KIIT Deemed to be University
Computer Networks Evaluation Schemes, (IT-3005)
SECTION-B(Answer Any Three Questions. Each Question carries 12 Marks)

Time: 1 Hour and 30 Minutes **(3×12=36 Marks)**

Question No	Questions	Marking
Q.8	Question -1 i. What do you mean by Domain Name Space and Fully Qualified domain name (FQDN)? **2 Marks** A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the internet. The FQDN consists of two parts: the hostname and the domain name. For example, an FQDN for a hypothetical mail server might be mymail.kiit.ac.in Explain the working of DNS and how it uses recursive and iterative resolution. **2 Marks** **Recursive DNS Query:** In a Recursive DNS Query, the DNS Client sends a Query to a DNS Server for name resolution. The reply to the DNS Query can be an answer to the query or an error message. In Recursive DNS Query, If the DNS Server doesn't know the answer to provide accurate answer to the DNS Client, DNS Server may query other DNS Servers on behalf of the DNS Client. **Iterative DNS Query:** In Iterative DNS Query, when a DNS Client asks the DNS server for name resolution, the DNS Server provides the best answer it has. If the DNS Server doesn't know the answer to the DNS Query from Client, the answer can be a reference to another lower-level DNS Server also. This lower-level DNS Server is delegated at the higher level DNS Server to be Authoritative for the DNS namespace which the DNS Query is related with. Once the DNS Client get the referral from higher level DNS Server, it can then send a DNS Query to the lower-level DNS server, got as referral. Briefly describes the different types of Resource records used in DNS. **2 Marks** The following resource record types are commonly used in DNS: Start of authority (SOA) Name server (NS) Pointer record (PTR) Address (A) IPv6 Address (AAAA) Mail exchange (MX) Canonical name (CNAME) Windows Internet Naming Service (WINS)	• Marks for each part carry equal weightage. • Marking for Sub-bit given in red colour. • Ref text book for theoretical descriptions .

ii. Discuss the functionality provided by DHCP Server.

3 Marks

The server has two basic functions: Managing IP addresses – The DHCP server controls a range of IP addresses and allocates them to clients, either permanently or for a defined period of time. The server uses a lease mechanism to determine how long a client can use a nonpermanent address.

Explain the need of running DHCP client on a well-known port instead of an ephemeral port. **3 Marks**

DHCP is based on the earlier BOOTP protocol which uses well known port numbers for both server and client instead of an ephemeral port. The server and the client communicate via broadcast and the server broadcasts the offered IP address to the client on UDP port 68. The use of a well-known port on the client's side is introduced to tackle the problem associated with this broadcast, which we will describe below.

Let's assume that host A is using the BOOTP client on ephemeral port 1883, and host B (which is on the same network) is using MQTT client on the same port. Now when the BOOTP server sends a broadcast reply message with the broadcast IP address 255.255.255.255 and destination port no. 1883, then host A will accept the correct message on its DHCP client on the application layer. But, the MQTT client which is running on the application layer of host B will get an incorrect message. The use of an well-known port (in our case 68) prevents the use of the same two destination port numbers and hence it prohibits other protocols from using the same port which is already in use by another protocol. In simple words, it prevents an application from getting a message from a completely different protocol.

Question -2

i. Describe how Web caching can reduce the delay in receiving a requested object. **3 Marks**

Web caching reduces the response time for client request. If there is a high-speed connection between the client and the cache, and if the cache has the requested object, then the cache will be able to deliver the object rapidly to the client.

Will Web caching reduce the delay for all objects requested by a user or for only some of the objects? Why? **3 Marks**

The web caching can reduce the response time of the client's request when the bottle bandwidth between the client and the server is much less than the bottleneck bandwidth between the client and the cache.

• Web caching can reduce the response time for the client requests when there is a high-speed connection between the client and cache, and the cache has the requested object.

• Web caching reduces the traffic on the institution's access link to the internet. Therefore, the institute doesn't have to update its bandwidth cables quickly. Thus, it can reduce the cost.

• If the cache memory size is high, it can handle many requests quickly. Thus, it reduces the response time.

• Finally, the traffic on the internet decreases substantially as a whole.

Therefore, the web caching reduces the delay in receiving the requests for all objects requested by the user.

ii. What do you mean by persistent and non-persistent connections?

- Marks for each part carry equal weightage.
- Marking for Sub-bit given in red colour.
- Ref text book for theoretical descriptions .

2 Marks

In persistent connections, the server leaves the TCP connection open after sending responses and hence the subsequent requests and responses between the same client and server can be sent. A nonpersistent connection is the one that is closed after the server sends the requested object to the client.

Explain the working of HTTP specifying the different steps associated between a HTTP client and server. Also specify different types of methods used by HTTP. **2 Marks + 2 Marks**

