B.Tech 4th Year, ECE

Subject: Data Communication Networks (REC-701)

Solutions

SECTION -A

Q1 (a): (i) ASCII (ii) EBCDIC (iii) image file

(b) (i)Transmitter (ii)Receiver (iii) Message (iv) Sender (v) Protocol

(c) Network **protocols** are **needed** because it include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received.

(d) Multipurpose Internet Mail Extensions

(e) In cryptography, a **certificate authority** or **certification authority** (CA) is an entity that issues digital **certificates**.

2(a) **The OSI Reference Model:**

The OSI model (minus the physical medium) is shown in Fig. This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995(Day, 1995). The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.

The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

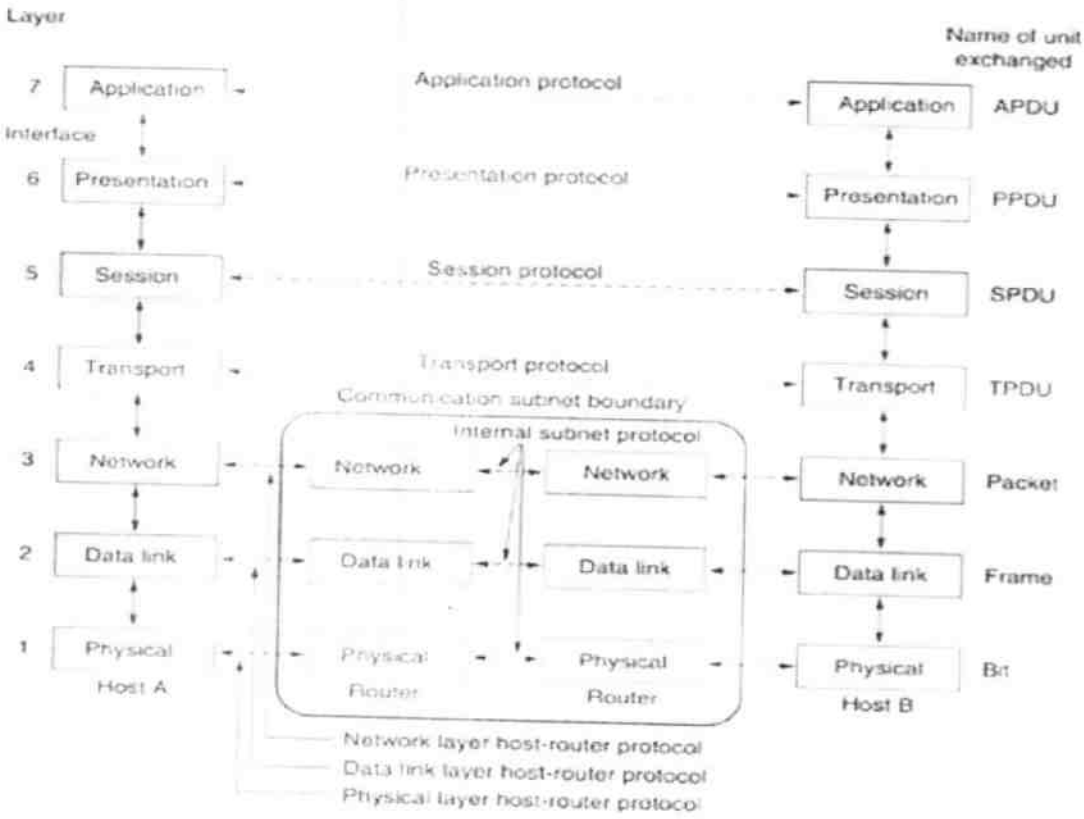


Fig.4: The OSI reference model

The Physical Layer:

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.

The Data Link Layer:

The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmits the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.

Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, this flow regulation and the error handling are integrated.

The Network Layer:

The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example, a terminal session (e.g., a login to a remote machine). Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. The control of such congestion also belongs to the network layer. More generally, the quality of service provided (delay, transit time, jitter, etc.) is also a network layer issue.

When a packet has to travel from one network to another to get to its destination, many problems can arise. The addressing used by the second network may be different from the first one. The second one may not accept the packet at all because it is too large. The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected. In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

The Transport Layer:

The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology. The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent. However, other possible kinds of transport service are the transporting of isolated messages, with no guarantee about the order of delivery, and the broadcasting of messages to multiple destinations. The type of service is determined when the connection is established.

