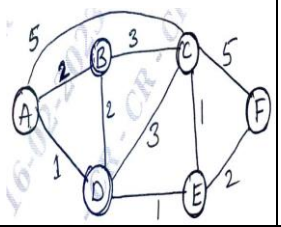
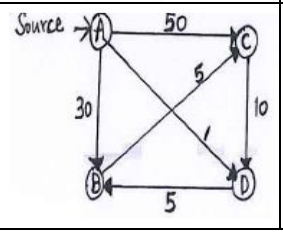
USN | | | | | | | | | | |

Internal Assessment Test 2–Jan-Feb 2024

Sub:	**Computer Networks**					Sub Code:	**21CS52**	Branch:	**AIML**	
Date:	**/02/24**	Duration:	**90 minutes**	Max Marks:	**50**	Sem/Sec:	**V**		**OBE**	

		Answer any FIVE FULL Questions		**MARKS**	**CO**	**RBT**
1	a	Explain 802.3 MAC frame format and also explain the different frames types in HDLC.		[10]	2	L2
2	a	What is IP addressing? Explain the classes of IP addressing with suitable examples.		[10]	3	L2
3	a	Differentiate between open loop and closed loop traffic control management? Describe any two mechanisms for open loop mechanisms.		[10]	3	L2
4	a	Differentiate between Leaky bucket and Token bucket approaches with diagrams.		[10]	3	L2
5	a	Differentiate between the header format of IPv4 & IPv6 and explain the fields involved in it.		[10]	3	L2
6	a	Consider the following networks with the indicated link costs. Apply link state routing algorithm to the following graph to compute the shortest path from source node “A” to all other nodes in the network.		[5]	3	L3
	b	Apply the distance vector routing algorithm to the following graph to compute the shortest path from source node “A” to all other nodes in the network.		[5]	3	L3

CI **CCI** **HoD**

USN | | | | | | | | | | |

Internal Assessment Test II –Feb. 2024

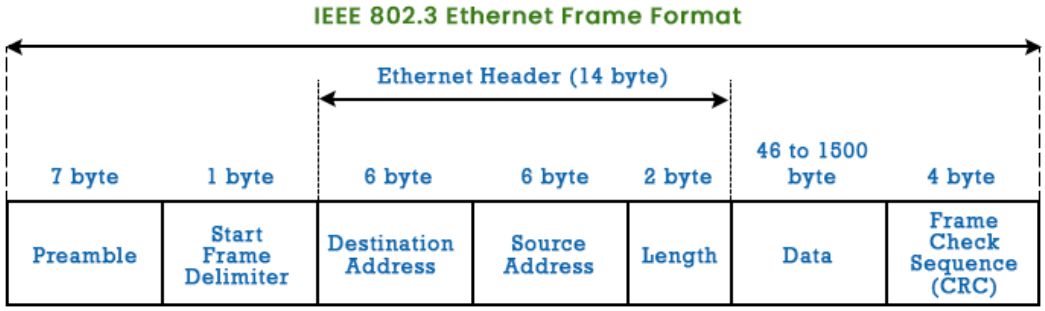
Sub:	Computer Networks					Sub Code:	21CS52	Branch:		AIML	
Date:	01/02/2024	Duration:	90 mins	Max Marks:	50	Sem / Sec:	A	Time	02.00 – 3:30AM	OBE	

Answer any FIVE FULL Questions

		MARKS	CO	RBT
1	**Explain 802.3 MAC frame format and also explain the different frames types in HDLC.**	[10]	CO2	L2

The IEEE 802.3 standard defines the fundamental frame format that is necessary for all MAC implementations. However, the core functionality of the protocol is being extended by several optional forms.

