

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
COLLEGE OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS LEARNING ASSESSMENT III



Sub Code/Name: 18CSC302J – COMPUTER NETWORKS

Set : EVEN

Class: III Year / V Sem/ B.Tech CSE, CSE Specialization

Date : 03.11.2023

Max Marks: 50

Duration : 90 mins

ANSWER KEY

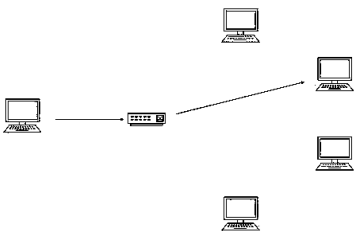
PART - A (10x1= 10)

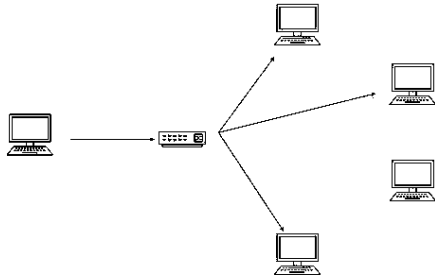
ANSWER ALL THE QUESTIONS

Q.No.	Questions	Marks	CO	BL	PI
1	Two bytes in hexadecimal notation require _____ hexadecimal digits. a) 4 b) 3 c) 5 d) 6	1	4	2	1.6.1
2	In an IPv6 header, the traffic class field is similar to which field in the IPv4 header? a) Fragmentation field b) Fast switching c) TOS field d) Option field	1	4	1	1.6.1
3	IPv6 does not use _____ type of address. a) Broadcast b) Multicast c) Any cast d) Unicast	1	4	1	1.6.1
4	Which term is not related to NAT a) inside local b) outside local c) inside global d) external global	1	5	1	2.6.2
5	Port Address Translation is also termed what? a) NAT Fast b) NAT Static c) NAT Overload d) Overloading Static	1	5	2	1.6.1
6	Which of the following terms is not associated with DSL? a) DSLAM b) CO c) Splitter d) CMTS	1	6	1	1.6.1
7	Home Internet Access is provided by _____ a) DSL b) FTTP c) Cable d) PPP	1	6	1	1.6.1

8	ATM and frame relay are _____ a) virtual circuit networks b) datagram networks c) virtual private networks d) virtual public networks	1	6	1	1.6.1
9	ATM standard defines _____ layers. a) 2 b) 3 c) 4 d) 5	1	6	1	1.6.1
10	PPP consists of _____ components a) Three (encapsulating, the Domain Name system) b) Three (encapsulating, a link control protocol, NCP) c) Two (a link control protocol, Simple Network Control protocol) d) One (Simple Network Control protocol)	1	6	1	1.6.1

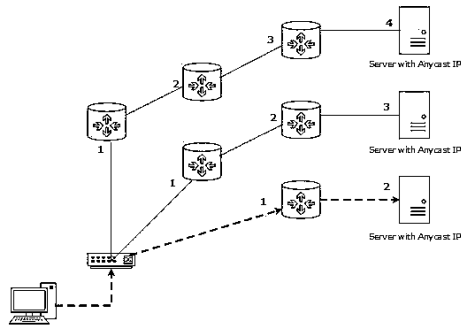
PART - B (4 X 4= 16)
ANSWER ANY FOUR OUT OF SIX QUESTIONS

Q.No.	Question	Marks	CO	BL	PI
11)	<p>Discuss about the types of IPV6 Addressing Modes</p> <p>Addressing mode refers to the mechanism of hosting an address on the network. 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.</p> <p>Unicast:</p> <p>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 interfaces which connects to that particular host.</p>  <p>Multicast:</p> <p>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.</p>	4	4	1	4.4.1



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.



Explain about Global Unicast Addresses.

Global Unicast Address is equivalent to IPv4 public address. Global Unicast Addresses in IPv6 are globally identifiable and uniquely addressable.

Global routing prefix	Subnet ID	interface ID
48 Bits	16 Bits	64 Bits

12)

The Most significant 48-bits are designated as global routing prefix which is assigned to a specific automatic system. The three most significant bits of the global routing prefix are always set to 001.

