USN | | | | | | | | | | |

Sub:	Computer Communication Networks					Sub Code:
Date:	16/12/2021	Duration:	90 Minutes	Max Marks:	50	Sem / Sec:

Answer any FIVE FULL Questions

1 Explain CSMA and explain the behavior of three persistence methods of CSMA.

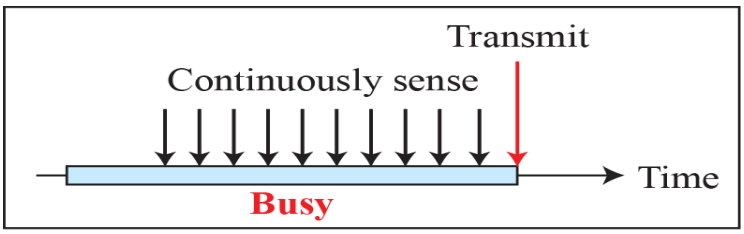
CSMA Explanation 4M

Persistence Methods 3 X 2 M (1 M diagram + 1 M Explanation

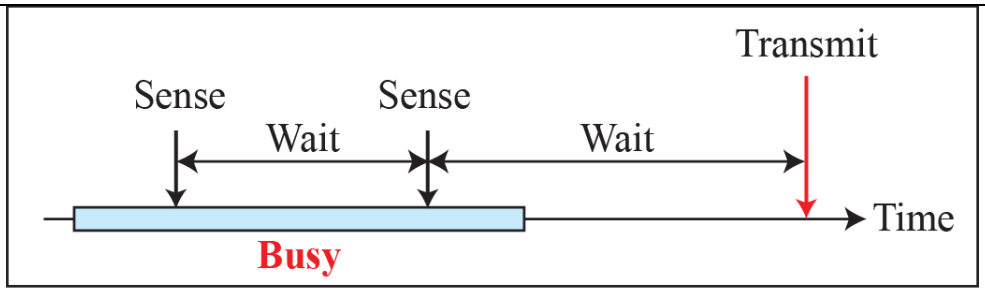
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- Each station "sense before transmit" or "listen before talk."
- CSMA can reduce the possibility of collision, but it cannot eliminate it.
- The possibility of collision still exists because of propagation delay(first bit)
- Vulnerable Time: The vulnerable time for CSMA is the propagation time Tp .
- This is the time needed for a signal to propagate from one end of the medium to the other

Persistence Methods

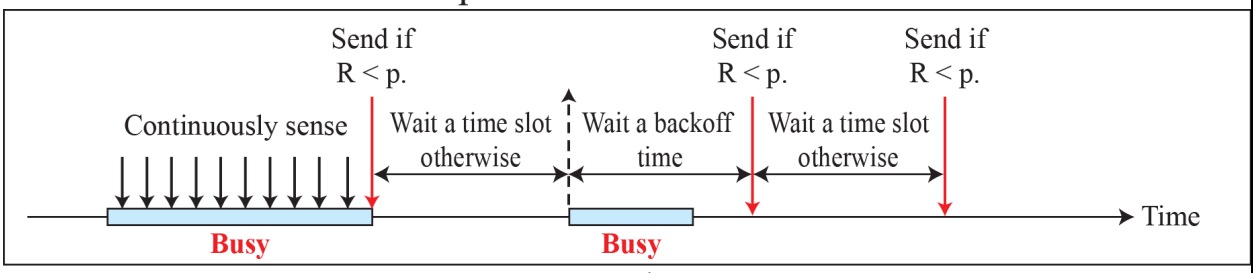
- What should a station do if the channel is busy?
- What should a station do if the channel is idle?
- Three methods : the 1-persistent method, the non persistent method, and the p-persistent method.
- **1-Persistent :**
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).
  This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately
- **Non persistent** ; In the non persistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.
- The non persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.
- **p-Persistent:**
- combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.
- In this method, after the station finds the line idle it follows these steps:
- 1. With probability *p, the station sends its frame.*
- 2. With probability *q = 1 - p, the station waits for the beginning of the next time slot* and checks the line again.
- a. If the line is idle, it goes to step 1.
- b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.