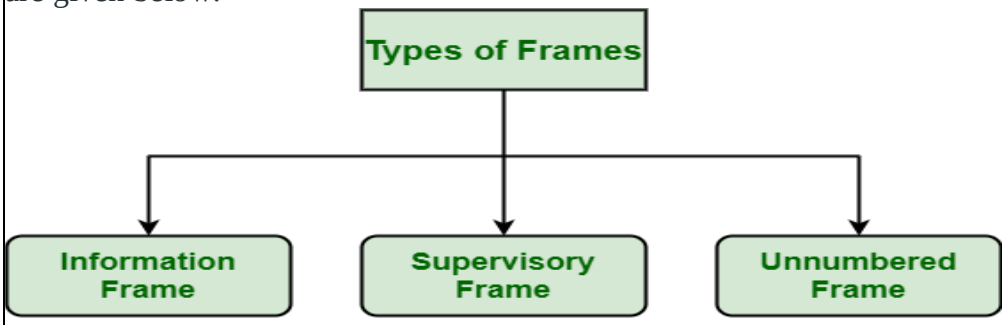
Preamble and SFD, which operate at the physical layer, begin an Ethernet frame. The packet's payload follows the Ethernet header, which includes the MAC addresses for the source and destination. CRC, the final field, is utilized to find errors. Let's now examine each section of the fundamental frame format.



1. **PREAMBLE** - Ethernet frames begin with a 7-byte. This is a sequence of alternate 0s and 1s that denotes the beginning of the frame and enables bit synchronization between the sender and receiver. PRE (Preamble) was initially developed to accommodate the loss of a few bits as a result of signal delays. However, the frame bits in high-speed Ethernet today are protected without the need for a preamble. Prior to the actual frame beginning, PRE (Preamble) alerts the receiver that a frame is about to start and enables the receiver to lock onto the data stream.
2. **Start of frame Delimiter (SFD)** - This 1-byte field is always set to **10101011**. The destination address is the next set of bits that will begin the frame, as indicated by SFD. The preamble is frequently referred to as 8 Bytes since SFD is sometimes seen as a component of PRE. The SFD notifies the station or stations that synchronization is now impossible.

3. **Destination Address** - This 6-Byte element contains the MAC address of the device for which the data is intended.
4. **Source Address** - This 6-byte element contains the source machine's MAC address. Since Source Address is always a unique address (Unicast), 0 is always the least significant bit of the first byte.
5. **Length** - A 2-Byte field called Length represents the size of an Ethernet frame as a whole. Due to some inherent constraints of Ethernet, this 16-bit field can store length values from 0 to 65534, but length values greater than 1500 are not permitted.
6. **Data** - This area, sometimes referred to as the Payload, is where the real data is placed. If Internet Protocol is utilised via Ethernet, both the IP header and data will be placed here. The longest possible piece of data might be 1500 bytes long. If the data length is less than the minimum length, which is 46 bytes, padding 0's are appended to make up the difference.
7. **Cyclic Redundancy Check (CRC)** - CRC is a field of 4 bytes. The data in this field is a 32-bit hash code created using the fields for the destination address, source address, length, and data. Data is damaged if the checksum calculated by the destination differs from the checksum value supplied.

High-Level Data Link Control (HDLC) generally provides flexibility to simply support all options that are possible in various data transfer modes and configurations. To provide flexibility, HDLC basically uses and explains three different types of frames. Type of frame is basically determined by control field of frame. Each type of frame generally serves as an envelope for transmission of various types of messages. These three different classes of frames used in HDLC are given below.



I-frame : I-frame stands for Information frames. This frame is generally used for transporting user data from network layer. These frames actually carry actual data or information of upper layer and some control information. This frame carries data along with both send sequence number and an acknowledgment number. It can also be used to piggyback acknowledgement information in case of ABM (Asynchronous Balanced Mode). The first bit of this frame of control field is 0.

S-frame : S-frame stands for Supervisory frames. These frames are basically required and essential for error control and flow control. They also provide control information. It contains or includes only an Acknowledgment number.

First two bit of this frame of control field is 10. S-frame does not have any information fields. This frame contains send and receive sequence numbers.

U-frame : U-frame stands for Unnumbered frames. These frames are also required in various functions like link setup and disconnections. These frames basically support control purposes and are not sequenced. First, two-bit of this frame of control field is 11. Some U-frame contains an information field depending on the type. These frames are also used for different miscellaneous purposes along with link management. U-frame is required for managing link itself.

2	**What is IP addressing? Explain the classes of IP addressing with suitable examples.**	[10]	CO 2	L2

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

TCP/IP defines five classes of IP addresses: class A, B, C, D, and E. Each class has a range of valid IP addresses. The value of the first octet determines the class. IP addresses from the first three classes (A, B and C) can be used for host addresses. The other two classes are used for other purposes – class D for multicast and class E for experimental purposes.

