Solved Paper 2016-17
Computer Network
B.Tech (IT) VI semester

SECTION – A

1.

(a)Write about user access in ISDN.

ISDN stands for Integrated Services Digital Network. It is a design for a completely digital telephone/telecommunications network. It is designed to carry voice, data, images, video, everything you could ever need. It is also designed to provide a single interface (in terms of both hardware and communication protocols) for hooking up your phone, your fax machine, your computer, your videophone, your video-on-demand system (someday), and your microwave.

- Two types of user access are defined
  - Basic Access - Consists of two 64Kbps user channels (B channel) and one 16Kbps signally channel (D channel) providing service at 144 Kbps.
  - Primary access - Consists of thirty 64Kbps user channels (B channels) and a 64 Kbps signally channel (D channel) providing service at 2.048Mbps (One 64 Kbps channel is used for Framing and Synchronization).

(b) List the advantages and disadvantages of star topology.

Advantages Of star topology

- This topology has the advantage of minimum data traffic along the cables (node to server only)., thus providing optimum performance.
- The main advantage of star LAN are that the access to the network i.e decision on when a station can or cannot transmit, is under central control.

Disadvantages of Star Topology

- Because single central machine must coordinate all communications, this topology requires an extremely powerful server. Hence Star Topology is expensive.
- Speed is generally limited and central switch is an obvious potential source of catastrophic failure i.e if centralised server fails, whole topology fails.

(c) Compare ALOHA with slotted ALOHA.

Pure ALOHA has a vulnerable time of 2 x *Tfr* . This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots of Tfr s and force the station to send only at the beginning of the time slot.

(d) State the requirements of CRC.

Cyclic redundancy checking is a method of checking for errors in data that has been transmitted on a communications link. A sending device applies a 16- or 32-bit polynomial to a block of data that is to be transmitted and appends the resulting cyclic redundancy code (CRC) to the block. The receiving end applies the same polynomial to the data and compares its result with the result appended by the sender. If they agree, the data has been received successfully. If not, the sender can be notified to resend the block of data.

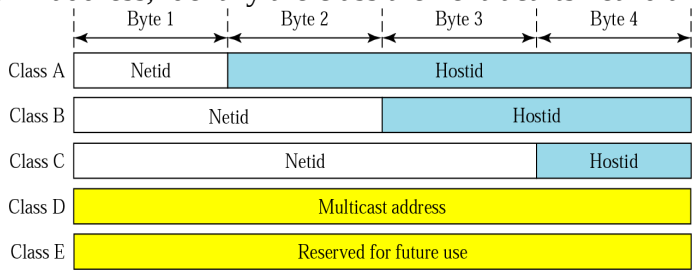
(e) Provide few reasons for congestion in a network.

The following factors responsible for congestion:

- Slow network links
- Shortage of buffer space
- Slow processors
- More input line

(f) With the given IP-address, how will you extract its net-id and host-id?

For any IP address, identify the class then extract its net-id and host-id.

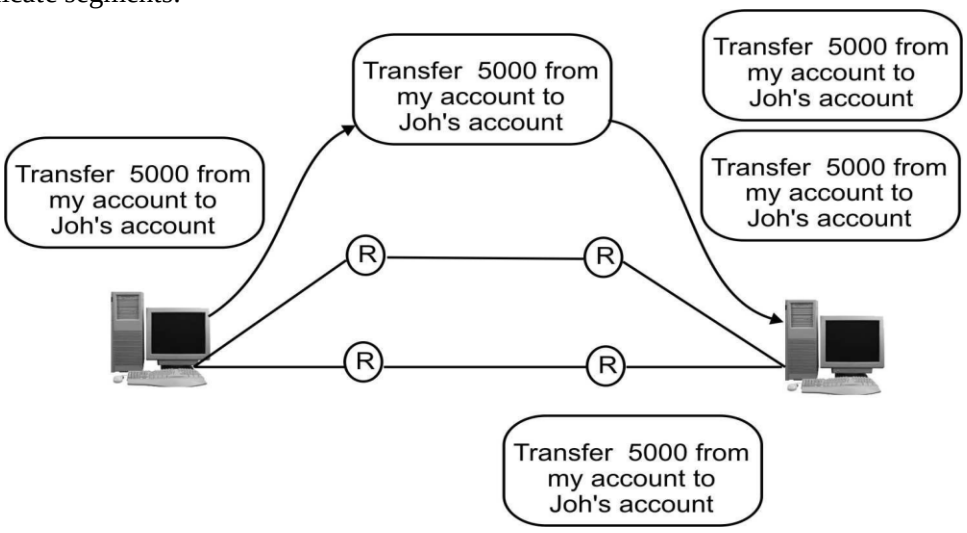


(g) What is piggybacking?

combine a data Frame with an ACK

(h) How does transport layer perform duplication control?

Duplication Controls: The aspect of reliability by the transport layer is duplication control as shown in figure. Transport layer functions must guarantee that no places of data arrive at the receiving system duplicated. As they allow identification of last packets, sequence no. allows the receiver to identify and discard duplicate segments.



(i) Mention the use of HTTP.

Hyper Text Transfer Protocol (HTTP) is a protocol, which is used for transmitting and receiving information across the Internet.

- URL begins with "http://"
- It uses port 80 for communication.

SECTION – B

2.