Question -3

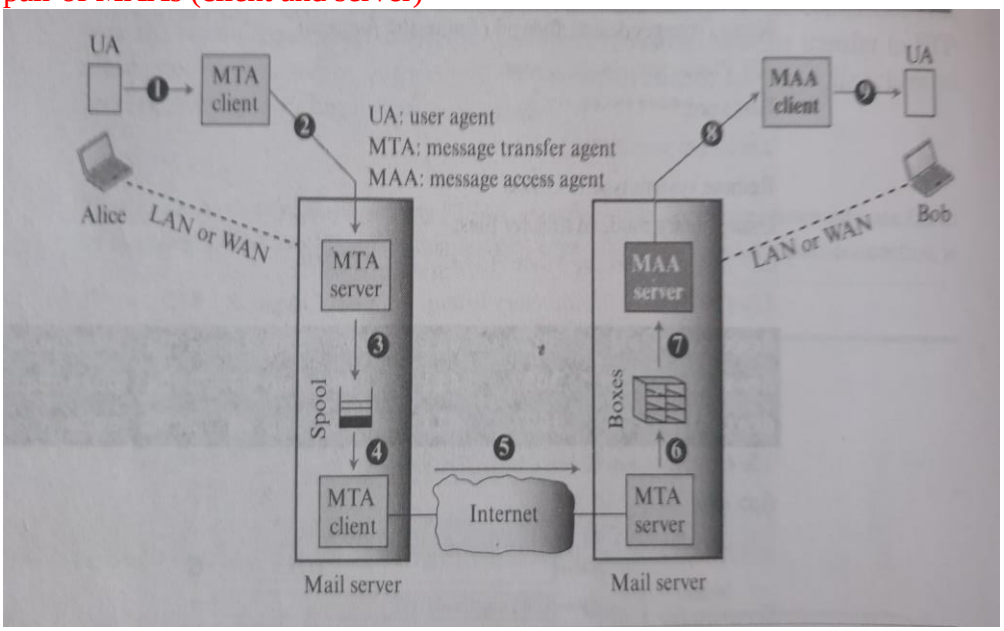
i. Briefly explain the working of an E-mail Application with the help of neat block diagram showing functional blocks like UA, MTA, MAA, Mail-Box, Message-Queue. **6 Marks**

- Marks for each part carry equal weightage.
- Marking for Sub-bit given in red colour.
- Ref text book for theoretical descriptions .

E-mail communication steps:

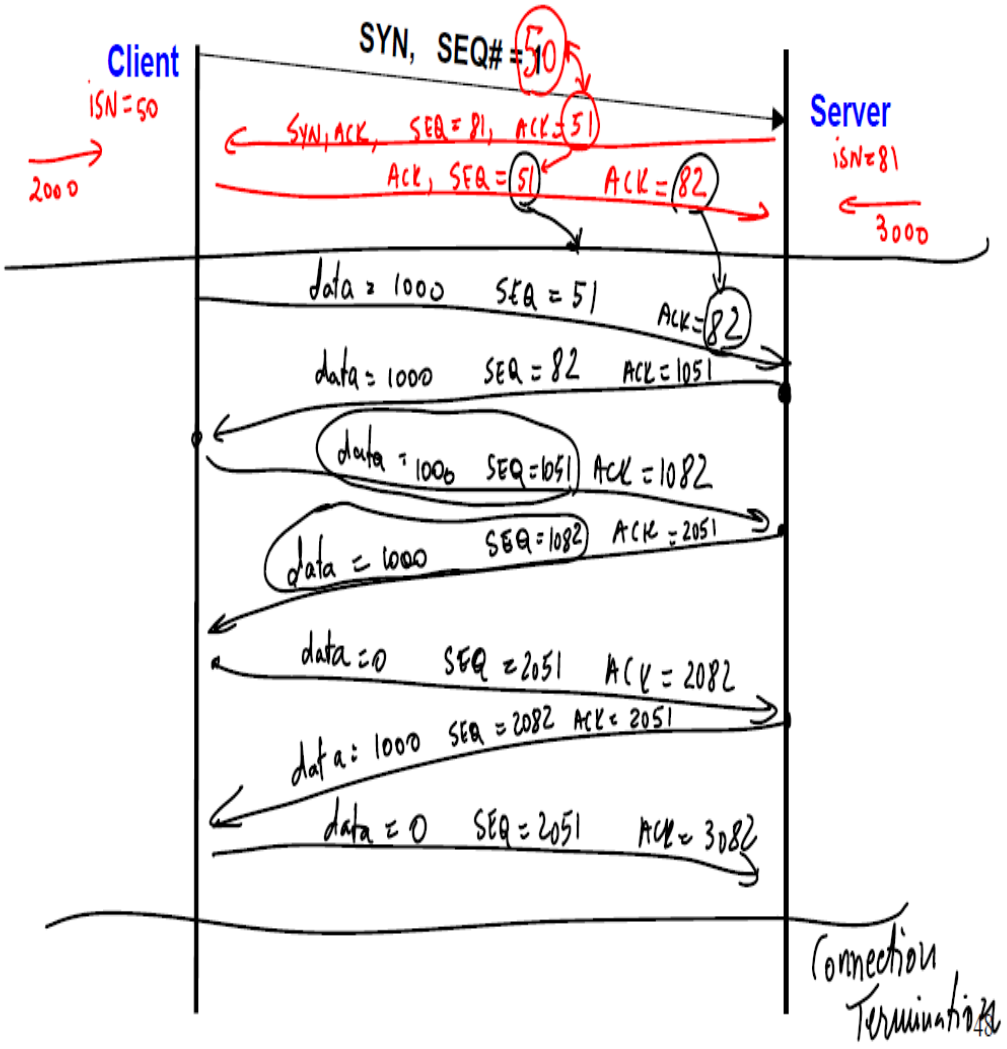
1. UA of client sends the e-mail to a MTA client
2. MTA Client program of Sender sends mail to Mail Server (Sender end). MTA Server program gets the mail.
3. MTA Server puts the e-mail in a MessageQueue (Spool)
4. At Mail Server at sender end the e-mail is fetched from the Spool and using a MTA client program it is forwarded to the relevant MTA Server program running on the receiver mail server.
5. MTA Server at receiver mail server forwards the e-mail to the designated Mail-Box of the destination user.
6. Based on the user destination: bob@hotmail.com the e-mail is PUT in to the mail-box database.
7. MAA Server fetches data from relevant Mail-box
8. When the receiver comes online MAA Server program running on the received mail-server forwards the mail to MAA client
9. MAA client deliver the data to UA of the receiver

