231

D

April - 24
PageNo - 8

Scoring Indicators - A

COURSE NAME : COMPUTER COMMUNICATION AND NETWORKS

COURSE CODE : 4132 **QID :2103230212**

<table>
<tr><th>Q No</th><th>Scoring Indicators</th><th>Split score</th><th>Sub Total</th><th>Total score</th></tr>
<tr><td></td><td>PART A</td><td></td><td></td><td>9</td></tr>
<tr><td>I. 1</td><td>Text, images, audio, video (Any two - 0.5 Marks each).</td><td></td><td>1</td><td rowspan="10"></td></tr>
<tr><td>I. 2</td><td>Open Systems Interconnection.</td><td></td><td>1</td></tr>
<tr><td>I. 3</td><td>Aloha, CSMA, CSMA/CD, CSMA/CA. (Any two)</td><td></td><td>1</td></tr>
<tr><td>I. 4</td><td>Attenuation is the loss of signal strength.</td><td></td><td>1</td></tr>
<tr><td>I. 5</td><td>Wifi, Bluetooth, WiMax, Satellite, Infrared etc. (Any two).</td><td></td><td>1</td></tr>
<tr><td>I. 6</td><td>128 bit.</td><td></td><td>1</td></tr>
<tr><td>I. 7</td><td>False</td><td></td><td>1</td></tr>
<tr><td>I. 8</td><td>Protocol, domain name, resource address within domain.</td><td></td><td>1</td></tr>
<tr><td>I. 9</td><td>Secure Shell</td><td></td><td>1</td></tr>
<tr><td></td><td>PART B</td><td></td><td></td><td>24</td></tr>
<tr><td>II. 1</td><td>The process of transfer of information from source to destination obeying a set of rules, called the protocol.

Elements: Sender, Receiver, Message, Protocol, Medium.</td><td>1.5

1.5</td><td>3</td><td></td></tr>
<tr><td>II. 2</td><td><table><tr><th>LAN</th><th>MAN</th></tr><tr><td>Local Area Network</td><td>Metropolitan Area Network</td></tr><tr><td>A group of computers within a small area.</td><td>Group of computer within a wider area than LAN, usually within a city.</td></tr><tr><td>high speed, low cost.</td><td>Low speed, high cost.</td></tr></table></td><td></td><td>3</td><td></td></tr>
</table>

<table>
<tr><td>II. 3</td><td>Flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver.</td><td></td><td>3</td><td></td></tr>
<tr><td>II. 4</td><td>- Minimize electromagnetic radiation.
- Resists external interference.
- Limit interference with adjacent twisted-pair cables.</td><td></td><td>3</td><td></td></tr>
<tr><td>II. 5</td><td><table><tr><th>Serial</th><th>Parallel</th></tr><tr><td>Single channel</td><td>Multiple Channel</td></tr><tr><td>bit-by-bit transmission</td><td>a block of data at once</td></tr><tr><td>long distance communication</td><td>short distance communication</td></tr><tr><td>low cost and slow speed</td><td>high speed, but low cost</td></tr><tr><td colspan="2">(Any three relevant points)</td></tr></table></td><td></td><td>3</td><td></td></tr>
<tr><td>II. 6</td><td>The IPv4 address is a 32-bit number that uniquely identifies a device in a computer network. An IPv4 address is written in decimal digits, divided into four 8-bit fields that are separated by periods. It consists of two parts, the network part and the host id within the network.
Example 192.168.1.5</td><td>2
1</td><td>3</td><td></td></tr>
<tr><td>II. 7</td><td>Communication between two nodes in an interconnected network can take place through many different paths. Routing is the process of selecting the best path using some predetermined rules. Selection of the best timely path improves the performance of the network.</td><td></td><td>3</td><td></td></tr>
<tr><td>II. 8</td><td>IP Range - 192.168.1.16 to 192.168.1.31

Mask 255.255.255.240 (or any IP address in the range/28)</td><td>1.5
1.5</td><td>3</td><td></td></tr>
<tr><td>II.9</td><td>Peer-to-peer architecture (P2P architecture), each workstation has the same capabilities and responsibilities. Each station can act as both client and server. P2P networks distribute the workload between peers, and all peers contribute and consume resources within the network without the need for a centralized server.</td><td></td><td>3</td><td></td></tr>
<tr><td>II.10</td><td>DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.</td><td></td><td>3</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>42</td></tr>
</table>

