Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2019

Course: Data Communication and Computer Networks **Semester: IV**
Program: B.Tech. (CSE, IBM All Branches) **Time 03 hrs.**
Course Code: CSEG 2009 **Max. Marks: 100**

Instructions:
1. Section A - 20 marks (Attempt All 5 Questions in this Section. Each question carries 4 marks)
2. Section B - 40 marks (Attempt All 4 questions. Each question carries 10 marks)
3. Section C - 40 marks (Attempt All 2 question. Each question carries 10 marks)

SECTION A

S. No.		Marks
Q 1	Enlist the scenarios where unguided communication media are preferred over guided media. Explain TWO advantages and TWO disadvantages of coaxial cable for communication. The **unguided media** is also called **wireless communication**. It does not require any physical medium to transmit electromagnetic signals. In unguided media, the electromagnetic signals are broadcasted through air to everyone. These signals are available to one who has the device capable of receiving those signal. The unguided media is also called unbounded media as it does not have any border limitation. The unguided media allows the user to connect all the time, as the communication is wireless the user can connect himself from anywhere to the network. Advantage: The cost of coaxial cable is less. It supports high bandwidth signal transmission compare to twisted pair. Disadvantage: It is bulky. As single cable is used for signal transmission across the entire network, in case of failure in one cable the entire network will be down.	**2+2**
Q 2	Differentiate the two protocols at transport layer TCP and UDP on various parameters.	**4**

UDP service:

- unreliable data transfer between sending and receiving process
- does not provide: connection setup, reliability, flow control, congestion control, timing, or bandwidth guarantee

TCP service:

- *connection-oriented:* setup required bw client, server
- *reliable transport* acks, retransmissions
- *flow control:* sender won't overwhelm receiver
- *congestion control:* for benefit of the Internet
- *does not provide:* timing, minimum bandwidth guarantees

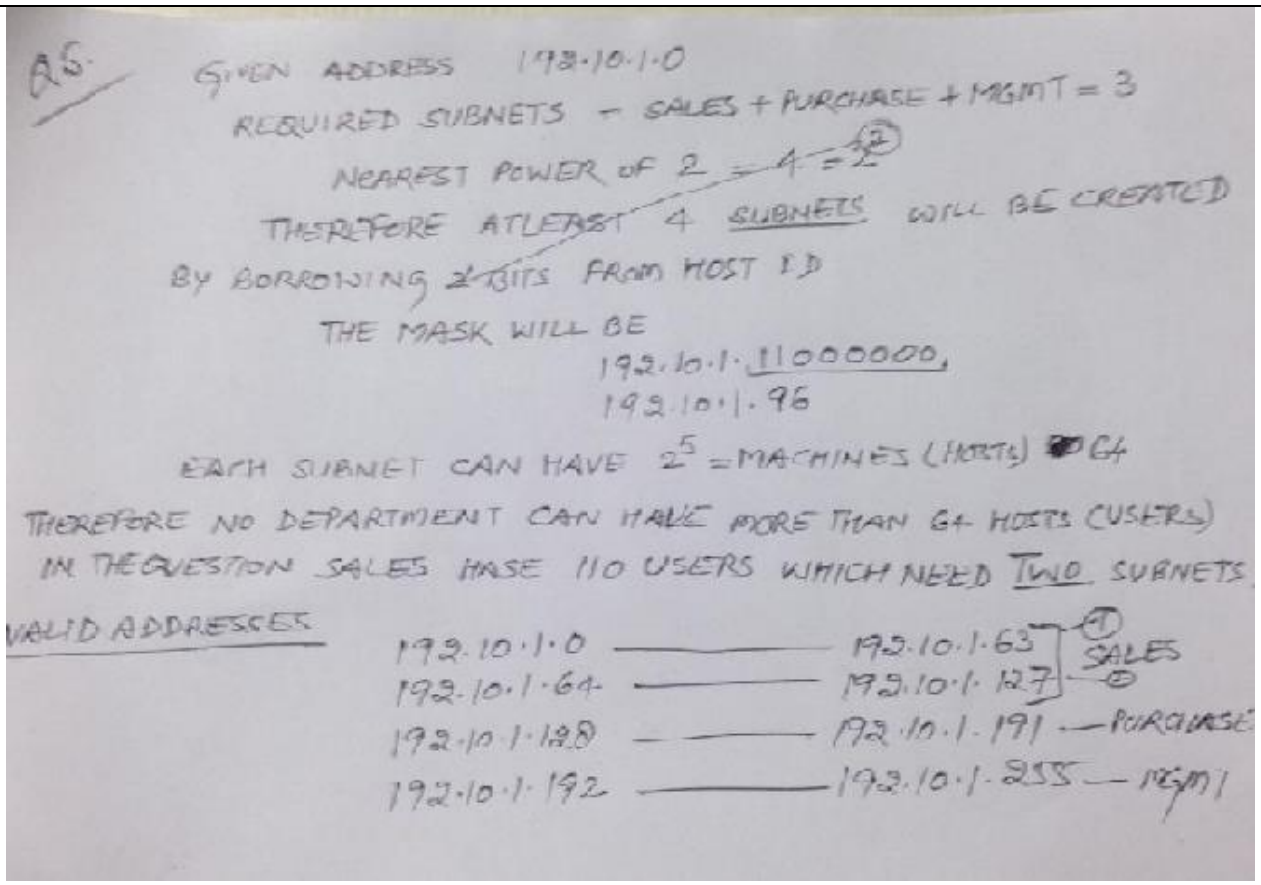
Q 3 Compare and contrast various switching techniques?

