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)***

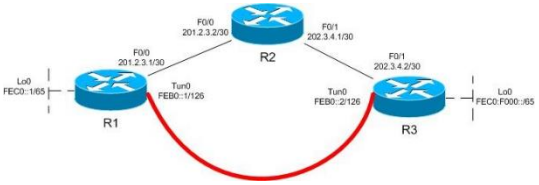
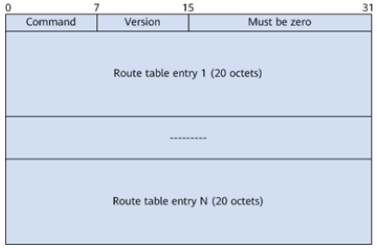
CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	L	H	-	H	L	-	-	-	L	L	-	H
CO2	M	H	-	M	L	-	-	-	M	L	-	H
CO3	M	H	-	H	L	-	-	-	M	L	-	H
CO4	M	H	-	H	L	-	-	-	M	L	-	H
CO5	H	H	-	H	L	-	-	-	M	L	-	H
CO6	L	H	-	H	L	-	-	-	L	L	-	H

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

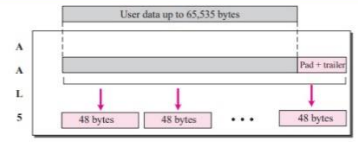
	calculate the best path to all destinations. 0 7 15 23 31 Version | Type | Packet length Router ID Area ID Checksum | Instance ID | 0 **MP-BGP4** (Modified ProtocolBorder Gateway Protocol):It is the only open standard Exterior Gateway Protocol available. BGP is a Distance Vector protocol that takes an 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

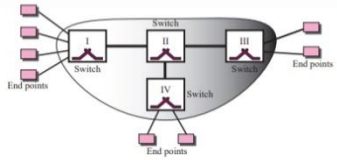
	a. How long does it take for a bit to travel from the beginning to the end of the network? *b*. Find the maximum time it takes to sense a collision (worst case). ii)The data rate of 10Base5 is 10Mbps. How long does it take to create the smallest frame? Show your calculations. a. Distance = Velocity × 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

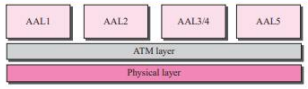
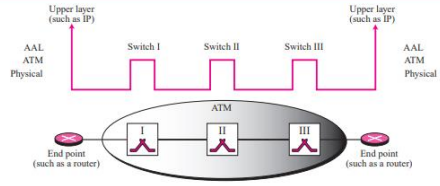
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

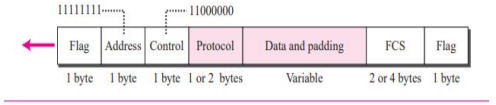
SRM Institute of Science and Technology
College of Engineering and Technology
School of Computing
SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

Set A

	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.

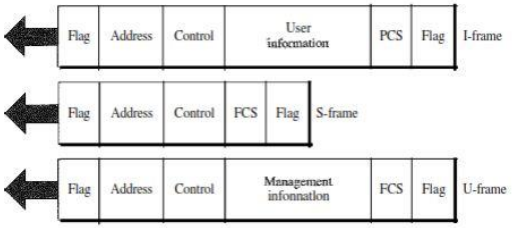


Fig no.29

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

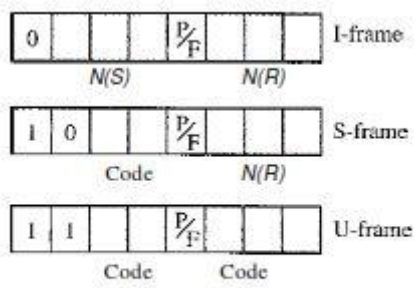


Fig no.30

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.

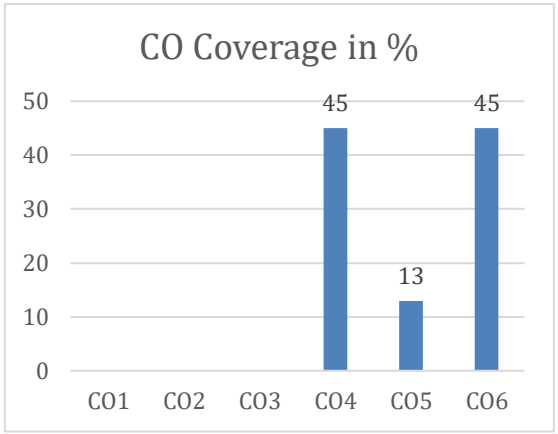
Control Fieldfor S-Frames Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than an acknowledgment). S-frames do not have information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

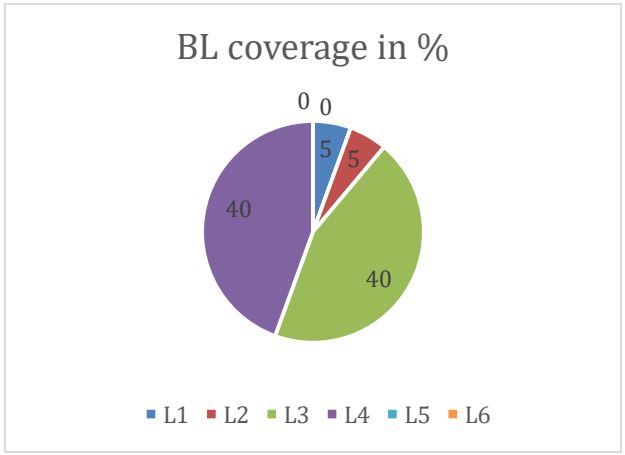
Receive ready (RR): If the value of the code subfield is 00, it is an RR S-frame. This kind of

