Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058, India
(Autonomous College Affiliated to University of Mumbai)

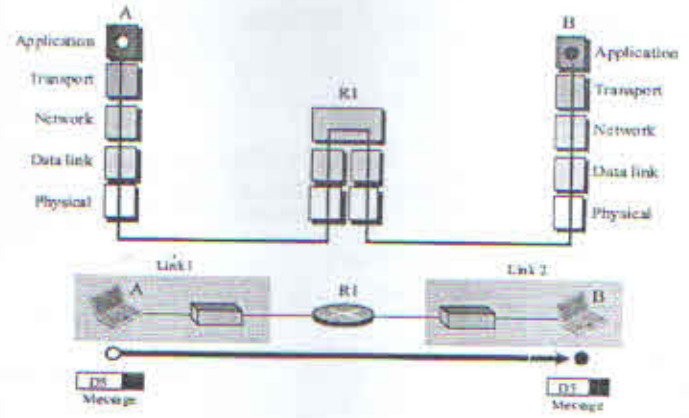
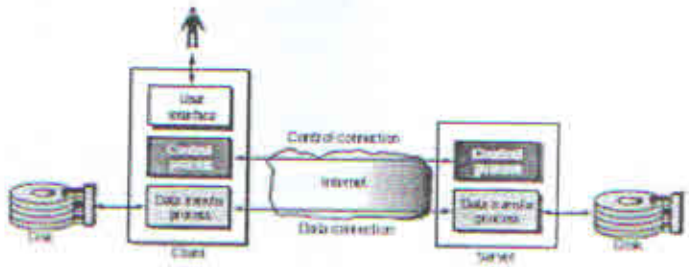
End Semester Examination

May-2/05/2018

Max. Marks: 100 Duration: 3 Hr
Class: T.E. Semester: VI
Course Code: ETC603 Branch: Electronics and Telecommunication
Name of the Course: Computer Communication Telecom Networks

Instruction:
(1) All questions Q1-Q5 are compulsory
(2) Assume suitable data if necessary
(3) Draw neat diagrams

Q No.		Max. Marks	CO
Q.1 (a)	What is the role of transport layer in OSI model Service Point Addressing: Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer. Segmentation and Reassembling: A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission. Connection Control: It includes 2 types: Connectionless Transport Layer : Each segment is considered as an independent packet and delivered to the transport layer at the destination machine. Connection Oriented Transport Layer : Before delivering packets, connection is made with transport layer at the destination machine. Flow Control: In this layer, flow control is performed end to end. Error Control: Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.	1*5=5	CO1
Q.1 (b)	Differentiate between layering architecture and TCP/IP protocol suit 1.TCP/IP is a client-server model, i.e. when the client requests for service it is provided by the server. Whereas, OSI is a conceptual model. 2.TCP/IP is a standard protocol used for every network including the Internet, whereas, OSI is not a protocol but a reference model used for understanding and designing the system architecture. 3.TCP/IP is a four layered model, whereas, OSI has seven layers. 4.TCP/IP follows Vertical approach. On the other hand, OSI Model supports Horizontal approach. 5.TCP/IP is Tangible, whereas, OSI is not. 6.TCP/IP follows top to bottom approach, whereas, OSI Model follows a bottom-up approach. 7.OSI model has a problem of fitting the protocols into the model.TCP/IP model does not fit any protocol 8.OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.	10	CO1

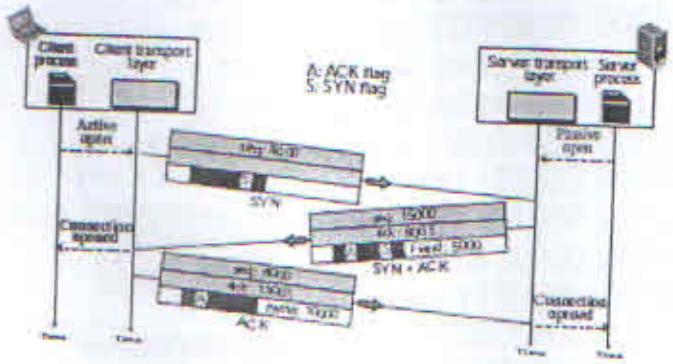
	OR		
Q.1 (b)	Show the communication at application layer for the simple private internet	10	CO1
			
