Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058, India

(Autonomous College Affiliated to University of Mumbai)

End Semester Examination

May-6/06/2018

Max. Marks: 100 Duration: 3 Hr

Class: T.E. Semester: VI

Course Code: ETC603 Branch: Electronics and Telecommunication

Name of the Course: Computer Communication Telecom Networks

Instruction:

(1) All questions Q1-Q5 are compulsory

(1) Attempt any Four from Q1

(2) Assume suitable data if necessary

(3) Draw neat diagrams

Q No.		Max. Marks	CO
Q.1 (a)		1*5=5	CO1
Q.1 (b)		5	CO4
Q.1 (c)		5	CO5

Circuit Switching	Packet Switching
Physical path between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Supports store and forward transmission

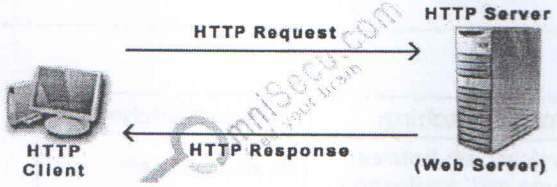
1. The sequence number of any packet can be found using the following relation:

$$\text{seqNo} = (\text{starting segNo} + \text{packet number} - 1) \bmod 2^m$$

in which m is the number of bits used to define the sequence number. The sequence number in this case is

$$\text{seqNo} = (0 + 100 - 1) \bmod 2^5 = 99 \bmod 32 = 3$$

The operation of Hypertext Transfer Protocol (HTTP) involves the communication between a Hypertext Transfer Protocol (HTTP) client application (Usually web browser) and a Hypertext Transfer Protocol (HTTP) server application (Web servers like IIS). Hypertext Transfer Protocol (HTTP) uses Transmission Control Protocol (TCP) as the Transport Layer Protocol at Well Known port number 80. Once the TCP connection is established, the two steps in Hypertext Transfer Protocol (HTTP) communication are 1) HTTP Client Request: Hypertext Transfer Protocol (HTTP) client sends an Hypertext Transfer Protocol (HTTP) Request to the Hypertext Transfer Protocol (HTTP) Server according to the HTTP standard, specifying the information the client like to retrieve from the Hypertext Transfer Protocol (HTTP) Server. 2) HTTP Server Response: Once the Hypertext Transfer Protocol (HTTP) Request arrived at the Hypertext Transfer Protocol (HTTP) server, it will process the request and creates an Hypertext Transfer Protocol (HTTP) Response message. The Hypertext Transfer Protocol (HTTP) response message may contain the resource the Hypertext Transfer Protocol (HTTP) Client requested or information why the Hypertext Transfer Protocol (HTTP) request failed.



