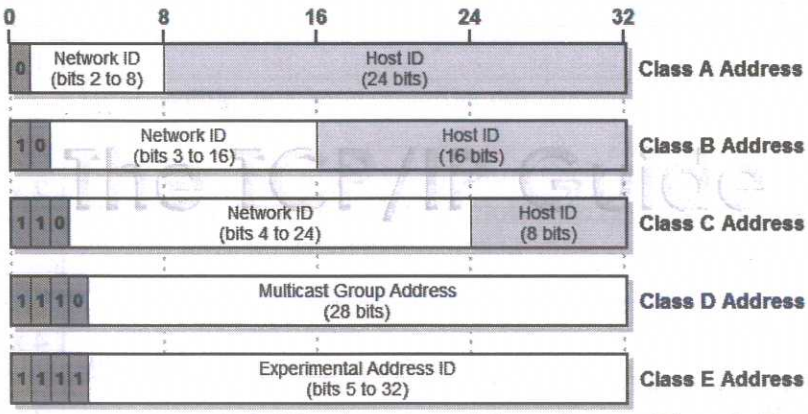
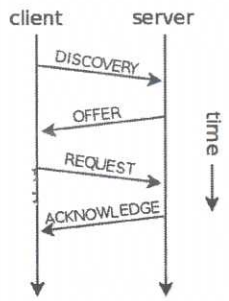
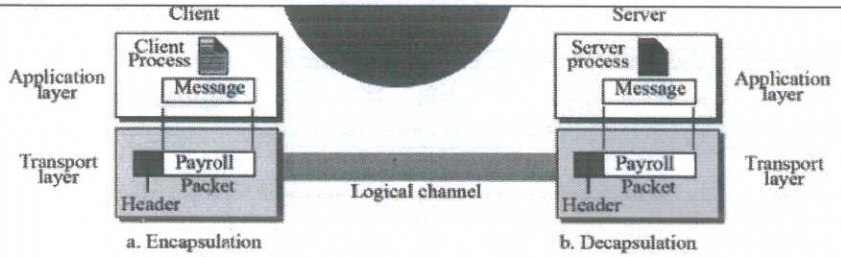
Code (15) 6131

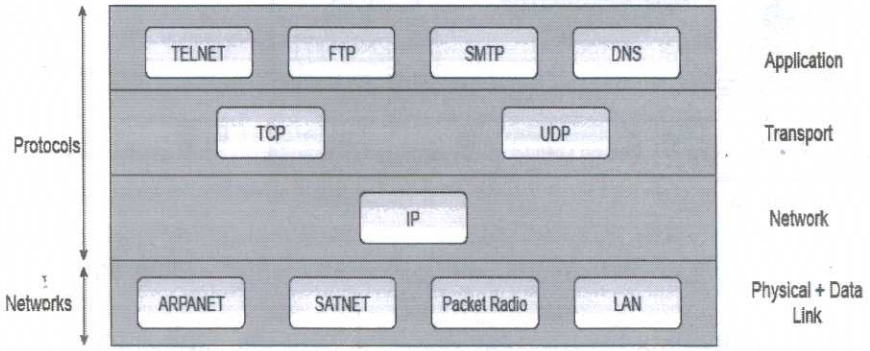
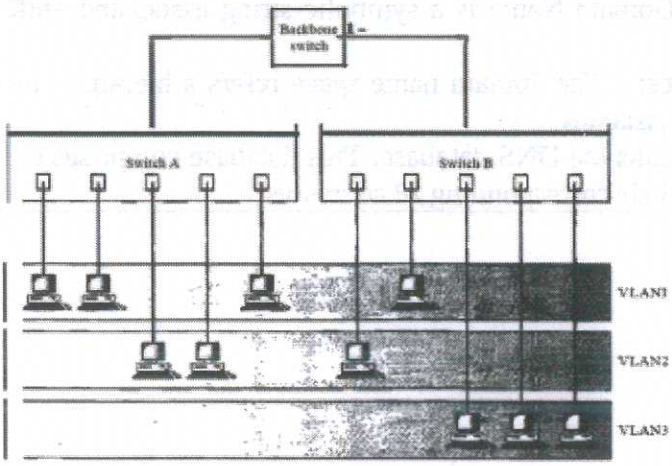
COMPUTER NETWORKS

