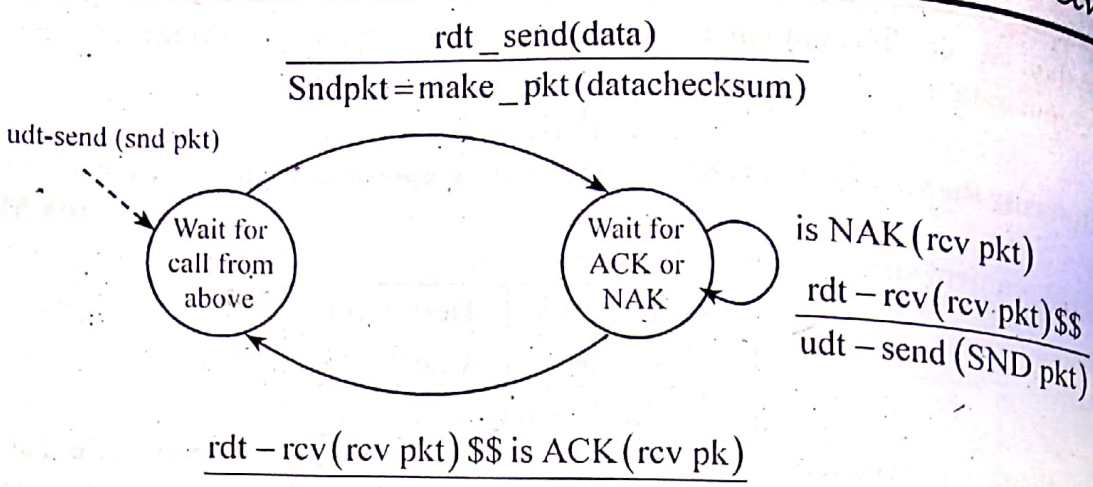
1011101110110101
1000111100001100
0100101011000010

Last addition has over flow, which is wrapped around. At the receiver , all four 16 bit words are added including checksum. If no errors are introduced , then sum at receiver will be 1111111111111111. If one of the bits is 0, then errors has been introduced into the packet.

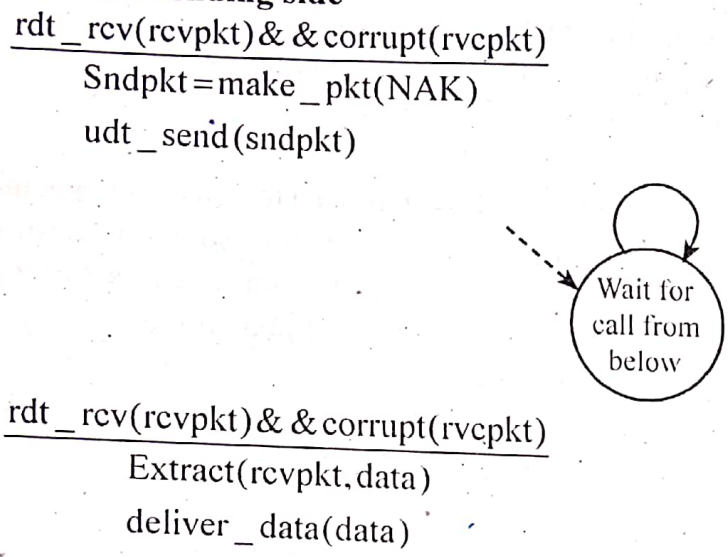
1's complement is obtained by converting all the 0's to 1's and converting an to 1's to 0's.

b. Design rdt 2.0 protocol. (08 Marks)

Ans. The send side of rdt 2.0 has two states. In the leftmost state, send side protocol is waiting for data to be paused down from upper layer. When the rdt _ send (data) event occurs, sender will create a pallet (snd pkt) containing data to be sent along with a packet checksum.



a. rdl 2.0 sending side



b. rdt 2.0 receiving side

Sndpkt = make_pkt (Ack)
udt_send(sndpkt)

rdt 2.0 - A protocol for a channel with bit errors.

When the sender is in the wait for ACK_NAK it cannot get more data from upper layer. Receiver side has rdt 2.0 has a single state. On packet arrival, receiver replies with either an ACK or NAK, depending on whether or not the received packet is corrupted. The notation rdt_rcv (rcvpkt) && corrupt (rcvpkt) corresponds to the event in which a packet is received and is found to be in error.

If an ACk packet is received rdt_rcv(rcvpkt) && in Ack(rcv/pkt) the sender known that the mostly recently transmitted packet has been received correctly & thus the protocol returns to the state of waiting for data from upper layer. The sender will not send a new piece of data until it is sure that the receiver has correctly received the current packet. Because of this behavioue, protocol rdt 2.0 are known as stop and wait protocols.

OR

4. a. **With a neat sketch, explain TCP segment and its services.** **(08 Marks)**

Ans. Refer Qno.3(a) MQP - 2.

b. **Explain how connection is established and tear down in TCP.** **(08 Marks)**

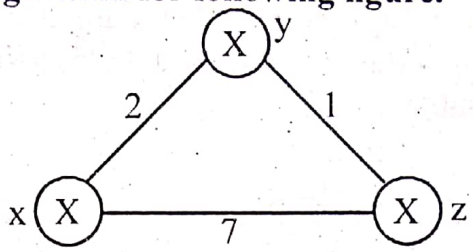
Ans. Refer Q.no.4(c) of MQP - 3.

Module - 3

5. a. **Draw Ipv6 datagram format, mention the significance of each field.** **(08 Marks)**

Ans. Refer Q.no.6(a) of Dec 17/ Jan 18.

b. **Apply distance vector algorithm for following figure.** **(08 Marks)**



Ans.

Node x table

From	Cost to x	Cost to y	Cost to z
x	0	2	7
y	∞	∞	∞
z	∞	∞	∞

From	Cost to x	Cost to y	Cost to z
x	0	2	3
y	2	0	1
z	7	1	0

From	Cost to x	Cost to y	Cost to z
x	0	2	3
y	2	0	1
z	3	1	0

Node y table

From	Cost to x	Cost to y	Cost to z
x	′	′	∞
y	2	0	1
z	∞	∞	∞

From	Cost to x	Cost to y	Cost to z
x	0	2	7
y	2	0	1
z	7	1	0

From	Cost to x	Cost to y	Cost to z
x	0	2	3
y	2	0	1
z	3	1	0

Node z table

From	Cost to x	Cost to y	Cost to z
x	∞	∞	∞
y	∞	∞	∞
z	7	1	0

From	Cost to x	Cost to y	Cost to z
x	0	2	7
y	2	0	1
z	3	1	0

From	Cost to x	Cost to y	Cost to z
x	0	2	3
y	2	0	1
z	3	1	0

The leftmost column of fig displays three initial routing tables for each of the three nodes. The second and third rows in this table are the most recently received distance vectors from nodes y & z respectively. Because at initialization , node x has not

received anything from node y or 2, the entries in second and third row are initialized to infinity.

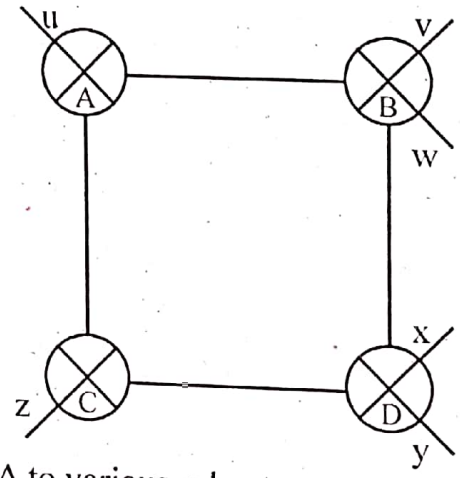
After initialization, each node send its distance vector to each of its two neighbors. After receiving the updates, each node recomputes its own distance vector.

OR

6. a. Illustrate routing info protocol (RIP) with suitable diagram. **(08 Marks)**

Ans. Routing info protocol (RIP) is intra as routing in internet. RIP is a distance vector protocol. RIP uses hop i.e., no. of subnets traversed along the shortest path from source router to destination subnet, including destination subnet. In RIP, routing updates are exchanged between neighbors approximately every 30 seconds using RIP response message. Response messages are also known as RIP advertisements. Each router maintains a routing table, it includes both the routers distance vector and routers forwarding table.

Ex :



No of hops from sources A to various subnets

Destination	Hops
u	1
v	2
w	2
x	3
y	3
z	2

If a router does not hear from its neighborer every 180 seconds, that is considered to be n longer reachable i.e., either neighbor has died or connecting link has gone down. When this happens, RIP modifies the local routing table and then propagates this info by sending advertisements to its neighboring routers.

b. Explain spanning tree algorithm. **(08 Marks)**

Ans. Refer Q.no.6(b) of MQP - 3.

Module - 4

7. a. **Define cellular network. Give the overview of GSM cellular network architecture.** **(08 Marks)**

Ans. Refer Q.no.7(b) of MQP - 2

b. **Explain the two different types of routing approaches to mobile node.** **(08 Marks)**

Ans. Refer Q.no.8(b) of MQP - 1 and Refer Q.no.7(a) of MQP - 2.

OR

8. a. **Explain the following concepts of mobile IP** **(08 Marks)**
i. Agent discovery
ii. Registration with home agent

Ans. i. Agent discovery
ii. Registration with home agent : Refer Q.no.8(a) of MQP - 1.

b. **Illustrate the steps involved when a base station does decide to hand-off mobile user.** **(08 Marks)**

Ans. Refer Q.no.7(a) of QMP - 3.

Module - 5

9. a. **Brief out three broad categories of multimedia network application.** **(08 Marks)**

Ans. Refer Q.no.9(a) of MQP - 3.

b. **Discuss the following :** **(08 Marks)**
i. Adaptive streaming
ii. DASH

Ans. i. Adaptive streaming

OR

10. a. **With a general format, explain the various fields of RTP.** **(08 Marks)**

Ans. RTP runs on UDP. Sending side encapsulates an media chunk within an RTP packet, then encapsulates the packet in UDP segment and then hands the segment to IP. The sending side proceeds each chunk of data with an RTP header. RTP header form RTP packet. At the receiver side, application receiver its RTP packet from socket.

Payload type	Sequence number	Timerstamp	Synchronization source identifier	Miscellaneous field

RTP header fields is shown above

The payload field is 7 bits long. For ex in audio stream payload type field is used to indicate the type of audio encoding.

- Sequence no field is 16 bits long. Sequence no increments by one for each RTP

packet sent. The receiver uses sequence no to detect packet loss and to restore packet sequence.

- Timestamp field is 32 bits long. It reflects the sampling instant of the first byte in the RTP data packet. The receiver can use timestamp to remove packet fitter. The timestamp clock continues to n cease at a constant rate even if the source is inactive.
- Synchronization source identifier (SSRC) : Field is 32 bits long . It identifies source of RTP stream. Each stream in an RTP session has a distance SSRC. SSRC is a number that the source assigns randomly when new stream is started.

b. Explain the working procedure of leaky bucket algorithm **(08 Marks)**

Ans. Refer Q.no. 1.(a) of MQP - 1.

Fifth Semester B.E. Degree Examination, CBCS - Dec 2018 / Jan 2019

Computer Networks

Time: 3 hrs. **Max. Marks: 80**

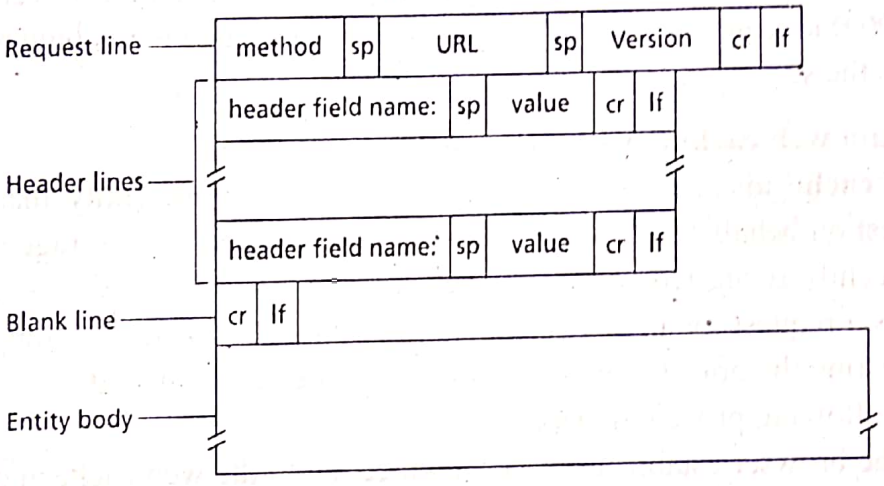
Note : *Answer any FIVE full questions, selecting ONE full question from each module.*

Module-1

1. a. Explain HTTP messages. **(08 Marks)**

Ans. There are two types of messages HTTP request message and restore messages. HTTP/1.0 allows three types of methods GET, POST and HEAD. The first line of an HTTP request message is called request time the subsequent times are called the header lines. The request line has three fields, method field, URL field and HTTP version field. Majority of HTTP request messages uses GET method. Header line specifies the user agent that is the browser type that is making request to the server.

Below is the general format of a request message

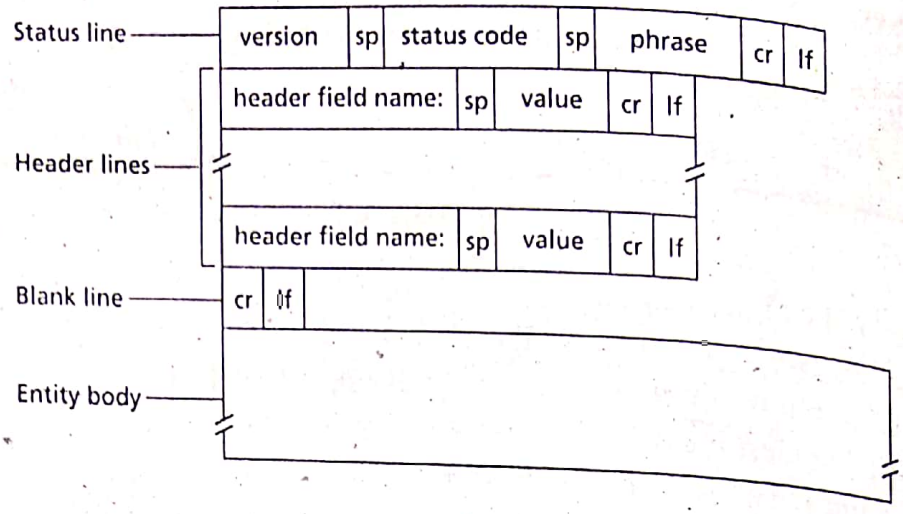


HTTP1.1 allows for additional methods PUT and DELETE. The DELETE method allow a user or an application to delete on a web server.

