Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Set - A

Academic Year: 2022-23 (ODD)

Test: CLA-T1 | Date: 07-09-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Hour
Year & Sem: III Year / V Sem | Max. Marks: 25

Course Articulation Matrix:

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	1	3	-	3	1	-	-	-	1	1	-	3

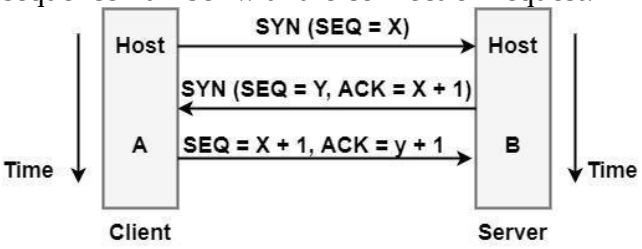
Part – A
(15 x 1 = 15 Marks)

Instructions: 1) Answer ALL questions. 2) The duration for answering the part A is 15 minutes (this sheet will be collected after 15 minutes). 3) Encircle the correct answer (if more than one is right answer encircle appropriately) 4) if any of the questions * indicates choose multiple answers.

Q. No	Question	Marks	BL	CO	PO	PI Code
1	**There are the following statements that are given below, which of them are correct OP code used in ARP message format? *** a. the OP code is used to specify the type of ARP message. b. the OP code is part of only the ARP request message. c. the OP code 1 is used for ARP request. d. the OP code 0 is used for ARP reply.	1	L1	1	1	1.6.1
2	**Which of the following is correct about User Datagram Protocol** a. UDP has flow control mechanism b. There is window mechanism in UDP c. There is no robust error control mechanism in UDP d. UDP provides error correction	1	L1	1	1	1.6.1
3	**Size of TCP segment header ranges between _____** a. 16 and 32 bytes b. 16 and 32 bits c. 20 and 60 bytes d. 20 and 60 bits	1	L1	1	1	1.6.1
4	**During error reporting, ICMP always reports error messages to _____** a. Destination b. Source c. Next router d. Previous router	1	L1	1	1	1.6.1
5	**In the_____algorithm of TCP, the size of the congestion window increases exponentially until it reaches a threshold.**	1	L1	1	1	1.6.1

	a. slow-start b. congestion avoidance c. congestion detection d. Congestion control					
6	**Transport layer aggregates data from different applications into a single stream before passing it to _____** a network layer b. data link layer c. application layer d. physical layer	1	L1	1	1	1.6.1
7	**UDP perform_____functions.** a. end-to-end reliable data delivery b. process-to-process communication c. host-to-host communication d. host-to-server communication	1	L1	1	1	1.6.1
8	**_____is a technique that refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.** a. Backpressure b. Discard c. Choke d. Explicit	1	L1	1	1	1.6.1
9	**The_____address, also known as the link address, is the address of a node as defined by its LAN or WAN.** a. Physical b. IP c. Port d. Specific	1	L1	1	1	1.6.1
10	**In IPv4, service type of service in header field, first 3 bits are called _____** a. Type of service b. Code bits c. Sync bits **d.** Precedence **bits**	1	L1	1	1	1.6.1

	Part – B **(5 x 2 = 10 Marks)**					
11	**i) An IP packet has arrived in which the offset value is 100, the value of HLEN is 5 and the value of the total length field is 100. What is the number of the first byte and the last byte?** **Each step carry 1 marks** Total length = 100 HLEN = 5*4 =20 Data length = total length – HLEN = 100-20 = 80 First byte = 100 *8 =800 Last byte = 800 +80 -1 =879	5	L3	1	2	2.6.3
	ii) Explain TCP Connection establishment process in detail with a neat diagram. **Diagram: 3marks** **Explanation: 7 marks** The three handshakes are discussed in the below steps: Step 1: SYN SYN is a segment sent by the client to the server. It acts as a **connection request** between the client and server.	10	L2	1	1	1.6.1

	It informs the server that the client wants to establish a connection. Synchronizing sequence numbers also helps synchronize sequence numbers sent between any two devices, where the same SYN segment asks for the sequence number with the connection request.  Three way Handshake Step 2: SYN-ACK It is an SYN-ACK segment or an SYN + ACK segment sent by the server. The ACK segment informs the client that the server has received the connection request and it is ready to build the connection. The SYN segment informs the sequence number with which the server is ready to start with the segments. Step 3: ACK ACK (Acknowledgment) is the last step before establishing a successful TCP connection between the client and server. The ACK segment is sent by the client as the response of the received ACK and SN from the server. It results in the establishment of a reliable data connection. After these three steps, the client and server are ready for the data communication process. TCP connection and termination are full-duplex, which means that the data can travel in both the directions simultaneously.					
	OR					
12	**i) List out the components of ARP packages and How the cache-control module is responsible for maintaining the cache table.** **1marks for list of components** **4 marks for cache control module explanation** Address Resolution Protocol Package has five components: Cache table. Queues. Output module. Input module. Cache-control module. • The cache-control module maintains the cache table. It checks the cache table entry by entry periodically, i.e. five seconds. • If the state field of the entry is FREE, it checks another entry. • If the state field of the entry is PENDING, the cache-control module increases the attempt field's value by 1. It then checks the value of the attempt field. If the attempt field's value is greater than the maximum limit that is allowed, it updates the state field to FREE and destroys	5	L2	1	1	1.6.1

	the corresponding queue. If the state field of the entry is RESOLVED, the cache-control module decreases the time outfield value by 1. It then checks the value of the time outfield. If the time outfield value is less than or equal to zero, it updates the state field of entry to FREE and destroys the corresponding queue.					
	ii) Calculate the checksum for the following IP packet: **4500 003c 1c46 4000 4006 b1e6 ac10 0a63 ac10 0a0c** Initially checksum value initialized as 0 and find checksum 4500 -> 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 003c -> 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 1c46 -> 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 4000 -> 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4006 -> 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0000 -> 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 //checksum field ac10 -> 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 0a63 -> 0 0 0 0 1 0 1 0 0 1 1 0 0 0 1 1 ac10 -> 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 0a0c -> 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0 24E17 - >1 0 0 1 0 0 1 1 1 0 0 0 0 1 0 1 1 1 SUM 4E19 - > 0 1 0 0 1 1 1 0 0 0 0 1 1 0 0 1 Sum+carry B1E6 -> 1 0 1 1 0 0 0 1 1 1 1 0 0 1 1 0 // IP Checksum **(OR)** Checksum value included in IP packet sequence solution becomes 4500 -> 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 003c -> 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 1c46 -> 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 4000 -> 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4006 -> 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0 b1e6 -> 1 0 1 1 0 0 0 1 1 1 1 0 0 1 1 0 //checksum field ac10 -> 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 0a63 -> 0 0 0 0 1 0 1 0 0 1 1 0 0 0 1 1 ac10 -> 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 0a0c -> 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0 2EBF5 -> 1 0 1 1 1 0 1 0 1 1 1 1 1 1 0 1 0 1 SUM EBF7 -> 1 1 1 0 1 0 1 1 1 1 1 1 0 1 1 1 Sum+carry 1408 -> 0 0 0 1 0 1 0 0 0 0 0 0 1 0 0 0 complemented sum **Error occurs in above packet sequence** **If students done both give full mark** **If students any one either checksum calculation or verification**	10	L3	1	2	2.6.3

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Set - B

Academic Year: 2022-23 (ODD)

Test: CLA-T1 | Date: 07-09-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Hour
Year & Sem: III Year / V Sem | Max. Marks: 25

Course Articulation Matrix:

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	1	3	-	3	1	-	-	-	1	1	-	3

Part – A
(15 x 1 = 15 Marks)

Instructions: 1) Answer ALL questions. 2) The duration for answering the part A is 15 minutes (this sheet will be collected after 15 minutes). 3) Encircle the correct answer (if more than one is right answer encircle appropriately) 4) if any of the questions * indicates choose multiple answers.

Q. No	Question	Marks	BL	CO	PO	PI Code
1	**How many bytes are reserved for target hardware address in ARP message format?** a. 4 bytes b. 6 bytes c. 8 bytes d. 16 bytes	1	L1	1	1	1.6.1
2	**The transport layer protocol used for real time multimedia, file transfer, e-mail and DNS respectively are** a. UDP,TCP,TCP and UDP b. TCP,UDP,UDP and TCP c. UDP,TCP,TCP AND UDP d. TCP,UDP,TCP AND UDP	1	L1	1	1	1.6.1
3	**Connection establishment in TCP is done by which mechanism?** a. Flow control b. Three-Way Handshaking c. Forwarding d. Synchronization	1	L1	1	1	1.6.1
4	**Which of these is not a type of error-reporting message?** a. Destination unreachable b. Source quench c. Router error d. Time exceeded	1	L1	1	1	1.6.1
5	**To accomplish flow control, TCP uses a _____ window protocol.** a. limited-size b. sliding c. fixed-size	1	L1	1	1	1.6.1

	d. variable					
6	**Which of the following is false with respect to UDP?** a. Connection-oriented b. Unreliable c. Transport layer protocol d. Low overhead	1	L1	1	1	1.6.1
7	**The value of acknowledgement field in a segment defines _____** a. sequence number of the byte received previously b. total number of bytes to receive c. sequence number of the next byte to be received d. sequence of zeros and ones	1	L1	1	1	1.6.1
8	**In case of time exceeded error, when the datagram visits a router, the value of time to live field is _____** a. Remains constant b. Decremented by 2 c. Incremented by 1 d. Decremented by 1	1	L1	1	1	1.6.1
9	**Which field helps to check rearrangement of the fragments?** a. offset b. flag c. ttl d. identifier	1	L1	1	1	1.6.1
10	**In IPv4 layer, datagram is of _____** a. Fixed length b. Variable length c. Global length d. Zero length	1	L1	1	1	1.6.1

SRM Institute of Science and Technology

Faculty of Engineering and Technology

SET - B

School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Academic Year: 2022 - 2023 (ODD)

Test: CLA - T1 **Date: 07-09-2022**
Course Code & Title: 18CSC302J – Computer Networks **Duration:** 1 Hrs
Year & Sem: III / V **Max. Marks:** 25

Course Articulation Matrix: ***(to be placed)***

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	1	3	-	3	1	-	-	-	1	1	-	3

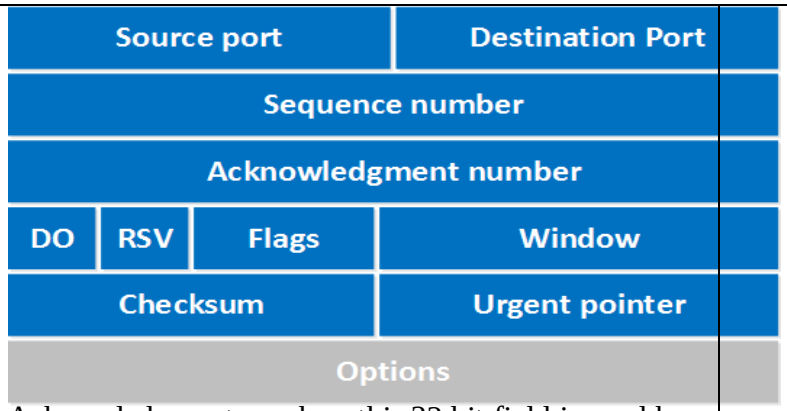
Part - A
(15 x 1 = 15 Marks)

Instructions: Answer all

Q. No	Answer with choice variable	Marks	BL	CO	PO	PI Code
1	**b. 6 bytes**	1	L1	1	1	1.6.1
2	**a. UDP,TCP,TCP and UDP**	1	L1	1	1	1.6.1
3	**b. Three-Way Handshaking**	1	L1	1	1	1.6.1
4	**c. Router error**	1	L1	1	1	1.6.1
5	**b. sliding**	1	L1	1	1	1.6.1
6	**a. Connection-oriented**	1	L1	1	1	1.6.1
7	**c. sequence number of the next byte to be received**	1	L1	1	1	1.6.1
8	**d. Decremented by 1**	1	L1	1	1	1.6.1
9	**a. offset**	1	L1	1	1	1.6.1
10	**b. Variable length**	1	L1	1	1	1.6.1

Part – B
(5 x 2 = 10 Marks)

11	i) **An IP datagram is carrying 1024 bytes of data. If there is no option information, what is the value of the header length field? What is the value of the total length field?** Data-size = 1024 bytes. Header-size = 20 bytes (since no option bytes present) HLEN = 20/4 = 5. Total length of datagram = 1024 + 20 = 1044 bytes	5	L3	1	2	2.6.3
	ii) **With a neat diagram Illustrate the various fields in TCP Header.** **Diagram: 3 marks** **Explanation: 7 marks** Let's walk through all these fields: Source port: this is a 16 bit field that specifies the port number of the sender. Destination port: this is a 16 bit field that specifies the port number of the receiver. Sequence number: the sequence number is a 32 bit field that indicates how much data is sent during the TCP session.	10	L2	1	1	1.6.1

	 Acknowledgment number: this 32 bit field is used by the receiver to request the next TCP segment. This value will be the sequence number incremented by 1. DO: this is the 4 bit data offset field, also known as the header length. It indicates the length of the TCP header so that we know where the actual data begins. RSV: these are 3 bits for the reserved field. They are unused and are always set to 0. Flags: there are 9 bits for flags, we also call them control bits. We use them to establish connections, send data and terminate connections: URG: urgent pointer. When this bit is set, the data should be treated as priority over other data. ACK: used for the acknowledgment. PSH: this is the push function. This tells an application that the data should be transmitted immediately and that we don't want to wait to fill the entire TCP segment. RST: this resets the connection, when you receive this you have to terminate the connection right away. This is only used when there are unrecoverable errors and it's not a normal way to finish the TCP connection. SYN: we use this for the initial three way handshake and it's used to set the initial sequence number. FIN: this finish bit is used to end the TCP connection. TCP is full duplex so both parties will have to use the FIN bit to end the connection. This is the normal method how we end an connection. Window: the 16 bit window field specifies how many bytes the receiver is willing to receive. Checksum: 16 bits are used for a checksum to check if the TCP header is OK or not. Urgent pointer: these 16 bits are used when the URG bit has been set, the urgent pointer is used to indicate where the urgent data ends. Options: this field is optional and can be anywhere between 0 and 320 bits.					
	OR					
12	**i) Brief about how error control mechanism is achieved through retransmission of segments.** **Retransmission –** When a segment is missing, delayed to deliver to a receiver, corrupted when it is	5	L2	1	1	1.6.1

	checked by the receiver then that segment is retransmitted again. Segments are retransmitted only during two events: when the sender receives three duplicate acknowledgements (ACK) or when a retransmission timer expires. 1. **Retransmission after RTO:** TCP always preserves one retransmission time-out (RTO) timer for all sent but not acknowledged segments. RTT is the time duration needed for a segment to reach the receiver and an acknowledgement to be received by the sender. 2. **Retransmission after Three duplicate ACK segments:** RTO method works well when the value of RTO is small. If it is large, more time is needed to get confirmation about whether a segment has been delivered or not. Sometimes one segment is lost and the receiver receives so many out-of-order segments that they cannot be saved. In order to solve this situation, three duplicate acknowledgement method is used and missing segment is retransmitted immediately instead of retransmitting already delivered segment. This is a fast retransmission because it makes it possible to quickly retransmit lost segments instead of waiting for timer to end.					
	ii) Calculate the checksum for the following ICMP packet: Type: Echo Request **Identifier : 123** **Sequence number : 20** **Message : COMPUTING** 8 and 0 -> 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 -> 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 // Checksum value 123 -> 0 0 0 0 0 0 0 0 0 1 1 1 1 0 1 1 20 -> 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 C&O -> 0 1 0 0 0 0 1 1 0 1 0 0 1 1 1 1 M&P -> 0 1 0 0 1 1 0 1 0 1 0 1 0 0 0 0 U&T -> 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 I&N -> 0 1 0 0 1 0 0 1 0 1 0 0 1 1 1 0 G&Pad-> 0 1 0 0 0 1 1 1 0 0 0 0 0 0 0 0 7AD0 -> 0 1 1 1 1 0 1 0 1 1 0 1 0 0 0 0 // SUM 852F -> 1 0 0 0 0 1 0 1 0 0 1 0 1 1 1 1 // Checksum	10	L3	1	2	2.6.3

Question Paper Setter **Approved by Audit Professor/ Course Coordinator**

*** Performance Indicators are available separately for Computer Science and Engineering in AICTE examination reforms policy.**

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Set - C

Academic Year: 2022-23 (ODD)

Test: CLA-T1 | Date: 07-09-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Hour
Year & Sem: III Year / V Sem | Max. Marks: 25

Course Articulation Matrix:

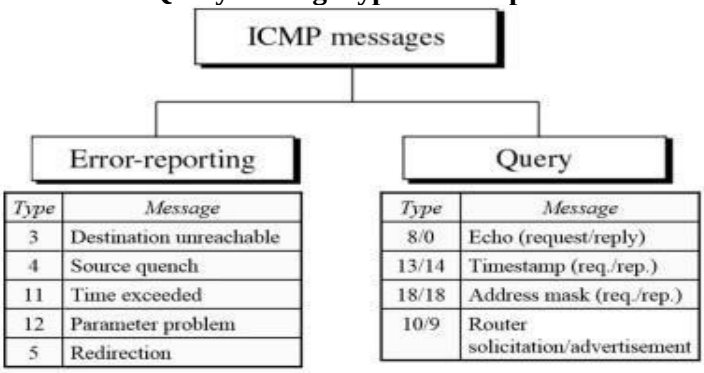
S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	1	3	-	3	1	-	-	-	1	1	-	3

Part - A
(15 x 1 = 15 Marks)

Instructions: 1) Answer ALL questions. 2) The duration for answering the part A is 15 minutes (this sheet will be collected after 15 minutes). 3) Encircle the correct answer (if more than one is right answer encircle appropriately) 4) if any of the questions * indicates choose multiple answers.