	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

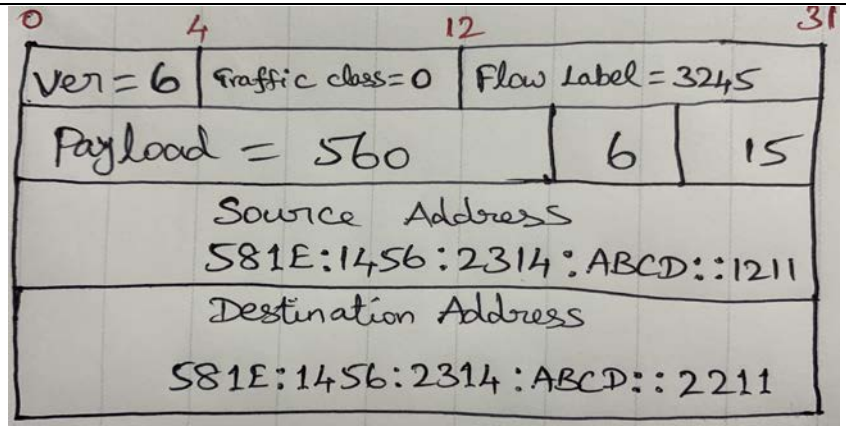
Test: CLA-T3 (ANSWER KEY)
Max. Marks: 50
Course Code & Title: 18CSC302J & COMPUTER NETWORKS

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

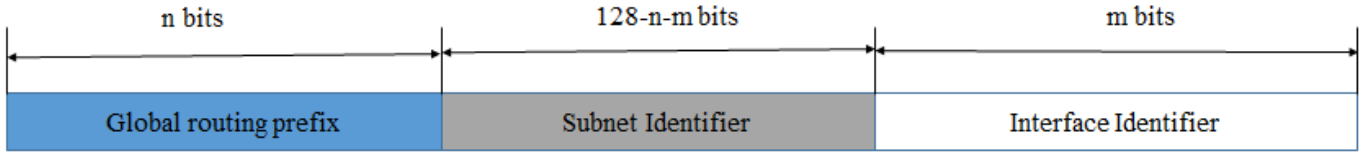
Part – A Instructions: Answer all the questions (1 x 10 = 10 Marks)						
Q. No	**Question**	**Marks**	**BL**	**CO**	**PO**	**PI Code**
1	In the IPv6 header, the traffic class field is similar to which field in the IPv4 header? **D) ToS field**	1	L1	4	1	1.6.1
2	Suppose two IPv6 nodes want to interoperate 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.** **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	5	L3	4	2	2.6.1

		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

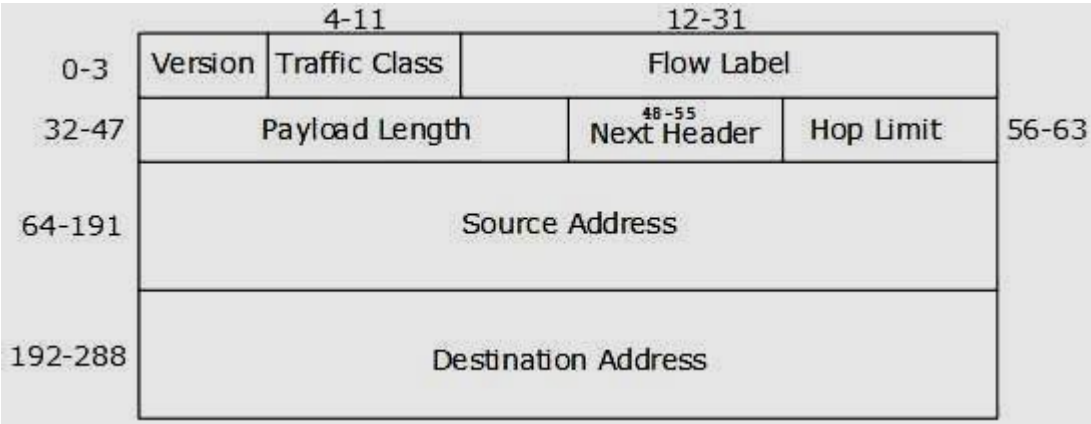
Block Assignment	Length of block
Global routing prefix (n)	48 bits
Subnet Identifier (128-n-m)	16 bits
Interface Identifier	64 bits

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.

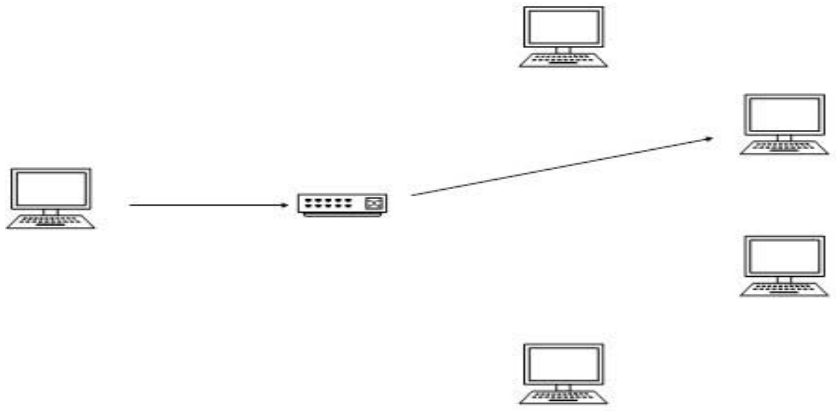
Subnet Identifier :
16 bit block is used to identify the specific subnet of an organization.
An organization can have upto 2^{16} subnets.