The electronic mail system needs two UAs, two pairs of MTAs (client and server) and a pair of MAAs (client and server)



	ii. Explain, why a push protocol will not be suitable rather a pull protocol will be used to download a message at the client end? **6 Marks** In push protocols, the client opens a connection to the server and keeps it constantly active. The server will send (push) all new events to the client using that single always-on connection. In other words, the server PUSHes the new events to the client. In pull protocols, the client periodically connects to the server, checks for and gets (pulls) recent events and then closes the connection and disconnects from the server. The client repeats this whole procedure to get updated about new events. In this mode, the clients periodically Pull the new events from the server. The difference is that in push protocols, you get new events (such as a new email, a new chat message, etc) literally instantly. But you may experience a small-time delay in pull protocols. Although many apps using the pull protocol, check for new events so regular (e.g. every 30 seconds) that the time delay is mostly not noticeable.	
Q. No: 9	Question -1 i. Distinguish between a time-out and 3-duplicate ACKs event. Which one is a stronger sign of congestion in the network? Explain the reason behind the same through an appropriate example. **2 Marks + 2 Marks + 2 Marks** A timeout clearly indicates serious path congestion, so you want to SLOW THE HELL DOWN and stop sending so much data. Cut the window down fast, and start up slow. This is the core of congestion control. A duplicate ACK (dupack) indicates a lost packet somewhere in the middle of a stream, but not necessarily path congestion and queue drop. Maybe there was an error on a link or a transient routing issue. The dupack is a trigger for "Fast Retransmit." Nevertheless, there MIGHT be congestion so you MAY want to slow down a bit. Especially in the face of multiple dupacks. The congestion is clearly not as bad as if you were getting timeouts, so less drastic measures are needed. TCP interprets timeouts as a sign of congestion. ii. Let the slow start begins with cwnd=1 at time t=0 with a maximum segment size is of 1500 Bytes. What is the RTT value when the cwnd is greater than 25KB? **6 Marks** Here MSS size is 1500 bytes i.e. every time 1MSS sent means 1500B data is sent so either you write in terms of MSS by adding 1 or in terms of data adding 1500B. The question in the link has started with window size 1(which is 1500B). The AIMD algorithm is applied when the segment being sent is lost or data size reaches threshold. We generally start from slow start phase i.e. 1st transmission 2MSS, i.e 1500*2=3KB 2nd 4MSS 4*1500=6KB 3rd 8MSS 8*1500=12KB 4th 16MSS 16*1500=24 KB So the RTT value is 5 when CWND is greater than 25KB.	• Marks for each part carry equal weightage. • Marking for Sub-bit given in red colour. • Ref text book for theoretical descriptions .

	Question -2 i. List out five key difference between TCP and UDP. Specify the applications those are using TCP and UDP respectively. Draw and explain TCP and UDP header. **2 Marks + 2 Marks + 2 Marks** TCP is a connection-oriented protocol whereas UDP is a connection less protocol. As TCP provides error checking support and also guarantees delivery of data to the destination router this make it more reliable as compared to UDP. While on other hand UDP does provided only basic error checking support using checksum so the delivery of data to the destination cannot be guaranteed in UDP as compared to that in case of TCP. In TCP the data is transmitted in a particular sequence which means that packets arrive in-order at the receiver.On other hand there is no sequencing of data in UDP in order to implement ordering it has to be managed by the application layer. TCP is slower and less efficient in performance as compared to UDP. Also, TCP is heavy-weight as compared to UDP. On other hand UDP is faster and more efficient than TCP. Retransmission of data packets is possible in TCP in case packet get lost or need to resend. On other hand retransmission of packets is not possible in UDP. Applications those use TCP: World Wide Web (WWW), email, File Transfer Protocol, Secure Shell, peer-to-peer file sharing, and streaming media. Applications those use UDP: Domain Name System (DNS), Simple Network Management Protocol (SNMP), Routing Information Protocol (RIP) and the Dynamic Host Configuration Protocol (DHCP) ii. Following are the information for a TCP Client and a Server: – The MSS (Maximum Segment Size) in both directions is 1000 bytes. – The ISN (Initial Sequence Number) for Client is 50 and for Server is 81. The Client sends 2000 bytes to the Server and the Server sends 3000 bytes to the client. Give the complete TCP message exchange between client and server. For each segment draw a vector showing the value of the SYN, ACK and FIN bits, with the value of the SEQ (Sequence Number) and the ACK (Acknowledgment Number). Assume no packets are lost and the application consumes the data as soon as it is received.? **6 Marks**	• Marks for each part carry equal weightage. • Marking for Sub-bit given in red colour. • Ref text book for theoretical descriptions .



Question -3

i. Why DNS uses UDP? Draw and explain the TCP segment format. Answer the followings: -

– The minimum and maximum size of a UDP segment.

The minimum would be 8 bytes for the UDP header. The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.

– The minimum and maximum size of the application-layer payload data that can be encapsulated in a UDP segment.

The minimum size of the application-layer payload is zero bytes and maximum size of the application-layer payload is 65,507 bytes (65,515−8).

– Minimum and maximum size of ethernet frame.

The minimum Ethernet Frame Size 64 Bytes and maximum size is 1518 bytes.

