Msbte-w22-22520 - Exam paper

Computer Engineering (University of Mumbai)

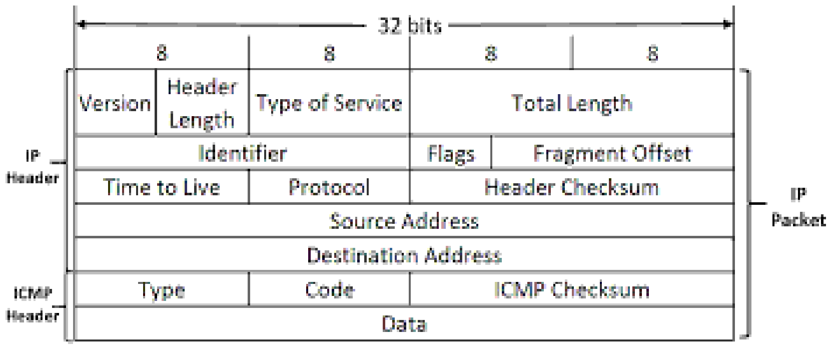
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2022 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code** **22520**

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills.
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for anyequivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.
8) As per the policy decision of Maharashtra State Government, teaching in English/Marathi and Bilingual (English + Marathi) medium is introduced at first year of AICTE diploma Programme from academic year 2021-2022. Hence if the students in first year (first and second semesters) write answers in Marathi or bilingual language (English +Marathi), the Examiner shall consider the same and assess the answer based on matching of concepts with model answer.

Q. No	Sub Q.N.	Answer	Marking Scheme
1.	 **a)** **Ans.**	**Attempt any FIVE of the following:** **Draw and label sketch of ICMPV4 packet format.** **ICMPV4 packet format** 	**10** **2M** ***Correct labelled diagram 2M***

b) **State the importance of IPV6 and IPC4.** **2M**

Ans. **Importance of IPV6 over IPV4 (any two)**

Any two points 1M each for relevant contents

i) huge number of IP addresses:

IPv6 has 128-bit addresses when compared to 32-bit addresses of IPv4 which results in a very large increase in the availability of IP addresses and creates a lot of advantages.

ii) End to End Connectivity:

IPv6 eliminates the need for NAT which results in better connectivity in peer-peer networks.

iii) Interoperability:

IPv6 promotes interoperability between different IPv6 implementations.

iv) Built-in Security: IPv6 provides authentication and encryption.

c) **Distinguish between SMTP and POP3 protocol (Any two points)** **2M**

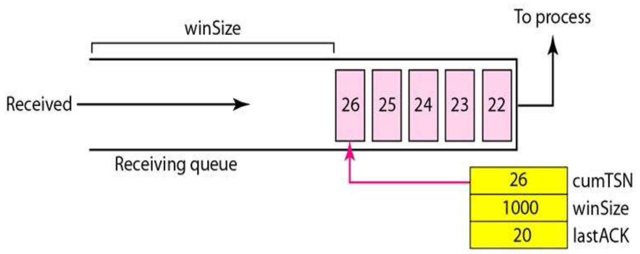
Ans.

Any two points 1M each for relevant contents

Parameter	SMTP	POP3
Full form	Simple Mail Transfer Protocol (SMTP).	Post Office Protocol 3 (POP 3)
Designed	SMTP is designed for sending the mails.	POP3 has been designed for receiving the mails.
Implementation	SMTP is implemented technically and physically on port number 25 of the system.	POP3 is implemented on port number 110.
Known as	SMTP is also known as the PUSH protocol.	POP3 is also known as POP protocol
Type	SMTP acts as a MTA (Message Transfer Agent) for sending the message to the receiver.	POP3 is a MAA (Message Access Agent) for accessing the messages from mailboxes.

Target Usage	SMTP transfers the mail from the sender's computer to the mailbox present on the receiver's mail server.	POP3 allows you to retrieve and organize mail from the mailbox on the receiver mail server to the receiver's computer.

	d) **Ans.**	**What is UDP? Which services are provided by UDP (Any two)?** **UDP(User Datagram Protocol):** UDP is a simple, datagram-oriented, transport layer protocol. It involves a minimum amount of communication mechanisms. It is a connectionless, reliable protocol. **UDP Services:** 1. Process-to-Process Communication: - UDP provides process-to-process communication using socket addresses, a combination of IP addresses and port numbers. 2. Connectionless Service: - UDP provides a connectionless service, i.e. each user datagram sent by UDP is an independent datagram. 3. UDP provides no flow control. 4. UDP does not provides no error control. 5. UDP does not provide congestion control. 6. UDP protocol encapsulates and decapsulates messages.	**2M** ***Definition 1M*** ***Any two services 1M***
	e) **Ans.**	**State importance of Routing table.** **Importance of Routing table** • Routing tables are essential in the routing because they maintain a map of connected networks, which ensures that the process of forwarding packets is as efficient as possible. • Without the presence of routing tables, routers would have no idea how to get packets to their intended destinations.	**2M** ***Correct explanation 2M***
	f) **Ans.**	**State the use of Telnet.** Followings are some of the uses of Telnet • TELNET is used to connect remote computers and issue commands on those computers. • It is used as a standard TCP/IP protocol for virtual terminal service which is given by ISO. • Telnet can be used to test or troubleshoot remote web or mail servers, as well as trusted internal networks.	**2M** ***Any two uses 1M each***

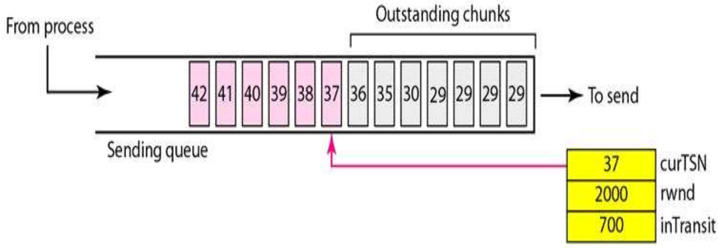
	g) Ans.	**State the concept of fragmentation in IPV4.** **The concept of fragmentation in IPV4** Fragmentation: When the maximum size of datagram is greater than maximum size of data that can be held a frame then the network layer divides the datagram received from x-port layer into fragments. **OR** Fragmentation is the division of an IP datagram into smaller units. After fragmentation, each fragment will have its own header with few fields changed and few fields remaining the same. **OR** In fragmentation, a datagram is divided into smaller units. Most of the fields of the original header are copied into the fragment header. The three fields' Flags, Fragmentation offset and Total length are altered	**2M** ***Correct concept 2M*** ***Example given as fragmentation may be considered***
2.	 a) Ans.	**Attempt any <ins>THREE</ins> of the following:** **Describe flow control under SCTP.** ***(Any other relevant explanation or example can be considered)*** **Flow control under SCTP** Flow control in SCTP is similar to that in TCP. Like TCP, SCTP executes flow control to prevent overwhelming the receiver. In SCTP, we need to handle two units of data, the byte and the chunk. The values of rwnd and cwnd are expressed in bytes; the values of TSN and acknowledgments are expressed in chunks. Current SCTP implementations still use a byte-oriented window for flow control. **Receiver Site:** The receiver has one buffer (queue) and three variables. The queue holds the received data chunks that have not yet been read by the process. The first variable holds the last TSN received,cumTSN. The second variable holds the available buffer size; winsize. The third variable holds the last accumulative acknowledgment, lastACK. The following figure shows the queue and variables at the receiver site.  winSize To process Received 26 25 24 23 22 Receiving queue 26 cumTSN 1000 winSize 20 lastACK	**12** **4M** ***Relevant Explanation of receiver 2M*** ***Relevant Explanation of sender 2M***

1. When the site receives a data chunk, it stores it at the end of the buffer (queue) and subtracts the size of the chunk from winSize. The TSN number of the chunk is stored in the cumTSN variable.
2. When the process reads a chunk, it removes it from the queue and adds the size of the removed chunk to winSize (recycling).
3. When the receiver decides to send a SACK, it checks the value of lastAck; if it is less than cumTSN, it sends a SACK with a cumulative TSN number equal to the cumTSN. It also includes the value of winSize as the advertised window size.

Sender Site:

The sender has one buffer (queue) and three variables: curTSN, rwnd, and inTransit, as shown in the following figure. We assume each chunk is 100 bytes long.

The buffer holds the chunks produced by the process that either have been sent or are ready to be sent. The first variable, curTSN, refers to the next chunk to be sent. All chunks in the queue with a TSN less than this value have been sent, but not acknowledged; they are outstanding. The second variable, rwnd, holds the last value advertised by the receiver (in bytes). The third variable, inTransit, holds the number of bytes in transit, bytes sent but not yet acknowledged. The following is the procedure used by the sender.



1. A chunk pointed to by curTSN can be sent if the size of the data is less than or equal to the quantity rwnd - inTransit. After sending the chunk, the value of curTSN is incremented by 1 and now points to the next chunk to be sent. The value of inTransit is incremented by the size of the data in the transmitted chunk.

2. When a SACK is received, the chunks with a TSN less than or equal to the cumulative TSN in the SACK are removed from the queue and discarded. The sender does not have to worry about them anymore.