HTTP Response Message

It has three sections - an initial status line, sin header lines and entity body. The entity body contains the required object. Status line has three fields - protocol version, status code and corresponding status message. Server uses connection : close header line to tell client is going to close the connection. Data header line indicates time and date when HTTP response was created and sent by the server. Last-modified indicates date and time when the object was created or last modified. Content length indicates the number of bytes in the object being sent. Content type indicates the object in the entity body is HTML text.

Below is the form at of response message.



Some common status code and associated phrases include

- 2000k - request succeeded and the info is returned in the response.
- 404 not found - requested document does not exist on the server.
- 400 Bad request - is a genetic error code indicating request could not be understood by the server.

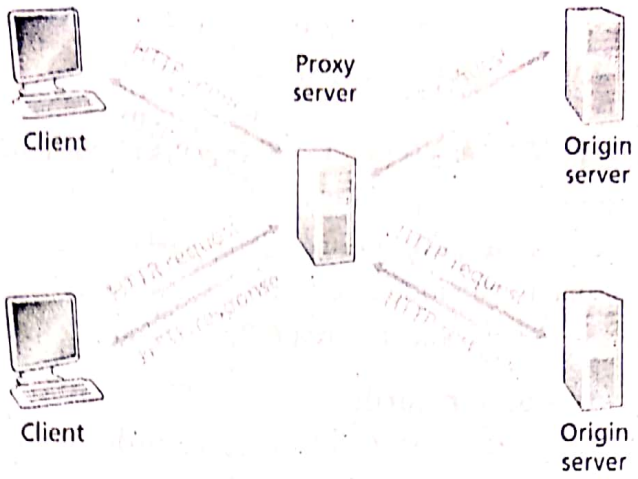
b. Explain web caching with diagram.

Ans. **Web cache also called proxy server** - is a network entity that satisfies HTTP request on behalf of origin web server. It has its own disk storage and keeps copies of recently requested objects in their storage. Once a browser is configured, each browser request for an object is first directed to web cache. Ex: Suppose a browser is requesting the object http://www.someschool.edu/campus.gif. **(08 Marks)**

The following procedure happens

- The browser establishes a TCP connection to the web cache and sends an HTTP request for the object to the web cache.
- The web cache checks to see if it has a copy of the object stored locally. If it has, it forwards the object within an HTTP response message to client browser.
- If it does not have, web cache opens TCP connection to the origin server i.e, www.school.edu. Web cache then sends an HTTP request for the object into the TCP connection. After receiving their request, origin server sends the object within an HTTP response to web cache.
- When the web cache receives the object, it stores a copy in the local storage and few as a copy.

Cache is both a server and a client at same time.



The total response time is the time from browser's request of an object is the sum of LAN delay, access delay and Internet delay.

OR

2. a. Explain FTP with its commands and replies. **(08 Marks)**

Ans. In FTP, the commands from client to server and replies from server to client are sent across control connection in 7 bit ASCII format. Each command consists of four upper case ASCII characters with optional arguments. Some of the commands are shown below.

- USER Username : Used to send user identification to the server.
- PASS Password : Used to send the password to the server.
- List : Used to ask the server to send back a list of all files in the current remote directory.
- RETR filename : Used to retrieve file from current directory.
- Stor file name : used to store a file into the current directory of remote host.

There is one to one correspondence between the user issued and FTP across control connection. Each common and is followed by a reply sent from server to client. The replies are three digit numbers with an optional message following number.

Some replies with the possible messages are shown below.

- 331 - User name ok, password required
- 125 - Data connection already open, transfer starting
- 425 - Can't open data connection
- 452 - Error writing file.

b. Explain SMTP. **(04 Marks)**

Ans. Simple mail transfer protocol(SMTP) transfers message from sender's mail to recipient's mail server. It uses 7-bit ASCII. Suppose Alice wants to send Bob a simple ASCII message following steps happens.

- Alice's invokes her user agent for e-mail, provides Bob's e-mail address, compose a message and instructs user agent to send the message.
- Alice's user agent sends the message to her mail server, where it is placed in a message queue.

- Client side of SMTP, running on Alice's mail server, sees the message in the message queue. It opens TCP connection to an SMTP server, running on Bob's mail server.
- After some initial SMTP hand shaking, SMTP client sends Alice message into TCP connection.
- At Bob's mail server, the server side of SMTP receives the message. Bob's mail server then places the message in Bob's mailbox.
- Bob invokes his user agent to read the message at his convenience.

c. Explain DNS resource record. **(04 Marks)**

Ans. DNS distributed database store resource records (RR). Each DNS reply message carries one or more resource records. A resource record is four types containing following fields (Name, Value, Type, TTL)

TTC is the time to live of resource record. It determines when a resource should be removed from cache. The remaining of Name and value depend on Type:

If type = A, then Name is a host name and value is the IP address for the host name.

If type = NS, then name is domain and value is the host name of an authoritative DNS server.

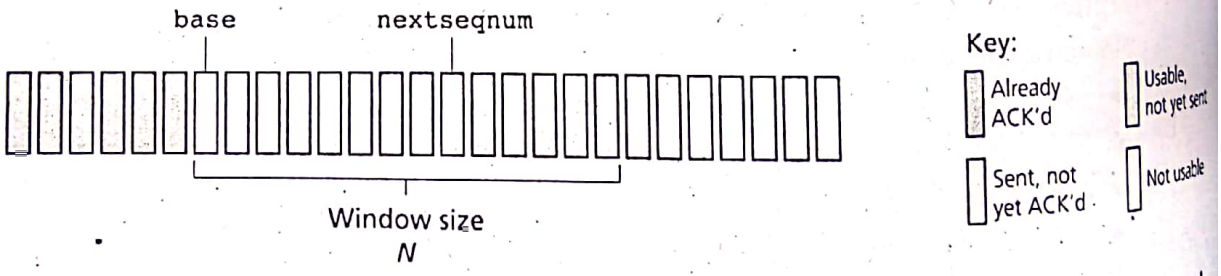
If type = Name , then value is a canonical host name for the alias host name Name.

If type = MX, then value is canonical name of a mail server that has an alias hast name Name.

Module-2

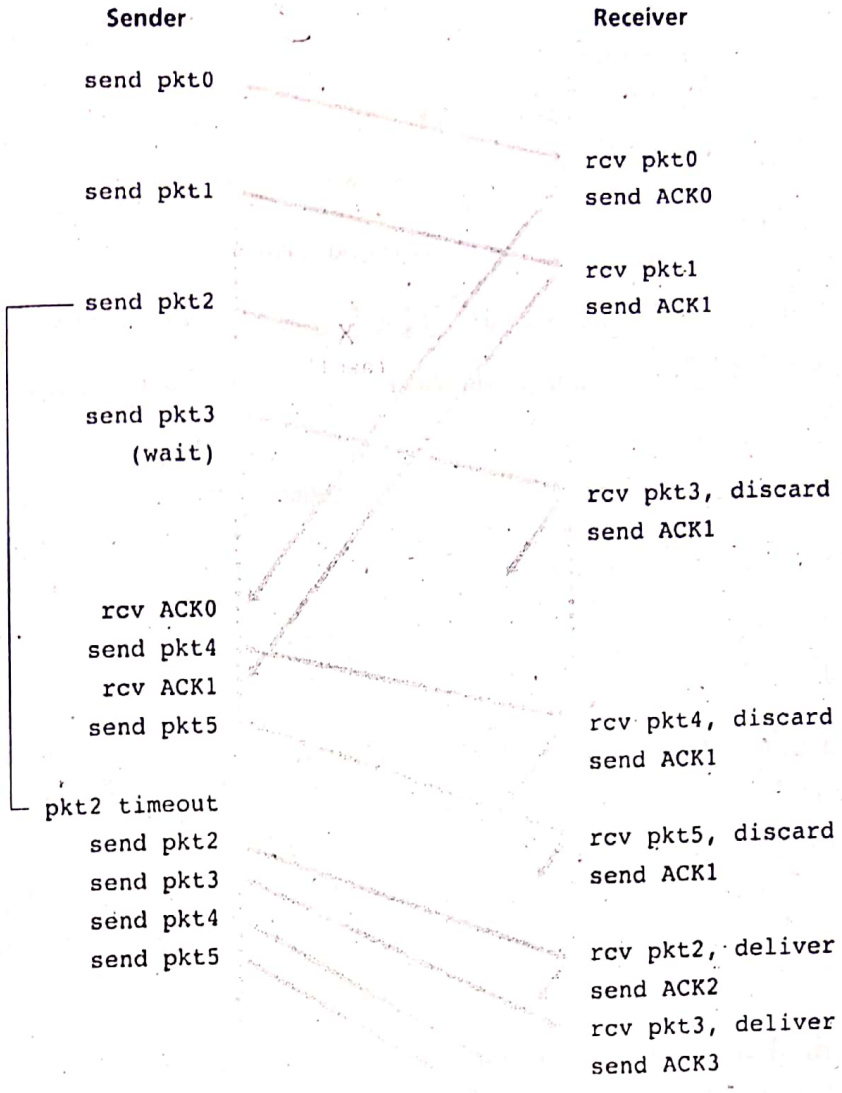
3. a. Explain Sender's view of sequence numbers and its operation in Goback N protocol. **(08 Marks)**

Ans. In Go - back - N (GBN) protocol, the sender is allowed to transmit multiple packets (when available) without waiting for an acknowledgment. It cannot have more than maximum value N of unacknowledged packets in the pipeline. Figure shown the sender's view os sequence numbers.



The range of permissible sequence numbers for transmitted but not yet acknowledged packets are viewed as window size N over the range of sequence numbers. As the protocol operates the window slides forward over the sequence number space. In GBN protocol, receiver discards out of order packets. Suppose packet n is expected, n+1 packet arrives, because the data must be delivered in order, the receiver buffers n+1 packet and then deliver the packet to upper layer after it has received packet N.

Figure shows the operation of GBN protocol for the case of four packets.

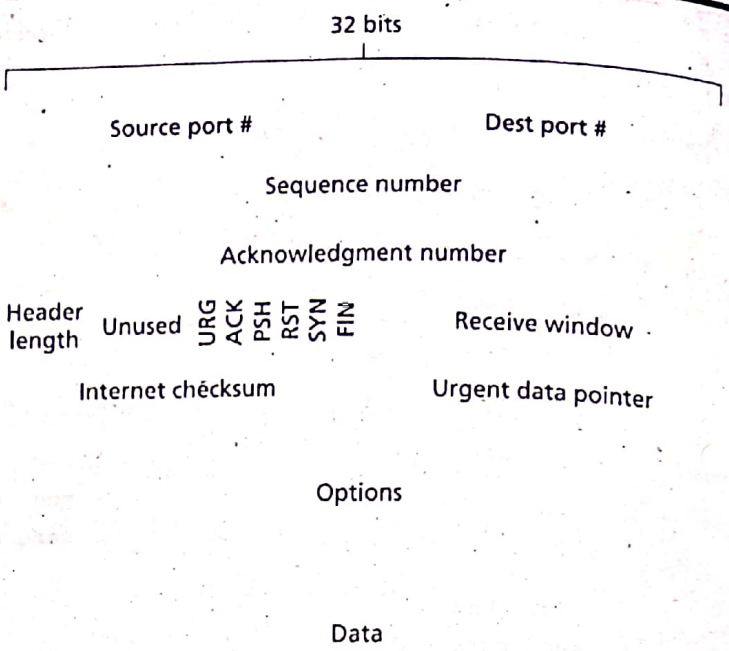


A packet's sequence number is carried in a fixed length field in the packet header. If K is the number of bits in the packet sequence number field, range of sequence numbers is $(0.2^k - 1)$

b. Draw TCP segment structure and explain. **(08 Marks)**

Ans. TCP structure includes source and destination post numbers used for multiplexing and de-multiplening.

- 32 bit sequence number field and 32 bit acknowledgment number field are used by TCP sender and receiver in implementing a reliable data transfer service.
- 16bit receive window field is used for flow control.
- 4 bit header length specifies the length of TCP header in 32 bit words.
- Optional and variable length options field is used when a sender and a receiver negotiate maximum segment size(MSS)
- Flag field contains 6 bits. ACK but is used to indicate that the value carried in the acknowledgement field is valid. RST, SYN, FW bits are used for connection setup and tear down. Setting PSH bit indicates receiver should pass data to the upper layer immediately. URG bit is used to indicate that there is data in the segment that the sending side upper layer entity has marked urgent.



The location of the last byte of the urgent data is indicated by 16 bit urgent data pointe field. TCP must inform the upper layer entity when urgent data exists and pass it pointer to the end of the urgent data. Two important fields in the TCP segment heade are sequence number field and acknowledgment number field. It includes a chec some field for error checking. TCP segment consist of header fields and data field.