The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size. For example, for the small number of networks with a very large number of hosts, the Class A was created. The Class C was created for numerous networks with small number of hosts.

Classes of IP addresses are:

Class	First octet value	Subnet mask
A	0-127	8
B	128-191	16
C	192-223	24
D	224-239	-
E	240-255	-

Consider the following IP addresses:

- **10.50.120.7** – because this is a Class A address, the first number (10) represents the network part, while the remainder of the address represents the host part (50.120.7). This means that, in order for devices to be on the same network, the first number of their IP addresses has to be the same for both devices. In this case, a device with the IP address of 10.47.8.4 is on

the same network as the device with the IP address listed above. The device with the IP address 11.5.4.3 is not on the same network, because the first number of its IP address is different.

- **172.16.55.13** – because this is a Class B address, the first two numbers (172.16) represent the network part, while the remainder of the address represents the host part (55.13). A device with the IP address of 172.16.254.3 is on the same network, while a device with the IP address of 172.55.54.74 isn't.

Class A Public & Private IP Address Range

Class A addresses are for networks with large number of total hosts. Class A allows for 126 networks by using the first octet for the network ID. The first bit in this octet, is always zero. The remaining seven bits in this octet complete the network ID. The 24 bits in the remaining three octets represent the hosts ID and allows for approximately 17 million hosts per network. Class A network number values begin at 1 and end at 127.

- Public IP Range: 1.0.0.0 to 127.0.0.0
  - First octet value range from 1 to 127
- Private IP Range: 10.0.0.0 to 10.255.255.255 (See Private IP Addresses below for more information)
- Subnet Mask: 255.0.0.0 (8 bits)
- Number of Networks: 126
- Number of Hosts per Network: 16,777,214

Class B Public & Private IP Address Range

Class B addresses are for medium to large sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. The first two bits in the first octet are always 1 0. The remaining six bits, together with the second octet, complete the network ID. The 16 bits in the third and fourth octet represent host ID and allows for approximately 65,000 hosts per network. Class B network number values begin at 128 and end at 191.

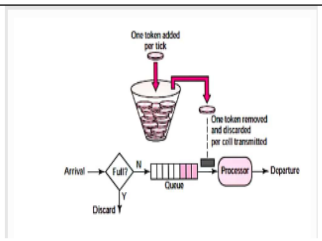
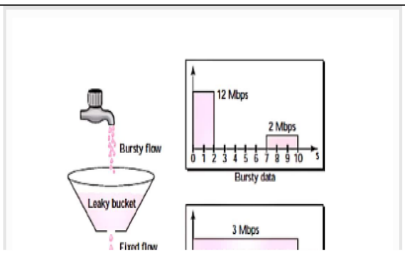
- Public IP Range: 128.0.0.0 to 191.255.0.0
  - First octet value range from 128 to 191
- Private IP Range: 172.16.0.0 to 172.31.255.255 (See Private IP Addresses below for more information)
- Subnet Mask: 255.255.0.0 (16 bits)
- Number of Networks: 16,382
- Number of Hosts per Network: 65,534

Class C Public & Private IP Address Range

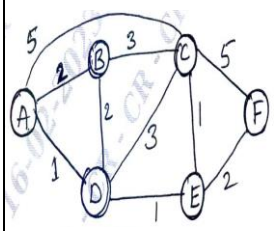
Class C addresses are used in small local area networks (LANs). Class C allows for approximately 2 million networks by using the first three octets for the network ID. In a class C IP address, the first three bits of the first octet are always 1 1 0. And the remaining 21 bits of first three octets complete the network ID. The last octet (8 bits) represent the host ID and allows for 254 hosts per network. Class C network number values begins at 192 and end at 223.

