Evaluation scheme : Computer Network (IT 3001)

Q1.
(a)

Broadcast	**Multicast**
The packet is transmitted to all the hosts connected to the network.	The packet is transmitted only to intended recipients in the network.
One-to-all.	One-to-many.
Broadcasting does not require any group management.	Multicasting requires group management to define the group of hosts/stations which will receive packets.
Bandwidth is wasted.	Bandwidth is utilized efficiently.
Unnecessarily huge amount traffic is generated in the network.	Traffic is under control.
Slow.	Fast.

(b)

- Security: Wireless networks are much more susceptible to unauthorized use. If you set up a wireless network, be sure to include maximum security. You should always enable WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access), which will improve security and help to prevent virtual intruders and freeloaders.
- Interference: Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.
- Inconsistent connections: How many times have you hears "Wait a minute, I just lost my connection?" Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.
- Power consumption: The wireless transmitter in a laptop requires a significant amount of power; therefore, the battery life of laptops can be adversely impacted. If you are planning a laptop project, be sure to have power plugs and/or additional batteries available.
- Speed: The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. In addition, if set up a wireless network at home, and you are connecting to the Internet via a DSL modem (at perhaps 3 Mbps), your wireless access to the Internet will have a maximum of 3 Mbps connection speed.

(c) In connection *Termination* : it takes **four segments** to terminate a connection since a **FIN** and an **ACK** are required in each direction.
(2) means that The received **FIN** (first segment) is acknowledged (**ACK**) by TCP
(3) means that sometime later the application that received the end-of-file will close its socket. This causes its TCP to send a **FIN**. And then the last segment will mean that The TCP on the system that receives this final **FIN** acknowledges (**ACK**) the **FIN**.

(d) Bridges are important in some networks because the networks are divided into many parts geographically remote from one another. Something is required to join these networks so that they can become part of the whole network. Take for example a divided LAN, if there is no medium to join these separate LAN parts an enterprise may be limited in its growth potential. The bridge is one of the tools to join these LANS.
Secondly a LAN (for example Ethernet) can be limited in its transmission distance. We can eliminate this problem using bridges as repeaters, so that we can connect a geographically extensive network within the building or campus using bridges. Hence geographically challenged networks can be created using Bridges.

Third, the network administrator can control the amount of traffic going through bridges sent across the expensive network media.

Fourth, the bridge is plug and play device so there is no need to configure the bridge. And suppose any machine was taken out from the network then there is no need for the network administrator to update the bridge configuration information as bridges are self configured. And also it provide easiness for the transfer of Data. Useful for data transfer.

(e)

1-persistent: 1-persistent CSMA is an aggressive transmission algorithm. When the transmitting node is ready to transmit, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits the message (a frame) unconditionally (i.e. with probability=1). In case of a collision, the sender waits for a random period of time and attempts the same procedure again. 1-persistent CSMA is used in CSMA/CD systems including Ethernet.

P-persistent: This is an approach between 1-persistent and non-persistent CSMA access modes. When the transmitting node is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits with probability *p*. If the node does not transmit (the

probability of this event is *1-p*), it waits until the next available time slot. If the transmission medium is not busy, it transmits again with the same probability *p*. This probabilistic hold-off repeats until the frame is finally transmitted or when the medium is found to become busy again (i.e. some other node has already started transmitting). In the latter case the node repeats the whole logic cycle (which started with sensing the transmission medium for idle or busy) again. p-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.

(f) The **jam signal** or **jamming signal** is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations of the collision and that they must not transmit.

(g) (1) TCP gives guarantee that a packet will reach on the destination without any duplication and the order of data will be same. On the other hand UDP does not give guarantee that data will reach on destination. it does not gives guarantee that data will be in the same order and it also does not give guarantee that data will reached on destination without any duplication.
(2) TCP is a reliable protocol but UDP is unreliable protocol.
(3) Data transmission is more dependable on TCP than UDP.
(4) As TCP is connection oriented protocol, it means that connection must be open between two ends before sending data. So both ends know all the things between a session as when the connection is closed and when it is opened. But in UDP when you send the data from one end then we cannot know whether data is reaching on the other end or not. As we just hope that it will reach on destination.