Comparison of the three switching techniques

Circuit Switching	Packet	Message
Dedicated path	No dedicated path	No dedicated path
Path established for entire conversation	Route established for each packet	Route established for entire conversation
Call set up delay	Packet transmission delay	Call set up delay, Packet transmission delay
Overload may block call set up	Overload increases packet delay	Overload may block call set up and increases packet delay
No speed or code conversion	Speed or code conversion	Speed or code conversio
Fixed bandwidth	Dynamic bandwidth	Dynamic bandwidth
No overhead bits after call set up	Overhead bits in each packet	Overhead bits in each packet

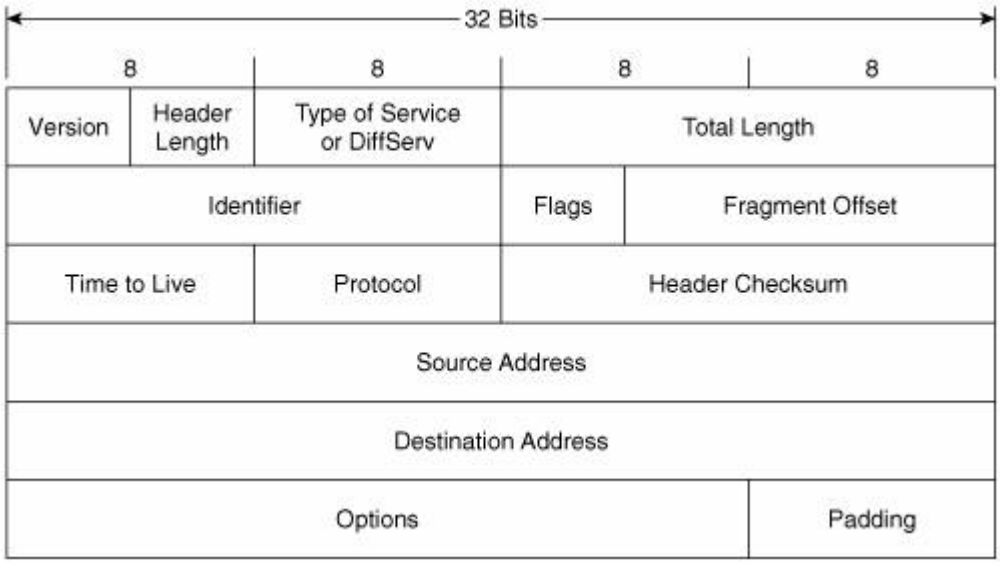
4

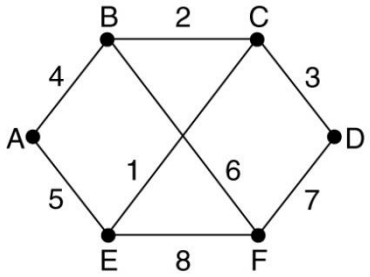
Q 4	Describe the significance of error detection and error correction mechanisms employed at data link layer. Enlist different mechanisms under both categories. **Error** A condition when the receiver's information does not matches with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0. **Error Detecting Codes (Implemented either at Data link layer of OSI Model)** Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message. Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors. Some popular techniques for error detection are: 1. Simple Parity check 2. Two-dimensional Parity check 3. Checksum 4. Cyclic redundancy check Correction: Hamming Codes.	**1+1+2**
Q 5	As you are an administrator of a network company, you are allotted a network address 192.10.1.0. There are 3 Departments Sales with 110 users, Purchase with 55 users and Management with 12 users. You need to create subnets for all these departments. Allocate valid IP addresses to all users.	**4**

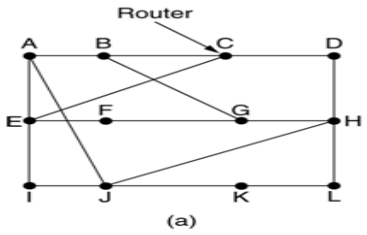


SECTION B

Q 6 Explain IPV-4 header format with suitable diagram, explicitly explaining all the fields and their relevance. **10**



	A header contains almost 13 multipurpose fields, which hold specific related object information such as application, data type and source/destination addresses. The following are detailed header field descriptions: • Version: This contains the Internet header format and uses only four packet header bits. • Internet header length (IHL): This 32-bit field stores IP header length