Computer Networks ct1

Computer Networks (SRM Institute of Science and Technology)

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

SET - A

DEPARTMENT OF DATA SCIENCE & BUSINESS SYSTEMS

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Academic Year: 2023 - 2024 (ODD)

Test: CLA - T1 | **Date: 08-08-2023**
Course Code & Title: 18CSC302J – Computer Networks | **Duration:** 50 Minutes
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	3	-	-	-	-	-	-	-	-	-	-	-
2	CO2	-	-	3	-	1	-	-	-	-	-	-	-

Part - A
(10 x 1 = 10 Marks)

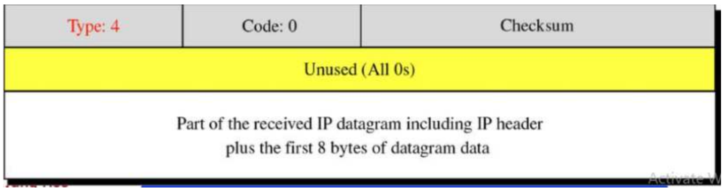
Instructions: Answer all

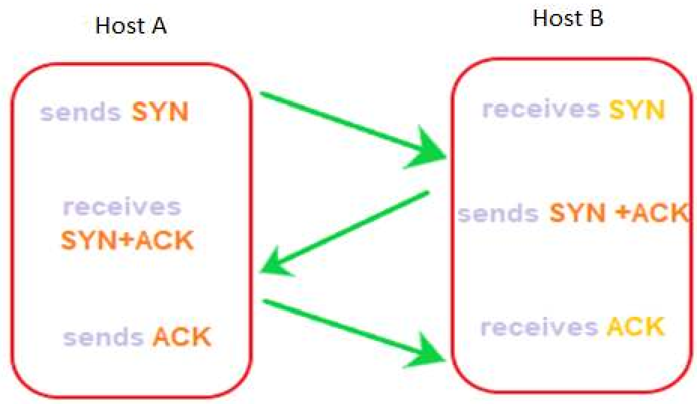
Q. No	Answer with choice variable	Marks	BL	CO	PO	PI Code
1	A host is connected to a Department network which is part of a University network. The University network, in turn, is part of the Internet. The largest network in which the Ethernet address of the host is unique? **a) The subnet to which the host belongs.** **b) The Internet (Answer)** **c) The University Network** **d) The Department Network** **Solution:** Address used in ethernet is MAC address, also known as ethernet address. MAC address of 2 host in any network cannot be same, since MAC address assigned by manufacture in such a way that no two system has same MAC. So largest network will be internet, because MAC of two system always unique.	1	L1	1	1	1.6.1
2	Which one of the following fields of an IP header is **NOT** modified by a typical IP router? **a) Checksum** **b) Time to live (TTL)** **c) Source address (Answer)** **d) Length** **Solution:** Router can not change the source address of the packet, rest of the fields can be changed.	1	L1	1	1	1.6.1
3	Consider the following Two statements. S1: Destination MAC address of an ARP reply is a broadcast address.	1	L1	1	1	1.6.1

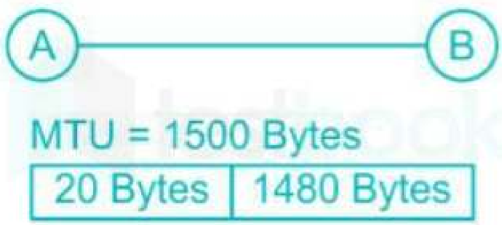
	S2: Destination MAC address of an ARP request is a broadcast address. Which of the choices are correct? **a) Both S1 and S2 are true** **b) Both S1 and S2 are false** **c) S1 is true and S2 is false** **d) S1 is false and S2 is true (Answer)** **Solution:** ARP request message is always broadcast and ARP reply message is unicast.					
4	Which of these is NOT a type of error-reporting message? **a) Destination unreachable** **b) Source quench** **c) Router error (Answer)** **d) Time exceeded** **Solution:** Router Error is not a type of error-reporting message in ICMP.	1	L1	1	1	1.6.1
5	Packets of the same session may be routed through different paths in **a) TCP, but not UDP** **b) TCP and UDP (Answer)** **c) UDP, but not TCP** **d) Neither TCP, Nor UDP** **Solution:** They are both protocols of Transport layer. Same session packets can be routed by different routes. The static routing is not used by most networks.	1	L1	1	1	1.6.1
6	Select the maximum size of data that the application layer can pass on to the TCP layer. **a) Any size (Answer)** **b) 2^{16} bytes** **c) 1500 bytes** **d) 2^{16} bytes – TCP header size** **Solution:** There is no restriction for application layer, so it can pass any size of data to the transport layer.	1	L1	1	1	1.6.1
7	**Match the following.** Field — Length in bits P. UDP Header's Port Number — I. 48 Q. Ethernet MAC Address — II. 8 R. IPv6 Next Header — III. 32 S. TCP Header's Sequence Number — IV. 16 **a) P-III, Q-IV, R-II, S-I** **b) P-II, Q-I, R-IV, S-III**	1	L2	2	3	3.1.5