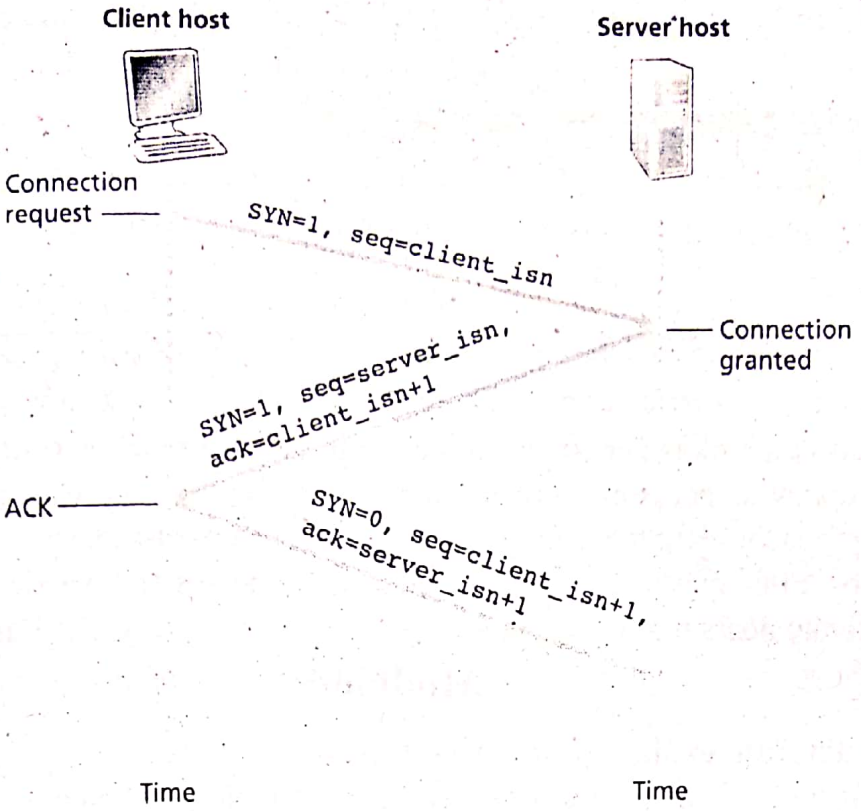
OR

4. a. Explain 3 way handshake and closing a TCP connection. **(08 Marks)**

Ans. **Step 1 :** Client side of TCP first sends a special TCP segment to the server - side TCP This special segment contains no application layer data. SYN bit is set to 1. Client randomly chooses an initial sequence number and puts this number in the sequence number field of initial TCP SYN segment. This segment is encapsulated within an IP datagram and sent to the server.

Step 2 : Once the IP datagram containing TCP SYN segment arise at the server host, server extracts the TCP SYN segment from datagram, allocates TCP buffers and variables to the connection and sends a connection granted segment to the client TCP. It contains three important piece of info. First SYN bit is set to 1, second acknowledgement field of TCP segment header is set to client_isn+1. Finally, server chooses its own initial sequence number (server_isn). The connection granted segment is also called referred to as SYNACK segment.

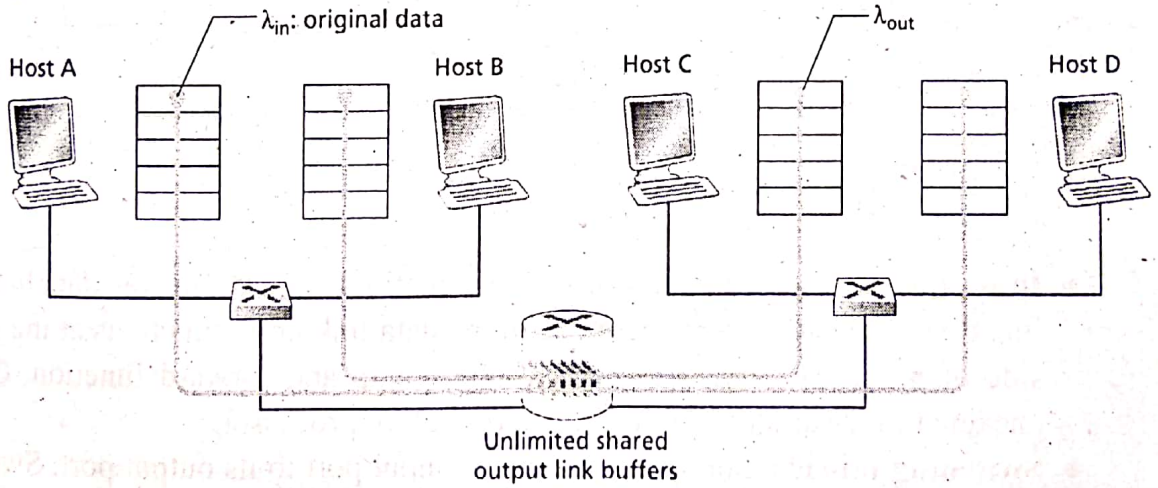
Step 3 : UPon receiving SYNACK segment, client also allocates buffers and variables to the connection. The client host then sends the server another segment. This last segment acknowledges servers connection granted segment. The SYN bit is set to 0, since the connection is established.



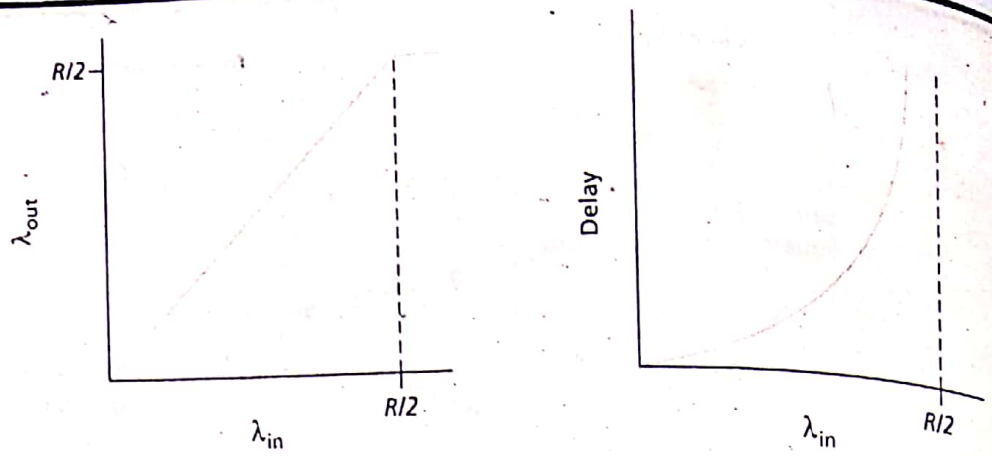
Once these three steps are completed , client and server host can send segments containing data to each other.

b. Explain the causes and costs of congestion. **(08 Marks)**

Ans. Causes and cost of congestion can be explained by taking any one of the scenario's Scenario : To senders, a router with infinite buffers two host (A and B) each have a connection that shares a single hop between source and destination as shown in figure.



Application in host A sends data into the connection at an average rate of λ in bytes/second. Each unit of data is sent only once into the socket. Data is encapsulated and sent no error recovery is included. Host A offers traffic to the router is λ in bytes/second. Host B also operate in similar manner. Packets from host A and B ran through a router and share outgoing link of capacity R. The router has buffers that allows it to store in coming packets when packet arrival exceeds outgoing link.



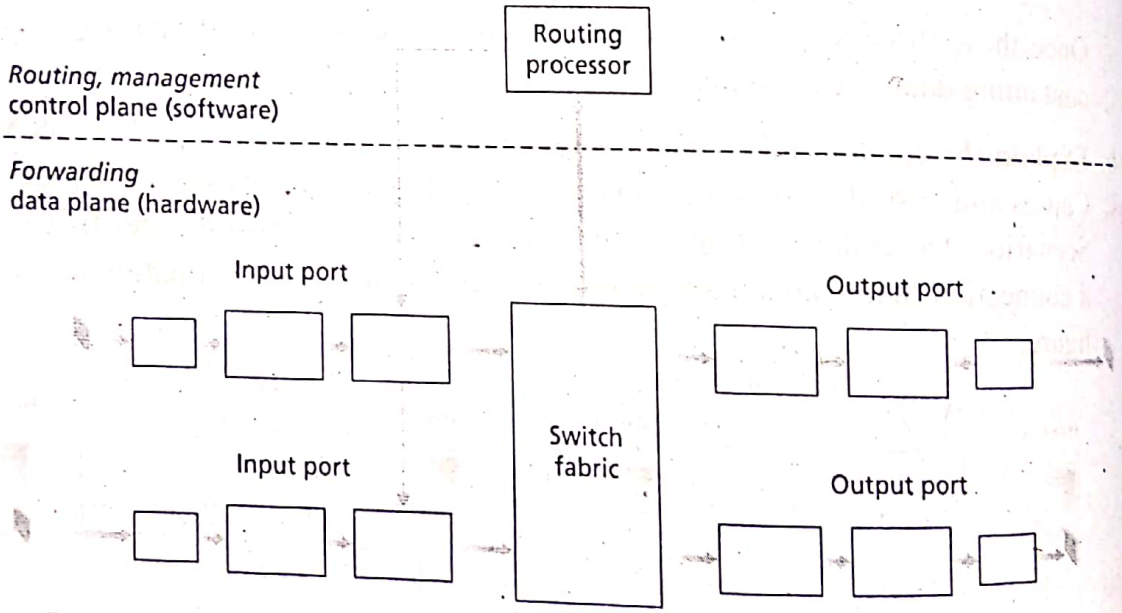
The left graph plots per connection through out as a function of connection sending rate. Achieving per connection through out utilizes the complete link. As the sending rate approaches R/2 the average delay becomes larger and larger.

The cost of congested network/- large queuing delays are experienced as the packet arrival rate nears the link capacity.

Module-3

5. a. With diagram explain router architecture. (08 Marks)

Ans. Forwarding and switching are the two main functions of router.



- **Input ports :** It performs physical layer functions. It performs the data link layer functions needed to inter operate with the data link layer functions at the remote side of incoming link. It also performs lookup and forward function. Control packet are forwarded from input port to routing processor.
- **Switching fabric :** Connects the router's input port to its output port. Switching fabric is completely contained within the router.
- **Output ports :** Stores the packets that have been forwarded to it through the switching fabric and then transmits the packets on the outgoing link. It performs the reverse data link layer function of the input port. When the link is bidirectional, an output port to the link will be paired with input port on same line card.

- **Routing processor :** Executes the routing protocol maintains the routing information and forwarding tables and performs network management functions within the router.

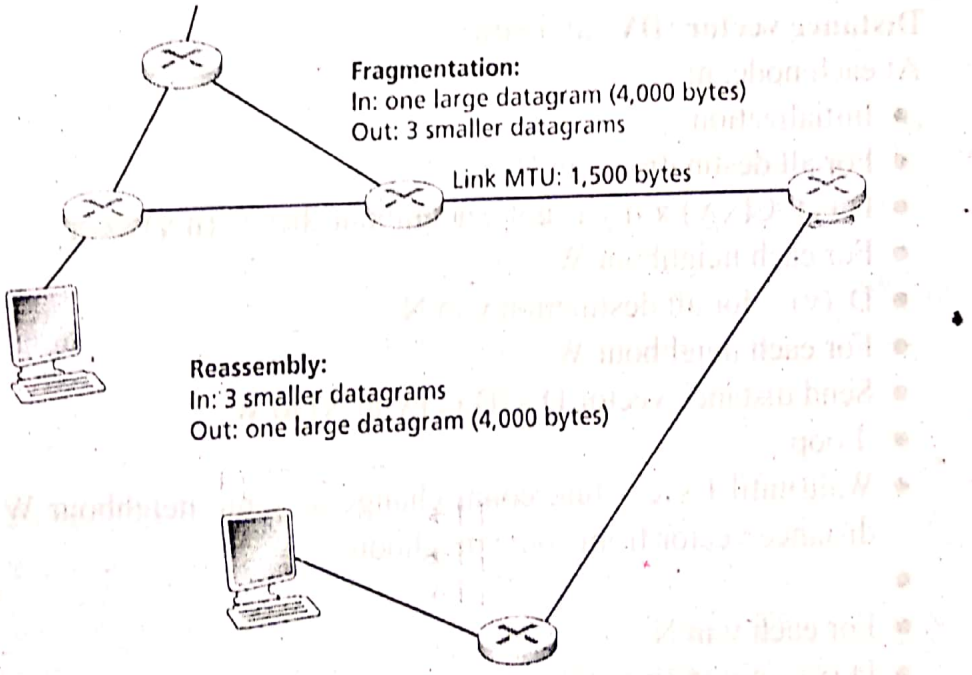
Multiple ports are often gathered together on a single line card within a router.

b. Explain IP fragmentation. **(08 Marks)**

Ans. The maximum amount of data a link layer frame can carry is called maximum transmission unit (MTU). Because each IP data gram is encapsulated within link layer format, transport from one router to next router places a limit on the length of IP packet. The solution is to fragment the data in the IP data gram into two or more smaller IP data gram, then send these smaller data gram over outgoing link. Each of these referred as fragment.

Fragment needs to be reassemble at transport layer before they reach destination. If some data gram are fragments, it needs to determined when it as received last fragment. To allow reassembling identification, flag and fragment offset fields are present in IP data gram. When a data gram is created, sending host stamps the data gram with an identification number and source and destination address. When a router needs to fragment the data gram, each resulting data gram is stamped with source address and destination address.

Example : A data gram of 4000 bytes arrives at a router and must be forwarded to a link with an MTU of 1,500 bytes. This implies that 3,980 bytes in the original data gram can be allocated to three separate fragments..



Fragment	Bytes	ID	Offset	Flag
1st	1480bytes in data field of IP datagram	777	Offset=0 (data should be inserted at beginning)	Flag=1 (there are more fragments)
2nd	1480bytes of data	777	Offset=185	Flag=1
3rd	1020bytes (3980-1480-1480) of data	771	Offset=370	Flag=0 (no more fragments)

OR

6. a. Explain distance vector algorithm. **(08 Marks)**

Ans. Distance vector algorithm is inter active, asynchronous and distributed. Each node receives some information from one or more of its directly attached neighbours. It is interactive in that this process continues on until no information is exchanged between neighbours. It is asynchronous in that it does not receive all of the nodes to operate in lock setup with each other.