Q.1 (c)	Explain the working principle of basic model of FTP	1+4=5	CO1
			

	The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred. Connections The two FTP connections, control and data, use different strategies and different port numbers. Control Connection The control connection is created in the same way as other application programs described so far. There are two steps: 1. The server issues a passive open on the well-known port 21 and waits for a client. 2. The client uses an ephemeral port and issues an active open. The connection remains open during the entire process. The service type, used by the IP protocol, is minimize delay because this is an interactive connection between a user (human) and a server. The user types commands and expects to receive responses without significant delay. Figure 21.2 shows the initial connection between the server and the client. Data Connection The data connection uses the well-known port 20 at the server site. However, the creation of a data connection is different from what we have seen so far. The following shows how FTP creates a data connection: 1. The client, not the server, issues a passive open using an ephemeral port. This must be done by the client because it is the client that issues the commands for transferring files 2. The client sends this port number to the server using the PORT command (we will discuss this command shortly). 3. The server receives the port number and issues an active open using the wellknown port 20 and the received ephemeral port number.		
Q.2 (a)	Describe the steps of connection establishment in 3 way handshaking in TCP	2+8=10	CO4

Three-Way Handshaking-The connection establishment in TCP is called three-way handshaking. In our example,an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol. The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This request is called a passive open. Although the server TCP is ready to accept a connection from any machine in the world, it cannot make the connection itself. The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP to connect to a particular server. TCP can now start the three-way handshaking process as shown in Figure To show the process we use time lines. Each segment has values for all its header fields and perhaps for some of its option fields too. However, we show only the few fields necessary to understand each phase. We show the sequence number, the acknowledgment number, the control flags (only those that are set), and window size if relevant. The three steps in this phase are as follows. 1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. The client in our example chooses a random number as the first sequence number and sends this number to the server. This sequence number is called the initial sequence number (ISN). Note that this segment does not contain an acknowledgment number. It does not define the window size either; a window size definition makes sense only when a segment includes an acknowledgment. The segment can also include some options that we discuss later in the chapter. Note that the SYN segment is a control segment and carries no data. However, it consumes one sequence number. When the data transfer starts, the ISN is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing one imaginary byte..

2.The server sends the second segment, a SYN + ACK segment with two flag bits set:SYN and ACK. This segment has a dual purpose. First, it is a SYN segment for communication in the other direction. The server uses this segment to initialize a sequence number for numbering the bytes sent from the server to the client. The server also acknowledges the receipt of the SYN segment from the client by setting the ACK flag and displaying the next sequence number it expects to receive from the client. Because it contains an acknowledgment, it also needs to define the receive window size, rwnd (to be used by the client), as we will see in the flow control section.

The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers. The client must also define the server window size. Some implementations allow this third segment in the connection phase to carry the first chunk of data from the client. In this case, the third segment must have a new sequence number showing the byte number of the first byte in the data. In general, the third segment usually does not carry data and consumes no sequence numbers.