	c) P-IV, Q-I, R-II, S-III (Answer) d) P-IV, Q-I, R-III, S-II **Solution:** UDP Header's Port number is **16** bits, MAC is 48 bits, IPv6 is 8 bits and TCP seq is 32 bits.					
8	Identify the correct order in which a server process must invoke the function calls accept, bind, listen, and recv according to UNIX socket programming. **a) Accept, bind, listen, recv** **b) Bind, listen, accept, recv (Answer)** **c) Listen, bind, accept, recv** **d) Accept, listen, bind, recv** **Solution:** bind, listen, accept and recv are the correct order of **server side** socket API functions.	1	L2	2	3	3.1.5
9	In a simple echo-request message, the value of the sum is 01010000 01011100. Then, value of checksum is ____________ **a) 10101111 10100011 (Answer)** **b) 01010000 01011100** **c) 10101111 01011100** **d) 10010000 10100011** **Solution:** Checksum is 1's complement of the sum	1	L1	2	3	3.1.5
10	The router forwards the received packet through many of its interfaces in **a) Unicasting (Answer)** **b) Multicasting (Answer)** **c) Broadcasting** **d) Multiple unicasting** **Solution:** The router receives packets from each interface via a network interface and forwards to many interfaces in multicasting.	1	L1	1	1	1.6.1

Part – B **(3 x 5 = 15 Marks)** **Instructions: Answer any 3 Questions**						
11	**An IP packet has arrived in which the offset value is 50, the value of HLEN is 10 and the value of the total length field is 200. What is the number of the first byte and the last byte? Is this the first fragment or intermediate fragment?**	5	L3	1	1	1.6.1

	ANSWER: **Given Data**: Fragment offset = 50 HLEN = 10 Total length field = 200 **Calculation**: Header length = 10 * 4 = 40 bytes Payload size = 200 – 40 = 160 bytes Fragment offset = 50 Hence, bytes ahead of this fragment = 50 * 8 = 400 **Total bytes in this datagram = 160 byte** If the first byte is 400, last byte will be = 400 + 160 - 1 **Last byte = 559** **This is not the first fragment because the offset value for the first fragment is always 00 (all 0's). So, this can be an intermediate or last fragment.**					
12	• **Draw the ICMP header with proper values for "Source quench" type error reporting.** • **Discuss about ICMP debugging tools.** **ANSWER:** **ICMP header for "Source Quench"**  **ICMP debugging tools** **Two tools that use ICMP for debugging: ping and traceroute** **Ping (1.5 Marks)** • **The ping program to find if a host is alive and responding.** • **Command : ping the ip of the host.(ping 152.18.1.3)** • **The source host sends ICMP echo request messages (type: 8, code: 0);** • **The destination, if alive, responds with ICMP echo reply messages.** • **Starts the sequence number from 0; this number is incremented by one each time a** • **new message is sent.** • **ping can calculate the round-trip time.** • **Inserts the sending time in the data section of**	2 3	L2	1	1	1.6.1

	the message. • **When packet arrives it subtracts the arrival time from the departure time to get the Round-Trip Time (RTT).** • **The TTL (time to live) field is encapsulates an ICMP message as 62, which means the** • **packet cannot travel more than 62 hops** **TRACE ROUTE** **(1.5 Marks)** • **The traceroute program in UNIX or tracert in Windows.** • **It is used to route the packets from source to destination.** • **The traceroute program find the address of router R & RTT between host A and router R.**					
13	**Assume host A wants to communicate with host B through Connection oriented protocol. Draw the timeline that shows the connection establishment steps and explain why we need those steps?** **ANSWER:** TCP is a connection-oriented protocol and every connection-oriented protocol needs to establish a connection in order to reserve resources at both the communicating ends. **Connection Establishment –**  Step 1: SYN • SYN is a segment sent by the host A to the host B. • It acts as a connection request between the A and B. It informs the host B that the host A 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.	5	L3	2	3	3.1.6

	Step 2: SYN-ACK • It is an SYN-ACK segment or an SYN + ACK segment sent by the host B. • The ACK segment informs the host A that the host B 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 host A and host B. • The ACK segment is sent by the host A as the response of the received ACK and SYN from the server. It results in the establishment of a reliable data connection. • After these three steps, the host A and host B are ready for the data communication process.					
14	**Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e., MTU = 1500 bytes) Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?** **ANSWER:**  User data = 8880 bytes UDP header size = 8 bytes	5	L3	2	3	3.1.6

	$\left.\begin{array}{r}\text{Total Size of input data}\\ \text{to Network Layer}\end{array}\right\} = 8880 + 8$ $= 8888$ bytes Number of fragments $= \left\lceil \frac{8888}{1480} \right\rceil = 6.005$ $= 7$ fragments $\left.\begin{array}{r}\text{Offset value of}\\ \text{last fragment}\end{array}\right\} = \frac{1480 \times 6}{8}$ $= 1110$ TCP or UDP will be added to the Data Unit received from Transport Layer to Network Layer. And fragmentation happens at Network Layer. So no need to add TCP or UDP header into each fragment.					