		The value of inTransit is reduced by the total size of the discarded chunks. The value of rwnd is updated with the value of the advertised window in the SACK.	
	b) Ans.	**What is Mobile IP? List and explain components of Mobile IP.** **Mobile IP:** Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without the user's sessions or connections being dropped. Mobile IP is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. **Components of Mobile IP** **1. Mobile Node(MN): -** Mobile Node (MN) is the hand-held communication device that the user carries. There are devices such as cell phones, PDA or laptops whose software enables network roaming capabilities. **2. Home Agent (HA): -** It is a router on the home network serving as the anchor point for communication with mobile nodes. It tunnels packet from a device on internet, called a correspondent node to a roaming mobile node. **3. Foreign Agent (FA): -** It is a router that may function as the point of attachment for MN when it roams to a foreign network delivering packets from the Home agent to mobile nodes. **4. Correspondent Node (CN): -** Correspondent Node (CN) is a device on the internet communicating to the mobile node. End host to which MN is corresponding (e.g. web server).	**4M** ***Definition 1M*** ***Listing 1M*** ***Explanation 2M for relevant contents***
	c) Ans.	**Describe DHCP with its operation and static and dynamic allocation** ***(Any relevant explanation can be considered)*** DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP. **Working of DHCP:** In a network, a DHCP server manages a pool of IP addresses, as well as default gateway details, DNS details and other information for the clients' network configuration. When a new computer is introduced	**4M** ***DHCP Operation 2M*** ***Static allocation 1M***

		into a DHCP server-enabled network, it will send a query to the DHCP server requesting all the necessary information. When the query reaches the DHCP server, it will grant the new computer a new IP address and a lease - a time frame for which the computer can use this IP address, as well as other configuration details. The whole process takes place immediately after the new computer boots, and to be successful, it has to be completed before initiating IP based communication with other hosts in the network. **Dynamic allocation** When the DHCP server is configured to use dynamic allocation, this means that it uses a lease policy. This way, when an assigned IP address from the available pool is no longer used, it will be transferred back to the pool, making it available for someone else to use. The advantage of this method is that the IP addresses are used to their maximum - as soon as they are no longer used by the client, they are instantly made available to others. The disadvantage of this method is that a client will always have a random IP address. **Static allocation** The static allocation method is very popular in modern ISP networks, which do not use dial-up methods. With the static allocation, the DHCP sever keeps a database with all clients' LAN MAC addresses and gives them an IP address only if their MAC address is in the database. This way, the clients can be sure that they will be getting the same IP address every time. A DHCP server can be set to work using a combination of the allocation methods. For example, in a public Wi-Fi network, all of the known hosts and permanent clients can use the static allocation, whereas for guests, the dynamic allocation is used. This way, known hosts can always use the same IP address and the IP address pool is equally available to everyone.	***Dynamic allocation 1M***
	d) **Ans.**	**Give use of OSPF with its reason.** **Following are the uses of OSPF with its reason** • Link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements.	**4M** ***Any four uses with reasons 1M each***

		- To handle routing efficiently and on time, this protocol divides an autonomous system into areas. - As the name suggested "shortest path first", OSPF calculates the shortest route to a destination through the network based on an algorithm. It uses the Dijkstra algorithm for calculating the shortest path. - Authentication type: There are two types of authentications, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for password that specifies the password-based authentication. - Area identification: It defines the area within which the routing takes place.	
3.	a) **Ans.**	**Attempt any <u>THREE</u> of the following:** **State significance of following related to IPV6** - **Auto configuration** - **Renumbering** **1. Auto Configuration:** Nodes can connect to a network and automatically generate global IPv6 addresses without the need for manual configuration or help of a server, such as a Dynamic Host Configuration Protocol (DHCP) server. **-When a host in IPv6 joins a network, it can configure itself using the following process:** - **Generate a link local address:** The device generates a link local address, which has 10 bits link local prefix (1111 1110 10), followed by 54 zeros, and followed by the 64-bit interface identifier, which any host knows how to generate it from its interface card. The result is a 128-bit link local address. - **Test the uniqueness of a link local address:** The node tests to make sure that the link local address that it generates is not already in use on the local network. The node sends a neighbour solicitation message by using the ND (Neighbour Discovery) protocol. In response, the local network listens for a neighbour advertisement message, which indicates that another device is already using the link-local address. If so, either a new link local address must be generated or auto-configuration fails, and another method must be used.	**12** **4M** ***Explanation of Auto configuration 2M*** ***Explanation of Renumbering 2M*** ***Any relevant explanation can be considered***

- **Assign a link local address:**

If the device passes the uniqueness test, the device assigns the link-local address to its IP interface. The link-local address can be used for communication on the local network but not over the Internet.

- **Contact the router:**

The node tries to contact a local router for more information about continuing the configuration. This contact is performed either by listening for router advertisement messages sent periodically by the routers or by sending a specific router solicitation message to ask a router for information about what to do next.

- **Provide direction to the node:**

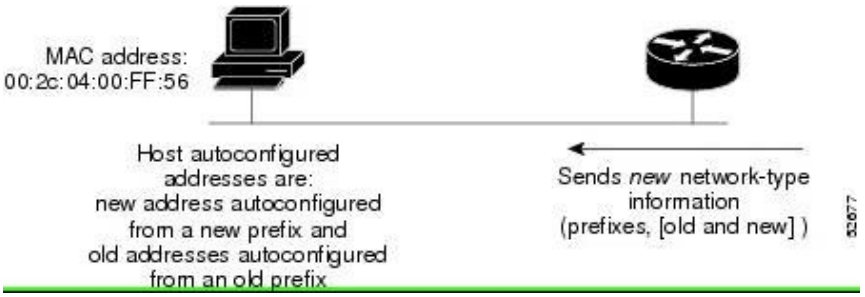
The router provides direction to the node about how to proceed with auto-configuration. Alternatively, the router tells the host how to determine the global Internet address.

- **Configure the global address:**

The host configures itself with its globally unique Internet address. This address is generally formed from a network prefix provided to the host by the router.

2. Renumbering:

To allow sites to change the service provider, renumbering of the address prefix (n) was built into IPv6 addressing. Each site is given a prefix by the service provider to which it is connected. If the site changes the provider, the address prefix needs to be changed.


MAC address:
00:2c:04:00:FF:56
Host autoconfigured addresses are: new address autoconfigured from a new prefix and old addresses autoconfigured from an old prefix
Sends *new* network-type information (prefixes, [old and new])
52677

A router to which the site is connected can advertise a new prefix and let the site use the old prefix for a short time before disabling it. In other words, during the transition period, a site has two prefixes.

The main problem in using the renumbering mechanism is the support of the DNS, which needs to propagate the new addressing associated with a domain name.

b) Ans. **Draw and explain TCP segment structure.** **4M**

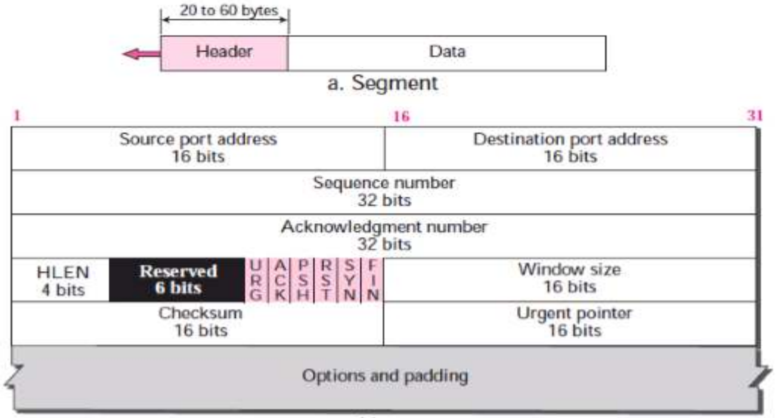
TCP is a reliable connection- oriented protocol i.e., connection is established between the sender and receiver before the data can be transmitted.

A Packet in TCP is called a segment. TCP segment consists of data bytes to be sent and a header that is added to the data by TCP as shown in following figure.

Diagram 1M

Explanation 3M

Any other relevant explanation shall be considered



The header of TCP segment can range from 20-60 bytes.40 bytes are for option. if there are no options, header is of 20 bytes else it can be of upmost 60 bytes.

Header Fields in TCP Segment Structure:

1) Source port address: -

This is a 16-bit field that defines the port number of the application program in the host that is sending the segment. This serves the same purpose as the source port address in the UDP header.

2) Destination port address: -

This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. This serves the same purpose as the destination port address in the UDP header.

3) Sequence Number: -

This 32-bit field defines the number assigned to the first byte of data contained in this segment. As we said before, TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a random number generator to create an initial sequence number (ISN), which is usually different in each direction.

4) Acknowledgment Number: -

This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number x from the other party, it defines x + 1 as the acknowledgment number. Acknowledgment and data can be piggybacked together.

5) Header length: -

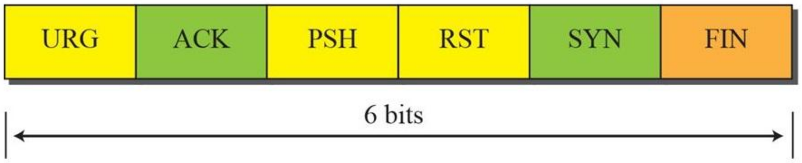
This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 (5 x 4 = 20) and 15 (15 x 4 = 60).

6) Reserved:-

This is a 6-bit field reserved for future use.

