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

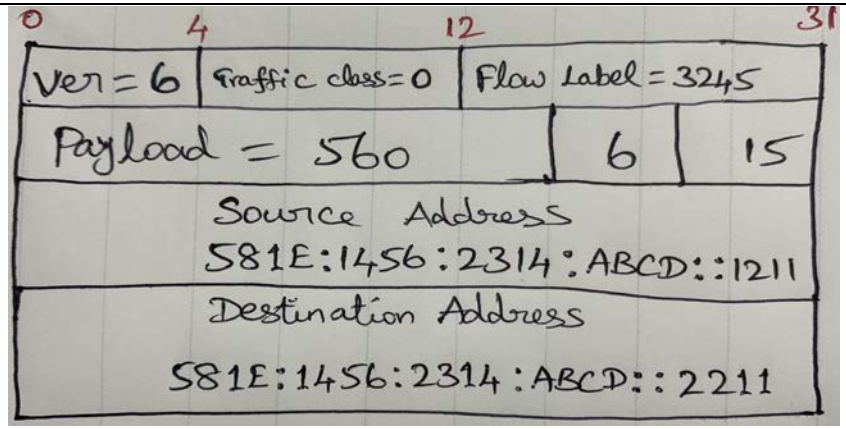
Test: CLA-T3 (ANSWER KEY)
Max. Marks: 50
Course Code & Title: 18CSC302J & COMPUTER NETWORKS

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

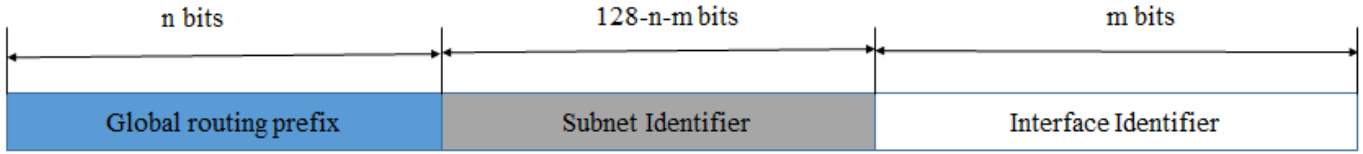
Part – A Instructions: Answer all the questions (1 x 10 = 10 Marks)						
Q. No	**Question**	**Marks**	**BL**	**CO**	**PO**	**PI Code**
1	In the IPv6 header, the traffic class field is similar to which field in the IPv4 header? **D) ToS field**	1	L1	4	1	1.6.1
2	Suppose two IPv6 nodes want to interoperate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

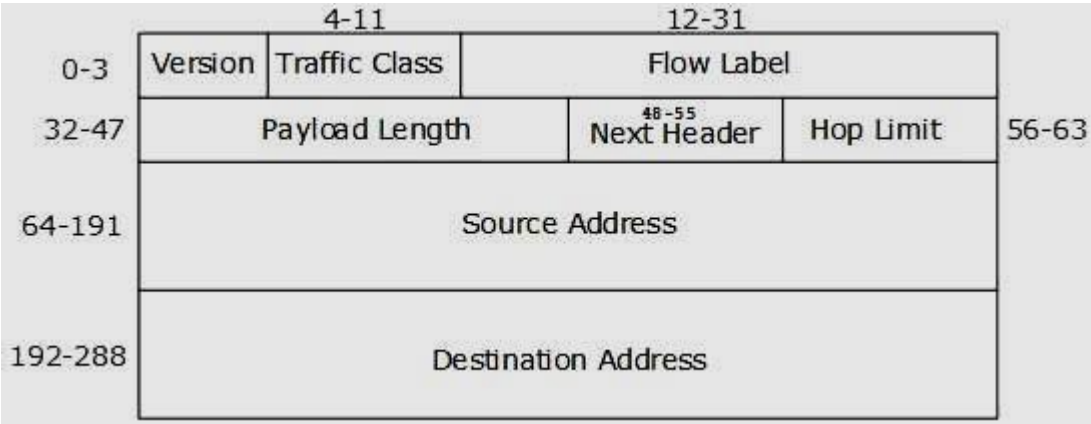
Block Assignment	Length of block
Global routing prefix (n)	48 bits
Subnet Identifier (128-n-m)	16 bits
Interface Identifier	64 bits

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.