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

SET - B

DEPARTMENT OF DATA SCIENCE & BUSINESS SYSTEMS
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Academic Year: 2023 - 2024 (ODD)

Test: CLA - T1 **Date: 08-08-2023**
Course Code & Title: 18CSC302J – Computer Networks **Duration:** 50 Minutes
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	3	-	-	-	-	-	-	-	-	-	-	-

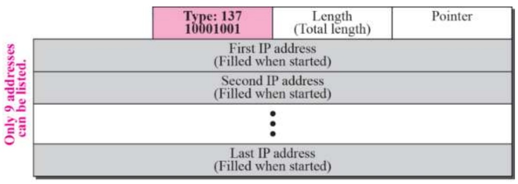
Part - A
(10 x 1 = 10 Marks)
Instructions: Answer all

Q. No	Answer with choice variable	Marks	BL	CO	PO	PI Code
1	Which field helps to check rearrangement of the fragments? **a) offset** **b) flag** **c) TTL** **d) identifer**	1	L1	1	1	1.6.1
2	Which of the following field in IPv4 datagram is not related to fragmentation? **a) Flags** **b) Offset** **c) TOS** **d) Identifier**	1	L1	1	1	1.6.1
3	__________ translates address consisting 32 bits into 48 bits. **a) FTP** **b) TCP** **c) RARP** **d) ARP**	1	L1	1	1	1.6.1
4	To determine whether or not a node is reachable, ________ message can be sent. **e) Echo-reply** **f) Echo-request** **g) Redirection** **h) Source-quench**	1	L1	1	1	1.6.1
5	What field uniquely identifies the kind of ICMP	1	L1	1	1	1.6.1

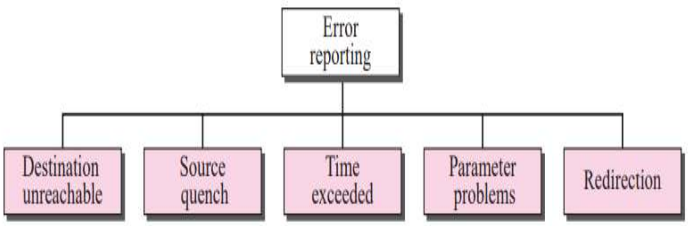
	message whether it is echo reply or echo request ? a) type b) Code c) Option d) Checksum					
6	Ping utility with the ______ option to implement the record route option. a) -R b) -G c) -g d) -rr	1	L1	1	1	1.6.1
7	**Formula for calculating Round-trip time.** a) Round -trip time = value of receive timestamp – value of original time stamp b) Round – trip time = time the packet returned – value of transmit timestamp c) Round-trip time = sending time + receiving time d) Round –trip time = receive timestamp – (original timestamp field + oneway time duration)	1	L2	1	1	1.6.1
8	Identify the wrong module in ARP package. e) Cache module f) Input module g) Resolution module h) Output module	1	L2	1	1	1.6.1
9	_____ bit is used to represent when unrecoverable errors happens or there is no chance of terminating the TCP connection normally. a) URG b) FIN c) RST d) PSH	1	L1	1	1	1.6.1
10	______ broadcasts packets, but creates loops in the systems. e) Forwarding f) Flooding g) Backwarding h) Multicasting	1	L1	1	1	1.6.1

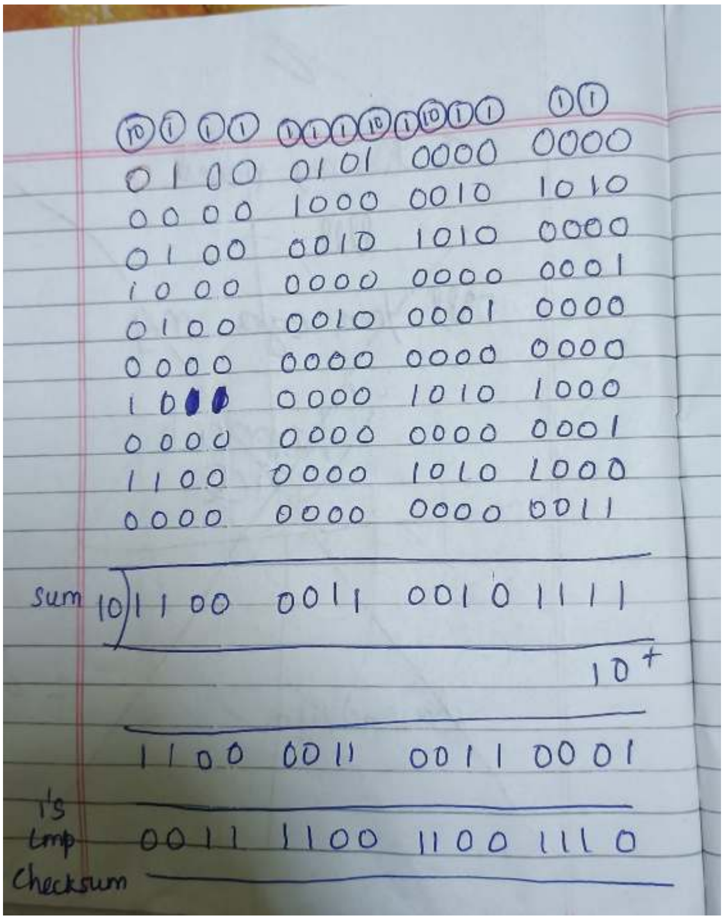
<table>
<tr><td colspan="7"><u>Part – B</u>
(3 x 5 = 15 Marks)
Instructions: Answer any 3 Questions</td></tr>
<tr><td>11</td><td>a) A packet has arrived in which the offset value is 200. What is the number of the first byte? Do we know the number of the last byte?