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.	10	L3	4	2	2.6.1

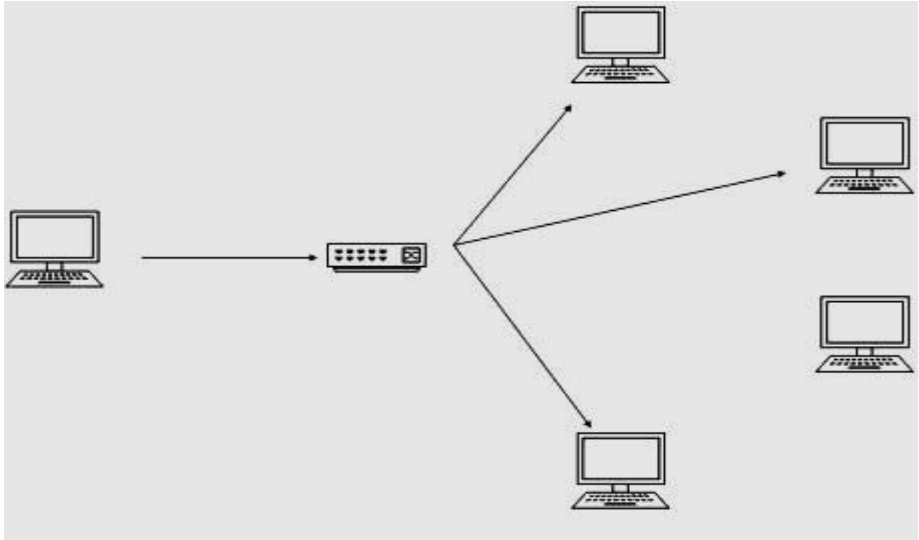
S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used

		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

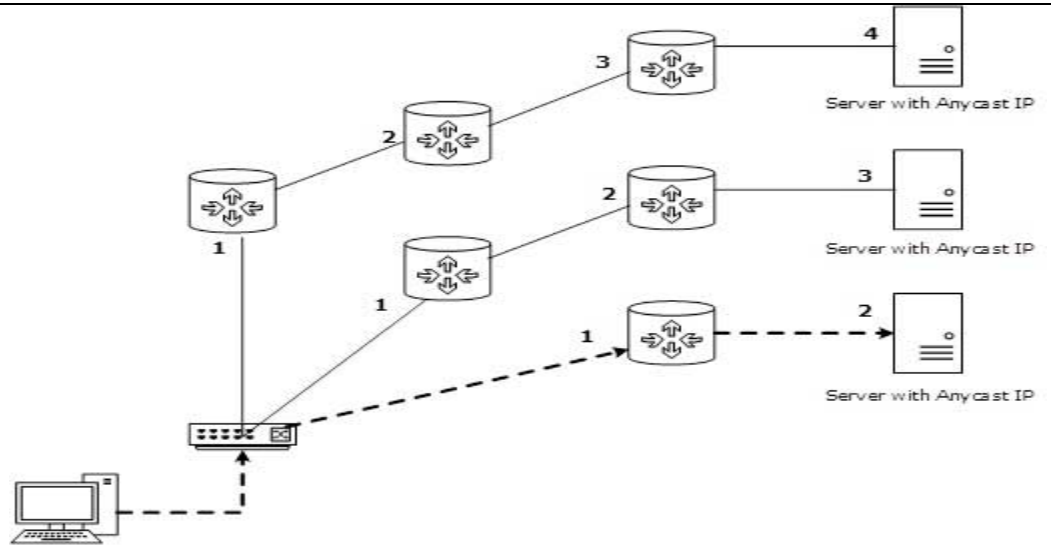
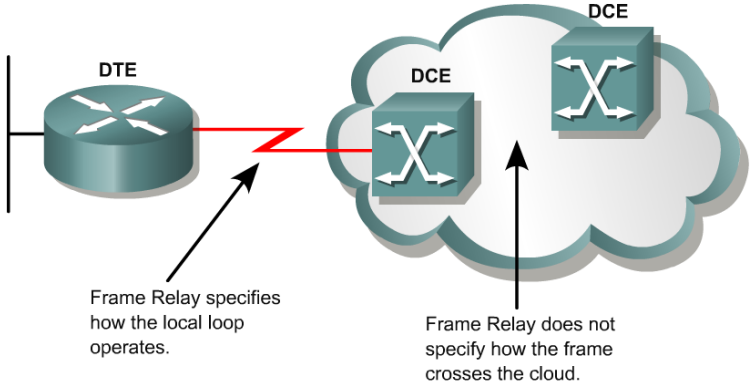
Multicast

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.

