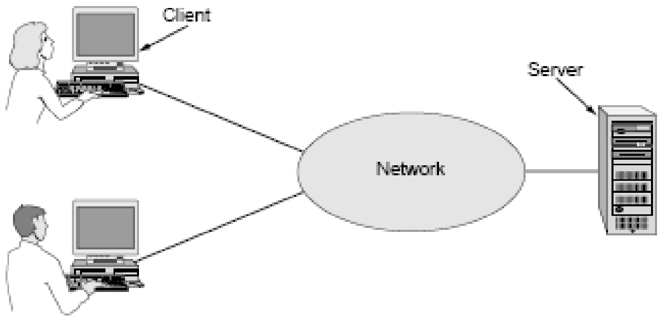
INTRODUCTION

The 20th century key technology has been information gathering, processing, and distribution. The development of the personal computer brought tremendous changes for business, industry, science, and education. The similar revolution is occurring in computer networks and data communications also. Technological advances are making it possible to carry more and faster data signals. The goal of computer networks is to exchange data such as text, audio and video from all parts of the world as efficiently as possible. For example we want to access the Internet to download and upload information quickly and accurately at any time.

When we communicate with the other that means we are sharing information. This kind of sharing can be local or remote. Suppose in between two persons local communications usually occurs face to face, where as remote communication takes place over two distinct places separated. Data communication is the exchange of data between two devices via some form of transmission medium such as a wire cable.

Computer Network: A network is a set of devices (often theses are known as nodes, computers, terminals, systems) connected by a communication link. A node can be a computer, printer or any other device. This device must be capable of sending and/or receiving data generated by other nodes of the network. It is an interconnected collection of autonomous computers. Two computers are said to be inter connected if they are able to exchange information. This connection need not be via a copper wire, fiber optics, microwave and communication satellites can also be used.



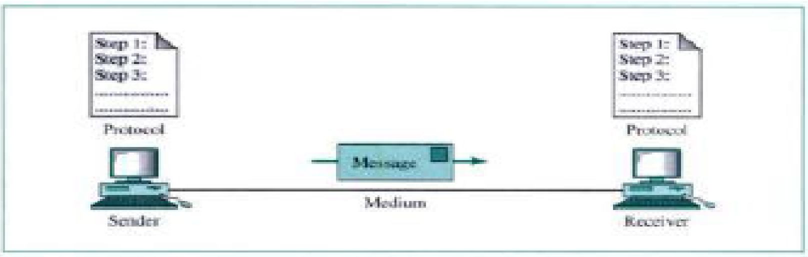
The effectiveness of data communication depends on the following four fundamental characteristics:

1. **Delivery:** The system must deliver information to the correct destination. Data must be received only by the intended device or user.
2. **Accuracy:** The system must deliver information accurately(reliably). Data should not be altered anywhere during the transmission. Such data is considered as uncorrected(unaltered) and will be accepted by the receiver.
3. **Timeliness:** The system must deliver data in timely manner. Data that is delivered late is not accepted and it is considered as useless.

4. **Jitter:** It refers to the variation in packet arrival time. It has the un even delivery in case of audio and video data. It occurs mostly in multimedia data.

Components of Computer Network:

A computer network system has five components that are participated in data communication.



1. **Message:** This is the kind of data to be transferred. Types of data are text, numbers, pictures, audio and video.
2. **Sender (source):** It is a device or user who sends the data. That is the owner of the information. It can be a computer, user, workstation, telephone, video camera, and so on.
3. **Receiver (Destination):** A device or user who receives information. It can be a computer, user, workstation, telephone, video camera, and so on.
4. **Transmission Medium:** This is a physical path by which a message or data travels from sender to receiver. Ex: twisted pair wires, coaxial cable, fiber optic cables, radio waves and satellite communications.
5. **Protocol:** A protocol is a set of rules and regulations that govern data communications. It is an agreement between the communication devices. This is a s/w which is developed to communicate data. Without a protocol, two devices may be connected but not communicate among themselves like a person speaking in English can not be understood by a person who speaks and understands only Telugu.

Representation of the Data:

Information can be represented in any of the form:

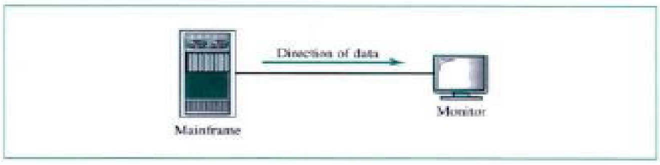
Text: Textual data is represented in bit pattern, that is a sequence of bits(0’s or 1’s). different sets of schemes are designed to represent text symbols. Each set is called a code, and the process of representing the symbols is known as coding(Encoding).

1. Unicode: uses 32 bits to represent a symbol or character used in any language in the world.
2. ASCII: Uses 7 bits to represent symbols. It is developed few decades ago. Now these 127 characters take place in the Unicode first 127 characters.

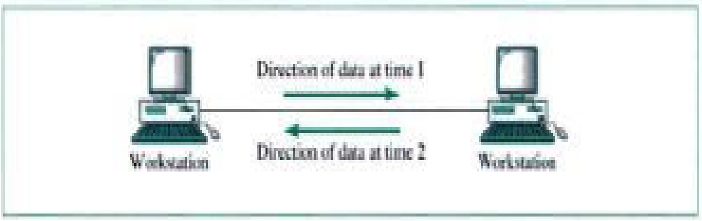
Numbers: Numbers are also represented by bit patterns. ASCII code is not used to represent numbers. The number is directly converted to a binary number to simplify mathematical operations. Different numbering systems are base 10(decimal), base 8(Octal), base 16(Hexa decimal), base 256(IP address).

Images: Images are also represented by bit patterns. An image is represented by a matrix of pixels(picture elements). Each pixel is a small dot. The size of pixels depends on resolution. There are several methods to represent images RGB, YCbCr,YCM,.. etc.
Audio: It refers to the recording or broadcasting of sound or music. This is different from text, numbers and images. It is continuous data, not discrete one.
Video: It refers to the recording or broadcasting of picture or movie.

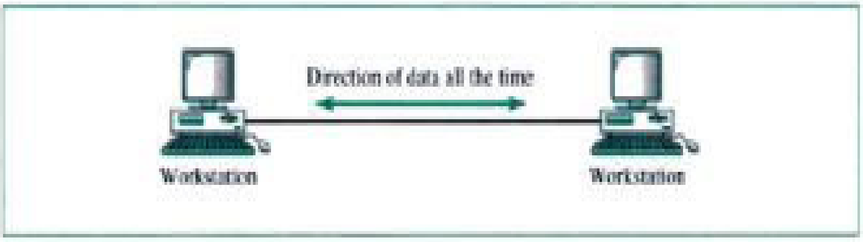
Direction of Data Flow (Data Transmission Modes): Communication between two devices can be simplex, half-duplex or full duplex.
Simplex: In simplex mode, communication is uni directional(only one way). That is only one of the two devices on the link can transmit data; the other one can receive. It uses the entire capacity of the channel to transmit data.
Ex: Keyboards and traditional monitors.



Half-Duplex: In half duplex mode, each station can both transmit and receive data, but not at the same time. When one device is sending, the other one can only receive, and vice versa. It is used when there is no need for communication in both directions at the same time. The entire capacity of the channel can be used for each direction.
Ex: walkie talkies.

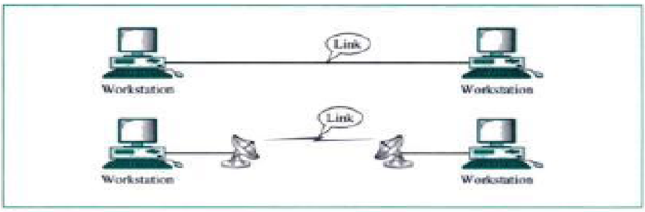


Full-Duplex: In full-duplex mode(also called duplex), both stations can transmit and receive simultaneously. The link must contain either the two physical separate transmission paths, one for sending and the other for receiving or the capacity of the entire channel is divided between signals traveling in both directions. This is used when communication in both directions is required all the time. However the capacity of the channel is divided in between the two directions.
Ex: Telephone

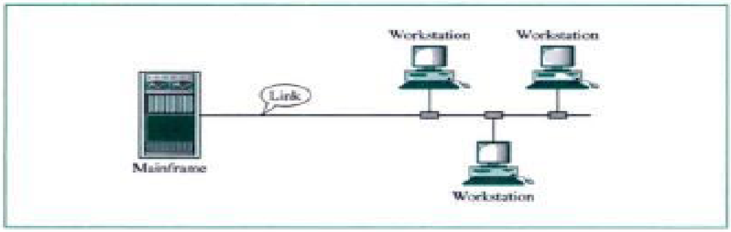


Physical Structures of the Network: A network is two or more devices connected through links. A link is a communication path that transfers data from one device to another. To see it looks like a line connecting two points(systems). But from the communication point of view there are two types of connections. Those are point to point and multi point.

Point to Point: A point to point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between these two devices.



Multi-Point: A multi point connection is one in which more than two specific devices share a single link. Here the capacity of the channel is shared either spatially or temporally(time). If several devices can use the same link simultaneously, it is a spatially shared connection. If users are taking turns then it is a time shared connection.



Distributed Processing: Most networks use distributed processing, in which a task or work is divided among multiple computers. Instead of one single large machine which is responsible for all aspects of process, separate computers are used to handle a subset of functions.

Comparison between Computer Networks and Distributed Systems

Computer Networks	**Distributed Systems**
The existence of multiple autonomous computers is visible	The existence of multiple autonomous computers is not visible
User can explicitly log on to the machine	User is not aware of that there are multiple processors. It is a virtual uni processor.
User can explicitly submit jobs, Remotely move files around and Handles network management personally.	All job allocations, file moving and storage is automatic.
	It is a software system built on the top of the network
User invokes everything	System invokes everything

Network Criteria: A computer network must be able to meet the following criteria.

1. Performance: Performance can be measured in many ways, including the transmission time and response time.

   Transmission time is the amount of time required for a message to travel from one device, to the other device.

   Response time is the amount of elapsed time between a request and a response.

   The performance of a network depends on many factors like

   → The number of users
   → The type of transmission medium
   → The amount of data distributed with in the given time(throughput)
   → The minimum time taken by a network to transfer data (delay)
   → Capabilities of the connected hardware
   → Efficiency of the software we are using.
2. Reliability: Network reliability is measured by the frequency of failure. The amount of time taken by a link to recover from a failure.
3. Security: Protects data from unauthorized access. Protects data from damage and development and implementing of policies and procedures to recover from breach(breaks or loop wholes) and data losses.

Uses of Computer Networks:

1. **Resource Sharing:** Information is available to any one on the network without concerning the physical location of the resource and the user
2. **Reliability:** By having the alternative sources of peripherals, we can achieve reliability. All files will be stored in one or more machines, so that if one machine fails, the other machine or system information can be used.
3. **Money Saving:** Normally small computers have a much better performance than larger computers. For example a main frame computer is 10 times more in fastness and 1000 times more in cost.
4. **Scalability:** By using multiple terminals it has the ability to increase system performance gradually as the work load increases, by adding more processors.

Applications of Computer Networks:

- **Access to Remote Information**
  - ✓ Academic information
  - ✓ Marketing and sales
  - ✓ Financial services
  - ✓ Manufacturing
  - ✓ World wide web
  - ✓ E-commerce
- **Person to Person communication**
  - ✓ E-mail
  - ✓ Chatting
  - ✓ Directory services

  - ✓ Electronic data interchange (EDI)
  - ✓ Teleconferencing
  - ✓ Video conferencing
  - ✓ SMS
  - ✓ MMS
- **Interactive Entertainment**
  - ✓ Cable TV
  - ✓ Games
  - ✓ Movies
  - ✓ Songs

Drawbacks:

- News groups (politics, Religion , sex)
- Messages need not be limited to text
- High resolution color photos, short video clips
- Child pornography
- Employee rights vs Employer rights (in censoring e-mails of employees).