To find the number of the first byte, we multiply the offset value by 8. This means that the first byte number is 1600. We cannot determine the number of the last byte unless we know the length of the data.

b) Write briefly about Strict-source-routing
It is used by the source to predetermine a route for the datagram as it travels through the Internet.
Dictation of a route by the source can be useful for several purposes.
The sender can choose a route with a specific type of service, such as minimum delay or maximum throughput.
Alternatively, it may choose a route that is safer or more reliable for the sender’s purpose.

</td><td>2

3</td><td>L3</td><td>1</td><td>1</td><td>1.6.1</td></tr>
<tr><td>12</td><td>Describe about the ICMP error-reporting messages with explanation.

Explanation Each 1 marks

</td><td>5</td><td>L2</td><td>1</td><td>1</td><td>1.6.1</td></tr>
</table>

13	**Calculate the checksum for a sample IPv4 packet received like this:** **4500 082A 42A0 8001 4210 XXXX B0A8 0001 C0A8 0003** **Where xxxx is the checksum that needs to be sent with the packet.**  0100 0101 0000 0000 0000 1000 0010 1010 0100 0010 1010 0000 1000 0000 0000 0001 0100 0010 0001 0000 0000 0000 0000 0000 1000 0000 1010 1000 0000 0000 0000 0001 1100 0000 1010 1000 0000 0000 0000 0011 sum 10) 1100 0011 0010 1111 10+ 1100 0011 0011 0001 1's cmp 0011 1100 1100 1110 Checksum	5	L3	1	1	1.6.1

14	**Write short notes on TCP Congestion Avoidance Phase.**
	➢ **Congestion window and congestion policy handles TCP congestion**
	➢ ***Congestion Window***
	    ➢ **Client window size (rwnd) decided by the available buffer space of Server**
	    ➢ **Ignored entity in deciding window size : Network Congestion**
	    ➢ **Sender window size determined by,**
	        ➢ **rwnd (receiver advertised window size) &**
	cwnd (Congestion window size)
	
	➢ ***Congestion Policy***
	➢ **Three phases : Slow Start, Congestion avoidance & Congestion detection**
	I. Slow Start (Exponential Increase)
		5	L3	1	1	1.6.1

	- ***Assumption:*** **rwnd(Sender Window Size) > cwnd(Congestion Window Size)** - **cwnd initialized to one Maximum window size (MSS)** - **On arrival of each ACK, cwnd increases by 1** - **Algorithm starts slowly & grows exponentially** - **Delayed ACK policy is ignored** **ii.** ***Congestion Avoidance : Additive Increase*** - **Slow start increases congestion window size (cwnd) exponentially** - **Congestion avoidance increases cwnd additively** - **Additive phase begins when slow start reaches ssthresh i.e. cwnd = I** - **Increase in cwnd is based on RTT & not on number of ACK's.** **iii.** ***Congestion Detection : Multiplicative Decrease Contd…*** **a) Time-out increases possibility of congestion. TCP reacts as follows:** - **Ssthresh set to half the value of rwnd** - **Cwnd initialized to 1** - **Slow start phase is initiated again** **b) Three duplicate ACK's indicates a weaker possibility of Congestion. Also called as fast transmission & fast recovery. TCP reacts as follows:** - **Ssthresh set to half the value of rwnd**					

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

SET - C

DEPARTMENT OF DATA SCIENCE & BUSINESS SYSTEMS
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Academic Year: 2023 - 2024 (ODD)

Test: CLA - T1 **Date: 08-08-2023**
Course Code & Title: 18CSC302J – Computer Networks **Duration:** 50 Minutes
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	3	-	-	-	-	-	-	-	-	-	-	-

Part - A
(10 x 1 = 10 Marks)
Instructions: Answer all

Q. No	Answer with choice variable	Marks	BL	CO	PO	PI Code
1	The checksum in IP must be recomputed at every router because of change in ____ fields. a)TTL, Options, Identification Number, Offset **b)TTL, Options, Datagram Length, Offset** c) TTL, Options, Data, Offset d) TTL, Header Length, Offset, ToS	1	L1	1	1	1.6.1
2	The intermediate routers between source and destination need the following information in IP header- **a)Version** b) Protocol c) Identification Number d) Source IP Address	1	L1	1	1	1.6.1
3	When the source does not trust the routers to route properly or source wishes to make sure that the packet does not stray from specified path, what options can be used? a)Loose source routing b)Trace route **c)Strict source routing** d)Internet Time Stamp	1	L1	1	1	1.6.1
4	If the value available in “fragment offset” field of IP header is 100, then the number of bytes ahead of this fragment is ___ ? a)100 B b)400 B **c)800 B** d)200 B	1	L1	1	1	1.6.1