7) Control Field:-

This field defines 6 different control bits or flags. These are 6, 1 bit control bits that controls connection establishment, connection termination, connection abortion, flow control, mode of transfer etc.



The function of control fields in TCP are:
URG: Urgent pointer is valid.
PSH: Request for push.
RST: Reset the connection.
SYN: Synchronize sequence numbers.
FIN: Terminate the connection.

8) Window Size: This field tells the window size of the sending TCP in bytes.

9) Checksum: This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

10) Urgent Pointer: This field (valid only if the URG control flag is set) used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

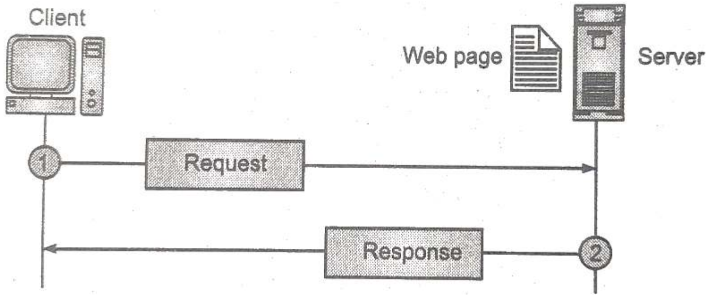
11) Options: There can be up to 40 bytes of optional information in the TCP header.

c) **With the help of Diagram, explain architecture of WWW.** **4M**

Ans. The WWW (World Wide Web) is a way of exchanging information between computers on the Internet.
WWW works on client server architecture, in which a client using a browser can access a service using a server.
Today, the WWW is a distributed client server service. The service provided is distributed over many locations called sites and each site holds one or more documents i.e., Web pages.

Diagram 2M

Explanation 2M



Client sends a request through its browser to the server using HTTP protocol which specifies the way the browser and web server communicates.

Then server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.

Now the browser receives the web page, it interprets it and display the contents of web page in web browser's window.

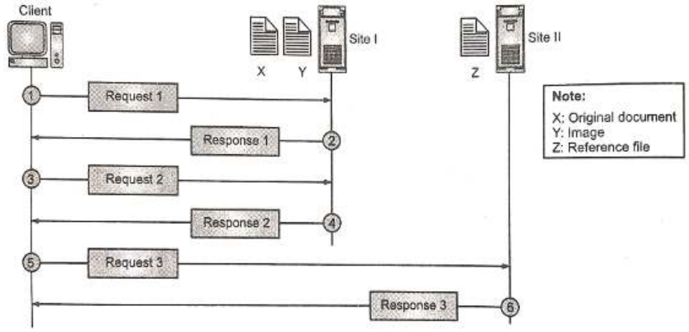


Fig. shows how WWW works.

The main web document and the image are stored in two separate files in the same site (file X and file Y) and the referenced text file is stored in another site (file Z).

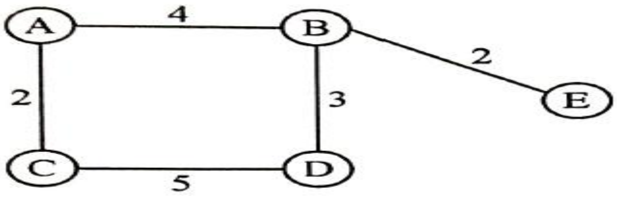
Since, we are dealing with three different files, (namely, X, Y and Z) we need three transactions if we want to see the whole document. The first transaction (request/response) retrieves a copy of the main document (file X), which has a reference (pointer) to the second and the third files.

When a copy of the main document is retrieved and browsed, the user can click on the reference to The image to invoke the second transaction and retrieve a copy of the image (file Y).

if the user further needs to see the contents of the referenced text file, she can click on its reference pointer) invoking the third transaction and retrieving a copy of the file Z.

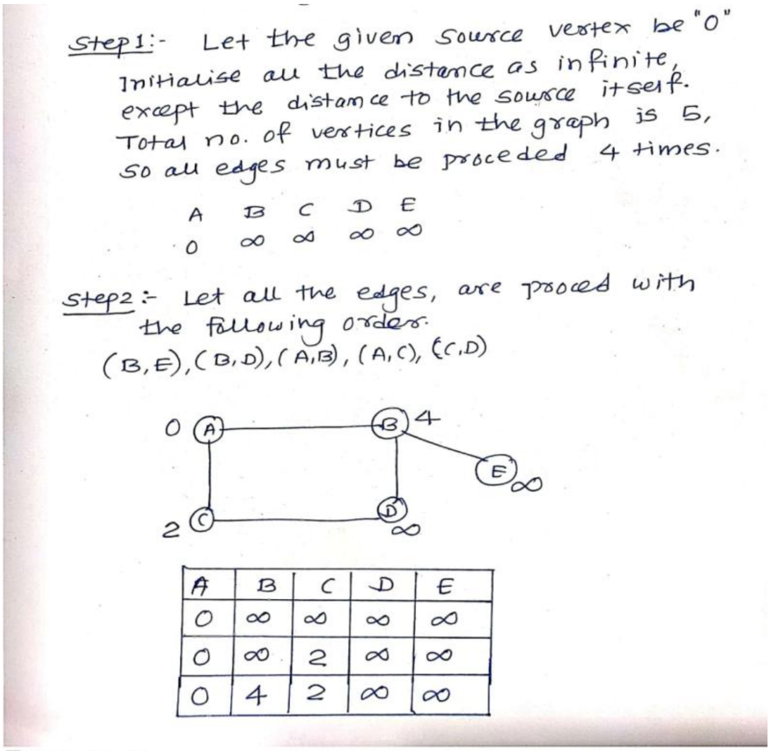
Note that although file x and y both are stored in site x, they are independent files with different names and addresses. Two transactions are needed to retrieve them.

d) **Use Bellman-ford algorithm to find the shortest distance for all node in the graph.** **4M**



Ans.

For each correct step 1M

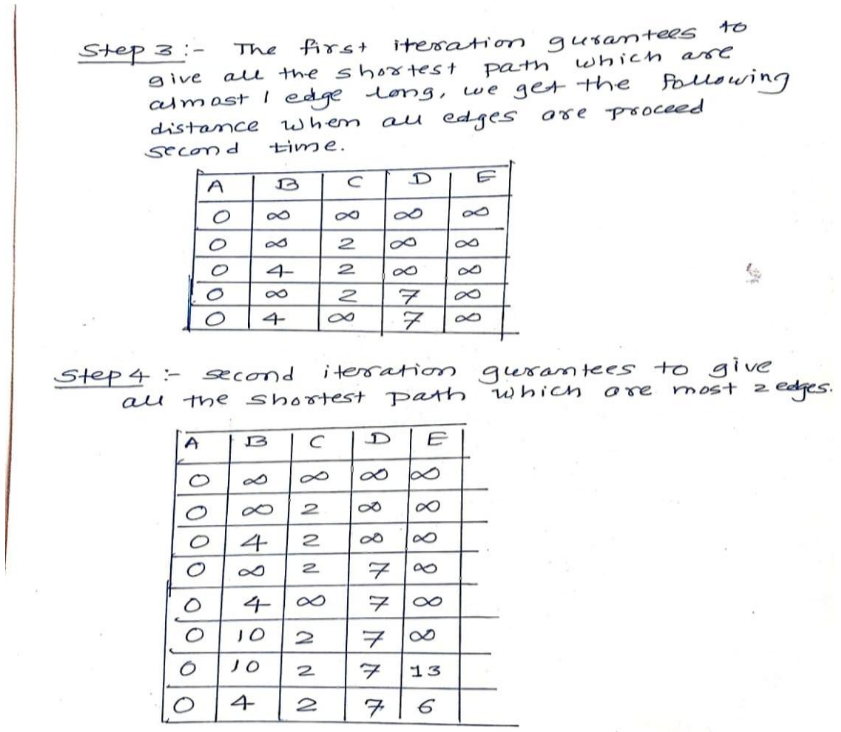


Step1:- Let the given source vertex be "0"
Initialise all the distance as infinite,
except the distance to the source itself.
Total no. of vertices in the graph is 5,
so all edges must be proceded 4 times.

A	B	C	D	E
0	∞	∞	∞	∞

Step2:- Let all the edges, are proced with the following order.
(B,E), (B,D), (A,B), (A,C), (C,D)

A	B	C	D	E
0	∞	∞	∞	∞
0	∞	2	∞	∞
0	4	2	∞	∞



Step 3 :- The first iteration gurantees to give all the shortest path which are almost 1 edge long, we get the following distance when all edges are proceed second time.

A	B	C	D	E
0	∞	∞	∞	∞
0	∞	2	∞	∞
0	4	2	∞	∞
0	∞	2	7	∞
0	4	∞	7	∞

Step 4 :- second iteration gurantees to give all the shortest path which are most 2 edges.