information. • Type of service (ToS): This provides network service parameters. • Datagram size: This contains combined data and header length. • Identification: This 16-bit field contains a specific number for primary data identification. • Flags: This router fragment activity is controlled by three flags. • Fragmentation offset: This is a fragment identification via offset value. • Time to Live (TTL): This contains the total number of routers allowing packet pass-through. • Protocol: This 8-bit field contains header transport packet information. • Header checksum: It checks and monitors communication errors. • Source address: It stores source IP address. • Destination address: It stores destination IP address. • Options: This is the last packet header field and is used for additional information. When it is used, the header length is greater than 32 bits.	
Q 7	a) Why routing is important in communication and which layer is responsible for routing in OSI model? With a suitable example explain Link State Routing algorithm. **Routing** is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet. **Network layer.** Any example can be taken.  (a) Link State Packets A: Seq. / Age / B 4 / E 5 B: Seq. / Age / A 4 / C 2 / F 6 C: Seq. / Age / B 2 / D 3 / E 1 D: Seq. / Age / C 3 / F 7 E: Seq. / Age / A 5 / C 1 / F 8 F: Seq. / Age / B 6 / D 7 / E 8 (b) **---OR---** b) Discuss the disadvantages of Distance Vector Routing algorithm. Consider the given topology (Fig. a) and the vectors received by router J from its neighbors. Based on this information calculate the new routing table of J. Show the detailed calculations.	**4+6**



(a)

To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6

Vectors received from J's four neighbors

Count to infinity problem.

New estimated delay from J

Line
A
A
I
H
I
I
H
H
I
–
K
K

New routing table for J

Q 8 Compare and contrast three IEEE standards 802.3, 802.4 and 802.5.

S. No.	IEEE Standard	Advantages	Disadvantages
		✓ Most widely type used at present, with a huge installed base and considerable operational experience. ✓ Protocol is very simple ✓ Stations can be added without making the network down.	✓ It has a substantial analog component in order to detect the weakest signal for collision. ✓ Protocol is non-deterministic (probabilistic), which