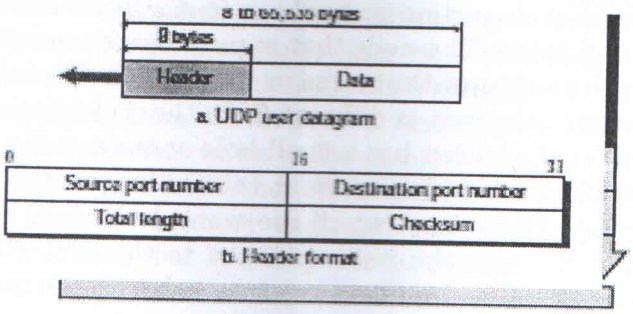
Q.1(d) 5 CO2

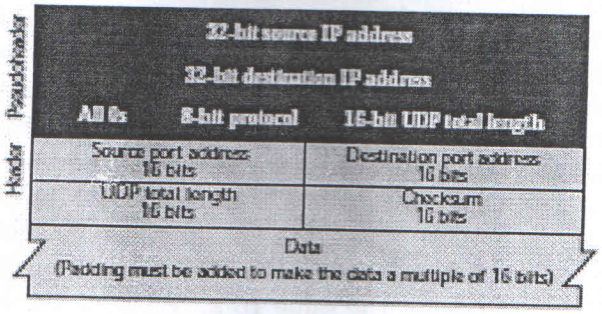
Sr no.	FDM	TDM
1.	The signals which are to be multiplexed are added in the time domain. But they occupy different slots in the frequency domain.	The signals which are to be multiplexed can occupy the entire bandwidth in the time domain.
2.	FDM is usually preferred for the analog signals.	TDM is preferred for the digital signals.
3.	Synchronization is not required.	Synchronization is required.
4.	The FDM requires a complex circuitry at Tx and Rx.	TDM circuitry is not very complex.
5.	FDM suffers from the problem of crosstalk due to imperfect BPF.	In TDM the problem of crosstalk is not severe.
6.	Due to bandwidth fading in the Tx medium, all the FDM channels are affected.	Due to fading only a few TDM channels will be affected.
7.	Due to slow narrowband fading taking place in the transmission channel may be affected in FDM.	Due to slow narrowband fading all the TDM channels may get wiped out.

Q.1(e) 5 CO2

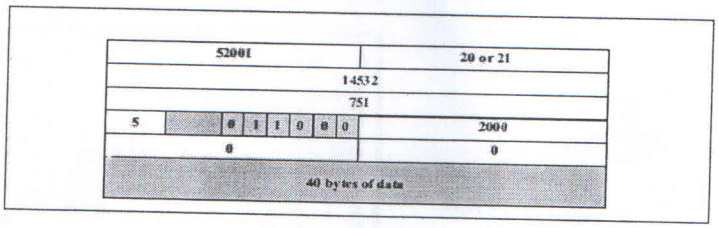
Source port number. This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535. If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host. If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number. Destination port number. This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number. If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number. In this case, the server copies the ephemeral port number it has received in the request packet. Length. This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be much less because a UDP user datagram is stored in an IP datagram with the total length of 65,535 bytes. The length field in a UDP user datagram is actually not necessary. A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram that defines the total length. There is another field in the IP datagram that defines the length of the header. So if we subtract the value of the second field from the first, we can deduce the length of the UDP datagram that is encapsulated in an IP datagram. However, the designers of the UDP protocol felt that it was more efficient for the destination UDP to calculate the length of the data from the information provided in the UDP user datagram rather than ask the IP software to supply this information. when the IP software delivers the UDP user datagram to the UDP layer, it has already dropped the IP header. Checksum. This field is used to detect errors over the entire user datagram (headerplus data). The pseudoheader is the part of the header of the IP packet in which the user datagram is to be encapsulated with some fields filled with 0s.If the checksum does not include the pseudoheader, a user datagram may arrive safe and sound. However, if the IP header is corrupted, it may be delivered to the wrong host. The protocol field is added to ensure that the packet belongs to UDP, and not to TCP. We will see later that if a process can use either UDP or TCP, the destination port number can be the same. The value of the protocol field for UDP is 17. If this value is changed during transmission, the checksum calculation at the receiver will detect it and UDP drops the packet. It is not delivered to the wrong protocol.

	Framing: Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer. 2.Physical Addressing: The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network. 3.Flow Control: A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side. 4.Error Control: Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames. 5.Access Control: Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.		
Q.1 (f)	Solution: a.The source port number is 0532 in hex and 1330 in decimal. b. The destination port number is 0017 in hex and 23 in decimal. c. The sequence number is 00000001 in hex and 1 in decimal. d. The acknowledgment number is 00000000 in hex and 0 in decimal. e. The HLEN = 5. The header is 5 4 = 20 bytes long.	5	CO2
Q.2 (a)		10	CO4