(a) Discuss the issues in the data link layer and about its protocol on the basis of layering principle.

Data Link Layer Design Issues

1. Providing a well-defined service interface to the network layer
2. Determining how the bits of the physical layer are grouped into frames
3. Dealing with transmission errors
4. Regulating the flow of frames so that slow receivers are not swamped by fast senders.

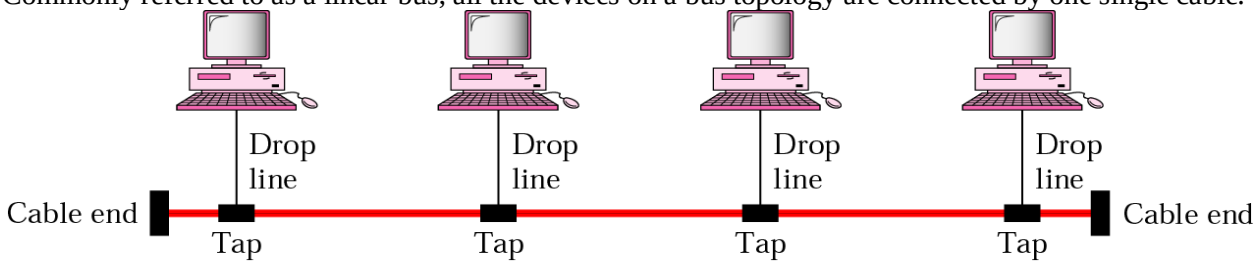
Other responsibilities of the data link layer include the following: Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames. Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one. Flow control. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver. Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame. Access control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time

(b) Explain network topological design with necessary diagram and brief the advantages and disadvantages of various topologies.

A Topology of the network defines the manner in which the network devices are arranged and connected to each other in a network. It defines the shape of communication network. There are following common types of network Topologies.

1. Bus Topology :

Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable.



Advantages:

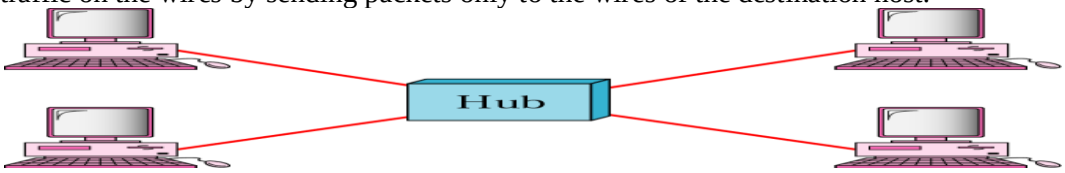
- Easy to use & inexpensive simple network
- Easy to extend thus allowing long distance traveling of signal
- Requires less cable length than a star topology

Disadvantages:

- Becomes slow by heavy network traffic with a lot of computer
- Difficult to troubleshoot & difficult to identify the problem if the entire network shut down
- Terminator is required at both ends of the backbone cable
- Not meant to be used as a stand alone solution in a large buildin

2. Star Topology

The star topology is the most commonly used architecture in Ethernet LANs. When installed, the star topology resembles spokes in a bicycle wheel. Larger networks use the extended star topology. When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



Advantages:

• Easy to modify and add new computer to a star network without disturbing the rest of the network

• Ease of diagnosis of network faults through the central computer

• Single computer failure do not necessarily bring down the whole star network

• Use of several cable types in the same network

Disadvantages:

• Requires more cable length than a linear topology.

• If the hub or concentrator fails, nodes attached are disabled.

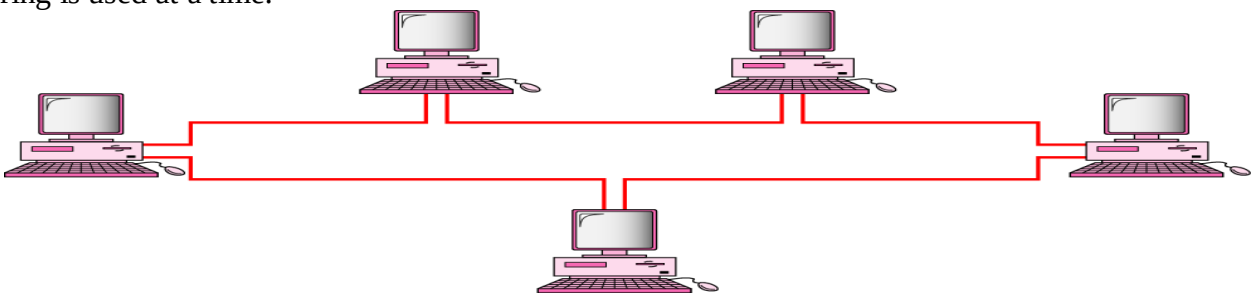
• More expensive than linear bus topologies because of the cost of the concentrators

3. Ring Topology :

A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame. The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.

• Single ring – All the devices on the network share a single cable

• Dual ring – The dual ring topology allows data to be sent in both directions although only one ring is used at a time.