Q. No	Question	Marks	BL	CO	PO	PI Code
1	**Which of the following number is assigned for IPv4 in the protocol type field of ARP message format?** A. 0x400 B. 0x100 C. 0x800 D. 0x200	1	L1	1	1	1.6.1
2	**In socket programming, the sequence of the system calls used in the UDP echo server at the server side** (i) sendto() (ii) recvfrom() (iii) socket() (iv) bind() a. (iii),(iv),(ii),(i) b. (ii),(iv),(iii),(i) c. (i),(iii),(ii),(i) d. (iii),(iv),(i),(ii)	1	L1	1	1	1.6.1
3	**In Three-Way Handshaking process, the situation where both the TCP's issue an active open is** _____ a. Mutual open b. Mutual Close c. Simultaneous open d. Simultaneous close	1	L1	1	1	1.6.1
4	**When a router cannot route a datagram or host cannot deliver a datagram, the datagram is discarded and the router or the host sends a_____message back to the source host that initiated the datagram.** a. Destination unreachable b. Source quench c. Router error d. Time exceeded	1	L1	1	1	1.6.1

5	**In the congestion avoidance algorithm, the size of the congestion window increases_____until congestion is detected.** a. exponentially b. additively c. multiplicatively d. suddenly	1	L1	1	1	1.6.1
6	**Beyond IP, UDP provides additional services such as _____** a. Routing and switching b. Sending and receiving of packets c. Multiplexing and demultiplexing d. Demultiplexing and error checking	1	L1	1	1	1.6.1
7	**UDP length =_____– IP header's length** a. IP length b. Total length c. Packet Header length d. UDP length	1	L1	1	1	1.6.1
8	**A bit can be set in a packet moving in the direction opposite to the congestion is called_____.** a. Implicit Signaling b. Explicit Signaling c. Backward Signaling d. Forward Signaling	1	L1	1	1	1.6.1
9	**The TTL field has value 10. How many routers (max) can process this datagram?** a. 11 b. 5 c. 10 d. 1	1	L1	1	1	1.6.1
10	**Which of these is not a type of error-reporting message?** a. Destination unreachable b. Source quench c. Router error d. Time exceeded	1	L1	1	1	1.6.1

<table>
<tr><th colspan="7">Part – B
(5 x 2 = 10 Marks)</th></tr>
<tr><td>11</td><td>i) An IP packet has arrived in which the offset value is 200, the value of HLEN is 5 and the value of the total length field is 100. What is the number of the first byte and the last byte?
Each step carry 1 marks
Total length = 200
HLEN = 5*4 =20
Data length = total length – HLEN = 200-20 = 180
First byte = 100 *8 =800
Last byte = 800 + 180 -1 =979</td><td>5</td><td>L3</td><td>1</td><td>2</td><td>2.6.3</td></tr>
<tr><td></td><td>ii) Describe about the error-reporting messages and query messages.
5marks for error reporting message types with explanation
5 marks for Query message types with explanation
 

<table>
<tr><th>Type</th><th>Message</th></tr>
<tr><td>3</td><td>Destination unreachable</td></tr>
<tr><td>4</td><td>Source quench</td></tr>
<tr><td>11</td><td>Time exceeded</td></tr>
<tr><td>12</td><td>Parameter problem</td></tr>
<tr><td>5</td><td>Redirection</td></tr>
</table>
<table>
<tr><th>Type</th><th>Message</th></tr>
<tr><td>8/0</td><td>Echo (request/reply)</td></tr>
<tr><td>13/14</td><td>Timestamp (req./rep.)</td></tr>
<tr><td>18/18</td><td>Address mask (req./rep.)</td></tr>
<tr><td>10/9</td><td>Router solicitation/advertisement</td></tr>
</table></td><td>10</td><td>L2</td><td>1</td><td>1</td><td>1.6.1</td></tr>
</table>

	OR					
12	**i) Write short notes on Silly Window Syndrome in TCP flow control.** **Silly Window Syndrome** is a problem that arises due to poor implementation of TCP. It degrades the TCP performance and makes the data transmission extremely inefficient. The problem is called so because: 1. It causes the sender window size to shrink to a silly value. 2. The window size shrinks to such an extent that the data being transmitted is smaller than TCP Header. The two major causes of this syndrome are as follows: 1. Sender window transmitting one byte of data repeatedly. 2. Receiver window accepting one byte of data repeatedly.	5	L2	1	1	1.6.1
	ii) How do I calculate the checksum for a sample IPv4 packet received like this: **4500 062A 42A1 8001 4210 XXXX C0A8 0001 C0A8 0003** **Where xxxx is the checksum that needs to be sent with the packet.** 4500 : 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 062A: 0 0 0 0 0 1 1 0 0 0 1 0 1 0 1 0 42A1: 0 1 0 0 0 0 1 0 1 0 1 0 0 0 0 1 8001: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 4210: 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0000: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 //Checksum field C0A8: 1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0001: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 C0A8: 1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0003: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 2D130: 10 1101 0001 0011 0000 //sum D132: 1101 0001 0011 0010 // sum 2ECD: 0010 1110 1100 1101 //checksum	10	L3	1	2	2.6.3

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Set - D

Academic Year: 2022-23 (ODD)

Test: CLA-T1 | Date: 07-09-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Hour
Year & Sem: III Year / V Sem | Max. Marks: 25

Course Articulation Matrix:

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO1	1	3	-	3	1	-	-	-	1	1	-	3

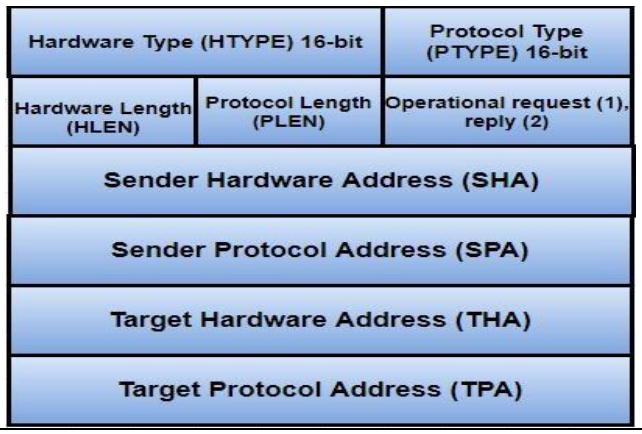
Part - A
(15 x 1 = 15 Marks)

Instructions: 1) Answer ALL questions. 2) The duration for answering the part A is 15 minutes (this sheet will be collected after 15 minutes). 3) Encircle the correct answer (if more than one is right answer encircle appropriately) 4) if any of the questions * indicates choose multiple answers.

Q. No	Question	Marks	BL	CO	PO	PI Code
1	**What command allows a user to view the ARP cache, and to add and delete entries?** a. ping b. ifconfig c. arp d. cp	1	L1	1	1	1.6.1
2	**What is the size of UDP header in bit?** a. 20 b.64 c.40 d. 8	1	L1	1	1	1.6.1
3	**The sizes of source and destination port address in TCP header are_____respectively.** a. 16-bits and 32-bits b. 16-bits and 16-bits c. 32-bits and 16-bits d. 32-bits and 32-bits	1	L1	1	1	1.6.1
4	**Two machines can use the timestamp request and timestamp replay messages to determine the _____ needed for an IP datagram to travel between them.** a. Half-trip time b. Round-trip time c. Travel time for the next router d. Time to reach the destination/source	1	L1	1	1	1.6.1
5	**The packet sent by a node to the source to inform it of congestion is called_____options** a. Explicit b. Discard c. Choke d. Backpressure	1	L1	1	1	1.6.1
6	**The port number is "ephemeral port number", if the source host is _____** a. NTP b. Echo	1	L1	1	1	1.6.1

	c. Server d. Client					
7	**What allows TCP to detect lost segments and in turn recover from that loss?** a. Sequence number b. Acknowledgment number c. Checksum d. Both Sequence & Acknowledgment number	1	L1	1	1	1.6.1
8	**During debugging, we can use the_____program to find if a host is alive and responding.** a. traceroute b. shell c. ping d. java	1	L1	1	1	1.6.1
9	**ICMP error message will not be generated for a datagram having a special address such as _____** a. 12.1.2.2 b. 11.1 c. 127 d. 127.0.0.0	1	L1	1	1	1.6.1
10	**Port number used by Network Time Protocol (NTP) with UDP is _____** a. 161 b. 123 c. 162 d. 124	1	L1	1	1	1.6.1

	Part – B **(5 x 2 = 10 Marks)**					
11	**i) An IP datagram is carrying 2048 bytes of data. If there is no option information, what is the value of the header length field? What is the value of the total length field?** Data-size = 2048 bytes. Header-size = 20 bytes HLEN = 20/4 = 5. Total length of datagram = 2048 + 20 = 2068 bytes	5	L3	1	2	2.6.3
	ii) With a neat diagram Illustrate the various fields in ARP Header. Diagram: 3marks **Explanation: 7marks** • **Hardware Type–**It is 1 for Ethernet. • **Protocol Type–**It is a protocol used in the network layer. • **Hardware Address Length–**It is the length in bytes so that it would be 6 for Ethernet. • **Protocol Address Length** – Its value is 4 bytes. • **Operation Code** indicates that the packet is an ARP Request (1) or an ARP Response (2).	10	L2	1	1	1.6.1

	• **Senders Hardware Address** – It is a hardware address of the source node. • **Senders Protocol Address** -It is a layer 3 address of the source node. • **Target Hardware Address** – It is used in a RARP request, which response impact both the destination's hardware and layer 3 addresses. **Target Protocol Address** – It is used in an ARP request when the response carries both layer 3 addresses and the destination's hardware. 					
	OR					
12	**i) write short notes on Error control in TCP is achieved through the use of three simple tools** Error control also includes a mechanism for correcting errors after they are detected. Error detection and correction in TCP is achieved through the use of three simple tools: checksum, acknowledgment, and time-out. ***Checksum:*** Each segment includes a checksum field which is used to check for a corrupted segment. ***Acknowledgment:*** TCP uses acknowledgments to confirm the receipt of data segments. ***Retransmission:*** The heart of the error control mechanism is the retransmission of segments. When a segment is corrupted, lost, or delayed, it is retransmitted.	5	L2	1	1	1.6.1
	ii) Calculate the checksum for the following UDP packet: **Source IP: 153.18.8.105** **Destination IP: 171.2.14.10** **Reserve bytes: 0** **Protocol: 17** **UDP pseudo header total length: 15** **Source port address:1087** **Destination port address:13** **UDP header length:15** **Checksum: Initial** **Message : TESTING**	10	L3	1	2	2.6.3

	153 & 18: 1 0 0 1 1 0 0 1 0 0 0 1 0 0 1 0 08& 105: 0 0 0 0 1 0 0 0 0 1 1 0 1 0 0 1 171 & 2 : 1 0 1 0 1 0 1 1 0 0 0 0 0 0 1 0 14 & 10 : 0 0 0 0 1 1 1 0 0 0 0 0 1 0 1 0 0 &17 : 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 15 : 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1087 : 0 0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 13 : 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 1 15 : 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 T & E : 0 1 0 1 0 1 0 0 0 1 0 0 0 1 0 1 S & T : 0 1 0 1 0 0 1 1 0 1 0 1 0 1 0 0 I & N : 0 1 0 0 1 0 0 1 0 1 0 0 1 1 1 0 G & Pad: 0 1 0 0 0 1 1 1 0 0 0 0 0 0 0 0 SUM : 1 0 0 1 0 1 1 0 1 1 1 0 1 0 1 1 Checksum: 0 1 1 0 1 0 0 1 0 0 0 1 0 1 0 0					

3Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Batch -1 Set - A

Academic Year: 2022-23 (ODD)

Test: CLA-T2 | Date: 19-10-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Period
Year & Sem: III Year / V Sem | Max. Marks: 25

Course Articulation Matrix:

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO2	2	3	-	2	1	-	-	-	2	1	-	3
2	CO3	2	3	-	3	1	-	-	-	2	1	-	3

Part – A
(5 x 1 mark = 5 Marks)

Instructions: 1) Answer ALL questions. 2) Write the correct answer in the answer booklet

Q. No	Question	Marks	BL	CO	PO	PI Code
1	SCTP allows_____service in each association. a) Single stream **b) Multistream** c) Double stream d) None of the above	1	L1	2	1	1.6.1
2	If error occurs in the data transfer between the client and the server, the send and receive function will return a) 0 b) 1 **c) -1** d) 0 or 1	1	L2	2	1	1.6.1
3	RPC works between two processes. These processes must be _____ a) on the same computer b) on different computers connected with a network **c) on the same computer and also on different computers connected with a network**	1	L1	2	1	1.6.1

	d) on none of the computers					
4	In the process of fetching a web page from a server , the HTTP request/response takes a) 2 RTT **b) 1 RTT** c) 4 RTT d) 3 RTT	1	L2	3	1	1.6.1
5	The facilities available in the internet are (i) electronic mail (ii) remote login (iii)file transfer (iv)word processing a. i, ii **b. i, ii, iii** c. i, ii, iv d. ii, iii and iv	1	L1	3	1	1.6.1

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Academic Year: 2022-23 (ODD)

Batch -1 Set - A

Test: CLA-T2 | Date: 19-10-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Period
Year & Sem: III Year / V Sem | Max. Marks: 25

Part – B
(2 x 10 marks = 20 Marks)

Instructions: Answer the questions

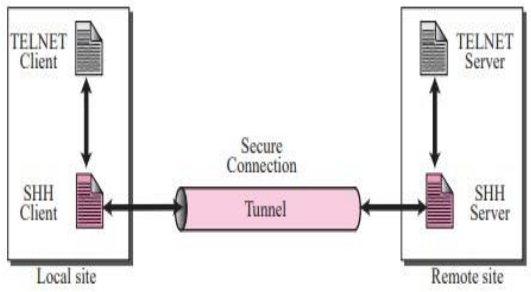
Q. No	Question	Marks	BL	CO	PO	PI Code
6 a.	If an application developer needs to modify the code that is running on a Linux server, How the developer establishes the remote connection in a secured mode and explains the connection protocol in detail.	10	L3	2	2	4.1.1

Answer:-

Port Forwarding

One of the interesting services provided by the SSH protocol is to provide **port forwarding**. We can use the secured channels available in SSH to access an application program that does not provide security services. Application such as TELNET (see Chapter 20) and SMTP (see Chapter 23) can use the services of SSH using port forwarding mechanism. SSH port forwarding mechanism creates a tunnel through which the messages belonging to other protocol can travel. For this reason, this mechanism is sometimes referred to as SSH **tunneling**. Figure 20.18 shows the concept of port forwarding.

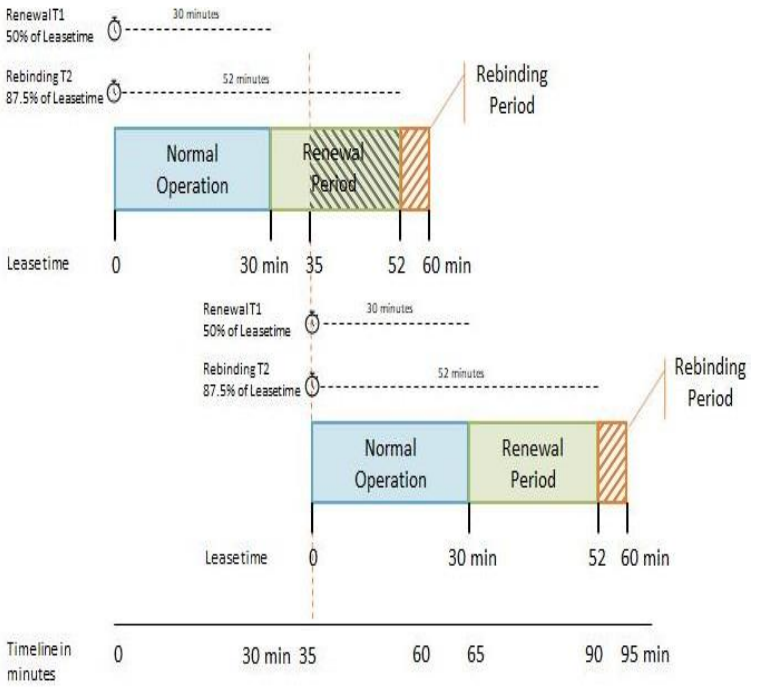
Figure 20.18 *Port Forwarding*

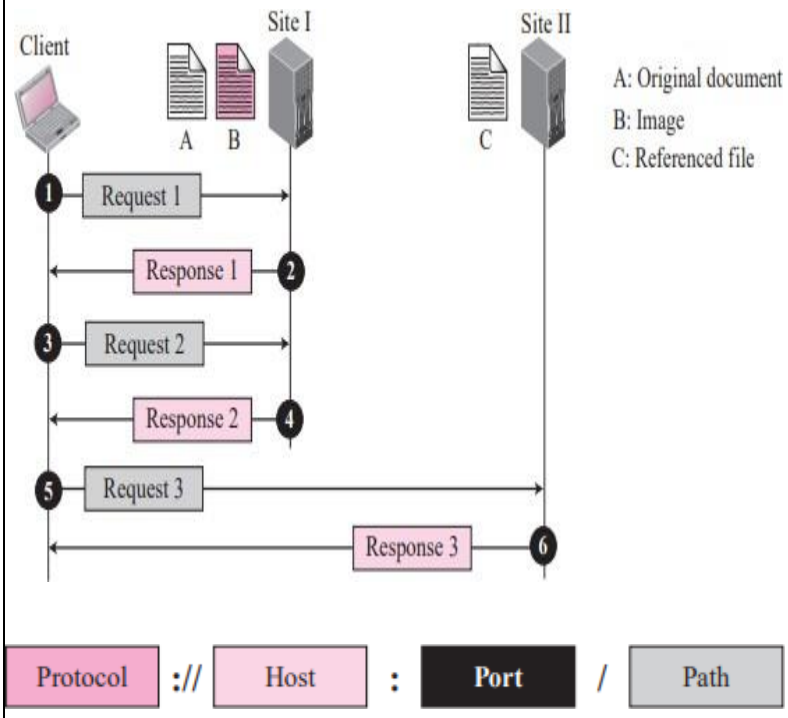


We can change a direct, but insecure, connection between the TELNET client and the TELNET server by port forwarding. The TELNET client can use the SHH client on the local site to make a secure connection with the SSH server on the remote site. Any

	request from the TELNET client to the TELNET server is carried through the tunnel provided by the SSH client and server. Any response from the TELNET server to the TELNET client is also carried through the tunnel provided by the SSH client and server.					
	(OR)					
6 b.	A receiver received a SCTP packet contains five different chunks such as chunk 1, chunk2 … chunk 5. Chunk 1 the value of type field is 1. Chunk 2 is a data chunk and its flag bits B and E shows the value 1 and 0. Chunk 3 is a data chunk and its flag bits indicates the value of B is 1 and E is 1. Chunk 4 the value of type field is 0, flag bits value of B is 0 and E is 1. 1. Identify the type of Chunk1 and give description for the same. What will be the value of flag field for the chunk1? (2) 2. What is the value of Chunk2 type field and chunk 2 is a fragment or not? (2) 3. What are all the data chunk is a fragment chunk 1, chunk2, chunk3 or chunk4? Give your justification for the same. (2) 4. In SCTP Packets How the receiver knows there is a padding or not? Give your justification. (2) 5. Chunk 5 carries no information. what will be the value of length field? (2) **Answer:-** 1. Identify the type of Chunk1 and give description for the same. What will be the value of flag field for the chunk1? (2) • The value of type field is 1. So chunk 1 is INIT chunk (initiation chunk). • Initiation chunk is the first chunk sent by an end point to establish an association 2. What is the value of Chunk2 type field and chunk 2 is a fragment or not? (2) • Chunk 2 is a data chunk. So its value of type field will be 0. • Chunk 2 is fragment because The B (beginning) and E (end) bits together define the position of a chunk in a message that is fragmented for the chunk 2 beginning is 1 and end is 0. 3. What are all the data chunk is a fragment chunk 1, chunk2, chunk3 or chunk4? Give your justification for the same. (2)	10	L2	2	2	2.7.1