a. 1-persistent



b. Nonpersistent

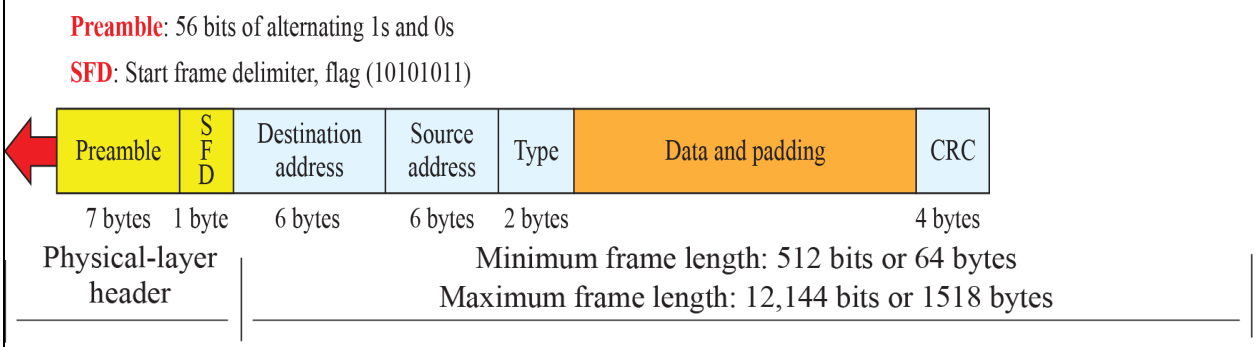


c. *p*-persistent

1-Persistent-after station finds the line idle, send its frame
Nonpersistent-senses the line; idle: sends immediately; not idle: waits random amount of time and senses again
p-Persistent-the channel has time slots with duration equal to or greater than max propagation time

2 Explain the IEEE frame format of standard Ethernet with neat diagram. What are the minimum and maximum frames lengths?

Diagram 4M
Explanation 4 M
Min & Max -2 M



Preamble. 7 bytes (56 bits) of alternating Os and Is that alerts the receiving system to the coming frame and enables it to synchronize its input timing.
The preamble is actually added at the physical layer and is not (formally)
part of the frame.
Start frame delimiter (SFD). (l byte: 10101011) the beginning of the frame.
The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address
Destination address (DA). 6 bytes and contains the physical address of the destination station or stations to receive the packet.
Source address (SA). 6 bytes and contains the physical address of the sender of the packet
Type. Gives the upper layer protocol whose packet is encapsulated in the frame. Eg- ARP,IP,OSPF.
Data. minimum of 46 and a maximum of 1500 bytes.If packet is <46 bytes padding is added
CRC. contains error detection information, in this case a CRC-32