	PART C			
III. 1	a) Diagram - 2 Marks b) Description - 5 Marks **1) Physical Layer** a) Physical, mechanical, and electrical specifications of the interface and transmission medium. b) Bit Representation and encoding. c) Data rate, Synchronization, Line Configuration, Topology, and transmission modes. . **2) Datalink Layer** a) Node-to-node frame delivery. b) Framing. c) Physical addressing d) Flow Control, Error Control, and Access Controls. **3) Network Layer** a) Packetization b) Source to Destination Packet delivery. c) Logical (IP) Addressing. d) Routing. **4) Transport Layer** a) Process to process message delivery. b) Service point (port) addressing. c) Segmentation and Reassembly d) Flow Control, Error Control, and Connection Controls. **5) Session Layer** a) Dialogue control and synchronization. b) Establishes, control, and maintains user sessions. **6) Presentation Layer** a) Translation b) Encryption c) Compression **7) Application Layer** a) User Interfaces to access network services. b) Protocols: NVT, Mail, file transfer, etc.	2 5	7	7

III. 2

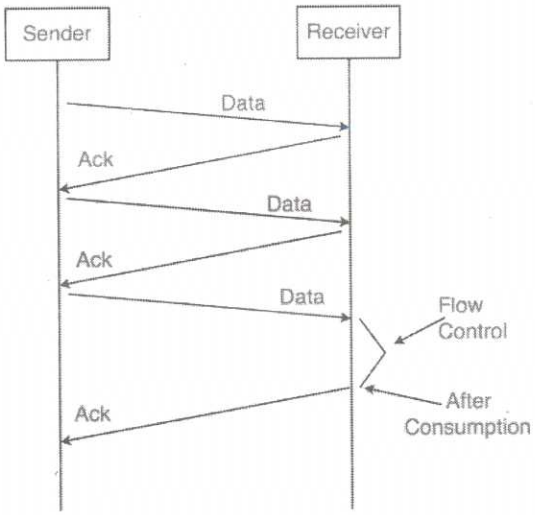
Layer	Protocols
Application	HTTP, NFS, DNS, telnet, SMTP, FTP
Transport	TCP, UDP
Internet	IP, ICMP, ARP
Link	Ethernet, Token Ring, FDDI

(with description of protocols in each layer)

7 7

III. 3

Stop and wait Protocol



Used in Connection-oriented communication and offers error and flow control.

Sender:

- Send one data packet at a time.
- Send the next packet only after receiving acknowledgement for the previous.

Receiver:

- Send acknowledgment after receiving and consuming a data packet.
- After consuming the packet, acknowledgment must be sent (Flow Control)

7 7

III. 4

Data-link layer takes the packets from the Network Layer and encapsulates them into frames. Also, it packs bits received from the physical layer into frames. 2

Parts of a Frame:

A frame has the following parts –

a) Frame Header – It contains the source and the destination addresses of the frame.

b) Payload field – It contains the message to be delivered.

c) Trailer – It contains the error detection and error correction bits.

d) Flag – It marks the beginning and end of the frame. 2

Types of Framing: Two types, fixed sized framing and variable sized framing.

7 7

	a) Fixed-sized Framing: Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. It does not require additional bits to identify the start and end of the frame. b) Variable – Sized Framing: Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame. Two approaches in variable sized frames, b1) Byte – Stuffing – A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing. b2) Bit – Stuffing – A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.	3		
III. 5	<table><tr><th>CSMA/CD</th><th>CSMA/CA</th></tr><tr><td>Collision detection protocol</td><td>collision avoidance protocol</td></tr><tr><td>Used in wired networks</td><td>used in wireless networks</td></tr><tr><td>IEEE 802.3 standard</td><td>IEEE 802.11 standard</td></tr><tr><td>More efficient than CSMA.</td><td>Similar to CSMA</td></tr><tr><td>Effective after collision</td><td>Effective before collision</td></tr><tr><td>Initially transmits the intent to send the data. Once an acknowledgment is received, the sender sends the data.</td><td>Resends the data frame in case a conflict occurs during transmission.</td></tr></table>		7	7
III. 6	In guided transmission, the signal travels through the boundaries of the physical medium. Optical fiber cables employ the principle of total internal reflection of light rays to transmit the signal. **Advantages** 1. Higher bandwidth. 2. Less signal attenuation. 3. Immunity to electromagnetic interference. 4. Resistance to corrosive materials. 5. Lightweight. 6. Greater immunity to tapping. **Disadvantages** 1. Installation and maintenance. 2. Unidirectional light propagation. 3. Cost.	2 3 2	7	7