	• Chunk 2 and chunk 4 is fragmented. • Chunk 1 is INIT chunk • Chunk 2, 3, and 4 having value of B and F. • Chunk2 B=1 and E=0 it is the first fragment. • Chunk3 B=1 and E=1 no fragment. • Chunk4 B=0 and E=1 it is the last fragment. 4. In SCTP Packets How the receiver knows there is a padding or not? Give your justification. (2) The length of the padding, if any, is not included in the calculation of the length field. This helps the receiver find out how many useful bytes a chunk carries. If the length field value is not a multiple of 4, the receiver knows there is padding. 5. Chunk 5 carries no information. what will be the value of length field? (2) If a chunk carries no information, the value of the length field is 4 (4 bytes).					
7 a.	The DHCP mandates a minimum address lease of 24 hours. Can you imagine a situation in which DHCP's lease time causes inconvenience? Explain with an example. **Answer:-** **Students needs to explain by considering their own scenario as an example given below.** **Scenario:** If you have a coffee bar and you get 400 visitors a day. They stay on average 30 to 60 minutes and you have a DHCP Pool of 200 IP Address (192.168.0.10 – 192.168.0.210 for example). When you leave the DHCP Lease Time on the default 24 hours (1440 minutes) after 200 guest no other guest can use the free WIFI network. Because all the 200 IP Addresses are reserved for the first 200 guests. So, in this case you want to lower the DHCP Lease Time to one hour for example. This way the reservation is	10	L3	3	2	2.7.1

	released soon enough for the other guests:  With a lease time one hour, the client will try to renew the lease after 30 minutes. At 35 min it contacts the DHCP server to extend/renew the lease. It's granted so the timers reset, a new lease is acquired for another 60 minutes. In total, the IP Address is reserved for 95 minutes. With 200 addresses available you can have 130 guests per hour on average on your network.					
	(OR)					
7 b.	Assume you need to retrieve a scientific document that contains one reference to another text file and one reference to a large image. The main document and the image are stored in two separate files on the same site (file A and file B); the referenced text file is stored on another site (file C). Demonstrate the three transactions to see the whole document. Also, give the uniform resource locator format to locate any kind of information on the Internet. **Answer:-**	10	L2	3	1	1.6.1


Client
Site I
Site II
A
B
C
A: Original document
B: Image
C: Referenced file
1
Request 1
Response 1
2
3
Request 2
Response 2
4
5
Request 3
Response 3
6

Protocol
://
Host
:
Port
/
Path

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Batch -1 Set - B

Academic Year: 2022-23 (ODD)

Test: CLA-T2 | Date: 19-10-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Period
Year & Sem: III Year / V Sem | Max. Marks: 25

Course Articulation Matrix:

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO2	2	3	-	2	1	-	-	-	2	1	-	3
2	CO3	2	3	-	3	1	-	-	-	2	1	-	3

Part – A
(5 x 1 mark = 5 Marks)

Instructions: 1) Answer ALL questions. 2) Write the correct answer in the answer booklet

Q. No	Question	Marks	BL	CO	PO	PI Code
1	Intel follows_____type of ordering to store the data. a. Both Little and Big Endian b. Little or Big Endian c. Big Endian **d. Little Endian**	1	L1	2	1	1.6.1
2	In a connection, the value of cwnd is 4000 and the value of rwnd is 5000. The host has sent 1,000 bytes, which have not been acknowledged. How many more bytes can be sent? a. 4000 b. 1000 c. 2000 **d. 3000**	1	L2	2	1	1.6.1
3	The FIN + ACK segment consumes_____sequence number if it does not carry data. a. 0 b. **1** c. 2 d. 3	1	L2	2	1	1.6.1
4	Which of the following statement is wrong? a) telnet is a general purpose client-server program b) telnet lets user access an application on a remote computer **c) telnet can also be used for file transfer** d) telnet can be used for remote login	1	L1	3	1	1.6.1
5	The port number_____and_____is used for data and control connection a) 21, 20	1	L1	3	1	1.6.1

	b) 20,21 c) 20,12 d) 12,21					

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Batch -1 Set - B

Academic Year: 2022-23 (ODD)

Test: CLA-T2 | Date: 19-10-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Period
Year & Sem: III Year / V Sem | Max. Marks: 25

Part – B
(2 x 10 marks = 20 Marks)

Instructions: Answer the questions

Q. No	Question	Marks	BL	CO	PO	PI Code
6 a.	The problem is to implement a client - server user-level application using sockets API in C/C++. The Server application has to support at least five clients simultaneously. Server accepts strings from clients (even multiple strings from each client) and replies with reverse strings. For example, when client sends "NAME", Server replies with "EMAN". Both server and client(s) have to output both sending & receiving strings on the terminal.	10	L3	2	2	2.6.3

Answer:-

Client

```
#include <arpa/inet.h>
#include <netinet/in.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/socket.h>
#include <unistd.h>

#define PORT 8090

// Driver code
int main()
{
    struct sockaddr_in address;
    int sock = 0, valread;
    struct sockaddr_in serv_addr;
    char str[100];

    printf("\nInput the string:");
    scanf("%[^\n]s", str);

    char buffer[1024] = { 0 };
```

```
    // Creating socket file descriptor
    if ((sock = socket(AF_INET,
                       SOCK_STREAM, 0))
        < 0) {
        printf("\n Socket creation error \n");
        return -1;
    }

    memset(&serv_addr, '0', sizeof(serv_addr));
    serv_addr.sin_family = AF_INET;
    serv_addr.sin_port = htons(PORT);

    // Convert IPv4 and IPv6 addresses from
    // text to binary form 127.0.0.1 is local
    // host IP address, this address should be
    // your system local host IP address
    if (inet_pton(AF_INET, "127.0.0.1",
                  &serv_addr.sin_addr)
        <= 0) {
        printf("\nAddress not supported \n");
        return -1;
    }

    // connect the socket
    if (connect(sock, (struct sockaddr*)&serv_addr,
                sizeof(serv_addr))
        < 0) {
        printf("\nConnection Failed \n");
        return -1;
    }

    int l = strlen(str);

    // send string to server side
    send(sock, str, sizeof(str), 0);

    // read string sent by server
    valread = read(sock, str, l);

    printf("%s\n", str);

    return 0;
}
```

Server

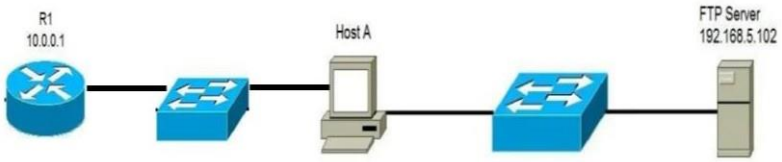
```
#include <netinet/in.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/socket.h>
#include <unistd.h>

#define PORT 8090
```

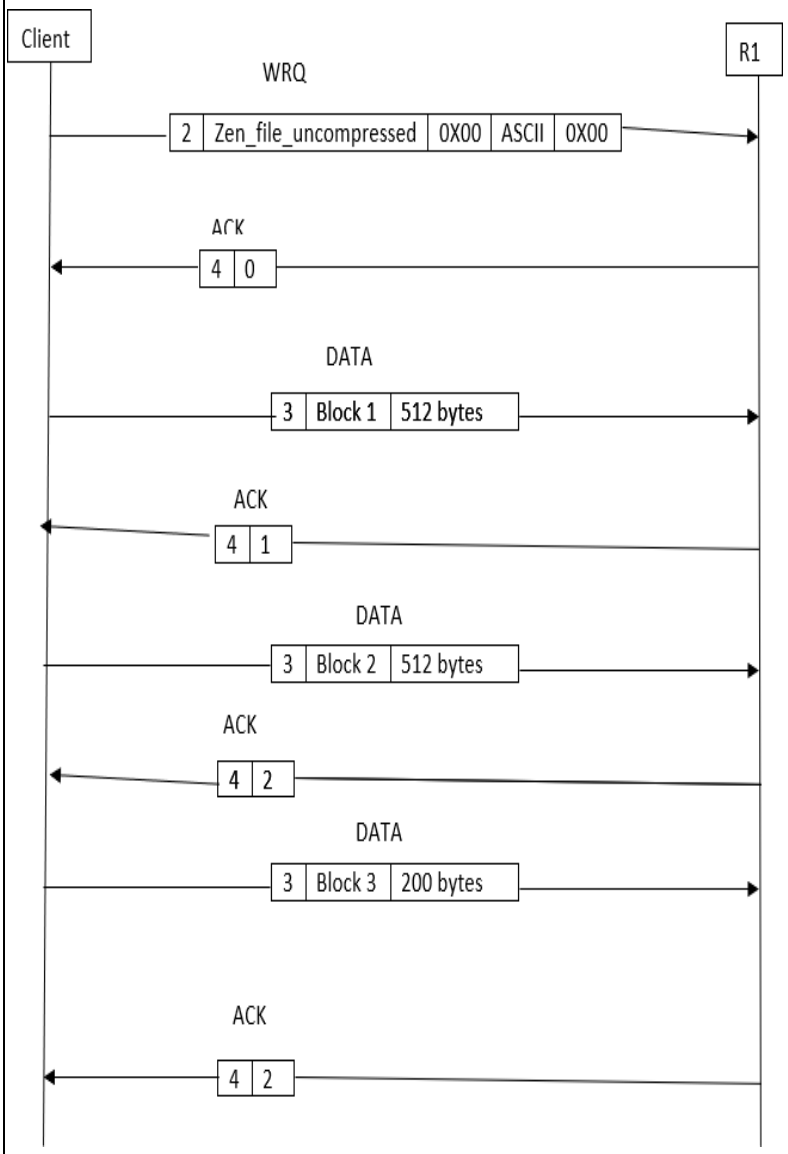
```
// Driver code
int main()
{
    int server_fd, new_socket, valread;
    struct sockaddr_in address;
    char str[100];
    int addrlen = sizeof(address);
    char buffer[1024] = { 0 };
    char* hello = "Hello from server";

    // Creating socket file descriptor
    if ((server_fd = socket(AF_INET,
                    SOCK_STREAM, 0)) == 0) {
        perror("socket failed");
        exit(EXIT_FAILURE);
    }

    address.sin_family = AF_INET;
    address.sin_addr.s_addr = INADDR_ANY;
    address.sin_port = htons(PORT);

    // Forcefully attaching socket to
    // the port 8090
    if (bind(server_fd, (struct sockaddr*)&address,
                    sizeof(address)) < 0) {
        perror("bind failed");
        exit(EXIT_FAILURE);
    }

    // puts the server socket in passive mode
    if (listen(server_fd, 3) < 0) {
        perror("listen");
        exit(EXIT_FAILURE);
    }
    if ((new_socket = accept(server_fd,
                (struct sockaddr*)&address,
                (socklen_t*)&addrlen)) < 0) {
        perror("accept");
        exit(EXIT_FAILURE);
    }

    // read string send by client
    valread = read(new_socket, str,
                sizeof(str));
    int i, j, temp;
    int l = strlen(str);

    printf("\nString sent by client:%s\n", str);

    // loop to reverse the string
    for (i = 0, j = l - 1; i < j; i++, j--) {
        temp = str[i];
        str[i] = str[j];
        str[j] = temp;
    }
```

	// send reversed string to client
	// by send system call
	send(new_socket, str, sizeof(str), 0);
	printf("\nModified string sent to client\n");
	
	return 0;
	}					

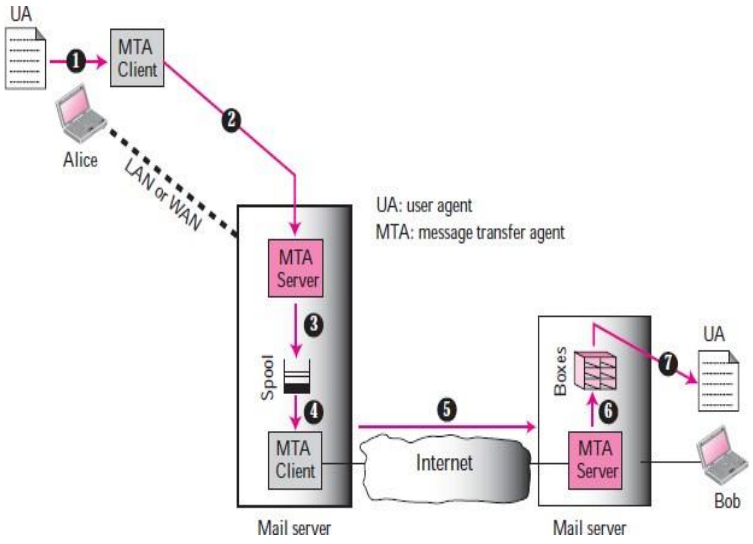
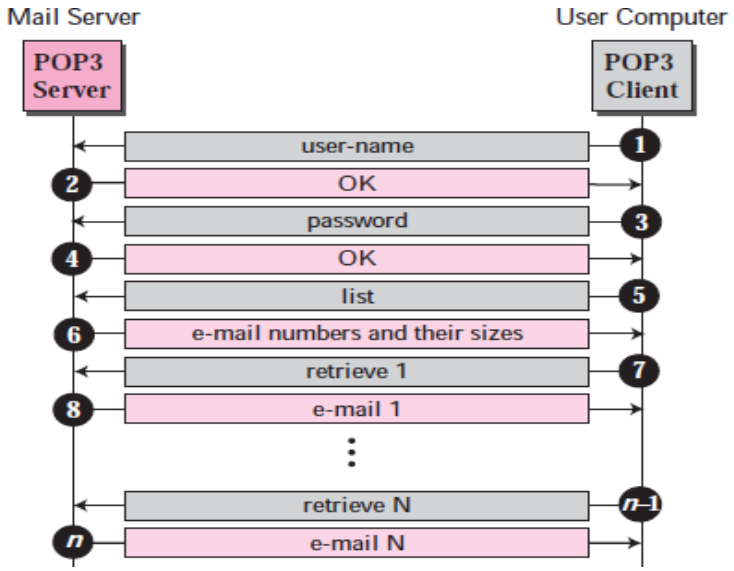
	(OR)					
6 b.	1. A client uses UDP to send data to a server. The data length is 16 bytes. Calculate the efficiency of this transmission at the UDP level (5 Marks) **Answer:-** Length of Header = 8 bytes Data length = 16 Bytes Total bytes transferred = Length of Header+ Data length = 24 bytes Efficiency = useful bytes transferred / Total Bytes Transferred = 16/24 =66.667% 2. Answer below question. i) Discuss about the types of Byte ordering. (2) ii) What are the examples of Byte ordering? (1) iii) Does bigendian affects file formats? (1) iv Which one is better byte ordering? (1) **Answer:-** i) An arrangement of bytes when data is transmitted over the network is called byte ordering. Different computers will use different byte ordering. ● When communication taking place between two machines byte ordering should not make discomfort. ● Generally an Internet protocol will specify a common form to allow different machines byte ordering. TCP/IP is the Internet Protocol in use. ● Two ways to store bytes : Big endian and little endian ● Big-endian –High order byte is stored on starting address and low order byte is stored on next address ● Little-endian –Low order byte is stored on starting address and high order byte is stored on next address	10	L2	2	1	1.6.1

	ii) Intel based processors are little endians. ARM processors were little endians. Current generation ARM processors are bi-endian. Motorola 68K processors are big endians. PowerPC (by Motorola) and SPARK (by Sun) processors were big endian. Current version of these processors are bi-endians. iii) File formats which have 1 byte as a basic unit are independent of e.g., ASCII files. Other file formats use some fixed endianness format e.g, JPEG files are stored in big endian format. iv) The term little and big endian came from Gulliver's Travels by Jonathan Swift. Two groups could not agree by which end an egg should be opened -a- the little or the big. Just like the egg issue, there is no technological reason to choose one-byte ordering convention over the other, hence the arguments degenerate into bickering about sociopolitical issues. As long as one of the conventions is selected and adhered to consistently, the choice is arbitrary.					

7 a.	 **1.** Zen access the host A machine needs to download the ascii file "Zen_file" in compressed form from the FTP Server. The file resides in the path "ftpd/user/Zen". Identify the suitable protocol and suggests Zen in framing the appropriate commands to download the file. **Answer:-** **File Transfer Protocol** 220 (Service ready) USER Zen 331 (User name OK. Password?) PASS yyy 230 (User login OK) PORT 1267 150 (Data Connection opens shortly) TYPE ASCII 200 (OK) STRU F 200 (OK) MODE C 200 (OK) RETR ftpd/user/Zen/Zen_file 250 (OK) (Data Transfer from server to client) 226 (Closing data connection) QUIT 221 (Service closing) **2.** Zen uncompresses the received Zen_file and needs to store in R1. The uncompressed Zen_file consumes 1224 bytes of data. Identify the suitable protocol and suggest Zen in framing message structure in writing the content to R1. **Answer:-** **Trivial File Transfer Protocol**	10	L3	3	2	2.6.3


Client
R1
WRQ
2
Zen_file_uncompressed
0X00
ASCII
0X00
ACK
4
0
DATA
3
Block 1
512 bytes
ACK
4
1
DATA
3
Block 2
512 bytes
ACK
4
2
DATA
3
Block 3
200 bytes
ACK
4
2

(OR)

7b.	1. In Email communication system, A sender is connected to the mail server via LAN/WAN, identify the component requirements and draw the system architecture. **Answer:-**  2. Why Message Access Agent is required, and with a neat interaction diagram, specify the interaction between user computer and POP3 server. **Answer:-** The actual mail transfer is done through message transfer agents. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA. The first and the second stages of mail delivery use SMTP. However, SMTP is not involved in the third stage because SMTP is a push protocol; it pushes the message from the client to the server.  	10	L2	3	1	1.6.1

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Batch -2 Set - C

Academic Year: 2022-23 (ODD)

Test: CLA-T2 | Date: 19-10-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Period
Year & Sem: III Year / V Sem | Max. Marks: 25

Course Articulation Matrix:

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO2	2	3	-	2	1	-	-	-	2	1	-	3
2	CO3	2	3	-	3	1	-	-	-	2	1	-	3

Part – A
(5 x 1 mark = 5 Marks)

Instructions: 1) Answer ALL questions. 2) Write the correct answer in the answer booklet

Q. No	Question	Marks	BL	CO	PO	PI Code
1	The Socket API function that converts an unconnected active TCP socket into a passive socket is_____. a. Bind Function b. Socket Function **c. Listen Function** d. Accept Function	1	L1	2	1	1.6.1
2	TCP connection is transferring the file of size 4000 bytes. The first byte is numbered 20,001. What will be the sequence number for the third segment if data are sent in four segments each carrying 1000 bytes? a. 20,001 b. 21,001 **c. 22,001** d. 23,001	1	L1	2	1	1.6.1
3	The UDP header in hexadecimal format is given as **CD83000B001C001C.** What is the source port number? **a. 52611** b. 52100 c. 52099 d. 52355	1	L2	2	1	1.6.1
4	The value of the magic cookie is _____ a. 99.130.81.88 **b. 99.130.83.99** c. 99.131.82.99 d. 99.99.99.99	1	L2	3	1	1.6.1
5	In the_____encoding scheme, 24 bits become 4 characters, and eventually are sent as 32 bits.	1	L1	3	1	1.6.1

	a. 8bit b. 16bit **c. base64** d. binary					

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Batch -2 Set - C

Academic Year: 2022-23 (ODD)

Test: CLA-T2 | Date: 19-10-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Period
Year & Sem: III Year / V Sem | Max. Marks: 25

Part – B
(2 x 10 marks = 20 Marks)

Instructions: Answer the questions

Q. No	Question	Marks	BL	CO	PO	PI Code
6 a.	User1 wants to communicate with user2 for transfer data with each other. For communicating of each user can create a socket module for data transfer. Each user can transmit data to another user. Format of the data transfer between host and user in byte order. The following question are as i) What is byte ordering in network programming? (2M) ii) Why byte order functions is need for network (2M) programming? iii) Socket module provides various functions for translating host order to network order (6M) **Solution:** i) This convention, known as network byte order, defines the bit-order of network addresses as they pass through the network. The TCP/IP standard network byte order is big-endian. In order to participate in a TCP/IP network, little-endian systems usually bear the burden of conversion to network byte order. ii) To allow machines with different byte order conventions communicate with each other, the Internet protocols specify a canonical byte order convention for data transmitted over the network. This is known as Network Byte Order. iii) htonl() translates an unsigned long integer into network byte order. htons() translates an unsigned short integer into network byte order. ntohl() translates an unsigned long integer into host byte order. ntohs() translates an unsigned short integer into host byte order.	10	L3	2	2	2.6.3
	(OR)					

6 b.	Alice and Bob discuss about the use of computer network for a particular application. They want to share multiple audio and video streams of data in each connection with increasing reliability or performance. They want to use a reliable message oriented protocol for this purpose. Help them with the explanation of such a protocol. Also differentiate in what ways this protocol is different from the existing protocols used for similar use. Outline the services provided by such protocol.	10	L2	2	1	1.6.1

Solution:

Key:

Identifying the need for SCTP (4)

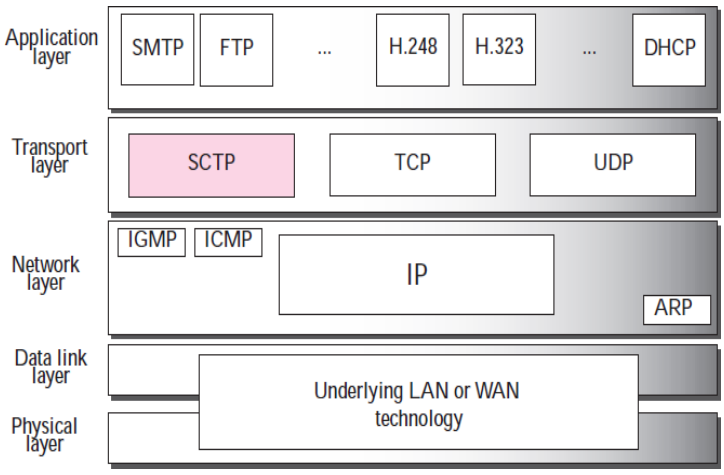
Comparison and contrasting of UDP, TCP, and SCTP (3)

Outlining the SCTP services (3)

SCTP (4):

SCTP is designed as a general-purpose transport layer protocol that can handle multimedia and stream traffic, which are increasing every day on the Internet.