Q.2 (b) Compare the TCP header and the UDP header. List the fields in the TCP header that are not part of the UDP header. Give the reason for each missing field. 5 CO4

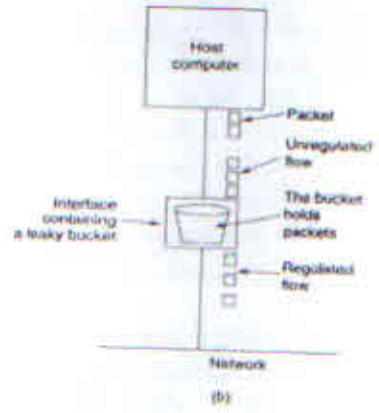
Fields	*UDP*	*TCP*	*Purpose*
Source Port Number	√	√	To define the source port number
Destination Port Number	√	√	To define the destination port number
Checksum	√	√	For error control
Total Length	√		It is not actually needed even in UDP
Sequence Number		√	For flow control
Acknowledgment Number		√	For flow control
Header Length		√	To define variable header length in TCP
Control Bits		√	To define different type of segments
Urgent Pointer		√	To define the end of urgent data
Options And Padding		√	To make TCP to use different options

OR

Q.2 (b) Explain the steps of checksum calculation using UDP protocol with example. 1+1+3=5 CO4

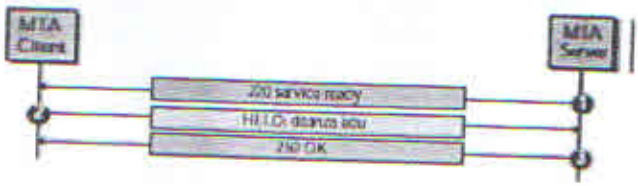
	10011001 00010010 → 153.18 00001000 01101001 → 8.105 10101011 00000010 → 171.2 00001110 00001010 → 14.10 00000000 00010001 → 0 and 17 00000000 00001111 → 15 00000100 00111111 → 1087 00000000 00001101 → 13 00000000 00001111 → 15 00000000 00000000 → 0 (checksum) 01010100 01000001 → T and E 01010011 01010100 → S and T 01001001 01001110 → I and N 01000111 00000000 → G and 0 (padding) 10010110 11101011 → Sum 01101001 00010100 → Checksum		
Q.2 (c)	In what way token bucket algorithm is superior to leaky bucket algorithm Token Bucket :The leaky bucket is very restrictive. It does not credit an idle host. For example, if a host is not sending for a while, its bucket becomes empty. Now if the host has bursty data, the leaky bucket allows only an average rate. The time when the host was idle is not taken into account. On the other hand, the token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1,000 ticks with 10 cells per tick. In other words, the host can send bursty data as long as the bucket is not empty. Figure The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1. Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data	1+4=5	CO4

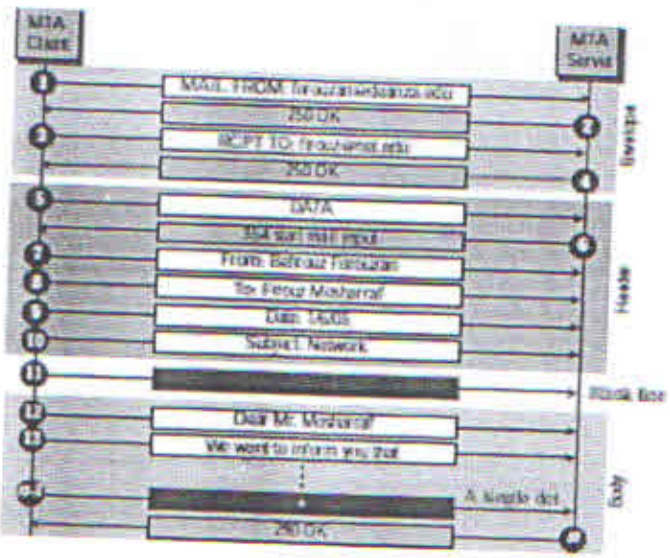
(a) A leaky bucket with water.

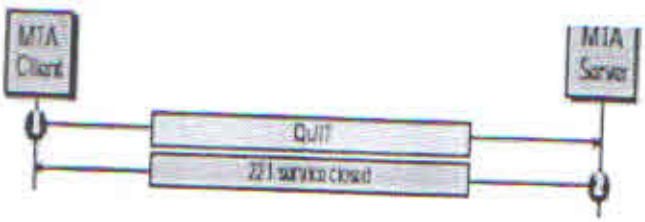


(b) a leaky bucket with packets.