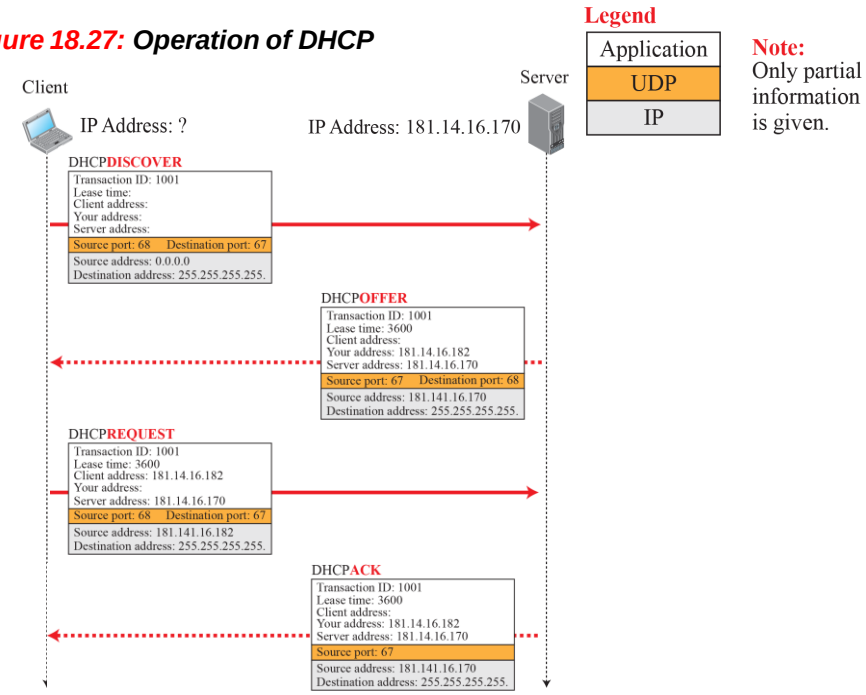
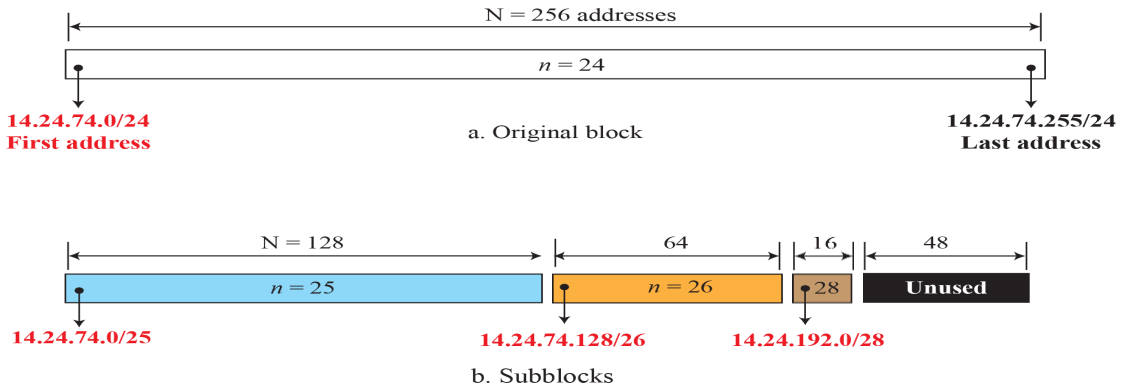
3	Explain the operation of DHCP with figure. **Diagram 7 M** **Explanation 3 M** address assignment in an organization can be done automatically using the Dynamic Host Configuration Protocol (DHCP). DHCP is an application-layer program, using the client-server paradigm ***Figure 18.27: Operation of DHCP***  18.51
4	An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 sub blocks of addresses to use in its three subnets: one sub block of 10 addresses, one sub block of 60 addresses, and one sub block of 120 addresses. Design the sub blocks. Find out the total number of unused address. **Each sub block 3 M =3 X 3M** **, unused address 1 M** **Solution** 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 subblocks, starting with the largest and ending with the smallest one. a. The number of addresses in the largest subblock, 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**. **b.** The number of addresses in the second largest subblock, 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**. **c.** The number of addresses in the smallest subblock, which requires 10 addresses, is not a power of 2. We allocate 16 addresses. The subnet mask for this subnet can be found as $n_1 = 32 - \log_2 \boldsymbol{16} = 28$. The first address in this block is 14.24.74.192/**28**; the last address is 14.24.74.207/**28** If we add all addresses in the previous subblocks, the result is 208 addresses, which means 48 addresses are left in reserve.

Figure 18.23: Solution to Example 4.5



18.44

5

a. Write the IP address in decimal dotted notation and find the class for following addresses.

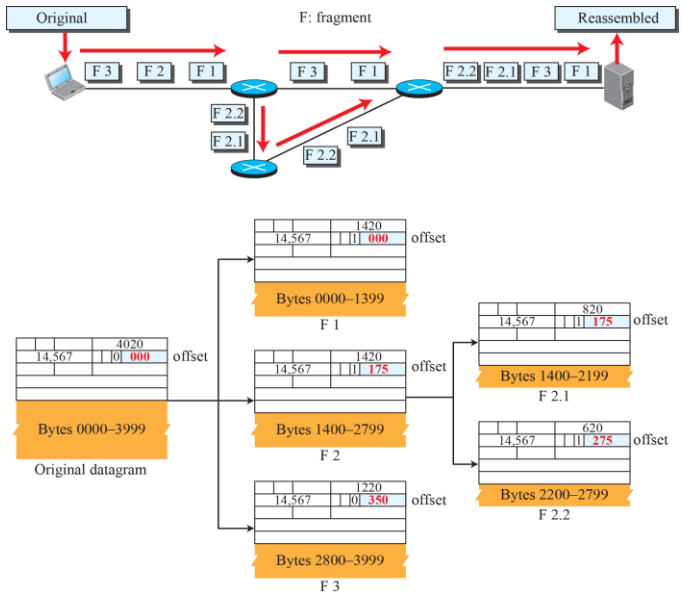
(i) 01110111 11110011 10000000 11011101
119.243.128.221 -**1M**
Class A- **1M**

(ii) 11101111 11000000 11110010 00011101
239.192.242.29 – **1M**
Class D- **1M**

b. Explain Fragmentation with the help of an example.
Diagram 5 M explanation 1 M

A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.