(h) For class C address, size of network field is 24 bits. But first 3 bits are fixed as 110; hence total number of networks possible is 2^{21}.

(I) There are some benefits from this arrangement, including:

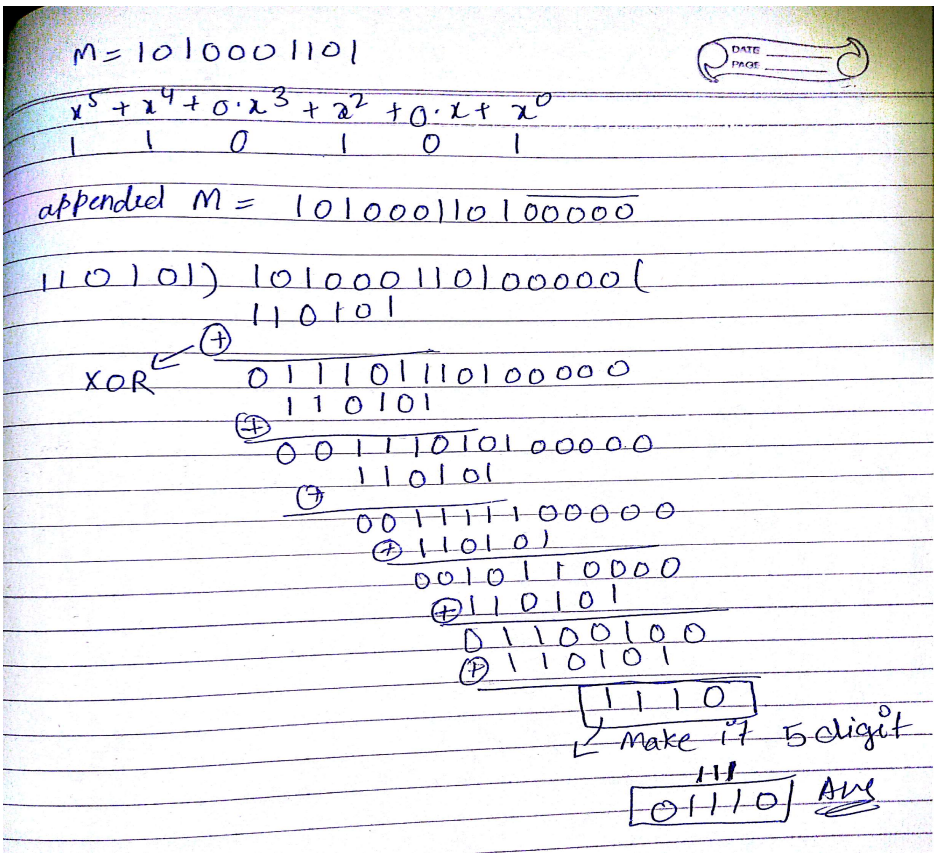
- There's no need for complicated framing on the control connection.
- Handling special cases, like cancelling a data connection, is simpler.
- You can have multiple transfers running at a time without having to establish multiple control connections.
- It enables a trick, known as FXP, that can allow you to make two FTP servers exchange data directly between each other.

(j) IP Address : 32-bit logical Address (Can be changed)
MAC Address : 48-bit physical address (Can't be changed)
SO, imagine your name as IP Address, which you can change at any point of time. And your residence as a MAC address, which you can only change when you shift your home. But can you change your name by shifting your body.. NO. right.

ARP : Address Resolution Protocol : Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

Q2.
(a) M = 1010001101
Divisor polynomial: 1.x5 +1.x4+0.x3+1.x2+0.x2+1.x0
Divisor polynomial bit= 110101
Bits to be appended to message= (divisor polynomial bits – 1) = 5
Append 5 zeros to message bits, modified message: 101000110100000

Now, divide and XOR the message with divisor polynomial bits. Make resultant reminder to 5 bit again and that is the CRC send along with the message.



(b) Piggybacking- 1 marks, selective repeat- 3 marks.

Q3.