Q.3 (a) Explain the phases of mail transfer with suitable diagram . 2+8=10 CO5

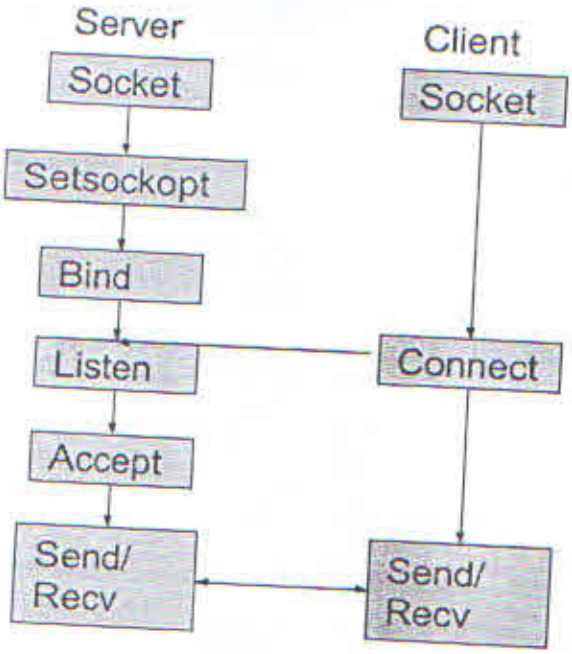






OR

Q.3 (a)	What is role of DNS in Internet? Explain the types of resolver. The process of converting a website name to an IP address consists of 2 steps. When we enter a website name into a web browser, II) types of Resolution i) Iterative Resolution ii) Recursive Resolution 1. Converts website name into the nameserver of the web hosting provider. 2. Converts the nameserver into the IP address of the server on which the website is hosted.	2+8=10	CO5
Q.3 (b)	What is socket programming? State and Explain the client server model Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket(node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server. What is socket programming? Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket(node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server.	1+4=5	CO5



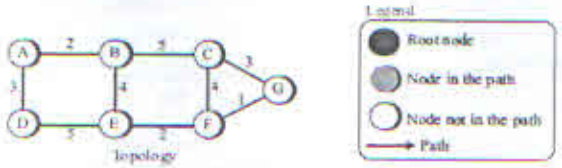
Q.3 (c)	Find the value of flags(in hexadecimal) field in DNS for a query message requesting an address and demanding a recursive answer.	5	CO5

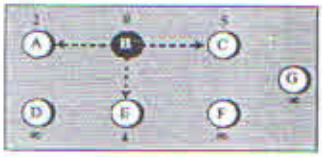
The following shows the individual fields.

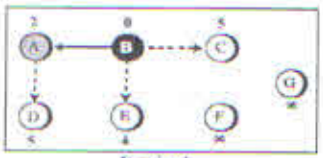
QR	OpCode	AA	TC	RD	RA	Three 0's	rCode
0	0000	0	0	1	0	000	0000

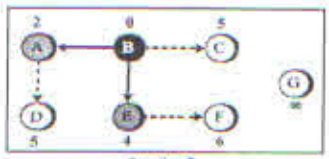
The flag is then $(00000001\ 0000000)_2$ or $(0100)_{16}$.