A	B	C	D	E
0	∞	∞	∞	∞
0	∞	2	∞	∞
0	4	2	∞	∞
0	∞	2	7	∞
0	4	∞	7	∞
0	10	2	7	∞
0	10	2	7	13
0	4	2	7	6

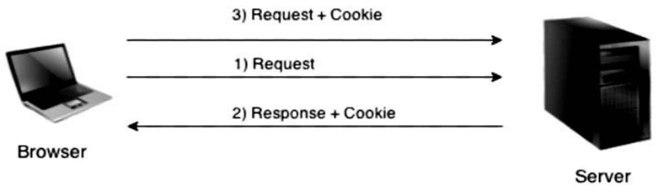
4. **Attempt any THREE of the following:** **12**

a) **Construct a diagram to show the application of cookies in a scenario in which the server uses Cookies for advertisement.** **4M**

Ans Cookies are small files which are stored on a user's computer. They are used to hold a modest amount of data specific to a particular client and website and can be accessed either by the web server or by the client computer

Diagram 1M

Steps 3M

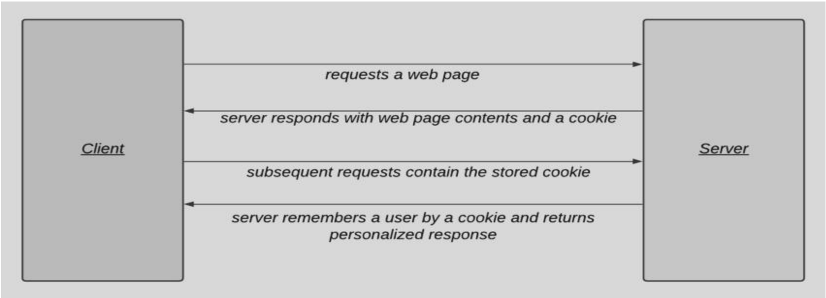


Any Relevant answer shall be considered

When cookies were invented, they were basically little documents containing information about you and your preferences. For instance, when you select your language in which you want to view your website, the website would save the information in a document called a cookie on your computer, and the next time when you visit the website, it would be able to read a cookie saved earlier.

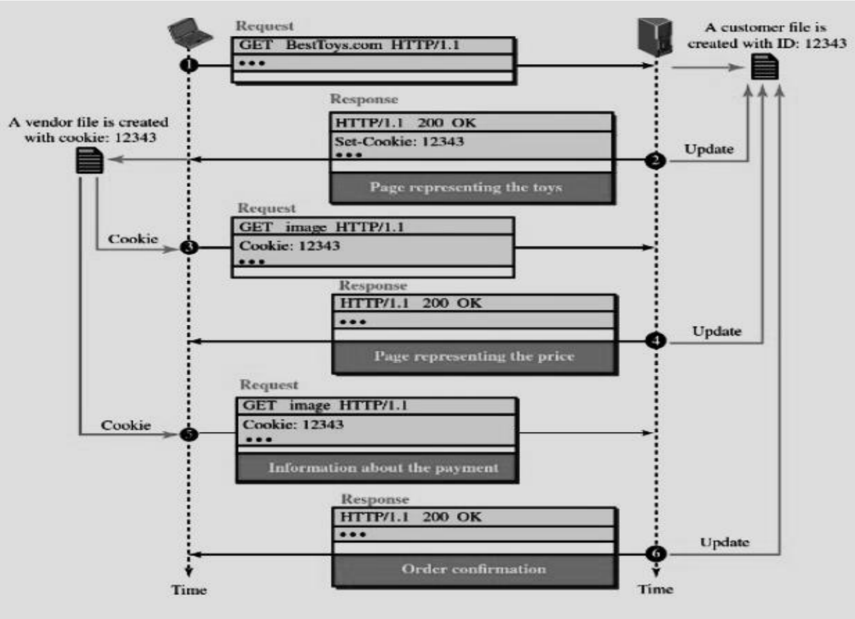
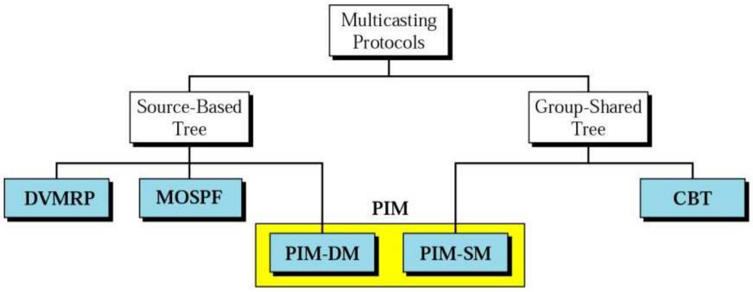
That way the website could remember your language and let you view the website in your preferred language without having to select the language again.

A cookie can contain any type of information such as the time when you visited the website, the items that you added into your shopping basket, all the links you clicked in website, etc. Cookies themselves contain no personally identifiable information. Depending on the publisher's and the user's settings, information associated with cookies used in advertising may be added to the user's Google Account.


Client
requests a web page
server responds with web page contents and a cookie
subsequent requests contain the stored cookie
server remembers a user by a cookie and returns personalized response
Server

Most commonly, AdSense sends a cookie to the browser when a user visits a page that shows Google ads. Pages with Google ads include ad tags that instruct browsers to request ad content from our servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google ads for this to happen; it just needs to include our ad tags, which might load a click tracker or impression pixel instead.

Following Fig. Example of how server uses cookies for advertisement.

		 Request GET BestToys.com HTTP/1.1 ••• A customer file is created with ID: 12343 1 Response HTTP/1.1 200 OK Set-Cookie: 12343 ••• Page representing the toys A vendor file is created with cookie: 12343 2 Update Request GET image HTTP/1.1 Cookie: 12343 ••• Cookie 3 Response HTTP/1.1 200 OK ••• Page representing the price 4 Update Request GET image HTTP/1.1 Cookie: 12343 ••• Information about the payment Cookie 5 Response HTTP/1.1 200 OK ••• Order confirmation 6 Update Time Time	
	b) **Ans.**	**List Intradomain multicast protocol. Explain any one in detail.** Intra domain routing protocols carry out the multi cast function within domains.  Multicasting Protocols Source-Based Tree Group-Shared Tree DVMRP MOSPF PIM PIM-DM PIM-SM CBT There are following three protocols play major roles in establishment multicast connections. 1) Multicast Distance Vector(DVMRP) 2) Multicast Link State(MOSPF) 3) Protocol Independent Multicast (PIM)	**4M** *Diagram 1M* *List 1M* *Any one explanation 2M*

1) Multicast Distance Vector (DVMRP):

Distance vector routing when extended to support multicast is called Distance Vector Multicast Routing Protocol (DVMRP).

The DVMRP is Multicast routing protocol that takes the routing decision based upon the source address of the packet. This algorithm constructs the routing tree for a network.

Whenever, a router receives a packet, it forwards it to some of its ports based on the source address of the packet. The rest of the routing tree is made by downstream routers. In this way, routing tree is created from destination to source.

The DVMRP protocol must achieve the following tasks:

1. It must prevent the formation of loops in the network.
2. It must prevent the formation of duplicate packets.
3. It must ensure that the path travelled by a packet is the shortest from its source to the router.
4. It should provide dynamic membership.

It is a following two-stage process:

1. Create a broadcast mechanism that allows a packet to be forwarded to all the networks on the internet.
2. Refine this mechanism so that it prunes back networks that do not have hosts that belong to the multicast group.

Multicast distance vector routing uses source-based trees, but the router never actually makes a routing table. When a router receives a multicast packet, it forwards the packet as though it is consulting a routing table.

We can say that the shortest path tree is evanescent. After its use (after a packet is forwarded) the table is destroyed. To accomplish this, the multicast distance vector algorithm uses a process based on following four decision-making strategies:

1. Flooding:

It is the first strategy that comes to mind. A router receives a packet and without even looking at the destination group address, sends it out from every interface except the one from which it was received.

Flooding accomplishes the first goal of multicasting: every network with active members receives the packet. However, so will networks without active members. This is a broadcast, not a multicast.

There is another problem is, it creates loops. A packet that has left the router may come back again from another interface or the same interface and be forwarded again.

Some flooding protocols keep a copy of the packet for a while and discard any duplicates to avoid loops. The next strategy, reverse path forwarding, corrects this defect.

2. Reverse Path Forwarding (RPF):

RPF is a modified flooding strategy. RPF eliminates the loop in the flooding processes.

In this strategy, the router only forwards those packets that have travelled the shortest path from source to destination.

To achieve this, the router pretends that it has a packet to send to the source from has arrived. In this way, the shortest path to the sender of the packet is computed.

If the same route is followed by the received packet, it is forwarded to the next router and it is discarded otherwise.

The reverse path forwarding ensures that the network receives a copy of the packet without formation of loops. A loop occurs when a packet that has left the router may come back again from another interface or the same interface and be forwarded again.

RPF does not guarantee that there would be no duplicate packets in the network i.e. the network may receive two or more copies.

The reason for this is that the routing is based on the source address and not on the destination address.

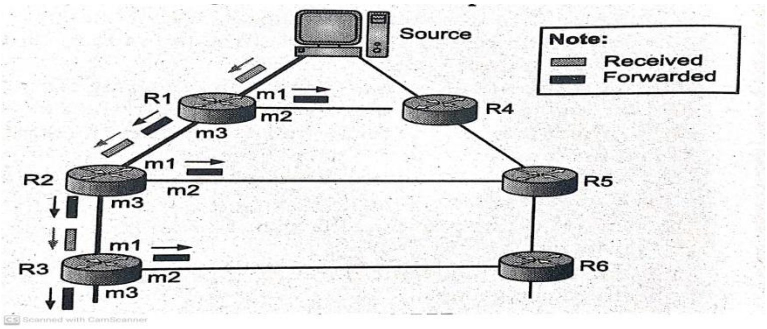


Fig. RPF

3. Reverse Path Broadcasting (RPB)

RPF does not guarantee that each network receives only one copy a network receives two or more copies. The reason is that RPF is not based on the destination address forwarding is based on the source address. In order to solve the problem, RPB is used.