NETWORK HARDWARE:

Classification of Networks: There is no general accepted rule into which all computer networks fall into one category. But two dimensions are very important, they are

1. Transmission Technology
2. Scale (size)

Transmission Technology: under the first dimension there are two classifications again.

1. Broadcast Networks
2. Point to Point Networks.

Broadcast Networks: It has a single communication channel and is shared by all the machines on the network. Messages that are sent by a single machine are received by all the others. An address field of the packet specifies the receiving person. After receiving, each one checks the address field, if it is their address they accept or else they just ignore the packet.

The broadcast systems generally allow the possibility of transferring a message to all the destinations by using a special code in the address field. Whenever a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of transmission is known as **broadcasting(one to all).** There is also some other form of broadcasting that is multicasting. Simply broadcasting is a process where a single message is received by all the persons in the network.

Multicasting: A single message is received by a subset of machines or by a group of people. (One to many communication)

Point to Point Networks: These networks have many connections between individual pars of machines. To go from source to destination, a packet on the type of a network may have to visit one or more intermediate routers. Smaller geographically localized networks prefer broadcast, where as larger networks prefer point to point networks.

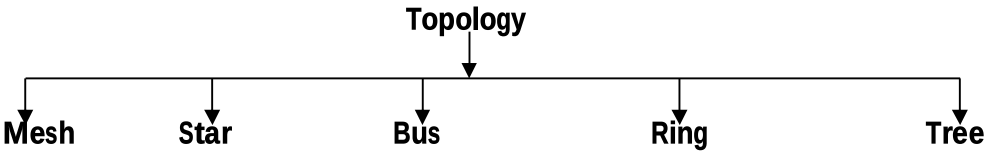
Uni casting: Information is received by a single recipient. (one to one communication)

Second classification of network is scale. Depending on the physical size of the machine and geographical area, networking types are classifies.

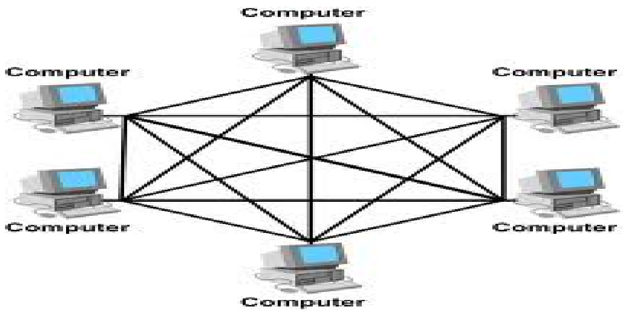
0.1 m	Circuit board	Data flow machines
1m	System	Personal Area Network
10m	Room	LAN
100m	Building	LAN
1 Km	Campus	LAN
10 Km	City	MAN
100 Km	Country	WAN
1000 Km	Continent	WAN
10000 Km	Planet	Internet

Before looking at the network hardware architecture let us discuss about various physical topologies of the network.

Physical Topology: The term physical topology of the network refers to the way a network is built out either physically or logically. It is a geometric representation of the relationship of all the links and linking devices (nodes) to each other. There are five basic topologies.



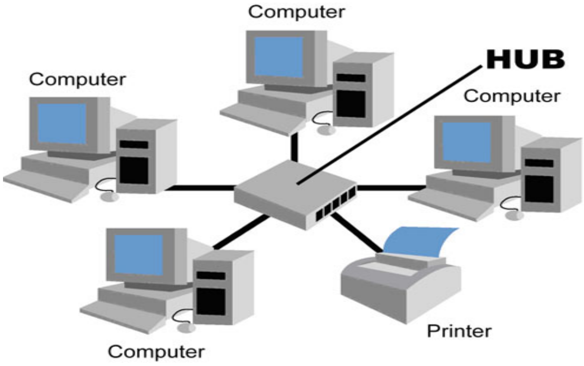
Mesh : Every device must have a dedicated point to point link to every other device. The term dedicated means it carries traffic only between the two devices that it connects. Therefore to link n number of devices we should have n(n-1)/2 physical channels (cables), to accommodate that many lines and every device on the network must have n-1 i/o ports. Mesh topology is used as a back bone connecting the main computer of hybrid network which includes some other topologies. Using mesh, to connect 8 devices we need 8(8-1)/2 that is 28 cables and n-1 that is we need 7 i/o ports.



Merits and Demerits of Mesh

Merits	Demerits
It guarantees that each connection can carry its own data load. So that it eliminates traffic problems	Many cables are required, since every device must be connected to every other device.
Robust, when one link becomes fail	Lot of i/o ports are required
It does not fail the entire system privacy, when every message pass through a dedicated line, only the corresponding destination receives it. No user can access this.	Installations and reconfigurations are difficult
Point to point links make fault detection and isolation easy.	Wiring is grater than the available space can accommodate. h/w required to connect each link is highly expensive.

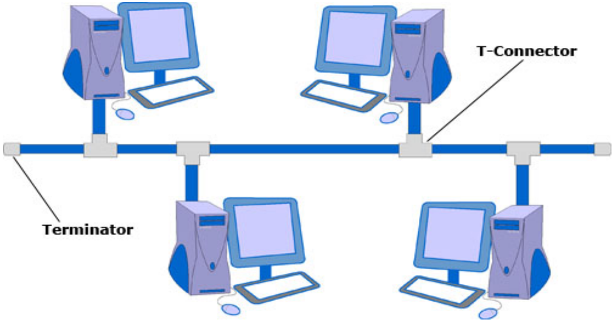
Star: In star topology each device has a dedicated point to point link only to a central controller, usually called a hub. These devices are not directly linked to each other. But it does not allow direct traffic between devices. The controller acts as an exchange. If one wants to transfer data to other, it sends data to the controller, and then it transfer data to other device.



Merits and Demerits:

Merits	Demerits
Less expensive than mesh	The whole network depends on a single node, that is hub
Each device needs only one link and one i/o port connected to any number of devices.	If the hub goes down, the entire system fails
Easy to install and reconfigure	Used in LANs. High speed LANs often use a star topology with a central hub.
Less cabling facilitate to add and delete devices to the hub.	Needs more cabling than other topologies like ring and bus
Highly robust if one link fails, only that link is affected. All other links remain active.	
Fault identification is easy	

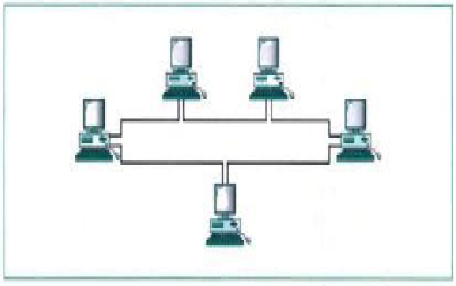
Bus: This is a multi point configuration topology. One long cable acts as a backbone to link all the devices in the network. Nodes are connected to the cable by drop lines and vampire taps. Drop line is a connection running between the main cable and terminals. A vampire tap is a connector that plugs into the main cable. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker after traveling some distance. That is why there is a limit on the number of taps a hub can have and the distance between each tap.

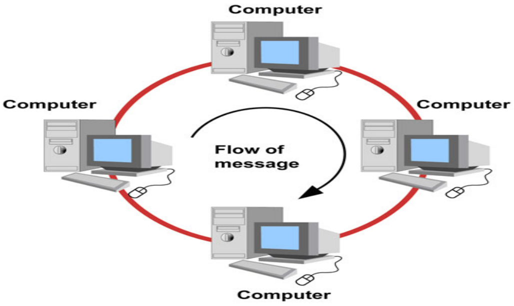


Merits and Demerits:

Merits	**Demerits**
Ease of installation	Difficult in reconfiguration and fault identification
Backbone cables can be used along the most efficient path, and drop lines of various lengths are used to establish.	It is usually designed to optimally efficient at installation. So difficult to add new devices.
It uses less cabling than others	Signal reflection can cause degradation in quality.
	To add new devices, it requires modification or replacement of the backbone.
	A fault or break in the cable stops entire transmission, even between devices on the same side. Damaged area reflects signals back in the original direction, creating noise in both directions.

Ring: In this case each device has a dedicated point to point line configuration only with 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 to the destination. Each device in the ring incorporates a repeater. When a device receives a signal which is intended to others, its repeater just regenerates the bits and passes them forward.

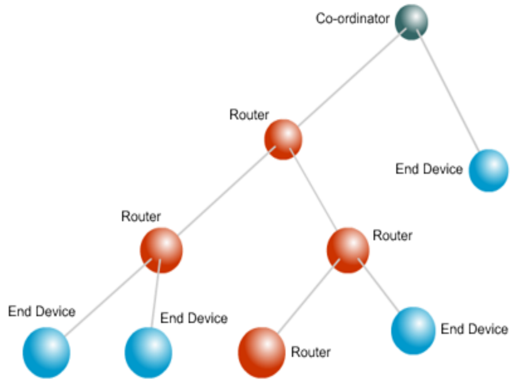


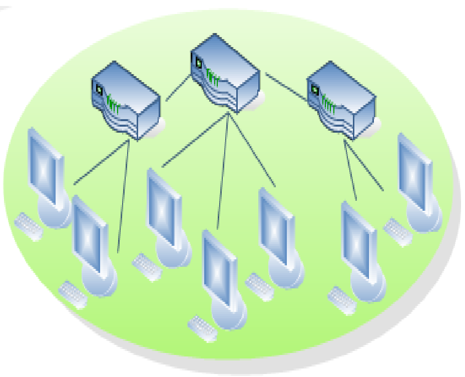


Merits and Demerits:

Merits	**Demerits**
Ease of installation and reconfigure	Unidirectional traffic can be a disadvantage.
Each device is linked to its only neighbors	A break in the ring can disable the ring network.
To add or delete a device requires to change only two connections	This weakness can be solved by using a dual ring or a switch capable of closing off the break.
Fault identification is simplified	

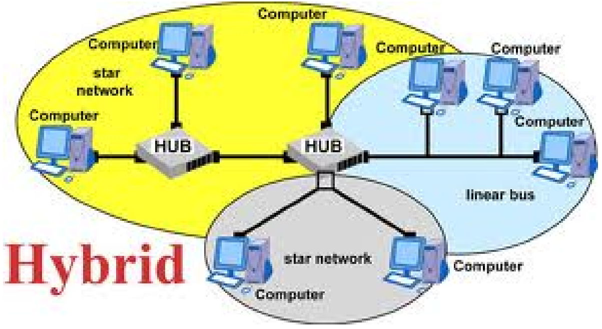
Tree Topology : This is also known as a segmented topology. Tree networks are formed by a number of linked linear buses but are most commonly broadband LAN which has a branching tree topology converging at head end. Throughput of broadband tree systems is high and limited only by the bandwidth of the cable. The maximum distance covered is greater than linear busses because many branches may be linked using repeaters. These systems span several kilometers and have extremely large number of stations added without reconfiguring the network.





The single point of vulnerability on a broadband tree is the head end equipment which is commonly duplicated. Cable or repeater failure elsewhere in the tree removes all stations in the branches beyond failure.

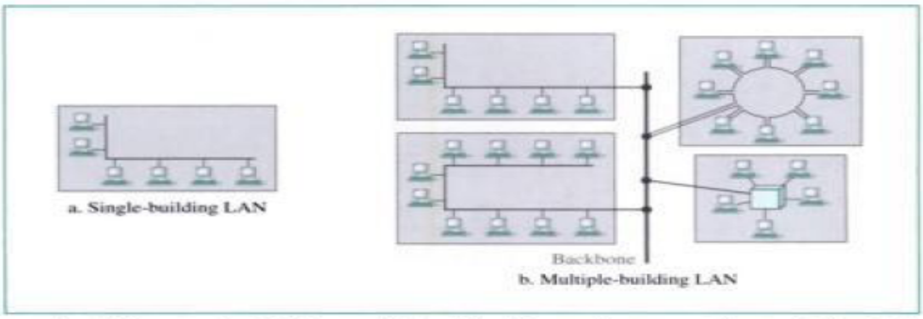
Hybrid Topology : Different network configurations have their own advantages and limitations. Hence, in reality, a pure star or ring or fully connected network is rarely used. Instead, an organization will use some sort of hybrid network, which is simply a combination of different types of networks, each following different topologies.