Advantages:

• Every computer is given equal access to the token; no one computer can monopolize the network

• Fair sharing of the network allows the network to degrade gracefully as more users are added

Disadvantages:

• Failure to one network can affect the whole network

• Difficult to troubleshoot a ring network

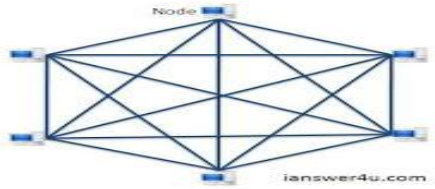
• Adding or removing computer disrupts the network

Ring network layout ring network is a topology of computer network where each node is connected to two other nodes, so as to create a ring. Ring networks tend to be inefficient when compared to Star networks because data must travel through less number of points before reaching its destination. For example , if a given ring network

has eight computers on it, to get from computer one to computer four, data must be travel from computer one, through computers two and three, and to it's destination at computer four. It could also go from computer one through eight, seven, six, and five until reaching four, but this method is slower because it travels through more computers. Ring network also carry the disadvantage that if one of the nodes in the network breaks then the entire network will break down with it as it requires a full circle in order to function.

4. Mesh Topology

In a mesh network topology, each of the network node, computer and other devices, are interconnected with one another. Every node not only sends its own signals but also relays data from other nodes. In fact a true mesh topology is the one where every node is connected to every other node in the network. This type of topology is very expensive as there are many redundant connections, thus it is not mostly used in computer networks. It is commonly used in wireless networks. Flooding or routing technique is used in mesh topology.



Advantages of Mesh topology

1) Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.

2) Even if one of the components fails there is always an alternative present. So data transfer doesn't get affected.

3) Expansion and modification in topology can be done without disrupting other nodes.

Disadvantages of Mesh topology

1) There are high chances of redundancy in many of the network connections.

2) Overall cost of this network is way too high as compared to other network topologies.

3) Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

(c) Consider the use of 10 K-bit size frames on a 10 Mbps satellite channel with 270 ms delay. What is the link utilization for stop-and-wait ARQ technique assuming $P=10^{-3}$?

We know link utilisation of a network = 1 / (1 + 2a) where

a = propogation time / transmission time

In calculating transmission time as we know in stop n wait ARQ , only 1 frame can be sent at a time hence the data size is taken of 1 frame only.

So transmission time = Data size / Data rate

= 10 * 103 bits / 10 * 106 bps

= 1 ms

Propogation delay given = 270 ms

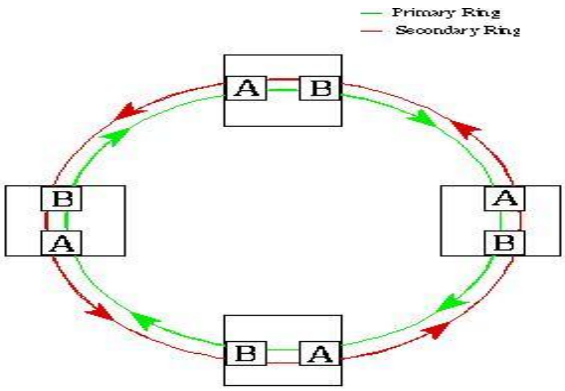
So the value of a as mentioned earlier = 270 / 1 = 270

So link utilisation = 1 / (1 + 2 * 270)

= 1 / (541)

= 0.19 %

(d) Brief about how line coding implemented in FDDI and describe its format.



Fiber Distributed Data Interface (FDDI) is a standard for data transmission in a local area network. It uses optical fiber as its standard underlying physical medium, although it was also later specified to use copper cable, in which case it may be called CDDI (Copper Distributed Data Interface), standardized as TP-PMD (Twisted-Pair Physical Medium-Dependent), also referred to as TP-DDI (Twisted-Pair Distributed Data Interface).

FDDI provides a 100 Mbit/s optical standard for data transmission in local area network that can extend in range up to 200 kilometers (120 mi). Although FDDI logical topology is a ring-based token network, it did not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol was derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

Frame format

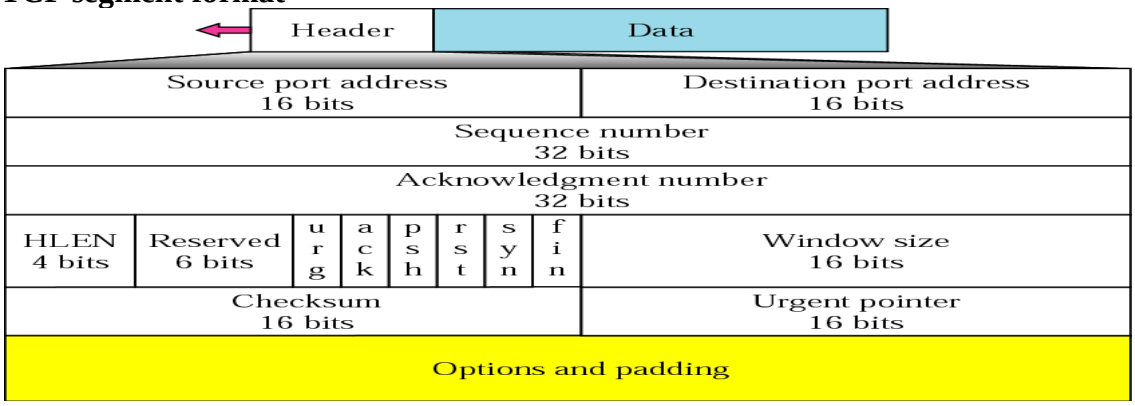
PA	SD	FC	DA	SA	PDU	FCS	ED/FS
16 bits	8 bits	8 bits	48 bits	48 bits	up to 4478x8 bits	32 bits	16 bits

Where PA is the preamble, SD is a start delimiter, FC is frame control, DA is the destination address, SA is the source address, PDU is the protocol data unit (or packet data unit), FCS is the frame check Sequence (or checksum), and ED/FS are the end delimiter and frame status. The Internet Engineering Task Force defined a standard for transmission of the Internet Protocol (which would be the protocol data unit in this case) over FDDI. It was first proposed in June 1989[5] and revised in 1990.[6] Some aspects of the protocol were compatible with the IEEE 802.2 standard for logical link control. For example, the 48-bit MAC addresses that became popular with the Ethernet family. Thus other protocols such as the Address Resolution Protocol (ARP) could be common as well.