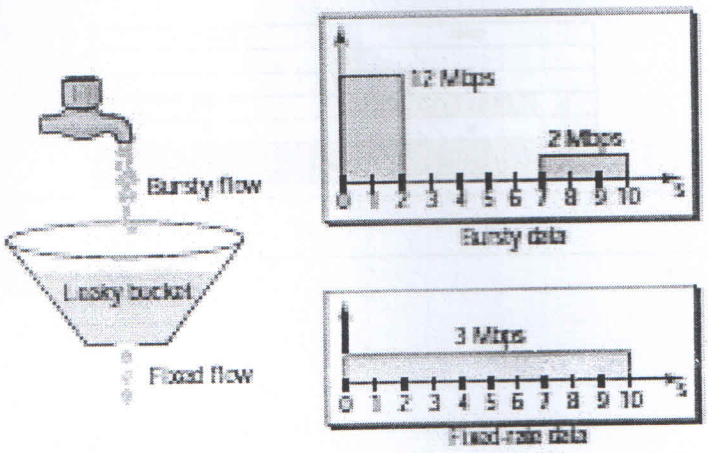


Q.2 (a)	OR	10	CO4



Q.2 (b)		2+8=10	CO4

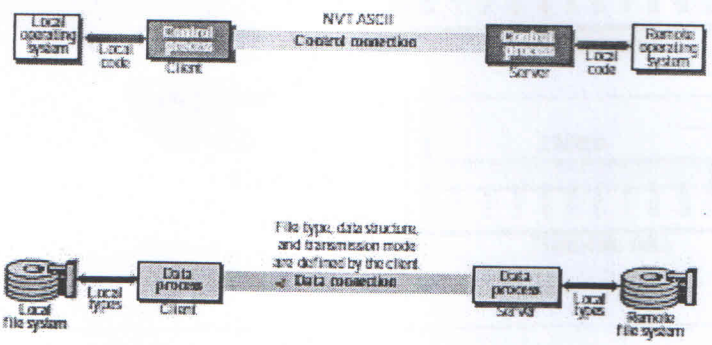
Implicit -In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. Explicit-The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method Leaky Bucket If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate. Figure 25.32 shows a leaky bucket and its effects. In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In Figure 25.32 the host sends a burst of data at a rate of 12 Mbps for 2 s,for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in 10 s. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10 s. Without the leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host. We can also see that the leaky bucket may prevent congestion. As an analogy, consider the freeway during rush hour (bursty traffic). If, instead, commuters could stagger their working hours, congestion on our freeways could be avoided



Q.3 (a)		4	CO5

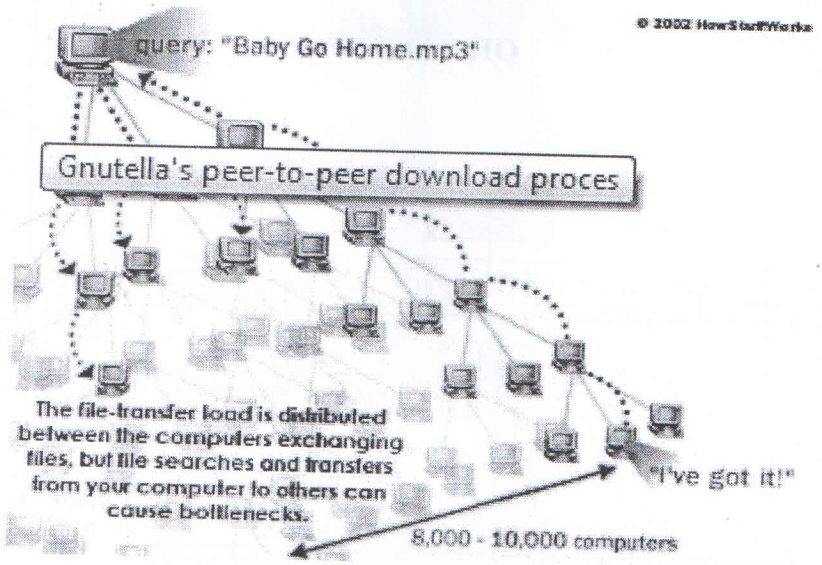
	Caching Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address. Reduction of this search time would increase efficiency. DNS handles this with a mechanism called caching. When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client. If the same or another client asks for the same mapping, it can check its cache memory and resolve the problem. However, to inform the client that the response is coming from the cache memory and not from an authoritative source, the server marks the response as unauthoritative. Caching speeds up resolution, but it can also be problematic. If a server caches a mapping for a long time, it may send an outdated mapping to the client. To counter this, two techniques are used. First, the authoritative server always adds information to the mapping called time-to-live (TTL). It defines the time in seconds that the receiving server can cache the information. After that time, the mapping is invalid and any query must be sent again to the authoritative server. Second, DNS requires that each server keep a TTL counter for each mapping it caches. The cache memory must be searched periodically and those mappings with an expired TTL must be purged.		
Q .3(a)	**OR** solution: PQDN (It does not end with dot.) b. FQDN (It does end with dot.) c. PQDN (It does not end with dot.) d. FQDN (It does end with dot.)	4	CO5
Q.3 (b)		8	CO5