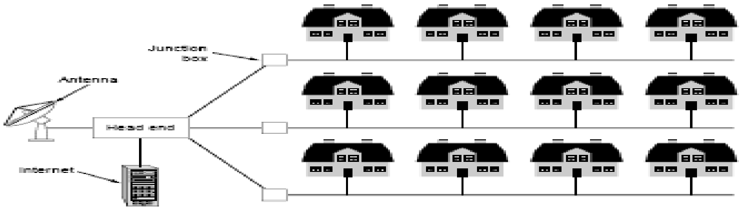
Categories of Networks: We generally refer three primary categories of networks: Local Area Networks, Metropolitan Area Networks, and Wide Area Networks. The type of network is determined by its topology, transmission technology and by its geographical area (size).

Local Area Networks: These are privately owned networks within a single building or campus of up to a few kilometers in size. Depending on the needs of an organization and the type of technology used in a LAN can be as simple as with two Pcs and a printer in someone's home office or it can be extended through out the company and include voice, video, and audio peripherals.

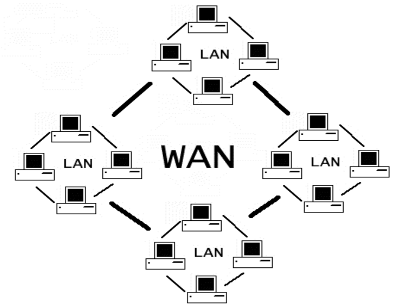
LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (ex: a printer), software, or data. A common example of a LAN is one of the computers may be given a large capacity disk drive and may become a server to other clients. Software can be stored on this central server and used as needed by the whole group. This kind of a LAN is known as disk less network and the terminals are known as dumb terminals. The other kind of a network has an interconnection with multiple standalone (autonomous) terminals which have their own hard disks and are controlled by a server system. LANs are restricted in size, which means that the worst case transmission time is bounded and known before transmission itself. LANs often use a transmission technology consisting of a single cable to which all the machines are connected. In general LAN topologies are bus, ring, star. Traditionally LANs have data rates up to 4 to 16 Mbps range. But today the transmission rate is increasing and it reaches up to 100 Mbps to Gigabit systems.

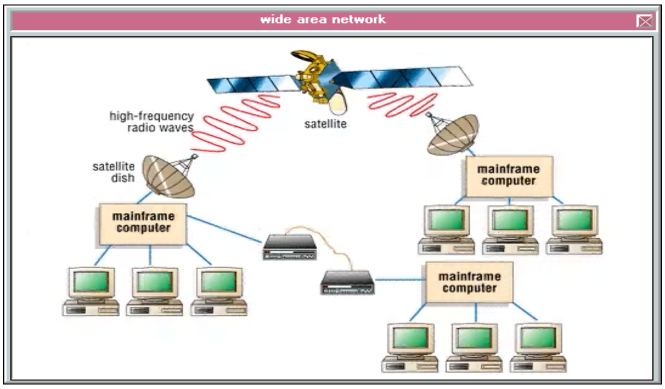


Metropolitan Area Networks: It is basically a bigger version of LAN and normally uses same technology. It is a single network such as a cable television network, or it may be a means of connecting number of LANs into larger network so that the resources may be shared LAN to LAN as well as device to device. Many telephone companies provide a popular MAN service called SMDS. A key aspect of MAN is that there is a broadcast medium to which all the computers are attached.



Wide Area Networks: It provides long distance transmission of data, voice, image, and video information over large geographical areas that may consists a country, continent or even the whole world. In contrast to LANs, WANs may use public, leased, or private communication devices, usually in combinations and can therefore spreads to unlimited number of miles. When a WAN is fully owned and used by a single private company is often referred to as Enterprise Network.



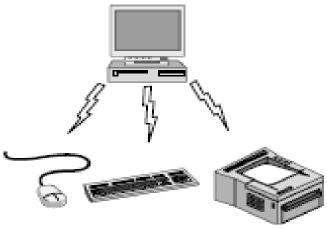


Wireless Networks: In the year 1901, the Italian Physicist Guglielmo Marconi demonstrated a ship to shore(beach) wireless telegraph using Morse code. Modern digital wireless systems have better performance, but the basic idea is the same. Wireless networks can be divided into 3 categories.

1. System Interconnection
2. Wireless LAN
3. Wireless WAN

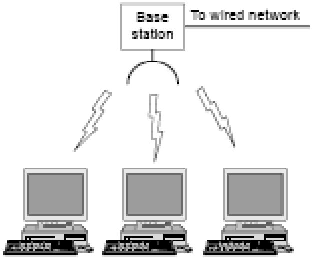
System Interconnection: This is the interconnecting the components of a computer using short range radio. Each computer has a monitor, keyboard, mouse and printer connected to the main unit(processor) by cables. Therefore for new users it is very hard to connect all the devices into the right plug, though they are represented by different colors. Therefore some companies designed a short range wireless network called **Bluetooth** to connect these components without wires. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer within the given range. No cables are required, and no need of installing any drivers also.

The system interconnection networks use the master slave paradigm. The system unit is normally master (server), it talks to the mouse, keyboard, etc., as slaves (clients). The master tells the slaves what address need to be used and when they need to broadcast and how long they need to transport data, and at what frequencies they can use and so on.



Bluetooth Configuration

Wireless LAN: These are the systems in which every computer has a radio modem and antenna with which it can communicate with other systems. Often there is an antenna on the ceiling that the machines can talk together. Suppose if systems are close enough, they can communicate together directly. Wireless LANs are common in small offices where Ethernet installation becomes difficult. For example in conference rooms and in other places.



Wireless LAN

Wireless WAN: This is used in wide area systems. The radio network used for cellular telephones is an example of a low bandwidth wireless system. This kind of wireless networks are from 3 generations

First generation : Analog used for voice only.
Second generation : digital used for voice only.
Third generation : digital used for both voice and data.

Cellular wireless networks are like wireless LANs except the distance is larger and bit rates are slow. In addition to these low speed networks, high bandwidth wide area networks are also developed.

Ex: Connecting individual mobile computers in a Flight

Home Networks: In the coming future most homes will set up a network among themselves. Every device in the home will be capable of communicating with every device and all of them will be accessible via Internet. Many devices can be networks. Some of the examples are

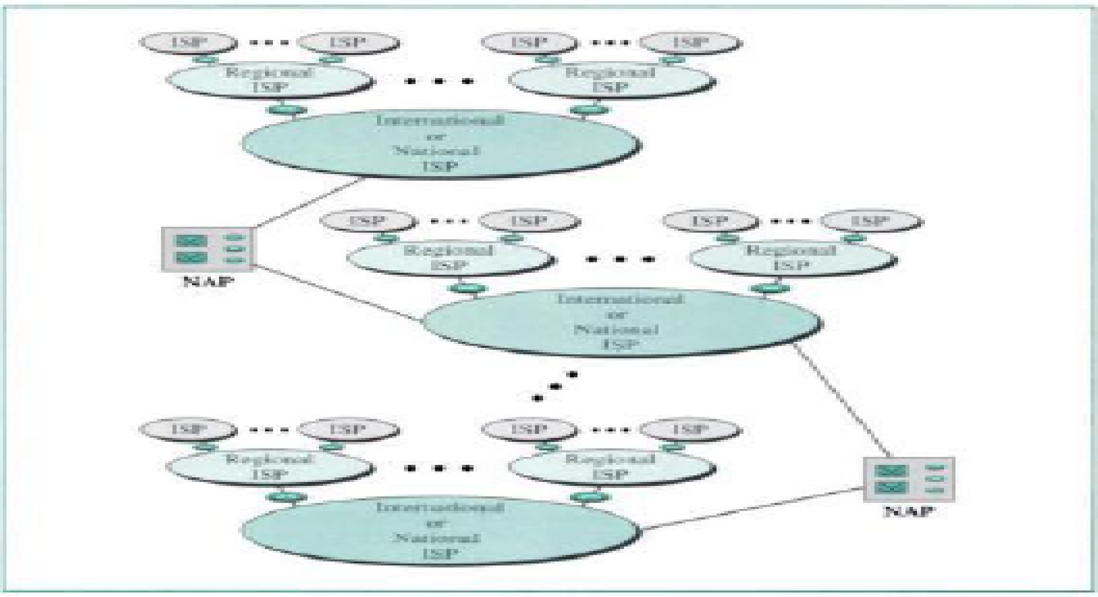
1. Computers (desktop Pc, notebook, PDA shared peripherals)
2. Entertainment (TV,DVD,VCR, camcorder, camera, stereo, MP3)
3. Telecommunications (telephone, mobile, intercom, fax)
4. Appliances (microwave, refrigerator, clock, furnace, lights)
5. Telemetry (utility meter, smoke/burglar alarm , thermostat, babycam)

Home networks are already used but in a limited way. That is only to connect the terminals from one house to another house. This kind of facilities will soon be implemented.

Internetworks: When two or more networks are interconnected, they become an inter network, or internet. Individual networks are joined into inter networks by the use of internetworking devices. These devices are routers and gateways. The term internet is used in two ways

1. internet : inter connection of networks

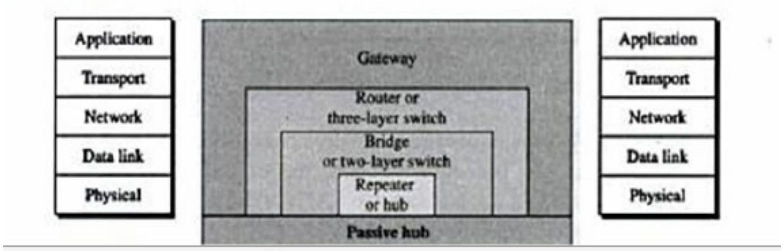
2. Internet : World wide web network.



Inter network(Internet)

Connecting Devices (Network h/w) :

Connecting devices are divided into 5 categories based on the layer in which they operate in a network.



The five categories contain devices which can be defined as

1. Those which operate below the physical layer such as a passive hub
2. those which operate at the physical layer (a repeater or an active hub)
3. The devices which operate at the physical and data link layers (a bridge or a two layer switch)
4. The devices which operate at the Physical, data link, and network layers. (a router or a 3 layer switch)
5. The devices which operate at all five(TCP/IP) or 7(OSI) layers is a gateway.

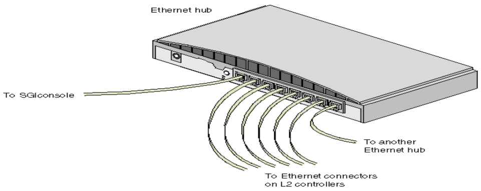
Repeaters: Repeaters are the devices that operate at the physical layer based on the reference model. The basic purpose of **a** repeater is to extend the transmission distance. Their primary purpose is to simply regenerate a signal received from input and strengthens the signal and forwards to its output.

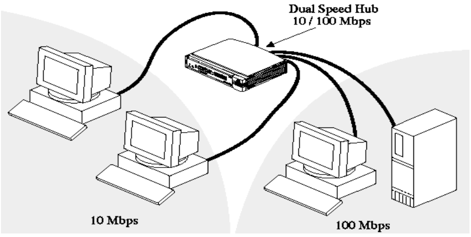
They provide signal amplification and also re-timing required to connect the connected segments. Repeaters are available in many types. These are of many types.

1. Single port repeater: It operates with actually two segments. One type has a signal taken from it to boost and pass to the next segment and the
2. Multi port repeater : It has one input port and multiple output ports.
3. Smart repeater : A hybrid device and very similar to a bridge in functionality. Packet filtering is done by smart repeaters.
4. Optical repeater : These repeaters repeat optical signals.

Repeaters are implemented in all types of cables.

HUB : All networks except those, using a coaxial cable require a central location to bring communication together. These central locations are called hubs. The hub organizes the cables and transmits incoming signals to the other segment. There are 3 kinds of hubs.