2 Marks + 2 Marks + 2 Marks

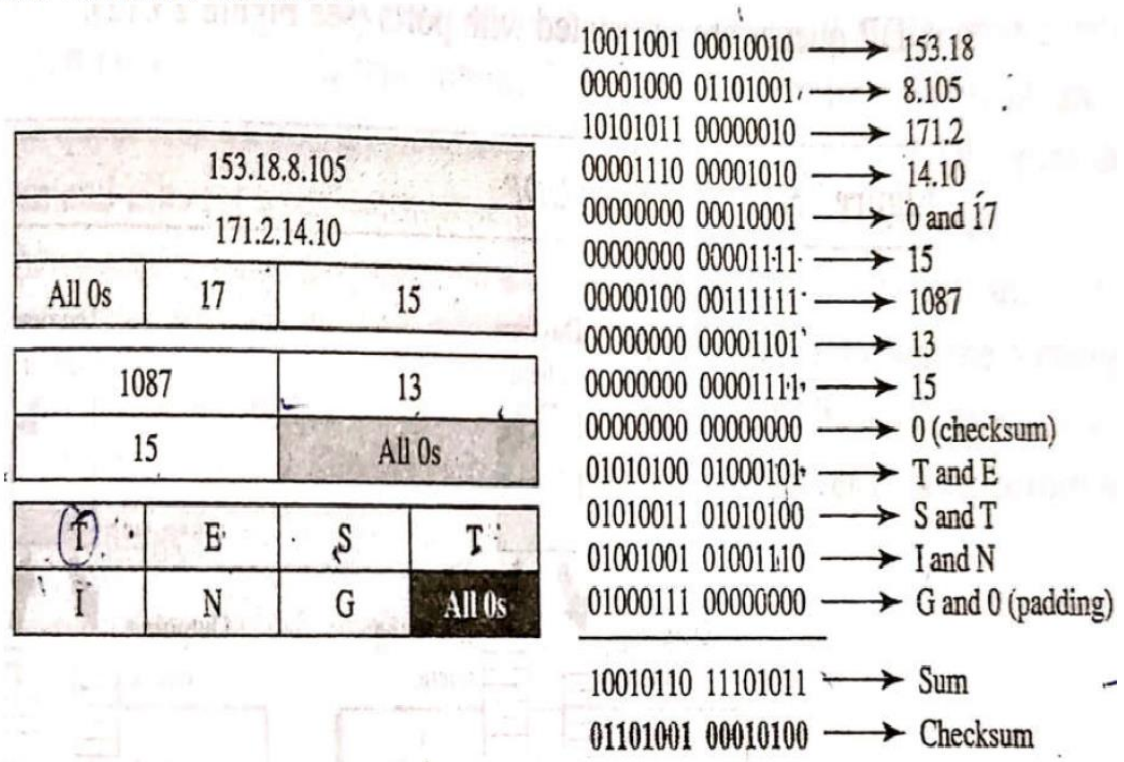
ii. A client is using a UDP socket 153.18.8.105:1087 to connect to a Daytime Server having socket 171.2.14.10:13. The UDP payload is “TESTING”.

Given data: ASCII Values in Decimal: E = 69; G = 71; I = 73; N = 78; S = 83; T = 84.

- Marks for each part carry equal weightage.
- Marking for Sub-bit given in red colour.
- Ref text book for theoretical descriptions .

Calculate the UDP Checksum for the Segment with above mentioned details

UDP Checksum Calculation



Q. No: 10

Question -1

i. An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks.

4 Marks

There are $2^{32-24} = 256$ addresses in this block.
The first address is 14.24.74.0/**24**;
The last address is 14.24.74.255/**24**.
To satisfy the third requirement, we assign addresses to sub blocks, starting with the largest and ending with the smallest one.
The number of addresses in the largest sub block, which requires 120 addresses, is not a power of 2.
We allocate 128 addresses.
The subnet mask for this subnet can be found as $n_1 = 32 - \log_2 128 = 25$.
The first address in this block is 14.24.74.0/**25**; the last address is 14.24.74.127/**25**.

The number of addresses in the second largest sub block, which requires 60 addresses, is not a power of 2 either.
We allocate 64 addresses.
The subnet mask for this subnet can be found as $n_2 = 32 - \log_2 64 = 26$.
The first address in this block is 14.24.74.128/**26**; the last address is 14.24.74.191/**26**.

The number of addresses in the largest sub block, which requires 120 addresses, is

- Marks for each part carry equal weightage.
- Marking for Sub-bit given in red colour.
- Ref text book for theoretical descriptions .

not a power of 2.
We allocate 128 addresses.
The subnet mask for this subnet can be found as $n_1 = 32 - \log_2 128 = 25$.
The first address in this block is 14.24.74.0/**25**; the last address is 14.24.74.127/**25**.

ii. A datagram of 3000 bytes with 40 bytes of IP header, received at router R1 and must be forwarded over a link with MTU of 500 bytes. Find out how many fragments need to be created with total length, MF bit, DF bit and offset value of each fragment.

4 Marks

Assume that the DF flag was not set
datagram = 3000 bytes
IP header =40 bytes
MTU = 500 bytes
Data=3000-40=2960bytes
Data in each fragment=500-40=460bytes
Number of fragment=2960/460=6.43=7
Fragment 1: Total length=500bytes, MF=1, DF=0, Offset=0.
Fragment 2: Total length=500bytes, MF=1, DF=0, Offset=57.
Fragment 3: Total length=500bytes, MF=1, DF=0, Offset=115.
Fragment 4: Total length=500bytes, MF=1, DF=0, Offset=172.
Fragment 5: Total length=500bytes, MF=1, DF=0, Offset=230.
Fragment 6: Total length=500bytes, MF=1, DF=0, Offset=287.
Fragment 7: Total length=240bytes, MF=0, DF=0, Offset=345.

iii. What are the advantages and drawback of classful addressing? Explain for each class. **4 Marks**

Advantages:
-Can recognize the class of the address from the address.
Drawbacks:
-Lack of Internal Address Flexibility: Big organizations are assigned large, "monolithic" blocks of addresses that don't match well the structure of their underlying internal networks.

-Inefficient Use of Address Space: The existence of only three block sizes (classes A, B and C) leads to waste of limited IP address space.

iv. -Proliferation of Router Table Entries: As the Internet grows, more and more entries are required for routers to handle the routing of IP datagrams, which causes performance problems for routers. Attempting to reduce inefficient address space allocation leads to even more router table entries.