Communication The FTP client and server, which run on different computers, must communicate with each other. These two computers may use different operating systems, different character sets, different file structures, and different file formats. FTP must make this heterogeneity compatible. FTP has two different approaches, one for the control connection and one for the data connection. We will study each approach separately. Communication over Control Connection FTP uses the same approach as TELNET or SMTP to communicate across the control connection. It uses the NVT ASCII character set (see Figure 21.4). Communication is achieved through commands and responses. This simple method is adequate for the control connection because we send one command (or response) at a time. Each command or response is only one short line so we need not worry about file format or file structure. Each line is terminated with a two-character (carriage return and line feed)end-of-line token. Communication over Data Connection-The purpose and implementation of the data connection are different from that of the control connection. We want to transfer files through the data connection. The client must define the type of file to be transferred, the structure of the data, and the transmission mode.Before sending the file through the data connection, we prepare for transmission through the control connection. The heterogeneity problem is resolved by defining three attributes of communication: file type, data structure, and transmission mode File Type FTP can transfer one of the following file types across the data connection: ASCII file. EBCDIC file. Image file. Data Structure File structure (default). The file has no structure. It is a continuous stream of bytes. Record structure. The file is divided into records. This can be used only with text files. Page structure. The file is divided into pages, with each page having a page number and a page header. The pages can be stored and accessed randomly or sequentially. Transmission Mode Stream mode. This is the default mode. Data are delivered from FTP to TCP as a continuous stream of bytes. Block mode. Data can be delivered from FTP to TCP in blocks. Compressed mode. If the file is big, the data can be compressed.

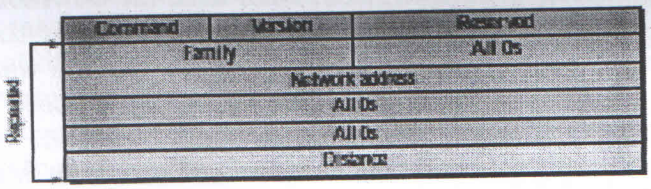


Q.3 (c) 8 CO5

Peer-to-peer file sharing is different from traditional file downloading. In peer-to-peer sharing, use a software program (rather than your Web browser) to locate computers that have the file you want. Because these are ordinary computers like yours, as opposed to servers, they are called peers. The process works like this: run peer-to-peer file-sharing software on computer and send out a request for the file you want to download. • To locate the file, the software queries other computers that are connected to the Internet and running the file-sharing software. • When the software finds a computer that has the file you want on its hard drive, the download begins. • Others using the file-sharing software can obtain files they want from your computer's hard drive. The file-transfer load is distributed between the computers exchanging files, but file searches and transfers from your computer to others can cause bottlenecks. Some people download files and immediately disconnect without allowing others to obtain files from their system, which is called leeching. This limits the number of computers the software can search for the requested file.



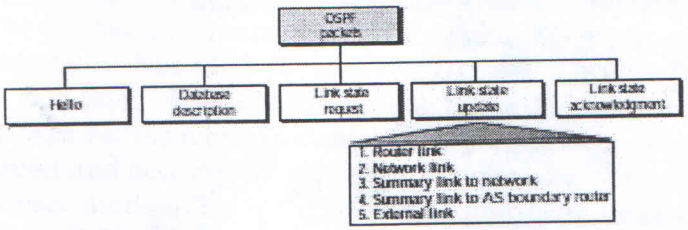
Q.4 (a)	RIP v1 uses what is known classful routing. Classful addressing is the use of Class A, Class B, and Class C addresses. (Class D is reserved for multicasts, and Class E is reserved for future use.)RIP v2 is a classless protocol and it supports classful, variable-length subnet masking (VLSM), CIDR, and route summarization.RIPv2 supports authentication of RIPv2 update messages. Authentication helps in confirming that the updates are coming from authorized sources. It also supports multicast routing updates to reduce resource consumption (as opposed to using broadcasting in RIP v1).RIP v2 can be useful in small, flat networks or at the edge of larger networks because of its simplicity in configuration and usage.	2+6=8	CO3