5	If the value in protocol field is 17, the transport layer protocol used is ______________ a) TCP **b) UDP** c) ICMP d) IGMP	1	L1	1	1	1.6.1
6	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
7	Which of these is not a type of error-reporting message? a) Destination unreachable b) Source quench **c) Router error** d) Time exceeded	1	L2	1	1	1.6.1
8	To achieve reliable transport in TCP, ____________ is used to check the safe and sound arrival of data. a) Packet b) Buffer c) Segment **d) Acknowledgment**	1	L2	1	1	1.6.1
9	What is the main advantage of UDP? a) More overload b) Reliable **c) Low overhead** d) Fast	1	L1	1	1	1.6.1
10	_________ is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer. a) TCP **b) UDP** c) IP d) ARP	1	L1	1	1	1.6.1

Part – B **(3 x 5 = 15 Marks)** **Instructions: Answer any 3 Questions**						
11	Suppose a router receives an IP packet containing 600 data bytes and has to forward the packet to a network with maximum transmission unit of 200 bytes. Assume that IP header is 20 bytes long. What are fragment offset values for divided packets? Draw the original	5	L3	1	1	1.6.1

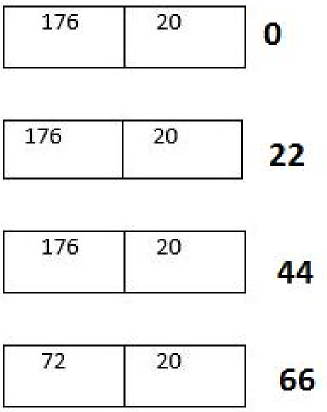
<table>
<tr><td></td><td>datagram and the fragmented datagram with identification field set as 12532.

DATA=600B, MTU = 200B ,IP HEADER = 20B.

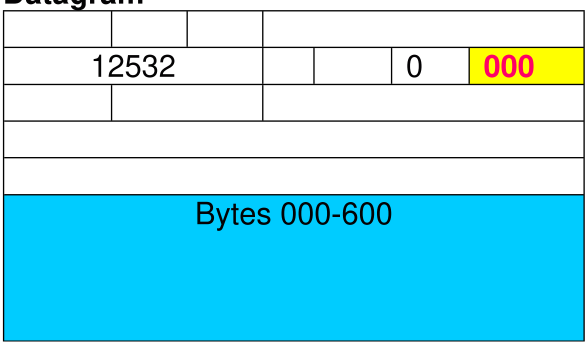
So in each frame 20B is reserved for IP HEADER ==> remaining is 180B

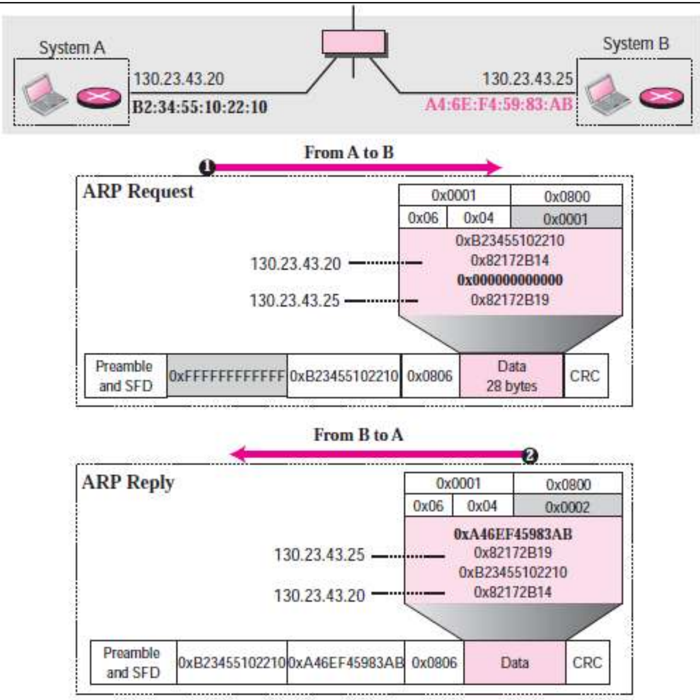
180 is not divisible by 8 , so we take 176 (nearest ones divisible by 8) as data along with 20B header.

we will get four segments like

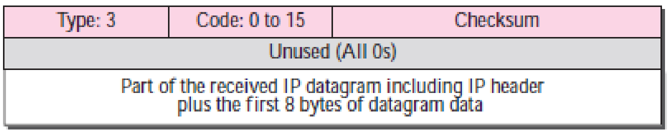


we will get fragment offset by dividing the datasent with 8 like 0 ,176 / 8 (22) , (176+176) / 8 (44) ,(176+176+176) / 8 (66).

Datagram

</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>12</td><td>A host with IP address 130.23.43.20 and physical address B2:34:55:10:22:10 has a packet to send to another host with IP address 130.23.43.25 and physical address A4:6E:F4:59:83:AB (which is unknown to the first host). The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.</td><td>5</td><td>L2</td><td>1</td><td>1</td><td>1.6.1</td></tr>
</table>

<table>
<tr><td></td><td>
</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>13</td><td>An ICMP message has arrived with the header (in hexadecimal): 03 03 10 20 00 00 00 00
What is the type of the message? What is the code? What is the purpose of the message? Draw the packet format with the specified fields.

Type 3
code 3
The port is unreachable. The application program (process) that the datagram is destined for is not running at the moment.