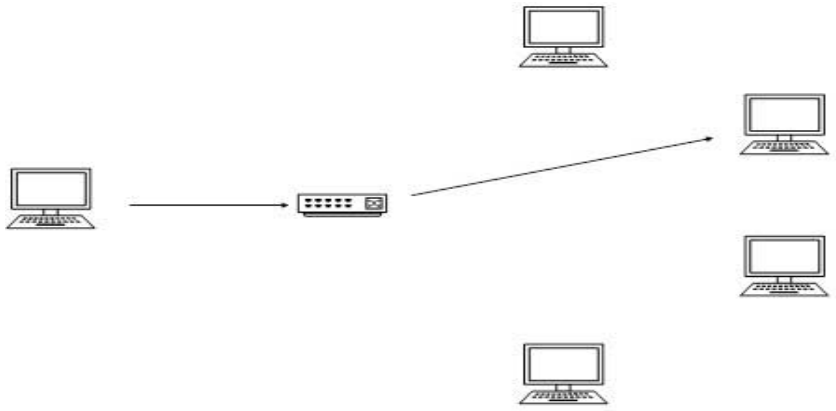
Subnet Identifier :
16 bit block is used to identify the specific subnet of an organization.
An organization can have upto 2^{16} subnets.

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

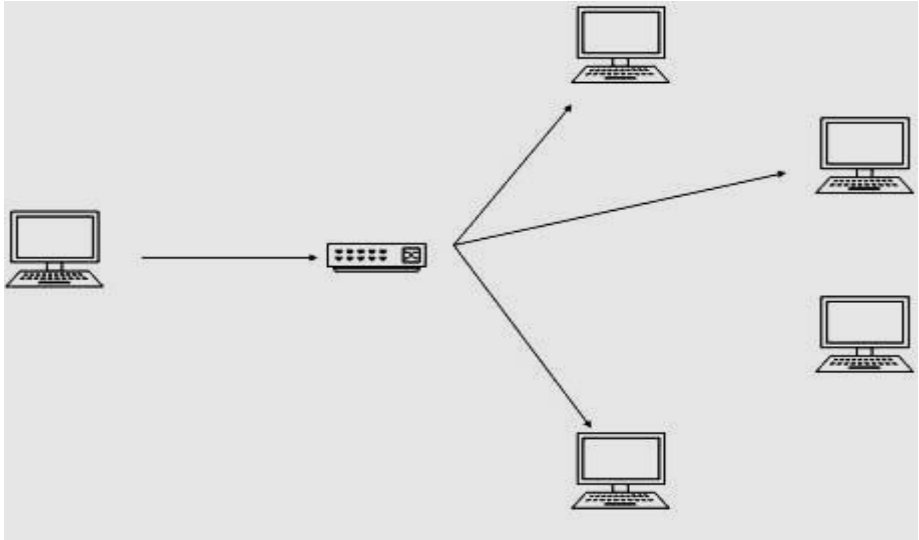
S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this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

