82

Apr.25

P-11

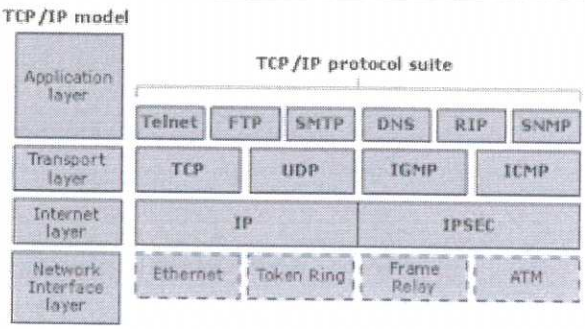
Scoring Indicators

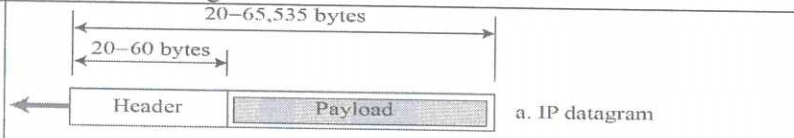
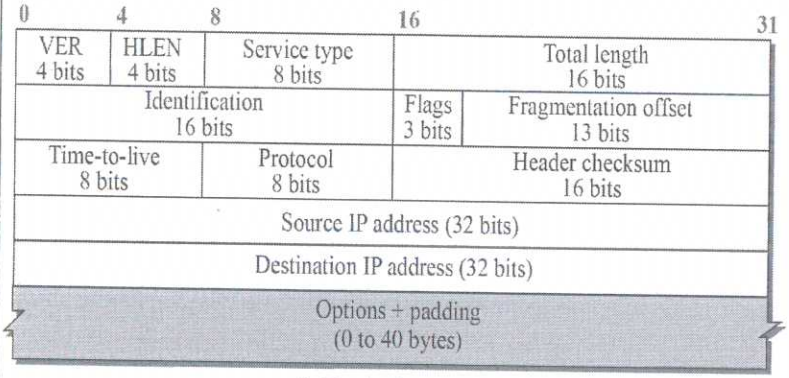
COURSE NAME: COMPUTER COMMUNICATION AND NETWORKS

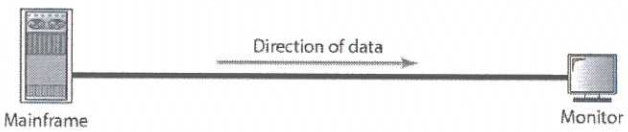
COURSE CODE: 4132 (REVISION 2021)

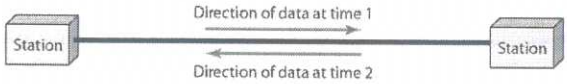
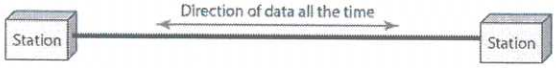
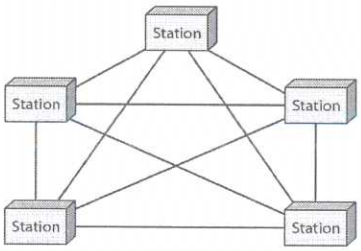
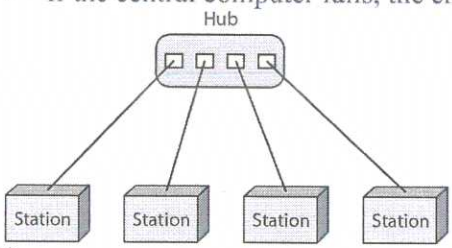
QID : 2103230214

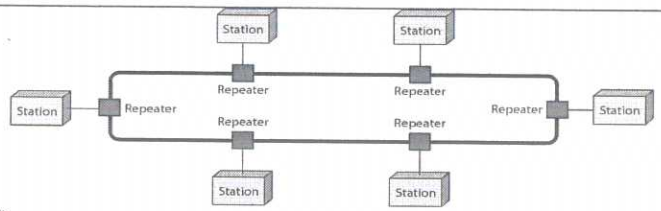
Q No	Scoring Indicators	Split score	Sub Total	Total score
	PART A			**9**
I. 1	Protocol is a set of rules that govern data communication.	1	1	
I. 2	Multipoint connection is one where more than two devices share a single link.	1	1	
I. 3	Digital data	1	1	
I. 4	Radio waves, microwaves, infrared etc. Any two	0.5 x 2	1	
I. 5	2^{32}	1	1	
I. 6	User datagrams	1	1	
I. 7	FTP, TELNET, HTTP, SSH, SMTP, POP, POP3, IMAP4 etc. Any two	0.5 x 2	1	
I. 8	SSH, TELNET	0.5 x 2	1	
I. 9	Domain Name System (DNS)	1	1	
	PART B			**24**
II. 1	Layer 7 Application Layer 6 Presentation Layer 5 Session Layer 4 Transport Layer 3 Network Layer 2 Data link Layer 1 Physical Listing each layer	0.5 x 7	3	
II. 2	**LAN** / **WAN** Local Area Network / Wide Area Network LAN is a group of devices / WAN is an arrangement of several	2 1	3	