(e) Enumerate on TCP header and working of TCP and differentiate TCP and UDP with frame format.

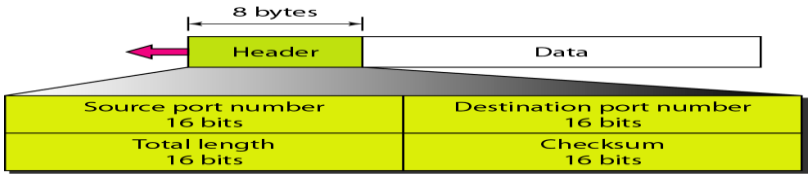
TCP is a connection-oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.

TCP segment format



Source Port. 16 bits.
Destination Port. 16 bits.
Sequence Number. 32 bits. The sequence number of the first data byte in this segment. If the SYN bit is set, the sequence number is the initial sequence number and the first data byte is initial sequence number + 1.
Acknowledgment Number. 32 bits. If the ACK bit is set, this field contains the value of the next sequence number the sender of the segment is expecting to receive. Once a connection is established this is always sent.
Data Offset. 4 bits. The number of 32-bit words in the TCP header. This indicates where the data begins. The length of the TCP header is always a multiple of 32 bits.
reserved. 3 bits. Must be cleared to zero.

UDP segment format



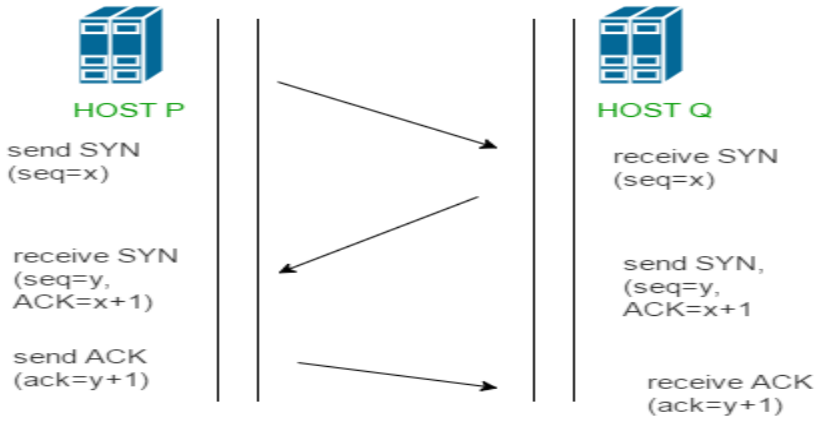
Difference between TCP and UDP

TCP	UDP
Reliability: TCP is connection-oriented protocol. When a file or message send it will get delivered unless connections fails. If connection lost, the server will request the lost part. There is no corruption while transferring a message.	*Reliability*: UDP is connectionless protocol. When you a send a data or message, you don't know if it'll get there, it could get lost on the way. There may be corruption while transferring a message.
Ordered: If you send two messages along a	*Ordered*: If you send two messages out, you don't

connection, one after the other, you know the first message will get there first. You don't have to worry about data arriving in the wrong order.	know what order they'll arrive in i.e. **no ordered**
Heavyweight: - when the low level parts of the TCP "stream" arrive in the wrong order, resend requests have to be sent, and all the out of sequence parts have to be put back together, so requires a bit of work to piece together.	*Lightweight*: No ordering of messages, no tracking connections, etc. It's just fire and forget! This means it's a lot quicker, and the network card / OS have to do very little work to translate the data back from the packets.
Streaming: Data is read as a "stream," with nothing distinguishing where one packet ends and another begins. There may be multiple packets per read call.	*Datagrams*: Packets are sent individually and are guaranteed to be whole if they arrive. One packet per one read call.
Examples: World Wide Web (Apache TCP port 80), e-mail (SMTP TCP port 25 Postfix MTA), File Transfer Protocol (FTP port 21) and Secure Shell (OpenSSH port 22) etc.	*Examples*: Domain Name System (DNS UDP port 53), streaming media applications such as IPTV or movies, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) and online multiplayer games etc

(f) Explain the three way handshaking protocol to establish the transport level connection

TCP provides reliable communication with something called **Positive Acknowledgement with .** three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established. Let us delve how this mechanism works :



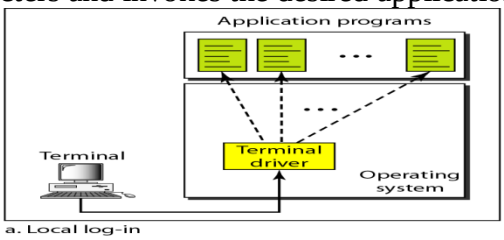
Step 1 (SYN) : In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with

- Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with
- Step 3 (ACK) : In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start eh actual data transfer

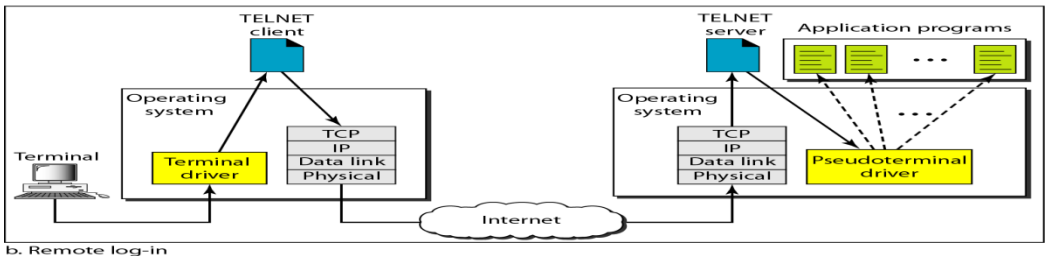
The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.

(g) Elaborate about TELNET and its working procedure.

TELNET is a general-purpose client-server program that lets a user access any application program on a remote computer; in other words, it allows the user to log onto a remote computer. After logging on, a user can use the services available on the remote computer and transfer the results back to the local computer. TELNET is an abbreviation for terminal network. TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system. Local Login When a user logs onto a local time-sharing system, it is called local login. As a user types at a terminal or at a workstation running a terminal emulator, the keystrokes are accepted by the terminal driver. The terminal driver passes the characters to the operating system. The operating system, in turn, interprets the combination of characters and invokes the desired application program or utility



a. Local log-in



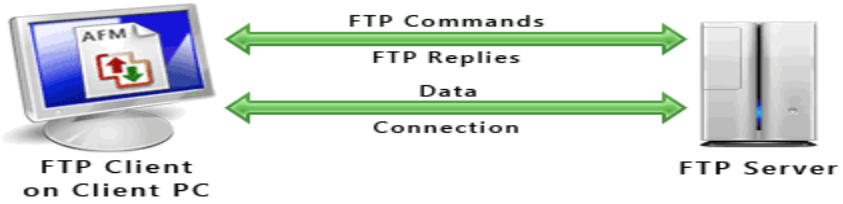
b. Remote log-in

The mechanism, however, is not as simple as it seems because the operating system may assign special meanings to special characters. For example, in UNIX some combinations of characters have special meanings, such as the combination of the control character with the character z means suspend; the combination of the control character with the character c means abort; and so on. Whereas these special situations do not create any problem in local login because the terminal emulator and the terminal driver know the exact meaning of each character or combination of characters, they may create problems in remote login. Which process should interpret special characters? The client or the server? We will clarify this situation later in this section. Remote Login When a user wants to access an application program or utility located on a remote machine, he or she performs remote login. Here the TELNET client and server programs come into use. The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them. The characters are sent to the TELNET client, which transforms the characters to a universal character set called network virtual terminal characters and delivers them to the local TCP/IP stack.

(h) How does FTP work? Differentiate between passive and active FTP.

File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. For example, two systems may use different file name conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach. FTP differs from other client/server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication. We need to transfer only a line of command or a line of response at a time. The data connection, on the other hand, needs more complex rules due to the variety of data types transferred. However, the difference in complexity is at the FTP level, not TCP.For TCP, both connections are treated the same.

Transferring files from a client computer to a server computer is called "uploading" and transferring from a server to a client is "downloading".



Requirements for using FTP

1. An FTP client like Auto FTP Manager installed on your computer
2. Certain information about the FTP server you want to connect to:
   a. The FTP server address. This looks a lot like the addresses you type to browse web sites.
   Example : Server address is "ftp.videodesk.net".
   Sometimes the server address will be given as a numeric address, like "64.185.225.87".
   b. A user name and password. Some FTP servers let you connect to them anonymously. For anonymous connections, you do not need a user name and password.

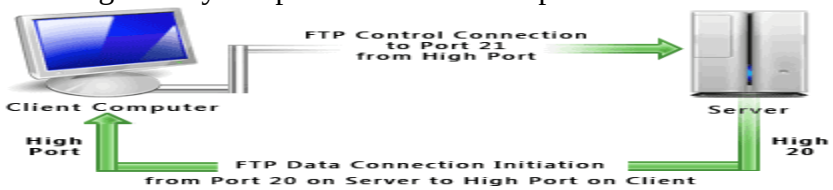
To transfer files, provide your client software (Auto FTP Manager) with the server address, user name, and password. After connecting to the FTP server, you can use Auto FTP Manager's File Manager to upload, download and delete files. Using the File Manager is a lot like working with Windows Explorer.