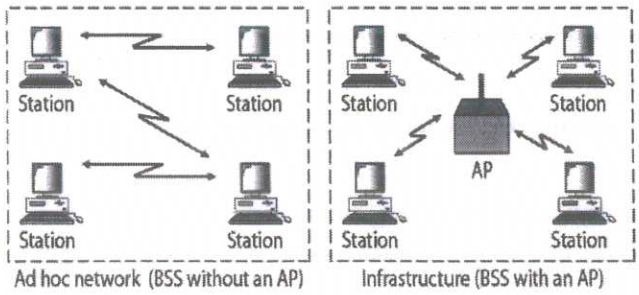
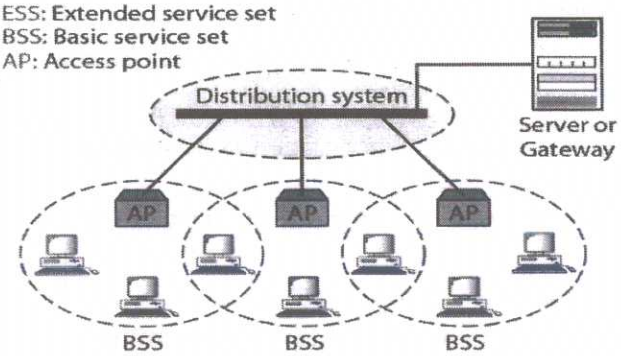
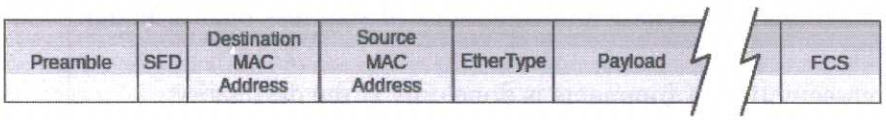
Scoring Indicators

Qn: No	Key	Split score	Total score
I 1	10Base5, 10Base2, 10BaseT, 10BaseF	4 x 0.5 marks	2
I 2	2^{32}	1 x 2 marks	2
I 3	Piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry acknowledgement for data arrived from B; when a frame is carrying data from B to A, it can also carry acknowledgement for data arrived from A.	2 x 1 marks	2
I 4	.com, .org, .biz, .net, .info etc. Any four	4 x 0.5 marks	2
I 5	HTTP, FTP, TELNET, SMTP, POP3 etc. Any two	2 x1 marks	2
II 1	1. Mesh • every node has a circuit connecting it to every other node in a network • very expensive to implement • reliable 2. Star • Devices are connected to a central computer, called a hub. • Nodes communicate across the network by passing data through the hub • If the central computer fails, the entire network becomes unusable 3. Ring • All of the nodes are connected in a closed loop. • Messages travel around the ring, with each node reading those messages addressed to it. 4. Bus • A bus is the central cable -- the main wire -- that connects all devices on a local-area network. • Bus networks are relatively inexpensive and easy to install for small networks. • Ethernet systems use a bus topology. Explanation of any two	2 x 3 marks	6
II 2	Hub: - • used to connect multiple network hosts. • when a host sends a data packet to a network hub, the hub		

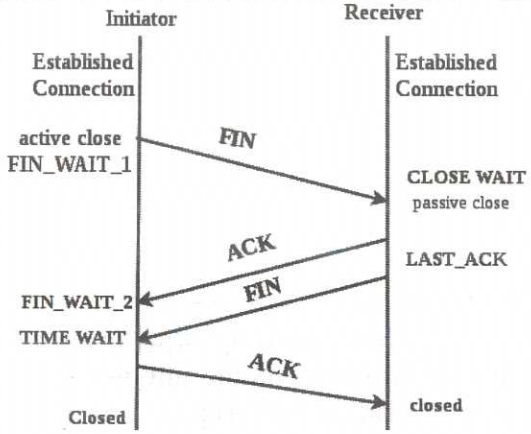
	copies the data packet to all of its ports connected to • amplifies the signal it receives Switch: - • a switch does 'filter and forwarding' with the data packets • when a packet is received at one of the interfaces of the switch, it filters the packet and sends only to the interface of the intended receiver Router: - • is responsible for routing traffic from one to another network. Listing any two Explanation of any two	2 x 1 mark3 2 x 2 marks	6
II 3	 Brief Explanation of four classes, Class A, B, C and D	4 x 1.5 marks	6
II 4	 1. DHCPDISCOVER - Client broadcast to locate available servers. 2. DHCPOFFER - Server to client in response to DHCPDISCOVER with offer of configuration parameters. 3. DHCPREQUEST - Client message to servers requesting offered parameters from one server and implicitly declining offers from all others 4. DHCPACK - Server to client with configuration parameters, including committed network address. Brief explanation of 4 steps	4 x 1.5marks	6