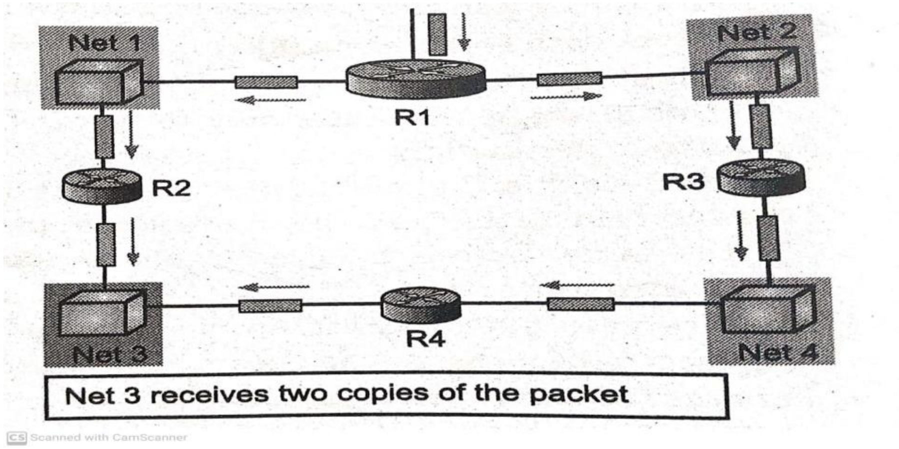

Net 1
Net 2
R1
R2
R3
R4
Net 3
Net 4
Net 3 receives two copies of the packet
CS Scanned with CamScanner

Fig. Problem with RPF

Consider the above Fig in which Net3 receives two copies of the packet even though each router just sends out one copy from each interface. There is duplication because a tree has not been made instead of a tree we have a graph. Net3 has two parents namely, routers R2 and R4.

In RPB method, one parent router is defined for each network. The network could accept the multicast packets from this parent router only. This router sends packets to those ports for which it is designated as parent.

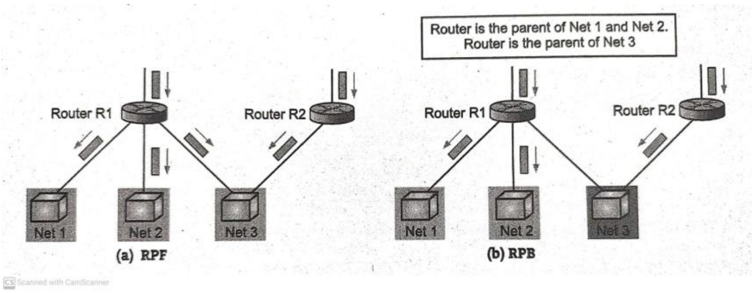
Thus, RPB principle allows a router to broadcast the packet in the network. This creates duplicate packets on the network and reduces the network efficiency

To eliminate duplication, we must define only one parent router for each network. We must have this restriction: A network can receive a multicast packet from a particular source only through a designated parent router.

Now the policy is clear. For each source, the router sends the packet only out of those interfaces for which it is the designated parent. This policy is called Reverse Path Broadcasting (RPB).

RPB guarantees that the packet reaches every network and that every network receives only one copy.

Following Fig, shows the difference between RPF & RPB


Router is the parent of Net 1 and Net 2.
Router is the parent of Net 3
Router R1
Router R2
Router R1
Router R2
Net 1
Net 2
Net 3
Net 1
Net 2
Net 3
CS Scanned with CamScanner

(a) RPF (b) RPB

4. Reverse Path Multicasting (RPM):

To overcome the problem of broadcasting in RPB, Reverse Path Multicasting in used. In RPM the desired multicast network tree is created by using two methods namely, Pruning and Grafting. A router can send a prune message to its upstream router whenever it finds that its network is not interested in a multicast packet. In this way a router prunes (cuts) its network from multicasting.

If a router receives prune message from all the downstream routers, it in turn, sends a prune Message to its upstream router.

To convert broadcasting to multicasting, the protocol uses following two procedures, pruning and grafting.

i) Pruning:

The designated parent router of each network is responsible for holding the membership information. This is done through the IGMP protocol.

The process starts when a router connected to a network finds that there is no interest in a multicast packet. The router sends a prune message to the upstream router so that it can prune the corresponding interface.

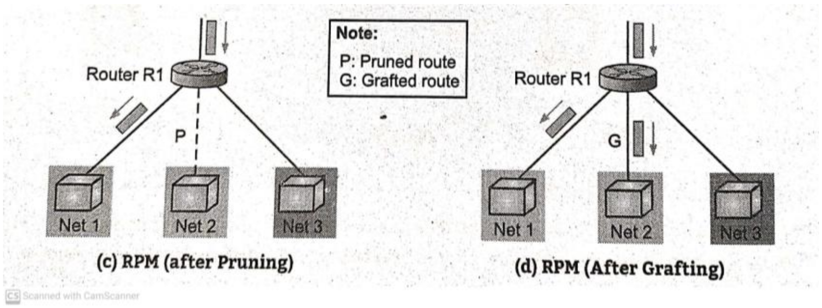
That is, the upstream router can stop sending multicast messages for this group through that interface. Now if this router receives prune messages from all downstream routers, it, in turn, sends a prune message to its upstream router.

(ii) Grafting:

What if a leaf router (a router at the bottom of the tree) has sent a prune message but suddenly realizes, through IGMP, that one of its networks is again interested in receiving the multicast packet?

It can send a graft message. The graft message forces the upstream router to resume sending the multicast messages.

Following Fig. shows the idea of pruning and grafting.



(c) RPM (after Pruning)

(d) RPM (After Grafting)

Fig.RPM Pruning and Grafting

2) Multicast Link State (MOSPF)

MOSPF protocol is an extension of the OSPF protocol that uses multicast link state routing to create source based trees.

MOSPF provides enhancements to OSPF Version 2 (OSPFV2) to support IP multicast routing.

The protocol requires a new link state update packet to associate the unicast address of a host with the group address only report directly connected hosts. This packet is called the group-membership LSA (Link State Advertisement).

MOSPF is a data driven protocol; the first time an MOSPF router sees a datagram with a given source and group address, the router constructs the Dijkstra shortest path tree.

MOSPF takes advantage of the link-state information maintained by OSPF.

Using the link-state and group membership information, MOSPF routers are able to calculate pruned source rooted shortest-path trees for multicast datagrams by using the Dijkstra's algorithm.

MOSPF also defines a mechanism for inter-AS multicast forwarding.

The biggest disadvantage of MOSPF is that every router must maintain membership information of every group. Therefore, MOSPF also scales poorly if there are many multicast groups.

When compared to DVMRP, MOSPF causes no useless data traffic.

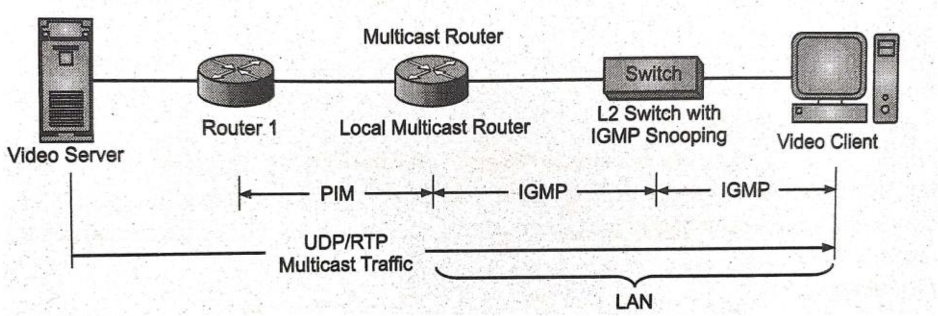
3) Protocol Independent Multicast (PIM)

PIM emerged as an algorithm to overcome the limitations of protocol such as the Distance Vector Multicast Routing Protocol (DVMRP), PIM was designed to avoid the dense-mode scaling issues of DVMRP and the potential performance issues of CBT (Core Base Tree) at the same time.

PIM is used for efficient routing to multicast groups that might span wide-area and inter domain internetworks. It is called "protocol independent" because it does not depend on a particular unicast routing protocol.

Protocol Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet.

PIM is not dependent on a specific unicast routing protocol; it can make use of any unicast routing protocol in use on the network. PIM does not build its own routing tables. PIM uses the unicast routing table for reverse path forwarding.



Protocol Independent Multicast (PIM) is the name given to two independent multicast routing protocols namely, Protocol Independent Multicast, Dense Mode (PIM-DM) and Protocol Independent Multicast, Sparse Mode (PIM-SM). Both protocols are unicast-protocol dependent, but the similarity ends here.

PIM-DM:

PIM Dense Mode (PIM-DM) is a multicast routing protocol designed with the opposite assumption to PIM-SM, namely that the receivers for any multicast group are distributed densely throughout the network.