It is a new reliable, message-oriented transport-layer protocol.



Comparison and contrasting of UDP, TCP, and SCTP (3)

UDP	TCP	SCTP
Message-oriented protocol	Byte-oriented protocol	Best features of UDP and TCP
UDP conserves the message boundaries	No preservation of the message boundaries	Preserves the message boundaries along with detection of lost data, duplicate data, and out-of-order data
UDP is unreliable	TCP is a reliable protocol	SCTP is a reliable message oriented Protocol
Lacks in congestion control and flow control	TCP has congestion control and flow control mechanisms	It has congestion control and flow control mechanisms

SCTP services (3)

Process-to-Process Communication

Multiple Streams

Multihoming

Full-Duplex Communication

Connection-oriented service

Reliable service

7 a.	A customer connects to the ISP and wants to send request for websites to the ISP. The servers and routers in the ISP send these requests to its own DNS cache server and Name Servers, sometimes have to send a query to a Root Name	10	L3	3	2	2.6.3

Server outside of the ISP if it is unable to resolve the requested domain name within its system. When the Root Server resolves the request, the ISP will add this information to its own DNS system.

The solution had to be able to capture DNS traffic in such a way that shows every bit of information about what was happening during the DNS query process, while also being able to store the data and able to run analysis on the data.

i) How do you capture DNS traffic and look at every specific detail of the packet in order to identify the issues, or important traffic information?

In order to solve the main issue for all DNS solutions is that they need to reply to queries quickly and with the correct information. The correct information means that the ISP can resolve the request with the correct address, and hopefully, not direct the end−user to a malicious site. Thus, one of the main problems DNS systems face is Security.

ii) Discuss about possible corruptions happening in DNS server records.

Solution:

i)

Traffic Analysis:

How do you capture DNS traffic and look at every specific detail of the packet in order to identify the issues, or important traffic information?

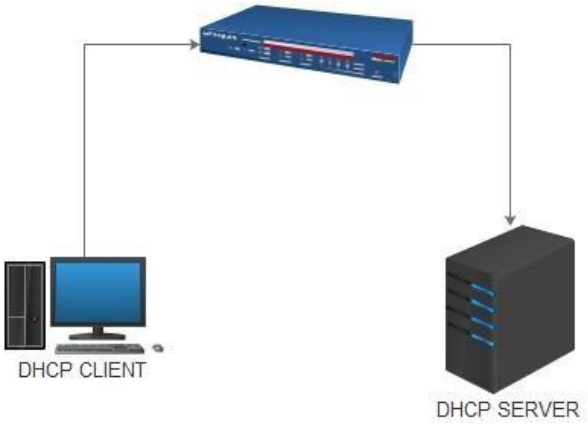
This was one of the major concerns for the ISP since their current solution could not capture and do a Deep Packet Inspection with the detail they needed. They needed to be able to look at captured data overa period of time and look at historical bits of information. This information could provide them the abilityto see traffic patterns, trends, errors, DNS attacks, and even misconfigured network elements such as routers, switches and DNS servers.

Another issue is that of dropped packets. Yes, packets can be dropped in a DNS query and an error is sentto the client. Through traffic analysis, the ISP can see why, and where, the packets are being dropped.

They also want to see when an address is queried and is not resolved, but directs the client to a default search engine or specific page. They want to be able to tell why it's not being resolved. It may not be a malicious redirect, but rather a request typed incorrectly by the client, or the domain may not exist anymore. There are many possibilities for this, but being able to find the exact reason why, quickly, is of major importance as the ISP has to be concerned with the satisfaction of their customers.

Differences between a DNS cache system and the Name Server can cause many issues for a DNS resolversystem. Symmetry between these systems is a key issue that the ISP was concerned about. If the DNS cache is not updated by the Name Servers, then it will always query the Name Servers for the domain name, creating an

	unnecessary step and extra traffic in the query process. ii) **Security Issues:** 1. DOS attacks − Servers supporting recursive DNS queries are vulnerable to phony requests thatflood a particular IP address with the results of each server's query. This can overwhelm the IPaddress with a volume of traffic, causing the site/server to crash. 2. Cache Poisoning − the attacker corrupts a DNS server by replacing a legitimate IP address in theserver's cache with a re−direct address in order to redirect traffic to a malicious website. 3. DNS amplification − a form of DDoS, the attacker takes advantage of a DNS server that permits recursive lookups and uses recursion to spread the attack to other DNS servers. The system sends requests to the targeted IP address (victim), causing a storm of responses to flood the IPaddress and shuts the site down. DNS Fast−Flux − is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever−changing network of compromised hosts acting as proxies. The basic idea behind Fast flux is to have numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records. 4. DNS Fast−Flux − is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever−changing network of compromised hosts acting as proxies. The basic idea behindFast flux is to have numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, through changingDNS records.					
(OR)						

7 b.	i) Can DHCP prevent unauthorized laptops from using a network that uses DHCP for dynamic addressing? ii) Explain the communication flow between a DHCP client and server on a network with two DHCP Servers. iii) Consider the below diagram, a DHCP client and server is connected to a switch. How does the DHCP process start?  	10	L2	3	1	1.6.1

Solution:

i) 3M

Answer – No, DHCP is not capable of distinguishing between a permanent MAC address and the address by the user. So, it cannot stop unauthorized access to a network and cannot control the IP addresses used by users.

ii) 3M

The first packet the DHCP Client initiates would be the DHCP Discover packet. The DHCP Discover packet is broadcast in nature and would be received by both the DHCP servers. The DHCP servers would respond with DHCP offer packet containing the IP addresses which they offer. Based on the first DHCP offer the client receives, the client would respond with DHCP request packet which contains the IP address which it would be using along with the DHCP servers IP address which had provide the respective. This packet is sent as broadcast. The packet, when received by the other DHCP server would understand that the IP address which it had leased to the client (In the DHCP offer packet) is not taken. So, the DHCP server would put the IP address back to its pool.

iii) 4M

The TCP/IP of the client would be configured with the option 'Obtain IP address automatically'. This is meant for DHCP clients. This configuration would automatically trigger a DHCP Discover packet from the PC. This packet

	would reach the DHCP server which would then respond with the DHCP offer packet.					

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Batch -2 Set - D

Academic Year: 2022-23 (ODD)

Test: CLA-T2 | Date: 19-10-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Period
Year & Sem: III Year / V Sem | Max. Marks: 25

Course Articulation Matrix:

S.No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1	CO2	2	3	-	2	1	-	-	-	2	1	-	3
2	CO3	2	3	-	3	1	-	-	-	2	1	-	3

Part – A (5 x 1 mark = 5 Marks)

Instructions: 1) Answer ALL questions. 2) Write the correct answer in the answer booklet

Q. No	Question	Marks	BL	CO	PO	PI Code
1	Winsock and Socket are examples of_____. a. DSL **b. API** c. IPX d. VCN	1	L1	2	1	1.6.1
2	Echo protocol in TCP uses_____port number to echo the received datagram back to the sender. **a. 7** **b.** 9 **c.** 11 **d.** 13	1	L2	2	1	1.6.1
3	A packet is carrying a COOKIE ECHO message and a DATA chunk. If the size of the cookie is 300 bytes and that of the user data is 15 bytes, what is the size of the packet? **a. 347** b. 350 c. 345 d. 315	1	L2	2	1	1.6.1
4	When both sender and receiver are connected to a mail server via a LAN or a WAN, we need_____. a. three UAs, and three pairs of MTAs b. two UAs, and two pairs of MTAs c. two UAs, two pairs of MTAs, and two pairs of MAAs **d. two UAs, two pairs of MTAs, and a pair of MAAs**	1	L1	2	1	1.6.1
5	_____is more powerful and complex than _____ a. POP3; IMAP4 **b. IMAP4; POP3** c. SMTP; POP3 d. SMTP; IMAP4	1	L1	2	1	1.6.1

Register Number															

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu

Academic Year: 2022-23 (ODD)

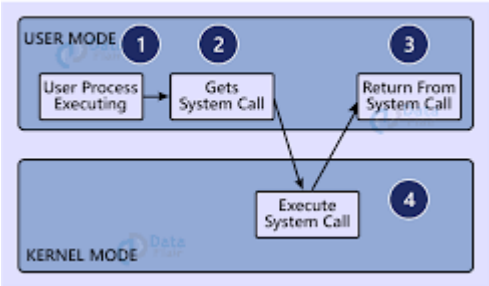
Batch -2 Set - D

Test: CLA-T2 | Date: 19-10-2022
Course Code & Title: 18CSC302J – Computer Networks | Duration: 1 Period
Year & Sem: III Year / V Sem | Max. Marks: 25

Part – B
(2 x 10 marks = 20 Marks)

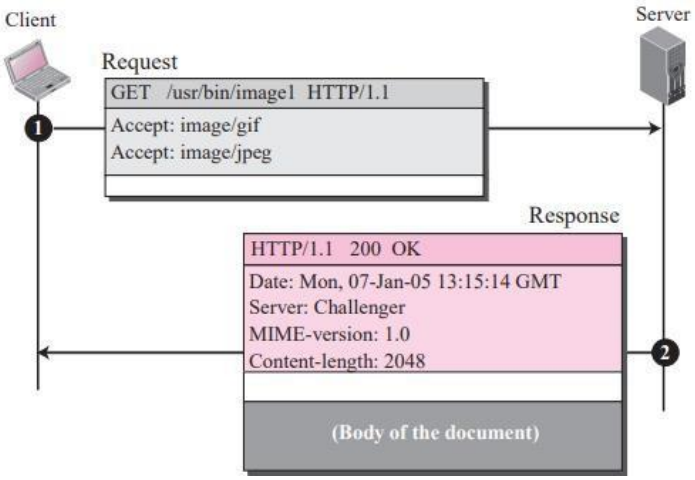
Instructions: Answer the questions

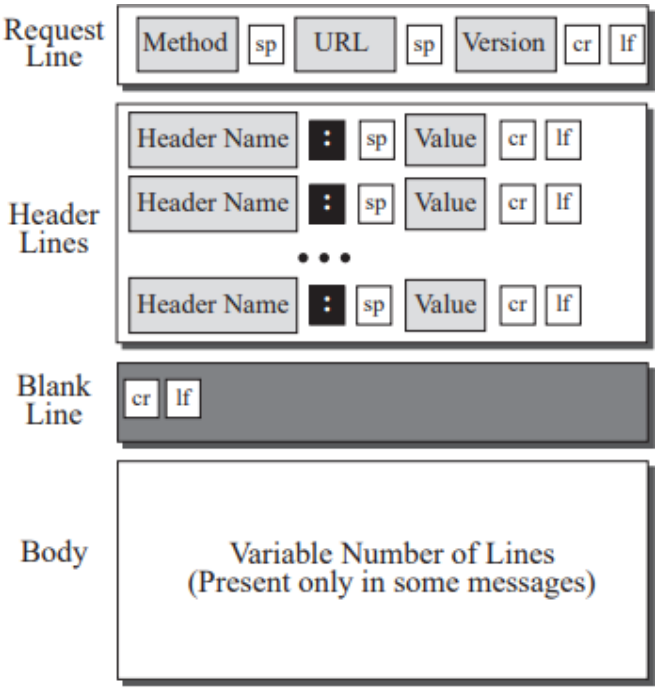
Q. No	Question	Marks	BL	CO	PO	PI Code
6 a.	Sam was studying for computer networks exam. While studying he got a doubt regarding which programmatic way provides the services to interact with the operating system. Help him in identifying the relevant concept to clear his doubt. Also list out the services provided by the identified concept with a diagrammatic representation. **Solution:** **System Call** In computing, a system call is the programmatic way in which a computer program requests a service from the kernel of the operating system it is executed on. A system call is a way for programs to interact with the operating system. A computer program makes a system call when it makes a request to the operating system's kernel. System call provides the services of the operating system to the user programs via Application Program Interface (API). It provides an interface between a process and operating system to allow user-level processes to request services of the operating system. System calls are the only entry points into the kernel system. All programs needing resources must use system calls. **Services Provided by System Calls:** 1. Process creation and management 2. Main memory management 3. File Access, Directory and File system management	10	L3	2	2	2.6.3

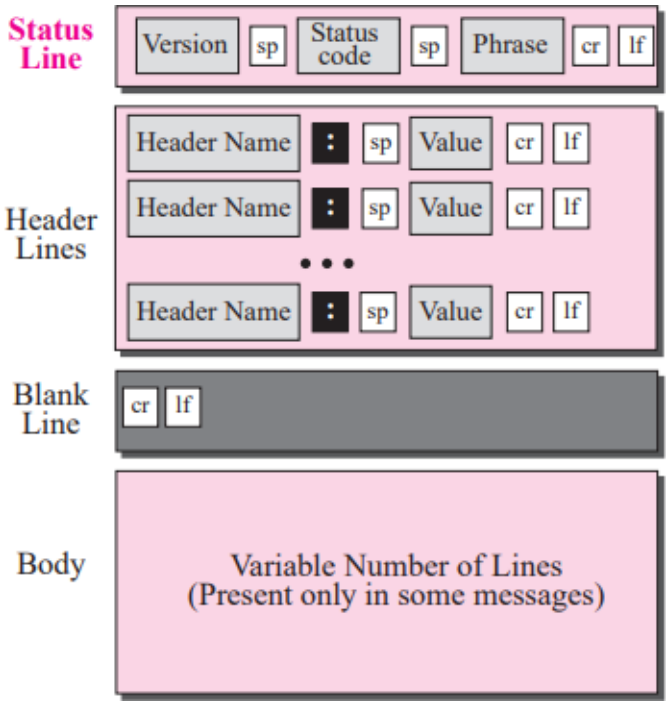
	4. Device handling(I/O) 5. Protection 6. Networking, etc. **Types of System Calls**: There are 5 different categories of system calls – 1. Process control: end, abort, create, terminate, allocate and free memory. 2. File management: create, open, close, delete, read file etc. 3. Device management 4. Information maintenance 5. Communication **WORKING OF A SYSTEM CALL**  					
(OR)						
6 b.	The following is a dump of a UDP header in hexadecimal format. 0045DF0000580000 i. What is the source port number? ii. What is the destination port number? iii. What is the total length of the user datagram? iv. What is the length of the data? v. Has the sender calculated checksum for this packet? **Solution:** a. 0045 = 69 b. DF00 = 57088 c. 0058 = 88 bytes d. 88 bytes – 8 bytes header= 80 bytes e. Last 16 bits are zeros so no calculated checksum	10	L2	2	1	1.6.1
7 a.	Sketch the format of the HTTP request and response message. Illustrate the following scenario, assume in HTTP transactions for communication between client and server use the GET method to retrieve an image with the URL, path	10	L3	3	2	2.6.3

/usr/bin/image1. The client can accept images in GIF or JPEG format. The request does not have a body. The response message must contain the date, server, MIME version, and length of the document which is 2048. Followed by a header the body of the document can be blank.

Solution:



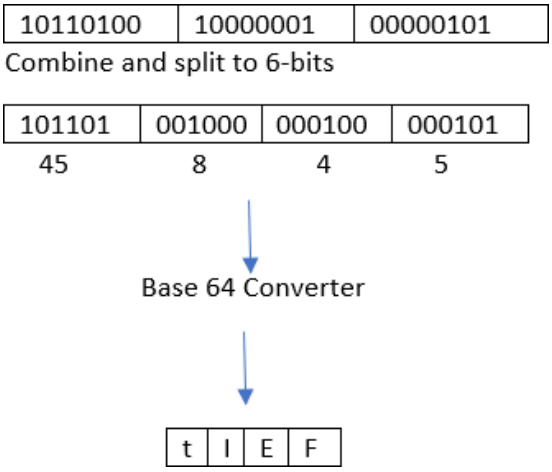




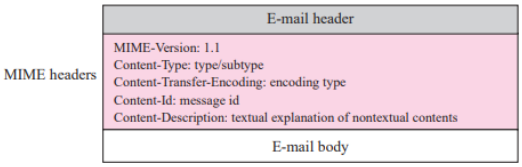
(OR)

7 b.	Rahul sends a mail to his parents. As Email has some limitations supplementary protocols are used so that non-ASCII data can be sent through e-mail. Some specific header fields are added with respective to the conversion done in the message. i. Explain as when the RFC subtype and Partial subtype will be used? ii. In Which type of the encoding scheme the non-ASCII character is represented as three characters. iii. Explain how the following set of bits (Non-Ascii Data) can be encoded using Base 64. 10110100 | 10000001 | 00000101 iv. Draw the structure of MIME Header for MIME version 1.1. **Solution:** a. RFC822, partial, and external-body. The subtype RFC822 is used if the body is encapsulating another message (including header and the body). The partial subtype is used if the original message has been fragmented into different mail messages and this mail message is one of the fragments. The fragments must be reassembled at the destination by MIME. Three parameters must be added: id, number, and the total. The id identifies the message and is present in all the fragments. The number defines the sequence order of the fragment. The total defines the number of fragments that comprise the original message. b. Quoted-printable	10	L2	3	1	1.6.1

c. Base64 transforms this type of data to printable characters, which can then be sent as ASCII characters or any type of character set supported by the underlying mail transfer mechanism. Base64 divides the binary data (made of streams of bits) into 24-bit blocks. Each block is then divided into four sections, each made of 6 bits



d.



SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Set A

Academic Year: 2022-23 (ODD) **Test: CLA-T3** **Year & Sem: III** Year / VI Sem
Date: - **Max. Marks:** 50 **Duration: 1 Hour 40 min**
Course Code & Title: 18CSC302J & COMPUTER NETWORKS

Course Articulation Matrix: ***(to be placed)***

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	L	H	-	H	L	-	-	-	L	L	-	H
CO2	M	H	-	M	L	-	-	-	M	L	-	H
CO3	M	H	-	H	L	-	-	-	M	L	-	H
CO4	M	H	-	H	L	-	-	-	M	L	-	H
CO5	H	H	-	H	L	-	-	-	M	L	-	H
CO6	L	H	-	H	L	-	-	-	L	L	-	H

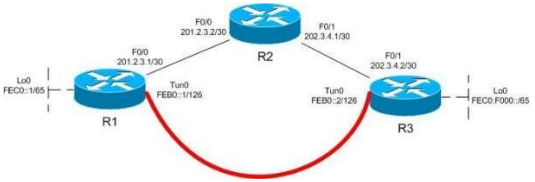
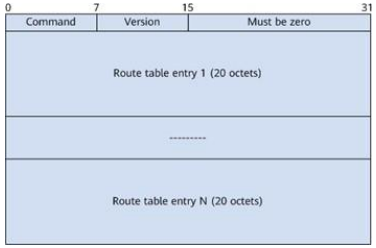
Part – A Instructions: Answer all the questions (1 x 10 = 10 Marks)

Q. No	Question	Marks	BL	CO	PO	PI Code
1	Which of the following is the shortest valid abbreviation for DE80:0000:0000:0100:0000:0000:0000:0123? a)DE80::100::123 b)DE8::1::123 **c)DE80::100:0:0:0:123** d)DE80:0:0:100::1230	1	L2	4	1	1.6.1
2	The length of IPv6 is_____bits a)64 b) 32 c)256 **d)128**	1	L1	4	1	1.6.1
3	The term for the packet counter that tells a router when to drop a packet in ipv6 is _____ a)Time To Live(TTL) **b) hop limit** c)Round Trip Time(RTL) d)hop count	1	L1	4	1	1.6.1
4	The IPv6 version of BGP is_____ **a) MP-BGPv4** b) BGPv5 c) BGP IPv6 d) MP-BGPv2	1	L2	4	1	1.6.1
5	The meaning of RA in IPv6 is _____ a) Reach advertisement b) RIP advertisement **c) Router advertisement** d) Reach Advance	1	L2	4	1	1.6.1
6	The high bit rate Digital Subscriber Line (HDSL) uses two twisted pairs to achieve a) Full duplex transmission b) Half duplex transmission' c)Encoding d)Decoding	1	L2	6	1	1.6.1
7	_____Channel is reserved for voice communication. a) Channel 0 b)Channel 1 c) Channel 2 c) Channel 3	1	L1	5,6	1	1.6.1
8	Virtual Private Network (VPN) is one of the applications of a)MAC Protocols b)SMTP c)IPSec d) TLS Protocol	1	L2	5,6	1	1.6.1
9	Which two options are valid WAN connectivity methods? a) PPPb)DSLc)WAP d)Ethernet	1	L1	5, 6	1	1.6.1
10	Which protocol does the PPP protocol to provide for handling the capabilities of the connection/link on the network? a)LCP b) NCP c)Both LCP and NCP d)TCP	1	L1	6	1	1.6.1
Part – B	**Instructions: Answer any 4 Questions**					**(10 x 4 = 40 Marks)**
11. a)	In computer networks, using IPv6 features explain the mechanism of hosting an address on the network along with the address types. Three major categories of IPv6 addresses: **Unicast**—A unicast address identifies a single interface.When a network device sends a packet to a unicast address, the packet goes only to the specific interface identified by that address.Unicast addresses support a global address scope and two types of local address scopes. A unicast address consists of *n* bits for the prefix, and 128 – *n* bits for the interface ID.	10	L3	4	2	2.6.1

	For a subscriber access network, the following types of unicast addresses can be used: **Global unicast address** - A unique IPv6 address assigned to a host interface. These addresses have a global scope and essentially the same purposes as IPv4 public addresses. Global unicast addresses are routable on the Internet. **Link-local IPv6 address** - An IPv6 address that allows communication between neighboring hosts that reside on the same link. Link-local addresses have a local scope, and cannot be used outside the link. They always have the prefix FE80::/10. **Loopback IPv6 address** - The IPv6 loopback address is 0:0:0:0:0:0:0:1, which can be notated as ::1/128. **Unspecified address** -An IPv6 unspecified address is 0:0:0:0:0:0:0:0, which can be notated as ::/128. **Multicast**—For a set of interfaces on the same physical medium. A packet is sent to all interfaces associated with the address.When a network device sends a packet to a multicast address, the device broadcasts the packet to all interfaces identified by that address.IPv6 does not support broadcast addresses, but instead uses multicast addresses in this role. Multicast addresses support 16 different types of address scope, including node, link, site, organization, and global scope.A 4-bit field in the prefix identifies the address scope. Multicast addresses use the prefix FF00::/8. The following types of multicast addresses can be used in an IPv6 subscriber access network: •**Solicited-node multicast address** - Neighbor					
	Solicitation(NS) messages are sent to this address. •**All-nodes multicast address** - Router Advertisement(RA) messages are sent to this address. •**All-nodes multicast address** - Router Advertisement (RA) messages are sent to this address. •**All-routers multicast address** - Router Solicitation (RS) messages are sent to this address. **Anycast**—For a set of interfaces on different physical media. A packet is sent to only one of the interfaces associated with this address, not to all the interfaces.					
	OR					
11. b)	Let's say that someone uses a laptop that is connected to a router for browsing a website. The laptop sends the request of the site in a packet to the router, which passes it along to the web. But first, the router changes the outgoing IP address from a private local address to a public address. If the packet keeps a private address, the receiving server won't know where to send the information back. For both economic and security purposes, describe the process of assigning a unique public IP address so the information will make it back to the laptop using the router's public address, not the laptop's private one. NAT is implemented on a network that requires few addresses to access the Global Internet. A routing table is created on the router that contains a list of 'Inside' local address mapped to 'inside' global (legal IP) address.	10	L4	4	2	2.6.4

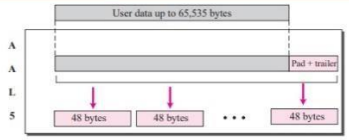
	In the example, the inside host wants to communicate with the outside world and the destination web server. Then it will send a data packet to the NAT-enabled gateway router of the network for further communication.The inside station sends the first packet to the router which is checked for address match in the NAT table. The gateway router learns the source IP address of the packet and looks up in the table whether the packet meets the condition for translation. The gateway router maintains an access control list (ACL) which locates the authenticated hosts for internal network translation purposes.The inside station connects to the outside station. Thus it will translate the inside local IP address into an inside global IP address. It will then saves this translation in the NAT table and the gateway router will route the packet to the destination. When the web server of the Internet reverts back to the request, the packet will revert back to the global IP address of the router. Now the gateway router will again look up in the NAT table to find out the translated IP address corresponding to the global address. It then translates it to the inside local address and then the data packet is delivered to the host.This mapping is stored as a simple entry in the NAT table. If a match is not found in the table then the packet is discarded. If no match is found, the router refers to the available pool of outside addresses to translate the inside address to an					

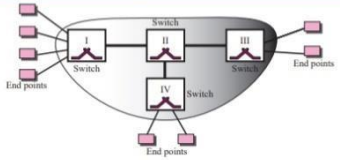
	outside address. The outside station receives the packet and replies to the outside addresses given by the NAT table.The router checks the table for inside to outside address mapping and forwards the packet to the inside station.The inside station receives the packet.					
12. a)	Consider a large enterprise specialized in exporting goods has approached you to modernize its network and to make sure that they are ready for the future implementation of IPv6. The backbone of the network is still based on IPv4, and you are not allowed to make any changes. Being a senior network engineer, give an explanation on how do you provide a way to use an existing IPv4 in transition to IPv6? There are different methods of tunneling IPv6 through an IPv4 backbone, and they are divided into two major groups which are automatic and manual. Automatic tunnels are configured by using IPv4 address information embedded in an IPv6 address – the IPv6 address of the destination host includes information about which IPv4 address the packet should be tunneled to. Configured tunnels must be configured manually. These tunnels are used when using IPv6 addresses that do not have any embedded IPv4 information. The IPv6 and IPv4 addresses of the endpoints of the tunnel must be specified. we will be using a manually configured IPv6 tunnel since this is for a enterprise and there will be very minimal management required. All IPv4	10	L4	4	2	2.6.1

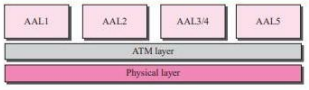
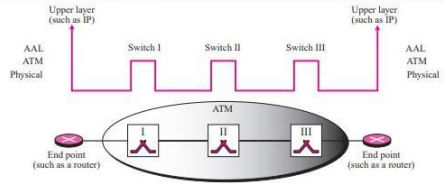
	and IPv6 addresses have been manually configured . OSPFv2 has been configured in the IPv4 domain for connectivity between the routers. Configure a IPv6 over IPv4 tunnel between router R1 and R3. Enable RIPNG on router R1,R2 and R3. R1:Enable IPv6 unicast routing, Configure a default IPv4 static route via R2,Configure Tun0 with a mode of ipv6ip, a source of F0/0, and the destination address of the Tun0 on R3,Configure IPv6 OSPF Area 0 on Lo0 and Tun0 R2:Configure the two interfaces with basic IP addressing R3:Enable IPv6 unicast routing,Configure a default IPv4 static route via R2,Configure Tun0 with a mode of ipv6ip, a source of F0/1, and the destination address of the Tun0 on R1,Configure IPv6 OSPF Area 0 on Lo0 and Tun0  **OR**					
12. b)	Elaborate in brief about IPv6 routing protocols that enable routers to exchange information about connected networks. (Any 3 protocols) •**Exterior Gateway Protocols** Exterior gateways protocols are used to exchange routing information among different Autonomous Systems (AS). - Border Gateway Protocol (BGP4+). - Exterior Gateway Protocol (EGP) •**Interior Gateway Protocols** Interior gateway protocols are used to handle routing information within Autonomous Systems (AS).The most common interior gateway routing protocols are two kinds, such as Distance vector protocols and link state protocols. ***Distance vector protocols*** - RIP (Routing information Protocol) - EIGRP (Enhanced Interior Gateway Routing Protocol) - IGRP (Interior Gateway Routing Protocol) ***Link state protocols*** - OSPF (Open Shortest Path First) - IS-IS (Intermediate System-to-Intermediate System) **RIPng (**Routing Information Protocol Next Generation): This is an Interior Routing Protocol and is a Distance Vector Protocol. RIPng has been upgraded to support IPv6.  **OSPFv3 (** Open Shortest Path First version 3):It is an Interior Routing Protocol modified to support IPv6. This is a Link-State Protocol and uses Djikrasta's Shortest Path First algorithm to	10	L3	4	2	2.6.4

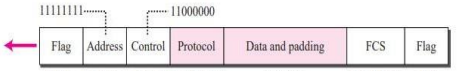
	calculate the best path to all destinations. 0 7 15 23 31 Version | Type | Packet length Router ID Area ID Checksum | Instance ID | 0 **MP-BGP4** **(**Modified ProtocolBorder Gateway Protocol):It is the only open standard Exterior Gateway Protocol available. BGP is a Distance Vector protocol that takes an Autonomous System as a calculation metric, instead of the number of routers as Hop. BGPv4 is an upgrade of BGP to support IPv6 routing. +---+ | Address Family Identifier (2 octets) | +---+ | Subsequent Address Family Identifier (1 octet) | +---+ | Length of Next Hop Network Address (1 octet) | +---+ | Network Address of Next Hop (variable) | +---+ | Number of SNPAs (1 octet) | +---+ | Length of first SNPA(1 octet) | +---+ | First SNPA (variable) | +---+ | Length of second SNPA (1 octet) | +---+ | Second SNPA (variable) | +---+ | ... | +---+ | Length of Last SNPA (1 octet) | +---+ | Last SNPA (variable) | +---+ | Network Layer Reachability Information (variable) | +---+					
13. a)	i) Imagine the length of a 10Base5 cable is 2500 meters. If the speed of propagation in a thick coaxial cable is 200,000,000 meters/second:	6+4	L4	6	2	2.6.1

	a. How long does it take for a bit to travel from the beginning to the end of the network? *b.* Find the maximum time it takes to sense a collision (worst case). ii)The data rate of 10Base5 is 10Mbps. How long does it take to create the smallest frame? Show your calculations. a. Distance = Velocity × Time $Time = \frac{Distance}{Velocity} = \frac{2500m}{200{,}000{,}000m/s} = \mathbf{12.5\mu s}$ Therefore, it takes 12.5µs for a bit to travel from beginning to the end of the network. b. Maximum time to sense a collision = 2 × 12.5 μs = **25 μs** ii) **Answer:** The smallest frame is 64 bytes or 512 bits. With a data rate of 10 Mbps, we have Tfr = (512 bits) / (10 Mbps) = 51.2 µs This means that the time required to send the smallest frame is the same at themaximum time required to detect the collision. **OR**					
13. b)	i) Find how an IP packet can be encapsulated in ATM cells using AAL5 layer. (4 marks)	10	L3	5,6	2	2.6.4

	AAL5, which is sometimes called the **simple and efficient adaptation layer (SEAL)**, assumes that all cells belonging to a single message travel sequentially and that control functions are included in the upper layers of the sending application. AAL5 is designed for connectionless packet protocols that use a datagram approach to routing (such as the IP protocol in TCP/IP). **The IP protocol uses the AAL5 sublayer.** AAL5 accepts an IP packet of no more than 65,535 bytes and adds an 8-byte trailer as well as any padding required to ensure that the position of the trailer falls where the receiving equipment expects it (at the last 8 bytes of the last cell). See Figure 3.37. Once the padding and trailer are in place, AAL5 passes the message in 48-byte segments to the ATM layer.  ii)Draw the architecture of an ATM network and explain its layers (6 marks)					

	ATM Architecture ATM is a switched network. The user access devices, called the end points, are connected to the switches inside the network. The switches are connected to each other using high-speed communication channels. Figure 3.33 shows an example of an ATM network. **Virtual Connection** Connection between two end points is accomplished through transmission paths (TPs), virtual paths (VPs), and virtual circuits (VCs). A **transmission path (TP)** is the physical connection (wire, cable, satellite, and so on) between an end point and a switch or between two switches. Think of two switches as two cities. A transmission path is the set of all highways that directly connects the two cities. *INTRODUCTION AND UNDERLYING TECHNOLOGIES* **Figure 3.33** *Architecture of an ATM network*  A transmission path is divided into several virtual paths. A **virtual path (VP)** provides a connection or a set of connections between two switches. Think of a virtual path as a highway that connects two cities. Each highway is a virtual path; the set of all highways is the transmission path.					

	ATM Layers The ATM standard defines three layers. They are, from top to bottom, the application adaptation layer, the ATM layer, and the physical layer as shown in Figure 3.35. **Figure 3.35** *ATM layers*  The physical and ATM layer are used in both switches inside the network and end points (such as routers) that use the services of the ATM. The application adaptation layer (AAL) is used only by the end points. Figure 3.36 shows the use of these layers inside and outside an ATM network. **Figure 3.36** *Use of the layers*  *AAL Layer* The **application adaptation layer (AAL)** allows existing networks (such as packet networks) to connect to ATM facilities. AAL protocols accept transmissions from upper-layer services (e.g., packet data) and map them into fixed-sized ATM cells. These transmissions can be of any type (voice, data, audio, video) and can be of variable or fixed rates. At the receiver, this process is reversed—segments are reassembled into their original formats and passed to the receiving service. Although four AAL layers have been defined the one which is of interest to us is AAL5, which is used to carry IP packets in the Internet.					
14. a)	i)Name the special protocol which helps to control and manage the transfer of data over telephone lines. ii) Explain about the layers of PPP? iii) Draw a neat diagram of PPP frame format and explain the fields in detail. Answer:	10	L3	6	2	2.6.4

	PPP The telephone line or cable companies provide a physical link, but to control and manage the transfer of data, there is a need for a special protocol. The **Point-to-Point Protocol (PPP)** was designed to respond to this need. *PPP Layers* PPP has only physical and data link layers. No specific protocol is defined for the physical layer by PPP. Instead, it is left to the implementer to use whatever is available. PPP supports any of the protocols recognized by ANSI. At the data link layer, PPP defines the format of a frame and the protocol that are used for controlling the link and transporting user data. The format of a PPP frame is shown in Figure 3.31. **Figure 3.31** *PPP frame*  The descriptions of the fields are as follows: 1. **Flag field.** The flag field identifies the boundaries of a PPP frame. Its value is 01111110. 2. **Address field.** Because PPP is used for a point-to-point connection, it uses the broadcast address used in most LANs, 11111111, to avoid a data link address in the protocol. 3. **Control field.** The control field is assigned the value 11000000 to show that, as in most LANs, the frame has no sequence number; each frame is independent. 4. **Protocol field.** The protocol field defines the type of data being carried in the data field: user data or other information. 5. **Data field.** This field carries either user data or other information. 6. **FCS.** The frame check sequence field is simply a 2-byte or 4-byte CRC used for error detection. **OR**					
14. b)	Organize the different types of HDLC frames and explain in detail. High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. To provide the flexibility necessary to support all the options possible in the modes and configurations just described, HDLC defines three types of frames:	10	L4	6	2	2.6.4

information frames (I-frames), supervisory frames (S-frames), and unnumbered frames (V-frames). Each type of frame serves as an envelope for the transmission of a different type of message. I-frames are used to transport user data and control information relating to user data (piggybacking). S-frames are used only to transport control information. V-frames are reserved for system management. Information carried by V-frames is intended for managing the link itself.

Frame Format:

Each frame in HDLC may contain up to six fields, as shown in Figure: a beginning flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field. In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.

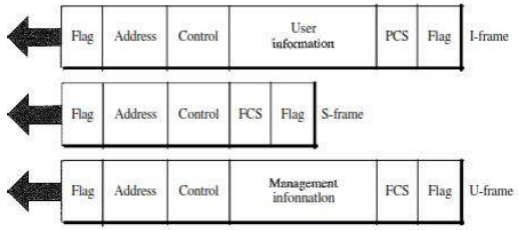


Fig no.29

Control Field The control field determines the type of frame and defines its functionality. So let us discuss the format of this field in greater detail. The format is specific for the type of frame, as shown in Figure

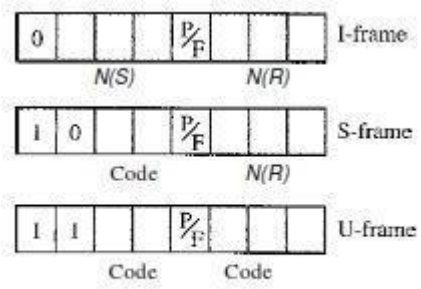


Fig no.30

Control Field for I-Frames:- I-frames are designed to carry user data from the network layer. In addition, they can include flow and error control information (piggybacking). The subfields in the control field are used to define these functions. The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame. The next 3 bits, called N(S), define the sequence number of the frame.