(a)

- Distance = 3000 km
- Bandwidth = 1.536 Mbps
- Packet size = 64 bytes
- Propagation speed = 6 µsec / km

Calculating Transmission Delay-

Transmission delay (T_t)

= Packet size / Bandwidth

= 64 bytes / 1.536 Mbps

= (64 x 8 bits) / (1.536 x10^6 bits per sec)

= 333.33 µsec

Calculating Propagation Delay-

For 1 km, propagation delay = 6µsec

For 3000 km, propagation delay = 3000 x6µsec =18000µsec

Calculating Value Of 'a'-

$a = T_p / T_t$

a = 18000µsec / 333.33 µsec

a = 54

Calculating Bits Required in Sequence Number Field-

Bits required in sequence number field

$= \lceil \log_2(1+2a) \rceil$

$= \lceil \log_2(1 + 2 \times 54) \rceil$

$= \lceil \log_2(109) \rceil$

$= \lceil 6.76 \rceil$

= 7 bits

Thus,

- Minimum number of bits required in sequence number field = 7
- With 7 bits, number of sequence numbers possible = 128
- We use only (1+2a) = 109 sequence numbers and rest remains unused.

(b) pkt switch VS circuit switch -4marks

Q4.
(a) Recursive and iterative DSN queries -2marks, one or more resource records in DNS reply- 2marks.

(b) In CSMA/CD, the transmitting node is listening for collisions while it transmits it's frame. Once it has finished transmitting the final bit without hearing a collision, it assumes that the transmission was successful. In this worst-case collision scenario, the time that it takes for a Node to detect that its frame has been collided with is twice the propagation delay. Hence to confirm that the collision has not occurred the condition for the minimum size of the packet is:

RTT = Transmission Time

Transmission Time = Length of packet / Bandwidth
RTT = 2 (d/v) = 2(2000/2×108)

Therefore to find minimum size of the packet,
RTT = Length of packet / Bandwidth
Length of packet = RTT x Bandwith
= 2(2000/2×108) x 107 = 200bits = 25bytes

Therefore, minimum size of the packet = 25bytes

Q5.
(a) – 4marks
(b) Maximum number of subnets = 2^6-2 =62.
Note that 2 is subtracted from 2^6. The RFC 950 specification reserves the subnet values consisting of all zeros (see above) and all ones (broadcast), reducing the number of available subnets by two.
Maximum number of hosts is 2^10-2 = 1022.
2 is subtracted for Number of hosts is also. The address with all bits as 1 is reserved as broadcast address and address with all host id bits as 0 is used as network address of subnet.
In general, the number of addresses usable for addressing specific hosts in each network is always 2^N – 2 where N is the number of bits for host id.

Q6.
(a) Congestion -1marks, TCP congestion control -3marks.
(b) Current size of congestion window in terms of number of segments
= (Size in Bytes)/(Maximum Segment Size)
= 32KB / 2KB
= 16 MSS

When timeout occurs, in TCP's Slow Start algorithm, threshold is reduced to half which is 16KB or 8MSS. Also, slow start phase begins where congestion window is increased twice. So from 1MSS to 8 MSS window size will grow exponentially.
Congestion window becomes 2MSS after one RTT and becomes 4MSS after 2 RTTs and 8MSS after 3 RTTs. At 8MSS, threshold is reached and congestion avoidance phase begins. In congestion avoidance phase, window is increased linearly. So to cover from

8MSS to 16MSS, it needs 8 RTTs

Together, 11RTTs are needed (3 in slow start phase and 8 in congestion avoidance phase).

Q7.
(a) IPV4 -4marks
(b) The maximum size of data field in each fragment = 480 (20 bytes IP header).
Thus the number of required fragments $= \left\lceil \frac{3000 - 20}{480} \right\rceil$
= 7

Each fragment will have Identification number 422. Each fragment except the last one will be of size 500 bytes (including IP header). The last datagram will be of size 120 bytes (including IP header). The offsets of the 7 fragments will be 0, 60, 120, 180, 240, 300, 360. Each of the first 6 fragments will have flag=1; the last fragment will have flag=0.

Q8.
(a) -4marks
(b) -4marks
(c) -4marks