Question -2

i. Explain why fragmentation occur in network communication with the fields required for fragmentation in IP header. 4 Marks

When a host sends an IP packet onto the network it cannot be larger than the maximum size supported by that local network. This size is determined by the network's data link and IP Maximum Transmission Units (MTUs) which are usually the same. A typical contemporary office, campus or data centre network provided over Ethernet will have 1500 byte MTUs.
However, packets that are initially transmitted over a network supporting one MTU may

- Marks for each part carry equal weightage.
- Marking for Sub-bit given in red colour.

need be routed across networks (such as a WAN or VPN tunnel) with a smaller MTU. In these cases, if the packet size exceeds the lower MTU the data in the packet must be fragmented (if possible). This means it is broken into pieces carried within new packets (fragments) that are equal to or smaller than the lower MTU. This is called Fragmentation and the data in these fragments is then typically reassembled when they reach their destination.
Fragmentation allows for;
Transport layer protocols to be ignorant of the underlying network architecture, reducing overheads.
IP And higher layer protocols to work across variable and diverse network paths and mediums without the need and overhead of a path discovery protocol (but see the PMTUD section).
Fragmentation has a number of drawbacks which result in it's use being avoided where possible, primarily:
The loss of a single fragment results in all the fragments having to be resent where a reliable transport layer protocol such as TCP is in use (in fact the sender resends one packet and fragmentation occurs once again).
Only the first fragment contains the high layer headers which can cause issues with firewalls, middle-boxes and routers (i.e. NAT functionality) that rely on inspecting those headers.
Fragmentation may result in out of order packet delivery and the need for reordering (especially if only some packets are fragmented or if link aggregation or other path splitting technologies are in use).

Ref text book for theoretical descriptions.

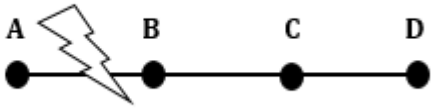
i. Explain the count to infinite problem? What are the approaches used to overcome this in distance vector routing? 4 Marks

Count to infinity problem:

1. One of the important issue in Distance Vector Routing is County of Infinity Problem.
2. Counting to infinity is just another name for a routing loop.
3. In distance vector routing, routing loops usually occur when an interface goes down.
4. It can also occur when two routers send updates to each other at the same time.

Example:

Link Between A & B is Broken



	A	B	C	D
A	0, -	1, A	2, B	3, C
B	1, B	0, -	2, C	3, D
C	2, B	1, C	0, -	1, C
D	3, B	2, C	1, D	0, -

Imagine a network with a graph as shown above in figure 4.8.

As you see in this graph, there is only one link between A and the other parts of the network.

Now imagine that the link between A and B is cut.

At this time, B corrects its table.

After a specific amount of time, routers exchange their tables, and so B receives C's routing table.

Since C doesn't know what has happened to the link between A and B, it says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A).

B receives this table and thinks there is a separate link between C and A, so it corrects its table and changes infinity to 3 (1 for B to C, and 2 for C to A, as C said).

Once again, routers exchange their tables.

When C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said).

This process loops until all nodes find out that the weight of link to A is infinity.

This situation is shown in the table below

In this way, Distance Vector Algorithms have a slow convergence rate.

	B	**C**	**D**
Sum of Weight to A after link cut	∞, A	2, B	3, C
Sum of Weight to A after 1st updating	3, C	2, B	3, C
Sum of Weight to A after 2nd updating	3, C	4, B	3, C
Sum of Weight to A after 3rd updating	5, C	4, B	5, C
Sum of Weight to A after 4th updating	5, C	6, B	5, C
Sum of Weight to A after 5th updating	7, C	6, B	7, C
Sum of Weight to A after nth updating	.....	....	....
∞	∞	∞	∞

One way to solve this problem is for routers to send information only to the neighbors that are not exclusive links to the destination.¬

For example, in this case, C shouldn't send any information to B about A, because B is the only way to A.

ii. You have been allocated a class B network address of 172.168.1.0 and are using the default subnet mask of 255.255.224.0. How may hosts can you have? Write the IP range of each subnetworks. 4 Marks

13 bits used for host address. So toatal no. of hosts are 2^13.

Maximum Subnet-8

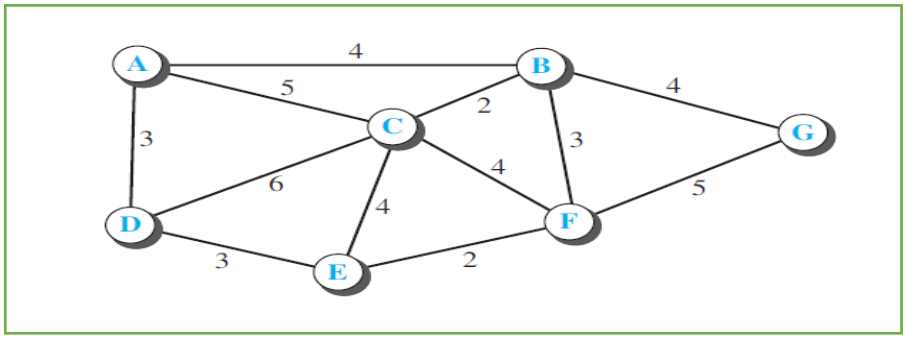
Host per subnet-8190

Ranges are- 172.168.0.1 - 172.168.31.254

Subnet id- 172.168.0.0
Broadcast id- 172.168.31.255

Question -3

i. Use Dijkstra's algorithm to find the shortest path tree and the forwarding table for node A in the following Figure.
(As the diagram not provided in the question so consider remaining two bits equally while awarding marks)