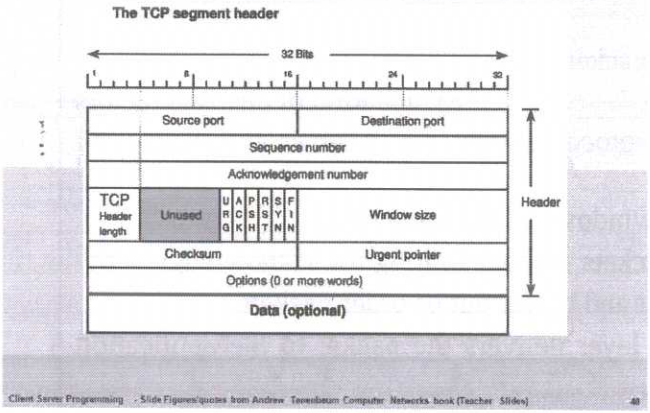
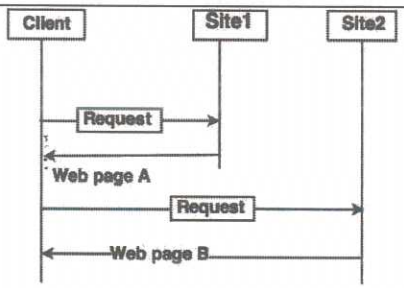
II 5	 Diagram Encapsulation: - Combining the message received from the application layer and transport layer header into a single unit by the transport layer protocol at the client/source. Encapsulation: - Seperating the transport layer header and the message by the transport layer protocol at the server/destination so that the message can be delivered to the application layer at the desination. Brief explanation	2 marks 2 x 2 marks	6
II 6	• For process that requires simple request-response communication without flow and error control • Suitable for processes with internal flow and error control mechanisms • Suitable for multicasting application • For management processes such as SNMP • For route updating protocols • For real-time interactive application Any six applications	6 x 1 marks	6
II 7	The Domain name system comprises of Domain Names, Domain Name Space and Name Server. Domain Names: - Domain Name is a symbolic string associated with an IP address. Domain Name Space: - The domain name space refers a hierarchy in the internet naming structure. Name server: - contains the DNS database. This database comprises of various names and their corresponding IP addresses.	3 x 2 marks	6

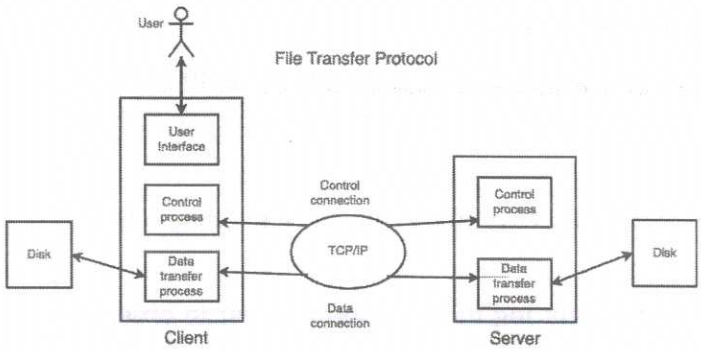
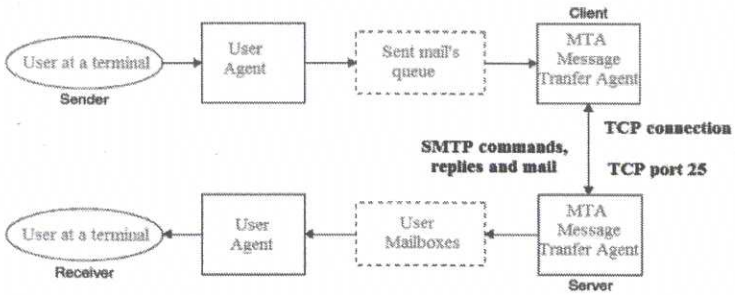
III a	 Diagram • Data link layer: - deals with hardware addressing and physical transmission of data. Also provides error control and framing. • Network layer: - defines the protocols which are responsible for logical transmission of data over the entire network. • Transport Layer: - provides end-to-end communication. Transport layer protocols ensure that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets. • Application Layer: -The application layer defines standard Internet services and network applications that anyone can use. Explanation of 4 layers	4 marks 4 x 1 marks	8
III b	• A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. • A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. • VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.  Diagram Explanation	3 marks 4 marks	7
IVa	Defines two Service sets : - BSS and ESS BSS-		8

	BSS: Basic service set AP: Access point  Diagram Explanation ESS – ESS: Extended service set BSS: Basic service set AP: Access point  Diagram Explanation	2 marks 2 marks 2 marks 2 marks	
IV b	 • PREAMBLE – 7-Bytes of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization. • Start of frame delimiter (SFD) –1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of frame. • Destination Address –6-Byte field which contains the MAC address of destination machine. • Source Address –6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0. • EtherType – 2 byte field Specifies the protocol being used in the network layer. • Payload – Contains the actual data to be transmitted. • Cyclic Redundancy Check (CRC) –4 Byte field contains checksum. If the checksum computed by destination is not same as sent checksum value, data received is corrupted. Diagram Brief explanation of all fields	3 marks 4 marks	7
V a	1. Each router prepares its routing table. By their local knowledge. each		