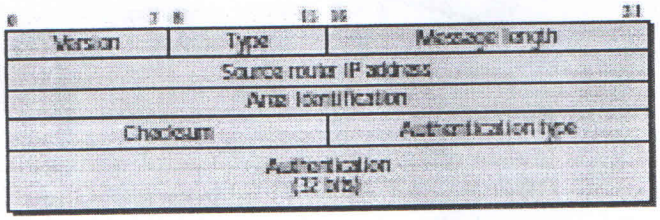


Command. This 8-bit field specifies the type of message: request (1) or response (2). Version. This 8-bit field defines the version. In this book we use version 1, but at the end of this section, we give some new features of version 2. Family. This 16-bit field defines the family of the protocol used. For TCP/IP the value is 2. Network address. The address field defines the address of the destination network. RIP has allocated 14 bytes for this field to be applicable to any protocol.However, IP currently uses only 4 bytes. The rest of the address is filled with 0s. Distance. This 32-bit field defines the hop count (cost) from the advertising router to the destination network.

OR

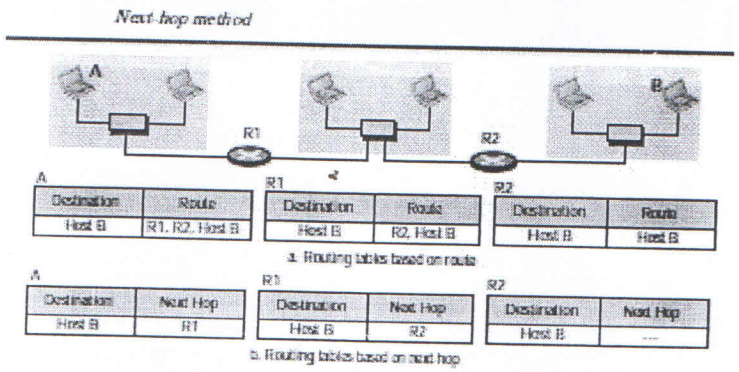
Q.4 (a) 2+6=8 CO3

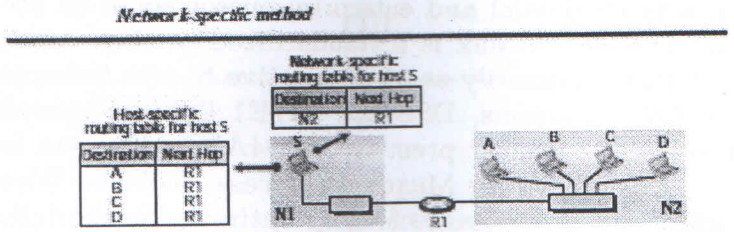


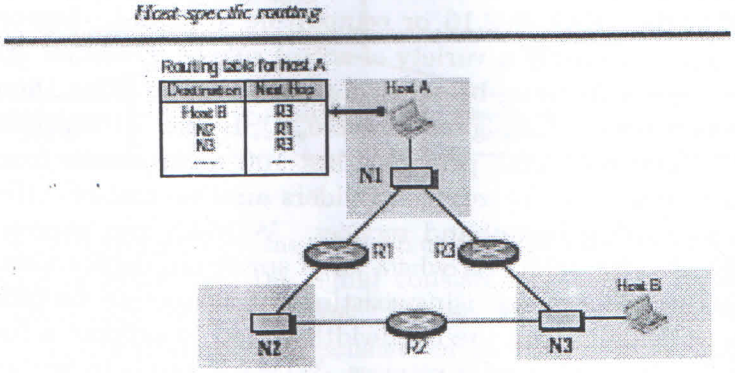


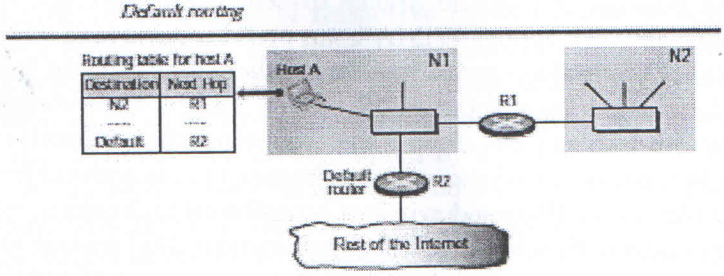
	Version.- This 8-bit field defines the version of the OSPF protocol. It is currently version 2. Type. -This 8-bit field defines the type of the packet. As we said before, we have five types, with values 1 to 5 defining the types. Message length. -This 16-bit field defines the length of the total message including the header. Source router IP address- This 32-bit field defines the IP address of the router that sends the packet. Area identification.-This 32-bit field defines the area within which the routing takes place. Checksum.-This field is used for error detection on the entire packet excluding the authentication type and authentication data field. Authentication type.-This 16-bit field defines the authentication protocol used in this area. At this time, two types of authentication are defined: 0 for none and 1 for password. Authentication.-This 64-bit field is the actual value of the authentication data. if the authentication type is 0, this field is filled with 0s. If the type is 1, this field carries an eight-character password.		
Q.4 (b)		8	CO3