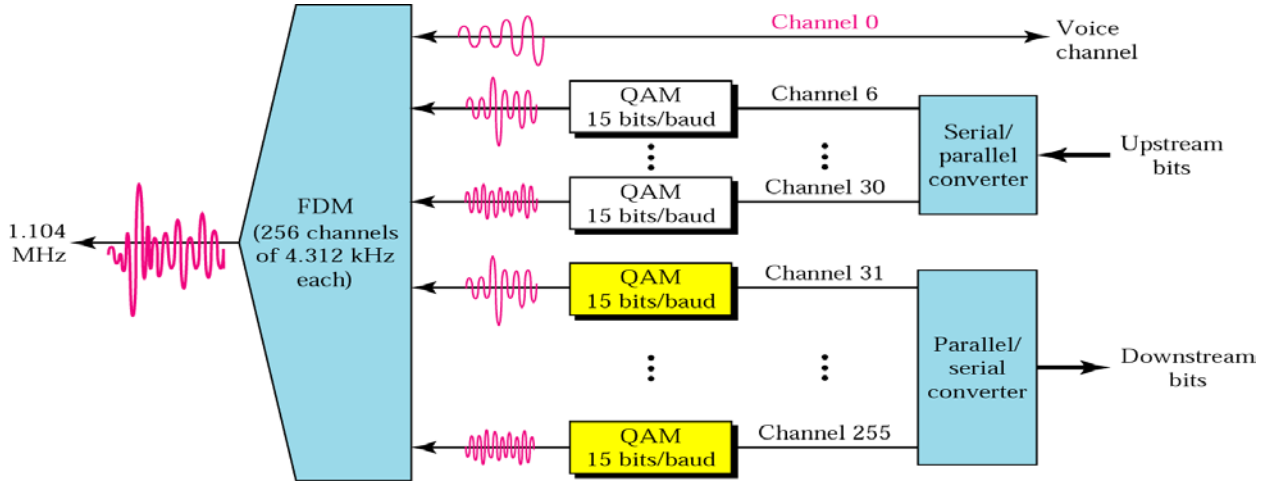


Anycast

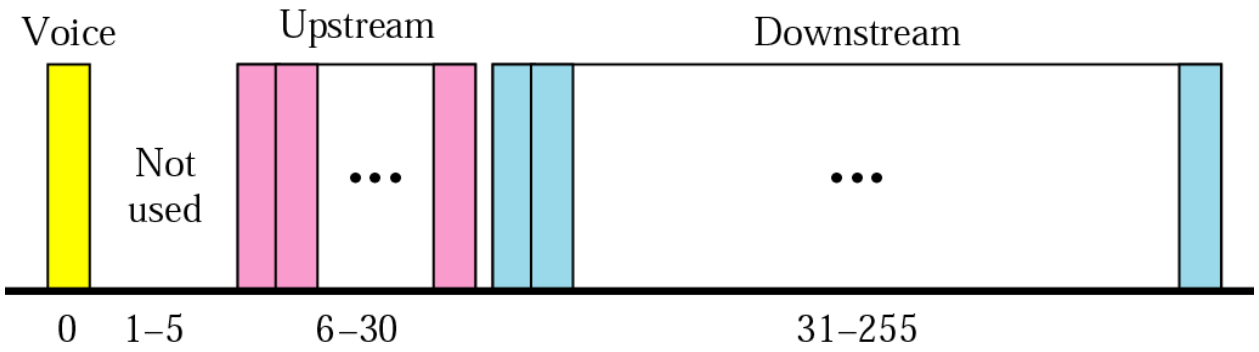
IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message. With the help of 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.					

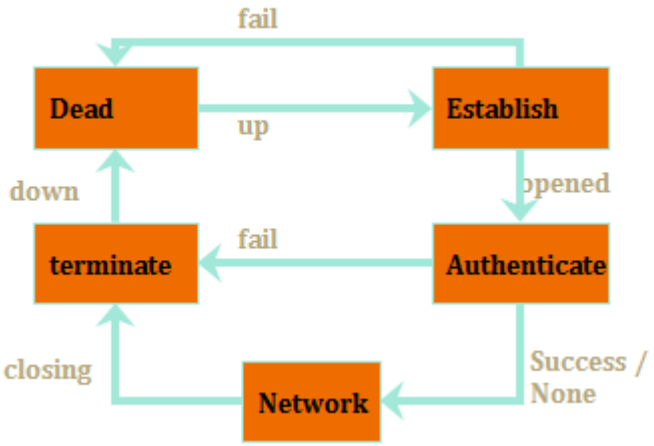
	● In most cases, these are packet switches, which are the devices that actually transmit data through the WAN. ● The connection between the customer and the service provider is known as the **User-to-Network Interface (UNI).** ● The **Network-to-Network Interface (NNI)** is used to describe how Frame 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.