Each node X begins with $D_x(Y)$, an estimate of the cost of the least - cost path from itself to node y, for all nodes in N. Let $D_x=(D_x(y):y \text{ in } N)$ be the node x's distance vector. Each node x maintains following routing data.

- For each neighbour V, cost C(x,v) from x to directly attached neighbour V.
- Node x's distance vector that is $D_x=(D_x(y):y \text{ in } N)$, containing x's estimate of its cost to all destinations y in N.
- The distance vector of each of its neighbour that is $D_v=(D_v(y):y \text{ in } N)$ for each neighbour V of N.

Distance vector (DV) algorithm

At each node, n:

- Initialization
- For all destination y in N:
- $D_x(y)=C(x,y)/\pi$ if y is not a neighbour then $C(n,y)=\infty/\pi$
- For each neighbour W
- $D_w(y)=$ for all destination y in N
- For each neighbour W
- Send distance vector $D_n=[D_n(y):y \text{ in } N]$ to W
- Loop
- Wait(until I see a link count change to some neighbour W or until I receive a distance vector from some neighbour W)
-
- For each y in N
- $D_n(y)=\min_v(C(n,v)+D_v(y))$
-
- If $D_x(y)$ changed for any destination y
- Send distance vector $D_x=[D_x(y)=y \text{ in } N]$ to all neighbour
-
- Forever

b. Explain 4 types of hierarchical OSPF routers. **(04 Marks)**

Ans. An OSPF is configured into areas. Within each area one more border router are responsible for routing. Four types of OSPF router are

- Internal routers : are in non-backbone areas and perform only intra AS routing.
- Area border routers - These routers belong to both an area and the backbone.
- Backbone routers (non border routers) : Perform routing within the backbone. Within a non-backbone area, internal router learn of the existence of routers to the other areas from information broadcast within the area by its backbone routers.
- Boundary routers : Exchanges routing information with routers belonging to other autonomous system. This router for example use BGP to perform inter as routing. It is through such a boundary router that other routers learn about paths to external networks.

Exactly one OSPF area in the AS is configured to be the backbone area.

c. Compare link state with distance vector algorithm. **(04 Marks)**

Ans. **Message complexity :** LS requires each node to know the cost of each link in the network. Whenever a link cost changes, new link cost must be sent to all nodes. BV algorithm requires messages exchanges between directly connected neighbours at each iteration. DV will propagate results of the changed link cost only if the new link cost result is changed.

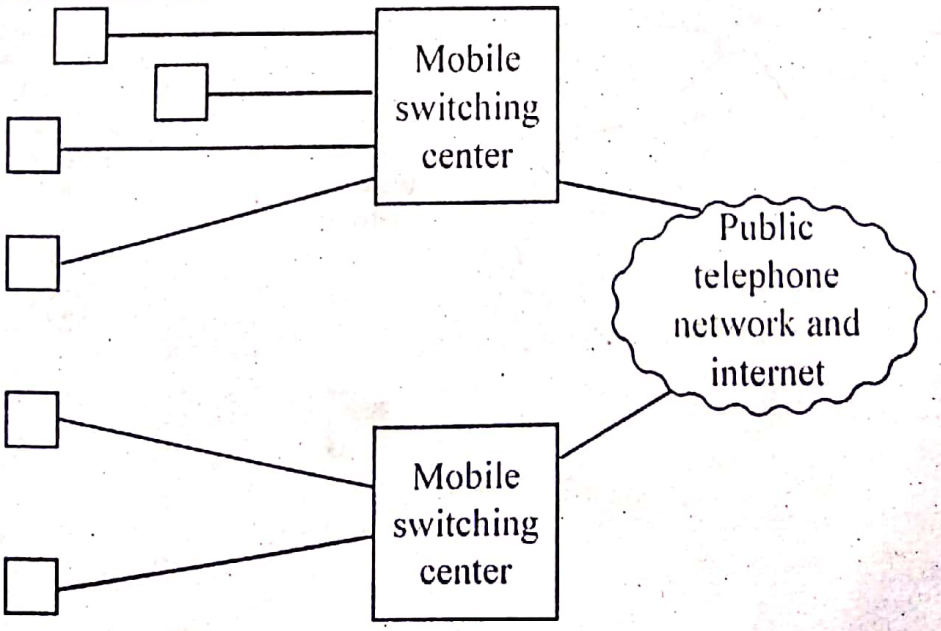
Speed of Convergence : Implementation of LS is an O (N^2) algorithm requiring O(NI/EI) messages. DV algorithm converges slowly and can have routing loops while the algorithm in is converging. DV refers from count to infinity problem.

Robustness : If a router fails, in LS a router broadcast an incorrect cost for one of its attached links. A node could also corrupt or drop any packet it received as a part of LS broadcast. In DV a node can advertise incorrect least paths to any or all destination. This cost routers to flood the malfunctioning router with traffic.

Module-4

7. a. Explain components of a cellular network architecture. **(08 Marks)**

Ans. Cellular refers to the fact geographical area is portioned into a number of geographic coverage areas called cells.



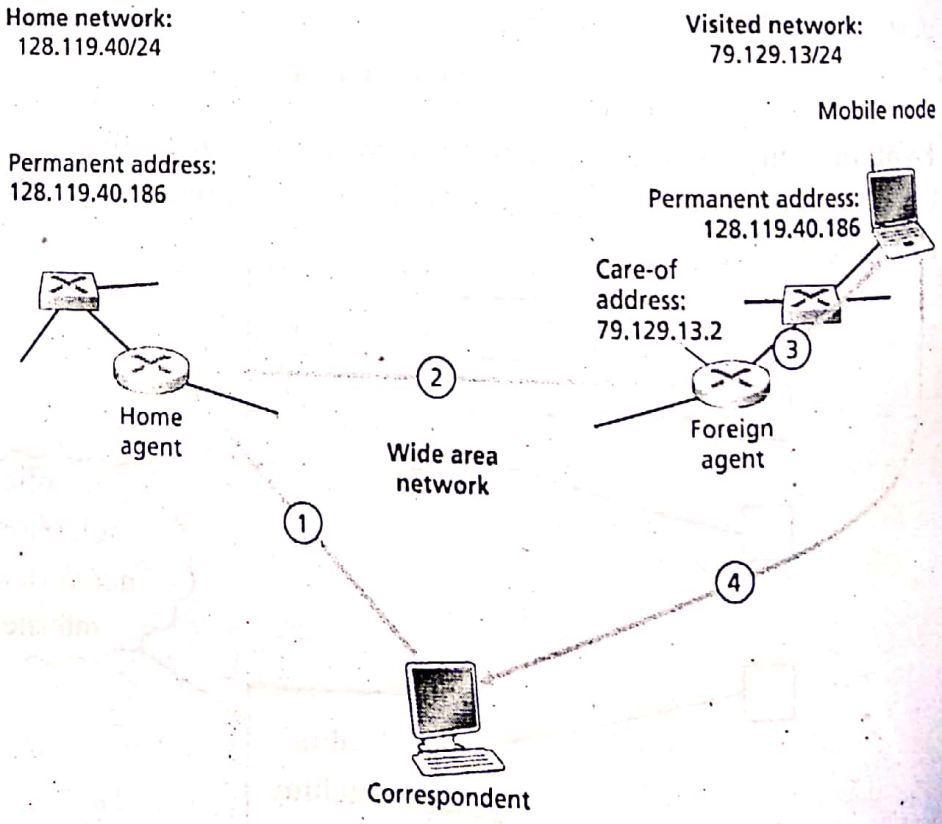
Each base station is connected to wide area network such as public switch telephone network (PSTN) or directly to internet via wired infrastructure. Each base station is connected to mobile switching centre (MSC) which manages call establishment and tear down to and from mobile users. An MSC contains much of functionality, calls need to share the portion of the radio spectrum that is allocated to cellular service. Two approaches are used - combination of frequently division multiplexing (FDM) and time division multiplexing (TDM)

Code division multiple access does not partition in frequently or in time. All users share the same radio frequency at same time. Each user in a cell is allocated a distinct sequence of bits called chipping sequence. When using FDM/TDM system, the receivers are sensitive to interference from other signals in same frequency band. A given frequency can be reused in FDM/TDM system only in cells that are located far to avoid such interference. Such frequency reused is major concern when designing CDMA systems.

b. Explain direct routing of a mobile node. **(08 Marks)**

Ans. Direct routing overcomes inefficiency of indirect routing, a correspondent agent in the correspondent's network first learns COA of mobile node. This is done by having correspondent agent query the home agent, mobile node has an up-to-date value for its COA registered with home agent. It introduces two challenges

- Mobile-users location protocol is needed for the correspondent agent to query home agent to obtain mobile node's COA.
- When the mobile node moves from one foreign network to another home agent is queried for the COA by correspondent agent only once at the beginning of session.

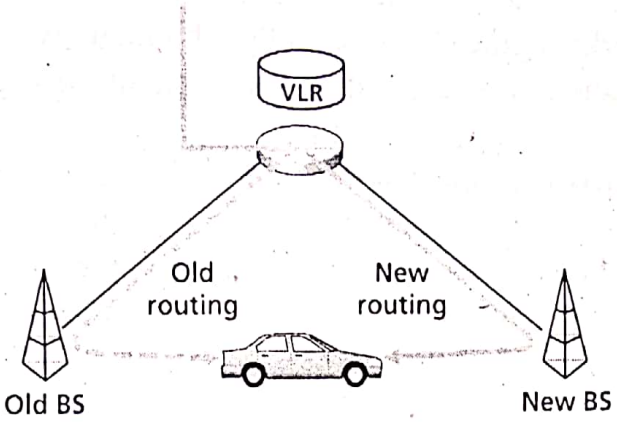


If the data is being forwarded to the mobile node in the foreign network, then foreign agent is identify (step1) as anchor foreign agent. When the mobile node moves to new foreign network (step2) the mobile node registers with new foreign agent (step3) and the new foreign agent provides the anchor foreign agent with mobile node's new COA (step4). When anchor foreign agent receives an encapsulated datagram for a departed mobile node it can then re-encapsulate the datagram and forward it to mobile node

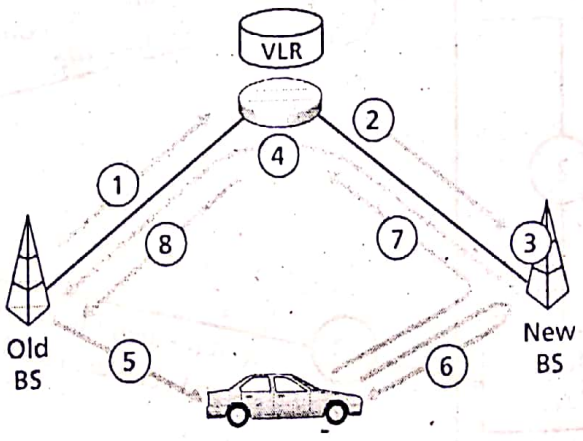
OR

8. a. Explain steps of handoff a mobile user. **(08 Marks)**

Ans. A hand of occurs when a mobile station changes its association from one base station to another base station.



- The old base station (BS) informs the visited MSC that a hand off is to be performed and the BS to which the mobile is to be handed off.
- Visited MSC initiates path setup to the new BS that a handoff is able to occur.
- The new BS allocates and activates a radio channel for use by the mobile.
- The new BS signal base to the visited MSC and the old BS that the visited MSC to new BS path that is established and the mobile needs to be handoff.
- The mobile is informed that it should perform a handoff..
- The mobile and the new BS exchange one or more messages to fully activate the new channel in BS.
- The mobile then sends a handoff complete message to the new BS which is forwarded upto the visited MSC. The visited MSC then reroutes the on-going call to the mobile via the new BS.
- The resources allocated along the path to the old BS are then released.



b. Explain HLR, VLR, home address, care-of-address. **(08 Marks)**

Ans. **HLR :** The home network maintains a database known as the home location register (HLR), which contains permanent cell phone number and subscriber profile info for each of its subscriber. HLR also contains info about the current location of these subscribers. HLR contains info to obtain an address in the visited network to which a call to the mobile user should be routed.

VLR : The visited network maintains a database known as the visitor location register (VLR). It contains an entry for each mobile user that is currently in the position of the network served by VLR. VLR entries come and go as mobile users enter and leave the network. VLR is co-located with the mobile switching centre(MSC).

Home Address : IN a network setting, permanent home of a mobile node is known as home network and the entity within the home network that performs the mobility management function and is called home agent. The permanent address is called home address.

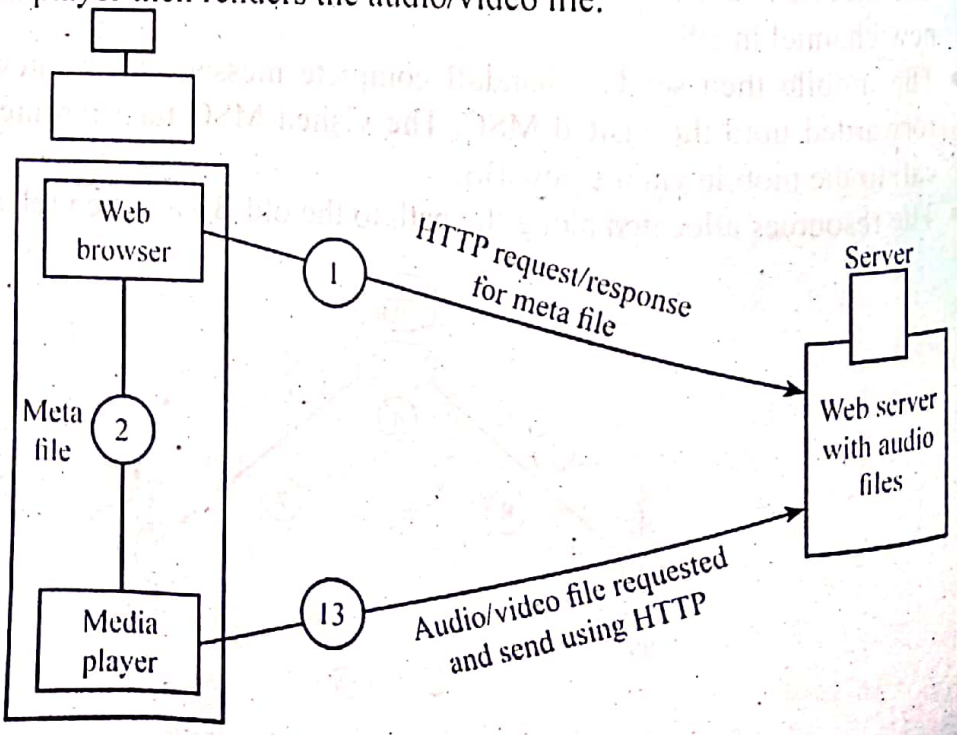
Case - of - Address : One role of the foreign agent is t create care-of -address for the mobile node, with the network partition of the COA matching that of foreign network. The address of foreign network is called Care - of - address. It is also known as foreign address. The network in which the mobile node is currently residing is known as foreign or united network.