- Public IP Range: 192.0.0.0 to 223.255.255.0
  - First octet value range from 192 to 223

	• Private IP Range: 192.168.0.0 to 192.168.255.255 (See Private IP Addresses below for more information) • Special IP Range: 127.0.0.1 to 127.255.255.255 (See Special IP Addresses below for more information) • Subnet Mask: 255.255.255.0 (24 bits) • Number of Networks: 2,097,150 • Number of Hosts per Network: 254			
3	**Differentiate between open loop and closed loop traffic control management? Describe any two mechanisms for open loop mechanisms?** **Open Loop** / **Closed Loop** Constructions: Simple constructions / Complex constructions Called: Non-feedback system / Feedback system Required Additional System: The system lacks a feedback loop / Has a feedback loop to control the state Reliability: Less reliable / More reliable Accuracy: Performs accurately under good calibration / Performs accurately due to the feedback system Optimization: Not possible / Possible Maintenance: Less maintenance needed / More maintenance required Inbuilt Components: Two components included / More components (like controller, feedback, and comparator) are present System Disturbance: Affected / Not affected Linearity: Non-linear / Linear Response: Fast / Slow Components: Controller and controlled process / Amplifier, controller, controlled process, feedback	[10]	CO 1	L2
4 (a)	**Differentiate between Leaky bucket and Token bucket approaches with diagrams.**	[10]	CO3	L2

Sr no.	Token Bucket	Leaky Bucket
1	Token bucket is token dependent.	Leaky bucket is token independent.
2	 Block diagram token bucket.	 Block diagram of leaky bucket.
3	If bucket is full token are discarded but not the packet.	If bucket is full packet or data is discarded.
4	Token bucket allows for large bursts to be sent faster by speeding up the output.	Leaky bucket sends the packets at an average rate.
5	Token bucket allows saving up of tokens (permission) to send large bursts.	Leaky bucket does not allow saving a constant rate is maintained.
6	Packets can only Transmitted when there are enough token.	Packet are transmitted continuously.
7	It save token.	It is does not save token.

6 a	**Write link state algorithm, consider the following networks with the indicated link costs. Apply link state routing algorithm to the following graph to compute the shortest path from source node "A" to all other nodes in the network.**	[5]	CO 3	L3



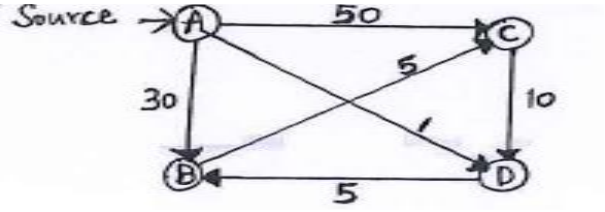
Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

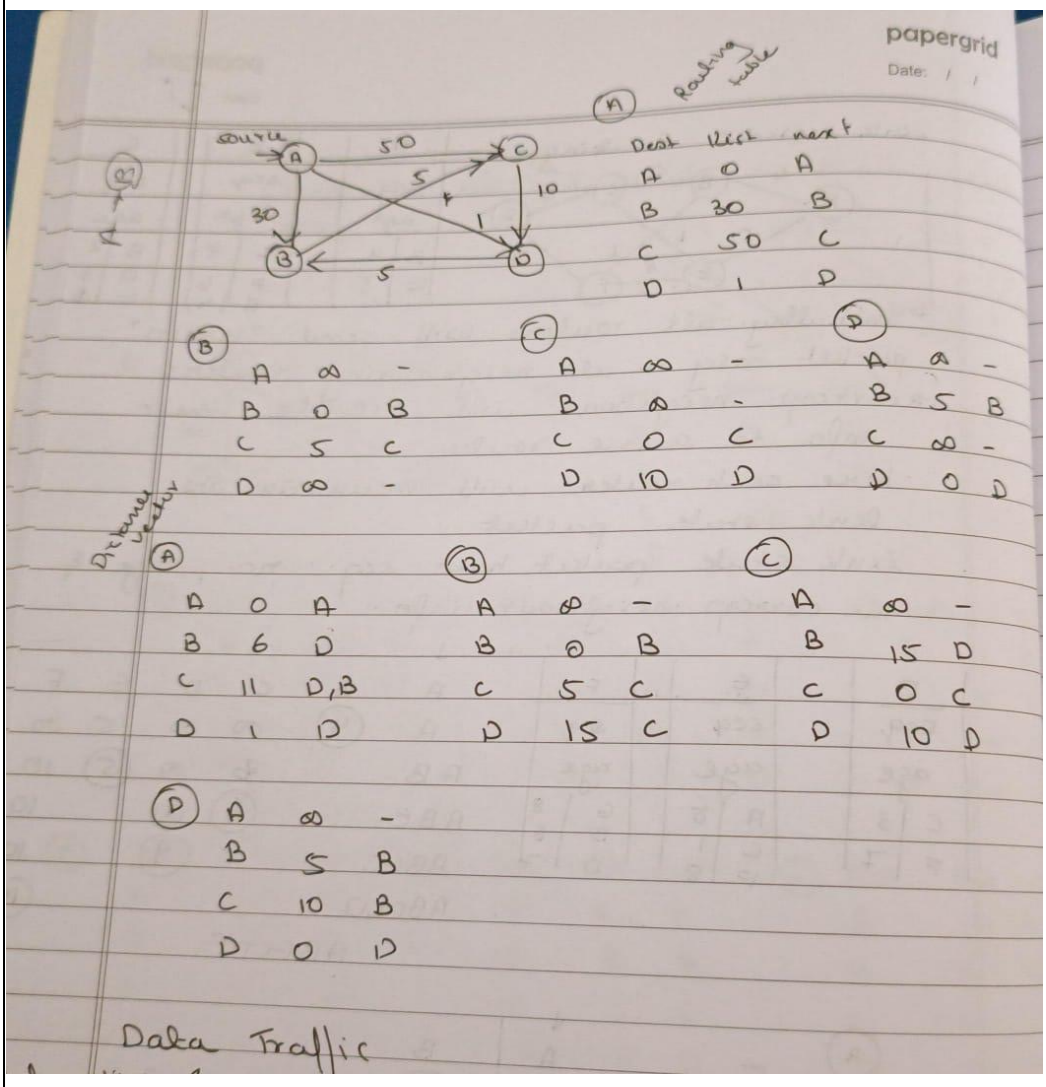
The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E
6	ADEBCF					

