UNIT-IV

DATA COMMUNICATION AND NETWORKS

Concepts of Data Communication, Types of Data-Communication Networks, Communications Media, Concepts of Computer Networks, the Internet, Intranet and Extranets: Operation of the Internet, Services provided by Internet, World Wide Web.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

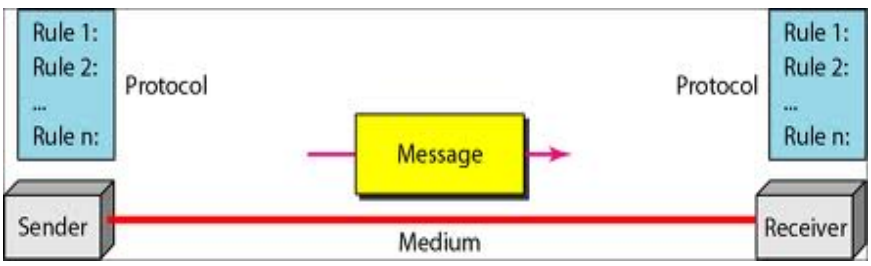
3. Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30ms delay and others with 40 ms delay, an uneven quality in the video is the result.

COMPONENTS:

A data communications system has five components

1. Message
2. Sender
3. Receiver
4. Medium
5. Protocol



1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Representation

Information today comes in different forms such as text, numbers, images, audio, and video.

Text

In data communications, text is represented as a bit pattern, a sequence of bits (0's or 1's). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII) developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. For example, an image can be divided into 1000 pixels or

10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.

After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black and white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel.

If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11.

There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

Video

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex

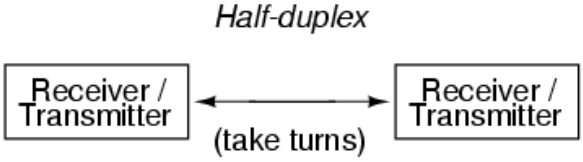
Simplex: In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept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

Simplex communication

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.



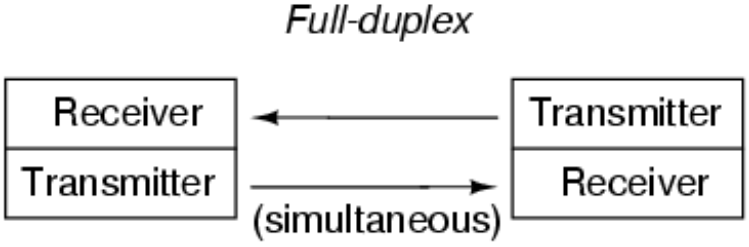
Full-Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously.

The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel 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.



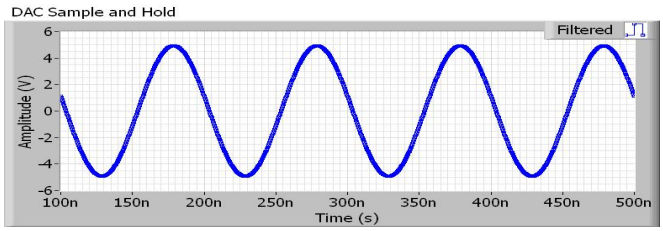
SIGNALS:

There are two types of signals to transfer data.

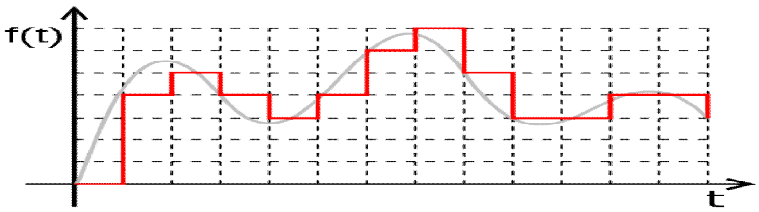
1. **Analog Signal**

2. **Digital Signal**

Analog signals: An analog signal are continuous and passes through or includes an infinite number of continuous values along its path. The curve representing the analog signal passes through an infinite number of points.



Digital signals can have only limited number of defined values. Although each value can be any number, it is as simple as 1 and 0.