The transport layer is a true end-to-end layer, all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages. In the lower layers,

the protocols are between each machine and its immediate neighbours, and not between the ultimate source and destination machines, which may be separated by many routers.

The Session Layer:

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

The Presentation Layer:

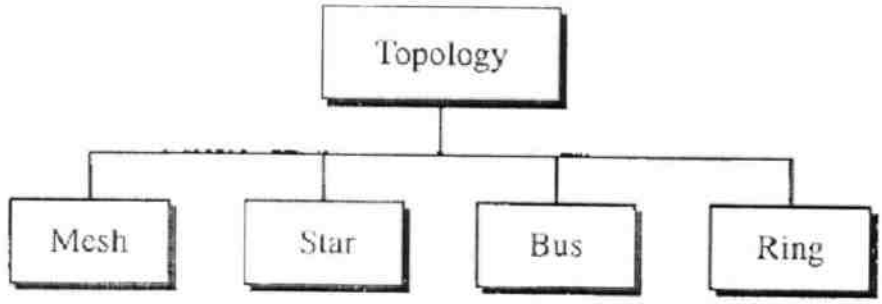
The presentation layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

The Application Layer:

The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.

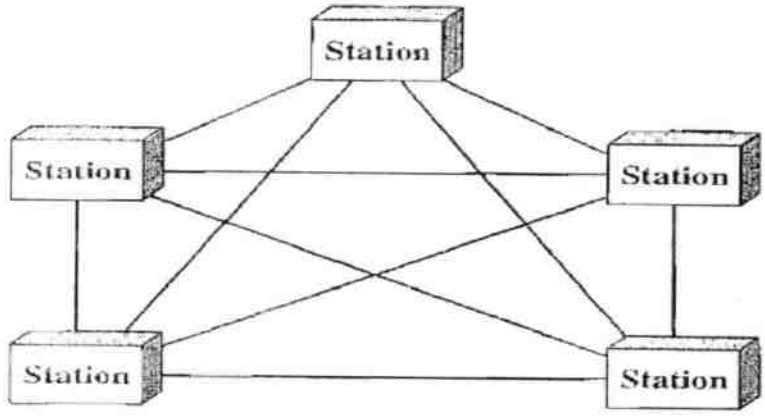
Physical Topology

The term *physical topology* refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring



Mesh: In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - 1 nodes, node 2 must be connected to $n - 1$ nodes, and finally node n must be connected to n - 1 nodes. We need $n(n - 1)$ physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need $n(n - 1)/2$ duplex-mode links.

To accommodate that many links, every device on the network must have $n - 1$ input/output *(VO)* ports to be connected to the other n - 1 stations.



Advantages:

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages:

1. Disadvantage of a mesh are related to the amount of cabling because every device must be connected to every other device, installation and reconnection are difficult.
2. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

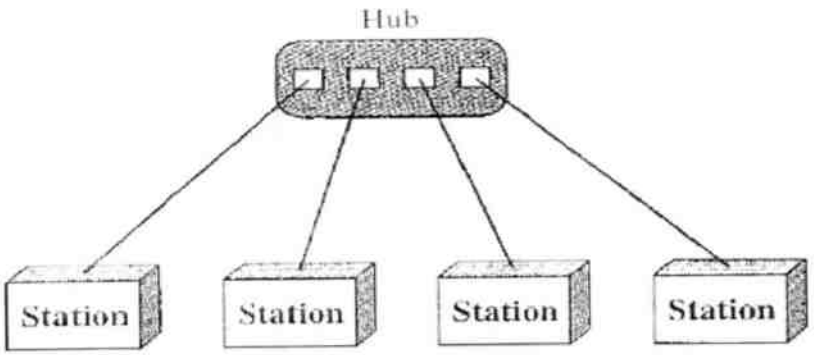
For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

Star Topology:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device .