PIM-DM is used when there is a possibility that each router is involved in multicasting (dense mode). In this environment, the use of a protocol that broadcasts the packet is justified because almost all routers are involved in the process.

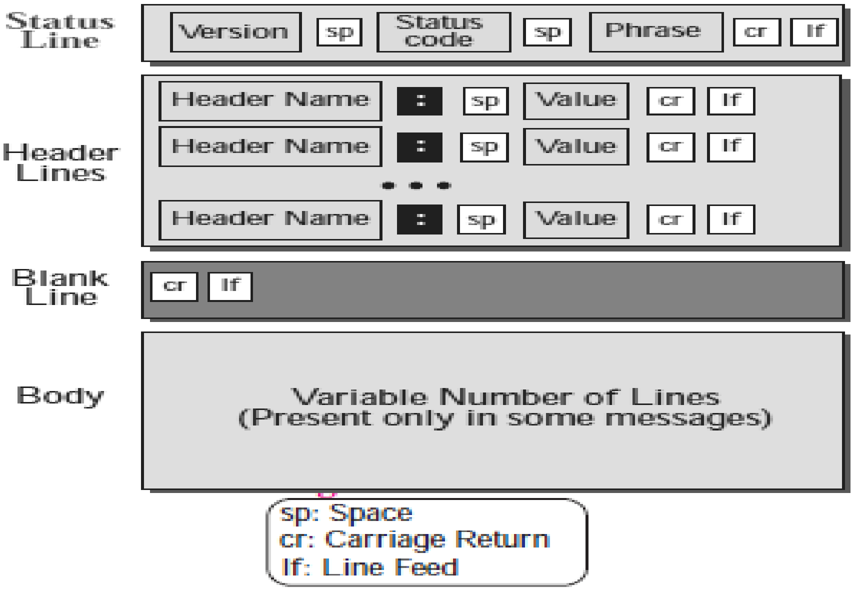
		PIM-DM is a source-based tree routing protocol that uses RPF and pruning/grafting strategies for multicasting. Its operation is like DVMRP; however, unlike DVMRP, it does not depend on a specific unicasting protocol. It assumes that the autonomous system is using a unicast protocol and each router has a table that can find the outgoing interface that has an optimal path to a destination. This unicast protocol can be a distance vector protocol (RIP) or link state protocol (OSPF). PIM-DM is used in a dense multicast environment, such as a LAN. PIM-DM uses RPF and pruning/grafting strategies to handle multicasting. However, it is independent from the underlying unicast protocol. **PIM-SM:** PIM Sparse Mode (PIM-SM) is a multicast routing protocol designed on the assumption that recipients for any particular multicast group will be sparsely distributed throughout the network. PIM-SM is used when there is a slight possibility that each router is involved in multicasting (sparse mode). In this environment, the use of a protocol that broadcasts the packet is not justified; a protocol such as CBT (Core Base Tree) that uses a group-shared tree is more appropriate. PIM-SM is a group-shared tree routing protocol that has a Rendezvous Point (RP) as the source of the tree. Its operation is like CBT; however, it is simpler because it does not require acknowledgment from a join message. PIM-SM is used in a sparse multicast environment such as a WAN. PIM-SM is similar to CBT but uses a simpler procedure.	
	c) **Ans.**	**Describe the HTTP Responses Message Format.** A Response message consists of a status line header line, a blank line and sometimes a body. HTTP Response sent by a server to the client. The response is used to provide the client with the resource it requested. It is also used to inform the client that the action requested has been carried out. It can also inform the client that an error occurred in processing its request.	**4M** *Diagram 1M* *Explanation 3M*

An HTTP response contains the following things:

1. Status Line
2. Response Header Fields or a series of HTTP headers
3. Blank Line
4. Message Body

Any relevant explanation shall be considered.

In the request message, each HTTP header is followed by a carriage returns line feed (CRLF). After the last of the HTTP headers, an additional CRLF is used and then begins the message body.



1) Status Line :

In the response message, the status line is the first line. The status line contains three items:

a) HTTP Version Number: It is used to show the HTTP specification to which the server has tried to make the message comply.

b) Status Code: It is a three-digit number that indicates the result of the request. The first digit defines the class of the response. The last two digits do not have any categorization role. There are five values for the first digit, which are as follows:

Code and Description:

1xx: Information
It shows that the request was received and continuing the process.

2xx: Success
It shows that the action was received successfully, understood, and accepted.

3xx: Redirection
It shows that further action must be taken to complete the request.

4xx: Client Error
It shows that the request contains incorrect syntax, or it cannot be fulfilled.

5xx: Server Error
It shows that the server failed to fulfil a valid request.

c) Reason Phrase: It is also known as the status text. It is a human-readable text that summarizes the meaning of the status code.

2) Header Lines :

The HTTP Headers for the response of the server contain the information that a client can use to find out more about the response, and about the server that sent it. This information is used to assist the client with displaying the response to a user, with storing the response for the use of future, and with making further requests to the server now or in the future. The name of the Response-header field can be extended reliably only in combination with a change in the version of the protocol.

3) Blank Line :

It contains cr (Carriage Return) & if (Line Feed)

4) Entire Body:

The body of the message is used for most responses. The exceptions are where a server is using certain status codes and where the server is responding to a client request, which asks for the headers but not the response body.

d) **List different timers used in TCP.** **4M**

Diagram 1M

List 1M

Explanation 2M

Any other relevant explanation shall be considered.

Ans. TCP uses several timers to ensure that excessive delays are not encountered during communications.
Several of these timers are elegant, handling problems that are not immediately obvious at first analysis. Each of the timers used by TCP is examined in the following subsections, which reveal its role in ensuring data is properly sent from one connection to another.
TCP implementations use at least four timers as shown in following Fig.

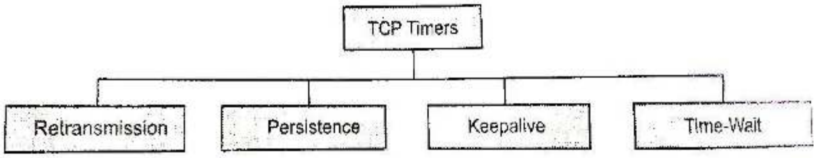


Fig.TCP Timers

1) Retransmission Timer:
To retransmit lost segments, TCP uses Retransmission Time Out (RTO). When TCP sends a segment the timer starts and stops when the acknowledgment is received.
If the timer expires timeout occurs and the segment is retransmitted. RTO (retransmission timeout is for 1 RTT) to calculate retransmission timeout we first need to calculate the RTT.

Three Types of RTT:

1. Measured RTT (RTTm): The measured Round Trip Time (RTT) for a segment is the time required for the segment to reach the destination and be acknowledged, although the acknowledgment may include other segments.

2. Smoothed RTT (RTTS): It is the weighted average of RTTm. RTTM is likely to change and its fluctuation is so high that a single measurement cannot be used to calculate RTO.

(i)	Initially	No value
(ii)	After the first measurement	RTTs=RTTm.
(iii)	After each measurement	RTTs-(1-1)*RTTs+t*RTTm.

3. Deviated RTT (RTTd): Most implementation do not use RTTS alone so RTT deviated is also calculated to find out RTO.

(i)	Initially	No value
(ii)	After first measurement	RTTd=RTTm/2
(iii)	After each measurement	RTTd=(1-k)*RTTd+k* (RTTm - RTTS)

Retransmission Timeout:

RTO Calculation: The value of RTO is based on the smoothed round-trip time and its deviation. Most implementations use the following formula to calculate the RTO:

Initial value → Original (given in question).

After any measurement→RTO=RTTs +4*RTTd

2) Persistent Timer:

To deal with a zero-window-size deadlock situation, TCP uses a persistence timer. When the sending TCP receives an acknowledgment with a window size of zero, it starts a persistence timer.

When the persistence timer goes off, the sending TCP sends a special segment called a probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged; it is even ignored inCalculating the sequence number for the rest of the data. The probe causes the receiving TCP to resend the acknowledgment which was lost.

3) Keepalive Timer:

A keepalive timer is used to prevent a long idle connection between two TCPs. If a client opens a TCP connection to a server transfers some data and becomes silent the client will crash.

In this case, the connection remains open forever. So a keepalive timer is used. Each time the server hears from a client, it resets this timer. The time-out is usually 2 hours. . If the server does not hear from the client after 2 hours, it sends a probe segment. If there is no response after 10 probes, each of which is 75 s apart, it assumes that the client is down and terminates the connection.

4) Time Wait Timer:

This timer is used during TCP connection termination. The timer starts after sending the last Ack for 2nd FIN and closing the

connection.
After a TCP connection is closed, it is possible for datagrams that are still making their way through the network to attempt to access the closed port. The quiet timer is intended to prevent the just closed port from reopening again quickly and receiving these last datagrams.
The quiet timer is usually set to twice the maximum segment lifetime (the same value as the Time- To-Live field in an IP header), ensuring that all segments still heading for the port have been discarded.

e) **Explain the working of SSH.** **4M**

Ans. SSH (Secure Shell) is the most popular remote login application program.
SSH uses client-server architecture in its implementation. An SSH server can be deployed and allow several SSH clients to connect to it. The architecture of SSH is shown in following Fig. and the SSH process is as follows:

Diagram 1M

Explanation 3M

Any relevant explanation may be considered

1) The SSH client on the left provides authentication to the SSH server on the right. In the initial connection, the client receives a host key of the server, therefore, in all subsequent connections, the client will know it is connecting to the same SSH server. This places less emphasis on the IP address of the SSH server, which can be easily spoofed, and more emphasis on the host key of the server, which cannot be spoofed very easily.
2) The SSH server determines if the client is authorized to connect to the SSH service by verifying the username/password or public key that the client has presented for authentication. This process is completely encrypted.
3) If the SSH server authenticates the client and the client is authorized, the SSH session begins between the two entities. All communication is completely encrypted.