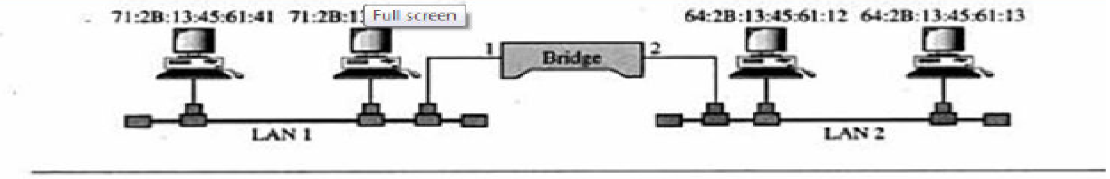
Passive Hub : A passive hub simply combines the signals of network segments. There is no signal regeneration. A passive hub reduces by half the maximum cabling distances permitted.

Ex: If a level of UTP is used which allows reliable signal strength between devices that are 300m apart, each segment from a passive hub can only extend 150m. With a passive hub, all computers receive signals sent from all other computers.

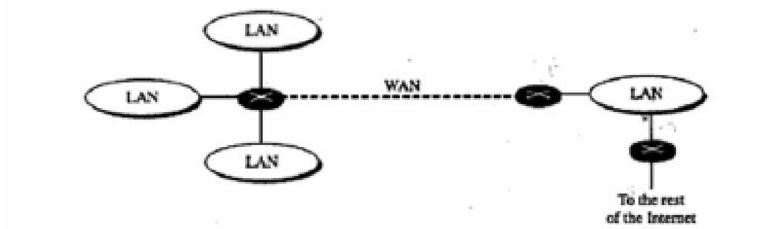
Active Hub : It regenerates or amplifies the signals. Because of this, the distance between devices can be increased. Some active hubs amplify noise as well as the signal. Active hubs are expensive and they are some times called multi port repeaters.

Intelligent Hub: It regenerates the signal and performs some network management and intelligent path selection. Intelligent hub includes switching hubs. Many switching hubs can choose that alternative path which, will be the quickest and send the signal in that way.

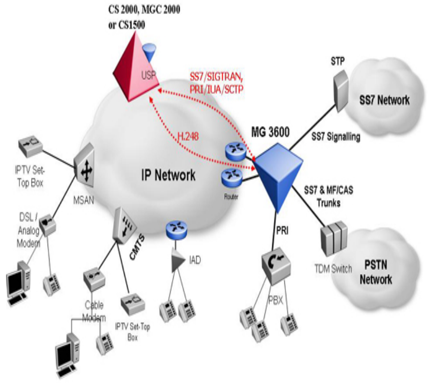
Bridges: Bridges connect different network segments. A bridge extends the maximum distance of a network by connecting separate network segments. Bridge simply passes on all the signals it receives. It reads the address of all the signals it receives. The bridge reads the physical location of the source and destination computers from this address. Bridges can divide busy networks into segments and reduce network traffic.

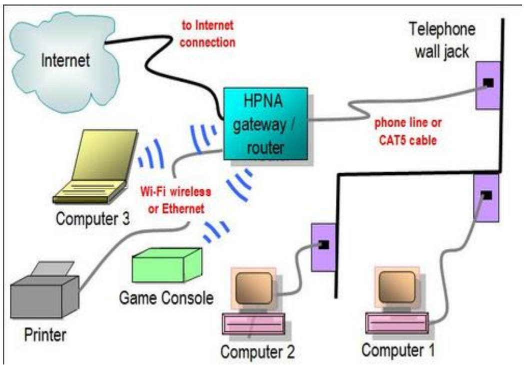


Routers : A router is a three layer, switch or device that routes packets based on their logical addresses(IP). A router normally connects LANs and WANs in the internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols. This is also known as a three-layer switch. It is a faster and more sophisticated. It allows faster table lookup and forwarding.



Gateway : A gateway is normally a computer that operates in all five layers of the internet or seven layers of OSI. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two inter networks that use different models. For example a network designed for OSI can be connected to work with a network using Internet model or from x.25 to internet. Some times these are called remote bridges.





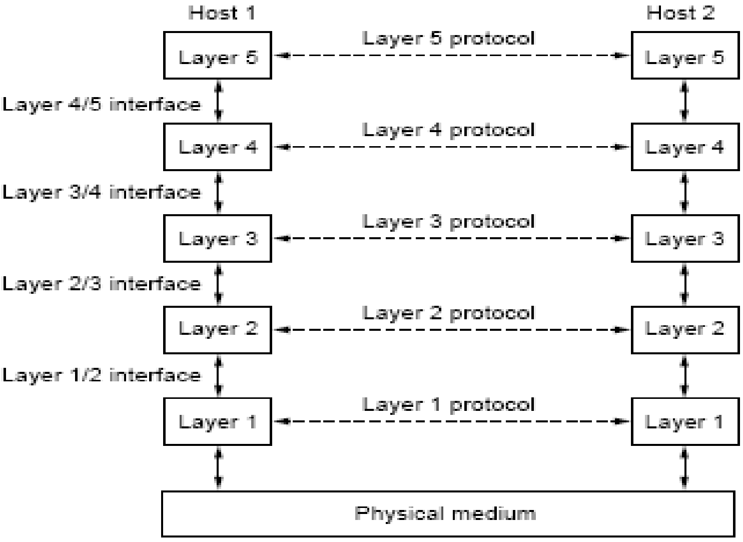
NETWORK SOFTWARE:

Network hardware is used to connect multiple terminals together. Though we established a network, we can not exchange data. Therefore it is necessary to implement network software. It includes a set of protocols.

Protocol: It is a set of rules and regulations that govern data communication. The rules and regulations are

- ✓ Data formatting
- ✓ Timing
- ✓ Sequencing
- ✓ Access Control and
- ✓ Error Control Mechanisms

Layered Architecture: To reduce the design complexity, most networks are organized as a series of layers or levels, each one built upon one below it. The number of layers, name of each layer, contents and functionality of each layer differ from network to network. But the main purpose of each layer is to provide certain services to the higher layers. Layer 'n' on one machine carries data to the layer 'n' on another machine. The entities that have the corresponding layers on different machines is called peers. But in reality there is no data that is directly transferred in between the layer n on two peers. And at the end of the last layer, we have a physical medium through which actual transmission occurs. Virtual communication is shown by dotted lines between the layers and the physical communication is shown by solid lines between the peers. Between each pair of adjacent layers, there is an interface. This interface defines the various primitive operations and services offered by the lower layer to the upper layer. A set of layers and protocols is called layered architecture.

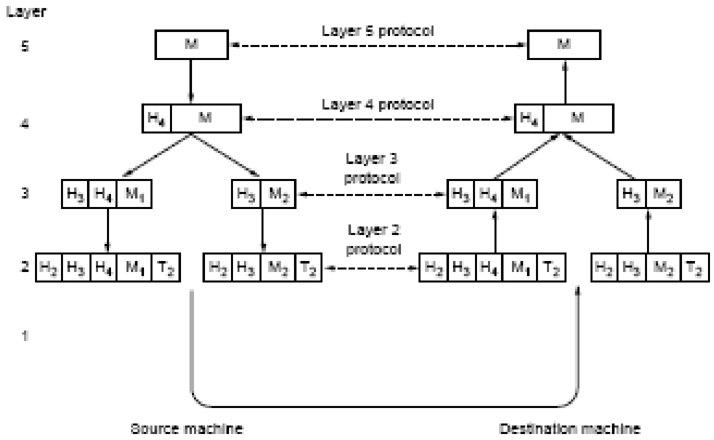


Here we are giving a five layered approach to understand the process. A set of layers and protocols is called network architecture. Data communication is achieved from one layer to another layer using this approach. A message M produced by an application process running at layer 5 and it is sent to the bottom layer 4 for transmission. Layer4 puts a header in front of the message to identify the message and passes the result to the layer3.

The header includes control information like sequence numbers, addresses, time to deliver the information to the layer 4 on the destination machine. In many networks layer4 does not have any limit to transport data, but there is a limit for layer3. Therefore layer 3 must break the incoming data into small units, packets and adds a layer 3 header to each unit or packet. Here in this example M splits into M1 and M2.

Layer 3 decides which of the outgoing layer is to be used to transport the data. That is it does routing mechanism. Layer 2 adds both header and trailer to each incoming data and sends them to layer1 for physical transmission.

At the receiving end, the message moves upward from one layer to another layer. Therefore at the sending side, the higher layers packets are encapsulated into the bottom layers data portion, and at the receiving side, packets are de capsulated and send them to the upper layer from bottom layers



Data flow from one layer to another layer

Design Issues of the Layers: Each layer is designed to do some functionality. The general functions of each layer are categorized as

1. Every layer needs a mechanism to identify senders and receivers (Addressing)
2. Data Transmission Mode. Simplex, Half Duplex, Full Duplex.
3. Error Controlling: By using various error detecting and correcting mechanisms, receiver must have some information to convey to the sender that the information has been received by receiver is correct or incorrect data.
4. Sequencing: Data must travel in sequential order
5. Flow Control
6. Fragmentation and Reassembling.
7. Channel allocation when multiple persons are trying to access the channel at once (multiplexing)
8. Routing, when multiple paths are available , the best suitable path will be selected among them to route packets

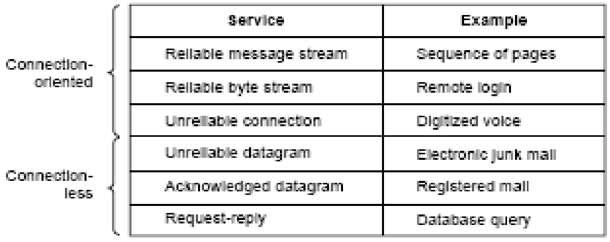
Connection-Oriented and Connectionless Services:

Layers offer two different types of services, that is connection oriented and connection less. By taking two best examples here we compare the two services.

Connection Oriented	Connection Less
Ex: Telephone service	Ex: Postal service
Each packet contains an identification number (telephone number)	Each packet carries full source and destination addresses.
Before sending the data a connection	Connection is established after the

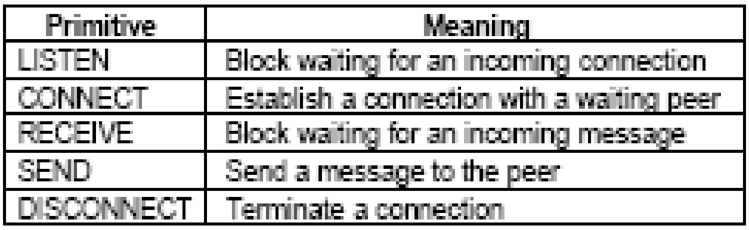
must be established. That is a circuit is required	transmission. There is no need of any path establishment. No circuit is required
Each virtual circuit requires a table space information	Subnet does not hold state information.
Once the connection is established all packets must follow the same path.	Each packet may follow different path.
All packets that are passing through a failed route will be terminated.	Router failures will not happen.
Congestion control is easy.	Congestion control is difficult.

Types of Services:



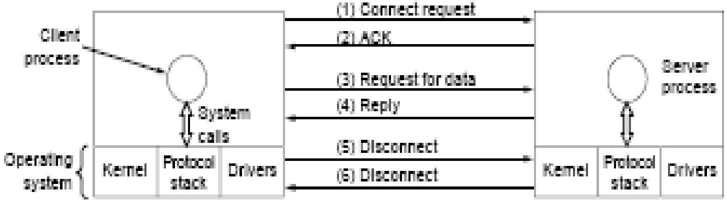
	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Service Primitives: A service is generally specified as a set of operations available to a user or to other device to access the service. The set of primitives available depends on the nature of the service we are providing. The primitives for connection oriented service are different from the connection less service. The generally available 5 service primitives are



Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

The process is explained using the following lines and figure.