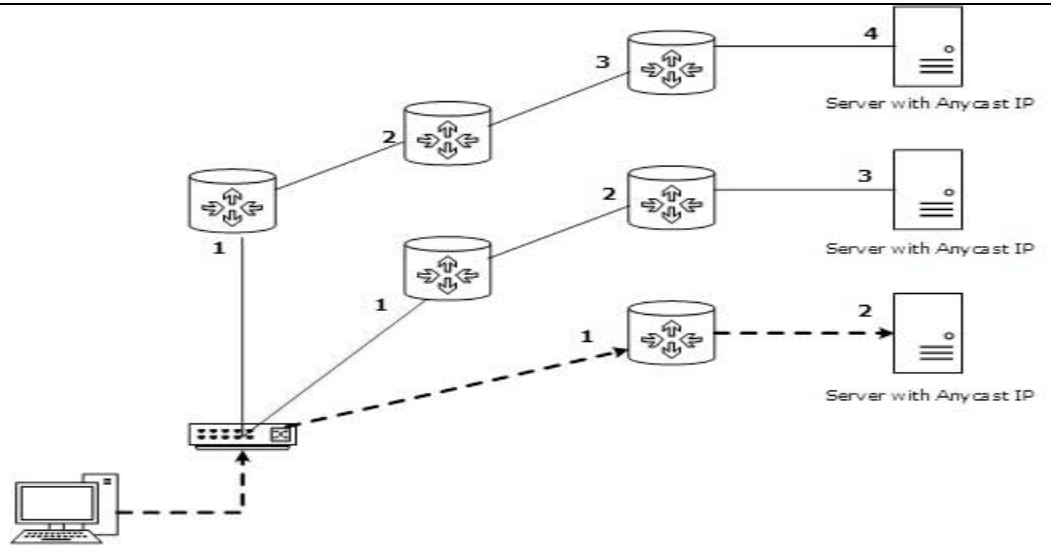
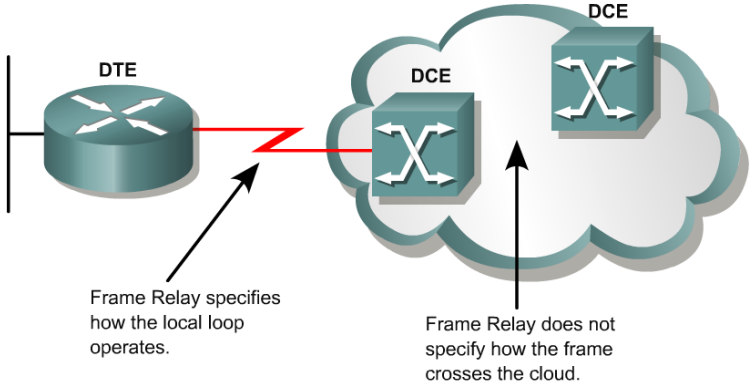
Multicast

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.