Global Unicast Address (GUA):

- 2000::/3 (First hexet: 2000::/3 to 3FFF::/3).
- Globally unique and routable.
- Similar to public IPv4 addresses.
- 2001:db8::/32 – RFC 2839 and RFC 6890 reserve this range of addresses for documentation.

4

4

2

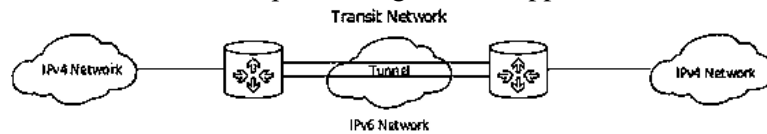
12.5.1

	<div data-bbox="349 163 906 358"><p>Global Unicast Subnet ID</p><p>2001:0db8:0000:0000:a111:b222:c333:abcd</p><p>Global Prefix Interface ID</p></div> <div data-bbox="276 407 995 553"><ul style="list-style-type: none">• 64-bit Interface ID = 18 quintillion (18,446,744,073,709,551,616) devices/subnet.• 16 bit subnet ID (initially recommended) = 65,536 subnets</div> <div data-bbox="223 562 794 593"><p>IPv6 Global Unicast Address Format Fields:</p></div> <div data-bbox="223 600 995 788"><p>1. Global routing prefix: global routing prefix is the portion of the address that is assigned by the provider such as an ISP to a customer or site. The most significant 48-bits are assigned as a Global routing prefix which is assigned to a specific autonomous system.</p></div> <div data-bbox="223 792 995 866"><p>2. Subnet ID: The subnet ID is the portion between the global routing prefix and the interface ID.</p></div> <div data-bbox="223 871 995 981"><p>3. Interface ID: The Interface ID is equal to the host part of an IPv4 address, It is must recommend that in most cases /64 subnets must be used which creates a 64-bit ID.</p></div>				
13	<div data-bbox="223 990 735 1021"><p>Illustrate about IPV4 to IPV6 Tunneling</p></div> <div data-bbox="223 1028 995 1254"><p>Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. It is unlike implementation of other new technologies where the newer one is backward compatible so the older system can still work with the newer version without any additional changes.</p></div> <div data-bbox="223 1258 995 1368"><p>To overcome this short-coming, we have a few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6.</p></div> <div data-bbox="223 1375 472 1406"><p>Dual Stack Routers</p></div> <div data-bbox="223 1413 995 1523"><p>A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.</p></div> <div data-bbox="384 1527 869 1758"><p>The diagram illustrates a dual-stack router setup. On the left, a server icon is shown with two dashed arrows pointing to a central router icon. The top arrow is labeled 'IPv6 Traffic' and the bottom arrow is labeled 'IPv4 Traffic'. The router icon has two circular arrows forming a loop around it. From the router, two solid arrows point to two cloud icons on the right. The top cloud is labeled 'IPv6 Network' and the bottom cloud is labeled 'IPv4 Network'.</p></div> <div data-bbox="223 1765 995 1915"><p>In the above diagram, a server having IPv4 as well as IPv6 address configured for it can now speak with all the hosts on both the IPv4 as well as the IPv6 networks with the help of a Dual Stack Router. The Dual Stack Router, can communicate with both the networks.</p></div>	4	4	3	4.4.1

It provides a medium for the hosts to access a server without changing their respective IP versions.

Tunneling

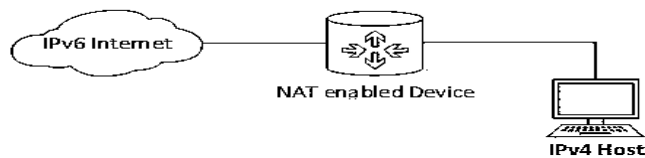
In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through a non-supported IP version.



The above diagram depicts how two remote IPv4 networks can communicate via a Tunnel, where the transit network was on IPv6. Vice versa is also possible where the transit network is on IPv6 and the remote sites that intend to communicate are on IPv4.

NAT Protocol Translation

This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa. See the diagram below:



A host with IPv4 address sends a request to an Ipv6 enabled server on Internet that does not understand Ipv4 address. In this scenario, the NAT-PT device can help them communicate. When the Ipv4 host sends a request packet to the Ipv6 server, the NAT-PT device/router strips down the Ipv4 packet, removes Ipv4 header, and adds Ipv6 header and passes it through the Internet. When a response from the Ipv6 server comes for the Ipv4 host, the router does vice versa.