10

	1	802.3 (CSMA/CD)	✓ The delay at low load is practically zero. (no token waiting)	makes it inappropriate for real-time work. ✓ It has also no priorities. ✓ Max cable length is limited (2.5 Km for 10Mbps). ✓ At high load, the presence of collisions becomes a major problem and can seriously affect the throughput.		
	2	802.4 (Token Bus)	✓ Uses highly reliable cable television equipments. ✓ It is more deterministic than 802.3, although repeated loss of token at critical times can introduce the uncertainness. ✓ Can easily handle shorter frames. (no limitation on frame size) ✓ It supports priorities and hence suitable for Real Time traffic. ✓ It also has excellent throughput and efficiency at high load.	✓ The protocol is extremely complex. ✓ It has substantial delay at low load. (waiting for token). ✓ It is poorly suited for FOC implementations.		
	3	802.5 (Token Ring)	✓ It uses point-to-point connections and hence the engineering is easy. ✓ Any transmission media can be used. ✓ The use of wire centers make the token ring the only LAN that can detect and eliminate cable failures automatically. ✓ Like 802.4, priorities also possible, although the scheme is not as fair. ✓ Very short and very large frames both are possible. ✓ At very high load, the throughput and efficiency are excellent.	✓ Presence of a monitor creates the problem, and overheads. ✓ Like 802.4, delay at low load.(wait for token)		
Q 9	a) What do you understand with Domain Name System (DNS)? **DOMAIN NAME SYSTEM** Application programs rarely refer to addresses by their binary addresses. Instead of binary numbers, they use ASCII strings, such as sudeep@yahoo.com . But the network itself only understands binary addresses, so some mechanism is					**3+4+3**

required to convert these ASCII strings to binary network addresses. This is achieved by with the help of **Domain Name System (DNS).**

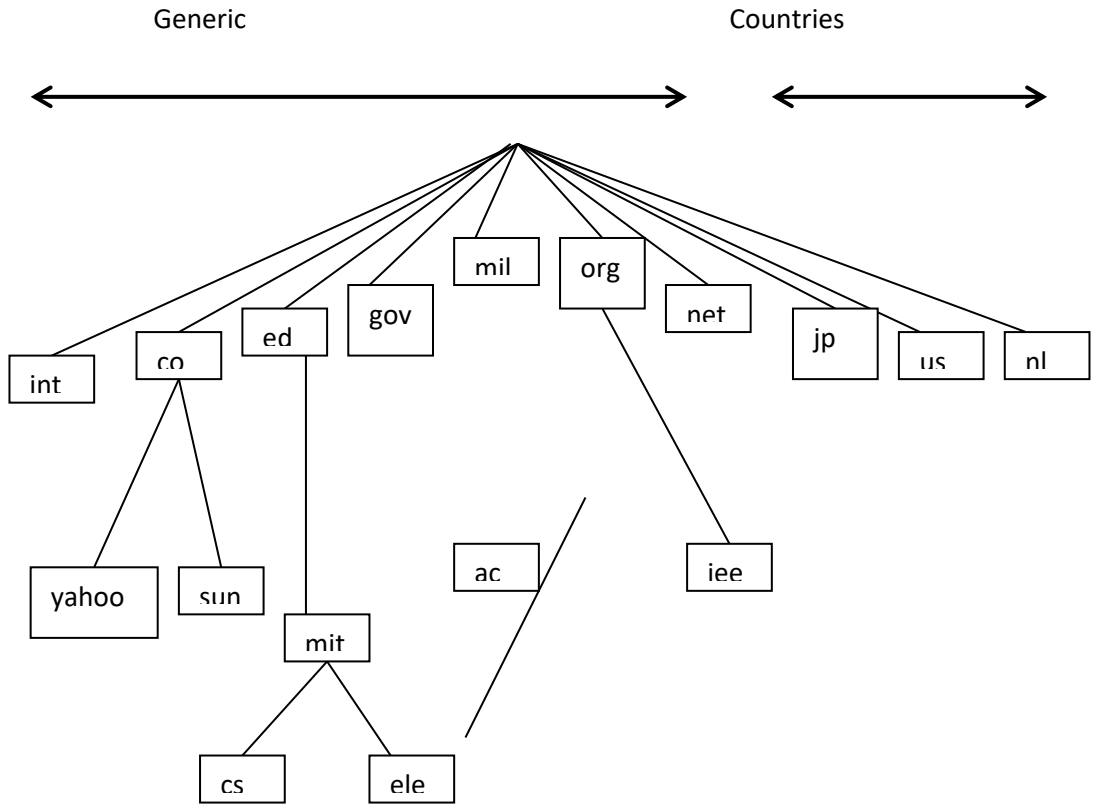
To map a name onto an IP address, an application program calls a library procedure called **resolver,** passing it the name as a parameter. The resolver sends a UDP packet to a local DNS server; which then looks up the name and returns the IP address to the resolver, which then returns it to the caller.

