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)***

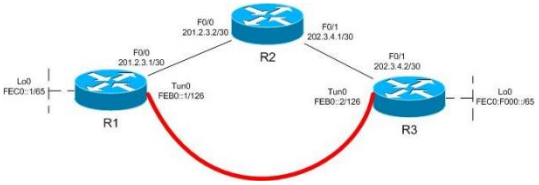
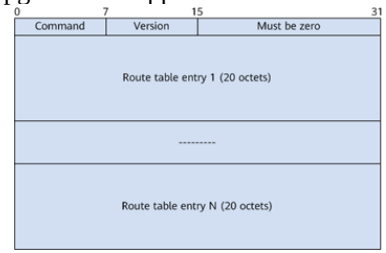
CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	L	H	-	H	L	-	-	-	L	L	-	H
CO2	M	H	-	M	L	-	-	-	M	L	-	H
CO3	M	H	-	H	L	-	-	-	M	L	-	H
CO4	M	H	-	H	L	-	-	-	M	L	-	H
CO5	H	H	-	H	L	-	-	-	M	L	-	H
CO6	L	H	-	H	L	-	-	-	L	L	-	H

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

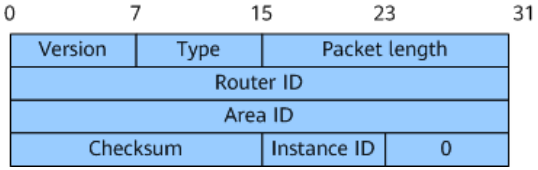
Q. No	Question	Marks	BL	CO	PO	PI Code
1	Which of the following is the shortest valid abbreviation for DE80:0000:0000:0100:0000:0000:0000:0123? a)DE80::100::123 b)DE8::1::123 **c)DE80::100:0:0:0:123** d)DE80:0:0:100::1230	1	L2	4	1	1.6.1
2	The length of IPv6 is _____ bits a)64 b) 32 c)256 **d)128**	1	L1	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

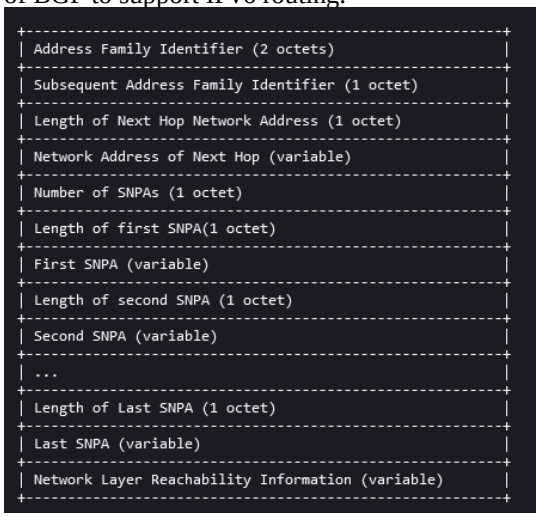
	In the example, the inside host wants to communicate with the outside world and the destination web server. Then it will send a data packet to the NAT-enabled gateway router of the network for further communication.The inside station sends the first packet to the router which is checked for address match 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.



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.



13. a)	i) Imagine the length of a 10Base5 cable is 2500 meters. If the speed of propagation in a thick coaxial cable is 200,000,000 meters/second:	6+4	L4	6	2	2.6.1

a. How long does it take for a bit to travel from the beginning to the end of the network?
b. Find the maximum time it takes to sense a collision (worst case).

ii)The data rate of 10Base5 is 10Mbps. How long does it take to create the smallest frame? Show your calculations.

a. Distance = Velocity × Time

$$Time = \frac{Distance}{Velocity} = \frac{2500m}{200{,}000{,}000m/s} = \mathbf{12.5\mu s}$$

Therefore, it takes 12.5µs for a bit to travel from beginning to the end of the network.