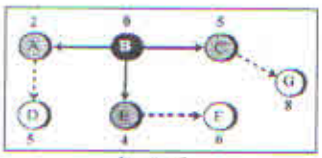
Q.4 (a)	Use the Dijkstra algorithm to find the shortest path tree for node B from the given Figure.	8+2=10	CO3

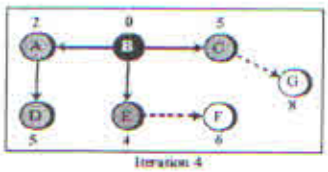


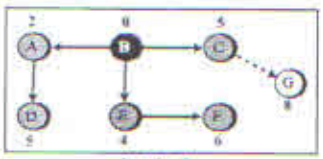


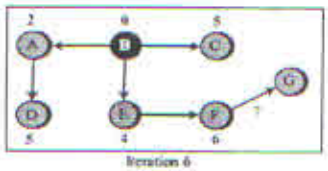










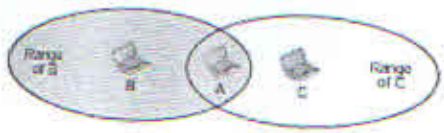


Q.4 (b)	List the features of OSPF. How bidirectional connection establish by OSPF?	2+8=10	CO3

	OSPF has the following features: a) It is effectively loop-free, having a maximum hop metric of 65,535 b) It can load balance network traffic between multiple paths of the same metric value c) It supports authentication using passwords and other methods d) It converges quicker than RIP since routing updates are sent immediately instead of periodically e) It uses less bandwidth since transmission take place only when routing changes occur f) It supports the logical grouping of network segments into areas (see the "Autonomous System" section below) g) It announces routes outside of an autonomous system within the autonomous system so that it can calculate costs to reach outside networks h) Since OSPF announces subnet masks, it supports CIDR , VLSM (Variable Length Subnetting), Supernetting (used to aggregate Class C networks) and non-contiguous network segments OSPF Message Types 		
	OR		
Q.4 (b)	What do you mean by 2 node instability in DVR ? How it is overcome?	4+6=10	CO3

	At the beginning both nodes A and B know how to reach node X. • Suddenly, link between A and X fails, and node a changes its table. • If A can send its table to B immediately, everything is fine. • Otherwise, if B sends its routing table to A before receiving A's routing table, the system becomes unstable. • Node A receives the update, assuming that B has found a way to reach X, and immediately updates the table. • Based on triggering update strategy, A send its new update to B. • Now, B thinks, something has changed around A and updates its routing table. • Node A thinks that route to X is through B and B thinks that route to X is through A. • In this way, the cost of reaching X gradually increases until it reaches infinity. • Lastly, both A and B get to know that X cannot be reached, and the system becomes unstable. Solution to Two-node Loop Instability:- 1.Defining Infinity 2. Split Horizon 3. Split Horizon and Poison Reverse Defining Infinity • The first obvious solution is to minimize or redefine infinity to a smaller number. • The infinity should be –Max (size of the network in each direction) + 1 , if the distance between each hop is considered as 1.Generally, in most implementations of distance vector routing protocol infinity is defined as 16. So, the size of the network in each direction should be 15.From here , DVR protocol cannot be used in large networks. Split Horizon • When node B gets A's table and thinks that optimum route to reach X is through A, it does not need to advertise this information to A; as the information has come from A only. • Node A keeps the value of the distance to X as infinity. • Later, when node A sends its routing table to B, node B also corrects its routing table. • As a result, the system becomes stable after the first update, i.e. both A and B knows that X is not reachable. Poison Reverse There is problem with split horizon- Distance Vector uses timer and if there are no news about a route , the node deletes the route from its table. In our scenario, when node B eliminates the route to X from its advertisement to X, node A cannot guess that this is due to split horizon or because B has not received any news about X recently.so to avoid this problem Split Horizon, is combined with another strategy called Poison Reverse.Node B can still advertise the value for X , but if the source of information is A, it can replace the distance with infinity as a warning:"Do not use this value, what I know about this route comes from you."		
Q.5 (a)	Classify the physical media for computer networks. Comment on ADSL and HFC technology	2+8=10	CO2