	connected in a small geographic area, such as houses, offices, or buildings.	devices attached over a network covering a broad area.			
	LAN covers a small geographical area, and it does not require any leased telecommunication lines.	WAN spreads over a large distance geographical area and requires leased telecommunication lines.			
	LAN is an interconnection of communicating devices.	WAN generally interconnects connecting devices such as switches and routers.			
	LAN is generally privately owned.	WAN is created and maintained by communication companies and leased by organizations to use.			
	LAN set up is not costly.	WAN set up is costly.			
II. 3	 Diagram with protocols given in each layer		3	3	
II. 4	1. Attenuation : • When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. • Thus strength of the signal decreases with increasing distance. 2. Distortion: • Distortion means that the signal changes its form or shape. • Distortion can occur in a composite signal made of different frequencies. 3. Noise: • The random or unwanted signal that mixes up with the original signal is called noise. • Several types of noise - thermal noise, induced noise, crosstalk, and impulse noise.		1 x 3	3	
II. 5	• CSMA stands for Carrier Sense Multiple Access. • It is a protocol used in the MAC sub layer of DLL. • This method was developed to reduce the number of collisions when two or more stations send their signals over data link layer. • It works based on the principle of "sense the medium before transmit".		0.5 x 6	3	

	• Before starting transmission each station needs to check the state of the medium. • If the line is free, the station sends the frame immediately, otherwise it waits for a random amount of time and senses the channel again.			
II. 6	 a. IP datagram  b. Header format	3	3	
II. 7	• UDP is suitable for simple request- response communication which doesn't require flow and error control. • UDP is suitable for applications with internal flow and error control mechanisms. • UDP is suitable for multicasting. • UDP is used for management processes such as SNMP. • UDP is used for route updating protocols. • UDP is used for interactive real-time applications. Any three	1 x 3	3	
II. 8	1. User Agent(UA) a. It is a software package. b. Creates, reads, replies to and forwards messages. c. Example : outlook 2. Message Transfer Agent (MTA) a. The actual mail transfer is done through MTA. b. To send a mail MTA client is needed and to receive a mail MTA server is needed. c. SMTP is a MTA. 3. Message Access Agent (MAA) a. In order to receive a mail, an MAA is needed.	1 x 3	3	

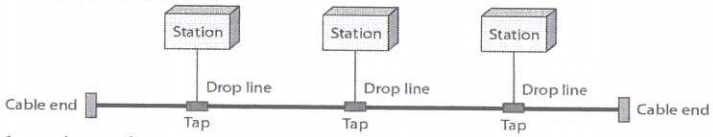
	b. The receiver pulls the message from mail server. c. MAA client will be running on receiver and MAA server on the mail server.			
I.9	• In peer to peer paradigm the responsibility is shared among peers. • A computer connected to the Internet can provide service at one time and receive service at another time. • It can provide and receive service at the same time also. • Peer-to-peer networks are easily scalable and cost effective. • Each computer in the peer to peer network manages itself. So, the network is quite easy to set up and maintain • It is difficult to provide overall security in the peer to peer network as each system is independent and contains its own data.	0.5 x 6	3	
II.10	Static Web documents: • Fixed content documents that are created and stored at the server. • When the client requests these documents, a copy of the document is sent. • User can use a browser to view the document. • Created using HTML, XML, XHTML etc Dynamic web documents: • Server creates the documents on client's request. • When the client requests the server runs a program or script to generate the page a copy of the document is sent. • Contents of a dynamic page may vary from one request to another. • Created using scripting languages like ASP, JSP, PHP etc Any 3 points about each	0.5 x 6	3	
	PART C			**42**
III. 1	• Simplex (one way street) ▪ The communication is unidirectional ▪ Only one device on a link can transmit; the other can only receive ▪ Use the entire capacity of the channel to send data ▪ Example: Keyboards, Monitors  • Half-Duplex (one-lane with two-directional traffic) ▪ Each station can both transmit and receive, but not at the same time ▪ When one device is sending, the other can only receive, and vice versa ▪ The entire capacity of a channel is taken over by the transmitting device	3.5 x2	7	7

	▪ Example: Walkie-talkies.  ● Full-Duplex (Duplex) (two-way street) ▪ Both stations can transmit and receive at same time ▪ Signals going in either direction sharing the capacity of the link ▪ The capacity of the channel is divided between signals travelling in both directions ▪ Example: Telephone network  Explanation of any two			
III. 2	Bus, star, Mesh and Ring 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.	1 3 x 2	7	7



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.



