Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(An Autonomous Institute Affiliated to University of Mumbai)

End Semester Examination

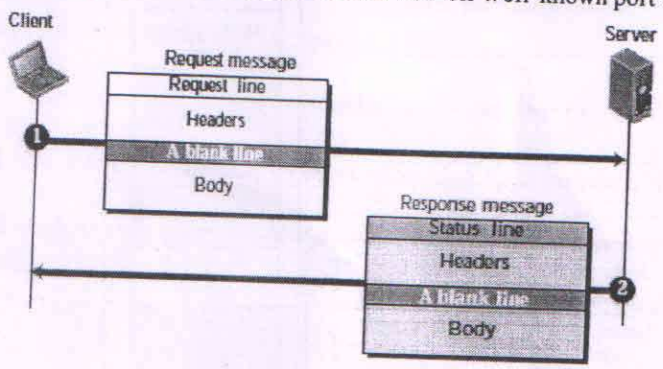
May 2019

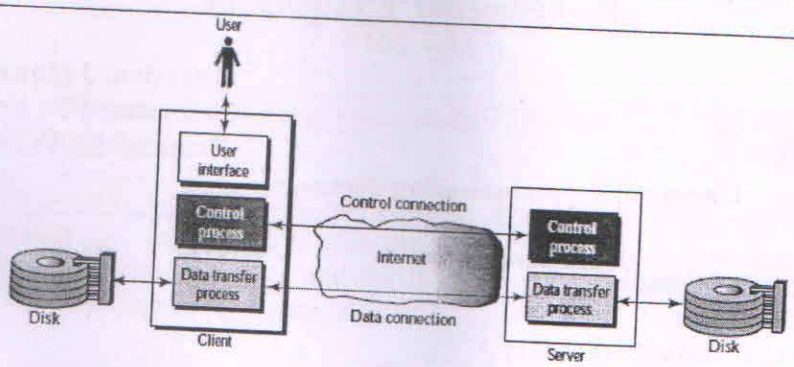
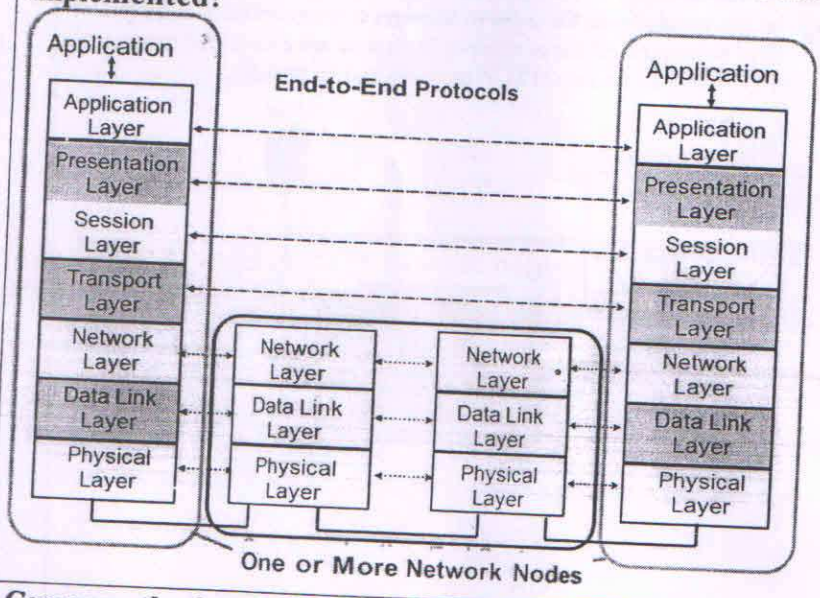
Max. Marks: 60 | **Duration: 3 Hours**
Class: TE | **Semester: VI**
Course Code: ET62 | **Branch: EXTC**
Name of the Course: Computer Communication Networks

Instructions:

(1) **All Questions are Compulsory**
(2) **Draw neat diagrams**
(3) **Assume suitable data if necessary**

Synoptic Answers

Question No.		Max. Marks	CO
1 (a)	**With the help of client server model, explain the working of HTTP.** **Answer:** The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. The commands from the client to the server are embedded in a request message. The contents of the requested file or other information are embedded in a response message. HTTP uses the services of TCP on well-known port 80.  **OR** **With the help of a neat diagram, explain how the communication between client and server happens in FTP.** **Answer:**	6	

			
Q 1 (b)	**Differentiate between:** 1. **Source routing versus Hop-by-Hop routing** 2. **Link-State routing versus Distance-vector routing.** **3 marks each, 4 points of difference**	6	
Q2 (a)	**With the help of a diagram, explain the seven layer OSI model, stating the function of each layer. Why was this model not practically implemented?** 	6	