DNS, however, is not stored in any one location. There are basically two reasons for this:

a. One host would never be able to handle the bundle of requests for address translation from throughout the world.
b. There will be single point of failure

Due these reasons, DNS is distributed among a collection of DNS servers scattered throughout the Internet.

The implementation part of this idea is very difficult and even more difficult to manage the quick translation of addresses. This is where the **domain name space** concept comes into the picture.



Internet is divided into several hundred top-level **domains** where each domain covers many hosts. Each domain is partitioned into many sub-domains and these are further divided. All these domains can be represented by a tree.

The top-level domains come in two flavors: ***generic*** and ***countries***.

The **generic** domains are:

int	Certain international organizations
com	Commercial Organizations
edu	Educational institutions
gov	Government Organizations
mil	Military services
org	Nonprofit Organizations
net	Network providers

The **country** domains include one entry for each country e. g. for India in, for Japan jp etc.

- ✓ Each domain is named by the path upward from it to the unnamed root. The components are separated by periods **(.)**.
- ✓ Domain names are case insensitive.
- ✓ Component names can be up to 63 characters long, and full path names must not exceed 255 characters.

Resource Records:

Every domain, whether it is a single host or a top-level domain, can have a set of **resource records** associated with it**.** A resource record is a five-tuple record. The format is as follows:

Domain_name ***Time_to_live*** ***Type*** ***Class*** ***Value***

1. Domain_name: tells the domain to which this record applies
2. Time_to_live: gives the indication that how stable the record is .(1 min to 1 day).
3. Type: tells what kind of record is this. The most important type is **A** which holds a 32-bit IP address for some host.
4. Class: For Internet information it is IN, for other information some other code may be used.
5. Value: Some additional information is kept here.

b) Name the different types of network topologies and brief their advantages?

BUS Topology

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

RING Topology

Advantages of Ring Topology

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

STAR Topology

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

MESH Topology

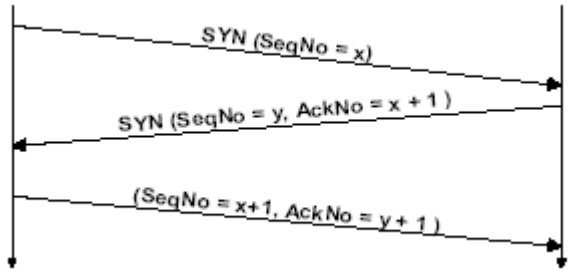
Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

	c) What is Piggybacking? For what purpose it is used and how is it helpful? Piggybacking data is a bit different from Sliding Window Protocol used in the OSI model. In the data frame itself, we incorporate one additional field for acknowledgment (called ACK). Whenever party A wants to send data to party B, it will carry additional ACK information in the PUSH as well. For example, if A has received 5 bytes from B, which sequence number starts from 12340 (through 12344), A will place "ACK 12345" as well in the current PUSH packet to inform B it has received the bytes up to sequence number 12344 and expects to see 12345 next time. (ACK number is the next sequence number of the data to be PUSHed by the other party.) Three rules govern the piggybacking data transfer. • If station A wants to send both data and an acknowledgment, it keeps both fields there. • If station A wants to send just the acknowledgment, then a separate ACK frame is sent. • If station A wants to send just the data, then the last acknowledgment field is sent along with the data. **Advantages** : Improves the efficiency, better use of available channel bandwidth.ion B simply ignores this duplicate ACK frame upon receiving .	
	SECTION-C	
Q 10	a) Write down the FOUR functions of Application layer. Specific functions provided by the application layer include the following :- **Network virtual terminal :-** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. **File transfer, access, and management :-** This application allows a user to access files in a remote host (to make changes or read data). **Mail services :-** This application provides the basis for e-mail forwarding and storage. **Directory services :-** This application provides distributed database sources and access for global information about various objects and services. b) Explain steps involved during connection establishment and connection termination in detail in TCP connection management with suitable diagram. **TCP Connection Management** TCP is a connection-oriented protocol. It establishes a virtual path between source and destination. Connection Management is the process of establishing, maintaining, and ending a connection. ***Connection Establishment***	**5+15**

TCP transmits in full-duplex mode. When two TCP's in two machines are connected, they are able to send and receive the segments simultaneously.