Explanation of any two

III. 3 Twisted pair, coaxial cable and fiber optic cable

1. Twisted-pair cables

- Twisted-pair use metallic (copper) conductors that accept and transport signals in the form of electric current.
- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

1

- The most common Twisted-pair cables connector is RJ45.
- Used in telephone lines and in Local Area Networks

2. coaxial cable

- Coaxial cable (coax) uses metallic (copper) conductors that accept and transport signals in the form of electric current.
- Coax has a central core conductor of solid wire (usually copper) enclosed in an insulating sheath.
- This in turn is encased in an outer conductor of metal foil.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.
- The most common type of connector is the Bayonet Neill-Concelman (BNC) connector.

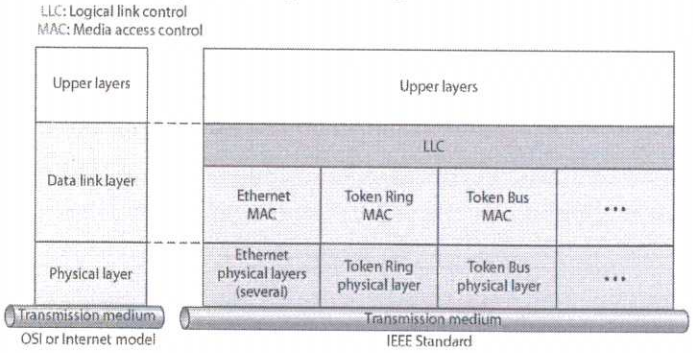
3 x 2

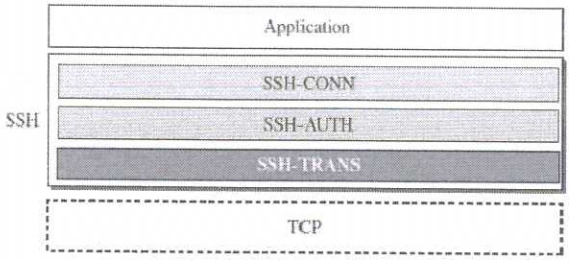
- Used in telephone lines, cable TV networks and Ethernet LANs.

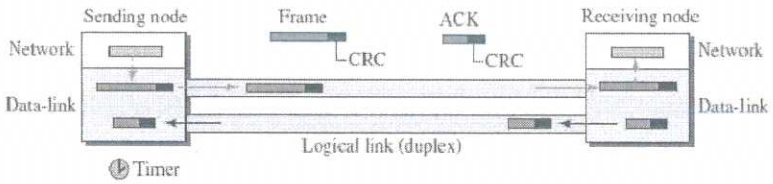
3. Fiber-Optic Cable

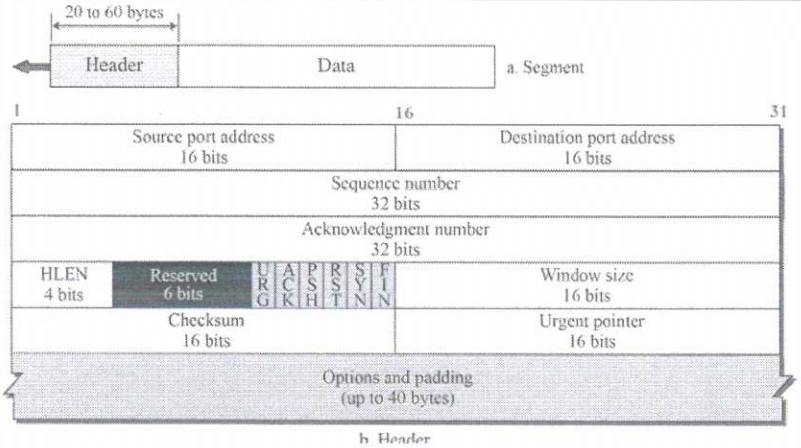
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.

7 7

	• The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding. Explanation of any two			
III. 4	• In 1985, the Computer Society of the IEEE started Project 802. • It was for setting standards to enable intercommunication among equipment from a variety of manufacturers. • Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.  • IEEE has divided data link layer into two sub layers: logical link control (LLC) and Media Access control (MAC). • LLC: handles flow control, error control and part of framing. • MAC: defines the specific access method for each LAN and performs part of framing function.	1 x 7	7	7
III. 5	• Link-state is used to define the characteristic of a link (an edge) that represents a network in the internet. • The collection of states for all links is called the link state database (LSDB). • Each router learns about its own links, i.e. its own directly connected networks. • Each router builds a Link-State Packet (LSP) containing the state of each directly connected link. • Each router floods the LSP to all neighbors, who then store all LSPs received in a database. • Each router uses the database to construct a complete map of the topology and computes the best path to each destination network using Dijkstra's algorithm. Algorithm Steps	1 x 7	7	7
III. 6	1. Process-to-process communication 2. Encapsulation and decapsulation 3. Flow control	2	7	7