A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

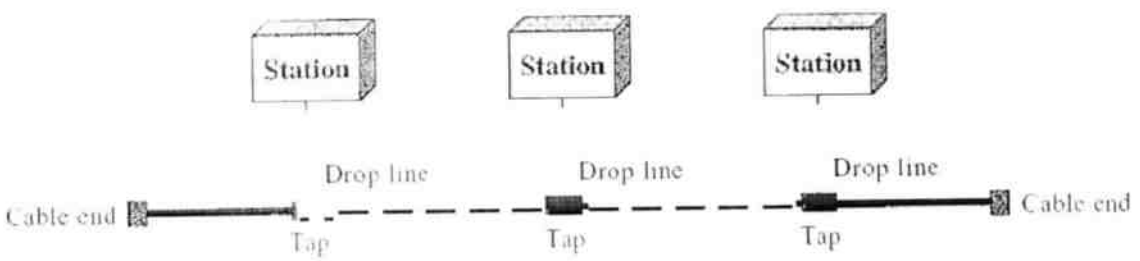
Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.



One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

Bus Topology:

The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network



Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

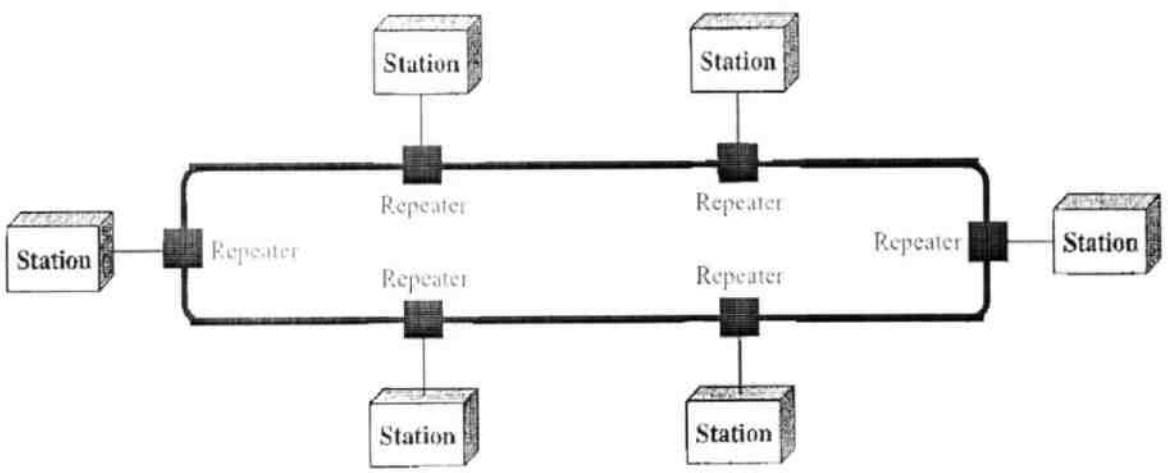
Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

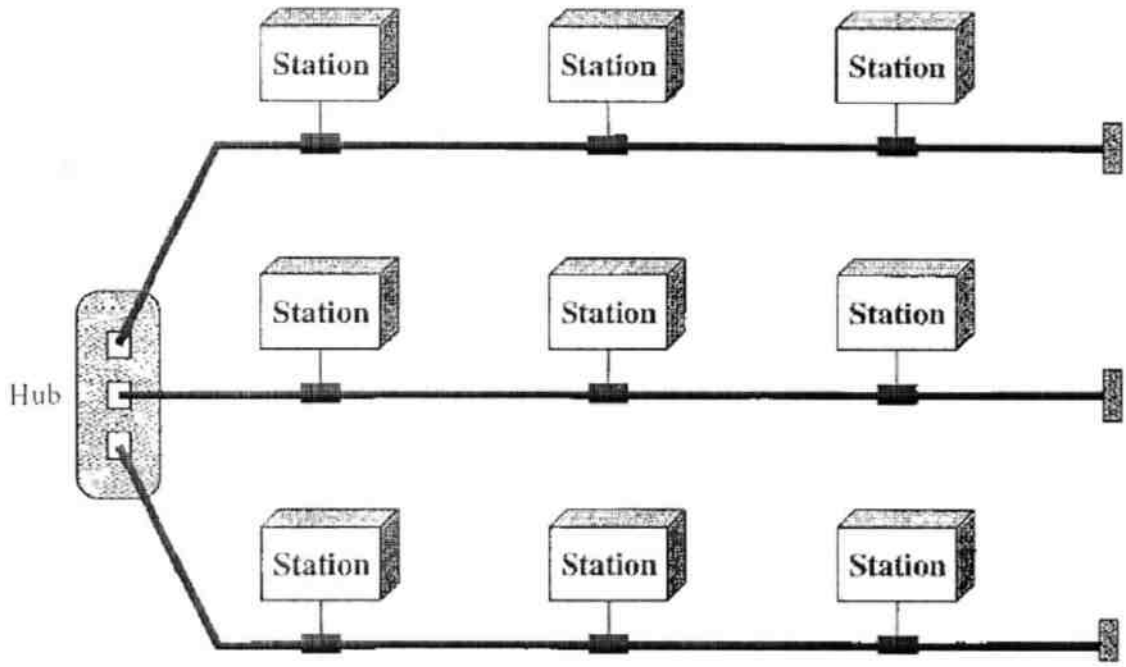
Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular.