Connections are established using the ***three-way handshake.*** To establish a connection, one side passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives.

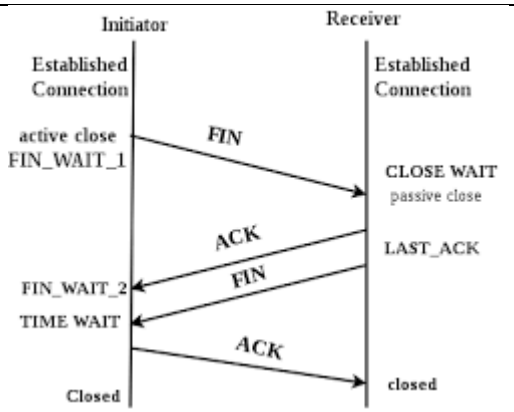


Now the three steps are as follows:

1. The other side executes a CONNECT primitive, specifying the IP address and the port number to which it wants to connect, the maximum TCP size it is willing to accept etc. It sends a TCP segment with SYN bit on and ACK bit off (SYN=1, ACK=0). This also contains the initialization sequence number used for numbering the bytes by the side.
2. When this segment arrives at the destination, the TCP there checks to see if there is a process that has done LISTEN on the port given in the destination address field. If not, it sends a reply with the RST bit on to reject the connection. If yes, then it can either accept or reject the connection. If it accepts, and acknowledgement segment is sent back. ACK field would be having the value of sequence number plus 1.
3. On receiving this segment, the first side acknowledges the receipt of the segment and start sending the data.

Connection Termination

Any of the two parties involved in exchanging data (client or server) can close the connection. When the connection in one direction is terminated, the other party may continue sending data in the other direction. Therefore, four steps are needed to close the connections in both directions simultaneously.



1. The client TCP sends the first segment, a FIN segment.
2. The server TCP sends the second segment, an ACK segment, to confirm the receipt of FIN segment from the client.
3. The server TCP can continue sending the data in the server-client direction. When it does not have any more data to send, it sends the third segments i.e. FIN.
4. The client TCP sends fourth segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server.

-----OR----

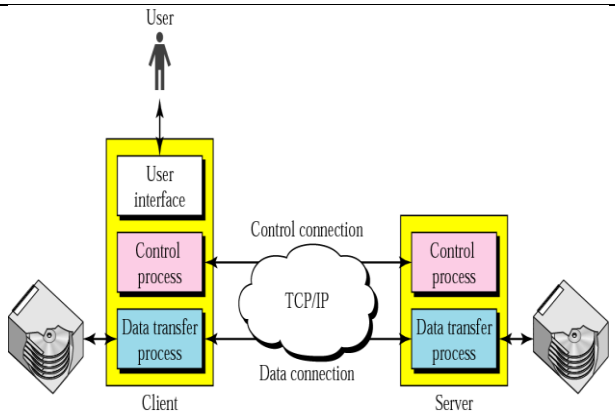
a) Explain FTP with suitable diagram.

FILE TRANSFER PROTOCOL (FTP)

FTP is a standard mechanism provided by the Internet for copying file from one host to another host. The problems which are to be addressed here are that two systems involved in transferring files may use different file name conventions, different ways to represent text data, different directory structures etc.

FTP uses the services of TCP. It needs two TCP connections. The well-known port 21 is used for the control connection, and the well-known port 20 is used for the data connection.

The basic model of FTP is given below.



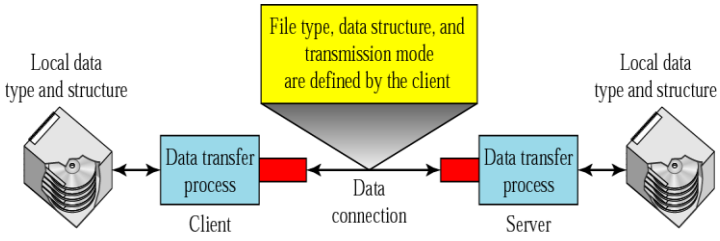
The client has three components: **user interface, client control process**, and the **client data transfer process**. The server has two components: the **server control process** and the **server data transfer process**.

The control connection is made between the control processes and the data connection is made between the data transfer processes.