</td><td>5</td><td>L3</td><td>1</td><td>1</td><td>1.6.1</td></tr>
<tr><td>14</td><td>Utilize the following is a dump of a TCP header in hexadecimal format:
$(05320017\ 00000001\ 00000000\ 500207FF\ 00000000)_{16}$
a. What is the source port number?
b. What is the destination port number?
c. What the sequence number?
d. What is the acknowledgment number?
e. What is the length of the header?
f. What is the type of the segment?
g. What is the window size?

Hexadecimal dump: (05320017 00000001 00000000 500207FF 00000000)

a. Source port number:</td><td>5</td><td>L3</td><td>1</td><td>1</td><td>1.6.1</td></tr>
</table>

	The source port number is the first 2 bytes of the TCP header. Source port: 05 32 = 1330 b. Destination port number: The destination port number is the next 2 bytes of the TCP header. Destination port: 00 17 = 23 c. Sequence number: The sequence number is the next 4 bytes of the TCP header. Sequence number: 00 00 00 01 = 1 d. Acknowledgment number: The acknowledgment number is the next 4 bytes of the TCP header. Acknowledgment number: 00 00 00 00 = 0 e. Length of the header: The length of the header is indicated by the "data offset" field in the TCP header. This field is 4 bits in size, representing the number of 32-bit words in the header. Data offset: 5 (in decimal) Header length: 5 * 4 bytes = 20 bytes f. Type of the segment: The type of the segment is indicated by the "flags" field in the TCP header. Specifically, the "flags" field contains multiple flags that indicate the type of segment. In this case, we need to examine the flags to determine the type. The hexadecimal value for the flags field is 5002, which in binary is: 0101 0000 0000 0010 The relevant flags here are: Bit 0: CWR (Congestion Window Reduced) flag Bit 2: SYN (Synchronize) flag Since both CWR and SYN flags are set, it seems like this packet might be part of a connection establishment (TCP handshake). g. Window size:					

	The window size is the next 2 bytes of the TCP header. Window size: 07 FF = 2047 In summary: a. Source port number: 1330 b. Destination port number: 23 c. Sequence number: 1 d. Acknowledgment number: 0 e. Length of the header: 20 bytes f. Type of the segment: Connection establishment (SYN flag set) g. Window size: 2047					

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

SET - D

DEPARTMENT OF DATA SCIENCE& BUSINESS SYSTEMS

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Academic Year:2023 - 2024 (ODD)

Test: CLA - T1 **Date: 08-08-2023**
Course Code &Title:18CSC302J – Computer Networks **Duration:**50Minutes
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	3	-	-	-	-	-	-	-	-	-	-	-
2	CO2	-	-	3	-	1	-	-	-	-	-	-	-

Part - A
(10 x 1 = 10 Marks)

Instructions: Answer all

Q.No	Answer with choice variable	Marks	BL	CO	PO	PI Code
1	In an IP packet, the value of HLEN is 1001 in binary. How many bytes of options are being carried by this packet? a.**16 bytes** b. 12 bytes c. 10 bytes d. 20 bytes	1	L1	1	1	1.6.1
2	A packet has arrived with an M bit value of 1 and a fragmentation offset value of zero. Which type of the fragment it is a. first fragment or fragment **b. first fragment or a middle fragment** c. first fragment **d.** Last fragment.	1	L1	1	1	1.6.1
3	Which field helps to check rearrangement of the fragments? **a) Offset** b) Flag c) TTL d) Identifier	1	L1	1	1	1.6.1
4	Communication offered by TCP is ________ a) **Full-duplex** b) Half-duplex c) Semi-duplex d) Byte by byte	1	L1	1	1	1.6.1
5	During error reporting, ICMP always reports error messages to ________	1	L1	1	1	1.6.1

	a) Destination **b) Source** c) Next router d) Previous router					
6	Which of the following is false with respect to TCP? a) Connection-oriented b) Process-to-process c) Transport layer protocol **d) Unreliable**	1	L1	1	1	1.6.1
7	Choose the correct ARP message components? A. Sender Hardware Address B. Sender Protocol Address C. Hardware Type D. Operation Options: a) A and B b) C and D c) A, B, and D **d) A, B, C, and D**	1	L2	2	3	3.1.5
8	**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	L2	2	3	3.1.5
9	What connects IP address to the Physical address of devices? **A. Address Resolution Protocol** B. File Transfer Protocol C. User Datagram Protocol D. Transmission Control Protocol	1	L1	2	3	3.1.5
10	Which of the following is false with respect to TCP? a)Connection-oriented b)Process-to-process c)Transport layer protocol **d) Unreliable**	1	L1	1	1	1.6.1

Part – B

(3 x 5 = 15 Marks)