	4. Error control 5. Congestion control Explanation of any two.	2.5 x 2		
III. 7	**HTTP Connections** • If the web pages we access are located in different servers we need to create a new connection for each page. • If the web pages are in the same server we have two options: – Non persistent connection – Persistent connection **HTTP – Non persistent connection** • One TCP connection is made for each request/response. • The steps in a non persistent connection are: - – The client opens a TCP connection and sends a request. – The server sends a response and closes the connection. – The client reads the data till end of file; then it closes the connection. **HTTP – persistent connection** • A single TCP connection is used to send and receive multiple HTTP requests/responses. • The steps in a persistent connection are: - 1. The client opens a TCP connection and sends a request. 2. The server sends a response and leaves the connection open more requests. 3. The clients send any number of requests and get responses from the server. 4. The server closes the connection on the request of the client or at time out.	3.5 x 2	7	7
III. 8	SSH is an application layer program used for remote logging and file transfer. SSH has three components.  1. SSH – transport layer protocol (SSH-TRANS) a. is an independent protocol used in the secure channel created on top of TCP. b. The services provided by SSH-TRANS are Privacy or confidentiality Data integrity Server authentication Compression of messages 2. SSH – authentication protocol (SSH-AUTH)		7	7

	a. After establishing a secure channel, the server needs to authenticated for the client. 3. SSH – connection protocol (SSH-CONN) a. SSH- CONN protocol lets the client to create multiple logical channel, each of which can be used for a different purpose.			
III. 9	 • Stop and Wait protocol offers flow and error control. • The sender sends one frame at a time and starts a timer and waits for acknowledgment. • Each frame carries a CRC for error detection. • The receiver after receiving the uncorrupted frame sends an acknowledgement. • A corrupted frame is not acknowledged. • If the sender receives an acknowledgement before the timer expires then it sends the next frame. • If the timer expires then the sender retransmits the previous frame assuming the frame is lost or corrupted.	1 x 7	7	7
III. 10	Framing, Flow Control and Error control. Framing: • The data link layer receives a raw bit stream from the physical layer that may not be error free. • To ensure a reliable transfer of bit streams to the network layer, the data link layer breaks the bit stream into frames. • It then computes the checksum for each frame, which is transmitted with the frame itself. • The destination host receives a frame and computes another checksum from its data to compare it with the transmitted frame. • This ensures that the data link layer of the receiver detects as well as correct frames. Flow Control: • If the sender transmits frames at a rate faster than the receiver can process then the frames will be discarded. • Flow control is needed to avoid this. • Flow control can be done in several ways; one is by the use buffers. • Buffers are used to store the frames at the sender and at the	1	7	7

	receiver. Error Control: • For the communication to be proper the packet received must be the packet sent. • If the packet is corrupted during transmission, it must be detected and corrected. • Data link layer implements error detection and correction. • CRC is one of the error detection method used in the data link layer.	2 x 3		
III. 11	 Outline the purpose of each field. Source port address: - port number of the application program in the sending host Destination Port address: - port number of the application program in the receiving host. Sequence Number: - byte number of the first byte of data contained in the segment. Acknowledgement Number: - Sequence number of the next expected segment. HLEN: -Header length; length of the TCP header in 4 bytes. Control flags: - this **field** contains 6 bits Window size: -This field defines the window size of the sending TCP. Checksum: - This 16-bit field contains the checksum. Urgent Pointer: -This field is valid only if the URG flag is set. Options and padding: - contains optional information in TCP header.	3 + 4	7	7
III. 12	The following services are provided by the network layer. 1. Packetizing:- • Network layer encapsulates the payload (data received from the upper layer) in a network layer packet at the source and decapsulates the payload from the network layer packet at the destination. • Network layer is responsible for delivery of packages from sender	7	7	7

	to receiver without changing or using the content. 2. Routing • Network layer is responsible for routing a packet from its source to destination. • More than one route is possible from source to destination. • Network layer is responsible for finding the best route. • Network layer uses different strategies for finding out the best route. 3. Forwarding: • It is the action applied by each router when a packet arrives at one of its interface. • The decision making is done by the router by using the forwarding/routing table. 4. Errol Control • The network layer of the Internet provides error control only for the network layer header by using a checksum field. 5. Flow Control • Flow control avoids flooding of receiver with packets. 6. Congestion Control • Congestion in the network layer is the situation in which too many datagrams are present in an area of the Internet. • Network layer provides congestion control. Brief explanation of any three (2 mark each)			