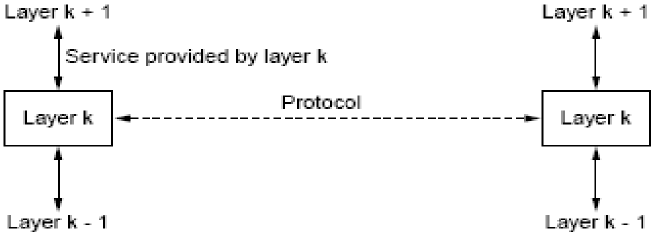
Client/Server interaction in a connection oriented network

1. Server executes LISTEN to indicate that is ready to accept incoming connections
2. After executing this, the server goes to the blocked status and waits for incoimg request.
3. client executes CONNECT request to enable a connection with the server machine. (1)
4. Now the client process is suspended until it receives some response from the server.
5. when the packet arrives at the server, it is processed by the server operating system.
6. Then the server unblocks its listener and sends an acknowledgement to the client. (2)
7. The arrival of ack releases the client from suspended state.
8. The server has to execute RECEIVE to prepare itself to accept a first request.
9. Client executes SEND to request for data.(3)
10. The arrival of the SEND packet unblocks the server to process client's request.
11. Now server sends reply to the client (4)
12. Client receives this, and process if it wants to send any more requests.
13. If the client does not have any more requests, then the client issues a DISCONNECT request to terminate the connection. (5)
14. When the sever gets this packet, it also issues a DISCONNECT to terminate the connection. (6)
15. When client receives this information, client also terminates its connection.

Relationship of Services to Protocols:

Service: A service is a set of functions or operations that a lower layer provides to upper layer. It defines them a set of operations that it performs for its users. It is related to an interface between two layers. Lower layer is a service provider and upper layer is a service user.

Protocol: A protocol is set of rules and regulations that govern the format and meaning of the frames, packets or messages that are exchanged by the two end parties within the layers.

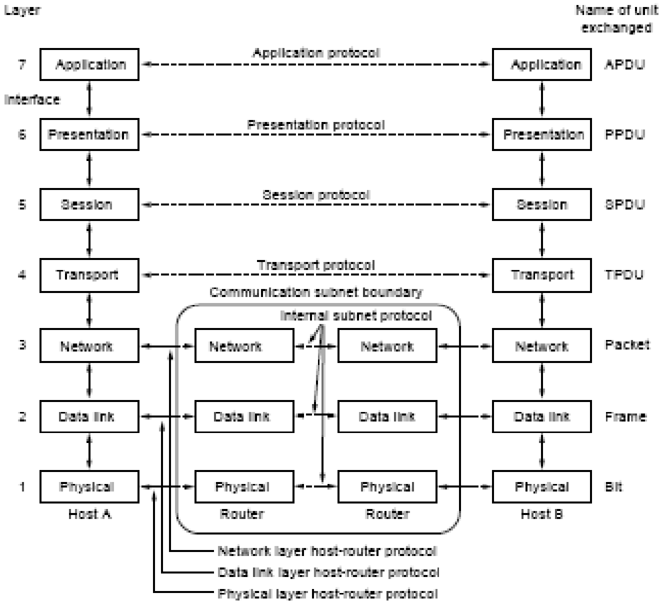


For example when we compare this, with our traditional programming languages a service is an abstract data type, or an object in object oriented programming languages. Where as a protocol is an implementation of the service which is not visible to the user of the service.

REFERENCE MODELS:

1. OSI Reference Model: It is developed by **I**nternational **S**tandards **O**rganization (**ISO**). This is also called the open systems interconnection model. This is a layered framework to design a network. The OSI model is designed with 7 layers. When the message travels from A to B, it has to pass through many intermediate nodes (terminals, routers). These intermediate nodes only involve the first 3 layers of the OSI model. Each layer defines a set of functions that are distinct from each of the other layers.

Interfaces between Layers: The data transmission is always top-down approach starting from the source station that is from the top most layer to the bottom layer. And vice versa data receiving is always from bottom up approach staring from the bottom layer to the top most layer. This is possible by an interface which lies in between all adjacent layers.



Organization of the Layers: The seven layers are organized in 3 subgroups.

Subgroup 1 - Network Support

Bottom 3 layers physical, Data-link, Network are the network support layers. These layers deal with the physical aspects of moving data from one device to the other.

Subgroup 2 – User Support

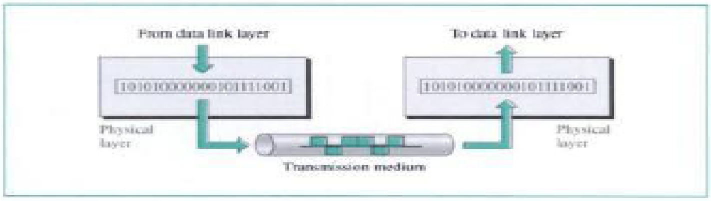
Upper 3 layers: Session, Presentation, Application are user support layers. They allow interoperability among unrelated software systems.

Subgroup 3 - End-to-End Support

Layer 4, the Transport Layer provides end to end reliable data transmission. Upper layers are almost always implemented in software, lower layers are a combination of h/w and s/w except the physical layer which is mostly with h/w.

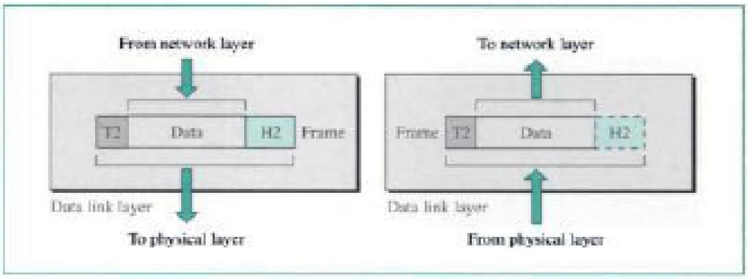
Design issues of the Layers:

Physical Layer : It transmits a bit stream over a physical medium. It deals with mechanical and electrical specifications of the transmission medium.



- **Physical Characteristics of Interfaces and Media :** It defines the physical characteristics of interfaces (bridge, hub) between devices and the transmission medium. It also defines the type of transmission medium that we have chosen to transmit data.
- **Representation of Bits :** To transfer bits, they must be encoded into either electric signal or optical signals based on the type of transmission media.
- **Data Transmission Rate (DTR) :** It defines the number of bits transmitted per second depending on our chosen transmission medium.
- **Synchronization of Bits :** The senders and receivers clocks must be synchronized at the physical level.
- **Line Configuration :** It defines either the devices are connected using point to point configuration or multi point configuration
- **Physical Topology :** It defines how devices are connected to a network.
  Mesh (Every device must be connected to every other device)
  Star (All devices are connected through a central hub)
  Ring (Every device is connected to the next forming a ring)
  Bus (Every device connected on a common link)
- **Transmission Mode :** It defines the direction of transmission (simplex, half-duplex, full-duplex).

Data-Link Layer : It is responsible for node to node delivery. Node to node delivery is achieved by using physical address of the node. It makes physical layers appears to be error free to upper layer that is to the network layer.



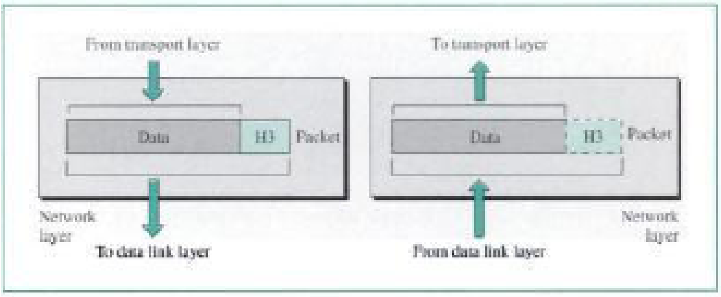
- **Framing :** It is a contiguous collection of bits. It divides the data which is in bit streams received from the physical layer into data units called frames.
- **Physical Addressing :** To distribute frames to different systems on the network, data link layer adds a header to the frame to define the physical address of

source and the destination. Each system will have a unique address in the world. The length of physical address is 48 bits. This is also called LAN address, node address, h/w address, MAC address, Ethernet address, NIC address. This is represented in hexadecimal notation.

- **Flow Control :** If the receiver's data receiving capability is less than the data transmission rate of the sender, data link layer applies flow control mechanisms to prevent the overflowing of data at the receiver station.
- **Error Control :** To provide reliability to the physical layer data, it adds functions to detect and retransmit damaged or lost frames. It also applies a mechanism to prevent from duplicated frames. Error control is normally achieved through a trailer field of the frame.
- **Access Control :** When two more devices are connected to the same link, this layer protocols are necessary to determine which device has access over the data.

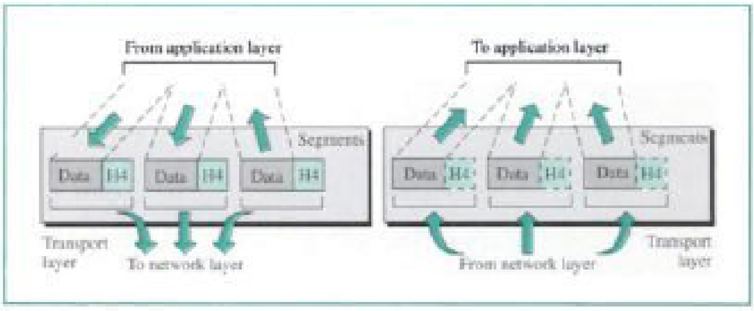
Network Layer : It is responsible for host to host delivery of a packet across multiple networks, Where as data link layer delivers the packet between two systems of a same network. Network layer take care of transferring a packet from its source to final destination.

If two systems are connected to the same network, there is no need of a network layer. When two systems are connected to different networks, then we need network layer to achieve source to destination delivery.

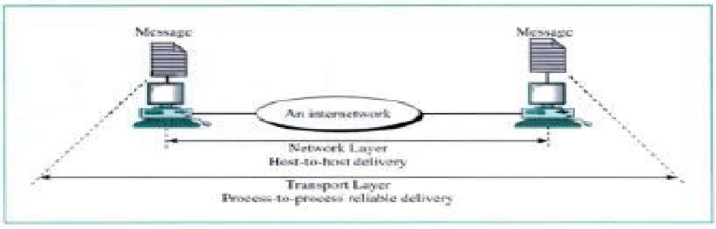


- **Logical Addressing :** If a packet passes from one network to another network, we need another address to distinguish the source and destination systems. Therefore network layer adds a header to the packet which includes logical address of the source and destination. This address is also known as IP address, internet address, host address.
- **Routing :** Establishing a suitable path between two devices. When independent networks are connected together to create an internetwork, or a large network, the interconnecting devices called routers or gateways must route the packets to their final destinations.

Transport Layer : It is responsible to provide end to end delivery of the entire message. To add security, the transport layer may create a connection between the two end ports. Creating a connection involves 3 stages, that is connection establishment, data transfer, connection termination (release).

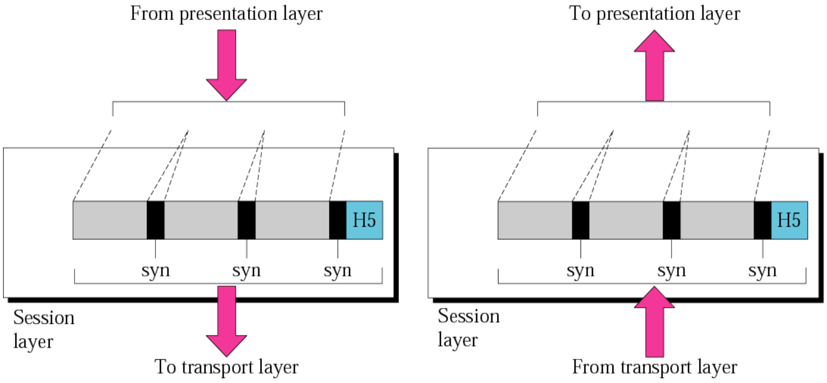


- **Service Point (Port) Addressing :** Sometimes users run multiple programs on the system at a time. That is why source to destination delivery means, delivering not only from one user to another, but also from a specific process(program) to the specific process of other user. Therefore the header of this layer includes the service point address or port address of each user's process. This is of length 16 bits. Port addresses range from 0 to 65535.
- **Segmentation and Reassembling:** Each message will be divided into the transmittable segments(packets) based on the capacity of the receiver. It also contains a sequential number of each segment. These sequential numbers helps us to reassemble the segments correctly after receiving by the receiver. Therefore we can easily identify and replace packets that were lost during transmission.
- **Connection Control :** This layer can be either connection oriented or connection less. Connection less transport layer treats each segment as an independent segment and delivers to the destination. Whereas a connection oriented transport layer first makes a connection with the destination, and delivers all the packets in the same route. After completion of the data transmission it terminates the connection.
- **Flow Control :** We use this feature to hide the errors of bottom layers and to enhance the quality of services provided by bottom layers.
- **Error Control :** To enhance the quality of service provided by the bottom layers again we use this function. Error correction can be achieved through retransmission.