Q2 (b)	**Compare the features of IPV6 and IPV4.**
	Answer:
	• **Longer address field:**
	  • 128 bits can support up to 3.4×10^{38} hosts
	• **Simplified header format:**
	  • Simpler format to speed up processing of each header
	  • All fields are of fixed size
	  • IPv4 vs IPv6 fields:
	  • Same: Version
	  • Dropped: Header length, ID/flags/frag offset,
		3	

	header checksum • Replaced: ▪ Datagram length by Payload length ▪ Protocol type by Next header ▪ TTL by Hop limit ▪ TOS by traffic class • New: Flow label • **Flexible support for options:** more efficient and flexible options encoded in optional *extension headers* • **Flow label capability:** "flow label" to identify a packet flow that requires a certain QoS • **Security:** built-in authentication and confidentiality • **Large packets:** supports payloads that are longer than 64 K bytes, called *jumbo* payloads. • **Fragmentation at source only:** source should check the minimum MTU along the path • **No checksum field:** removed to reduce packet processing time in a router		
Q3 (a)	**An organization is granted the block 130.56.0.0/16. The administrator wants to create 1024 subnets.** **a. Find the subnet mask. (1 mark)** **b. Find the number of addresses in each subnet. (1 mark)** **c. Find the first and the last address in the first subnet. (2 marks)** **d. Find the first and the last address in the last subnet (subnet 1024). (2 marks)** **Answer:** a. log21024 = 10 Extra 1s = 10 Possible subnets: 1024 Mask: /26 b. 232□ 26 = 64 addresses in each subnet c. **First subnet:** The first address is the beginning address of the block. **first address in subnet 1:** 130 . 56 . 0 . 0 To find the last address, we need to write 63 (one less than the number of	6	

addresses in each subnet) in base 256 (0.0.0.63) and add it to the first address (in base 256).

first address in subnet 1: 130 . 56 . 0 . 0

number of addresses: 0 . 0 . 0 . 63

last address in subnet 1: 130 . 56 . 0 . 63

d.

Last subnet (Subnet 1024):

To find the first address in subnet 1024, we need to add 65,472 (1023 · 64) in base 256 (0.0.255.92) to the first address in subnet 1.

first address in subnet 1 130 . 56 . 0 . 0

number of addresses: 0 . 0 . 255 . 192

first address in subnet 1024: 130 . 56 . 255 . 192

first address in subnet 500: 130 . 56 . 255 . 192

number of addresses: 0 . 0 . 0 . 63

last address in subnet 500: 130 . 56 . 255 . 255

OR

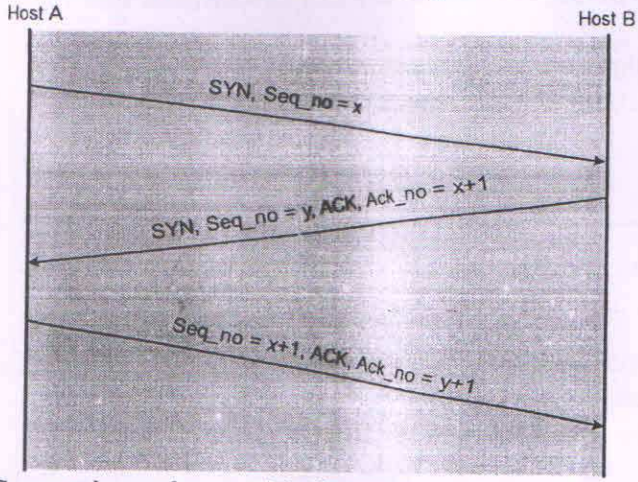
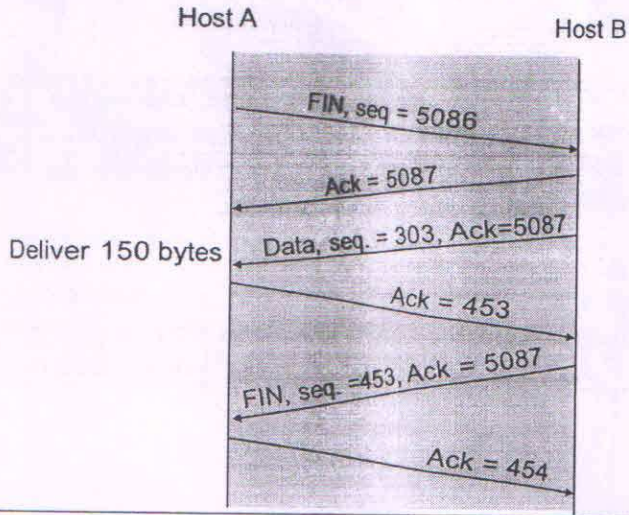
An ISP is granted a block of addresses starting with 130.56.0.0/22. The ISP wants to distribute these blocks to 100 customers as follows:

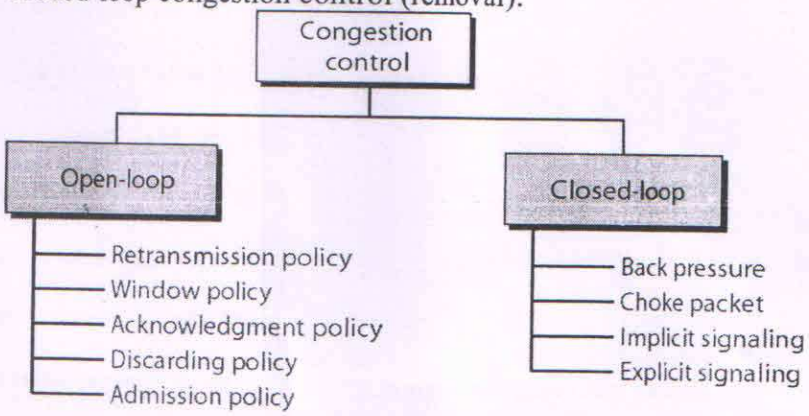
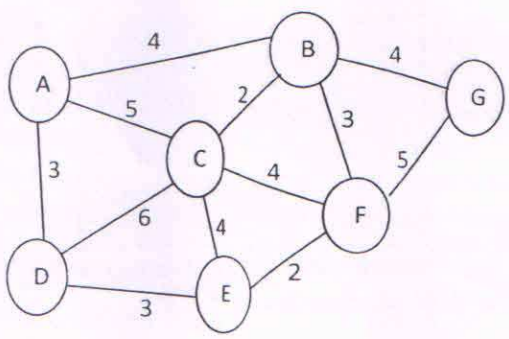
a) **The first group has 5 medium sized businesses: each needs 64 addresses.**
b) **The second group has 25 small businesses; each needs 16 addresses.**
c) **The third group has 70 customers; each needs 4 addresses.**
d) **Design the sub-blocks and give the slash notation for each sub-block.**
e) **Find out how many addresses are still available after each allocation.**

Solution:

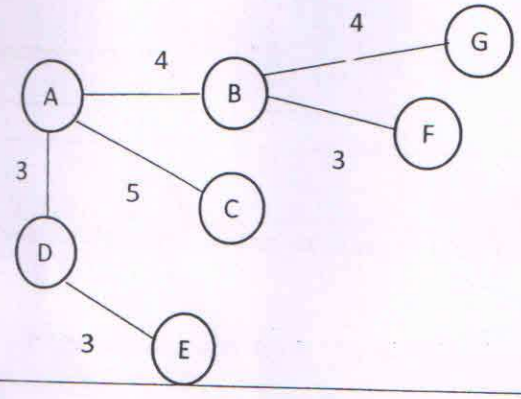
a) Total no. of addresses: $2^{32-22}=2^{10}=1024$
First group: 64 addresses, subnet mask is 6 bits i.e. /28, total addresses required is 64X 5 = 320.

b) Second group: 16 addresses, subnet mask is 4 bits i.e. /26, total addresses required is 16X 25 = 400.

	c) Third group: 4 addresses, subnet mask is 2 bits i.e. /24, total addresses required is 4X 70 = 280. d) Total addresses consumed are:320+400+280=1000 e) Addresses remaining = 1024-1000=24.		
Q3 (b)	**Explain the connection establishment and connection release procedure for TCP.** **Answer:** Connection Establishment with diagram 3 marks  Connection release with diagram 3 marks 	6	
Q4 (a)	**What do you mean by congestion control? Explain any one congestion control mechanism in TCP.** **Answer:** **Explanation of congestion control 3 marks, any one technique in detail 3 marks**		

	• Congestion in a network may occur if the load on the network—the number of packets sent to the network—is greater than the capacity of the network—the number of packets a network can handle. • Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity. • Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. • In general, we can divide congestion control mechanisms into two broad categories: • open-loop congestion control (prevention) and • closed-loop congestion control (removal). 		
Q4 (b)	**Differentiate between flat addressing and Hierarchical addressing. Consider the network shown in the figure. Using link state algorithm** find the shortest path tree and the forwarding table for node A for the topology shown in the figure below.  **Solution:**	6	

Iteration	N	B	C	D	E	F	G
Initialization	{A}	4	5	3	∞	∞	∞
1	{A,D}	4	5	3	6	∞	∞
2	{A, D,B}	4	5	3	6	7	8
3	{A, D,B, C}	4	5	3	6	7	8
4	{A, D,B, C, E}	4	5	3	6	7	8
5	{A, D,B, C, E, F}	4	5	3	6	7	8
6	{A, D,B, C, E, F, G}	4	5	3	6	7	8



Q5 (a)	**Write a note on firewalls.** **OR** **With the help of an example, explain the public key cryptography technique.**	6	
Q5 (b)	**Explain the working of OSPF with the help of different types of packet messages. State the advantages of OSPF over RIP.** **Working of OSPF with different types of packets 4 marks, eadvantage over RIP 2 marks)**	6	