Compare and Contrast DSL Vs Cable

Cable	DSL
Raw speed is 30 Mbps, but is reduced to 20-25 Mbps when sharing bandwidth.	From 128 Kbps to over 100 Mbps (using latest DSL standards such as VDSLv2).
Shared-speed varies depending on the number of subscribers on the network	Not shared-Constant Speed
Home Networking: Possible	Home Networking: Possible
Need Security software	Need Security software from ISP
Costs around the same as DSL, but gives a better speed to cost ratio, making it effectively cheaper than DSL.	Costs the same as cable, but is significantly slower compared to cable, making it more expensive in effect.

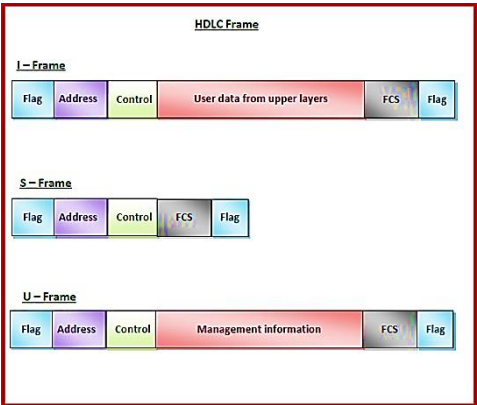
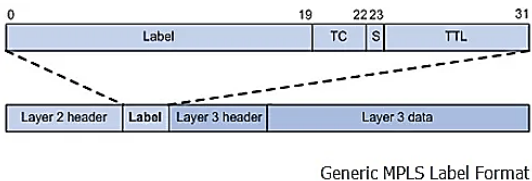
14)

4

6

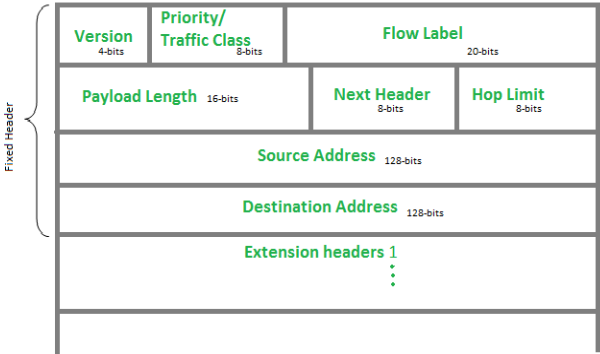
1

2.6.4

15	<p>Describe the types of HDLC Frame</p> <p><i>Types of HDLC Frames</i></p> <p>There are three types of HDLC frames. The type of frame is determined by the control field of the frame –</p> <ul style="list-style-type: none"> • 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. 	4	5	1	2.7.1
16)	<p>Summarize about MPLS frame format.</p>  <p>MPLS label format or MPLS frame format. As shown a MPLS label is inserted between layer 2 header and layer 3 header of any packet. It is four bytes in size and consists of following fields.</p> <ul style="list-style-type: none"> • Label: 20 bit size label value • TC: 3 bit in size. It defines class of service. It is used for QoS. • S (Stack): 1 bit in size. A label stack can comprise multiple labels. The label nearest to the Layer 2 header is called "top label". The label nearest to the Layer 3 header is called "bottom label". 	4	5	2	1.6.1

	<p>The S field is set to value 1 if the label is bottom label and set to 0 for all other label stack entries.</p> <ul style="list-style-type: none"> • TTL (Time to Live): 8 bit in size, It is used for routing loop prevention. 				
--	--	--	--	--	--