Process to Process Delivery

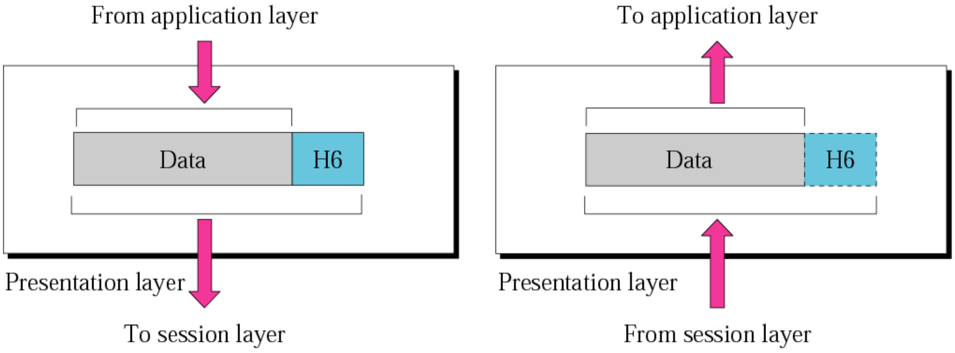
Session Layer : The services provided by first three layers are sufficient from some processes. It is a network dialog controller. It establishes, maintains and synchronizes the interaction between communicating parties.



- **Dialog Control :** It allows two systems to enter into a dialog. It allows the communication between two processes to take place either in a half duplex or full duplex.
- **Synchronization :** It allows a mechanism to add check points into a stream of data.

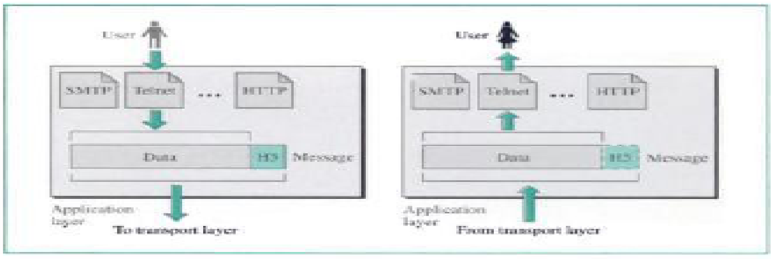
Ex: If a systems is sending a file of 2000 pages, it is good to insert check points after every 100 pages to ensure that each 100 page unit is received and acknowledged independently. That means if a crash happens during the transmission of page 512, retransmission begins at page 501. Pages 1 to 500 need not be retransmitted.

Presentation Layer : It is connected with syntax and semantics of the information exchanged between two systems.



- **Translation (Encoding) :** Two processes usually exchange information in the form of strings, numbers and so on. The information should be changed to bit streams before being transmitted, because different computers use different encoding schemes. This layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender side changes the information to the common format and the presentation layer at the receiver side changes the common format to into its receiver dependant format.
- **Encryption :** To carry confidential information, a system must be able to ensure privacy. Encryption means the sender transforms the original information to some other format, and transfers it to destination, upon receiving this, the destination has to decrypt it and gets the original message.
- **Compression :** Data compression reduces the size of the data. It very useful in the transmission of image, audio and video.

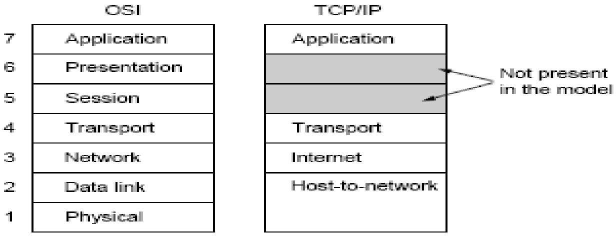
Application Layer : Application layer enables the user, whether the human or s/w to access the network. It provides user interfaces and support for services such as E-mail, remote file access and transfer, shared database management, and other types of distributed information services. It provides X.400 services like message handling services and X.500 services like directory services.



- **Network Virtual Terminal :** It is a s/w version of a physical terminal and allows a user to log on to a remote terminal. The users terminal talks to the s/w terminal, which in turn talks to the host and vice versa.
- **File Transfer Access and Management :** It allows a user to access and to retrieve files and also allows to manage or control files in a remote system.
- **Mail Services :** It provides the basis for E-mail forwarding and storage.
- **Directory Services :** It provides distributed database sources and access for global information about various objects and service.

2. TCP/IP Reference Model : It is the grand parent of all computer networks, the ARPAENT and its successor, the World wide internet. This was first defined by Vint Cerf and Bob khan in the year 1974.

Architecture:



Host to Network Layer : This model does not say really much about what happens here, except the host has to connect to the network using some protocols. So it can send packets over it.

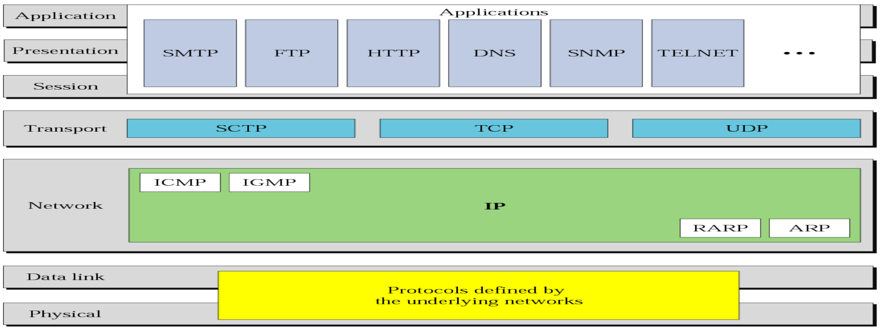
Internet Layer : It provides a packet switching network based on a connection less internet work layer. It permits the host to insert packets into any network and allow them travel independently to destination. They may even arrive in an irregular order than they were sent, in this case it is the duty of upper layers to arrange them in a sequential order. It defines them in a official packet format called IP. This layer functionality is equal to the OSI n/w layer.

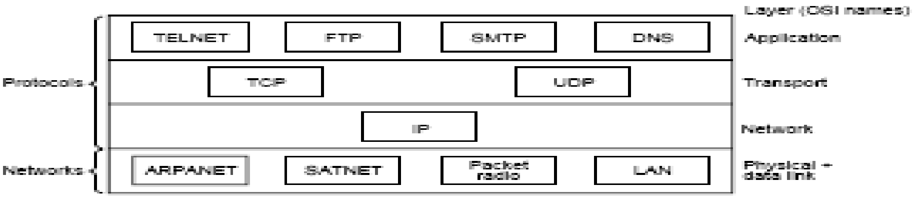
Transport Layer : It is designed to enable connection between source and destination peer entities. This is also same as OSI transport. Two end to end protocols are defined here.

1. TCP: Is a connection oriented reliable protocol which allows a byte stream starting from source machine to destination machine to be delivered with out error. It fragments the incoming byte stream into discrete messages and passes each one to the internet layer. At the destination, the receiving TCP reassembles the received messages into the o/p stream. TCP also handles flow control to make sure a fast sender can not swamp(flood) slow receiver with more messages that it can handle.
2. UDP: It is an unreliable connection less protocol for applications that do not want TCP's sequencing and flow control.

Application Layer : TCP/IP does not have any session or presentation layers. It contains all the higher layer protocols. TELNET,FTP,SMTP,DNS,HTTP,NNTP.

Protocols and Networks in TCP/IP :





Comparison of OSI and TCP/IP :

OSI	TCP/IP
Number of layers is 7	Number of layers is 5 (4 when physical and data link layers are merged).
OSI supports both connection oriented and connection less in network layer.	Network layer has only one service that is connection oriented service.
Transport layer has only connection oriented service.	Transport layer supports both connections oriented and connection less service.
OSI layers were defined before the protocols are implemented	Protocols implemented first and the model was just a description of the existing protocols.

Critique of the OSI Reference Model : Neither the OSI model and its protocols not the TCP/IP reference model and its protocols are perfect. Here we have four criticisms under OSI

1. **Bad Timing :** By the time this model was invented, TCP/IP protocols were already in wide spread use by research universities. When the OSI came, they did not want to support a second protocol stack until they were forced to. So there were no initial offerings. Every company is waiting for every other to use it first, no one went first and so OSI never happened.
2. **Bad Technology :** The second reason that OSI never success is both the model and protocols are flawed. The session layer has very little use in most applications, and the presentation layer is nearly empty. In fact, the original proposal to British government is only had 5 layers, not seven. In contrast to the session and presentation, data link and network layers are so full and work has split them into multiple sub layers, each with different functions. The OSI model along with the associated service definitions and protocols is extraordinarily complex.
3. **Bad Implementations :** With enormous complexity of the model and the protocols, it is not surprise that initial implementation were huge, un widely and slow.
4. **Bad politics :** OSI model and protocols have been less than a resounding success, there are still a few organizations interested in it, mostly European telecommunication PTTs that still have a monopoly on telecommunication.

Critique of the TCP/IP Reference Model : The TCP/IP model and ptotocols have their own problems.

1. The model does not clearly distinguish the concepts of service, interface, and protocol.

2. The TCP/IP model is not at all general and is poorly suited to describe any protocol stack.

3. The host to network layer is not really a layer at all in the normal sense and the term is sued to context of the layered protocols.

4. It does not distinguish the physical and data link layers. These are completely different.

Example Networks :

Novell Netware : The most popular network system in the PC world is Novell Netware. It is based on the client-server model. Netware uses a proprietary protocol stack in the following figure.

<table>
<tr><td>SAP</td><td colspan="2">File server</td><td>...</td></tr>
<tr><td colspan="2">NCP</td><td colspan="2">SPX</td></tr>
<tr><td colspan="4">IPX</td></tr>
<tr><td>Ethernet</td><td colspan="2">Tokenring</td><td>ARCnet</td></tr>
<tr><td>Ethernet</td><td colspan="2">Token ring</td><td>ARCnet</td></tr>
</table>

It is based on the Old Xerox Network Systems XNS. It looks like OSI and is not based on it. It is like TCP/IP. The physical and data link layers can be chosen from among various industry standards, Ethernet, IBM Token Ring and ARCnet. The Network layer runs on unreliable connection less internet work protocol IPX. IPX is functionally similar to IP, except that it use 10 byte address instead of using 4 byte address.

Above IPX, we have a connection oriented NCP (Network Core Protocol). It also divides various other services besides user data transport and is really the heart of netware. A second protocol SPX is also available, but provides only transport. TCP is another option. Applications can choose any one of them. Now here we have the format of IPX.

2	2	1	12	12	12	variable
Checksum	Packet Length	Transport control	Packet Type	Destination Address	Source Address	Data

A Novell Netware IPx packet

Checksum field is rarely used, because the data link layer also provides checksum.

The packet length field tells the length of the packet (header + data)

The transport control field counts the number of networks that the packet has visited. When this exceeds a maximum count, the packet is discarded.

The packet type field is used to mark various control packets.

The two addresses each contain 32 bit IP address, 48 bit machine number, and 16 bit local process address.

ARPANET : ARPANET was the first network. In the mid of 1960's mainframe computers were stand alone devices. Computers from different manufacturers were unable to communicate with one another. The advanced research project agency (ARPA) in the department of defense DOD found a way to connect computers together so that the researchers can share their articles, information.

In 1960, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas to establish a small network of connected computers. The idea was that each computer would be attached to a specialized computer called Interface Message Processor(IMP). The IMP's in turn, would be connected to each other. Each IMP had to be able to communicate with other IMP and to its own host.