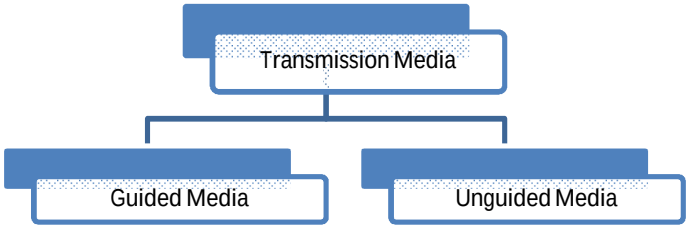
Data can be analog or digital. Analog data are continuous and take continuous values.
Digital data have discrete states and take discrete values.
Signals can be analog or digital. Analog signals can have an infinite number of values in a range; digital signals can have only a limited number of values.

TRANSMISSION MEDIA:

In telecommunications, transmission media can be divided into two broad categories: Guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.

1. Guided media.

2. Unguided media.



Guided Media are the physical links through which signals are confined to narrow path. These are called as guided media. The Guided media can be divided into three types. Such as

1. Twisted pairs cable 2. Coaxial Cable 3. Fiber optic cable

Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

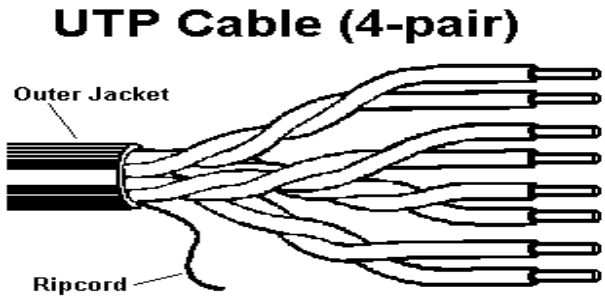
Twisted Pair Cable:

The most popular network cabling is twisted pair. It is light weight, easy to install, inexpensive and support many different types of network. It also supports the speed of 100 mps.Twisted pair cabling is made of pairs of solid or stranded copper twisted along each other. The twists are done to reduce vulnerably to EMI and cross talk. The number of pairs in the cable depends on the type. The copper core is usually 22-AWG or 24-AWG, as measured on the American wire gauge standard. There are two types of twisted pairs cabling

1. Unshielded twisted pair (UTP)
2. Shielded twisted pair (STP)

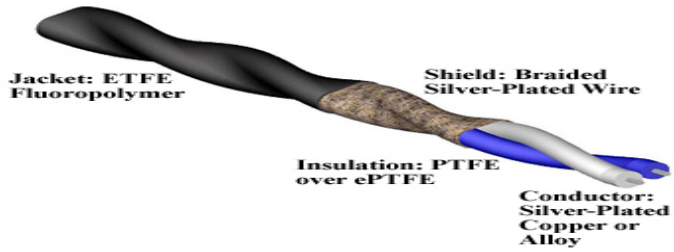
Unshielded twisted pair (UTP)

UTP is more common. It can be either voice grade or data grade depending on the condition. UTP cable normally has an impedance of 100 ohm. UTP cost less than STP and easily available due to its many use. There are five levels of data cabling.



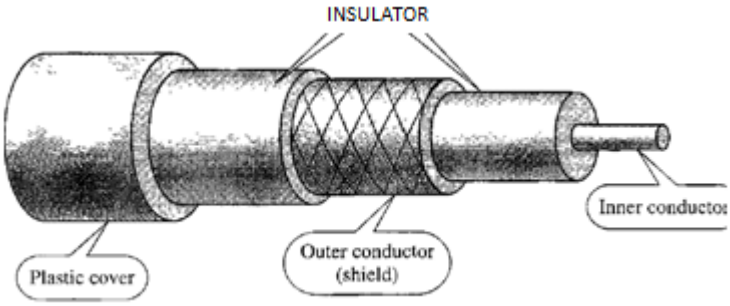
Shielded twisted pair (STP):

It is similar to UTP but has a mesh shielding that's protects it from EMI which allows for higher transmission rate.



Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover



Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiber-optic cable.

Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable.