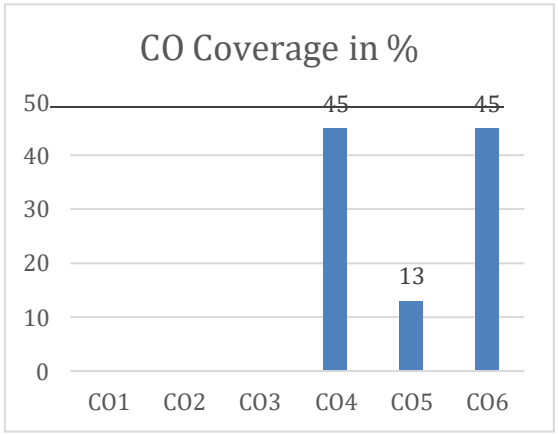
Control Fieldfor S-Frames Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than an acknowledgment). S-frames do not have information fields. If the first 2 bits of the control field is 10, this means the frame is an S-frame.

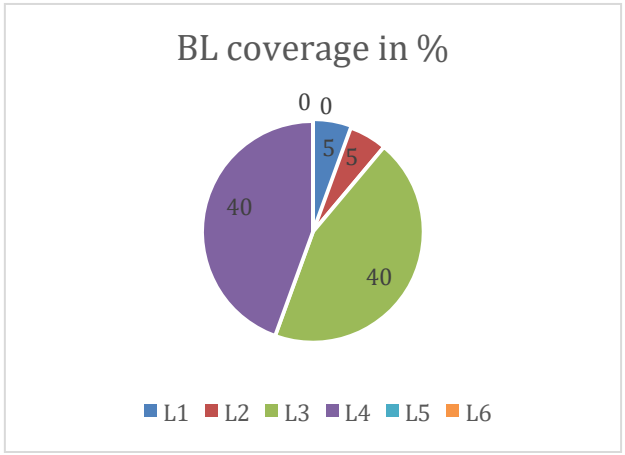
Receive ready (RR): If the value of the code subfield is 00, it is an RR S-frame. This kind of

	frame acknowledges the receipt of a safe and sound frame or group of frames. In this case, the value N(R) field defines the acknowledgment number. Receive not ready (RNR): If the value of the code subfield is 10, it is an RNR S-frame. **Reject (REJ):** If the value of the code subfield is 01, it is a REJ S-frame. This is a NAK frame, but not like the one used for Selective Repeat ARQ. It is a NAK that can be used in Go-Back-N ARQ to improve the efficiency of the process by informing the sender, before the sender time expires, that the last frame is lost or damaged. The value of NCR) is the negative acknowledgment number. **Selective reject (SREJ):** If the value of the code subfield is 11, it is an SREJ S-frame. This is a NAK frame used in Selective Repeat ARQ. Note that the HDLC Protocol uses the term selective reject instead of selective repeat. The value of N(R) is the negative acknowledgment number. **Control Field for V-Frames** Unnumbered frames are used to exchange session management and control information between connected devices. Unlike S-frames, U-frames contain an information field, but one used for system management information, not user data. As with S-frames, however, much of the information carried by U-frames is contained in codes included in the control field.					

***Program Indicators are available separately for Computer Science and Engineering in AICTE examination reforms policy.**

Course Outcome (CO) and Bloom's level (BL) Coverage in Questions





Approved by the Audit Professor/Course Coordinator

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Academic Year: 2022-23(ODD)
Date: 23-11-2022

Test: CLA-T3 (ANSWER KEY)
Max. Marks: 50
Course Code & Title: 18CSC302J & COMPUTER NETWORKS

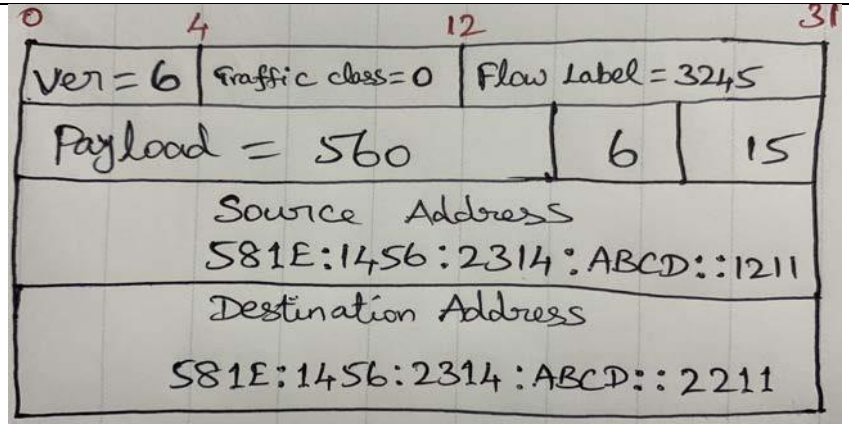
Year & Sem: II I Yr / VI Sem
Duration: 1 Hour 40 min

Part – A Instructions: Answer all the questions (1 x 10 = 10 Marks)						
Q. No	**Question**	**Marks**	**BL**	**CO**	**PO**	**PI Code**
1	In the IPv6 header, the traffic class field is similar to which field in the IPv4 header? **D) ToS field**	1	L1	4	1	1.6.1
2	Suppose two IPv6 nodes want to interoperate using IPv6 datagrams, but they are connected to each other by intervening IPv4 routers. The best solution here is _____ **B) Tunneling**	1	L1	4	1	1.6.1
3	Which among the following features is present in IPv6 but not in IPv4? **B) Anycast address**	1	L1	4	1	1.6.1
4	In an IPv6 datagram, M bit is 0, value of HLEN is 5, value of total length is 700 and offset value is _____ **D) 700**	1	L2	4	1	1.6.1
5	To determine which version to use when sending a packet to a destination, the source host queries which of the following? **B) Domain name server**	1	L1	4	1	1.6.1
6	When a router is connected to a Frame Relay WAN link using a serial DTE interface, how is the clock rate determined? **A) Supplied by the CSU/DSU**	1	L1	6	1	1.6.1

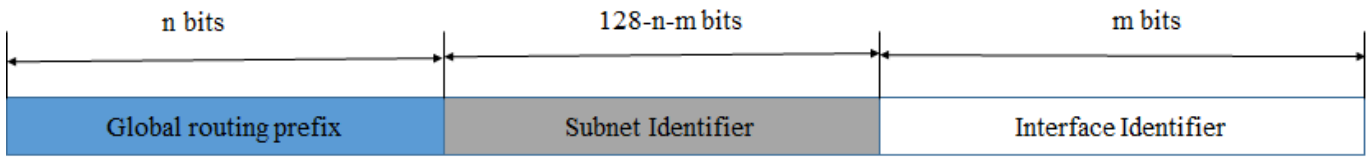
7	The command required for connectivity in a Frame Relay network if inverse ARP is not operational **D) Frame Relay – MAP**	1	L1	6	1	1.6.1
8	Suppose that you have a customer who has a central HQ and six branch offices. They anticipate adding six more branches in the near future. They wish to implement a WAN technology that will allow the branches to economically connect to HQ and you have no free ports on the HQ router. Which of the following would you recommend? **B) Frame Relay**	1	L2	5	1	1.6.1
9	A software organization is implementing dial-up services to enable remote-office employees to connect to the local network. The company uses multiple routed protocols, needs authentication of users connecting to the network, and since some calls will be long distance, needs call-back support. Which of the following protocols is the best choice for these remote services? **D) PPP**	1	L2	5, 6	1	1.6.1
10	_____ describes the creation of private networks across the Internet, enabling privacy and tunneling of non-TCP/IP protocols? **a) VPN**	1	L1	6	1	1.6.1
Part – B (10 x 4 = 40 Marks) Instructions: Answer any 4 Questions						
11. A)	**(i) Compare and contrast IPv4 & IPv6.**	5	L3	4	2	2.6.1

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration

	The Security feature is dependent on application	IPSEC is an inbuilt security feature in the IPv6 protocol					
	In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header					
	In IPv4 checksum field is available	In IPv6 checksum field is not available					
	It has broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available					
	IPv4 has a header of 20-60 bytes.	IPv6 has header of 40 bytes fixed					
	IPv4 consist of 4 fields which are separated by dot (.)	IPv6 consist of 8 fields, which are separated by colon (:)					
	IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C , Class D , Class E.	IPv6 does not have any classes of IP address.					
	IPv4 supports VLSM (Variable Length subnet mask).	IPv6 does not support VLSM.					
	(ii) An IPv6 packet consists of the base header and a TCP segment. The length of data is 560 bytes. Show the packet and enter a value for each field.						

	 • Version : 4-bit field to specify the version (value is 6 for IPv6) • Traffic Class: Distinguish the payload. • Flow label: Mention special handling for a particular flow of data. • Payload length: Defines the length of the IP datagram in payload (560 bytes). • Next Header : Optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP (value is 6 for TCP). • Hop Limit : TTL (Value is 15) • Source Address: Original source address. • Destination Address: Final destination of datagram. **(OR)**					
11. B)	**Draw and explain the three levels of hierarchy of global unicast address.**	10	L3	4	2	2.6.4

Three Levels of Hierarchy



Global Unicast Address

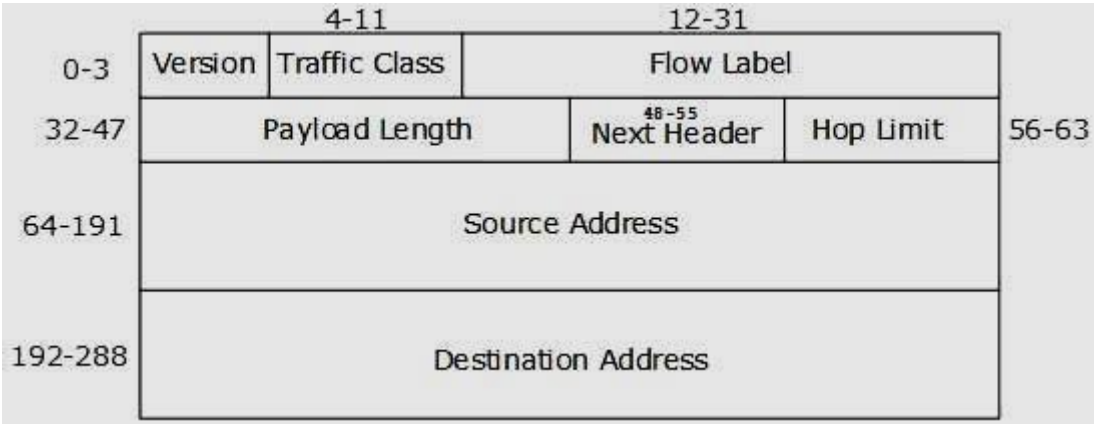
Block Assignment	Length of block
Global routing prefix (n)	48 bits
Subnet Identifier (128-n-m)	16 bits
Interface Identifier	64 bits

Recommended length for each block in Global unicast address

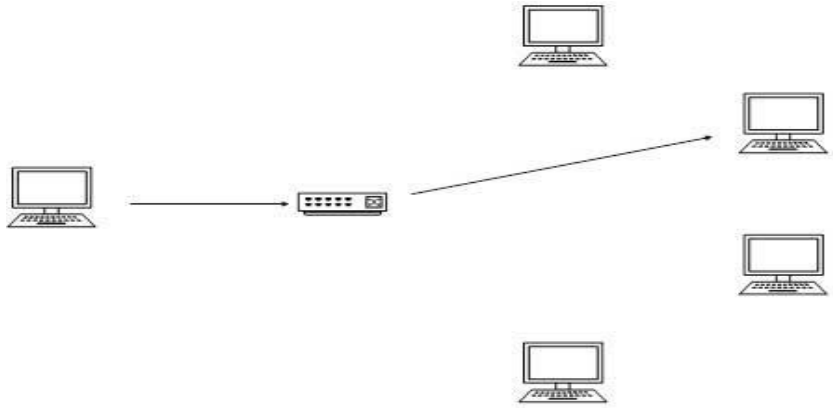
Global Routing Prefix :
The first 48 bits of a global unicast address are called global routing prefix.
They are used to route the packet through the Internet to the organization site such as ISP that owns the block.
The first three bits in this part is fixed (001), Remaining 45 bits can defined up to 245 sites
The global routers in the Internet route a packet to its destination site based on the value of n.

Subnet Identifier :
16 bit block is used to identify the specific subnet of an organization.
An organization can have upto 2^{16} subnets.

Interface Identifier :
Last 64 bits refers to the interface identifier. It is similar to the hostId in IPV4 scheme.
In IPV4 addressing, there is no relation between the hostid (32 bits) and MAC(48 bits) due to the difference in length.
Physical address whose length is less than 64 bits can be embedded as the whole or part of the interface

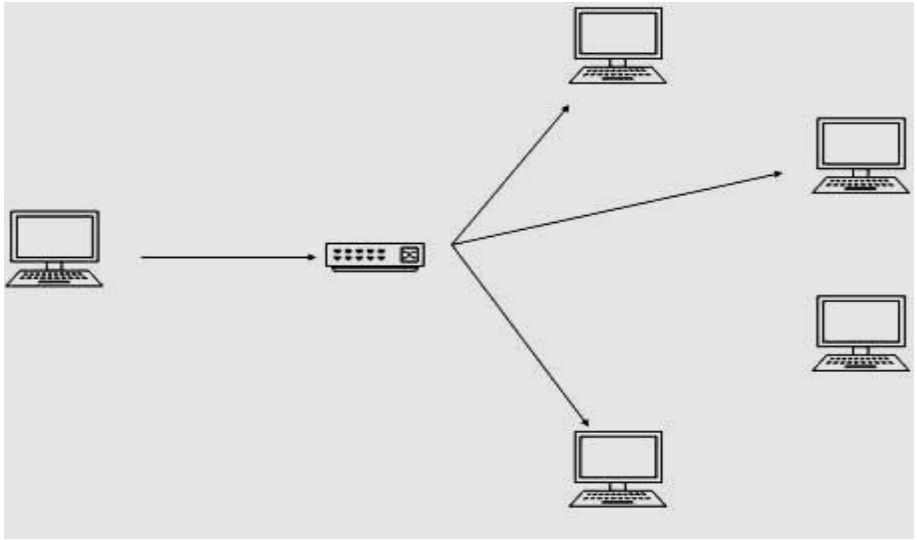
	identifier, eliminating the mapping process with the help of IPv6. Two common physical addressing scheme can be considered for this purpose: the 64-bit extended unique identifier (EUI-64) defined by IEEE and the 48-bit physical address defined by Ethernet.					
12. A)	**Illustrate the base header format of IPv6 datagram.**  IPv6 fixed header is 40 bytes long and contains the following information. **S.N.** | **Field & Description** 1 | **Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110. 2 | **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used	10	L3	4	2	2.6.1

		for Explicit Congestion Notification (ECN).						
	3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.						
	4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.						
	5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.						
	6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.						
	7	**Source Address** (128-bits): This field indicates the address of originator of the packet.						

	8 **Destination Address** (128-bits): This field provides the address of intended recipient of the packet. **(OR)**					
12. B)	**Interpret the various addressing modes of IPV6 with neat sketches.** IPv6 offers several types of modes by which a single host can be addressed. More than one host can be addressed at once or the host at the closest distance can be addressed. **Unicast** In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment.When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host. 	10	L3	4	2	2.6.4

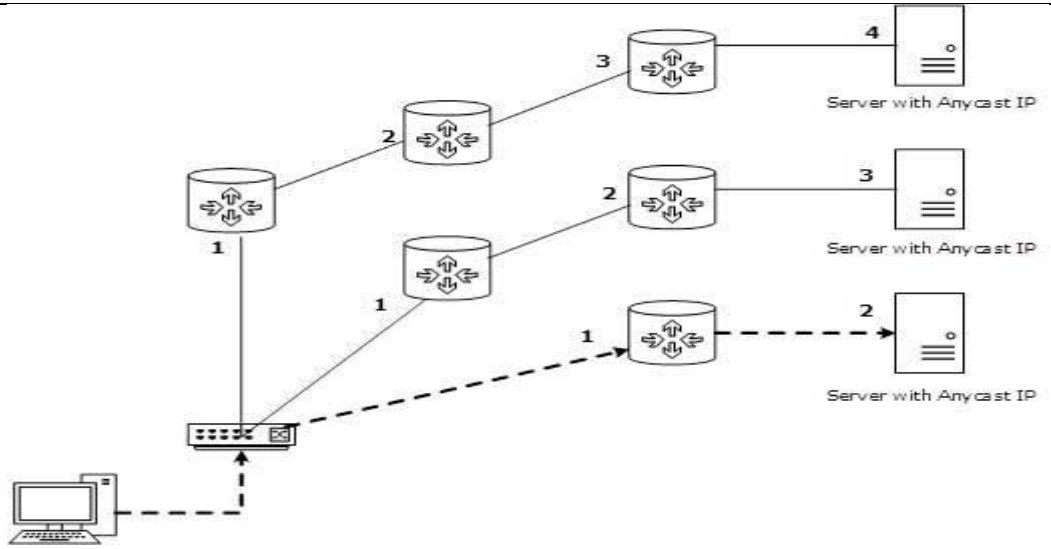
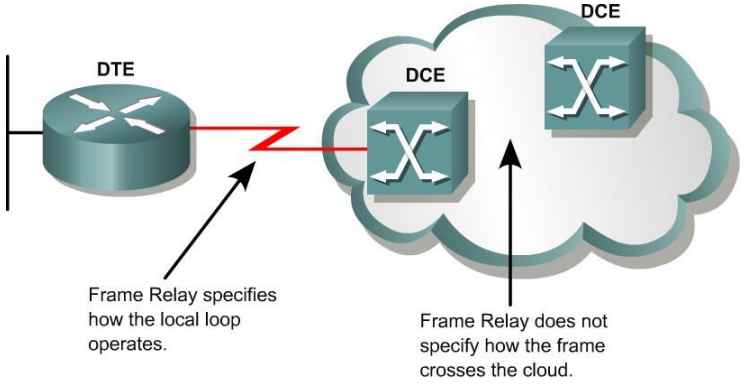
Multicast

The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All the hosts interested in that multicast information, need to join that multicast group first. All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.