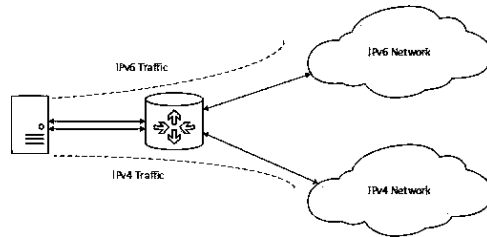
PART - C (2 X 12= 24)
ANSWER ALL THE QUESTIONS

Q.No.	Question	Marks	CO	BL	PI
17.a	<p>Explain about IPV6 Packet Format and Extension Headers?</p> <p>IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let's look at the header of IP version 6 and understand how it is different from the IPv4 header.</p> <p>IP version 6 Header Format :</p>  <p>Version (4-bits): Indicates version of Internet Protocol which contains bit sequence 0110.</p> <p>Traffic Class (8-bits): The Traffic Class field indicates class or priority of IPv6 packet which is similar to <i>Service Field</i> in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet.</p> <p>Flow Label (20-bits): Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service.</p> <p>Payload Length (16-bits): It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload.</p> <p>Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header.</p>	12	4	2	2.6.2

	<p>Hop Limit (8-bits): Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.</p> <p>Source Address (128-bits): Source Address is the 128-bit IPv6 address of the original source of the packet.</p> <p>Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.</p> <p>Extension Headers: In order to rectify the limitations of the <i>IPv4 Option Field</i>, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.</p> <div><div><div>IPv6 Header</div><div>Next Header</div></div><div><div>Extension Header 1</div><div>Next Header</div></div><div><div>Extension Header 2</div><div>Next Header</div></div><div><div>Extension Header n</div><div>Next Header</div></div><div><div>Upper Layer Data</div></div></div> <p>IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:</p> <table><thead><tr><th>Order</th><th>Header Type</th><th>Next Header Code</th></tr></thead><tbody><tr><td>1</td><td>Basic IPv6 Header</td><td>-</td></tr><tr><td>2</td><td>Hop-by-Hop Options</td><td>0</td></tr><tr><td>3</td><td>Destination Options (with Routing Options)</td><td>60</td></tr><tr><td>4</td><td>Routing Header</td><td>43</td></tr><tr><td>5</td><td>Fragment Header</td><td>44</td></tr><tr><td>6</td><td>Authentication Header</td><td>51</td></tr><tr><td>7</td><td>Encapsulation Security Payload Header</td><td>50</td></tr><tr><td>8</td><td>Destination Options</td><td>60</td></tr><tr><td>9</td><td>Mobility Header</td><td>135</td></tr><tr><td></td><td>No next header</td><td>59</td></tr><tr><td>Upper Layer</td><td>TCP</td><td>6</td></tr><tr><td>Upper Layer</td><td>UDP</td><td>17</td></tr><tr><td>Upper Layer</td><td>ICMPv6</td><td>58</td></tr></tbody></table> <div><p>Example: TCP is used in IPv6 packet</p><div><div>Next Header= 6</div><div>TCP header</div><div>TCP data</div></div><p>Example2:</p><div><div>Next Header= 43</div><div>Routing Extension Header</div><div>Next Header= 6</div><div>TCP header</div><div>TCP data</div></div></div>	Order	Header Type	Next Header Code	1	Basic IPv6 Header	-	2	Hop-by-Hop Options	0	3	Destination Options (with Routing Options)	60	4	Routing Header	43	5	Fragment Header	44	6	Authentication Header	51	7	Encapsulation Security Payload Header	50	8	Destination Options	60	9	Mobility Header	135		No next header	59	Upper Layer	TCP	6	Upper Layer	UDP	17	Upper Layer	ICMPv6	58				
Order	Header Type	Next Header Code																																													
1	Basic IPv6 Header	-																																													
2	Hop-by-Hop Options	0																																													
3	Destination Options (with Routing Options)	60																																													
4	Routing Header	43																																													
5	Fragment Header	44																																													
6	Authentication Header	51																																													
7	Encapsulation Security Payload Header	50																																													
8	Destination Options	60																																													
9	Mobility Header	135																																													
	No next header	59																																													
Upper Layer	TCP	6																																													
Upper Layer	UDP	17																																													
Upper Layer	ICMPv6	58																																													
OR																																															
17.b	<p>Illustrate about IPV4 to IPV6 Tunneling</p> <p>Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. It is unlike implementation of other new technologies where the newer one is backward compatible so the older system can still work with the newer version without any additional changes.</p> <p>To overcome this short-coming, we have a few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6.</p>	12	5	2	1.6.1																																										

Dual Stack Routers

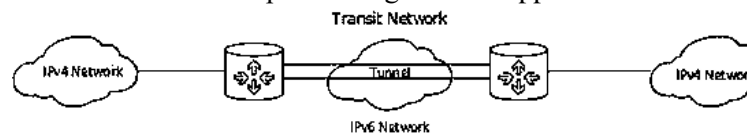
A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.