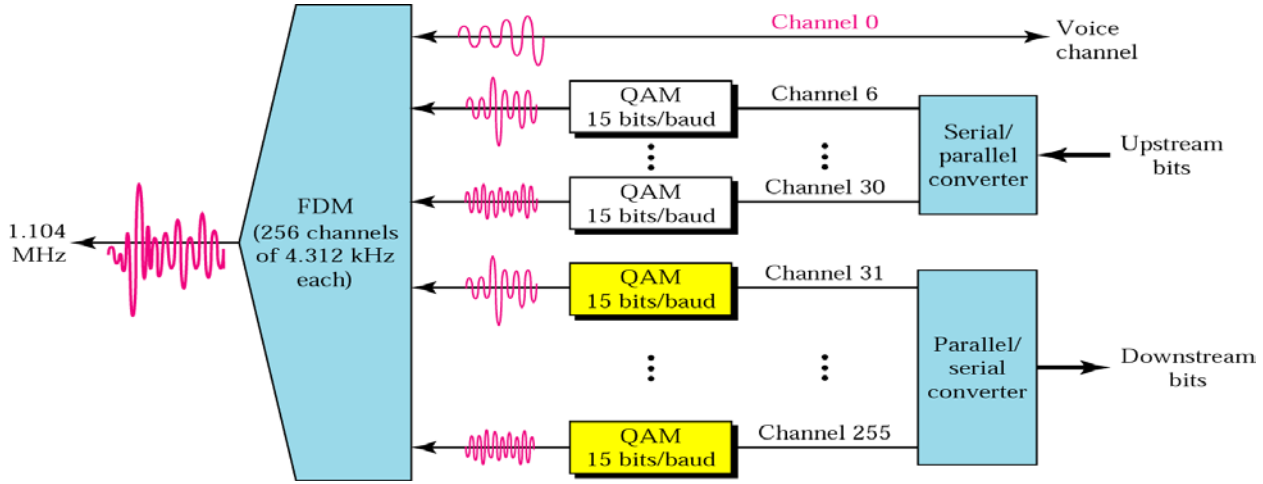


Anycast

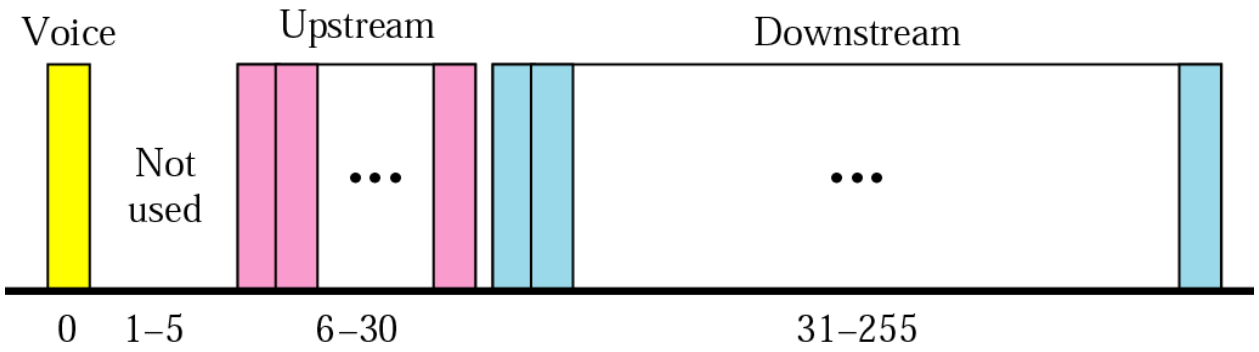
IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message. With the help of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

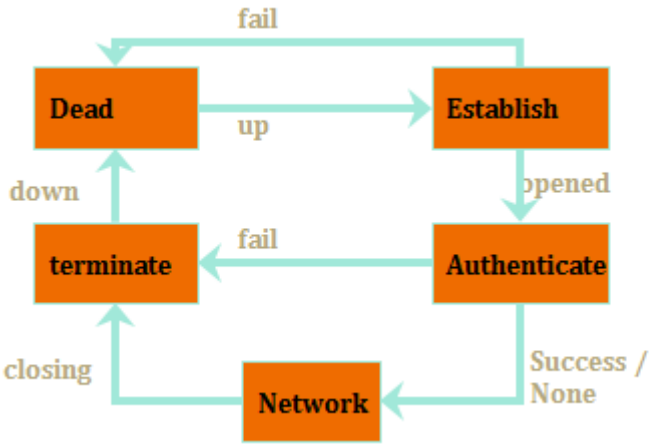
	● In most cases, these are packet switches, which are the devices that actually transmit data through the WAN. ● The connection between the customer and the service provider is known as the **User-to-Network Interface (UNI).** ● The **Network-to-Network Interface (NNI)** is used to describe how Frame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

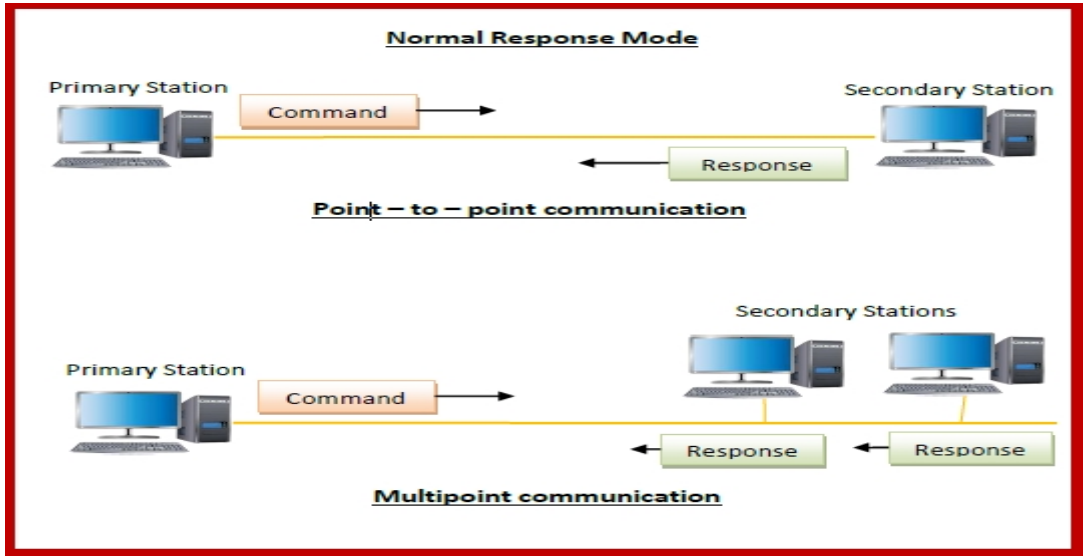
The telephone line or cable companies provide a physical link, but to control and manage the transfer of data, there is a need for a special protocol. The **Point-to-Point Protocol (PPP**) was designed to respond to this need.