Ring Topology In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along



A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break. Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular. Hybrid Topology A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure



2(c)

At the physical **layer**, communication is direct between devices. At the higher **layers**, however, communication must move down through the **layers** on sending device, over to receiving device, and then back up through the **layers**.

2(d)

Essential components of mail system

In order to learn how email system works or how email travels from source to destination, we have to understand following essential components.

Email Client or Mail User Agent (UA)

An email client or user agent is a software or program which is used to compose and read the email. At sender side, it is used to compose and send the email. At receiver side, it is used to read and reply the received email. MS Outlook, MacOS Mail, /bin/mail, Alpine and Gmail are some examples of email client.

Mail Submission Agent (MSA)

MSA takes mail from user agent and deliver them to a mail transfer agent. MSA was developed later in email system. It was invented to reduce some burden from MTA.

If implemented, MSA sits between user agent and mail transfer agent. It secures connection between UA and MTA by implementing encryption and authentication. Besides this, it can perform a lot more tasks based on its configuration such as rewriting mail header and performing security checks.

3(a):-

Stands for "**Peer to Peer**." In a **P2P** network, the "**peers**" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a **P2P** network becomes a file server as well as a client.

36)

Different Layers of TCP/IP Reference Model

Below we have discussed the 4 layers that form the TCP/IP reference model:

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.

3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

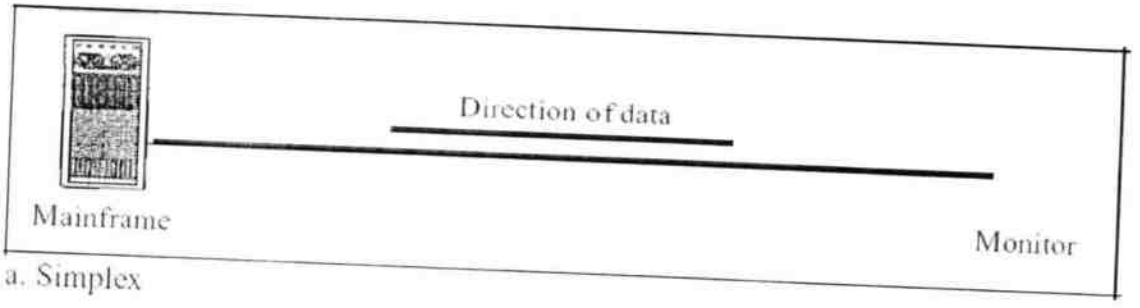
1. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
    - **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
    - **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Q4(a)

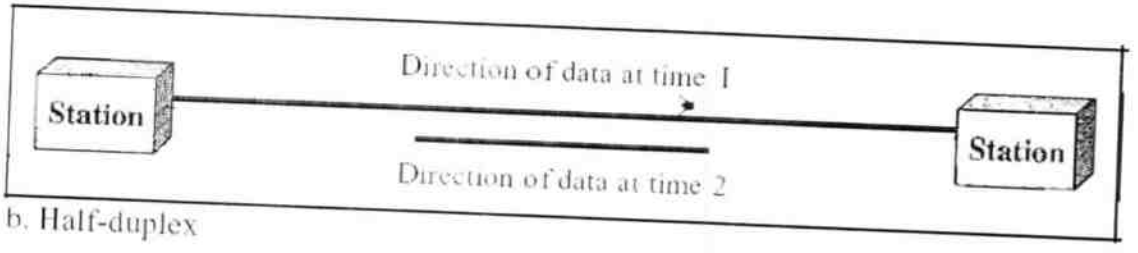
File Transfer Protocol (**FTP**) is a client/server **protocol** used for **transferring** files to or exchanging files with a host computer. ... Anonymous **FTP** allows users to access files, programs and other **data** from the Internet without the need for a user ID or password.