FTP uses one connection for commands and the other for sending and receiving data. FTP has a standard port number on which the FTP server "listens" for connections. A port is a "logical connection point" for communicating using the Internet Protocol (IP). The standard port number used by FTP servers is 21 and is used only for sending commands. Since port 21 is used exclusively for sending commands, this port is referred to as a command port. For example, to get a list of folders and files present on the FTP server, the FTP Client issues a "LIST" command. The FTP server then sends a list of all folders and files back to the FTP Client. So what about the internet connection used to send and receive data? The port that is used for

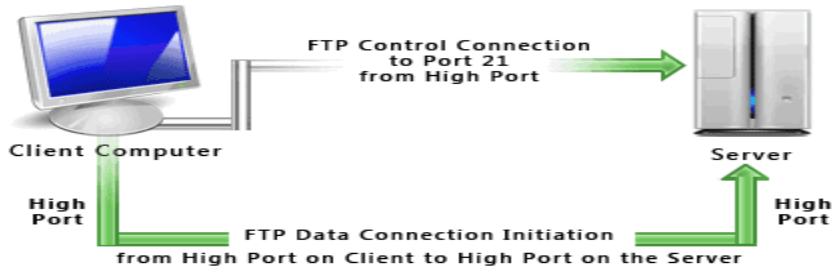
transferring data is referred to as a data port. The number of the data port will vary depending on the "mode" of the connection. (See below for Active and Passive modes.)

Active and Passive Connection Mode

The FTP server may support Active or Passive connections or both. In an Active FTP connection, the client opens a port and listens and the server actively connects to it. In a Passive FTP connection, the server opens a port and listens (passively) and the client connects to it. You must grant Auto FTP Manager access to the Internet and to choose the right type of FTP Connection Mode. Most FTP client programs select passive connection mode by default because server administrators prefer it as a safety measure. Firewalls generally block connections that are "initiated" from the outside. Using passive mode, the FTP client (like Auto FTP Manager) is "reaching out" to the server to make the connection. The firewall will allow these outgoing connections, meaning that no special adjustments to firewall settings are required. If you are connecting to the FTP server using Active mode of connection you must set your firewall to accept connections to the port that your FTP client will open. However, many Internet service providers block incoming connections to all ports above 1024. Active FTP servers generally use port 20 as their data port.



It's a good idea to use Passive mode to connect to an FTP server. Most FTP servers support the Passive mode. For Passive FTP connection to succeed, the FTP server administrator must set his / her firewall to accept all connections to any ports that the FTP server may open. However, this is the server administrator's problem (and standard practice forj servers). You can go ahead, make and use FTP connections.



Once the FTP Client manages to open the internet connections, one for command and one for data, it starts communicating with the FTP server. You are now ready to transfer your files and folders between the two connected computers with Auto FTP Manager.

SECTION – C

3 (i) Explain functionalities of every layer in OSI reference model with neat block diagram.

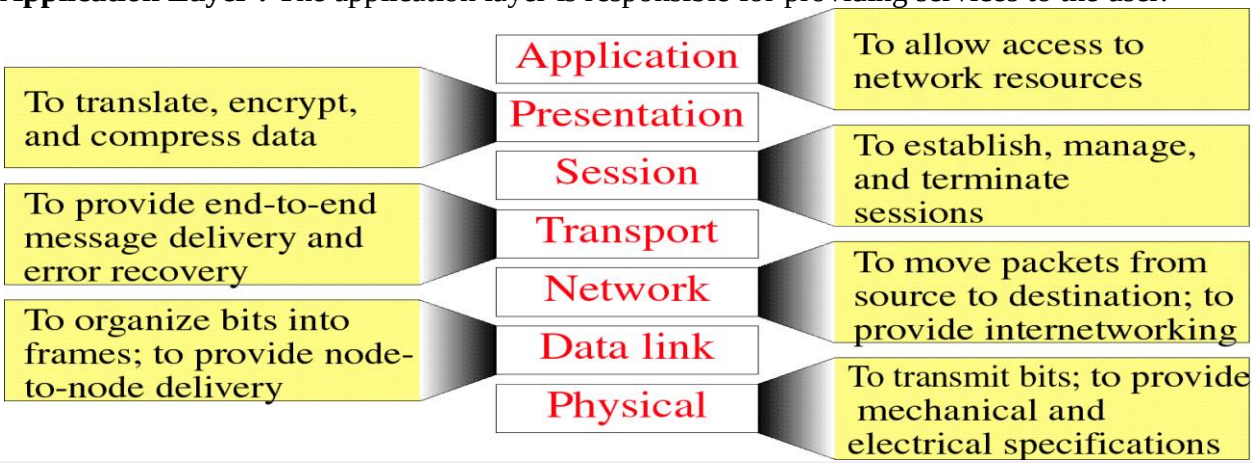
Physical Layer : The physical layer is responsible for transmitting individual bits from one node to the next.

Data Link Layer : The data link layer is responsible for transmitting frames from one node to the next.

Network Layer: The network layer is responsible for the delivery of packets from the original source to the final destination.

Transport Layer : The transport layer is responsible for delivery of a message from one process to another.