Module-5

9. a. With diagram, explain naive architecture for audio/video streaming. **(08 Marks)**

Ans. In the naive architecture

- The browser process establishes TCP connection with web server and requests audio/video file with an HTTP request message.
- Web server sends the audio/video file to the browser in an HTTP response message.
- Content type header line in HTTP response message indicates a specific audio/video encoding.
- Media player then renders the audio/video file.



- The user clicks on a hyperlink for audio/video file.
- Hyperlink does not point directly to audio/video file but instead into a meta file. It contains URL of actual audio/video file.
- Client browser examines the content type header line of the response message, launches associated media player and passes entire body of the response message.
- Media player after TCP connection directly with the HTTP server. The media player sends an HTTP request message for the audio/video file into the TCP connection.
- The audio/video file is sent within an HTTP response message to the media player. The media player streams out the audio/video file.

b. Explain audio compression in internet. **(08 Marks)**

Ans. Before audio and video can be transmitted over a computer network it must be digitised and compressed. All transmitted info must be represented as a sequence of bits.

A continuously varying analog audio signal is converted to digital signal as follows

- The analog signal is first sampled at some fixed rate, for example at 8000 samples per second. The value of each sample is an arbitrary real number.
- Each of the samples is rounded to one of a finite number of values. This operation is referred to as Quantization. The number of finite values called Quantization values - is power of two for En 256 Quantization values.
- Each Quantization value is represented by a fixed number of bits. EX : If there are 256 Quantization values then each value is represented by 1 byte. Each of the samples is converted into its bit representation. Bit representation of all samples are concatenated together to form digital representation of signal.

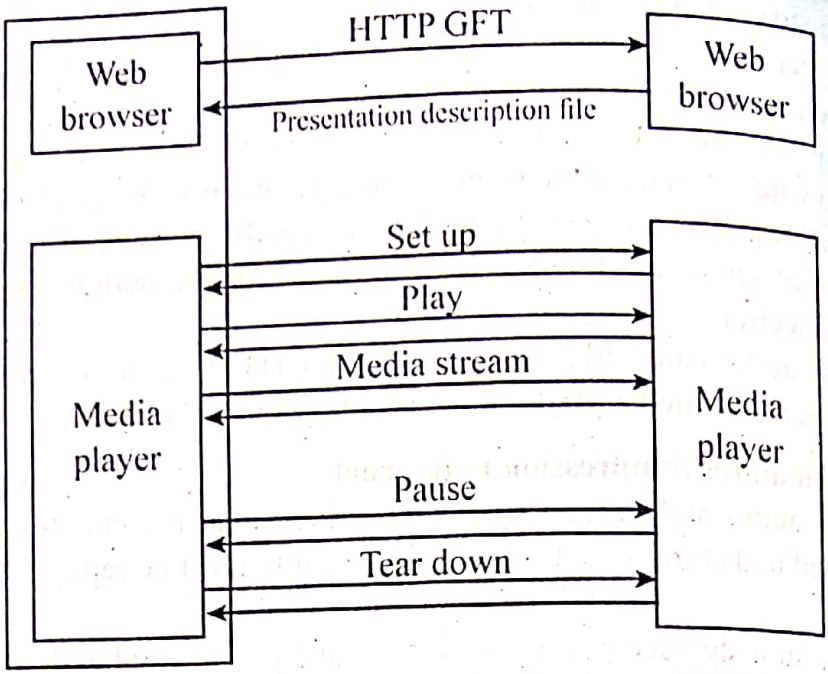
The basic encoding technique is called pulse code modulation (PCM) with a sampling rate of 8000 samples per second.

OR

10. a. With diagram, explain interaction between client and server using RTSP. **(08 Marks)**

Ans. Real Time Streaming Protocol(RTSP) allows a media player to control the transmission of media stream. Control actions include pause/resume, repositioning of playback, fast-forward and rewind RTSP is an out band protocol. RTSP messages are sent out of band where as the media stream, whose packet structure is not defined by RTSP is considered "in-band". RTSP message use port number 544 from media stream.

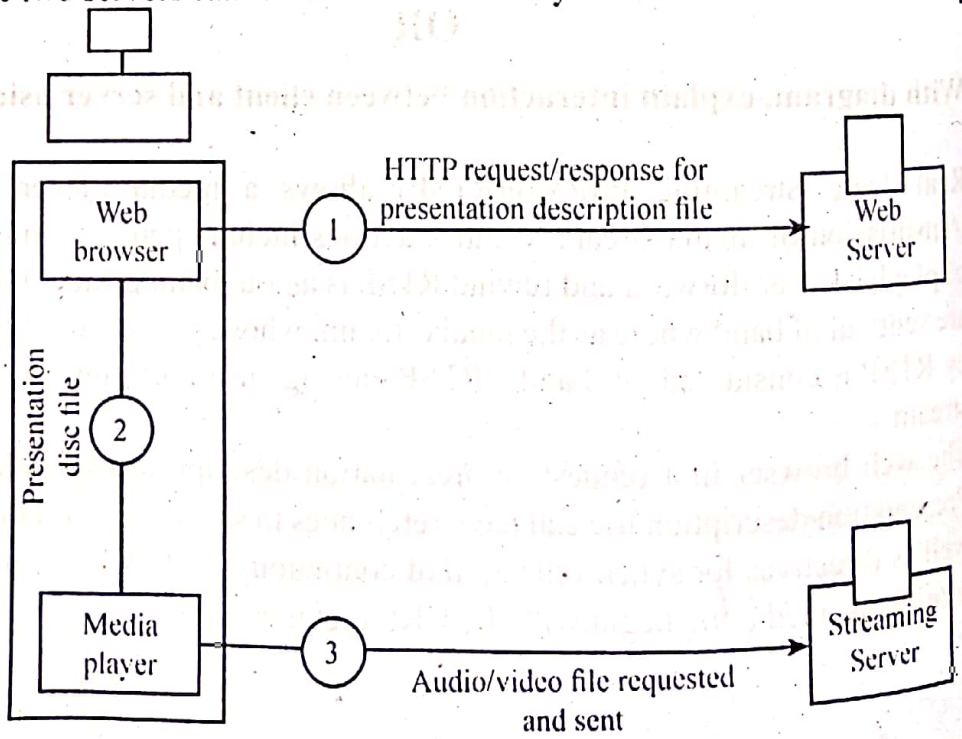
The web browser first requests a presentation description file from a web server. Presentation description file can have references to several continuous media files as well as directives for synchronization of continuous media files. Each reference to a continuous media file begin with the URL method rtsp://.



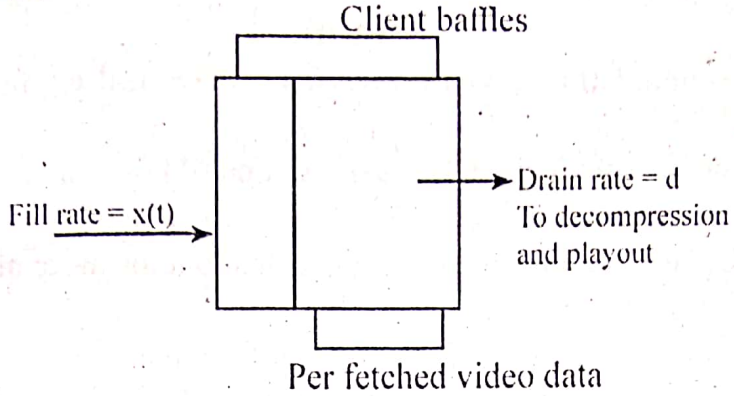
Web server encapsulates presentation description file in an HTTP response message and sends message to the browser. When the browser receives message, it invokes media player based on content type field of the message. The player sends an RTSP SETUP RTSP play request and server responds with ok message. Later the RTSP sends an RTSP PAUSE request and server responds with ok message. Finally tear down phase happens and connection is terminated.

b. Explain how streaming from streaming server to a media player is done. **(08 Marks)**

Ans. The architecture requires two servers. One server, the HTTP server, server web pages (including meta files). The second server, the streaming server serves the audio/video files. The two servers can run on the same end system or on two distinct end systems.



- The audio/video is sent over UDP at a constant rate equal to the drain rate at the receiver.
- This is same as the first option, but the media player delays playout for two to five seconds in order to eliminate network induced jitter. Client accomplishes this task by placing compressed media it received from the network into a client buffer as shown in figure.



- The media is sent over TCP. The server pushes the media file into the TCP socket as quickly it can. Client reads from the TCP socket as quickly as it can and places the compressed video into the media player buffer.

Fifth Semester B.E. Degree Examination, CBCS - June / July 2019
Computer Networks

Time: 3 hrs. Max. Marks: 80

Note : *Answer any FIVE full questions, selecting ONE full question from each module.*

Module-1

1. a. Describe in detail the services offered by DNS and explain the DNS message format. (08 Marks)

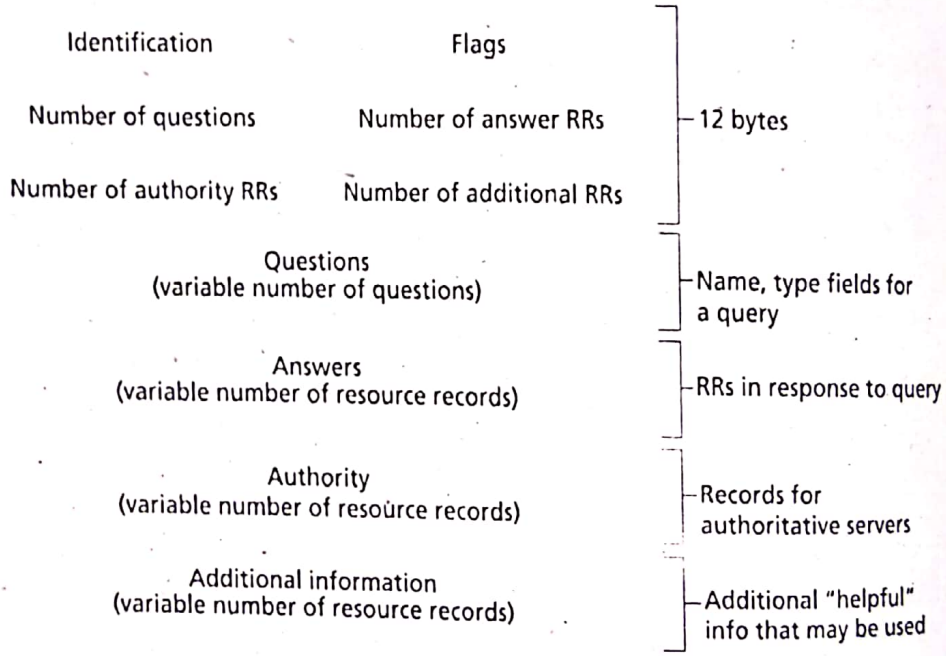
Ans. The main service offered by DNS is translation of host names to IP addresses. Other additional services are

(1) Host aliasing - A host can have more than one or more alias names. Canonical hostname is used by DNS.

(2) Mail server aliasing - It is desirable that E-mail addresses must be mnemonic.

(3) Load distribution - DNS is used to perform load distribution among replicated server.