	Copper Coaxial Cable - Thick or Thin Unshielded Twisted Pair - CAT 3,4,5,5eand6 Optical Fiber Multimode Singlemode Wireless Short Range Medium Range (Line of Sight)Satellite DSL (ADSL): ADSL, like a 56K modem,provides higher speed (bit rate) in the downstream direction (from the Internet to the resident) than in the upstream direction (from the resident to the Internet). That is the reason it is called asymmetric. Unlike the asymmetry in 56K modems, the designers of ADSL specifically divided the available bandwidth of the local loop unevenly for the residential customer. The service is not suitable for business customers who need a large bandwidth in both directions. Voice. Channel 0 is reserved for voice communication.Idle. Channels 1 to 5 are not used, to allow a gap between voice and data communication. Upstream data and control. Channels 6 to 30 (25 channels) are used for upstream data transfer and control. One channel is for control, and 24 channels are for data transfer. If there are 24 channels, each using 4 kHz (out of 4.312 kHz available) with 15 bits per Hz, we have 24 4000 15, or a 1.44-Mbps bandwidth, in the upstream direction. Downstream data and control. Channels 31 to 255 (225 channels) are used for downstream data transfer and control. One channel is for control, and 224 channels are for data. If there are 224 channels, we can achieve up to 224 4000 15, or 13.4 Mbps Because of the high signal/noise ratio, the actual bit rate is much lower than the above-mentioned rates. The bit rates are as follows: Upstream: 64 kbps to 1 Mbps Downstream: 500 kbps to 8 Mbps HFC Network- The second generation of cable networks is called a hybrid fiber-coaxial (HFC) network The network uses a combination of fiber-optic and coaxial cable. The transmission medium from the cable TV office to a box, called the fiber node, is optical fiber; from the fiber node through the neighborhood and into the house, the medium is still coaxial cable. One reason for moving from traditional to hybrid infrastructure is to make the cable network bidirectional (two-way).Bandwidth- Even in an HFC system, the last part of the network, from the fiber node to the subscriber premises, is still a coaxial cable. This coaxial cable has a bandwidth that ranges from 5 to 750 MHz (approximately). The cable company has divided this bandwidth into three bands: video, downstream data, and upstream data. Video Band. The downstream-only video band occupies frequencies from 54 to 550 MHz. Since each TV channel occupies 6 MHz, this can accommodate more than 80 channels. Downstream Data Band. The downstream data (from the Internet to the subscriber premises) occupies the upper band, from 550 to 750 MHz. This band is also divided into 6-MHz channels. The downstream data can be received at 30 Mbps. The standard specifies only 27 Mbps. However, since the cable modem is connected to the computer through Upstream Data Band. The upstream data (from the subscriber premises to the Internet) occupies the lower band, from 5 to 42 MHz. This band is also divided into 6-MHz channels. The upstream data band uses lower frequencies that are more susceptible to noise and interference. Theoretically, downstream data can be sent at 12 Mbps (2 bits/Hz 6 MHz). However, the data rate is usually less than 12 Mbps.		
Q.5 (b)	Explain working principle of satellite communication. List the advantage of satellite communication	3+2=5	CO2

	A satellite is a body that moves around another body in a mathematically predictable path called an Orbit. A communication satellite is nothing but a microwave repeater station in space that is helpful in telecommunications, radio, and television along with internet applications.A repeater is a circuit which increases the strength of the signal it receives and retransmits it. But here this repeater works as a transponder, which changes the frequency band of the transmitted signal, from the received one.The frequency with which the signal is sent into the space is called Uplink frequency, while the frequency with which it is sent by the transponder is Downlink frequency. Advantages of satellite communications such as Flexibility ;Ease in installing new circuits,Distances are easily covered and cost doesn't matter, Broadcasting possibilities Each and every corner of earth is covered User can control the network		
	OR		
Q.5 (b)	In the standard Ethernet, If the maximum propagation time is 25.6 microseconds what is the minimum size of the frame. **Solution** The frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet, as we discussed before	5	CO2
Q.5 (c)	What are the Hidden node and Exposed Node issue in CSMA/CD B and C are hidden from each other with respect to A 	2+3=5	CO2