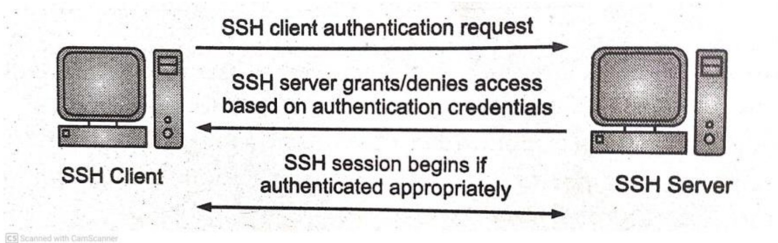
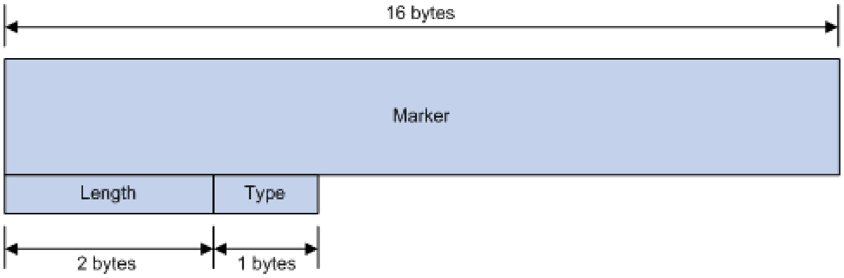

SSH client authentication request
SSH server grants/denies access based on authentication credentials
SSH session begins if authenticated appropriately
SSH Client
SSH Server

Fig. SSH Communication from an SSH Client to an SSH Server

		The steps involved in creating an SSH session go like this: 1. Client contacts server to initiate a connection. 2. The server responds by sending the client a public cryptography key. 3. The server negotiates parameters and opens a secure channel for the client. 4. The user, through their client, logs into the server.	
5.		**Attempt any <u>TWO</u> of the following:**	**12**
	a)	**Describe the BGP3 in detail.**	**6M**
	Ans.	• To denote any protocol used to pass routing information between two autonomous systems, Computer scientists use the term Exterior Gateway Protocol (EGP). Currently a single exterior protocol is used in most TCPJIP internets. Known as the Border Gateway Protocol (BGP), it has evolved through four (quite different) versions one of the versions is BGP3. • Two systems form a transport protocol connection between one another. They exchange messages to **open** and confirm the connection parameters. The initial data flow is the entire BGP routing table. • Incremental **updates** are sent as the routing tables change. BGP does not require periodic refresh of the entire BGP routing table. Therefore, a BGP speaker must retain the current version of the entire BGP routing tables of all of its peers for the duration of the connection. • **Keepalive** messages are sent periodically to ensure the liveness of the connection. • Notification messages are sent in response to errors or special conditions. If a connection encounters an error condition, a **notification** message is sent and the connection is closed. • Connections between BGP speakers of different ASs are referred to as "external" links. BGP connections between BGP speakers within the same AS are referred to as "internal" links. • Messages are sent over a reliable transport protocol connection. A message is processed only after it is entirely received. The maximum message size is 4096 octets. All implementations are required to support this maximum message size.	***Explanation 3M for Message Format diagram and explanation with message types 3M***

- The smallest message that may be sent consists of a BGP header without a data portion, or 19 octets.
- **Message Format**



- **Marker**

If the Type of the message is OPEN, or if the Authentication Code used in the OPEN message of the connection is zero, then the Marker must be all ones. The Marker can be used to detect loss of synchronization between a pair of BGP peers, and to authenticate incoming BGP messages.

- **Length**

This 2-bytes unsigned integer indicates the total length of the message, including the header, in bytes.

- **Type**

This 1-byte unsigned integer indicates the type code of the message. The following type codes are defined:

1 - OPEN
2 - UPDATE
3 - NOTIFICATION
4 – KEEPALIVE

- **OPEN Message**

After a transport protocol connection is established, the first message sent by each side is an OPEN message. If the OPEN message is acceptable, a KEEPALIVE message confirming the OPEN is sent back. Once the OPEN is confirmed, UPDATE, KEEPALIVE, and NOTIFICATION messages may be exchanged.

- **UPDATE Message**

UPDATE messages are used to transfer routing information between BGP peers. The information in the UPDATE packet can be used to construct a graph describing the relationships of the various Autonomous Systems.

		• **NOTIFICATION Message** A NOTIFICATION message is sent when an error condition is detected. The BGP connection is closed immediately after sending it. • **KEEPALIVE Message** BGP does not use any transport protocol-based keep-alive mechanism to determine if peers are reachable. Instead, KEEPALIVE messages are exchanged between peers often enough.	
	b) **Ans.**	**State the need for** **1. Sequence Control** **2. Error Control** **3. Flow Control in Networking** **Sequence Control** The 32-bit sequence number field defines the number assigned to the first byte of data contained in this segment. TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a Random number generator to create an initial sequence number (ISN), which is usually different in each direction. We know that a TCP sequence number is 32 bit. So it has finite (from 0 to (232-1) = 4 Giga sequence numbers) and it means we will be able to send only 4GB of data with a unique sequence number not more than that. It helps with the allocation of a sequence number that does not conflict with other data bytes transmitted over a TCP connection. An ISN is unique to each connection and separated by each device. **Error Control** Error Control mechanisms are useful to ensure reliability service of TCP. To provide reliable service TCP detects and corrects errors. Error control mechanisms are useful for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments. Error detection and correction in TCP is achieved through the use of three simple tools: checksum, acknowledgment, and time-out.	**6M** *2M for each*

Flow Control

Flow control make it possible for sender to send the amount of data bytes that can be sent without worrying an acknowledgment and is one of the most important duties of the data link layer. In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver.

The flow Control procedures not allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data, if sender sends data in a much speed data loss may occur to overcome this problem flow control procedures are needful.

c) **Explain the process of transition from of IPv4 to IPv6 for a network.** 6M

Ans. Three Transition from IPv4 to IPv6 strategies are

2M for each transition

1. Dual Stack
2. Tunnelling
3. Header Translation

1. Dual Stack

In this kind of strategy, a station has a dual stack of protocols run IPv4 and IPv6 simultaneously.

To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

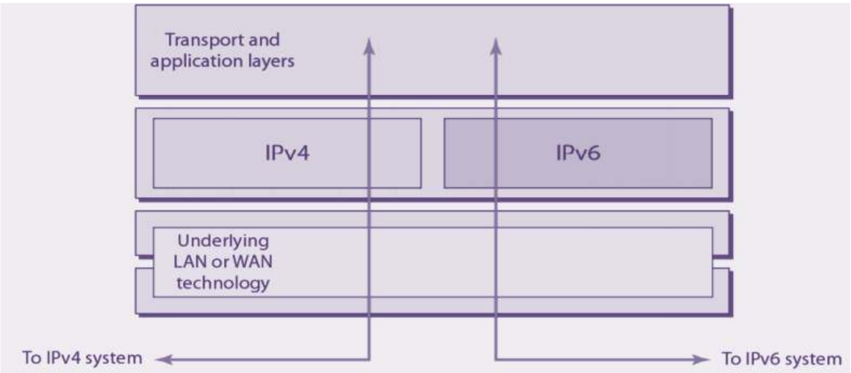

Transport and application layers
IPv4
IPv6
Underlying LAN or WAN technology
To IPv4 system
To IPv6 system

Fig. Dual Stack

2. Tunnelling

Tunnelling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4.

- To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region.
- To make it clear that the IPv4 packet is carrying an IPv6 packet as data.

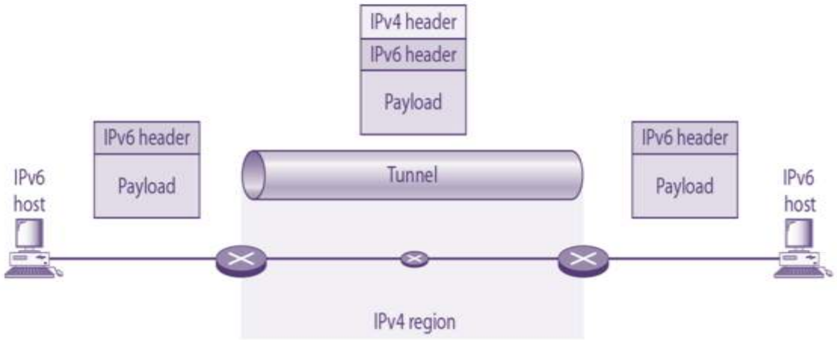


Fig. Tunnelling

3. Header Translation

In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header see figure.