By 1969, ARPANET was a reality. First time, four nodes, at the University of California at Los Angles, the University of Santa Barbara, Stanford Research Institute and the University of Uttah. All these exchanged their information using NCP(Network Core(control) Protocol).

NSFNET : In 1983, ARPANET split into two n/ws MILNET (for military) and ARPANET (for non Military). Another milestone in the Internet history was a creation of CSNET in 1981 with the success of CSNET, the NSF(National Scientific Foundation), in 1986 sponsored NSFNET, a backbone that connected to five supercomputers centers located through out the united states.

INTERNET : The number of networks, machines and users connected to the ARPANET grew rapidly after the TCP/IP became the official protocol on January 1, 1983. When NSFNET and ARPANET were interconnected the growth became oriental. In the mid 1980's people began considering the collection of networks as an Internet. To place a system on the Internet, it must run TCP/IP protocol stack with an IP address. And it sends all IP packets to all other machines on the network.
The main applications of the Internet

1. E-mail : Used to compose, send and receive mail are the facilities of the Internet since from ARPANET.
2. NEWS : Newsgroups are specialized forums where users of common interest can exchange information. Thousands of news groups exists on technical, non technical, computer science, recreation and politics.
3. Remote Login: Using the TELNET, Rlogin or other programs, users anywhere in the internet can log into any other on which they have an account.
4. File Transfer : Using FTP it is possible to copy files from one machine on the internet to another.

Connection Oriented Networks :

1. X.25 Networks : X.25, introduced in the 1970's. It is an International Telecommunication Union Standard for WAN communication. This was the first switched Wide Area Network to become popular both in Europe and US. Still it is used in Europe, but it is disappearing from US. It was mostly used in public network to connect individual computers or LANS. It provides an End to End service.

X.25 defines procedures for exchanging data between user devices and a packet network node. It is an interface between data terminal equipment(DTE) and data circuit equipment(DCE) for terminals operating in the packet mode on public data networks. It specifies an interface between a host system and a packet switching network. The standard physically uses 3 layers. That is physical, link layer and packet layer.

These three layers correspond to the bottom 3 layers of OSI. The physical layer deals with the physical interface between computer and the link that attaches that station to the packet switching node. The physical level of X.25 does not perform significant control functions.

The link layer provides for the reliable transfer of data across the physical link by transmitting the data as a sequence of frames. The link layer standard is referred to as Link Access Protocol Balanced(LAPB). LAPB is a subset of HDLC.

Though we use X.25 as a Wide Area network to carry IP packets from one part of the world to other, there was always a conflict between IP and X.25. IP is a 3rd layer protocol. An IP packet is supposed to be carried by a second layer protocol called X.25. X.25 was designed before the internet, actually it is a 3 layer protocol. It has its own network layer. IP packets had to be encapsulated into the x.25 packet. Another problem with X.25 is that it was designed at that time when transmission media were not very reliable (that is when there is no use of optical fibers). For this reason, X.2 5 makes error control and flow control at both the layers that is in data link and network layers. This makes transmission very slow.

2. Frame Relay : Frame relay provides real time communication between end users. Frame relay networks pass frames from origin to destination without intermediate nodes performing packet assembly and disassembly. Frame relay is designed to support data in bursts and in high speed. It is not a store and forward but rather a bidirectional conversational method of communication.

Frame relay operates on multiple principles. These are virtual links, permanent virtual connections, and the data link connection identifier. Frame relay support variable length of data units. Frame relay does not work well in systems that are delay sensitive that is digitized voice and compressed voice.

It is a switched technology that provides low level that is physical and data link services. It was designed to replace X.25 technology. Frame relay has some advantages over X.25.

1. High Data Rate : Frame relay originally was designed to provide 1.544 Mbps data rate. But today most versions can handle up to 44.736 Mbps.

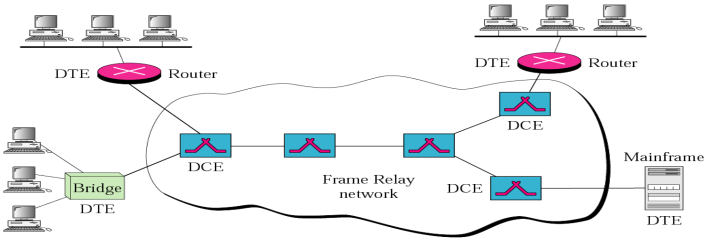
2. Bursty Data : It supports variable rate data. Bursty data needs bandwidth on demand. That means user needs different bandwidth allocations at different times. Frame relay accepts bursty data.

3. Less overhead due to improved transmission media : By improving the quality of transmission media these networks are more reliable and less error prone.

Virtual connection is the basic principle of frame relay. Frame relay uses 3 kinds of virtual circuits.

1. Switched Virtual Circuit (SVC) : This is similar to telephone systems. Message passed from source to destination to set up call and to bring it down. Whenever the circuit is required, a request is made. Some information like bandwidth allocation parameters, Quality of Service parameters and virtual channel identifiers are provided in the call set up phase.
2. Permanent Virtual Circuit (PVC) : PVC is a point to point connections. These are dedicated and used for long periods of time. Commands are still used to set-up the call and to bring it down. The difference between PVC and SVC is duration.
3. Multicast Virtual Circuit (MVC) : MVCs are best described as being a connection between groups of users through which individual users can use SVC connections as well as PVC connections. It is a permanent. It is used as a local management interface extension.

Frame Relay Architecture : The devices that connect users to the network are DTEs (Data Terminal Equipments). The Switches that route the frames through the network are DCE (Data Communicating Equipments). Frame relay is normally used as a WAN to connect LANS or mainframe computers. Frames like other switched LANs use virtual circuits and virtual circuit identifiers. Frame relay has only physical and data link layers. So no specific protocol is defined for the physical layer. It supports any of the protocols supported by ANSI.



Comparison between Frame relay and X.25

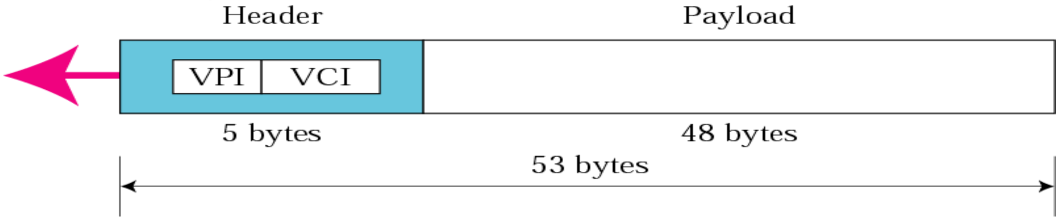
S.No	Frame relay	X.25
1	Allows Bursty data transmissions	Allows fixed data transmissions
2	Multiplexing and switching is done at data link layer	Multiplexing and switching is done at network layer
3	Hop to hop error checking and flow controlling is not done	Hop to hop error checking and flow control is done at data link layer
4	End-to-end flow and error control is not done	End-to-end flow and error control is done at the network layer
5	Congestion control is required	Congestion control is not required
6	To control call signals it requires separate logical connection from user data	To control call signals it uses same connection

3. ATM (Asynchronous Transfer Mode): It is a cell relay protocol designed by the ATM forum and adopted by ITU-T.

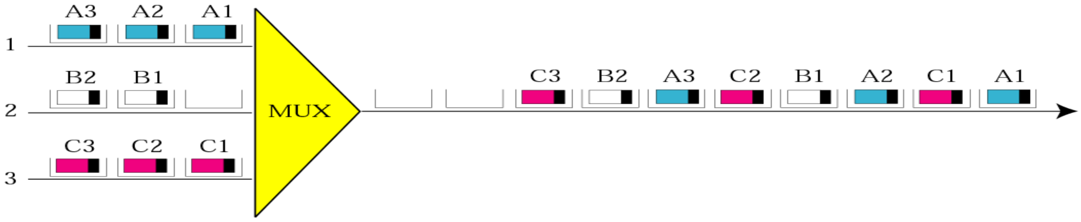
Design Goals :

1. Need for a system to optimize the use of high data rate transmission media, like fiber.
2. Need for a system that can interface with existing systems
3. Need to design a system that can be implemented inexpensively.
4. The new system must support existing tele communication interfaces.
5. The new system must be connection oriented to ensure accurate and predictable delivery.

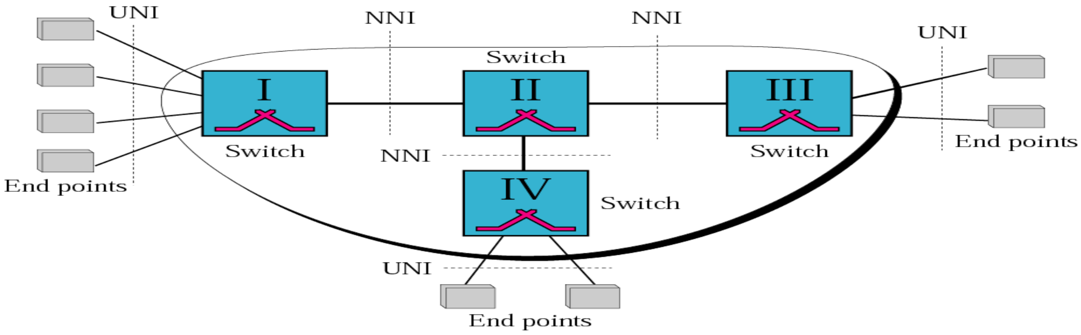
Cell Networks : ATM is a cell network. A cell is a small unit of fixed size data. Cells are multiplexed through other cells and are routed through cell network. A cell is 53 bytes length with 5 bytes allocated to header and remaining 48 bytes carry payload. Most of the header is occupied by the VPI(Virtual Path Identifier) and VCI(Virtual Circuit Identifier).



Asynchronous TDM : ATM uses asynchronous time division multiplexing in the following way. That is at the first cycle of the clock, channel 2 has no cell. Therefore the slot is left as empty

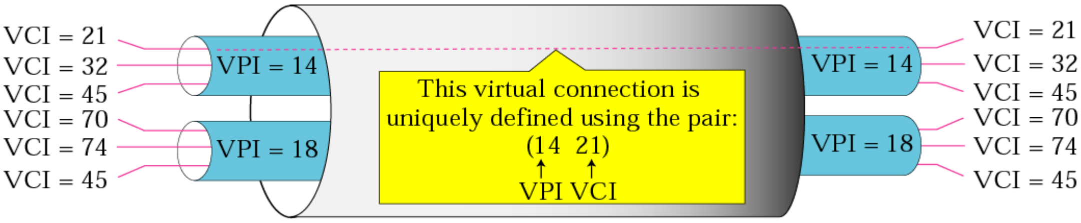


ATM Architecture : It is a cell switched network. The user access devices are connected through UNI(user to Network Interface) to switch inside the network and all the switches are connected through NNI(Network to Network Interfaces).



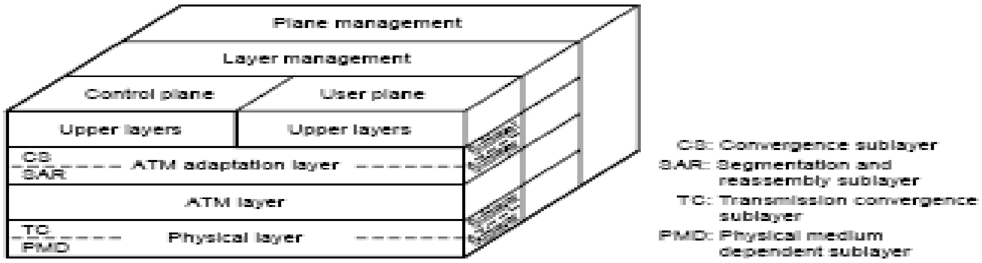
Virtual Connection : Connection between two end points is accomplished through Transmission paths, Virtual paths and Virtual circuits. A Transmission Path is the physical connection between wire, cable, satellite,... and end point and switch or between two switches. A Transmission path is a set of all highways that directly connects two cities. A transmission path is divided into several virtual paths. Each high way is a virtual path. Set of all high ways is a transmission path.