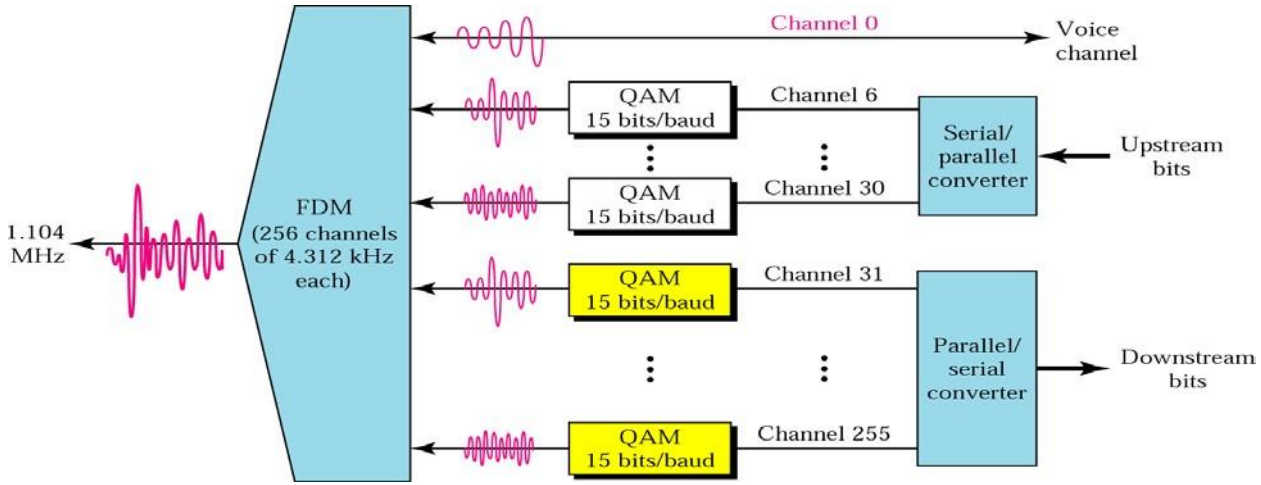


Anycast

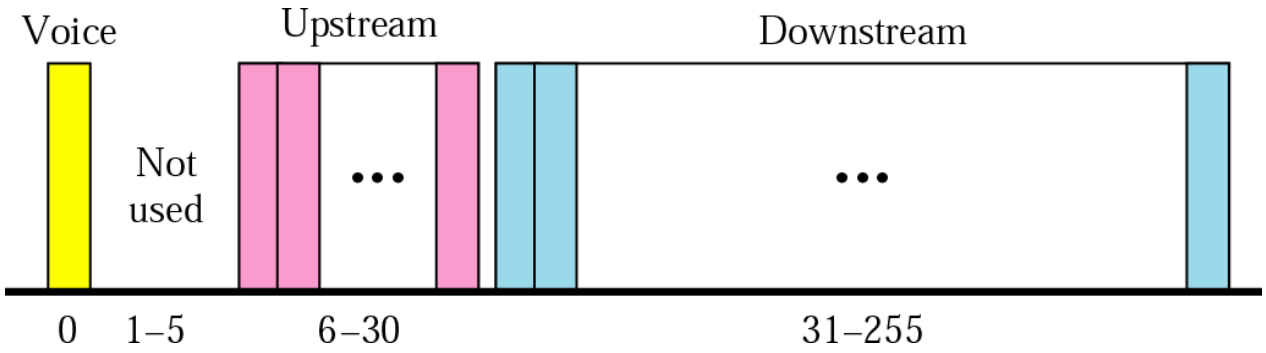
IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.

						
13. A)	**Frame relay architecture and Frame Call Control.**  ● **Frame Relay** is a packet-switched, connection-oriented, WAN service. ● It operates at the data link layer of the OSI reference model.	6+4	L3	5	2	2.6.1

	● Frame Relay uses a subset of the high-level data link control (HDLC) protocol called Link Access Procedure for Frame Relay (LAPF). ● Frames carry data between user devices called data terminal equipment (DTE), and the data communications equipment (DCE) at the edge of the WAN. ● Frame Relay does not have the sequencing, windowing, and retransmission mechanisms that are used by X.25. ● Without the overhead, the streamlined operation of Frame Relay outperforms X.25. ● Typical speeds range from 1.5 Mbps to 12 Mbps, although higher speeds are possible. (Up to 45 Mbps) ● The network providing the Frame Relay service can be either a carrier-provided public network or a privately owned network. ● Because it was designed to operate on high-quality digital lines, Frame Relay provides no error recovery mechanism. ● If there is an error in a frame it is discarded without notification. ● A Frame Relay network may be privately owned, but it is more commonly provided as a service by a public carrier. ● It typically consists of many geographically scattered Frame Relay switches interconnected by trunk lines. ● Frame Relay is often used to interconnect LANs. When this is the case, a router on each LAN will be the DTE. ● **Access Circuit** - A serial connection, such as a T1/E1 leased line, will connect the router to a Frame Relay switch of the carrier at the nearest point-of-presence for the carrier. ● DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of the customer. ● The customer may also own this equipment. ● Examples of **DTE** devices are routers and Frame Relay Access Devices (FRADs). ● A FRAD is a specialized device designed to provide a connection between a LAN and a Frame Relay WAN. ● **DCEs** are carrier-owned internetworking devices. ● The purpose of DCE equipment is to provide clocking and switching services in a network.					

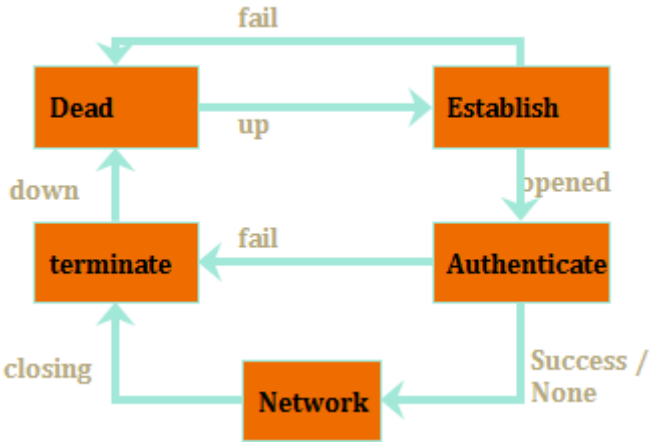
	● In most cases, these are packet switches, which are the devices that actually transmit data through the WAN. ● The connection between the customer and the service provider is known as the **User-to-Network Interface (UNI).** ● The **Network-to-Network Interface (NNI)** is used to describe how Frame Relay networks from different providers connect to each other. **(OR)**					
13. B)	**(i) DSL uses a modulation technique called DMT. Find some information about this modulation technique and how it can be used in DSL**. Modulation technique that has become standard for ADSL is called the discrete multi tone technique (DMT)  ● Voice : channel 0 is reserved for voice	5 5	L3	5	2	2.6.4

- Idle : channel 1 to 5 are not used; gap between voice and data communicaiton
- Upstream data and control : channels 6 to 30 (25channels); one channel for control
- Downstream data and control : channels 31 to 255(225 channels); 13.4 Mbps; one channel for control



(ii) PPP goes through different phases, which can be shown in a transition state diagram. Find the transition diagram for PPP connection.

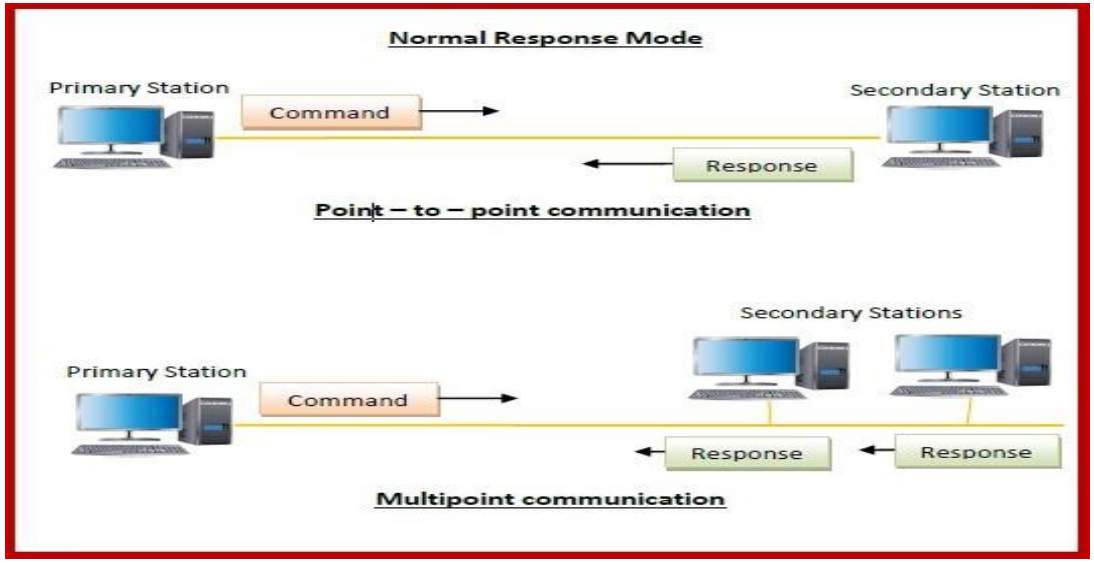
The telephone line or cable companies provide a physical link, but to control and manage the transfer of data, there is a need for a special protocol. The **Point-to-Point Protocol (PPP**) was designed to respond to this need.

	 **PPP STATES** • Dead • Establish • Authenticate • Network • terminate 1. DEAD:It means that the link is not being used . 2. ESTBLISHING:-When one of the end machine starts the communication, the connection goes into the establishing state. 3. AUTHENATICATING:-The user sends the authenticate request packet & includes the user name & password. 4.NETWORKING:-The exchange of user control and data packets can started. 5.TERMINATING:-The users sends the terminate the link. With the reception of the terminate.					
14. A)	**Explain the operation of the HDLC protocol and its frames with neat sketches.** High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.	10	L2	6	2	2.6.4

Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **Normal Response Mode (NRM)** − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



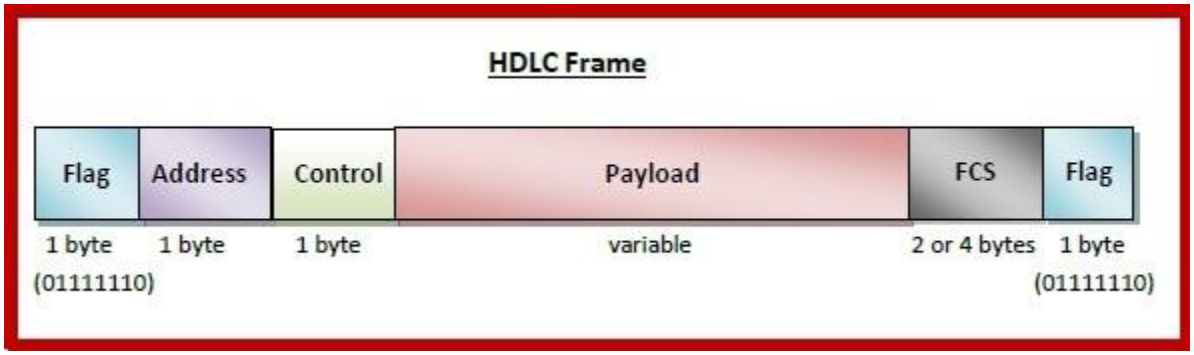
Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.

HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies

according to the type of frame. The fields of a HDLC frame are −

- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

- **I-frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.

	• **S-frame** − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10. • **U-frame** − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11. **(OR)**					
14. B)	**Sketch and discuss in detail about the ATM protocol architecture.** ATM is a connection-oriented network at a point where the sender or user which access devices are known as end-point, these end-points connected through a user to network interface (UNI) to the switches on the network, these switches provide a network to network interface (NNI). The architecture of the ATM is shown in the figure	10	L3	6	2	2.6.4

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

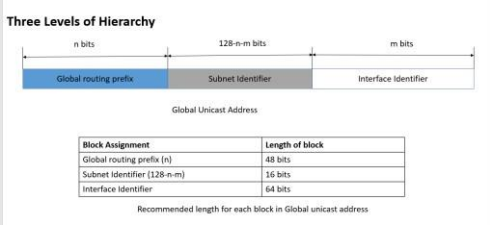
Set - C

Academic Year: 2022-23 (ODD) **Test: CLA-T3** **Year & Sem: III** Year / VI Sem
Date: - **Max. Marks:** 50 **Duration: 1 Hour 40 min**
Course Code & Title: 18CSC302J & COMPUTER NETWORKS

Course Articulation Matrix: ***(to be placed)***

CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO1 1	PO1 2
CO 4	M	H	-	H	L	-	-	-	M	L	-	H
CO 5	H	H	-	H	L	-	-	-	M	L	-	H
CO 6	L	H	-	H	L	-	-	-	L	L	-	H

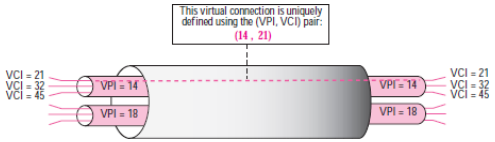
Part – A Instructions: Answer all the questions						**(1 x 10 = 10 Marks)**
Q. No	**Question**	**Marks**	**BL**	**CO**	**PO**	**PI Code**
1	**Select the correct statement when describing a global unicast address?** a) Packets addressed to a unicast address are delivered to a single interface b) These are like private addresses in IPV4 in that they are not meant to be routed c) These are typical publicly routable addresses, just like routable address in IPv4. d) These addresses are meant for non-routing purposes, but they are almost globally unique so it is unlikely that they will have an address overlap. **Ans-C**	1	L2	4	1	1.6.1
2	**1. Which statements about IPv4 and IPv6 addresses are true?** a) An IPv4 address is 32 bits long, represented in hexadecimal. b) An IPv6 address is 128 bits long, represented in hexadecimal. c) An IPv4 address is 32 bits long, represented in decimal. d) An IPv6 address is 128 bits long, represented in decimal. **Ans-B &C**	1	L 1	4	1	1.6.1
3	**2. Which among the following features is present in IPv6 but not in IPv4?** a) Fragmentation b) Header checksum c) Options d) Auto configuration **Ans-D**	1	L 1	4	1	1.6.1
4	**3. In IPv6 header, the base header can be followed by up to_____extension headers.** a)4 b)8 c)6 d)7 **Ans: B**	1	L 2	4	1	1.6.1
5	Suppose two IPv6 host want to interoperate using IPv6 datagrams, but they are connected to each other by intervening IPv4 routers._____is used as a medium to communicate the transit network with these different IP versions. a) Dual stack b) Tunneling c) Conversion d) Translation **Answer: B**	1	L 2	4	1	1.6.1
6	1. A_____is an extension of an enterprise's private intranet across a public	1	L 2	6	1	1.6.1

	network such as the internet, creating a secure private connection. a) VNP b) VPN c) VSN d) VSPN **Ans: b**					
7	The PPP encapsulation _____ a) Provides for multiplexing of different network-layer protocols b) Requires framing to indicate the beginning and end of the encapsulation c) Establishing, configuring and testing the data-link connection d) Provides interface for handling the capabilities of the connection/link on the network **Ans-A**	1	L 1	5,6	1	1.6.1
8	In point to point Protocol the framing techniques done according to the a) Bit Oriented Protocol b) Byte Oriented Protocol c) High-level Data link Protocol d) link Control Protocol **Ans-B**	1	L 2	5,6	1	1.6.1
9	Which Layer does MPLS Work on? (a) It functions in layer 2 **(b) It functions between layers 2 and 3** (c) It functions between layers 1 and 2 (d) It functions in layer 3 **Ans-B**	1	L 1	5, 6	1	1.6.1
10	1. How many fields frame in High-level Data Link Control (HDLC) may contain (a) Three field (b) Four fields (c) Five fields **(d) Six fields** **Ans-d**	1	L 1	6	1	1.6.1
Part – B	**Instructions: Answer any 4 Questions**			**Marks)**		**(10 x 4 = 40**
11. a)	Draw and explain the three levels of hierarchy of global unicast address. (10 marks) Primary used to address the System for one-one Communication mechanism i.e host to host direct communication over the internet. Global unicast address is equivalent to public IPV4 address Global unicast address objective is to reach any host globally across the internet uniquely Address block refer this is called global unicast address block CIDR Notation for the block is 2000::/3, where 3 refers to that 3 leftmost bit is common for all address in this block (001) The size of the address space is 2^{125} which is more than for expansion of internet in many years  **Global Routing Prefix :**	10	L 3	4	2	2.6.1

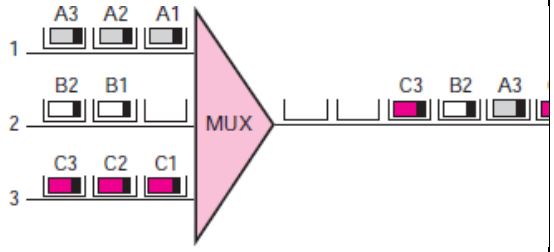
	The first 48 bits of a global unicast address are called global routing prefix. They are used to route the packet through the Internet to the organization site such as ISP that owns the block. The first three bits in this part is fixed (001), Remaining 45 bits can defined up to 245 sites The global routers in the Internet route a packet to its destination site based on the value of n. **Subnet Identifier :** 16 bit block is used to identify the specific subnet of an organization. An organization can have upto 2^{16} subnets. **Interface Identifier :** Last 64 bits refers to the interface identifier. It is similar to the hostId in IPV4 scheme. In IPV4 addressing, there is no relation between the hostid (32 bits) and MAC(48 bits) due to the difference in length. Physical address whose length is less than 64 bits can be embedded as the whole or part of the interface identifier, eliminating the mapping process with the help of IPv6. . Two common physical addressing scheme can be considered for this purpose: the 64-bit extended unique identifier (EUI-64) defined by IEEE and the 48-bit physical address defined by Ethernet. **OR**					
11. b)	i) Consider a host with Ethernet address (F5-A9-23-11-9B-E3) has joined the network. What would be its global unicast address if the global unicast prefix of the organization is 3A21:1216:2165 and the subnet identifier is A245:1232.(5 marks) Soln: Step 1 : Creating a local link address by adding 10 bit prefix (1111 1110 10) and 54 zeros and append its 64 bit interface ID extracted from the Ethernet address : FE80 : :F7A9-23FF-FE11-9BE3(by inverting the seventh bit of 1st octet and adding FFFE after the third octet) Step 2 : On assuming this uniqueness it send the router solicitation message upon receiving the advertisement message it complete the auto configuration process by extracting the global unicast prefix and subnet identifier from the message as follows 3A21:1216:2165:A245:1232 and append it to the local link address **3A21:1216:2165:A245:1232: F7A9-23FF-FE11-9BE3** ii) Explain IPv6 auto configuration. (5 marks) **Auto Configuration process:** a. Host create a link local address by taking 10 bit local prefix (1111 1110 10) and add 54 zeros and adding 64 bits interface identifier of its own from the interface card which makes as 128 bit link local address. b. The host verifies the uniqueness of the link local address by sending the neighbour	5+5	L 4	4	2	2.6.4

	solicitation message and waits for the neighbour advertisement message. Incase if any of the host address matches then auto configuration process results in failure which can be counter by either DHCP or manual configuration c. If the uniqueness test for link local address is successful, then the host send router solicitation message to the local router. If the local router running in the network sends a router advertisement message from which thee host extract the global unicast prefix and the subnet prefix and append the same with local link to complete the address. Incase if the router cant help for auto configuration it inform the host by setting the flag in the advertisement message.					
12. a)	i) Show the abbreviations for the following addresses: (4 marks) a) 0000:0000:FFFF:0000:0000:0000:0000:0000 b) 1234:2346:0000:0000:0000:0000:0000:1111 c) 0000:0001:0000:0000:0000:0000:1200:1000 d) 0000:0000:0000:0000:0000:FFFF:24.123.12.6 **Solution** a. 0:0:FFFF:: b. 1234:2346::1111 c. 0:1::1200:1000 d. ::FFFF:24.123.12.6	+6	L 4	4	2	2.6.1

	ii) Demonstrate the three-level hierarchy of global unicast address. (6 marks) **OR**					
12. b)	Elaborate in brief about IPv6 routing protocols that enable routers to exchange information about connected networks. (Any 3 protocols) **Neighbor Discovery Protocol** **IPv6 nodes which share the same physical medium (link) use Neighbor Discovery Protocol (NDP) to:** ▪ **Discover their mutual presence** ▪ **Determine link-layer addresses of their neighbors (equivalent to ARP)** ▪ **Find routers** ▪ **Maintain neighbors' reachability information**	10	L 3	4	2	2.6.4
13. a)	ATM creates a fixed route between two points data usage. ATM Switching techniques creates fixed route between the data points before the communication begins and it uses TDM technique to transmit the data. Explain how the connections are established to transmit the data Virtual Connection Connection between two end points is accomplished through transmission paths (TPs), virtual paths (VPs), and virtual circuits (VCs). A transmission path (TP) is the physical connection (wire, cable, satellite, and so on) between	6+4	L 4	6	2	2.6.1

	an end point and a switch or between two switches. Think of two switches as two cities. A transmission path is the set of all highways that directly connects the two cities. A transmission path is divided into several virtual paths. A virtual path (VP) provides a connection or a set of connections between two switches. Think of a virtual path as a highway that connects two cities. Each highway is a virtual path; the set of all highways is the transmission path. Cell networks are based on virtual circuits (VCs). All cells belonging to a single message follow the same virtual circuit and remain in their original order until they reach their destination.  The figure also shows the relationship between a transmission path (a physical					