	 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.



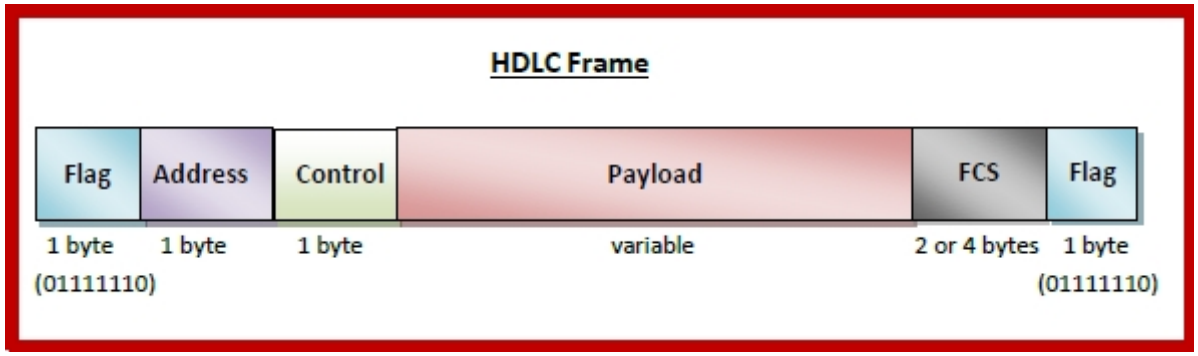
Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.

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)