Figure 19.7: Detailed fragmentation example



19.89

6 Explain distance vector routing algorithm with some example. Also discuss two node infinity problem

Distance vector diagram – 3 M
Updating Diagram 3M
Explanation 2 M
Count to infinity problem – 2M

DISTANCE-VECTOR ROUTING

- The distance-vector (DV) routing uses the goal to find the best route.
- The first thing each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbors.
- The incomplete trees are exchanged between immediate neighbors to make the trees more and more complete and to represent the whole internet.
- router continuously tells all of its neighbors what it knows about the whole internet,
  (although the knowledge can be incomplete).

Figure 20.5: ***The first distance vector for an internet***

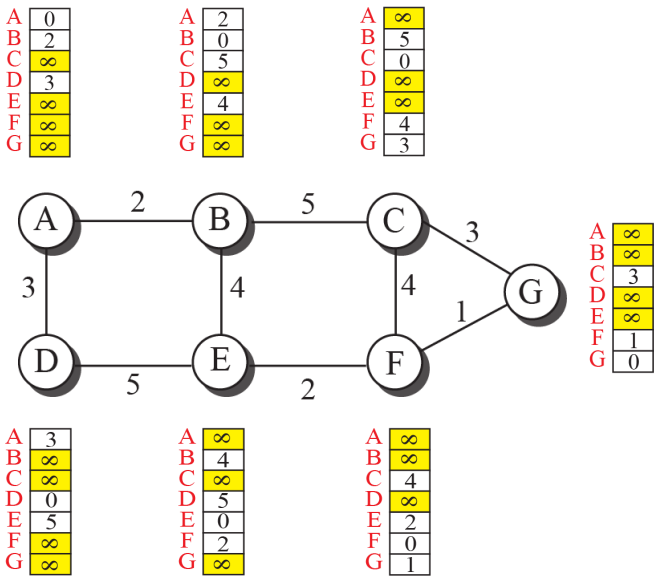
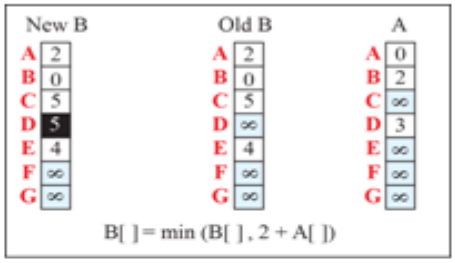
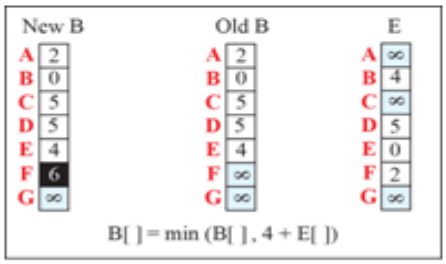