4(b) **Data Flow**

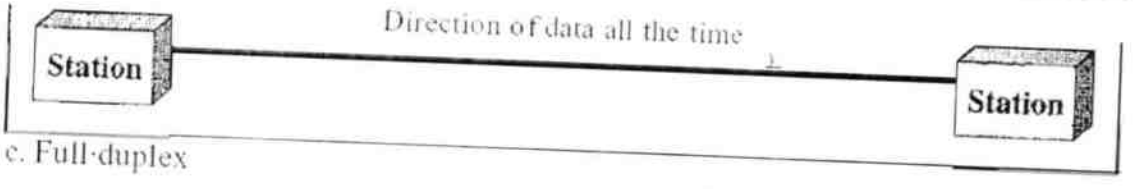
Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure



a. Simplex



b. Half-duplex



c. Full-duplex

Simplex:

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex:

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa The half-duplex mode is like a one-lane road with traffic allowed in both directions.

When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex:

In full-duplex both stations can transmit and receive simultaneously (see Figure c). The full-duplex mode is like a tW<D-way street with traffic flowing in both directions at the same time. In full-duplex mode, si~nals going in one direction share the capacity of the link: with signals going in the other din~c~on. This sharing can occur in two ways: Either the link must contain two physically separate t:nmsmissilDn paths, one for sending and the other for receiving; or the capacity of the ch:arillilel is divided between signals traveling in both directions. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

5(a)

Logical Address: An IP address of the system is called logical address. This address is the combination of Net ID and Host ID. This address is used by network layer to identify a particular network (source to destination) among the networks. This address can be changed by changing the host position on the network. So it is called logical address.

Physical address: Each system having a NIC (Network Interface Card) through which two systems physically connected with each other with cables. The address of the NIC is called Physical address or mac address. This is specified by the manufacturer company of the card. This address is used by data link layer.

Port Address: There are many application running on the computer. Each application run with a port no. (Logically) on the computer. This port no. for application is decided by the Kernal of the OS. This port no. is called port address.

5(b)

Digital Signature is a process that guarantees that the contents of a message have not been altered in transit.

When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your public and private key pair.

Your client can still read it, but the process creates a "signature" that only the server's public key can decrypt. The client, using the server's public key, can then validate the sender as well as the integrity of message contents.

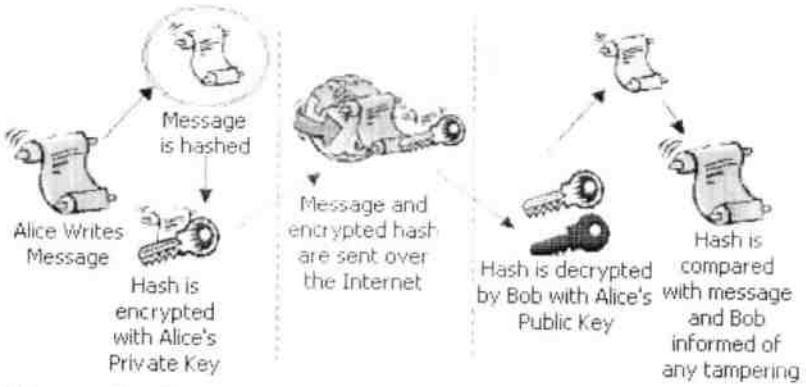
Whether it's an email, an online order or a watermarked photograph on eBay, if the transmission arrives but the digital signature does not match the public key in the digital certificate, then the client knows that the message has been altered.

How does a Digital Signature Work?

The digital signature can be considered as a numerical value that is represented as a sequence of characters. The creation of a digital signature is a complex mathematical process that can only be created by a computer.

Consider a scenario where Alice has to digitally sign a file or an email and send it to Bob.