In the above diagram, a server having IPv4 as well as IPv6 address configured for it can now speak with all the hosts on both the IPv4 as well as the IPv6 networks with the help of a Dual Stack Router. The Dual Stack Router, can communicate with both the networks. It provides a medium for the hosts to access a server without changing their respective IP versions.

Tunneling

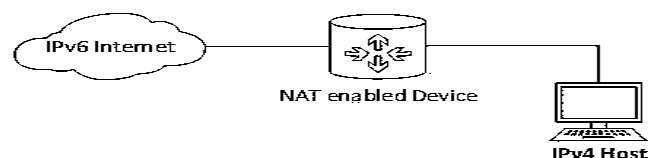
In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through a non-supported IP version.



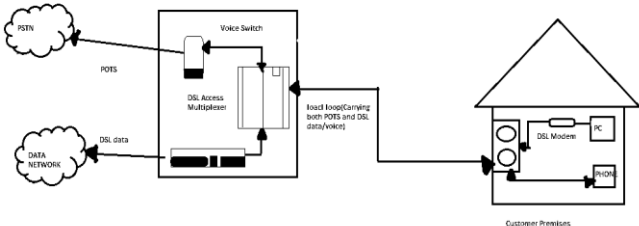
The above diagram depicts how two remote IPv4 networks can communicate via a Tunnel, where the transit network was on IPv6. Vice versa is also possible where the transit network is on IPv6 and the remote sites that intend to communicate are on IPv4.

NAT Protocol Translation

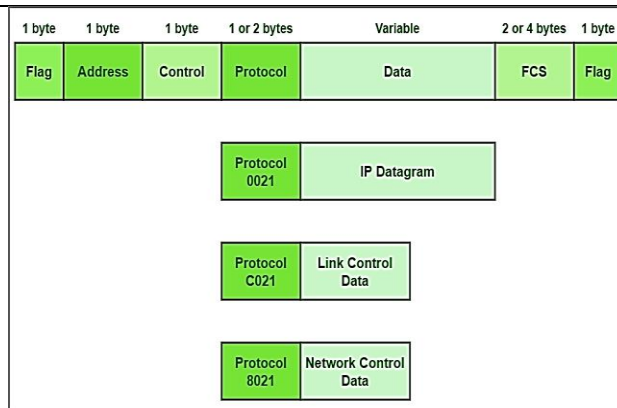
This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa. See the diagram below:



A host with IPv4 address sends a request to an Ipv6 enabled server on Internet that does not understand Ipv4 address. In this scenario, the NAT-PT device can help them communicate. When the Ipv4 host sends a request packet to the Ipv6 server, the NAT-PT device/router strips down the Ipv4 packet,

	removes Ipv4 header, and adds Ipv6 header and passes it through the Internet. When a response from the Ipv6 server comes for the Ipv4 host, the router does vice versa.				
18.a	<p>Describe in detail about DSL Technology in detail with neat sketch and its benefits?</p> <p>DSL (Digital Subscriber Line, originally, Digital Subscriber Loop) is a technology where a DSL line is used to connect to the internet and transmit digital data through copper telephone lines. DSL has been one of the most popular ways ISPs (Internet Service Providers) provide DSL broadband or DSL internet connection to the internet users.</p> <p>How does DSL work?</p> <p>DSL providers bring a network connection into your home or business through telephone lines, allowing you to use the internet and make telephone calls at the same time. This aspect is the main advancement from the dial-up, where you could do only one activity (internet or call) at a time.</p> <p>It works so because the DSL technology divides the telephone signals into three bands of frequencies. While one band facilitates telephone calls, the other two bands connect you to the internet through the process of uploading and downloading online activity.</p> <p>DSL companies provide hardware, similar to the cable modem, called a DSL transceiver to its subscribers. This hardware only works for DSL connections, and in many cases only the connections provided by the same ISP.</p> <p>The modem connected to the computer separates the voice from data (bands) as explained above and as shown in the below diagram. You can also connect Ethernet to DSL to connect your local network to a DSL network.</p>  <p>In a DSL network, the telephone lines will run from your wall to the outside to the ISP hub. The DSL cables that are used to send data back and forth are mostly ADSL lines. The Asynchronous DSL means that one side of the line (download) is bigger than the other side (upload). What ADSL does is fast downloads and slow to moderate speed uploads, which is what is commonly in demand.</p>	12	6	3	2.6.3