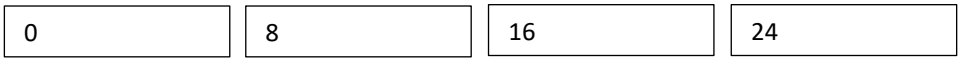
ii. Discuss the significance of MAC address, IP address and port numbers explain each with an example. Can we exclude any address during the communication between source to destination? 6 Marks

All device on the same network subnet have different MAC address so to uniquely identify a end device, MAC address is used. MAC address ensures that the physical address of the end device in same network subnet is unique where as IP address ensures that the logical address of the end device is unique.
MAC address are 12 digit hexadecimal number which is 48 bits in length in which the first 24bits represents ID number of the adapter manufacturer and the second half which is last 24bits represents the serial number assigned to the adapter by the manufacturer.
MAC address are written in extra space or colons or periods such as :
With out any separator : 00A0C914C829
Extra space after every two digits : 00 A0 C9 14 C8 29
Extra space after every four digits : 00A0 C914 C829
Colon after every two digits : 00:A0:C9:14:C8:29
Colon after every four digits : 00A0:C914:C829
Period after every two digits : 00.A0.C9.14.C8.29
Period after every four digits : 00A0.C914.C829
in which 00:A0:C9 represents the manufacturer is Intel Corporation.

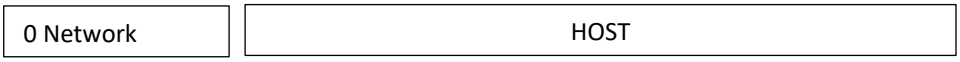
IP address is also used for uniquely identify a computer but refers to the logical address of the computer. IP address is a decimal number that defines the routing information.
IP address composed of four set of numbers and each separated by a decimal point.
IP address are 32 bit binary strings broken up into four 8-bit sequence of which is converted to decimal.
IP address are divided into five classes A,B,C,D,E in which the initial bit determine which class an address belongs to and the class differs in how much of address is taken up with network address and how much of address is taken up with host address.

offsets

- Marks for each part carry equal weightage.
- Marking for Sub-bit given in red colour.
- Ref text book for theoretical descriptions .

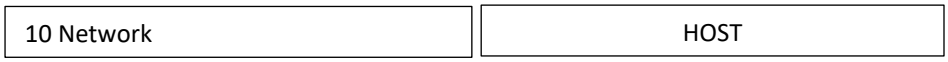


Class A



Range : 1.0.0.0 to 127.255.255.255

Class B

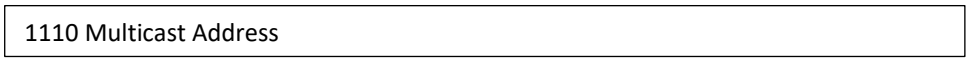


Range : 128.0.0.0 to 191.255.255.255

Class C

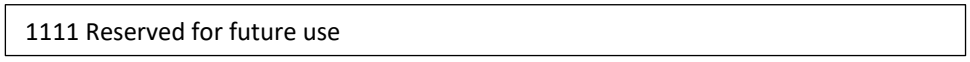
Range : 192.0.0.0 to 223.255.255.255

Class D



Range : 224.0.0.0 to 239.255.255.255

Class E



Range : 240.0.0.0 to 255.255.255.255

For example : 172.168.10.3 belongs to class B
10.10.10.10 belongs to class A
192.168.1.5 belongs to class C

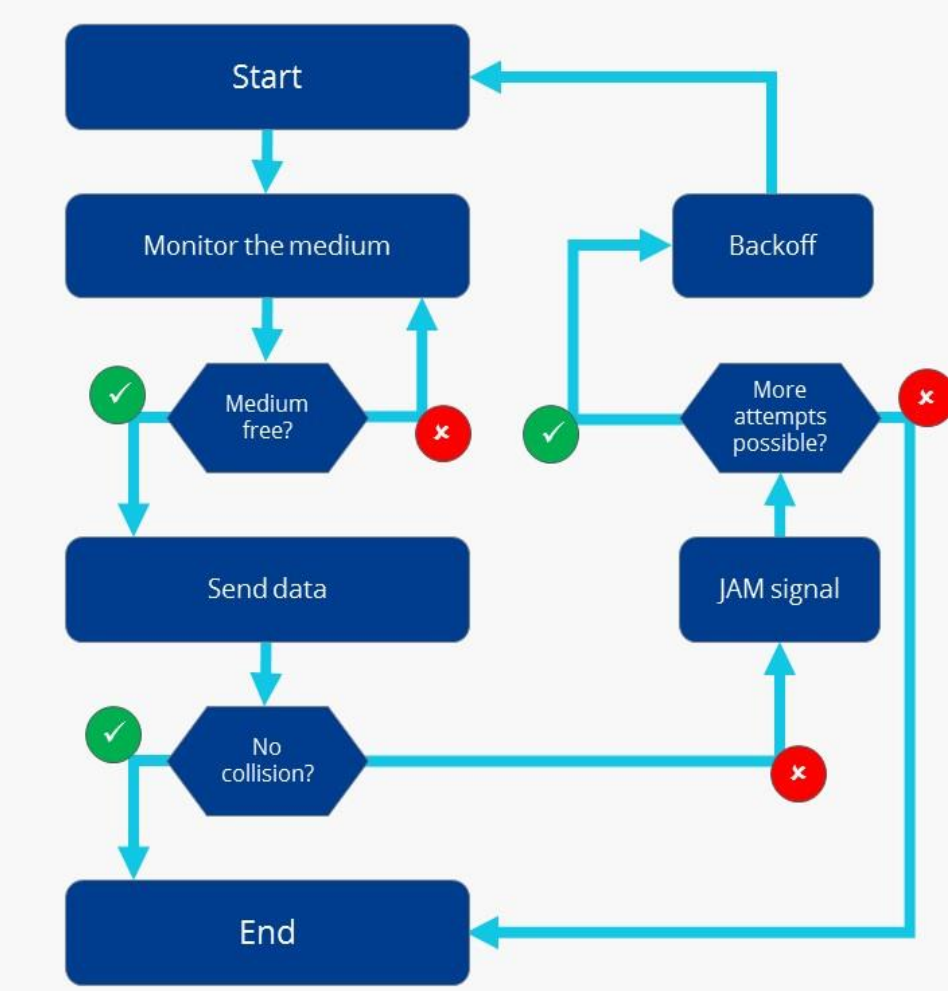
Port number in a network is used to uniquely identify a transaction by specifying both the host and the service. Port numbers are necessary to differentiate between different IP services such as mail service like SMTP, web service like HTTP, file transfer like FTP etc.
Port numbers are 2 bytes in length and can have value from 0 to 65535 depending upon the memory support.
For example in a simple internet mail system for sending service SMTP generally uses TCP port number is 25 and for receiving POP from the client it uses TCP port number 110. So here the port number distinguish the service when both of them running on same host system.