Fiber Optic cable

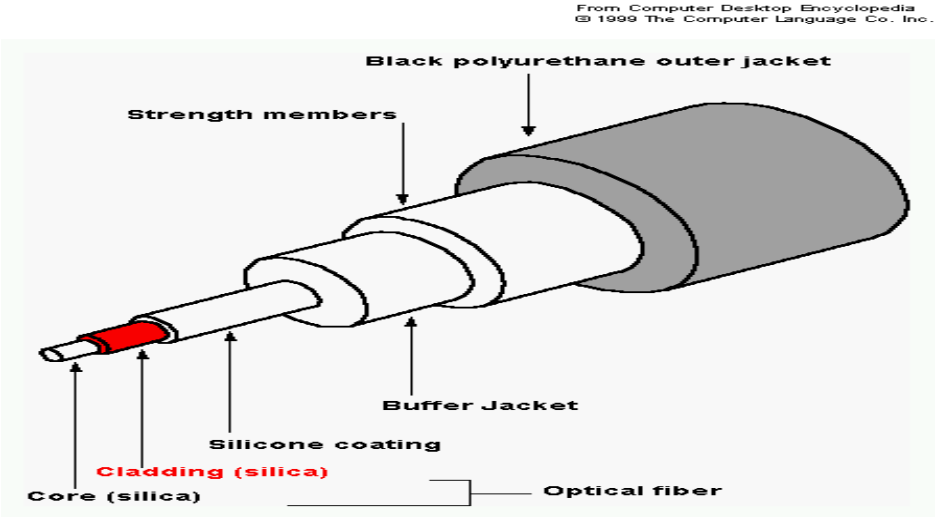
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps. The SONET network provides such a backbone.

Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides

the connection to the user premises. This is a cost-effective configuration since the narrow bandwidth requirement at the user end does not justify the use of optical fiber.



Advantages and Disadvantages of Optical Fiber

Advantages

Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial).

- Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.
- Less signal attenuation. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.
- Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.
- Light weight. Fiber-optic cables are much lighter than copper cables.
- Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages

There are some disadvantages in the use of optical fiber.

- Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.

- Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- Cost. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

UNGUIDED MEDIA: WIRELESS

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation.

In **ground propagation**, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance.

In **sky propagation**, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.

In **line-or-sight propagation**, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

We can divide wireless transmission into three broad groups: **radio waves, microwaves, and infrared waves.**

Radio Waves

Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves.

The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, cordless phones, are examples of multicasting

Microwaves

Electromagnetic waves having frequencies between I and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.

The following describes some characteristics of microwave propagation:

- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for longdistance communication.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore wider sub-bands can be assigned, and a high data rate is possible
- Use of certain portions of the band requires permission from authorities.

Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

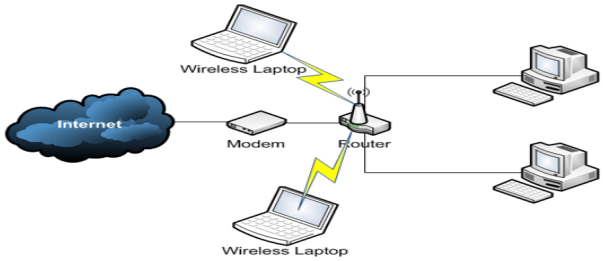
Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Devices used in networking:

Mainly four devices are used in networking:-

- Modem
- Hub
- Switch
- Router

❖ **MODEM-(modulator-demodulator):**

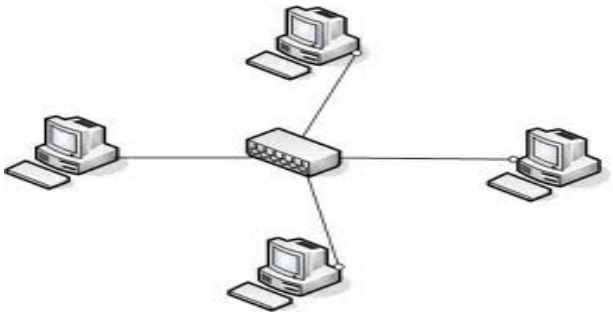


A modem is a device that modulates an analog carrier signal to encode digital information and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analog signals, from light emitting diodes to radio.

There are two types of modem:-

1. Internal modem 2. External modem

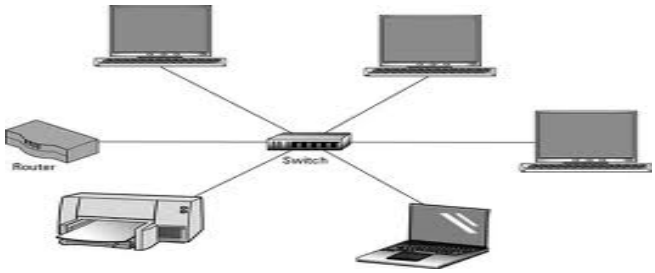
❖ **HUB:**



A common connection point for devices in a network. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