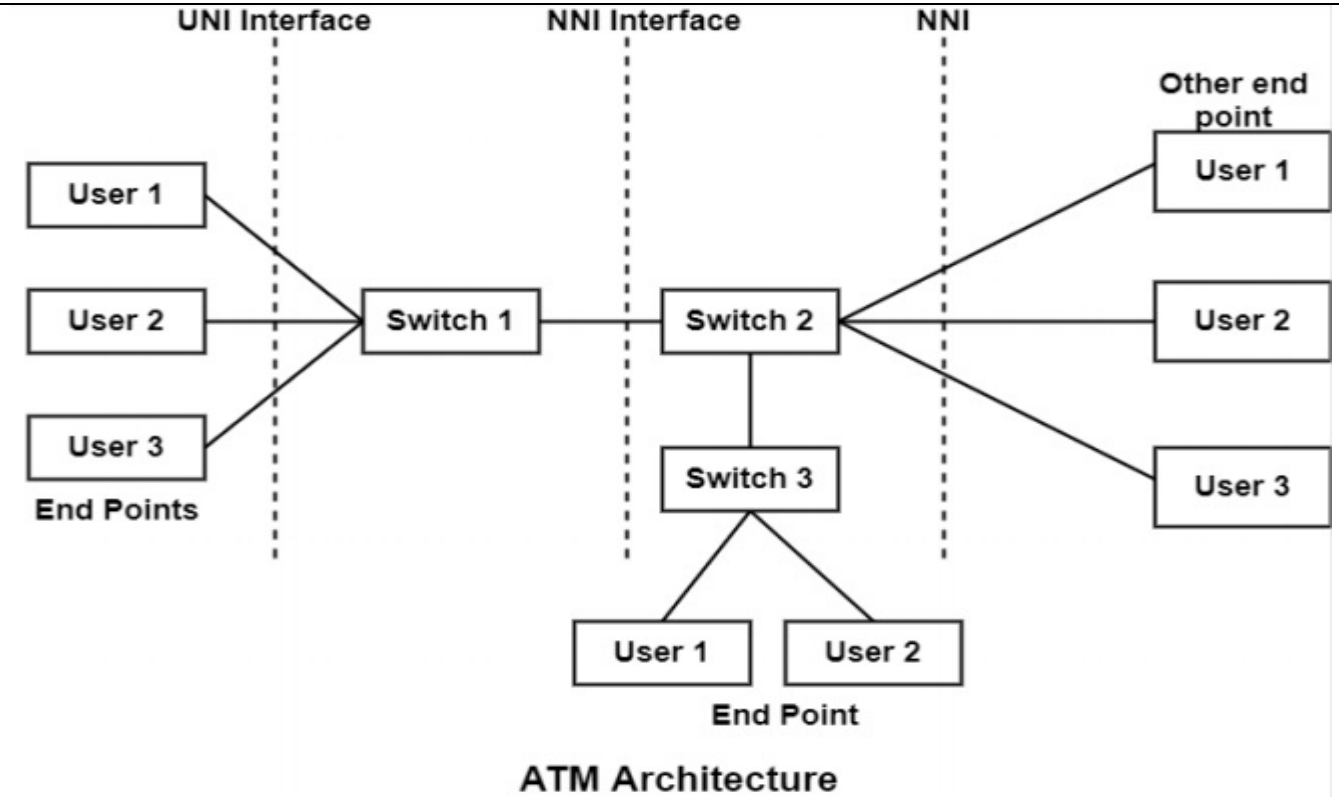


Types of HDLC Frames

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.

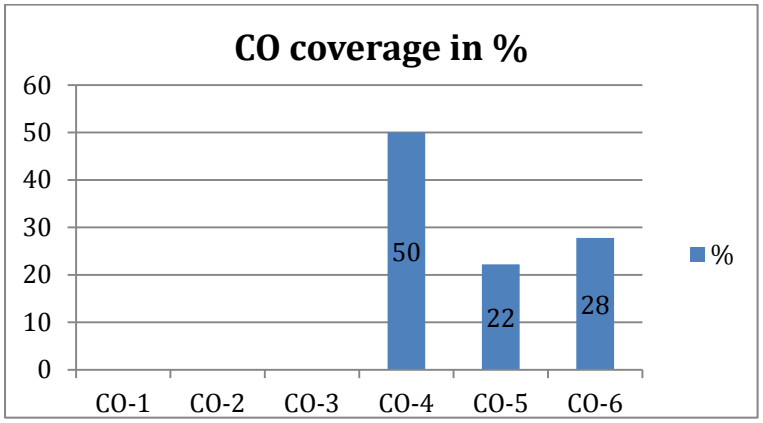
Virtual Path

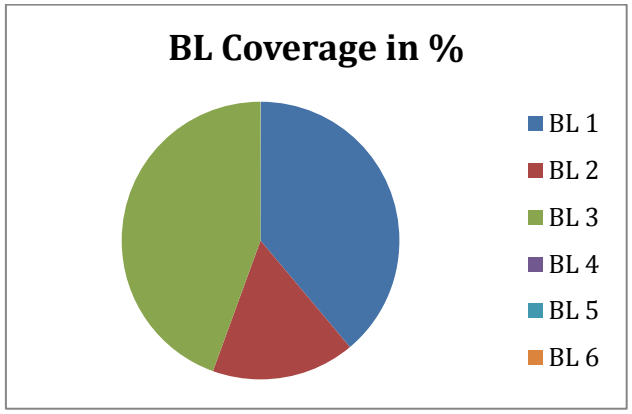
The transmission path is logically divided into separate virtual paths identified using the virtual

	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