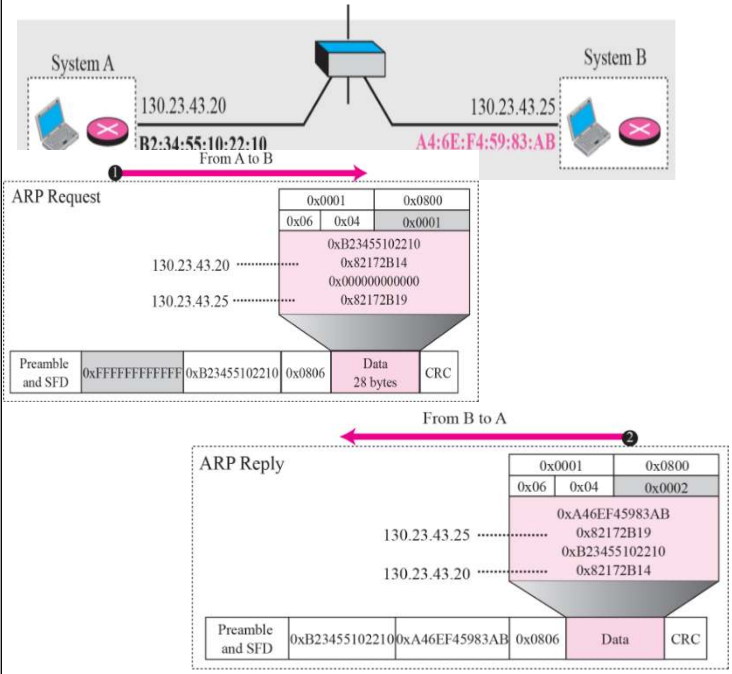
Instructions: Answer any 3 Questions

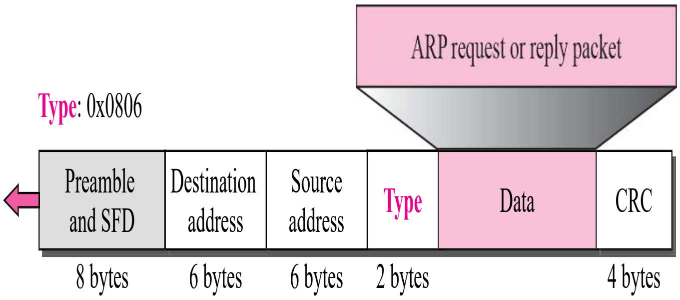
11	**A host with IP address 120.24.42.18 and physical address A2:34:55:10:22:10 has a packet to send to another host with IP address 120.20.41.25 and physical address B4:6E: F4:59:83:AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.**	5	L3	1	1	1.6.1

Sender hardware address: This is a variable-length field defining the physical address of the sender.
For example, for Ethernet this field is 6 bytes long.
Sender protocol address: This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.
Target hardware address: This is a variable-length field defining the physicaladdress of the target.
Target protocol address: This is a variable-length field defining the logical (forexample, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

Encapsulation

An ARP packet is encapsulated directly into a data link frame. For example, an ARP packet is encapsulated in an Ethernet frame. Note that the type field indicates that the data carried by the frame is an ARP packet.





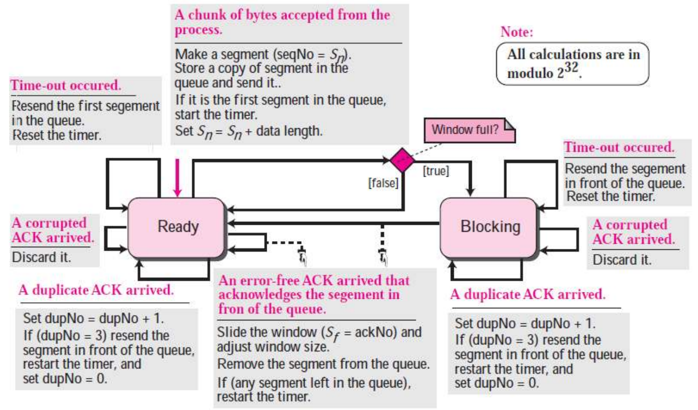
12	**8 &0**	00001000 00000000	2	L2	1	1	1.6.1
	0	00000000 00000000					
	123	00000000 01111011	3				
	20	00000000 00010100					
	71& 111	01000111 01101111					
	111 & 67	01101111 01100100					

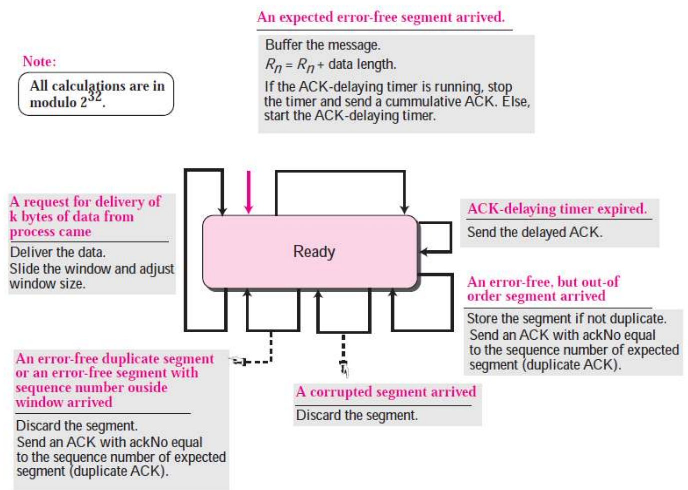
<table>
<tr><td></td><td>Sum: 10111111 01100010
Checksum: 01000000 10011101</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>13</td><td>
<table>
<tr><th>ARP</th><th>RARP</th></tr>
<tr><td>A protocol used to map an IP address to a physical (MAC) address</td><td>A protocol used to map a physical (MAC) address to an IP address</td></tr>
<tr><td>To obtain the MAC address of a network device when only its IP address is known</td><td>To obtain the IP address of a network device when only its MAC address is known</td></tr>
<tr><td>Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address</td><td>Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address</td></tr>
<tr><td>IP addresses</td><td>MAC addresses</td></tr>
<tr><td>Widely used in modern networks to resolve IP addresses to MAC addresses</td><td>Rarely used in modern networks as most devices have a pre-assigned IP address</td></tr>
<tr><td>ARP stands for Address Resolution Protocol.</td><td>Whereas RARP stands for Reverse Address Resolution Protocol.</td></tr>
<tr><td>Through ARP, (32-bit) IP address mapped into (48-bit) MAC address.</td><td>Whereas through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.</td></tr>
</table>
</td><td>5</td><td>L3</td><td>2</td><td>3</td><td>3.1.6</td></tr>
<tr><td>14</td><td>
Discuss about TCP Error control with mechanism
TCP protocol has methods for finding out corrupted segments, missing segments, out-of-order segments and duplicated segments.
Error control in TCP is mainly done through the use of three simple techniques :