The control connection is maintained during the entire FTP session. The data connection is opened when data are ready to transfer and closed when not needed.

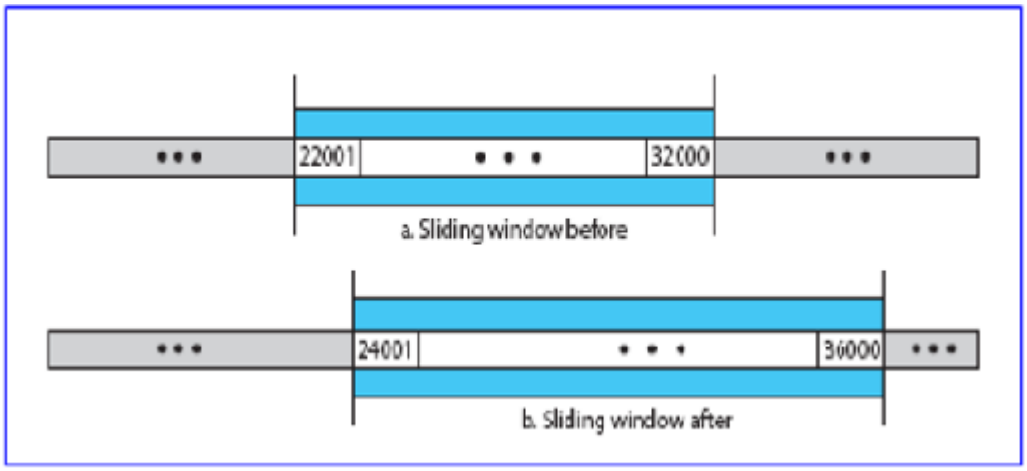
Communication

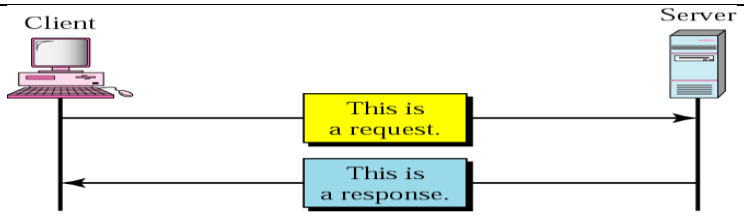
FTP uses the same approach as SMTP to communicate across the control connection. For transfer of files, data connection is used. The client must define the type of file to be transferred (ASCII, EBCDIC, Imagefile), the structure of the data, and the transmission mode. Before sending the file through data connection, we prepare for transmission through the control connection.



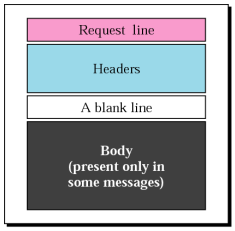
b) How window management takes place in TCP through which flow control is achieved. Explain with the help of following scenario:

A TCP connection is using a window size of 1000 B and the previous acknowledgment number was 22,001. It receives a segment with acknowledgment number 24,001. Draw a diagram to show the situation of the window after and before the acknowledgment is received. If the window size is changed to 11000 B and 9000 B separately then what will be the situation.

	(*you may take different scenario on your own but will lose 2 marks*) ***Window Management in TCP (Flow Control)*** Flow control defines the amount of data a source can send before receiving an acknowledgement from the destination. A sliding window is used to make transmission more efficient as well as to control the flow of data so that the destination does not become overwhelmed with data. TCP's slide window protocol is byte-oriented. The implementation of the sliding window protocol is same as in data link protocols. But the window management is not directly tied to acknowledgement. The sender window size is totally controlled by the receiver window value (the number of empty locations in the receiver buffer). The size of receiver window can be dynamically increased or decreased by the destination.  	
Q 11	Write short notes on the followings: a) HTTP **HYPERTEXT TRANSFER PROTOCOL (HTTP)** The Hypertext Transfer Protocol (HTTP) is used mainly to access data on the World Wide Web. The protocol transfers data in the form of plain text, hypertext, audio, video, and so on. HTTP functions like a combination of FTP and SMTP. It is similar to FTP because it transfers files and uses the services of TCP. However, it uses only one TCP connection. There is no separate control connection; only data are transferred between the client and the server. A client sends a request, which looks like mail, to the server. The server sends back the response, which looks like a mail reply to the client (like SMTP).	**20**



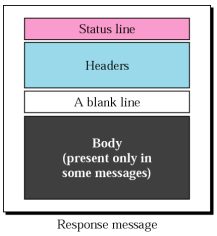
There are two general types of HTTP messages: **request** and **response**. Both message types follow almost the same format.