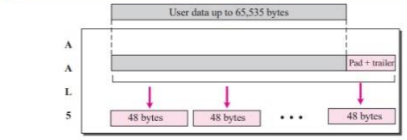
b. Maximum time to sense a collision = 2 × 12.5 μs = **25 μs**

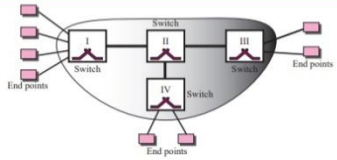
ii) **Answer:**

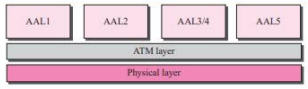
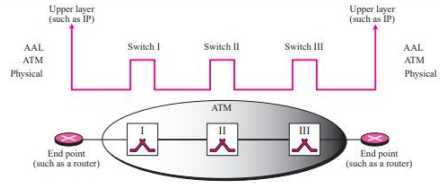
The smallest frame is 64 bytes or 512 bits.
With a data rate of 10 Mbps, we have
Tfr = (512 bits) / (10 Mbps) = 51.2 µs
This means that the time required to send the smallest frame is the same at themaximum time required to detect the collision.

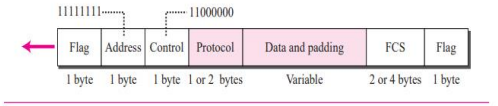
OR

13. b)	i) Find how an IP packet can be encapsulated in ATM cells using AAL5 layer. (4 marks)	10	L3	5,6	2	2.6.4

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

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

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

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

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

Frame Format:

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

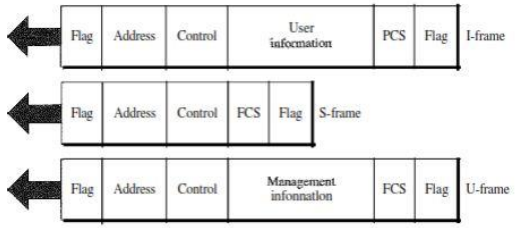


Fig no.29

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

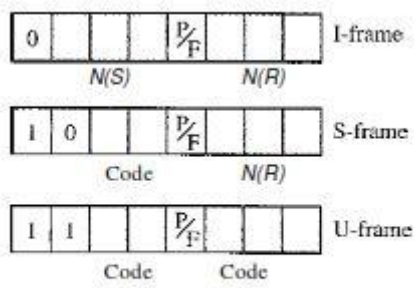


Fig no.30

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

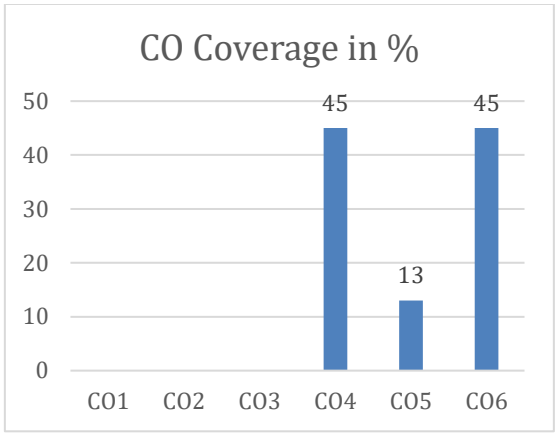
Control Fieldfor S-Frames Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than an acknowledgment). S-frames do not have information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

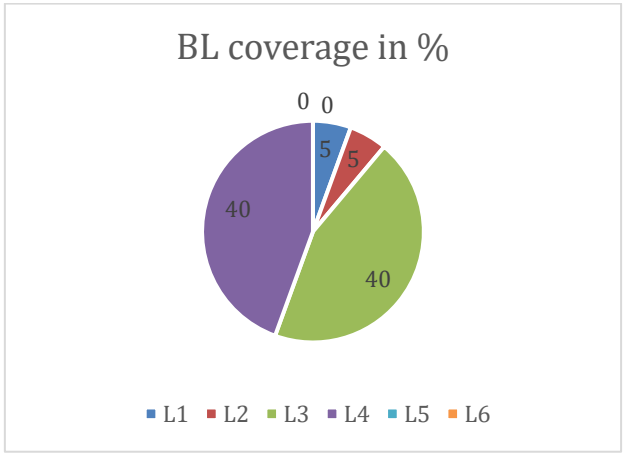
Receive ready (RR): If the value of the code subfield is 00, it is an RR S-frame. This kind of

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

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

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





Approved by the Audit Professor/Course Coordinator