	router knows about- • All the routers present in the network • Distance to its neighboring routers 2. Each router exchanges its distance vector with its neighboring routers. 3. Each router prepares a new routing table using the distance vectors it has obtained from its neighbors. The new distance vector is calculated using the following formula: $d_x(y) = \min_v\{ c(x,v) + d_v(y)\}$ for each node y in N 4. step 3 is repeated for (n-2) times if there are n routers in the network. 5. After this, routing tables converge / become stable. Algorithm steps Example illustration	5 marks 3 marks	8
V b	IP Fragmentation is a process of dividing the datagram into fragments during its transmission. It is done by intermediary devices such as routers at the destination host at network layer. • Each network has its maximum transmission unit (MTU). • It dictates the maximum size of the packet that can be transmitted through it. • Data packets of size greater than MTU cannot be transmitted through the network. • So, datagrams are divided into fragments of size less than or equal to MTU. • The reassembling of fragments is done only at the destination. Definition Need for fragmentation Reassembly	2 marks 3 marks 2 marks	7
VI a	• Path Vector Routing is a routing algorithm in unicast routing protocol of network layer. • The principle of path vector routing is similar to that of distance vector routing. • It assumes that there is one node in each autonomous system that acts on behalf of the entire autonomous system is called Speaker node. • The speaker node in an AS creates a routing cable and advertises to the speaker node in the neighbouring ASs. • A speaker node advertises the path, not the metrics of the nodes, in its autonomous system or other autonomous systems. Explanation Example illustration	5 marks 3 marks	8
VI b	Performance can be measured using delay, throughput and packet loss. • Delay ❖ Can be divided into four types ❖ Transmission, propagation, processing and queueing	2	

	• Throughput ❖ Number of bits passing through a point in a second • Packet loss ❖ Number of packets lost during transmission Explanation of any two factors	2 x 2.5 marks	7
VII a	• Selective repeat protocol allows the receiver to accept and buffer a packet. • Send and Receive windows of the same size. • Sender can send packets without waiting for acknowledgement. • Receiver can accept and buffer out of order packets. • Receiver transport layer delivers the packet to the application layer in order. • Acknowledgement number in selective repeat is not cumulative. • Retransmission is only for the packets those are not acknowledged. • Selective repeat more efficient when compared to stop and wait and go-back-n. Working Send and receive window Acknowledgement efficiency	2 marks 2 marks 2 marks 2 marks	8
VII b	 1. FIN segment from client to server 2. FIN + ACK from server to client; connection from client to server closed; no more data from client to server. 3. ACK from client to server ; Connection terminated from the server to the client. Diagram Explanation of each step	4 marks 3 x 13 marks	7

VIII a	**TCP Segment Structure** The TCP segment header  Format Brief explanation of each field	4 marks 4 marks	8
VIII b	Transmission Sequence Number (TSN) Stream identifier (SI) Stream Sequence Number (SSN) SCTP Packet Acknowledgement Number Any four features	7 marks	7
IX a	 **Architecture of WWW** The World Wide Web (WWW) is a collection of documents and other web resources which are identified by URLs, interlinked by hypertext links, and can be accessed and searched by browsers via the Internet. The WWW consists of web client, web server and the web pages. Web Client (Browser): Web browser is a program, which is used to communicate with web server on the Internet. Server: The web pages are stored at the server. Web Pages: Each web page is identified by a Uniform Resource Locater (URL) Path is the pathname of the file where the file is stored. World Wide Web definition Explanation of three components	2 marks 3 x 2 marks	8

IX b	 • File Transfer Protocol (FTP) is an application layer protocol which moves files between local and remote file systems. • It runs on the top of TCP. • To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection. Control Connection: - used for sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files etc. Control connection is initiated on port number 21. Data connection: -For sending the actual file, FTP makes use of data connection. Data connection is initiated on port number 20. FTP – definition Data connection Control Connection	3 marks 2 marks 2 marks	7
X a	Simple Mail Transfer Protocol (SMTP) is the standard protocol for email services on a TCP/IP network. SMTP provides the ability to send and receive email messages. SMTP is an application-layer protocol that enables the transmission and delivery of email over the Internet. SMTP is generally integrated within an email client application. SMTP usually is implemented to operate over Internet port 25.  Definition Uses working	2 marks 3 marks 3 marks	8

X b	TELNET stands for TERminal NETwork. Telnet (TN) is a networking protocol and software program used to access remote computers and terminals over the Internet or a TCP/IP computer network. Designed for remote server access, management and client/server architectures. Telnet was often used to remotely log in to a remote server in order to conduct business such as editing files, running various programs or checking email on that system. Typically, you would use Telnet to connect to the system, then enter a username and password in order to access a command line on that system. Telnet is uncommon now, because it is unencrypted. Telnet also doesn't support modern graphical user interfaces. Definition Uses Working Drawbacks	 2 marks 1 mark 2 marks 2 marks	7