	<p>The two primary types of DSL connections are – asymmetric (ADSL) and symmetric (SDSL) while ADSL is cheaper and more popular because of its faster download speed than upload speed, the download and upload speeds are equal in SDSL, which professionals who have to back up large volumes of data to the cloud and VPN users prefer over ADSL.</p> <p>One important thing to note here is that the more distant your connection is from the Service Provider hub, the quality and speed of your dial-up connection will be poor. That means the speed and quality of the connections that are closer to the ISP hub will be better.</p> <p>Benefits:</p> <p>It allows you to make phone calls and connect to internet simultaneously</p> <ul style="list-style-type: none"> • It's faster and provides a consistent and stable internet speed • You can select the suitable price plan, based on the speed you want • There is no need for additional wiring as a DSL connection makes use of your existing telephone wiring • DSL internet is still a very cost-effective option as compared to the other available options 				
OR					
18.b	<p>Illustrate in detail about the PPP Frame Format and its 3 main components.</p> <p>PPP Frame Format : PPP frame is generally required to encapsulate packets of information or data that simply includes either configuration information or data. PPP basically uses the same basic format as that of HDLC. PPP usually contains one additional field i.e. protocol field. This protocol field is present just after control field and before information or data field.</p>	12	6	3	2.7.1



PPP Frame Format

Various fields of Frame are given below :

1. **Flag field** – PPP frame similar to HDLC frame, always begins and ends with standard HDLC flag. It always has a value of 1 byte i.e., 01111110 binary value.
2. **Address field** – Address field is basically broadcast address. In this, all 1's simply indicates that all of the stations are ready to accept frame. It has the value of 1 byte i.e., 11111111 binary value. PPP on the other hand, does not provide or assign individual station addresses.
3. **Control field** – This field basically uses format of U-frame i.e., Unnumbered frame in HDLC. In HDLC, control field is required for various purposes but in PPP, this field is set to 1 byte i.e., 00000011 binary value. This 1 byte is used for a connection-less data link.
4. **Protocol field** – This field basically identifies network protocol of the datagram. It usually identifies the kind of packet in the data field i.e., what exactly is being carried in data field. This field is of 1 or 2 bytes and helps in identifies the PDU (Protocol Data Unit) that is being encapsulated by PPP frame.
5. **Data field** – It usually contains the upper layer datagram. Network layer datagram is particularly encapsulated in this field for regular PPP data frames. Length of this field is not constant rather it varies.
6. **FCS field** – This field usually contains checksum simply for identification of errors. It can be either 16 bits or 32 bits in size. It is also calculated over address, control, protocol, and even information fields. Characters are added to frame for control and handling of errors.

	<p><i>Components of PPP</i></p> <p>Point - to - Point Protocol is a layered protocol having three components –</p> <ul style="list-style-type: none"> • Encapsulation Component – It encapsulates the datagram so that it can be transmitted over the specified physical layer. • Link Control Protocol (LCP) – It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links. • Authentication Protocols (AP) – These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are – <ul style="list-style-type: none"> ○ Password Authentication Protocol (PAP) ○ Challenge Handshake Authentication Protocol (CHAP) • Network Control Protocols (NCPs) – These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are – <ul style="list-style-type: none"> ○ Internet Protocol Control Protocol (IPCP) ○ OSI Network Layer Control Protocol (OSINLCP) ○ Internetwork Packet Exchange Control Protocol (IPXCP) ○ DECnet Phase IV Control Protocol (DNCP) ○ NetBIOS Frames Control Protocol (NBFCP) ○ IPv6 Control Protocol (IPV6CP) 				
--	--	--	--	--	--

Prepared by

Ms. S. Abirami

Course coordinator

Dr. S.S.Sathya

HOD/CSE

Dr. K. Raja