A static routing table is created, maintained, and updated by a network administrator, manually. A static route to every network must be configured on every router for full connectivity. This provides a granular level of control over routing, but quickly becomes impractical on large networks. A dynamic routing table is created, maintained, and updated by a routingprotocol running on the router. Examples of routing protocols include RIP(Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), and OSPF (Open Shortest Path First). 1.Next-Hop Method- One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop instead of information about the complete route. The entries of a routing table must be consistent with each other. 2.Network-Specific Method A second technique to reduce the routing table and simplify the searching process is called the network-specific method. Here, instead of having an entry for every destination host connected to the same physical network, we have only one entry that defines the address of the destination network itself. In other words, we treat all hosts connected to the same network as one single entity. For example, if 1000 hosts are attached to the same network, only one entry exists in the routing table instead of 1000. 3Host-Specific Method- In the host-specific method, the destination host address is given in the routing table. The rationale behind this method is the inverse of the network-specific method. Here efficiency is sacrificed for other advantages: Although it is not efficient to put the host address in the routing table, there are occasions in which the administrator wants to have more control over routing. For example, in Figure 6.5 if the administrator wants all packets arriving for host B delivered to router R3 instead of R1, one single entry in the routing table of host A can explicitly define the route. Host-specific routing is used for purposes such as checking the route or providing security measures. 4.Default Method- Another technique to simplify routing is called the default method.In Figure 6.6 host A is connected to a network with two routers. Router R1 routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the default (normally defined as network address 0.0.0.0).