DNS message format



- The first 12 bytes is the header section, First field is 16 bit no that identifies query. Identifies is copied into reply message to a query.
- The question section contains info about the query that is being made. This section includes a name field that contains name that is being queried and a type field that indicates the type of question being asked.
- In a reply from DNS server, answer section contains the resource records for the name that was originally queried.
- The authority section contains records of other authoritative servers.
- The additional section contains other helpful records. For ex, answer field in a reply to an MX query contains a resource record providing canonical ostname of a mail server. Additional section contains a Type A record providing IP address for Canonical hostname of mail server.

b. Illustrate the basic operation of SMTP and FTP. **(08 Marks)**

Ans. Refer Q.No. 2.a. and 2.b. of Dec 18 / Jan 19

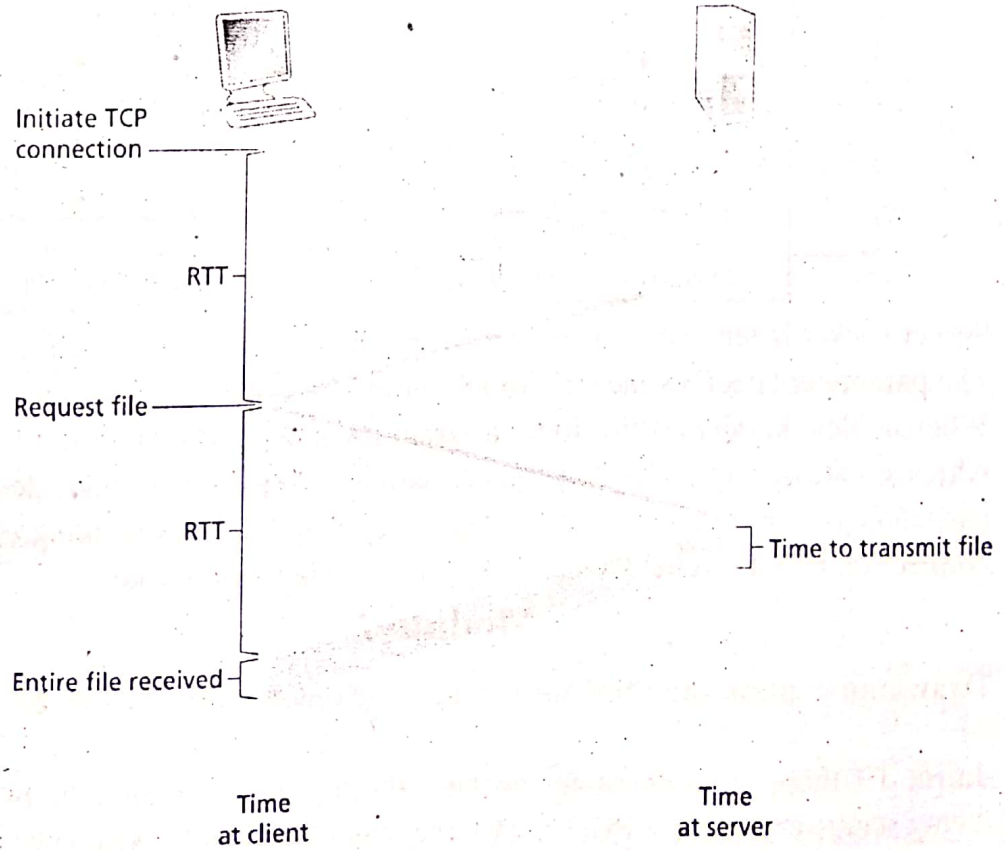
OR

2. a. Explain the persistent and non-persistent connection of HTTP. **(08 Marks)**

Ans. **Non-persistent connection :-** Web page needs to be transferred from server to client, the following steps take place

1. The HTTP client process initiates a TCP connection to the server www.school.edu on port number 80.
2. The HTTP client sends an HTTP request message to the server via its socket associaed with TCP connection. Request message includes the path name / someDepartment/home.index.
3. HTTP server process receives the request message via its socket associated with connection retrieves the object.
4. HTTP server process tells TCP to close the TCP connection (But TCP doen't actually terminate the connection until it knows for sure that the client has received response message intact)
5. HTTP client receives the response message. TCP connection terminates. Message indicates an encapsulated object is an HTML file. The client extracts the file from the response message, examines the HTML file, and finds references to JPEG objects.
6. The first four steps are then repeated for each of the referenced JPEG objects.

Round trip time is the time it takes for a small packet to travel from client to server and then back to client



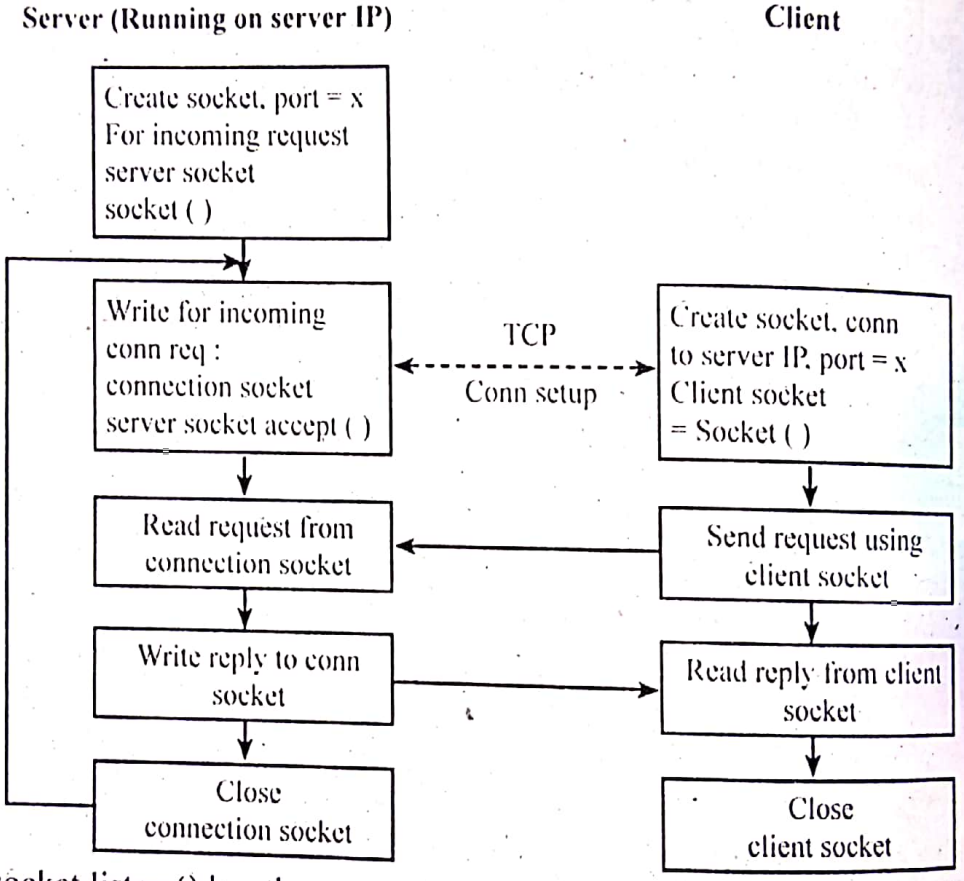
With persistent connections, server leaves the TCP connection open often sending a response. Sub request and responses between the same client and server can be sent over same connection.

There are two versions of persistent connection - without pipe lining and with pipe lining. For version without pipe lining client issues a new request only when the previous response has been received.

Default mode of HTTP uses persistent connections with pipe lining. With pipe lining, HTTP client issues a request as soon as it encounter a reference. Client can make back to back requests for referenced objects.

b. Define a socket. Describe the socket programming using TCP. **(08 Marks)**

Ans.



Server socket listen () has the server listen for TCP connection requests from client. The parameter specifies the maximum number of queered connection.

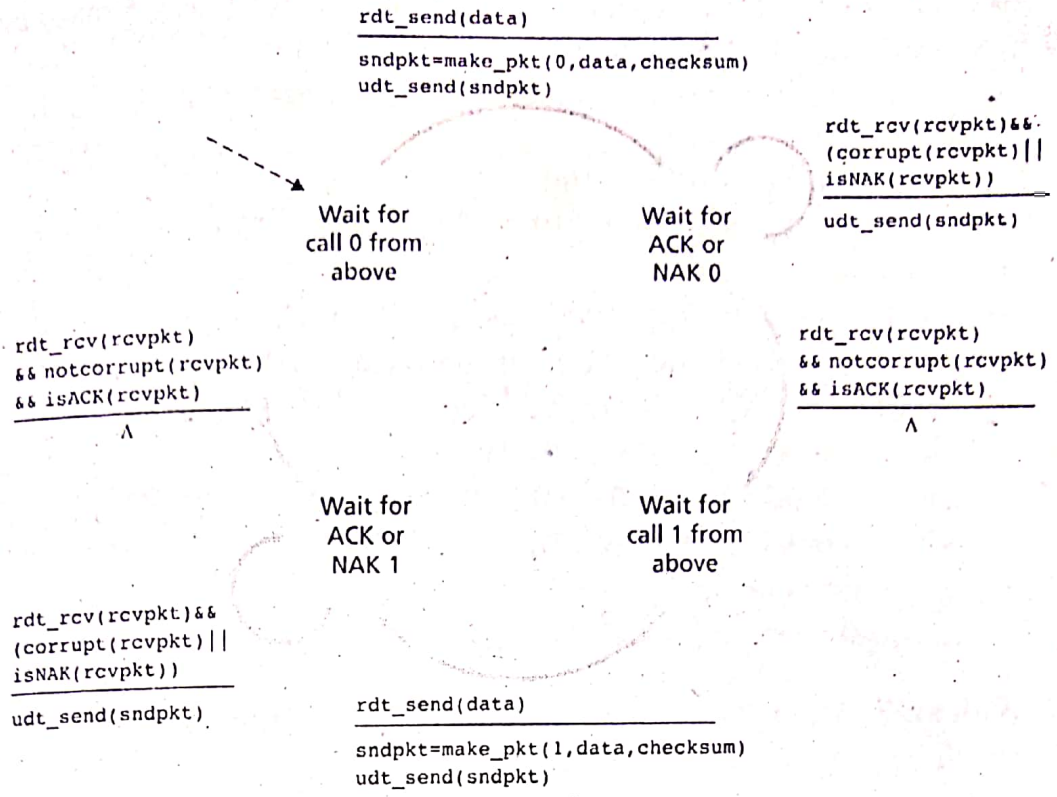
When a client knocks on the door, program invokes accept method for server socket, which creates a new socket in server, called connection socket, dedicated to this particular client. The client and server then complete handshaking creating a TCP connection between client socket and server connection socket.

Module-2

3. a. Draw and explain the FSM for sender and receiver side of rdt 2.1 protocol. **(08 Marks)**

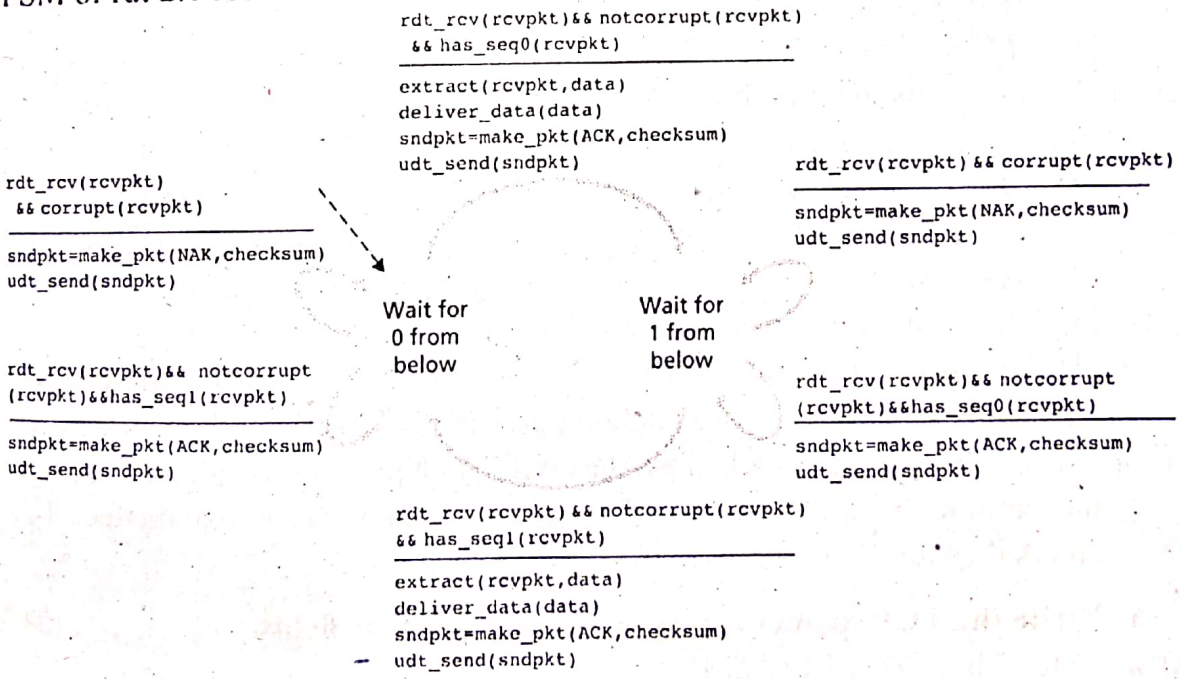
Ans. In rdt 2.1 there are more states because the protocol contains the packet currently being sent (by sender) or expected (at receiver) should have sequence number 0 or 1.

FSM of sender is shown below.



Protocol rdt 2.1 uses both positive and negative acknowledgements from the receiver to the sender. When an out of order packet is received, the receiver sends a positive acknowledgment for the packet is has received.

FSM of rdt 2.1 receives is shown below



b. Elaborate the three-way handshaking procedure used in TCP. (04 Marks)

Ans. Refer Q.No. 4.a. of Dec 18 / Jan 19

c. Suppose that 2 measured sample RTT values are 106 ms and 120 ms. Compute (i) Estimated RTT after each of these sample RTT value is obtained, Assume a

= 0.125 and estimated RTT is 100 ms just before first of the sample obtained. (ii) Compute DevRTT, Assume P = 0.25 and DevRTT was 5 msec before first of these samples are obtained.

Ans. (i) Estimated RTT = $(1 - \alpha)$. Estimated RTT _ α. Sample RTT **(04 Marks)**

(a) Sample RTT = 106ms

Estimated RTT = $(1 - 0.125). 100 \times 10^{-3} + 0.125 \times 106 \times 10^{-3}$

$= 0.875 . 100 \times 10^{-3} + 0.125 . 106 \times 10^{-3} = 10.75$ rms

(b) Sample rtt = 120ms

Estimated rtt = $(1 - 0.125) . 100 \times 10^{-3} + 0.125 \times 120 \times 10^{-3}$

$= 0.875 . 100 \times 10^{-3} + 0.125 \times 120 \times 10^{-3}$

(ii) Dev RTT = $(1 - \beta) .$ Dev rtt + $\beta |$ Sample rtt – Estimated RTT $|$

$= (1 - 0.25) . 5 \times 10^{-3} + 0.25 | 106 \times 10^{-3} - 100.75 \times 10^{-3} |$

$= 0.75 \times 5 \times 10^{-3} + 0.25 | 5.25 | \times 10^{-3}$

$= 3.75 + 0.3125 \times 10^{-3}$

$= 5.06$ ms

OR

4. a. With an FSM, explain the three phases of congestion control.

Ans. The three phases of congestion control are **(08 Marks)**

(1) Slow start phase

(2) Congestion avoidance phase

(3) Congestion detection phase

(1) Slow start phase :- When a TCP connection begins, value of congwin is initialized to 1 resulting an initial sending rate of roughly MSS/RTT.

Ex if MSS = 500 bytes and RTT = 200 msec, the resulting initial sending rate is only about 20 kbps. During the initial phase called slow start (SS) TCP sender begins by transmitting at a slow rate but increases its sending rate exponentially.