Figure 20.6: Updating distance vectors



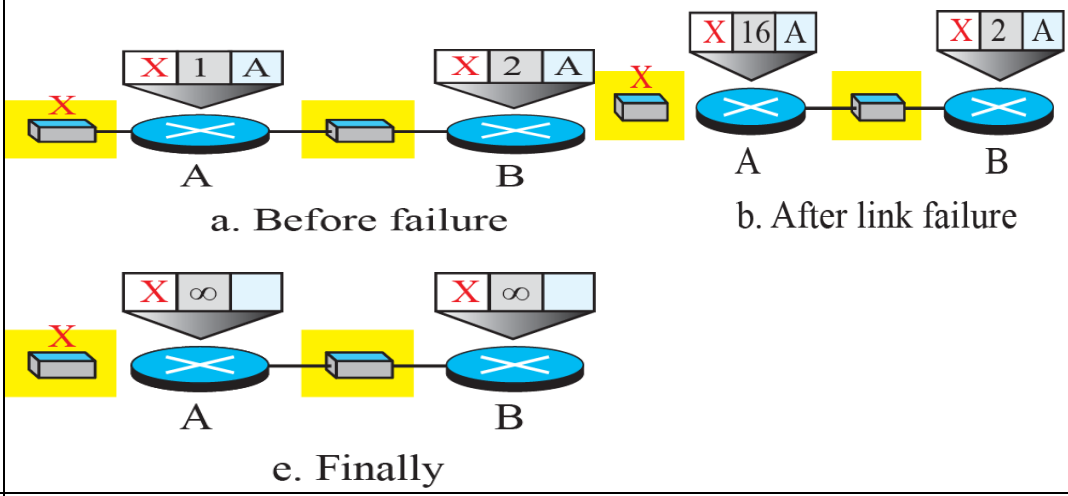
a. First event: B receives a copy of A's vector.

Note:
X[ ]: the whole vector



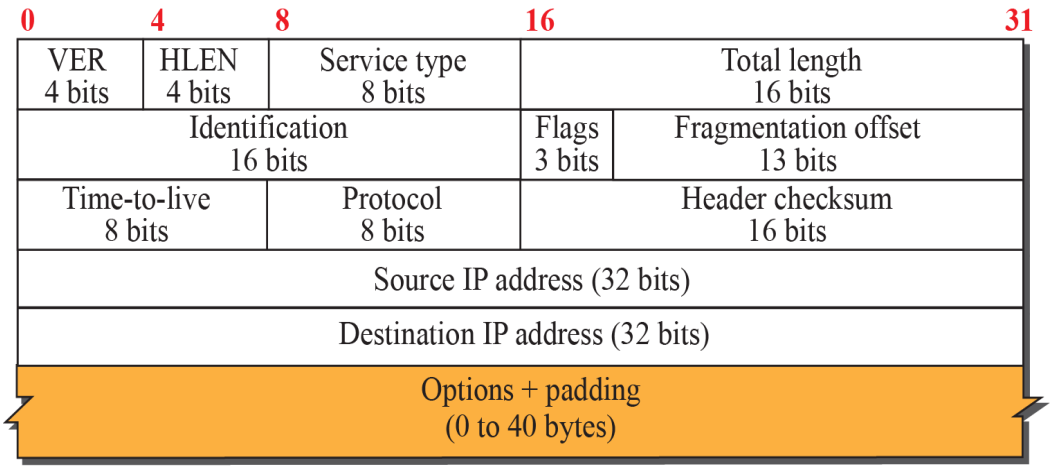
b. Second event: B receives a copy of E's vector.

20.70



7 a. Explain the IPV4 datagram frame format with neat diagram.

Diagram 4 M
Explanation 3 M



b. Header format

Version (VER). This 4-bit field defines the version of the IPv4 protocol. Currently the version is 4.
o Header length (HLEN). This 4-bit field defines the total length of the datagram header in 4 byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
o Services. This field, previously called service type, is now called differentiated services.
The total length field defines the total length of the datagram including the header.
o Identification,Flags, Fragmentation offset.- used in fragmentation
Time to live. A datagram has a limited lifetime in its travel through an internet.
This field was originally designed to hold a timestamp, which was decremented by each visited router.
The datagram was discarded when the value became zero
Protocol. This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IPv4 datagram is delivered
Checksum. The checksum
o Source address. This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.
o Destination address. This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

b. Identify if the following Ethernet MAC addresses are unicast, multicast or broadcast. **3M**

i) 41:20:1B:2E:08:EE- MULTICASTING
ii) 4A:FF:10:01:11:00-UNICASTING
iii) FF:FF:FF:FF:FF:FF.-BROAD CASTING

8 Create the shortest path tree for the following network graph using Dijkstra Algorithm.

Explanation 3 M
Diagram 7M

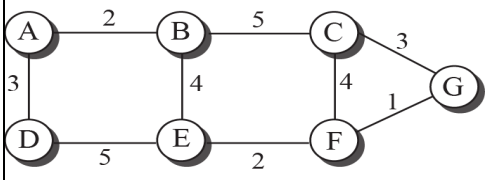


***Figure 20.10:* Least-cost tree**