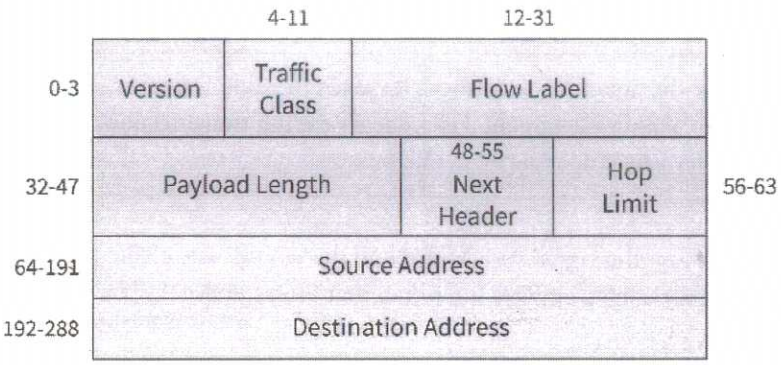
III. 7

TCP vs UDP

Basis	TCP	UDP
Definition	Establishes a virtual circuit before transmitting the data.	transmits the data directly to the destination without verifying whether the receiver is ready to receive.
Connection Type	Connection Oriented	Connection Less
Speed	Slow	High
Reliability	Reliable	Un-reliable
Header size	20 bytes	8 bytes
Ack	Yes	No
Retransmission	Yes	No

7 7

III. 8



3

4

7 7

Picture - 3 Marks Definition of components - 4 Marks

III. 9

The distance vector routing algorithm works by having each router maintain a routing table, giving the best-known distance from source to destination and which route is used to get there. These tables are updated by exchanging the information with the neighbor having a direct link. 2

Algorithm

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from 5

7 7

<table>
<tr><td></td><td>each of its neighbors.
3. A router recalculates its distance vector when:
☐ It receives a distance vector from a neighbor containing different information than before.
☐ It discovers that a link to a neighbor has gone down.
The DV calculation is based on minimizing the cost to each destination</td><td></td><td></td><td></td></tr>
<tr><td>III. 10</td><td>Comparison of IPv4 and IPv6
<table>
<tr><th>Property</th><th>IPv4</th><th>IPv6</th></tr>
<tr><td>Addressing</td><td>i) 32 bit
ii) Dotted decimal notation
iii) 4 Octets (4 * 8 =32)
iv) Generates 4 billion unique addresses.</td><td>i) 128 bit
ii) Hexadecimal values with colons
iii) 8 Fields, each with 2 octets, total 16 octets.
iv) Generates 340 undecillion numbers.</td></tr>
<tr><td>Classes</td><td>Five different classes- Class A, B, C, D and E.</td><td>Classes not supported</td></tr>
<tr><td>Address Configuration</td><td>Supports Manual and DHCP.</td><td>Supports Manual, DHCP, auto-configuration and renumbering.</td></tr>
<tr><td>Checksum field</td><td>Available in IPv4</td><td>Not Available in IPv6.</td></tr>
<tr><td>Security</td><td>Security depends on application.
Encryption and authentication not supported,</td><td>IPSEC security feature.
Supports encryption and authentication</td></tr>
</table>
(Any seven points, one mark each)</td><td></td><td>7</td><td>7</td></tr>
<tr><td>III. 11</td><td>File Transfer Protocol: Standard protocol for transmitting the files from one host to another reliably and efficiently. In FTP architecture, there are three types of processes in the client and two types in the server.
Two types of connections:
i)Control connection: Port 21. Simple rules for connection. Connection between the control process to exchange control signals and responses. Remains connected till the end of the active session.
ii)Data Connection: Port 20. Complex rules. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.
Merits
☐ Speed: The fastest way for file transfer.</td><td>1.5
1.5
2</td><td>7</td><td>7</td></tr>
</table>

	☐ Efficient: do not need to complete all the operations to get the entire file. ☐ Security: Protected with user credentials. ☐ Back & forth movement: Two way transfer of files. **Demerits** ☐ File size limit: 2 GB limit ☐ Security issues: Data is not encrypted. ☐ Multiple receiving is not supported.	2		
III. 12	HTTP connections are broadly categorized into two types i.e. Non-Persistent and Persistent. In persistent connection HTTP, multiple objects can be sent over a single TCP connection. A persistent HTTP connection can be either Non-pipelined or Pipelined. **1 Mark** **a) Non-Pipelined:** A non-pipelined HTTP connection is a connection in which, the client can send a request to the server only if the previous request that was sent by the client has been acknowledged by the server. **1 Mark** **b) Pipelined:** A pipelined HTTP connection is a connection in which, the client can send a request to the server even if the previous request that was sent by the client has not been acknowledged by the server. **1 Mark** **<u>Advantages of Persistent HTTP</u>** 1. Persistent HTTP saves CPU resources and time since the opening of the connection takes place only once. 2. It gives a fast start to send any object from a source to a destination. Also, it results in relatively less network congestion and latency on subsequent HTTP requests compared to non-persistent HTTP. **2 Marks** **<u>Disadvantages of Persistent HTTP</u>** 1. Persistent HTTP results in a waste of network resources since the connection remains open even when there is no transmission of data. 2. It is less secure than non-persistent HTTP since the connection once opened remain always open. **2 Marks**	1 1 1 2 2	7	7