(2) Additive increase / multiplicative decrease :- It is also known as congestion avoidance. A TCP sender additively increases its rate when it per receiver that end of path is congestion free and multiplicatively decreases its rate when it detects (via a loss event) that the path is congested.

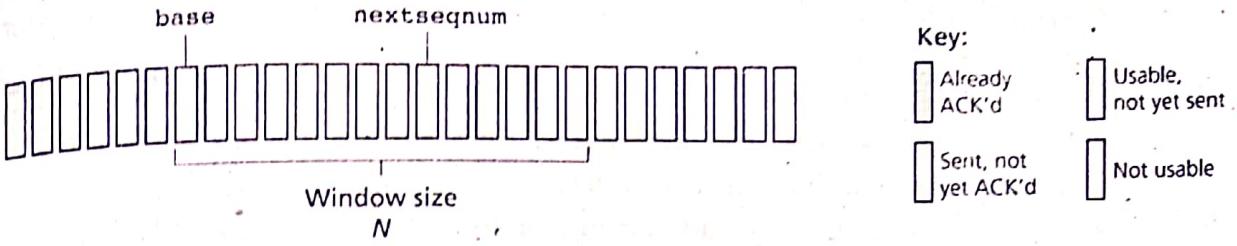
(3) Reaction to time out events :- This is congestion detection phase TCP manages more complex dynamics by maintaining a variable called threshold, which determined the window size at which slow start will end and congestion avoidance will begin. the variable threshold is set to a large value so that it has no initial effect. TCP sender enters the slow start phase after a timeout event.

b. Write the TCP segment structure and explain its fields.

Ans. Refer 3.b. of Dec 18 / Jan 19 **(04 Marks)**

c. Elaborate the working of Go-Back N protocol.

Ans. In Go-back-N protocol, the sender is allowed to transmit multiple packets (When available) without waiting for an acknowledgment, and is constrained to have no more than some maximum allowable number N, of unacknowledged packets in pipeline. **(04 Marks)**

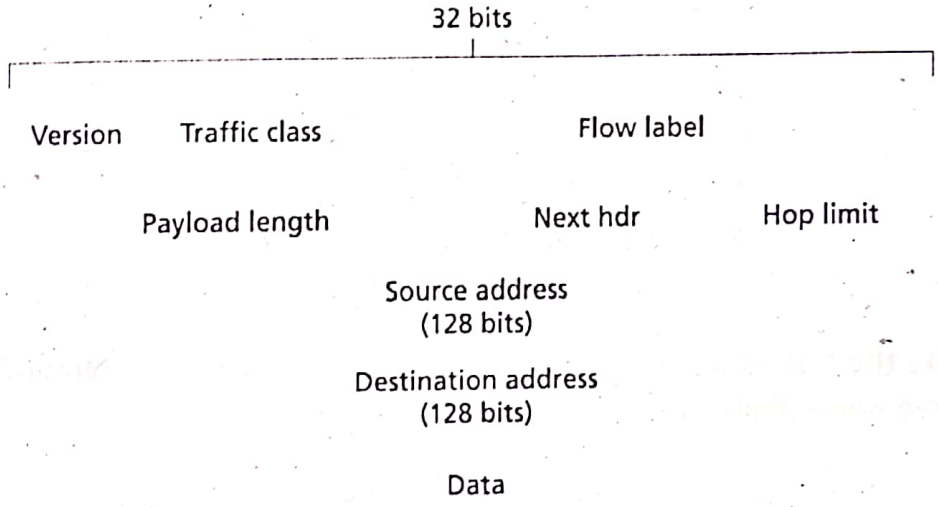


As the protocol operates, the windows slides forward [ ] - Not usable over the sequence number. N is refereed as the window size and GBN protocol as sliding window protocol. A packet's sequence number is carried in a fixed-length field in the packet header. If k is the number of bits in the packet sequence number field, the range of sequence numbers is thus [0,2k – 1].Sequence number in the interval (0, base-1) correspond to packets that have already been transmitted and acknowledged. Interval [base, next sequence - 1] correspond to the packets that have been sent but not yet acknowledged. Sequence numbers in the interval [next sequence, base+N–1] can be used for packets that can be sent immediately.

Module-3

5. a. **Give the format of IPV6 datagram and explain the fields.** **(06 Marks)**

Ans.



- **Expanded addressing capabilities.** IPv6 increases the size of the IP address from 32 to 128 bits and it has streamlined 40 byte header.
- **Flow labeling and priority.** IPV6 has an state that allows labeling of packets belonging to particular flows
- **Version.** This 4-bit field identifies the IP version number.
- **Traffic class.** This 8-bit field is similar to type of service.
- **Flow label.** is used to identify a flow of datagrams and is 20 bits
- **Payload length.** Is a 16-bit value i.e., an unsigned integer giving the number of bytes in the IPv6 datagram following the fixed-length, 40-byte datagram header.
- **Next header.** identifies the protocol to which the contents of this datagram will be delivered

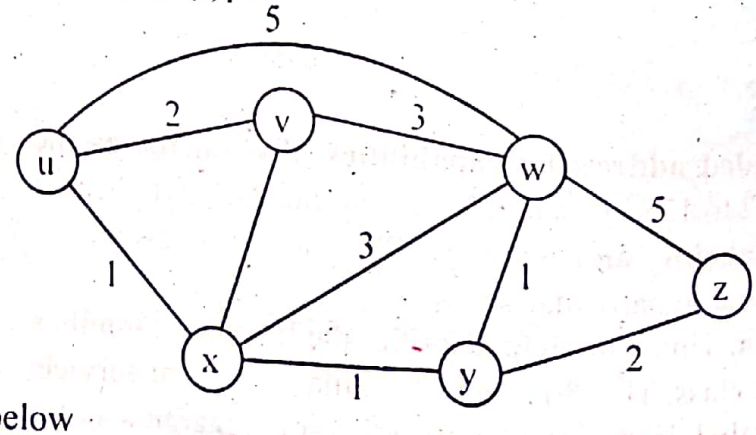
- **Hop limit.** The contents of this field are decremented by one by each router that forwards the datagram. If the hop limit counter reaches zero, the datagram is discarded.
- **Source and destination addresses.** The various formats of the IPv6 128-bit address are described in RFC 4291.
- **Data.** This is the payload portion of the IPv6 datagram. When the datagram reaches its destination, the payload will be removed from the IPV6 datagram and passed on to the protocol specified in the next header field.

b. What are the message types used in IGMP? (03 Marks)

Ans.

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

c. Write the link state routing algorithm and apply it to the following graph with source node [Refer Fig.Q5(c)] is (07 Marks)



Ans. The algo is as below

1. Initialization:
2. $N' = \{u\}$
3. for all nodes v
4. if v is a neighbor of u

5. then D(v) = c(u,v)
6. else D(v) = ∞
7
8. Loop
9. find w not in N' such that D(w) is a minimum
10. add w to N'
11. update D(v) for each neighbor v of w and not in N':
12. D(v) = min(D(v), D(w) + c(w,v))
13. /* new cost to v is either old cost to v or known least path cost to v plus cost from w to v */
14. until N' = N

- In the initialization step, the currently known least-cost paths from u to its directly attached neighbors, v, x, and w.
- In the first iteration, we look among those nodes not yet added to the set N' and find that node with the least cost as of the end of the previous iteration.
- In the second iteration, nodes v and y are found to have the least-cost path. The cost to the remaining nodes not yet in N' i.e., nodes v, w and z are updated via line 12 of the algorithm.

Step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

OR

6. a. What is routing? Write the structure of a router. **(07 Marks)**

Ans. Refer Q.No. 5.a. of Dec 18 / Jan 19

b. List the broadcast routing algorithms? Explain any one of them. **(04 Marks)**

Ans. The broadcast algorithms are

(1) Uncontrolled flooding
(2) Controlled flooding
(3) Spanning tree broadcast

Uncontrolled flooding :- The source node sends a copy of the packet to all of its neighbors. When a node receives a broadcast packet, it duplicates the packet and forwards it to all of its neighbors. If the graph is connected, this scheme will eventually deliver a copy of the broadcast packet to all nodes in the graph. This simple scenario results in the endless cycling of two broadcast packets, one clockwise, and one counterclockwise. This broadcast storm, resulting from the endless multiplication of broadcast packets. The most obvious technique for achieving broadcast is flooding approach. In that two floodings types are there uncontrolled and controlled.

c. Describe the intra-AS routing protocols in detail **(05 Marks)**

Ans. Thre are two intra-AS routing protocols routing information protocol (RIP) and open shortest path first (OSPF). In RIP routing updates are enchanged between neighbours approximately every 30 seconds using a RIP response message. The response message sent by a router or a host contains a list upto 25 destination subnets within an AS, and senders distance to each of those subnets. Response messages are also known as RIP advertisements. RIP is a distance vectors protocol and version is specified in RFC 1058. RIP uses term hop which is the number of subnets traversed along the shortest path from source router to destination.

OSPF is a links state protocol that uses flooding of link state information. With OSPF, a router constructs a complete topological map (graph) of the entire autonomous system. The router then locally run Dijsktra's shortest path algorithm to determine a shortest path tree to all subnets. A router broadcasts routing information to all other routers in the autonomous system and also to its neighbouring routers. A router broadcasts link state information whenever there is a change in a link's state.

Module-4

7. a. Illustrate the two different approaches for routing to a mobile node. (08 Marks)

Ans. The two different approaches are (a) Indirect routing (b) Direct routing

(a) Indirect routing

The correspondent simply addresses the datagram to the mobile node's permanent address and sends the datagram into the network. Home agent responsible for interacting with a foreign agent to track the mobile node's COA. Its second job is to be on the lookout for arriving datagrams addressed to nodes whose home network is that of the home agent but currently resident in a foreign network.

The home agent intercepts these datagrams and then forwards in two-step process. The datagram is first forwarded to the foreign agent, using the mobile node's COA (Case of address) and then forwarded from the foreign agent to the mobile node

Indirect - routing provides following functions

(a) A mobile node to foreign agent protocol.

(b) A foreign agent to home agent registration protocol.

(c) A home agent datagram encapsulation protocol.

(d) A foreign agent decapsulation protocol.

(b) Direct routing to mobile node

In the direct routing approach, a correspondent agent in the correspondent's network first learns the COA of the mobile node. This can be done by having the correspondent agent query the home agent the mobile node has an up-to-date value for its COA registered with its correspondent agent. Two additional challenges are

(1) mobile-user location protocol

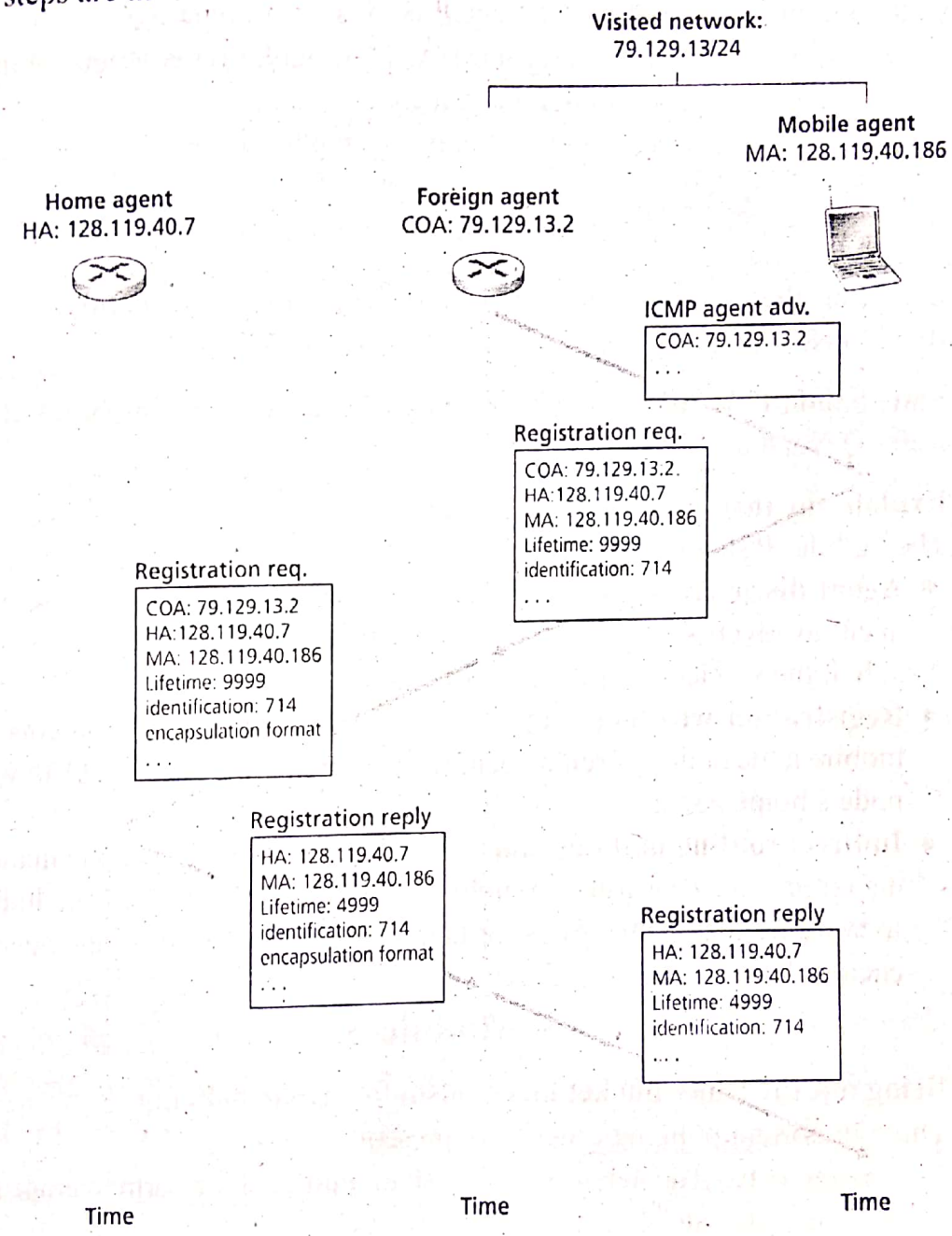
(2) When the mobile node moves from one foreign network to another, how will data now be forwarded to the new foreign network

Solution is to find the anchor foreign agent. When the mobile node moves to a new foreign network, the mobile node registers with the new foreign agent, and the new

foreign agent provides the anchor foreign agent with the mobile node's new COA). When the anchor foreign agent receives an encapsulated datagram for a departed mobile node, it can then re-encapsulate the datagram and forward it to the mobile node using the new COA. If the mobile node later moves yet again to a new foreign network, the foreign agent in that new visited network would then contact the anchor foreign agent in order to set up forwarding to this new foreign network.

b. With a neat diagram, bring out the steps for mobile node registration to home agent. **(08 Marks)**

Ans. Four steps are involved



1. Following the receipt of foreign agent advertisement, a mobile node sends a mobile IP registration message to the foreign agent. The registration message is carried within a UDP datagram and sent to port 434. The registration agent carries a COA advertised by the foreign agent, the address of the home agent, the

permanent address of the mobile node (MA), the requested lifetime of registration, and a 64-bit registration identification.