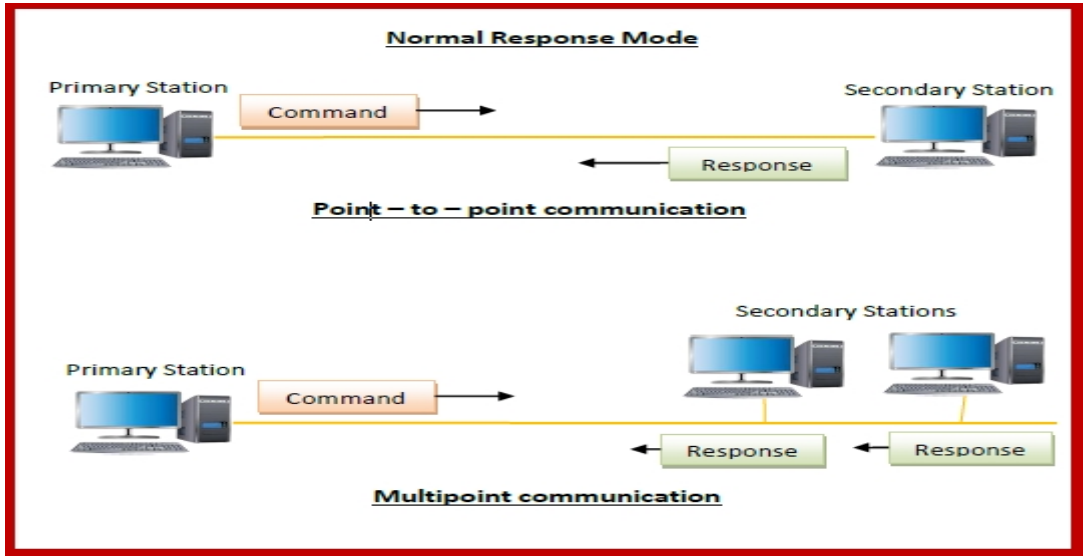
The telephone line or cable companies provide a physical link, but to control and manage the transfer of data, there is a need for a special protocol. The **Point-to-Point Protocol (PPP**) was designed to respond to this need.

	 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.



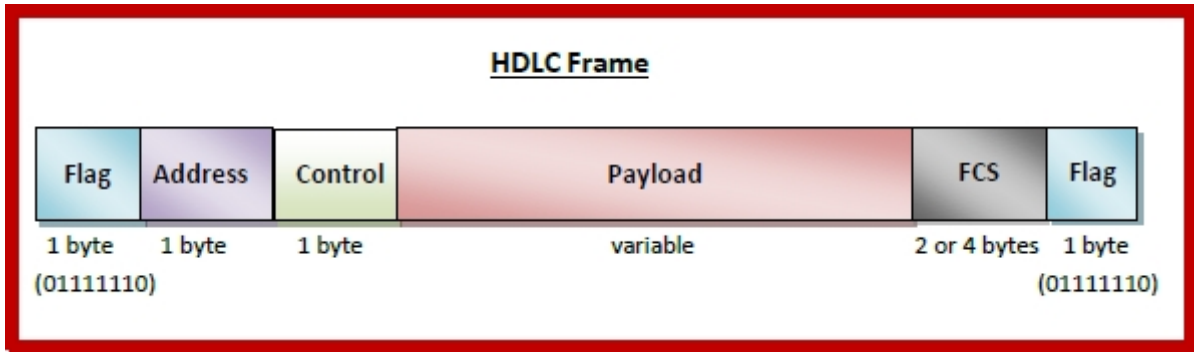
Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.

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)