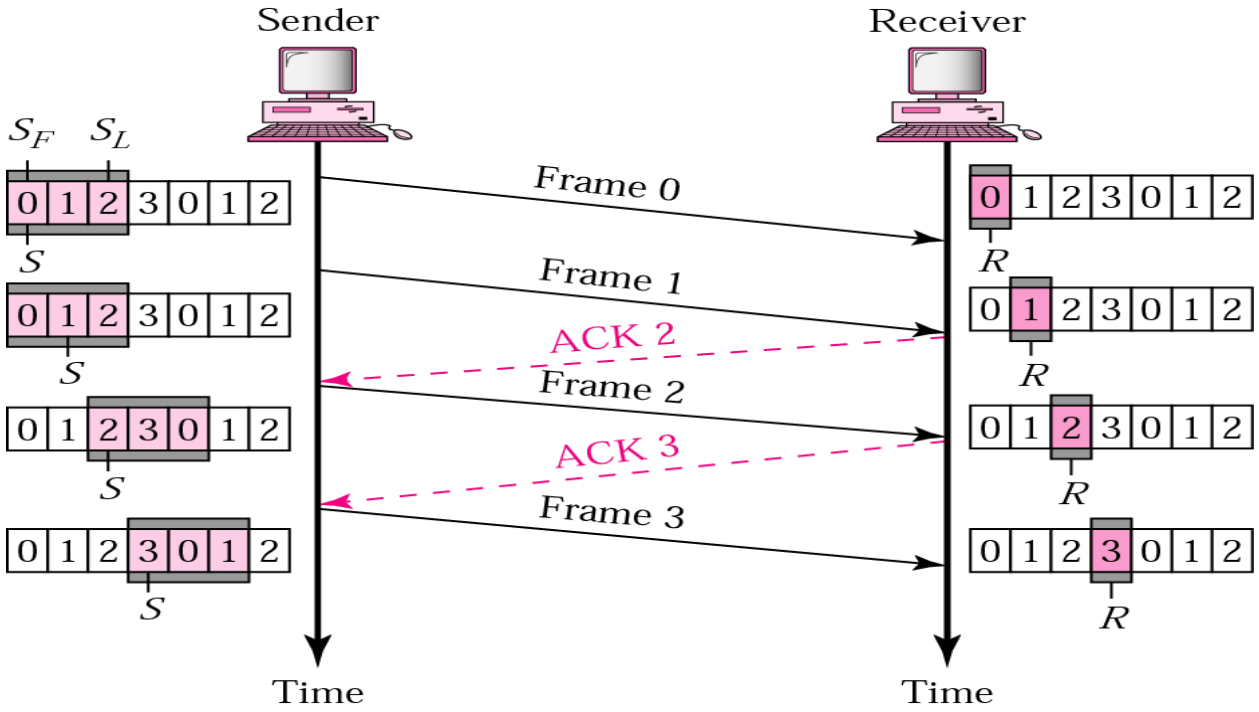
Application Layer : The application layer is responsible for providing services to the user.



OSI 7-layer model and roles of functions modules		
Layer	Name	Functions / Roles
7	Application Layer	It provides interfaces to use networks for software (server/client application) which uses networks (data communications). It defines the processes that the users directly interact with, such as telnet and ftp.
6	Presentation Layer	It converts the data gotten from layer 5 into user-friendly formats and the data sent from layer 7 into formats suitable for communication. In short, it converts the formats of data gotten from layer 7. It defines the data expression such as compression and character code.
5	Session Layer	Based on the specification of each application which uses networks, it establishes sessions on communications. It defines connections, terminations and so on between computers.
4	Transport Layer	It provides basic data transfer services, ensuring the reliability of data transfer. It provides mechanisms for the establishment, maintenance, and termination of virtual circuits, transport fault detection and recovery, and information flow control. While the session layer is based on requests from applications, all the functions of the transport layer are provided for all data in common.

3	Network Layer	It decides appropriate communication paths between two hosts (end systems) which communicate on networks, based on IP Addresses. It only decides communication paths and is not involved in the quality of communications.
2	Data Link Layer	It defines communication methods between computers connected to networks directly. It realizes the specification of hosts to be communicated and reliable data transfer, based on MAC Addresses (physical addresses). In other words, It realizes the reliable transmission between two points based on MAC addresses. The difference from layer 3 is that while the network layer decides paths including them between networks, the data link layer acquires the communication between adjacent nodes (exactly, broadcast segments and broadcast domains) within a network. The difference from layer 4 is that the data link layer provides interfaces for applications (for example, provides services for the session layer) and realise the highly functional data transmission.
1	Physical Layer	It is a protocol to decide physical signals and connection methods in networks. It defines function modules which define the maximum transfer rate, D/A-A/D conversion and maximum transfer (communication) distance to implement, cable materials and connector shapes. (Cables and connector are called network media.)

(ii) Illustrate the performance issues for GO-BACK-N data link protocol.



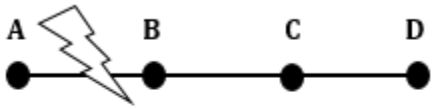
4 . Describe the problem of count to infinity associated with distance vector routing technique.

Count to infinity problem:

1. One of the important issue in Distance Vector Routing is County of Infinity Problem.
2. Counting to infinity is just another name for a routing loop.
3. In distance vector routing, routing loops usually occur when an interface goes down.
4. It can also occur when two routers send updates to each other at the same time.

Example:

Link Between A & B is Broken



	A	B	C	D
A	0, -	1, A	2, B	3, C
B	1, B	0, -	2, C	3, D
C	2, B	1, C	0, -	1, C
D	3, B	2, C	1, D	0, -

Now imagine that the link between A and B is cut. At this time, B corrects its table. After a specific amount of time, routers exchange their tables, and so B receives C's routing table. Since C doesn't know what has happened to the link between A and B, it says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A). B receives this table and thinks there is a separate link between C and A, so it corrects its table and changes infinity to 3 (1 for B to C, and 2 for C to A, as C said). Once again, routers exchange their tables. When C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said). This process loops until all nodes find out that the weight of link to A is infinity. This situation is shown in the table below. In this way, experts say DV algorithms have a slow convergence rate.