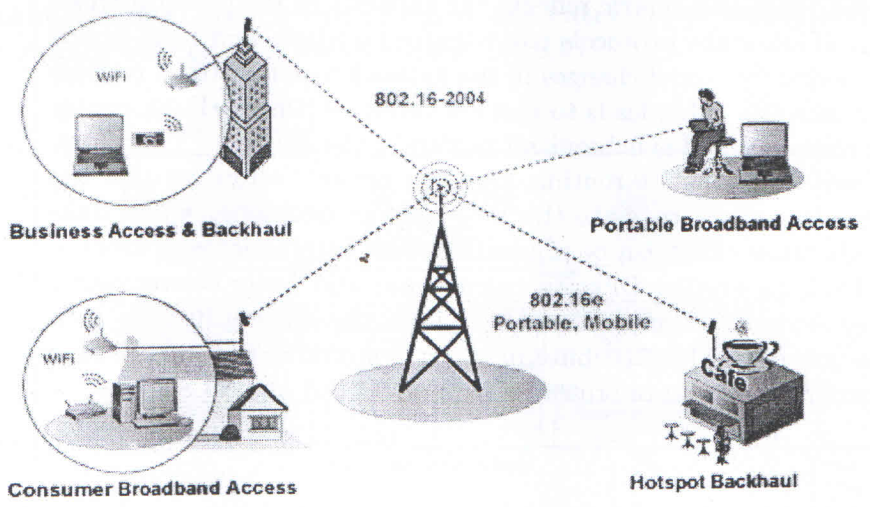






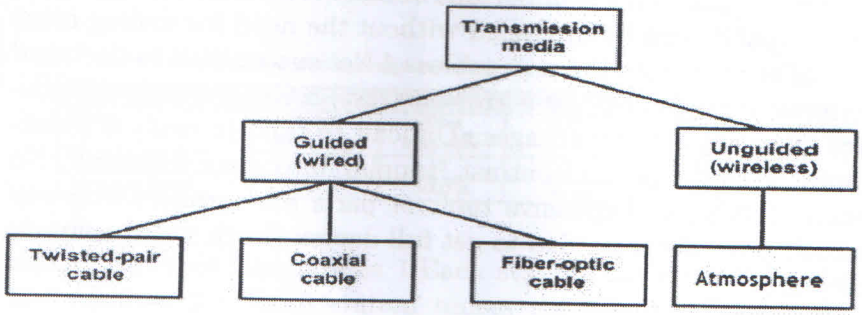
Q.4 (c)	Link-state protocols use cost metrics to choose paths through the network. The cost metric reflects the capacity of the links on those paths. •Link-state protocols use triggered updates and LSA floods to immediately report changes in the network topology to all routers in the network. This leads to fast convergence times. •Each router has a complete and synchronized picture of the network. Therefore, it is very difficult for routing loops to occur. •Routers use the latest information to make the best routing decisions. •The link-state database sizes can be minimized with careful network design. This leads to smaller Dijkstra calculations and faster convergence. •Every router, at the very least, maps the topology of its own area of the network. This attribute helps to troubleshoot problems that can occur. •Link-state protocols support CIDR and VLSM.	4	CO2
Q.5 (a)		8	CO2

WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way. Loosely, WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises. WiMAX is Acronym for Worldwide Interoperability for Microwave Access. Based on Wireless MAN technology. A wireless technology optimized for the delivery of IP centric services over a wide area. A scalable wireless platform for constructing alternative and complementary broadband networks. A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard. Importance WiMAX can satisfy a variety of access needs. Potential applications include extending broadband capabilities to bring them closer to subscribers, filling gaps in cable, DSL and T1 services, WiFi, and cellular backhaul, providing last-100 meter access from fibre to the curb and giving service providers another cost-effective option for supporting broadband services. WiMAX can support very high bandwidth solutions where large spectrum deployments (i.e. ¿10 MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth neded to support a full range of high-value multimedia services. WiMAX can help service providers meet many of the challenges they face due to increasing customer demands without discarding their existing infrastructure investments because it has the ability to seamlessly interoperate across various network types. WiMAX can provide wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive voice-over-IP (VoIP) to real-time streaming video and non-real-time downloads, ensuring that subscribers obtain the performance they expect for all types of communications. WiMAX, which is an IP-based wireless broadband technology, can be integrated into both wide-area third-generation (3G) mobile and wireless and wireline networks allowing it to become part of a seamless anytime, anywhere broadband access solution.