- Alice selects the file to be digitally signed or clicks on 'sign' in her email application
- The hash value of the file content or the message is calculated by Alice's computer
- This hash value is encrypted with Alice's Signing Key (which is a Private Key) to create the Digital Signature.
- Now, the original file or email message along with its Digital Signature are sent to Bob.
- After Bob receives the signed message, the associated application (such as email application) identifies that the message has been signed. Bob's computer then proceeds to:
    - Decrypt the Digital Signature using Alice's Public Key
    - Calculate the hash of the original message
    - Compare the (a) hash it has computed from the received message with the (b) decrypted hash received with Alice's message.
- Any difference in the hash values would reveal tampering of the message.



How do I create a Digital Signature?

You can obtain a digital signature from a reputable certificate authority such as Section, or you can create it yourself. You need a digital certificate to digitally sign a document. However, if you create and use a self-signed certificate the recipients of your documents will not be able to verify the authenticity of your digital signature. They will have to manually trust your self-signed certificate.

If you want the recipients of your documents to be able to verify the authenticity of your digital signature then you must obtain a digital certificate from a reputable CA. After downloading and installing the certificate - you will be able to use the 'Sign' and 'Encrypt' buttons on your mail client to encrypt and digitally sign your emails. This makes more sense in a business scenario, as it assures the recipient that it was genuinely sent by you and not by some impersonator.

Other Uses for Digital Signature

Sometimes you need proof that the document came from you and no one has tampered with it since you sent it. Digital Signature with your SSL Certificate fills the bill.

On the other hand, sometimes you need to prove that a document came from someone else and has not been altered along the way. In legal matters, for example, you may need to prove that a contract has not been altered since someone sent it as an email.

Because the computer tenaciously pairs the Digital Signature to one saved version of the document, it is nearly impossible to repudiate a digitally signed document.

Or, if you are a developer distributing software online, you may need to reassure your customers that your executables really are from you. Put a Code Signing Certificate in your toolkit.

Types of digital signatures

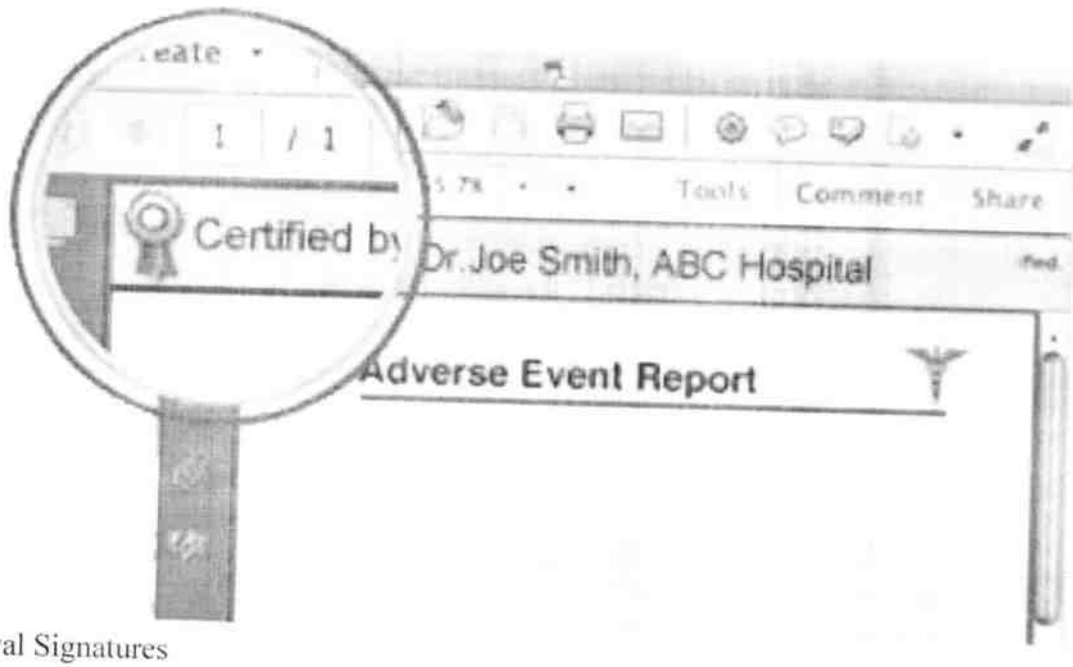
Different document processing platforms support and allow the creation of different types of digital signatures.