We cannot exclude any address during communication between source to destination.

	iii. Specify the range of port address used for well-known ports and at least mention five port addresses used by popular applications? Mention the Private IP address and their uses. 6 Marks Range of port address for well known ports are from 0 to 1023. 1. File Transfer Protocol (Data Transfer) - 20 2. Simple Mail Transfer Protocol(E-Mail Routing) - 25 3. HTTP(World Wide Web) - 80 4. POP3 - 110 5. HTTPS - 443 6. IMAP - 143 Private IP address used with a local network for unique identification of machine. It is used for communication with in the network. Local network operator creates private IP address using network operating system and these are free of cost. Range of private IP address : 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255 Private IP address are only reserved for use within private or corporate network which cannot be seen outside of the network and they are more secure as compare to the public ones.	
Q. No: 11	Question -1 i. The minimum frame size needed for 10 Mbps Ethernet is 512 bits. For 100 Mbps Ethernet, what should this size (in bits) be if we assume same network diameter? Is this packet size desirable or not? Justify. **6 Marks** Fast Ethernet operates at 100Mbps. For the most part, the scheme/protocol remains the same as the 10Mbps case, except now the maximum length of the network is shortened. Maximum frame size is still kept 512 bits, which now arrive 10 times faster than they do in 10Mbps Ethernet, which the result being that the network must be 10 times smaller, or somewhere around 512 meters, which practical length being somewhere around 250 meters. There is also a new "Auto Negotiation" feature, which allows 100 Mbps Ethernet to talk to the regular Ethernet (10Mbps). i. In which persistent techniques used by CSMA protocol, a channel can be idle at the end of a transmission even when there are nodes with traffic to send. Discuss, why CSMA protocol alone is not able to handle the collision rather a collision detection scheme is added on top of it to handle the same. **6 Marks** In non-persistent CSMA, when a transmitting station has a frame to send and it senses a busy channel, it waits for a random period of time without sensing the channel in the interim, and repeats the algorithm again. It rate of collisions is much reduced than 1-persistent CMSA. This is because each station waits for a random amount of time before attempting retransmission. The probability that multiple stations will wait for same amount of time is extremely low. So, collision between contending stations is greatly reduced. It reduces the bandwidth usage of network. This is because the channel remains idle even if there are stations who have frames to transmit. This occurs since each station wait for a random time before attempting retransmission. There may be multiple stations who are waiting while the channel is idle. CSMA/CD stands for Carrier Sense Multiple Access/Collision Detection, with collision	• Marks for each part carry equal weightage. • Marking for Sub-bit given in red colour. • Ref text book for theoretical descriptions .

detection being an extension of the CSMA protocol. This creates a procedure that regulates how **communication must take place in a network with a shared transmission medium**. The extension also regulates how to proceed if collisions occur i.e. when two or more nodes try to send data packets via the transmission medium (bus) simultaneously and they interfere with one other.

The CSMA/CD process is very similar. First, the station monitors the transmission medium. As long as this is occupied, the monitoring will continue. **Only when the medium is free** and for a certain time (in interframe spacing), will the station send a data packet. Meanwhile, the transmitter continues to monitor the transmission medium to see if it detects any data collisions. If no other participant tries to send its data via the medium by the end of transmission, and no collision occurs, the transmission has been a success. Working of CSMA/CD shown below.



Question -2

i. Describe the Frame format of Ethernet in detail. Justify, why there is a restriction on the minimum as well as maximum frame size of Ethernet.

6 Marks

ii. Explain how CRC is used in detecting errors for the polynomial, g(x)=x^4+x+1. Consider the information sequence 1101011011.