	B	C	D
Sum of Weight to A after link cut	∞, A	2, B	3, C
Sum of Weight to A after 1st updating	3, C	2, B	3, C
Sum of Weight to A after 2nd updating	3, C	4, B	3, C
Sum of Weight to A after 3rd updating	5, C	4, B	5, C
Sum of Weight to A after 4th updating	5, C	6, B	5, C
Sum of Weight to A after 5th updating	7, C	6, B	7, C
Sum of Weight to A after nth updating	.....	....	....
∞	∞	∞	∞

5. Explain the SNMP protocols in detail.

A large part of being a system administrator is collecting accurate information about your servers and infrastructure. There are a number of tools and options for gathering and processing this type of information. Many of them are built upon a technology called **SNMP**.

SNMP stands for simple network management protocol. It is a way that servers can share information about their current state, and also a channel through which an administer can modify pre-defined values. While the protocol itself is very simple, the structure of programs that implement SNMP can be very complex.

In this guide, we will introduce you to the basics of the SNMP protocol. We will go over its uses, the way that the protocol is typically used in a network, the differences in its protocol versions, and more.

Basic Concepts

SNMP is a protocol that is implemented on the application layer of the networking stack (click here to learn about networking layers). The protocol was created as a way of gathering information from very different systems in a consistent manner. Although it can be used in connection to a diverse array of systems, the method of querying information and the paths to the relevant information are standardized.

There are multiple versions of the SNMP protocol, and many networked hardware devices implement some form of SNMP access. The most widely used version is SNMPv1, but it is in many ways insecure. Its popularity largely stems from its ubiquity and long time in the wild. Unless you have a strong reason not to, we recommend you use SNMPv3, which provides more advanced security features.

In general, a network being profiled by SNMP will mainly consist of devices containing **SNMP agents**.

An agent is a program that can gather information about a piece of hardware, organize it into predefined entries, and respond to queries using the SNMP protocol.

The component of this model that queries agents for information is called an SNMP **manager**. These machines generally have data about all of the SNMP-enabled devices in their network and can issue requests to gather information and set certain properties.

SNMP Managers

An SNMP manager is a computer that is configured to poll SNMP agent for information. The management component, when only discussing its core functionality, is actually a lot less complex than the client configuration, because the management component simply requests data.

The manager can be any machine that can send query requests to SNMP agents with the correct credentials. Sometimes, this is implemented as part of a monitoring suite, while other times this is an administrator using some simple utilities to craft a quick request.

Almost all of the commands defined in the SNMP protocol (we will go over these in detail later) are designed to be *sent* by a manager component. These include GetRequest, GetNextRequest, GetBulkRequest, SetRequest, InformRequest, and Response. In addition to these, a manager is also designed to *respond to* Trap, and Response messages.

SNMP Agents

SNMP agents do the bulk of the work. They are responsible for gathering information about the local system and storing them in a format that can be queried.updating a database called the "management information base", or **MIB**.

The MIB is a hierarchical, pre-defined structure that stores information that can be queried or set. This is available to well-formed SNMP requests originating from a host that has authenticated with the correct credentials (an SNMP manager).

The agent computer configures which managers should have access to its information. It can also act as an intermediary to report information on devices it can connect to that are not configured for SNMP traffic. This provides a lot of flexibility in getting your components online and SNMP accessible.

SNMP agents respond to most of the commands defined by the protocol. These include GetRequest, GetNextRequest, GetBulkRequest, SetRequest and InformRequest. In addition, an agent is designed to send Trap messages.

SNMP Protocol Commands

One of the reasons that SNMP has seen such heavy adoption is the simplicity of the commands available. There are very few operations to implement or remember, but they are flexible enough to address the utility requirements of the protocol.

The following PDUs, or protocol data units, describe the exact messaging types that are allowed by the protocol:

- **Get**: A Get message is sent by a manager to an agent to request the value of a specific OID. This request is answered with a Response message that is sent back to the manager with the data.
- **GetNext**: A GetNext message allows a manager to request the next sequential object in the MIB. This is a way that you can traverse the structure of the MIB without worrying about what OIDs to query.
- **Set**: A Set message is sent by a manager to an agent in order to change the value held by a variable on the agent. This can be used to control configuration information or otherwise modify the state of remote hosts. This is the only write operation defined by the protocol.
- **GetBulk**: This manager to agent request functions as if multiple GetNext requests were made. The reply back to the manager will contain as much data as possible (within the constraints set by the request) as the packet allows.
- **Response**: This message, sent by an agent, is used to send any requested information back to the manager. It serves as both a transport for the data requested, as well as an acknowledgement of receipt of the request. If the requested data cannot be returned, the response contains error fields that can be set with further information. A response message must be returned for any of the above requests, as well as Inform messages.
- **Trap**: A trap message is generally sent by an agent to a manager. Traps are asynchronous notifications in that they are unsolicited by the manager receiving them. They are mainly used by agents to inform managers of events that are happening on their managed devices.
- **Inform**: To confirm the receipt of a trap, a manager sends an Inform message back to the agent. If the agent does not receive this message, it may continue to resend the trap message.

With these seven data unit types, SNMP is capable of querying for and sending information about your networked devices.