Cell networks are based on virtual circuits. All cells belonging to a single message that follow the same virtual circsuiyet and remain in their original order until they reach their destination.

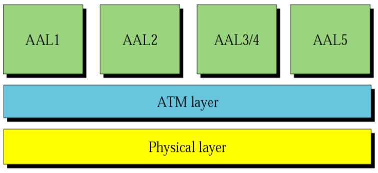


The above diagram shows the relation ship between a transmission path, virtual path, and a virtual circuit that logically connects two points together. In a virtual circuit network to route a packet from one end poin to another, the virtual connections need to be identified. That is why ATM designers created a two level hierarchy that is a Virtual Path Identifier VPI and a Virtual Circuit Identifier VCI.

ATM Layers : The ATM standard defines 3 layers. They are, from top to bottom application adaptation layer, ATM Layer, Physical Layer.



ATM REFERENCE MODEL



Application Adaptation Layer : It allows existing networks to connect facilities. ATM protocols accept transmission from upper layer services, and map them into fixed size ATM cells. These transmissions can be of any type (voice, data, audio and video) and can be of variable or fixed rates

AAL 1 : It is designed for constant bit rate data coming from applications that generate and consume bits at a constant rate. In these transmission delays must be minimal and transmission must simulate real time. Real time voice and real time audio are examples.

AAL 2 : It is designed for variable bit rate data coming from applications that generate and consume bits at a variable rates. In these applications bit rates are vary from section to section of the transmission, but within established parameters. Compressed audio, video data are best examples.

AAL ¾ : It is designed for connection less packet protocols that use virtual circuits.

AAL 5 : It is designed for connection less packet protocols that use dtagram approach to route the packets from one end to other.

ATM Layer : Deals with cell and cell transport. Defines the layout of a cell and gives the meaning of a header field. It also deals with establishment and release of virtual circuits. Congestion control is also possible. It provides routing, traffic management, switching and multiplexing services. It processes outgoing traffic by accepting them into 53-byte cells by the addition of a 5 byte header.

Physical Layer : It defines the transmission medium, bit transmission, encoding and electrical to optical transformation. It provides convergence with physical transport protocols, such as SONET as well as mechanisms for transforming the flow of cells into a flow of bits.

some times ATM is treated as a 3 dimensional reference model.

USER Plane : Data transport , flow control and error correction

Control Plane : connection management.

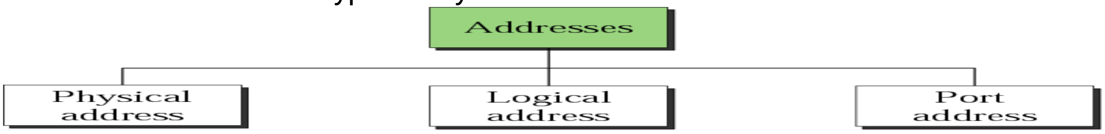
PMD Sub layer : Interfaces with the actual cable. It moves the bits on and off and handles the bit timing.

TC Sub layer : this is a transmission convergence sub layer. When cells are transmitted, the TC layer sends them as a string of bits to the PMD layer. Its job is to convert the bit stream into a cell stream from the PMD sub layer. It handles the issues of cell starting and ending locations. AAL layers are also split into two different layers like CS layer and SAR layers.

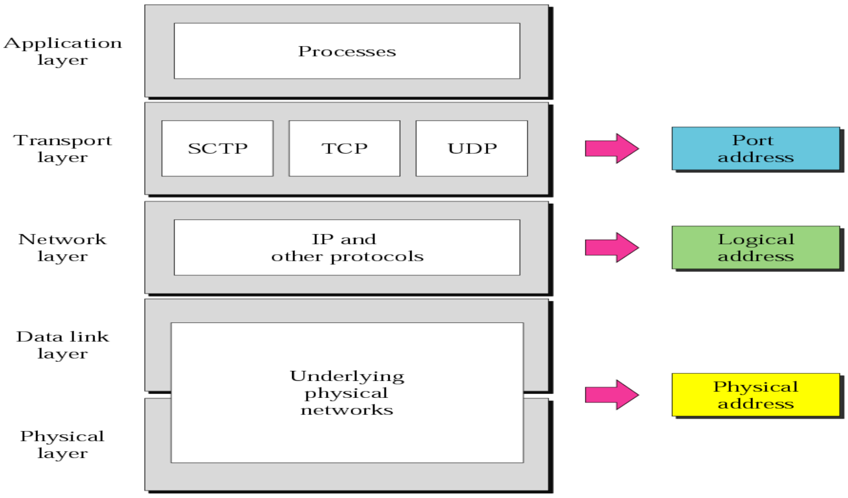
SAR Layer : It breaks the packets into cells while transmitting and assembles them back together at the receiving end.

CS Layer : convergence sub layer makes it possible to have different ATM systems that offer various kinds of services to different applications. File transfer and video on demand have different requirements regarding error handling, timing, etc.

Addressing : The different level of addressing is used in TCP/IP protocols. Basically these addresses are of three types. They are classified as :



Relationship of layers and addresses in TCP/IP :



Physical Address : This address present in physical and data link layer. This is a node address. The length of this address is 48 bits. Out of 48 bits 24 bits are assigned by NIC uniquely. This address is stored in the ROM of LAN card. This is also known as MAC address, LAN address, H/W address, Ethernet Address, NIC address. This is the unique address. No two systems can have the same physical address. This is denoted

by hexa decimal notation. Every byte is separated by a : (colon) notation. Each byte is represented with two hexa decimal digits.
Ex : ***07:01:02:01:2C:4B***

Logical Address : This address present in network layer. This is a host address. The length of this address is 32 bits. This address consists of host identification and network identification. This is also known as Internet address, IP address or host address. It is represented by dotted decimal notation. Each byte is delimited by a dot operator, and the numbers are represented in decimal notation.
Ex : 192.168.100.23

Port Address : This address present in Transport Layer. This is an end to end address. This is also known as process identification number, process address, service point address or transport address. The length of address is 16 bits. Therefore we can have 65,536 addresses available starting from 0. Each protocol and application (task) will be assigned by a number.
Ex : http : 80, ftp :20,21, Telnet :23

Socket Address : This is a combination of IP address and Port address. The length of socket address is 48 bits (32+16). This is used to identify an individual connection.

UNIT-1 Objective Type QUESTIONS

1. The --------------are the rules that govern a communication exchange.
   a. Media b. Criteria c**. Protocols** d. All of the above

2. The -------- is the physical path over which a message travels
   a. Protocol b. **Medium** c. signal d. All of the above

3. Frequency of failure and network recovery time after a failure are measures of the --------------------of a network
   a. Performance b. **reliability** c. security d. feasibility

4. The performance of data communications network depends on ---------------
   a. The no of users b. the transmission media c. h/w and s/w d. **All**

5. The Viruses are a network --------------- issue.
   a. performance **b. security** c. reliability d. All

6. The ---------------is the division of one task among multiple computers
   a. **Distributed processing** b. distributed messaging
   c. distributed telephony d. Electronic messaging

7. If a protocol specifies that data should be send at 100 Mbps, this is a ---------issue
   a. Syntax b. Semantics c. **Timing** d. None of the above

8. ________ defines how a particular pattern to be interpreted, and what action is to be taken based on that interpretation.
   a. Semantics b. Syntax c. Timing d. none of the above

9. The ----- defines the structure and format of the data meaning the order in which they are transmitted
   a. **syntax** b. semantics c. timing d. none

10. Which topology requires a central controller or hub ?
    a. Mesh b. **Star** c. Bus d. Ring

11. Which topology requires a multipoint connection?
    a**. Mesh** b. star c. Bus d. Ring

12. communication between a computer and a keyboard involves------ transmission
    a. **Simplex** b. Half-duplex c. Full Duplex d. automatic

13. In a network with 25 computers, which topology would acquire the most extensive cabling?
    a**. Mesh** b. star c. Bus d. Ring
14. A television broadcast is an example of ------------------ transmission
    a**. simplex** b. half-duplex c. full duplex d.automatic

15. In a ---------topology, if there are n devices in a network, each device has n-1 ports for cables.
    a**. Mesh** b. star c. Bus d. Ring
16. A ------------connection provides a dedicated link between two devices.
    a**. Point to Point** b. Multipoint c. Primary d. Secondary

17. In a ------connection, more than two devices can share a single link .
    a**.** Point to Point b. **Multipoint** c. Primary d. Secondary

18. In ---------transmission, the channel capacity is shared by both communicating devices at all times.
    a. simplex b. half-duplex c**. full duplex** d. half-simplex

19. Tata Mc Hill publishing company has headquarters in Delhi, and branch offices at Pakistan, Singapore, Malesia, America is probably connected by a -------------
    a. LAN b. MAN c. **WAN** d. none of the above

20. An organization has a network consisting of two workstations and one printer. This is most probably a -----------
    a. **LAN** b. MAN c**.** WAN d. none of the above

21. Which topology requires a point to point configuration ?
    a**. Mesh** b. star c. Bus d. Ring

22. In a ---------link, the only traffic is between the two connected devices.
    a. secondary b. primary c. **dedicated** d. None of the above

23. In a mesh topology, the relationship between one device and another is -------
    a. Primary to peer b. peer to primary **c. peer to peer** d. primary to secondary

24. A cable break in a ------ topology stops all transmission
    a**.** Mesh b. star c. **Bus** d. primary

25. A network that contains multiple hubs is most likely configured in a --- topology
    a**.** Mesh b. star c. Bus d. **Tree**

26. Security and privacy are less of an issue for devices in a --------- topology
    a**.** Mesh b. star c. **Bus** d. Tree

27. The OSI model consists of ----------- layers
a. 3 b. 5 c**. 7** d. 8

28. The layer decides the location of synchronization points
a. Transport b**. session** c. presentation d. application

29. The end to end delivery of the entire message is the responsibility of the ----- layer.
a. network b. **Transport** c. session d. Presentation

30. Which of the following are the functions of application layer/
a. network virtual terminal b. file transfer c. mail services **d. All of the above**

31. Which layer is very closest to the transmission medium?
a. data link b. **physical** c. network d. transport

32. In which layer a data unit is called as Frame ?
a. physical b. transport c. **data link** d. application

33. Encryption and Decryption are the functions of which layer?
a**. presentation** b. physical c. session d. data link

34. Dialog control is a function of which layer/
a. physical b. network c. transport d. **session**

35. Mail and directory services are the functions of which layer?
a. presentation **b. application** c. session d. transport

36. Node to Node delivery is possible by which layer
a. network b. **data link** c. transport d. presentation

37. When the packet moves from the lower layers to the upper layers, then headers are ---------
a. added b. **subtracted** c. rearranged d. modified

38. When the packet moves from upper to lower layers, then headers are ----
a**. added** b. subtracted c. rearranged d. modified

39. Which layer lies between data link and transport layer
a. physical b**. network** c. session d. presentation

40. Which layer does translations from one character code another occur?
a. transport b. session c**. presentation** d. application

41. Which layer changes bits into electro magnetic signals?
a. presentation b**. physical** c. transport d. application

42. Which layer uses the trailer field to do error correction?
a. physical b. network c. transport d. **data link**

43. Physical layer is concert with the transmission of ----on the physical medium.
a. protocols b. dialogs c. programs d. **bits**

44. Which layer works as a mediator between user support and network support layers
a. session b**. transport** c. network d. data link

45. Which layer provides host to host delivery?
a. data link b. transport c. **network** d. physical

46. Checkpoints exists in ------ layer
a. presentation b. **session** c. transport d. physical

47. How many port addresses are available?
a. 16 b. 256 c**. 65,536** d. 65,535

48. What is the length of IP address in bits?
a. 16 b**. 32** c. 256 d. 4

49. logical addresses are represented in ----------- format
a. decimal b. numeric c. dotted decimal d. hexa decimal

50. Physical addresses are represented in -------------format
a. dotted decimal b**. hexa decimal** c. octal d. binary

51. ATM networks are treated as a ---------------------- network
a. frame b. packet c. **cell** d. data unit

52. The length of ATM cell is ------------ bytes long
a. 51 b. 52 c. 53 d. 43