2. The foreign agent receives the registration message and records the mobile node's permanent IP address. The foreign agent now knows that it should be looking for datagrams containing an encapsulated datagram whose destination address matches the permanent address of the mobile node.
3. The home agent receives the registration request and checks for authenticity and correctness. The home agent binds the mobile node's permanent IP address with the COA. In future, datagrams arriving at the home agent and addressed to the mobile node will now be encapsulated. The home agent sends a mobile IP registration reply containing the HA, MA, actual registration lifetime, and the registration identification of the request.
4. The foreign agent receives the registration reply and then forwards it to the mobile node.

OR

8. a. Bring out the components of 3G Cellular Network architecture. **(08 Marks)**

Ans. Refer Q.No. 7.a. of Dec 18 / Jan 19

b. State handoff? What are the steps involved in accomplishing handoff. **(05 Marks)**

Ans. Refer Q.No. 8.a. of Dec 18 / Jan 19

c. Explain the three phases of mobile IP. **(03 Marks)**

Ans. The mobile IP standard consists of three main pieces

- **Agent discovery** - Mobile IP defines the protocols used by a home or foreign agent to advertise its services to mobile nodes, and protocols for mobile nodes to solicit the services of a foreign or home agent.
- **Registration with home agent** - Mobile IP defines the protocols used by the mobile node and/or foreign agent to register and deregister COAs with a mobile node's home agent.
- **Indirect routing of datagrams** - The standard also defines the manner in which datagrams are forwarded to mobile nodes by a home agent, including rules for forwarding datagrams, rules for handling error conditions, and several forms of encapsulation.

Module-5

9. a. Bring out the leaky bucket mechanism for traffic policing. **(07 Marks)**

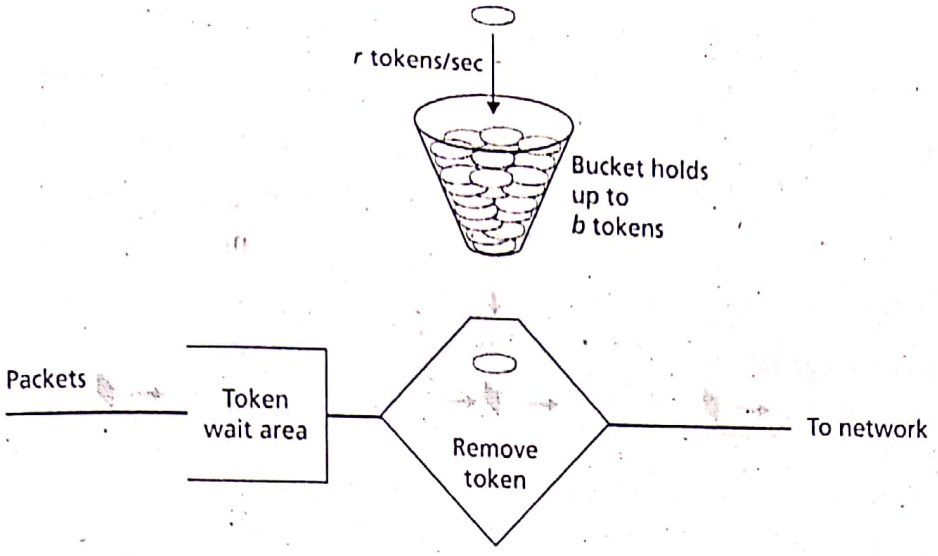
Ans. Three important policing criteria are present

1) Average rate - The network may wish to limit the long-term average rate at which a flow's packets can be sent into the network.

2) Peak rate - Peak rate constraint limits the maximum number of packets that can be sent over a shorter period of time.

3) Burst size - The network may wish to limit the maximum number of packets that can be sent into the network over an extremely short interval of time

The leaky bucket mechanism is an abstraction that can be used to characterized these policing limits



Suppose that before a packet is transmitted into the network, it must first remove a token from the token bucket. If the token bucket is empty, the packet must wait for a token. These can be atmost b tokens in the bucket, minimum burst size for a leaky bucket period flow is b packets. Because the token generation rate is r, maximum number of packets that can enter the network of any interval of time length t is rtt+5. Thus, token generation rate, r serves to limit the long - term average rate at which packets can enter the network. Two leaky bucket can be used to police a flow's peak rate in addition to the long term average rate.

b. Classify the multimedia network applications. **(03 Marks)**

Ans. These are three classes of multimedia applications

(1) Streaming stored audio/video - Client requests on demand compressed audio or video files that are stored on servers.

(2) Streaming - In streaming stored audio/video application, a client typically begins playout of the audio/video a few seconds after it begins receiving the file from the server.

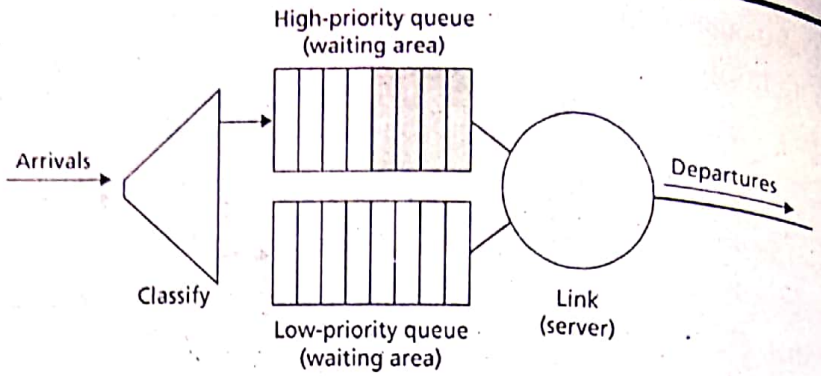
(3) Real time interaction audio/video - This allows people to use audio/video to communicate with each other in real time. Real time interactive audio is often referred to as internet phone.

c. Describe the link scheduling mechanisms. **(06 Marks)**

Ans. Following are the scheduling mechanisms

(1) First in First out - Packets arriving at the link output queue wait for transmission if the link is currently busy transmitting another packet. If there is not sufficient buffering space to hold the arriving packet, the queue's packet-discarding policy then determines whether the packet will be dropped (lost) or whether other packets will be removed. It is first come first serve basis.

(2) Priority queuing - Packets arriving at the output link are classified into priority classes at the output queue, as shown in Figure



A packets priority class may depend on an enplicity masking that it carries in packet header, its source or destination IP address its destination post number ot other criteria.

(3) Round Robin and Weighted fair queuing (WFQ)

Under the round robin queuing discipline, packets are sorted into classes as with priority queuing. A class 1 packet is transmitted, followed by a class 2 packet, followed by a class 1 packet, followed by a class 2 packet, and so on. A work serving round robin discipline looks for a packet of a given class but finds none will immediately check the next class in round robin sequence.

A generalized abstraction of round robin queuing is weighted for queuing. Arriving packets are classified and queued in the appropriate per clan waiting area. A WFQ scheduler will serve classes in a circular manner first serving class 1 then serving class 2. WFQ will immediately move on to the next class in the service sequence when it finds an empty class queue.

OR

10. a. List the categories of streaming stored video. Explain any one of them.(08 Marks)

Ans. The categories of stores video are

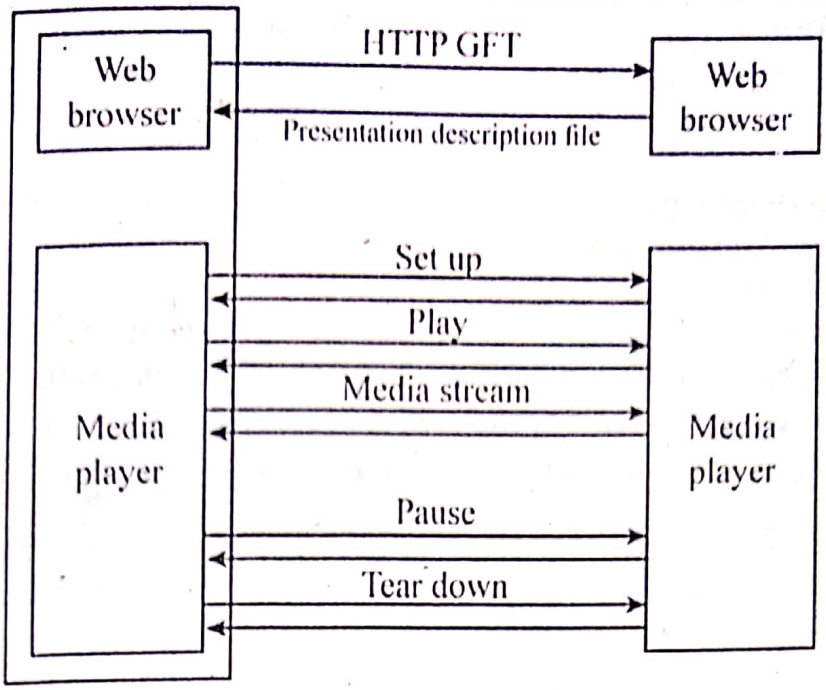
(1) Accessing video through a web server

(2) Sending multimedia from a streaming server to a helper application

(3) Real time streaming protocol

Real time streaming protocol allows a media player to control the transmission of media stream. Control actions include pause/resume, repositioning of playback, fast forward and rewind. RTSP is an out of band protocol. RTSP message are sent out of band where as media stream, whose packet is not defined by RTSP is considered "in-band". RTSP messages use a different port no 544 from media stream.

The web browser first requests a presentation description file from a web server. Each reference to the continues media file begins with URL method RTSP II.



The web server encapsulates the presentation description file in an HTTP response message and sends the messages to the browser. When the browser receives the HTTP response message, the browser involves a media player based on content type field of the message. The presentation description file includes references to media stream using URL method rtsp 11. The player and the server then send each other a series of RTSP messages. The player sends an RTSP SETUP PLAY request and server responds with RTSP ok message. When the uses is finished, media player sends an RTSP TEAR DOWN request and the server confirms with RTSP ok response.

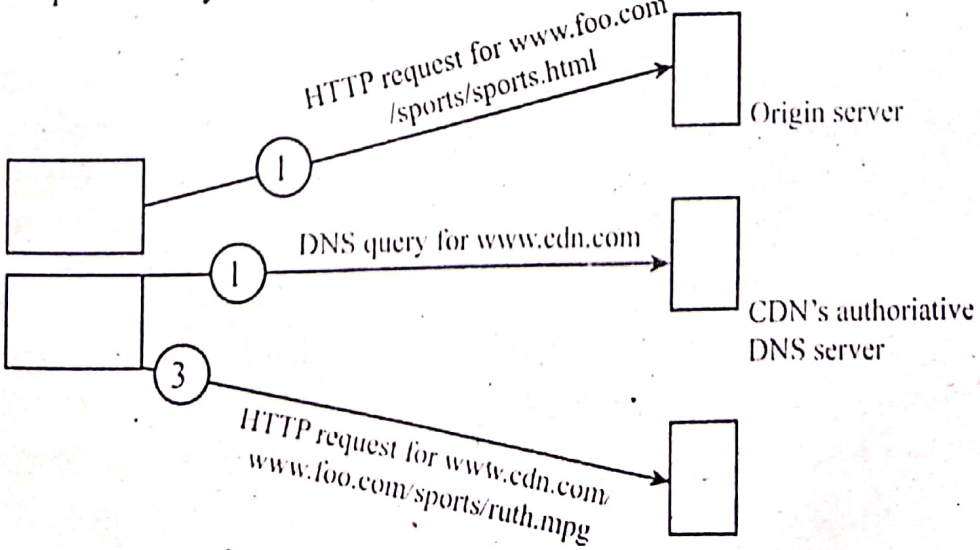
b. Explain the working of CDN. **(08 Marks)**

Ans. A CDN company typically provides its content distribution services as follows.

1) The CDN company installs hundreds of CDN servers throughout the internet. CDN servers are placed in data center.

2) The CDN replicates its customer's content in CDN server, whenever a customer updates its content, CDN redistributes the fresh content to CDN servers.

3) CDN Company provides a mechanism so that when a client requests content, the content is provided by CDN server that can but deliver content to specific client.



(1) The browser sends its request for base HTML object to origin server. www.foo.com which sends requested HTML object to the browse. The browser passes the HTML file and finds reference to http : \\www.cdn.com\www.foo.com/sports/ruth.mpg

(2) The browser then does a DNS lookup on www.cdn.com with is the host name for referenced URL. DNS is configured so that all queries about www.cdn.com that arrive to root DNS server are sent to an authoritative DNS server receives the query. it entracts IP address of requesting browser.

(3) DNS in the requesting client receives a DNS reply with the IP address. The browser then sends in HTTP request to CDN server with that IP address. The browser obtains ruth.mpg from this CDN server. For subsequent requests from www.CDN.com, the client continues to use the same CDN server since the IP address for www.CDN.com is in the DNS cache.