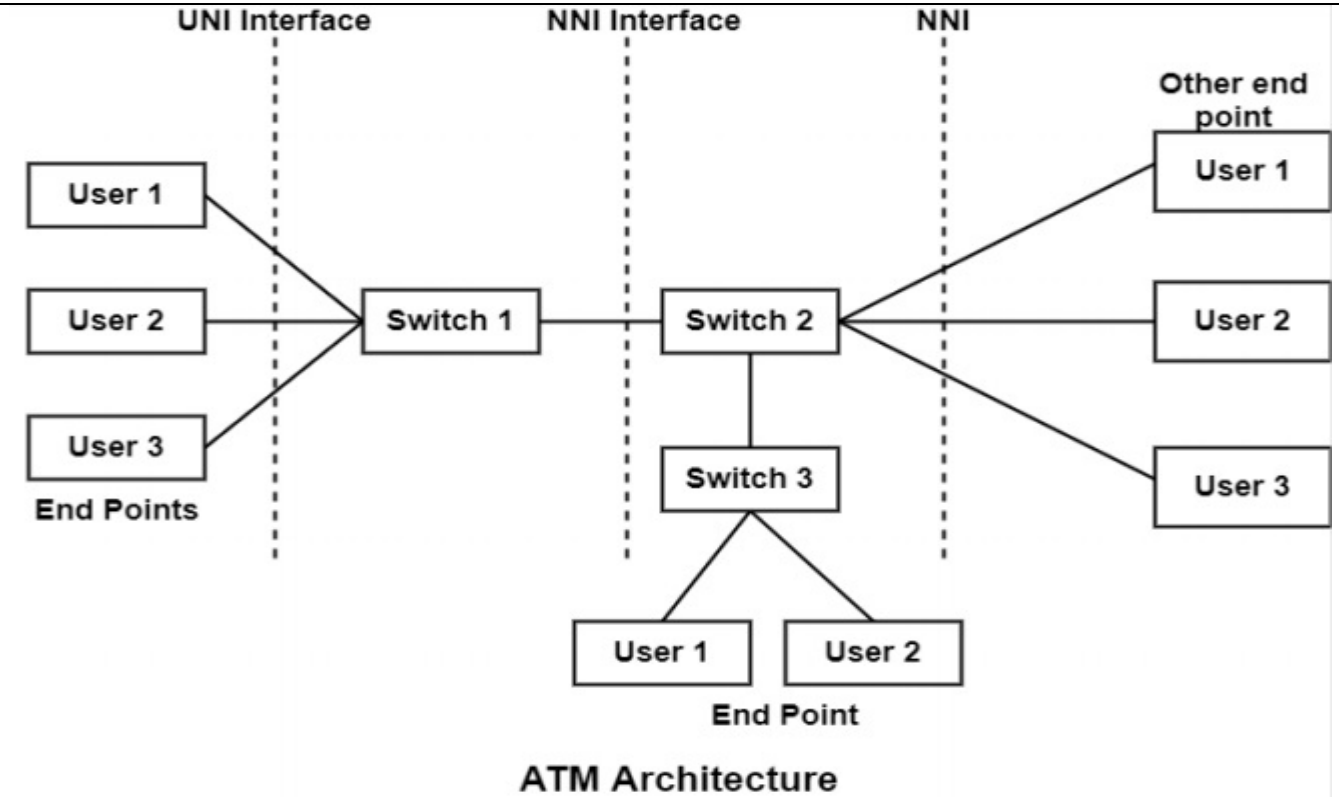


Types of HDLC Frames

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



ATM Architecture

ATM transfers the information through a transmission path which is made up of a logical virtual path and virtual channel. The transmission path consists of the physical cable, which is connected to an ATM switch. The cables have a transfer speed of up to 155 megabits per second on an optical fiber link.

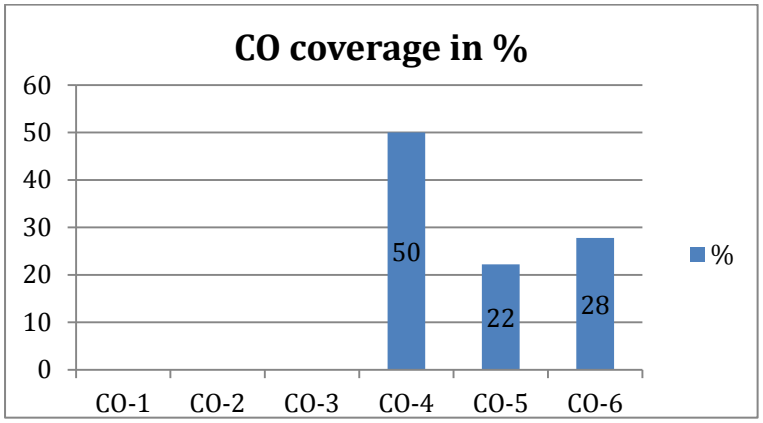
Virtual Path

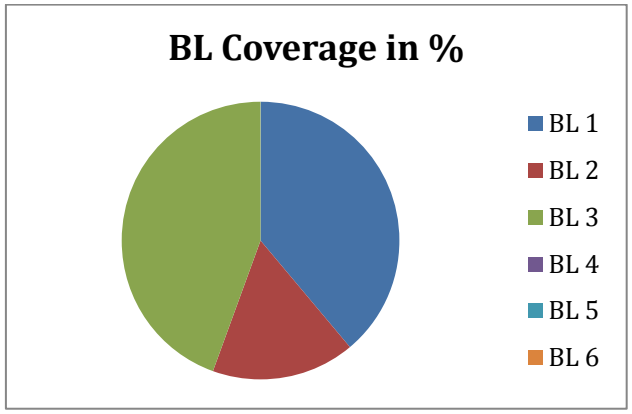
The transmission path is logically divided into separate virtual paths identified using the virtual

	path identifier (VPI) in the ATM header. ## Virtual Channel The bandwidth of a logical virtual path is further divided into a separate channel. Each channel is given a virtual channel identifier in the ATM header. ## Traffic flow through the Network A two-tiered addressing design is used with the following elements being contained in the addressing assignments. • **Virtual Channel:** A virtual channel represents the structure of a single network connection data flow between two ATM end-users. The ATM standards represent this as a unidirectional connection between two end-points on the network. • **Virtual Path:** A virtual path can carry one or more virtual channels by the network. It is represented as a group of channels between the two end-points.					

***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





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

Set - C

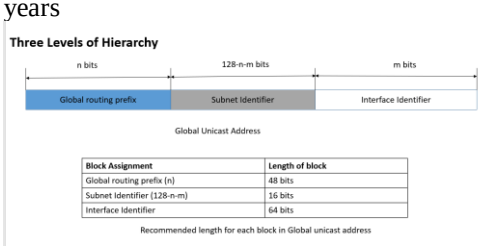
Academic Year: 2022-23 (ODD) **Test: CLA-T3** **Year & Sem: III** Year / VI Sem
Date: - **Max. Marks:** 50 **Duration: 1 Hour 40 min**
Course Code & Title: 18CSC302J & COMPUTER NETWORKS

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)**

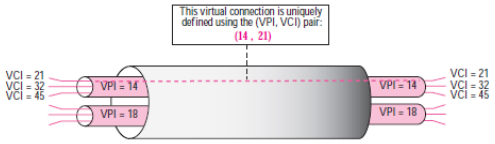
Q. No	Question	Marks	BL	CO	PO	PI Code
1	**Select the correct statement when describing a global unicast address?** a) Packets addressed to a unicast address are delivered to a single interface b) These are like private addresses in IPV4 in that they are not meant to be routed c) These are typical publicly 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 (10 x 4 = 40 Marks)						
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

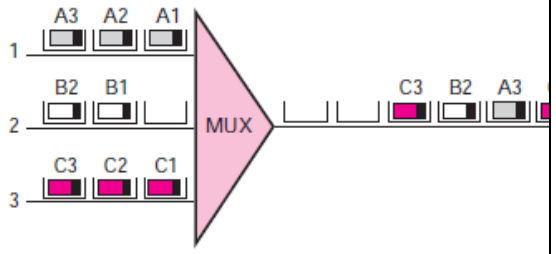
	The first 48 bits of a global unicast address are called global routing prefix. They are used to route the packet through the Internet to the organization site such as ISP that owns the block. The first three bits in this part is fixed (001), Remaining 45 bits can defined up to 245 sites The global routers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