Checksum – Every segment contains a checksum field which is used to find corrupted segments. If the segment is corrupted, then that segment is discarded by the destination TCP and is considered lost.
Acknowledgement – TCP has another mechanism called acknowledgement to affirm that the data segments have been delivered. Control segments that contain no data but have sequence numbers will be acknowledged as well but ACK segments are not acknowledged.
Retransmission
When a segment is missing, delayed to deliver to a receiver, corrupted when it is 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.
Retransmission after RTO:
TCP always preserves one retransmission time-out (RTO) timer for all sent but not acknowledged segments.
When the timer runs out of time, the earliest segment is retransmitted. Here no timer is set for acknowledgement.

</td><td>5</td><td>L2</td><td>2</td><td>3</td><td>3.1.6</td></tr>
</table>

	• In TCP, the RTO value is dynamic in nature and it is updated using the round trip time (RTT) of segments.
	• RTT is the time duration needed for a segment to reach the receiver and an acknowledgement to be received by the sender.
	• Retransmission
	• When a segment is missing, delayed to deliver to a receiver, corrupted when it is 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.
	• Retransmission after RTO:
	• TCP always preserves one retransmission time-out (RTO) timer for all sent but not acknowledged segments.
	• When the timer runs out of time, the earliest segment is retransmitted. Here no timer is set for acknowledgement.
	• In TCP, the RTO value is dynamic in nature and it is updated using the round trip time (RTT) of segments.
	• RTT is the time duration needed for a segment to reach the receiver and an acknowledgement to be received by the sender.
	
	d) ***Out-of-Order Segments***
	➢ Out-of-Order segments are not discarded by TCP
	➢ TCP flags such segments as out-of-order and store them temporarily until missing segments arrive
	TCP makes sure that data segments are delivered in sequence to the process
	
	e) ***FSM for Data Transfer in TCP***
	➢ FSM – Finite State Machine
	➢ Similar to Selective repeat and Go Back-N protocol
	➢ ***Sender-side & Receiver Side FSM***
	    ➢ ***Assumption :*** Unidirectional communication
	    ➢ ***Ignored Parameters:*** Selective ACK and Congestion Control
	    ➢ Nagle's algorithm / Windows shutdown not included in FSM
	    ➢ ***Advantage:*** Fast transmission policy using 3 duplicate ACK segments
	    ➢ ***Bi-directional FSM :*** Complex and more practical					


A chunk of bytes accepted from the process.
Make a segment (seqNo = S_n). Store a copy of segment in the queue and send it..
If it is the first segment in the queue, start the timer.
Set $S_n = S_n$ + data length.
Note:
All calculations are in modulo 2^{32}.
Time-out occured.
Resend the first segement in the queue. Reset the timer.
Window full?
[false]
[true]
Ready
Blocking
Time-out occured.
Resend the segement in front of the queue. Reset the timer.
A corrupted ACK arrived.
Discard it.
A corrupted ACK arrived.
Discard it.
A duplicate ACK arrived.
Set dupNo = dupNo + 1.
If (dupNo = 3) resend the segment in front of the queue, restart the timer, and set dupNo = 0.
An error-free ACK arrived that acknowledges the segement in fron of the queue.
Slide the window (S_f = ackNo) and adjust window size.
Remove the segment from the queue.
If (any segment left in the queue), restart the timer.
A duplicate ACK arrived.
Set dupNo = dupNo + 1.
If (dupNo = 3) resend the segment in front of the queue, restart the timer, and set dupNo = 0.


An expected error-free segment arrived.
Buffer the message.
$R_n = R_n$ + data length.
If the ACK-delaying timer is running, stop the timer and send a cummulative ACK. Else, start the ACK-delaying timer.
Note:
All calculations are in modulo 2^{32}.
A request for delivery of k bytes of data from process came
Deliver the data.
Slide the window and adjust window size.
Ready
ACK-delaying timer expired.
Send the delayed ACK.
An error-free, but out-of order segment arrived
Store the segment if not duplicate.
Send an ACK with ackNo equal to the sequence number of expected segment (duplicate ACK).
An error-free duplicate segment or an error-free segment with sequence number ouside window arrived
Discard the segment.
Send an ACK with ackNo equal to the sequence number of expected segment (duplicate ACK).
A corrupted segment arrived
Discard the segment.