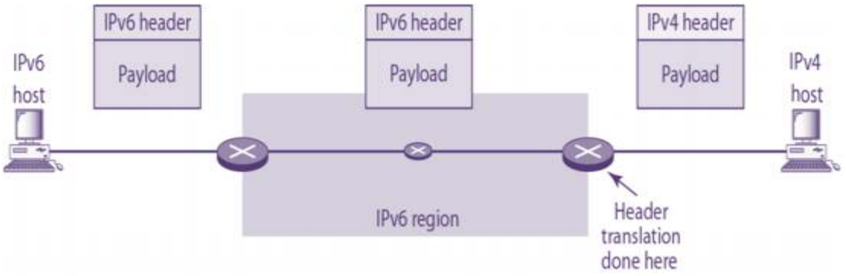


Fig. Header Translation

6.		**Attempt any TWO of the following:**	**12**

a) **With a suitable example, explain Link State Routing algorithm. What are the serious drawbacks of Link State Routing Algorithm?** **6M**

(Any relevant explanation can be considered)

Ans. In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

4M for explanation with example

2M for drawbacks

1. Creation of the states of the links by each node, called the link state packet(LSP).
2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
3. Formation of a shortest path tree for each node. (Dijkstra algorithm)
4. Calculation of a routing table based on the shortest path tree.

Example*(Any relevant example explained can be considered)*

Consider a sample network of networks. There are seven networks numbered 1 to 7, connected to each other by six routers A through F. As we will notice, each router is connected to at least two networks, but it may also be connected to more than two networks, e.g., router A in the figure.

Assume the following are cost values

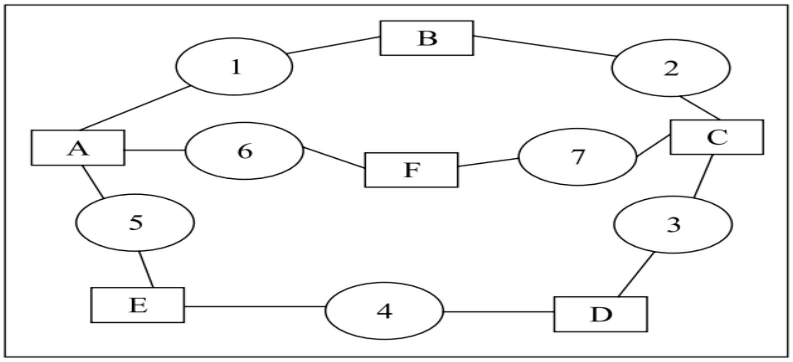
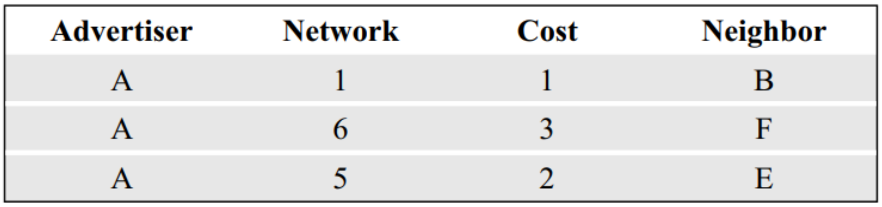


Fig. A graph for Internet (Where nodes denotes routers)

Periodically, each router sends a very small greeting packet to each of its neighbors and expects a response back from the neighbor. If the neighbor reverts, the original router considers that the neighbor is up and running, and accordingly determines the cost based on the factors discussed earlier. Otherwise, the neighbor is considered to be in some error.

Using this information, the original router then sends information about all its neighbors to the entire Internet in a process called flooding, as discussed earlier. For this, it sends a special packet called Link State Packet (LSP) to all other routers via its neighbors.

For example, a sample portion of the LSP (shown only for router A about its neighbors) could take the form as shown below

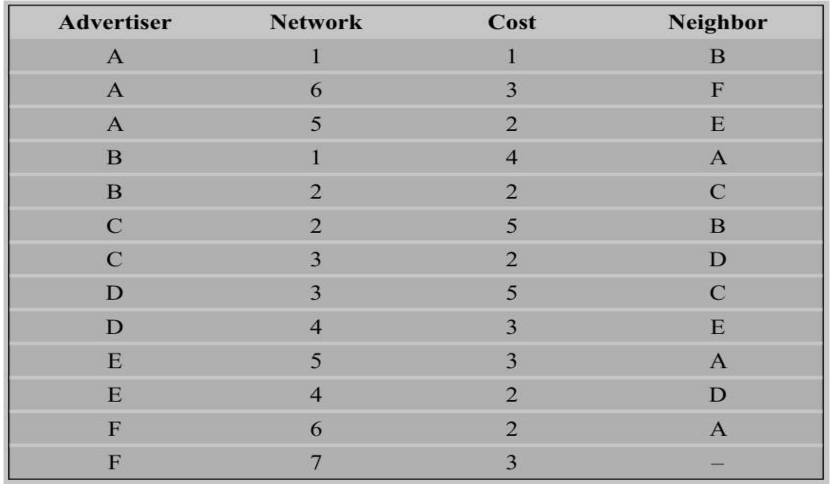


Advertiser	Network	Cost	Neighbor
A	1	1	B
A	6	3	F
A	5	2	E

LSP for router A (Cost is Assumed in example)

For example, the first row says that between router A (the first column) and router B (the fourth column), there is network 1 (the second column), and that the cost of going from router A to router B is 1 (the fourth column).

Every router receives every LSP packet, and uses it to create a local database called link state database. Thus, a link state database is a collection of all LSPs. Every router stores such a database on its disk, and uses it for routing packets. A sample link state database for our example Internet is shown below



Advertiser	Network	Cost	Neighbor
A	1	1	B
A	6	3	F
A	5	2	E
B	1	4	A
B	2	2	C
C	2	5	B
C	3	2	D
D	3	5	C
D	4	3	E
E	5	3	A
E	4	2	D
F	6	2	A
F	7	3	–

Link State Database

Having constructed the link state database, each router executes an

		algorithm called Dijkstra algorithm to create its routing table. This algorithm considers the Internet as a graph, and finds the distance along a shortest path from a single node of the graph to all other nodes in the graph. Using this information, a routing table is created to compute the shortest path. This algorithm must be run for each routing table once. **Drawbacks** • **Memory Requirements** − the link-state routing algorithm creates and maintains a database and SPF tree. The database and SPF tree required more memory than a distance vector algorithm. • **Processing Requirements** − to build a complete map of the topology Link-state routing protocols also require more CPU processing. • **Bandwidth Requirements** − The link-state routing protocol floods link-state packet during initial start-up and also at the event like network breakdown, and network topology changes, which affect the available bandwidth on a network. If the network is not stable it also creates issues on the bandwidth of the network. •	
	b) Ans.	**For the IP addresses given below** **1. Identify the classes to which the following IP address belongs to** **2. Identify network address sections** **3. Identify host address section** **4. Calculate number of hosts that can be assigned with each network** **i. 22.34.45.133** **ii. 12.12.12.12** **iii. 192.0.233.26** **iv. 126.123.16.87** **22.34.45.133**= 00010110.00100010.00101101.10000101 IP address class = Class A Network Section = 00010110 = 22 Host Section = 00100010.00101101.10000101= 34.45.133 Number of Host/Network = 2^{24}-2 = 16,777,214 **12.12.12.12**= 00001100.00001100.00001100.00001100 IP address class = Class A Network Section = 00001100 = 12	6M *Each IP address description* $1\frac{1}{2}M$

		Host Section = 00001100.00001100.00001100= 12.12.12 Number of Host/Network = 2^{24}-2 = 16,777,214 **192.0.233.26**= 11000000.00000000.11101001.00011010 IP address class = Class C Network Section = 11000000.00000000.11101001 = 192.0.233 Host Section = 00011010= 26 Number of Host = 2^{8}-2 = 154 **126.123.16.87**= 01111110.01111011.00010000.01010111 IP address class = Class A Network Section = 01111110 = 126 Host Section = 01111011.00010000.01010111= 123.16.87 Number of Host = 2^{24}-2 = 16,777,214	
	c) **Ans.**	**Describe e-mail security over non-secure channel.** ***(Note: Any other description of the concept shall be considered.)*** • Email security describes different techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss or compromise. • Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. • Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email encryption often includes authentication. • Email allows attackers to use it as a way to cause problems in attempt to profit. Whether through spam campaigns, malware and phishing attacks, sophisticated targeted attacks, or business email compromise (BEC), attackers try to take advantage of the lack of security of email to carry out their actions. • Since most organizations rely on email to do business, attackers exploit email in an attempt to steal sensitive information. • Because email is an open format, it can be viewed by anyone who can intercept it. It can be easily read and the contents of an email by intercepting it. • Email Security Policies can be established by viewing the contents of emails flowing through their email servers. It's important to	**6M** ***Any six points 1M each***

		understand what is in the entire email in order to act appropriately. After these baseline policies are put into effect, an organization can enact various security policies on those emails. • These email security policies can be as simple as removing all executable content from emails to more in-depth actions, like sending suspicious content to a sandboxing tool for detailed analysis. • If security incidents are detected by these policies, the organization needs to have actionable intelligence about the scope of the attack. • Enforce email encryption policies to prevent sensitive email information from falling into the wrong hands. • An email gateway scans and processes all incoming and outgoing email and makes sure that threats are not allowed in. Because attacks are increasingly sophisticated, standard security measures, such as blocking known bad file attachments, are no longer effective.	