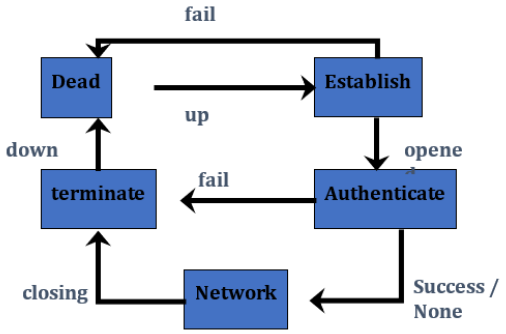
	connection), virtual paths (a combination of virtual circuits that are bundled together because parts of their paths are the same), and virtual circuits that logically connect two points together. In a virtual circuit network, to route data from one end point to another, the virtual connections need 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

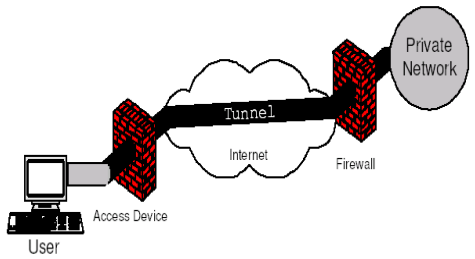
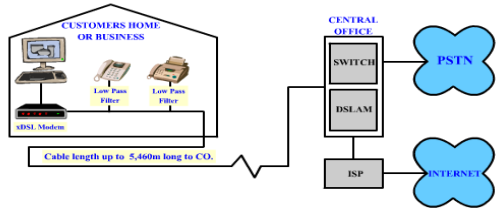
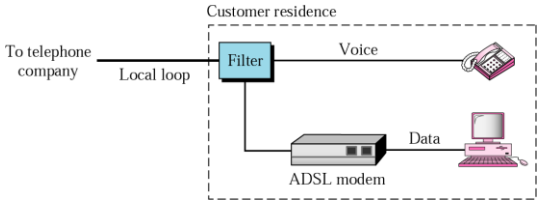
	Asynchronous Transfer Mode—to multiplex cells coming from different channels. It uses fixed-size slots the size of a cell. ATM multiplexers fill a slot with a cell from any input channel that has a cell; the slot is empty if none of the channels has a cell to send. The following figure shows how cells 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. 					

	[redacted] information identifying 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					

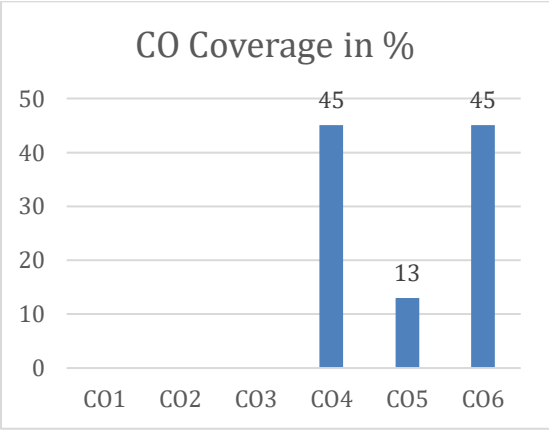
	the terminate.  **Tunneling & PPP** Tunneling - definition The process of running one network protocol on top of another. Common use: VPN (Virtual Private Network) Tunneling method Extending the link between the HDLC driver and the rest of PPP over a separate network PPP tunneling protocols L2TP, L2F(**Layer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

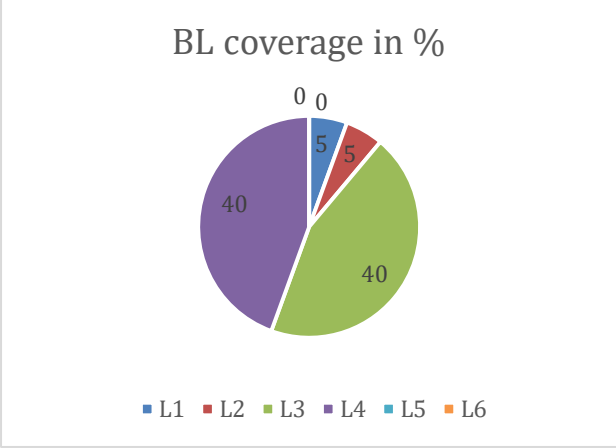
	 **OR**					
14. b)	Elaborate DSL and ADSL in detail. Answer DSL  ADSL  	10	L 4	6	2	2.6.4

***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





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

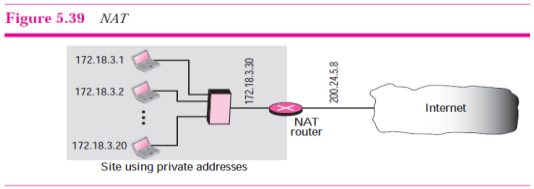
Set - D

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

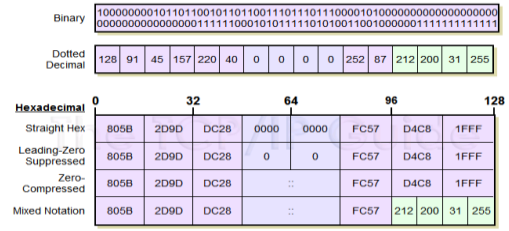
Course Articulation Matrix: ***(to be placed)***