6 b) Apply the distance vector routing algorithm to the following graph to compute the shortest path from source node "A" to all other nodes in the network





CO PO Mapping

CO-PO and CO-PSO Mapping

CO-PO and CO-PSO Mapping																				
Course Outcomes		**Blooms Level**	**Modules covered**	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**	**PSO3**	**PSO4**
CO1	Analyze and compare various networking protocols.	**L1**	**7,8, 9,10 ,11, 12**	2	-	-	-	-	-	-	1	1	-	-	2	-	2	-	-
CO2	Demonstrate the working of different concepts of networking	**L2**	**7,8, 9,10 ,11, 12**	2	3	3	-	-	-	-	1	1	-	-	2	-	2	-	-
CO3	Implement, analyze and evaluate networking protocols in NS2 / NS3 and JAVA programming language	**L3**	**1,2, 3,4, 5,6**	2	2	3	-	-	-	-	1	1	-	-	2	-	2	-	-

COGNITIVE LEVEL	REVISED BLOOMS TAXONOMY KEYWORDS

L1	List, define, tell, describe, identify, show, label, collect, examine, tabulate, quote, name, who, when, where, etc.
L2	summarize, describe, interpret, contrast, predict, associate, distinguish, estimate, differentiate, discuss, extend
L3	Apply, demonstrate, calculate, complete, illustrate, show, solve, examine, modify, relate, change, classify, experiment, discover.
L4	Analyze, separate, order, explain, connect, classify, arrange, divide, compare, select, explain, infer.
L5	Assess, decide, rank, grade, test, measure, recommend, convince, select, judge, explain, discriminate, support, conclude, compare, summarize.

PROGRAM OUTCOMES (PO), PROGRAM SPECIFIC OUTCOMES (PSO)				CORRELATION LEVELS	
PO1	Engineering knowledge	PO7	Environment and sustainability	0	No Correlation
PO2	Problem analysis	PO8	Ethics	1	Slight/Low
PO3	Design/development of solutions	PO9	Individual and team work	2	Moderate/ Medium
PO4	Conduct investigations of complex problems	PO10	Communication	3	Substantial/ High
PO5	Modern tool usage	PO11	Project management and finance		
PO6	The Engineer and society	PO12	Life-long learning		
PSO1	Develop applications using different stacks of web and programming technologies				
PSO2	Design and develop secure, parallel, distributed, networked, and digital systems				
PSO3	Apply software engineering methods to design, develop, test and manage software systems.				
PSO4	Develop intelligent applications for business and industry				