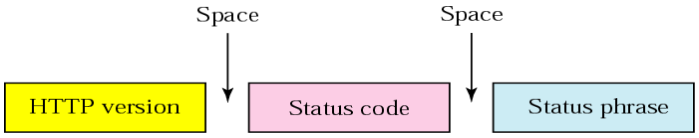
Request message

A request message consists of a request line, headers, and sometimes a body.

A response message consists of a status line, a header, and sometimes a body.



Response message



b) OSPF vs BGP

Points	OSPF	BGP
Acronym For	Open Shortest Path First.	Border Gateway Protocol.
Gateway Protocol	OSPF is an internal gateway protocol.	BGP is an external gateway protocol.
Implementation	Easy to Implement.	Complex to Implement.
Convergence	Fast.	Slow.
Design	Hierarchical Network Possible.	Fully Meshed.
Need of Device Resources	Memory & CPU Intensive.	Depends on the size of the routing table but scales better than OSPF.
Scaled Networks	OSPF is mainly used on smaller scale networks that are centrally administered.	BGP protocol is mainly used on very large-scale networks, like the internet.
Function	OSPF will always search for the fastest route, and not the shortest, in spite of its name.	BGP focuses in determining the best path for a datagram.
Algorithm Used	Dijkstra Algorithm.	Best Path Algorithm.
Protocol	IP Protocol.	TCP Protocol.
Port	89.	179.
Type	Link State.	Path Vector.

c) TDM vs FDM

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 .

d) SNMP

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

It is another protocol included in TCP/IP suite. The SNMP is a management protocol which takes care of the working of other network protocols by allowing the network managers to locate the problems and make adjustments. It runs on the top of UDP.

A network manager runs a management client program at a site that communicates with a management server program. The sever programs are run on remote hosts/routers. Both of these programs use commands defined by the SNMP protocol. These commands define how to request information from a server and send information to a server or client.

The routers and hosts SNMP manages are called objects. These objects are defined in a particular language e.g. Abstract Syntax Notation.1 (ASN.1).

Each object's server maintains a database of information that describes its characteristics and activities called Management Information Base (MIB). In all there are eight categories of information specified by MIB:

- **System:** describes the host/router OS and contains information such as when the server was booted, its location etc.
- **Interface:** describes each network interface and contains items such as transmission rate, number of pkts discarded for various reasons etc.
- **Address Translation:** contains a table used to change an IP address into a network-specific one.
- **IP:** describes information specific to the Internet Protocol and contains information like time-to_live value for IP pkts, number of datagrams forwarded to TCP/UDP, number of fragments created, routing tables etc.
- **ICMP:** describes information specific to the ICMP. It contains the counters tracking the numbers of each type of control message sent by ICMP.
- **TCP:** It contains the information like number of TCP connections, number of failed connections attempts etc.
- **UDP:** It contains the number of datagrams delivered, discarded, or received etc.
- **EGP:** contains the counters to track the number of EGP messages sent and received.

Following are some commands through which SNMP issues requests and gets the responses etc:

- ✓ **GetRequest:** Requests are issued by this command specifying command code, object name, and specification of MIB variable requested.
- ✓ **GetNextRequest:** Similar to GetRequest except that the request is for values of variables that "follow" to those specified in previous request.
- ✓ **GetResponse:** A response sent in the response of GetRequest and contains values requested or error codes.
- ✓ **SetRequest:** This command allows the network manager to update values of MIB variables maintained by the objects.
- ✓ **Trap:** This is sent from server to the manager when specific conditions or events have occurred.
  - **Coldstart trap:** The management program has been initialized with changes in object's MIB.
  - **Warmstart trap:** Reinitialization has occurred, but no change in object's MIB.
  - **Linkdown trap:** A communication link has failed.
  - **Linkup trap:** A previously failed communication has been restored.
  - **EgpNeighborLoss trap:** The station has lost contact with an EGP peer neighbor.