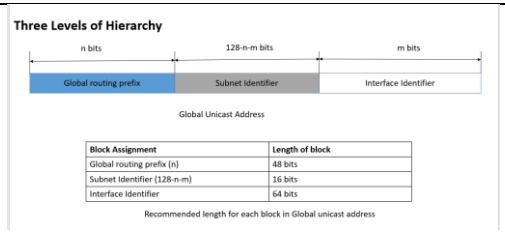
CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO12
CO 4	M	H	-	H	L	-	-	-	M	L	-	H
CO 5	H	H	-	H	L	-	-	-	M	L	-	H
CO 6	L	H	-	H	L	-	-	-	L	L	-	H

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 172.18.3.1 172.18.3.2 172.18.3.20 172.18.3.30 200.24.5.8 NAT router Internet Site using private addresses • 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 :

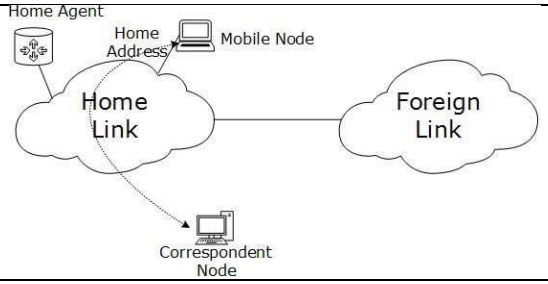
Last 64 bits refers to the interface identifier. It is similar to the hostId in IPV4 scheme.

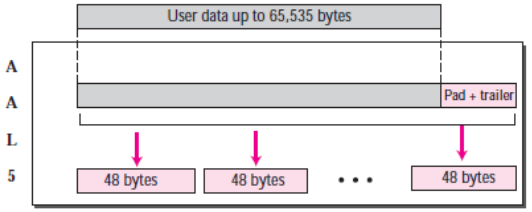
In IPV4 addressing, there is no relation between the hostid (32 bits) and MAC(48 bits) due to the difference in length.

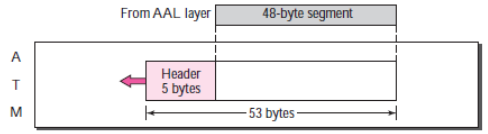
Physical address whose length is less than 64 bits can be embedded as the whole or part of the interface identifier, eliminating the mapping process with the help of IPv6.

. 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.

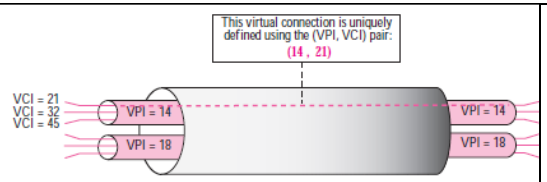
	OR					
12. b)	Explain IPV6 Mobility in detail. • When a host is connected to a link or network, it acquires an IP address and all communication take place using that IP address on that link. As soon as, the same host changes its physical location, that is, moves into another area / subnet / network / 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

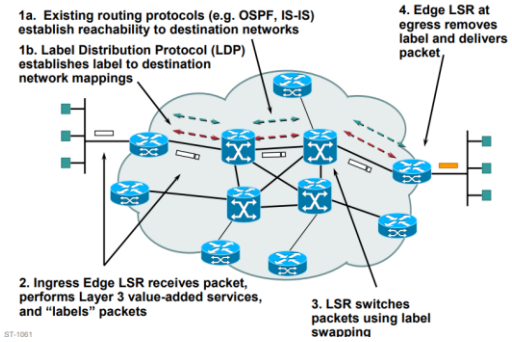
	and can be of variable or fixed rates. At the receiver, this process is reversed—segments are reassembled into their original formats and passed to the receiving service. Although four AAL layers have been defined the one which is of interest to us is AAL5, which is used to carry IP packets in the Internet. 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					

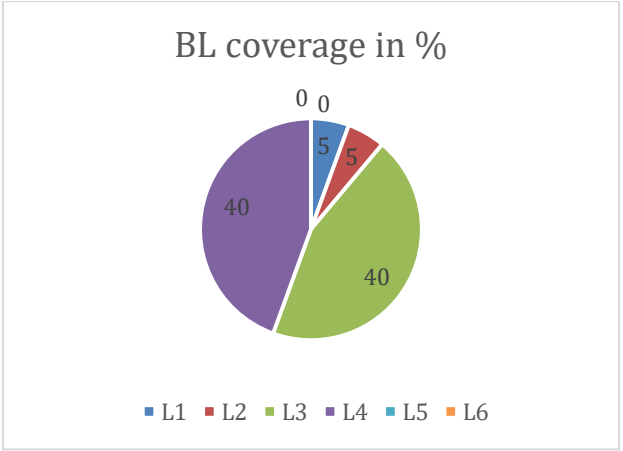
	receiving equipment expects it (at the last 8 bytes of the last cell). Once the padding and trailer are in place, AAL5 passes the message in 48-byte segments to the ATM layer. **ATM Layer** The ATM layer provides routing, traffic management, switching, and multiplexing services. It processes outgoing 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.  					



Approved by the Audit Professor/Course Coordinator

***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