- Adobe supports - certified and approval digital signatures
- Microsoft Word supports - visible and non-visible digital signatures

Certified Signatures

Adding a certifying signature to a PDF document indicates that you are the author of the document and want to secure the document against tampering.

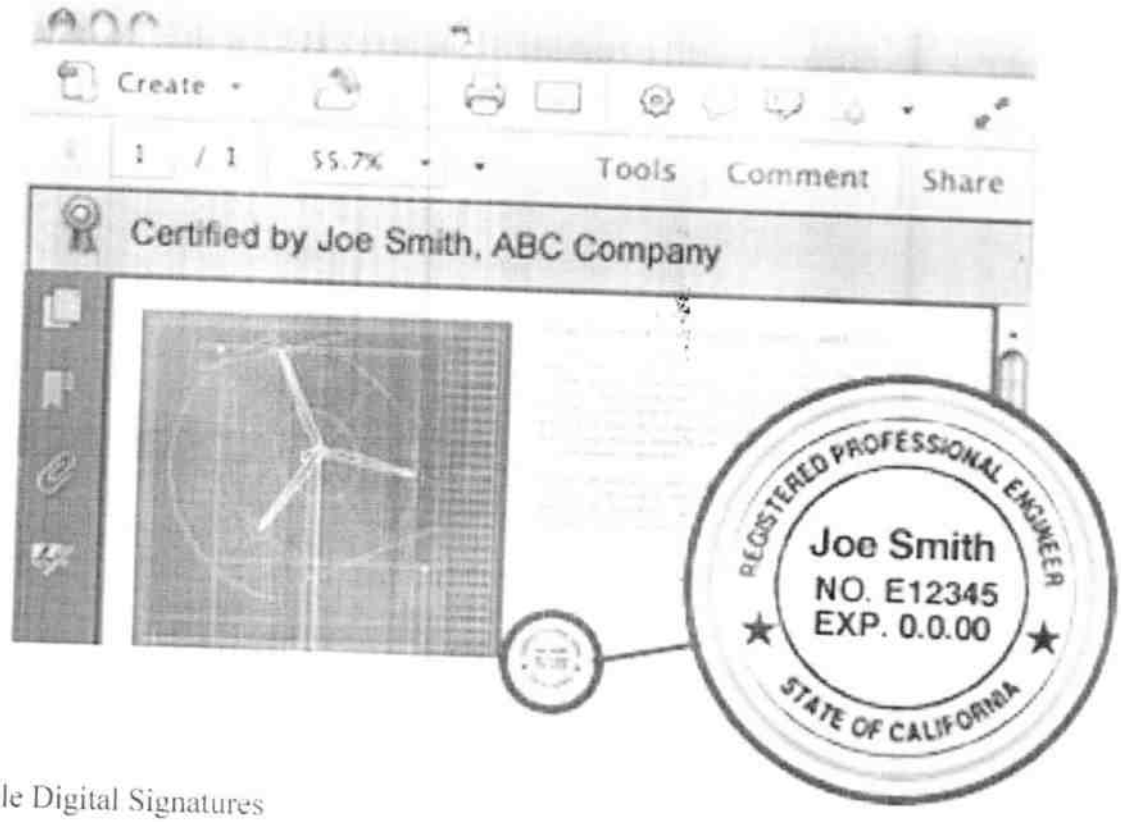
Certified PDF documents display a unique blue ribbon across the top of the document. It contains the name of the document signer and the certificate issuer to indicate the authorship and authenticity of the document.



Approval Signatures

Approval signatures on a document can be used in your organization's business workflow. They help optimize your organization's approval procedure. The process involves capturing approvals made by you and other individuals and embedding them within the PDF document.

Adobe allows signatures to include details such as an image of your physical signature, date, location, and official seal.



Visible Digital Signatures

These allow a single user or multiple users to digitally sign a single document. The signatures would appear on the document in the same way as signatures are applied on a physical document.

Invisible Digital Signatures

Documents with invisible digital signatures carry a visual indication of a blue ribbon in the task bar. You can use invisible digital signatures when you do not have to or do not want to display your signature, but you need to provide indications of the authenticity of the document, its integrity, and its origin.