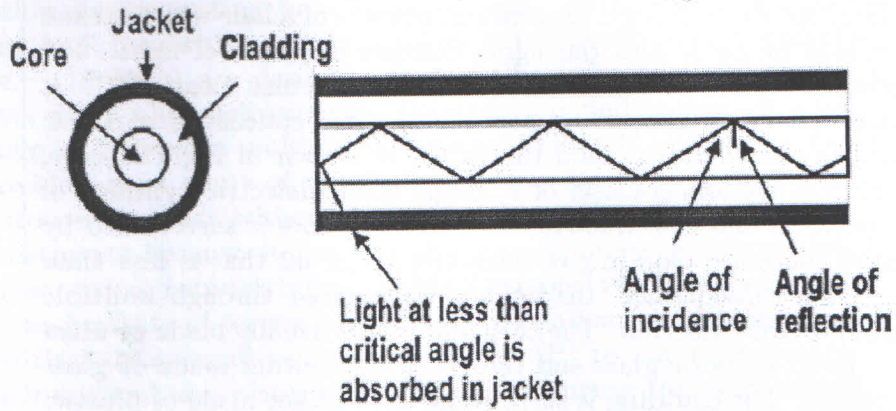
OR

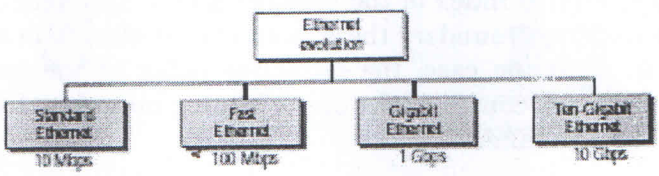
Q.5 (a)		2+6=8	CO2



In fiber optic technology, the medium consists of a hair-width strand of silicon or glass, and the signal consists of pulses of light. For instance, a pulse of light means "1", lack of pulse means "0". It has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket as shown in Fig.The core, innermost section consists of a single solid dielectric cylinder of diameter d1 and of refractive index n1. The core is surrounded by a solid dielectric cladding of refractive index n2 that is less than n1. As a consequence, the light is propagated through multiple total internal reflection. The core material is usually made of ultra pure fused silica or glass and the cladding is either made of glass or plastic. The cladding is surrounded by a jacket made of plastic. The jacket is used to protect against moisture, abrasion, crushing and other environmental hazards.Optical fibers are available in two varieties; Multi-Mode Fiber (MMF) and Single-Mode Fiber (SMF). For multi-mode fiber the core and cladding diameter lies in the range 50-200m and 125-400m, respectively. Whereas in single-mode fiber, the core and cladding diameters lie in the range 8-12m and 125m, respectively. Single-mode fibers are also known as Mono-Mode Fiber. Moreover, both single-mode and multi-mode fibers can have two types; step index and graded index. In the former case the refractive index of the core is uniform throughout and at the core cladding boundary there is an abrupt change in refractive index. In the later case, the refractive index of the core varies radially from the centre to the core-cladding boundary from n1 to n2 in a linear manner.

Advantages-Very high data rate, low error rate. 1000 Mbps (1 Gbps) over distances of kilometers common. Error rates are so low they are almost negligible. 2.Difficult to tap, which makes it hard for unauthorized taps as well. This is responsible for higher reliability of this medium.Much thinner (per logical phone line) than existing copper circuits. Because of its thinness, phone companies can replace thick copper wiring with fibers having much more capacity for same volume. This is important because it means that aggregate phone capacity can be upgraded without the need for finding more physical space to hire the new cables. 4.Not susceptible to electrical interference (lightning) or corrosion (rust).5.Greater repeater distance than coax.Disadvantages:•Difficult to tap. It really is point-to-point technology. In contrast, tapping into coax is trivial. No special training or expensive tools or parts are required.One-way channel. Two fibers needed to get full duplex (both ways) communication.



Q.5 (b)	Assume that minimum frame size is 65 bytes or 520 bits. We have L=T*R, Where L is the length of the frame, T is the time, and R is the data rate. We can say T=L/R The time can be calculated as T= L/R= (520 bits)/ (10,000,000)bits/ second= 0.000052s=52 microsec.	4	CO2
Q.5 (c)		4+4=8	CO2

Summary of Standard Ethernet implementations

Characteristics	10Base5	10Base2	10Base-T	10Base-F
Medium	Thick coax	Thin coax	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m

Summary of Fast Ethernet implementations

Characteristics	100Base-TX	100Base-FX	100Base-T4
Media	STP	Fiber	UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m

Summary of Gigabit Ethernet implementations

Characteristics	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T4
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m

Standard Ethernet Similarities 1.Each station has an equal right to the medium 2. Each station senses the medium Difference: CSMA/CD- a station can send if it senses no signal on the line. CSMA/CA: a station needs to inform other stations that it needs the medium for a specific amount of time. CSMA/CD: Collision can occur CSMA/CA: Collisions are avoided