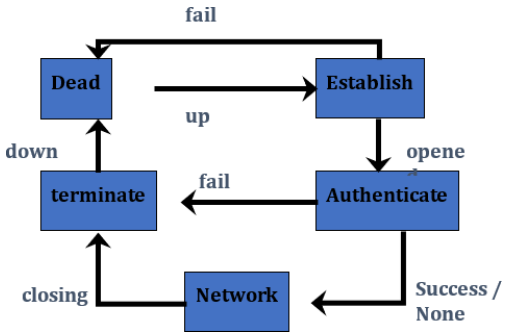
	connection), virtual paths (a combination of virtual circuits that are bundled together because parts of their paths are the same), and virtual circuits that logically connect two points together. In a virtual circuit network, to route data from one end point to another, the virtual connections need to be identified. For this purpose, the designers of ATM created a hierarchical identifier with two levels: a virtual path identifier (VPI) and a virtual circuit identifier (VCI). The VPI defines the specific VP and the VCI defines a particular VC inside the VP. The VPI is the same for all virtual connections that are bundled (logically) into one VP.					
13. b)	Using TDM, each user is assigned a fixed time slot , and no other station can send in that time. Is a station has nothing to transmit when its time slot comes up, the time slot is sent empty and wated. Explain how the empty time slots are handled by ATM efficiently. ATM uses asynchronous time-division multiplexing—that is why it is called	10	L 3	5,6	2	2.6.4

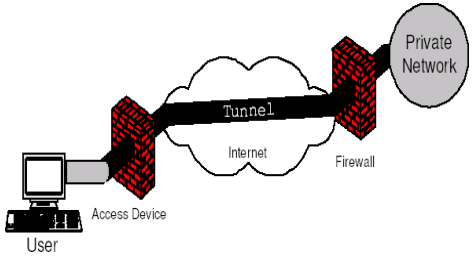
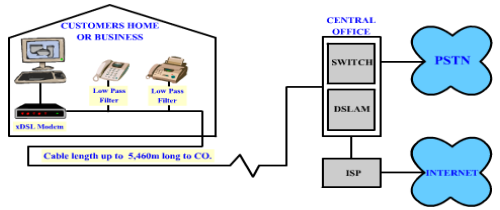
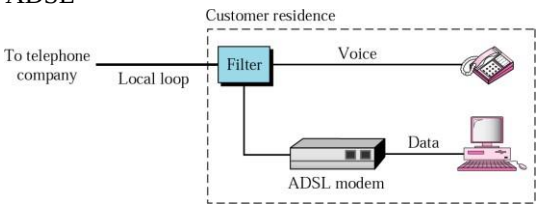
	Asynchronous Transfer Mode—to multiplex cells coming from different channels. It uses fixed-size slots the size of a cell. ATM multiplexers fill a slot with a cell from any input channel that has a cell; the slot is empty if none of the channels has a cell to send. The following figure shows how cells from three inputs are multiplexed. At the first tick of the clock, channel 2 has no cell (empty input slot), so the multiplexer fills the slot with a cell from the third channel. When all the cells from all the channels are multiplexed, the output slots are empty. 					

	information identifuing the source of the transmission contained in the header of each ATM cell.					
14. a)	I am with problems on the my connection PPP. I created static router, the communication between routers is established, I obtain connection to IP of the LAN port on the routers, my problem is that I do not obtain connection the stations of the side of the LAN, only until the IP of the port LAN of routers. What it is necessary so that the communication continues until its final destination? **Answer** If you can reach the LAN of the remote router and the remote router can reach your LAN, then routing is functioning correctly. If the workstations at either LAN can't ping each other, then make sure the default gateway of the workstations is pointing to their respective LAN IP of the local router. **PPP** The telephone line or cable companies provide a physical link, but to control and manage the transfer of data,	10	L 3	6	2	2.6.4

	there is a need for a special protocol. The **Point-to-Point Protocol (PPP**) was designed to respond to this need. **PPP** is comprised of three main components: A method for encapsulating multi-**protocol** datagrams. A Link Control **Protocol** (LCP) for establishing, configuring, and testing the data-link connection. A family of **Network** Control **Protocols** (NCPs) for establishing and configuring different **network**-layer **protocols**) Support multiple network protocols Link configuration Error detection Establishing network addresses Authentication Extensibility PPP relies on another DLP – **HDLC** – to perform some basic operations After the initial handshake, PPP executes its own handshake PPP itself consists of two protocols:					

	LCP – Link Control Protocol **NCP** – Network Control Protocol 1. DEAD:It means that the link is not being used . 2. ESTBLISHING:-When one of the end machine starts the communication, the connection goes into the establishing state. 3. AUTHENATICATING:-The user sends the authenticate request packet & includes the user name & password. 4. NETWORKING:-The exchange of user control and data packets can started. 5. TERMINATING:-The users sends the terminate the link. With the reception of					

	the terminate.  **Tunneling & PPP** Tunneling - definition The process of running one network protocol on top of another. Common use: VPN (Virtual Private Network) Tunneling method Extending the link between the HDLC driver and the rest of PPP over a separate network PPP tunneling protocols L2TP, L2F(**Layer 2 Forwarding)**, PPTP(Point-to-Point_Tunneling_Protocol) & ethernet (PPPoE)					

	 **OR**					
14. b)	Elaborate DSL and ADSL in detail. Answer DSL  ADSL  	10	L 4	6	2	2.6.4

***Program Indicators are available separately for Computer Science and Engineering in AICTE examination reforms policy.**
Course Outcome (CO) and Bloom's level (BL) Coverage in Questions

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Set - C

SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

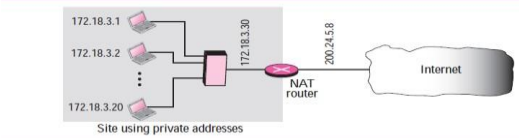
Set - D

Academic Year: 2022-23 (ODD) **Test: CLA-T3** **Year & Sem: III** Year / VI Sem
Date: - **Max. Marks:** 50 **Duration: 1 Hour 40 min**
Course Code & Title: 18CSC302J & COMPUTER NETWORKS

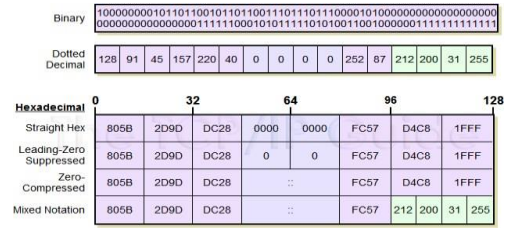
Course Articulation Matrix: ***(to be placed)***

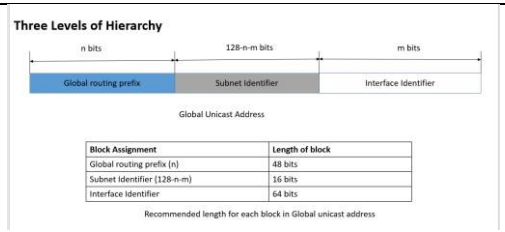
CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO12
CO 4	M	H	-	H	L	-	-	-	M	L	-	H
CO 5	H	H	-	H	L	-	-	-	M	L	-	H
CO 6	L	H	-	H	L	-	-	-	L	L	-	H

Part – A Instructions: Answer all the questions						**(1 x 10 = 10 Marks)**
Q. No	**Question**	**Marks**	**BL**	**CO**	**PO**	**PI Code**
1	In subcategories of reserved address in IPV6, address that is used by a host to test itself without going into network is called_____ a) Unspecified address **b) Loopback address** c) Compatible address d) Mapped address **Ans-B**	1	L 2	4	1	1.6.1
2	In contrast to IPV4, IPV6 uses_____times more bits to address a device on the internet. a) 3 b) **4** c) 5 d) 6 **Ans-b**	1	L 1	4	1	1.6.1
3	When the sender wants to use IPV6, but the receiver doesn't understand IPV6, Header translation uses_____address to translate an IPv6 address. A) IP B) Physical C) Mapped D) MAC **Answer: C) Mapped**	1	L 1	4	1	1.6.1
4	How IPV6 will communicate with multiple hosts? a) Broadcasting b) Unicasting **c) Multicasting** d) Anycasting **Ans-C**	1	L 2	4	1	1.6.1
5	The existing local loops with Asymmetric Digital Subscriber Line (ADSL) can handleband widths up to a) 1.1 Hz b) 1.1 kHz c) 1.1 MHz d) 1.1GHz **Ans: c**	1	L 2	4	1	1.6.1
6	1. An Asymmetric Digital Subscriber Line (ADSL) is not suitable for	1	L 2	6	1	1.6.1

	a) Games b) Businesses c) Residential users d) Downloading **Ans: b**					
7	A family of network control protocols (NCPs) _____ a) Are a series of independently defined protocols that provide a dynamic b) Are a series of independently-defined protocols that encapsulate c) Are a series of independently defined protocols that provide transparent d) The same as NFS **Ans-B**	1	L 1	5,6	1	1.6.1
8	A Link Control Protocol (LCP) is used for _____ a) Establishing, configuring and testing the data-link connection b) Establishing and configuring different network-layer protocols c) Testing the different network-layer protocols d) Provides for multiplexing of different network-layer protocols ANS-A	1	L 2	5,6	1	1.6.1
9	Choose the multiplexing techniques used by ATM a) Frequency Division Multiplexing b) Asynchronous Frequency Division Multiplexing c) Time Division Multiplexing	1	L 1	5, 6	1	1.6.1
	d) Asynchronous Time Division Multiplexing **Ans: d) Asynchronous Time Division Multiplexing**					
10	In ATM cell network, cells belongs to a single message ----- a) Follow different paths b) Follow same path c) Arrive out of order d) No flow control **Ans: b) Follow same path**	1	L 1	6	1	1.6.1
Part – B	**Instructions: Answer any 4 Questions**			**Marks)**		**(10 x 4 = 40**
11. a)	Explain about Implementation of Network Address Translation . **Figure 5.39** *NAT*  • Figure 5.39 shows a simple implementation of NAT. • The private network uses private addresses. The router that connects the network to the global address uses one private address and one global address. • The private network is transparent to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8. • Generally, the border router is configured for NAT i.e the router which has one interface in local (inside)	10	L 3	4	2	2.6.1

	network and one interface in the global (outside) network. • When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. • When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address. • If NAT run out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent. **OR**					
11. b)	Interpret the various addressing modes of IPV6 with neat sketches. • **128 bits (or 16 bytes) long:** four times as long as its predecessor. • **2^{128}** : about 340 billion billion billion billion different addresses • **Colon hexadecimal notation**: • addresses are written using 32 hexadecimal digits. • digits are arranged into 8 groups of four to improve the readability. • Groups are separated by colons **2001:0718:1c01:0016:020d:56ff:fe77:52a3** • Note: • DNS plays an important role in the IPv6 world	10	L 4	4	2	2.6.4

	• (manual typing of IPv6 addresses is not an easy thing, • Some **zero suppression rules** are allowed to lighten this task at least a little.  					
12. a)	Draw and explain the three levels of hierarchy of global unicast address. (10 marks) Primary used to address the System for one-one Communication mechanism i.e host to host direct communication over the internet. Global unicast address is equivalent to public IPV4 address Global unicast address objective is to reach any host globally across the internet uniquely Address block refer this is called global unicast address block CIDR Notation for the block is 2000::/3, where 3 refers to that 3 leftmost bit is common for all address in this block (001) The size of the address space is 2^{125} which is more than for expansion of internet in many years	4+6	L 4	4	2	2.6.1



Global Routing Prefix :

The first 48 bits of a global unicast address are called global routing prefix.

They are used to route the packet through the Internet to the organization site such as ISP that owns the block.

The first three bits in this part is fixed (001),

Remaining 45 bits can defined up to 245 sites

The global routers in the Internet route a packet to its destination site based on the value of n.

Subnet Identifier :

16 bit block is used to identify the specific subnet of an organization.

An organization can have upto 2^{16} subnets.

Interface Identifier :

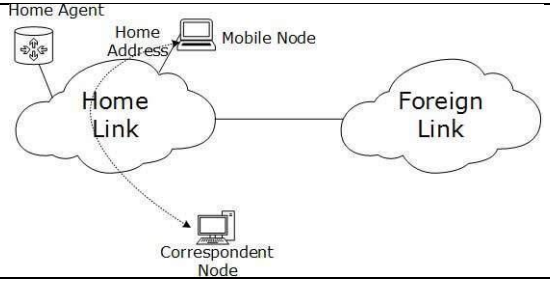
Last 64 bits refers to the interface identifier. It is similar to the hostId in IPV4 scheme.

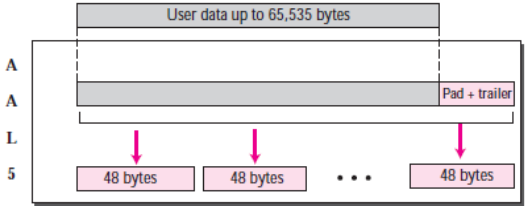
In IPV4 addressing, there is no relation between the hostid (32 bits) and MAC(48 bits) due to the difference in length.

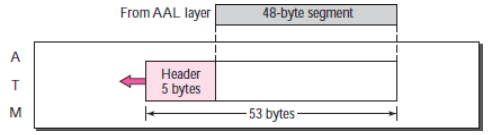
Physical address whose length is less than 64 bits can be embedded as the whole or part of the interface identifier, eliminating the mapping process with the help of IPv6.

. Two common physical addressing scheme can be considered for this purpose: the 64-bit extended unique identifier (EUI-64) defined by IEEE and the 48-bit physical address defined by Ethernet.

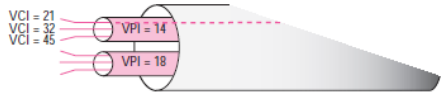
	OR					
12. b)	Explain IPV6 Mobility in detail. • When a host is connected to a link or network, it acquires an IP address and all communication take place using that IP address on that link. As soon as, the same host changes its physical location, that is, moves into another area / subnet / network / link, its IP address changes accordingly, and all the communication taking place on the host using old IP address, goes down. IPv6 mobility provides a mechanism for the host to roam around different links without losing any communication/connection and its IP address • Mobile Node: The device that needs IPv6 mobility. • Home Link: This link is configured with the home subnet prefix and this is where the Mobile IPv6 device gets its Home Address. • Home Address: This is the address which the Mobile Node acquires from the Home Link. This is the permanent address of the Mobile Node. If the Mobile Node remains in the same Home Link, the communication among various entities take place as usual. • Home Agent: This is a router that acts as a registrar for Mobile Nodes. Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses, and their present IP addresses.	10	L 3	4	2	2.6.4

						
13. a)	The key feature of ATM is to transmit voice, videos and images simultaneously over a single or integrated corporate network with Higher transmission capability. Explain how the different traffic characteristic are handled by the ATM. **ATM Adaptation Layer (AAL) Types** In order for ATM to support a variety of services with different traffic characteristics and system requirements, it is necessary to adapt the different classes of applications to the ATM layer. This function is performed by the AAL, which is service-dependent. The application adaptation layer (AAL) allows existing networks (such as packet networks) to connect to ATM facilities. AAL protocols accept transmissions from upper-layer services (e.g., packet data) and map them into fixed-sized ATM cells. These transmissions can be of any type (voice, data, audio, video)	10	L 4	6	2	2.6.1

	and can be of variable or fixed rates. At the receiver, this process is reversed—segments are reassembled into their original formats and passed to the receiving service. Although four AAL layers have been defined the one which is of interest to us is AAL5, which is used to carry IP packets in the Internet. AAL5, which is sometimes called the simple and efficient adaptation layer (SEAL), assumes that all cells belonging to a single message travel sequentially and that control functions are included in the upper layers of the sending application.  AAL5 accepts an IP packet of no more than 65,535 bytes and adds an 8-byte trailer as well as any padding required to ensure that the position of the trailer falls where the					

	receiving equipment expects it (at the last 8 bytes of the last cell). Once the padding and trailer are in place, AAL5 passes the message in 48-byte segments to the ATM layer. **ATM Layer** The ATM layer provides routing, traffic management, switching, and multiplexing services. It processes outgoing traffic by accepting 48-byte segments from the AAL sublayer. The addition of a 5-byte header transforms the segment into a 53-byte cell  **OR**					
13. b)	ATM Switching techniques creates fixed route between the data points before the communication begins and it uses TDM technique to transmit the data. Explain how the connections are established to transmit the data Virtual Connection Connection between two end points is accomplished through	10	L 3	5,6	2	2.6.4

	transmission paths (TPs), virtual paths (VPs), and virtual circuits (VCs). A transmission path (TP) is the physical connection (wire, cable, satellite, and so on) between an end point and a switch or between two switches. Think of two switches as two cities. A transmission path is the set of all highways that directly connects the two cities. A transmission path is divided into several virtual paths. A virtual path (VP) provides a connection or a set of connections between two switches. Think of a virtual path as a highway that connects two cities. Each highway is a virtual path; the set of all highways is the transmission path. Cell networks are based on virtual circuits (VCs). All cells belonging to a single message follow the same virtual circuit and remain in their original order until they reach their destination.					

	 The figure also shows the relationship between a transmission path (a physical connection), virtual paths (a combination of virtual circuits that are bundled together because parts of their paths are the same), and virtual circuits that logically connect two points together. In a virtual circuit network, to route data from one end point to another, the virtual connections need to be identified. For this purpose, the designers of ATM created a hierarchical identifier with two levels: a virtual path identifier (VPI) and a virtual circuit identifier (VCI). The VPI defines the specific VP and the VCI defines a particular VC inside the VP. The VPI is the same for all virtual connections that are bundled (logically) into one VP.					

14. a)	Explain how VPN is designed to securely connect two geographically-distributed sites. ● VPN is a network that is private but virtual. ● It is private because it guarantees privacy inside the organization. ● It is virtual because it does not use real private WANs; the network is physically public but virtually private. Routers R1 and R2 use VPN technology to guarantee privacy for the organization.  **OR**	10	L 3	6	2	2.6.4
14. b)	MPLS Operations • MPLS - Multi Protocol Label Switching • A protocol to establish an end-to-end path from source to the destination. • To setup this path basically using labels - Require a protocol to set up the labels along the path. It builds the connection oriented service on the IP network • MPLS is an efficient encapsulation mechanism • A hop-by-hop forwarding mechanism • MPLS packets can run on other layer 2 technologies such as ATM, PPP, POS, FR, Ethernet • Labels can be used as designators	10	L 4	6	2	2.6.4

	- example: IP prefixes, ATM VC, or a bandwidth guaranteed path. • This technique designed to speed up and shape traffic flows across enterprise wide area and service provider networks.