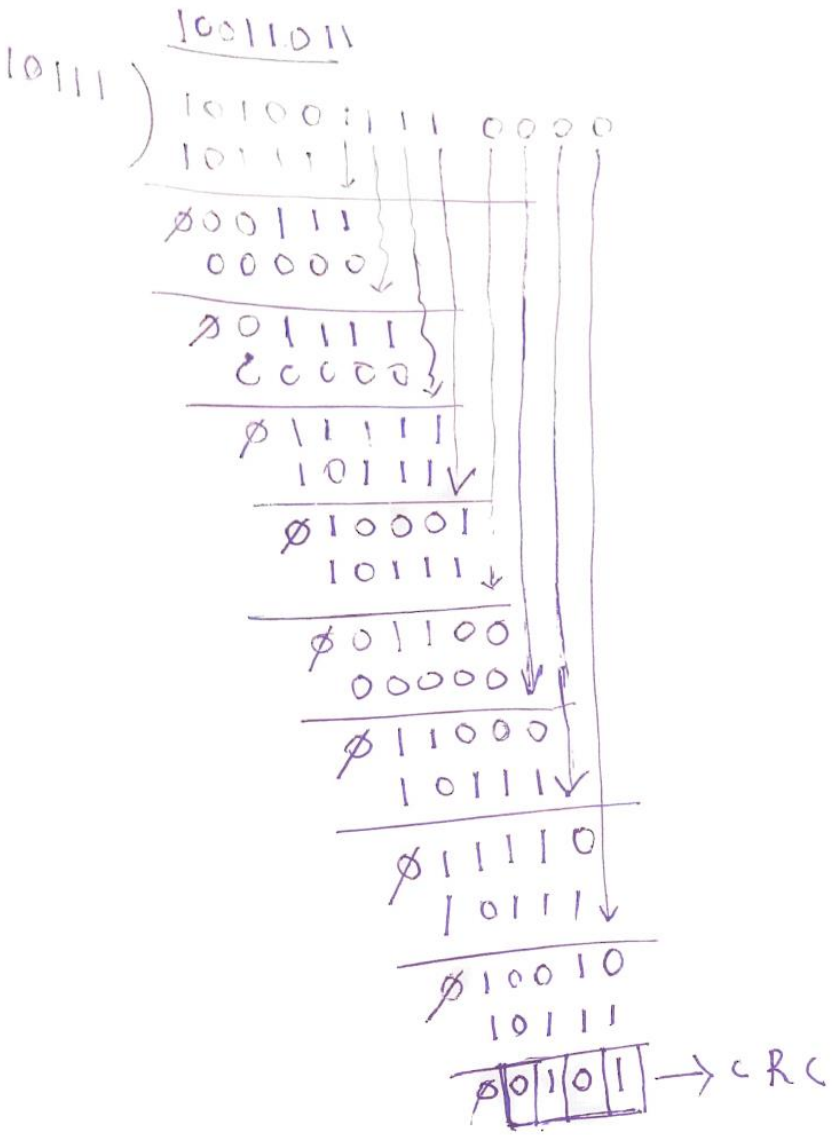
(i) Find the codeword.

(ii) If the code word has error in third bit, what does receiver obtain when it does error checking.

2 Marks+ 2 Marks+ 2 Marks

- Marks for each part carry equal weightage.
- Marking for Sub-bit given in red colour.
- Ref text

		book for theoretical descriptions .
	Question -3 i. Given the data word 101001111 and the divisor 10111, show the generation of the CRC codeword at the sender site. Assume the codeword has not corrupted during transmission and show at the receiver end that the data has received correctly. **6 Marks**	• Marks for each part carry equal weightage. • Marking for Sub-bit given in red colour. • Ref text book for theoretical descriptions .



Code = 10100111100101 ⟶ Send.

At receiver

10111) 10100 1111 0101

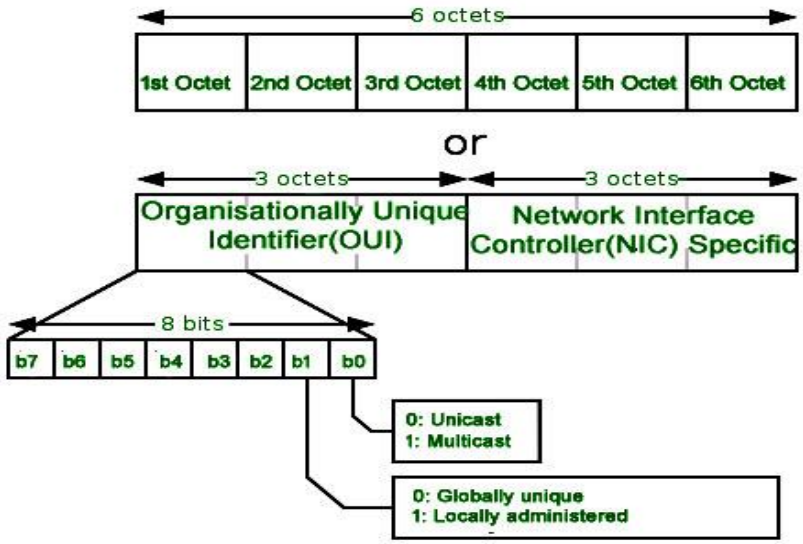
.
.
.
.
.

10000 → Then no error

ii. Explain Addressing and Channel access control mechanism for Ethernet LAN.

6 Marks

Media Access Control Address is a physical address which works at Data Link Layer.
Media Access Control (MAC) Address –
MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers
Logical Link Control(LLC) Sublayer
Media Access Control(MAC) Sublayer
MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.



Format of
MAC Address –
MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (**Organizational Unique Identifier**).
Types of MAC Address –
1. Unicast – A Unicast addressed frame is only sent out to the interface leading to specific NIC. If the LSB (least significant bit) of first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.
2. Multicast – Multicast address allow the source to send a frame to group of devices. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) of first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.
3. Broadcast – Similar to Network Layer, Broadcast is also possible on underlying layer(Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred as broadcast address. Frames which are destined with MAC address FF-FF-FF-FF-FF-FF will reach to every computer belong to that LAN segment

	Channel access control mechanism The channel access control mechanisms provided by the MAC layer are also known as a multiple access method. This makes it possible for several stations connected to the same physical medium to share it. Examples of shared physical media are bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links. The multiple access method may detect or avoid data packet collisions if a packet mode contention based channel access method is used, or reserve resources to establish a logical channel if a circuit-switched or channelization-based channel access method is used. The channel access control mechanism relies on a physical layer multiplex scheme. The most widespread multiple access method is the contention-based CSMA/CD used in Ethernet networks. This mechanism is only utilized within a network collision domain, for example an Ethernet bus network or a hub-based star topology network. An Ethernet network may be divided into several collision domains, interconnected by bridges and switches.	