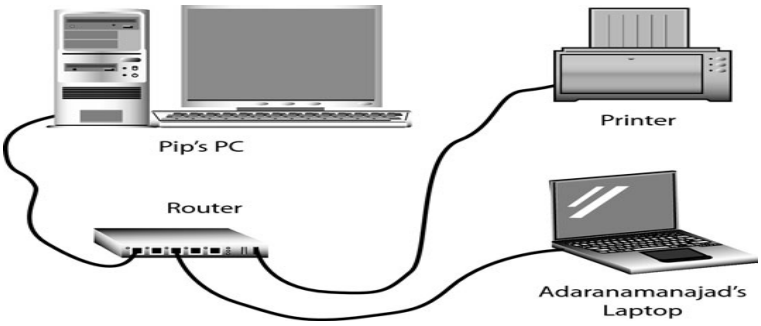
❖ **Switch:**

A network switch is a small hardware device that joins multiple computers together within one local area network (LAN). Network switches appear nearly identical to network hubs, but a switch generally contains more intelligence than a hub. Unlike hubs, network switches are capable of inspecting data packets as they are received, determining the source and destination device of each packet, and forwarding them appropriately. By delivering messages only to the connected device intended, a network switch conserves network bandwidth and offers generally better performance than a hub.



❖ **Router:**

A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table it directs the packet to the next network on its journey. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it gets to its destination node.



TYPES OF COMMUNICATION NETWORKS:

Local Area Networks:

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size,

(2) Their transmission technology, and

(3) Their topology.

LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines once used in rural areas. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps Various topologies are possible for broadcast LANs. In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending. An arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet, for example, is a bus-based broadcast

network with decentralized control, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later.

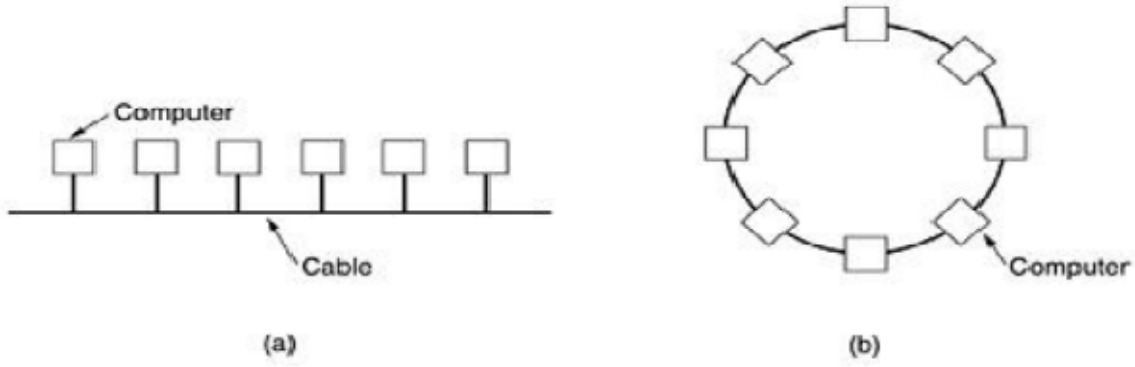


Fig.1: Two broadcast networks. (a) Bus. (b) Ring.

A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted. As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring. Various methods, such as having the machines take turns, are in use. IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.

Metropolitan Area Network:

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses. At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only. To a first approximation, a MAN might look something like the system shown in Fig. Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16.

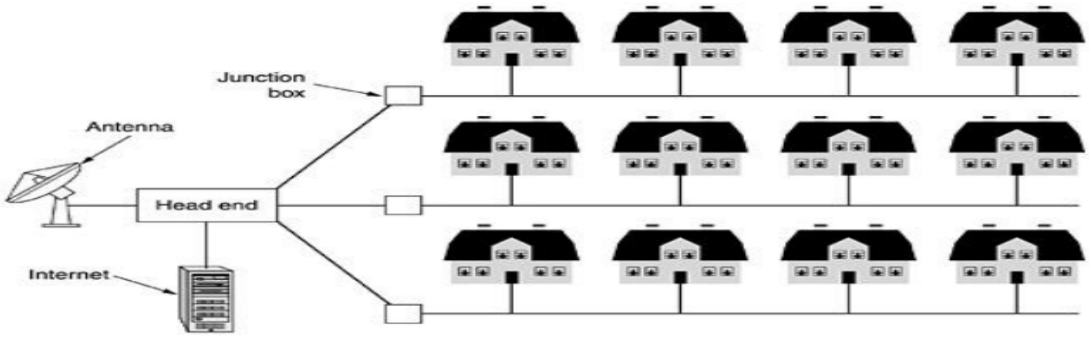
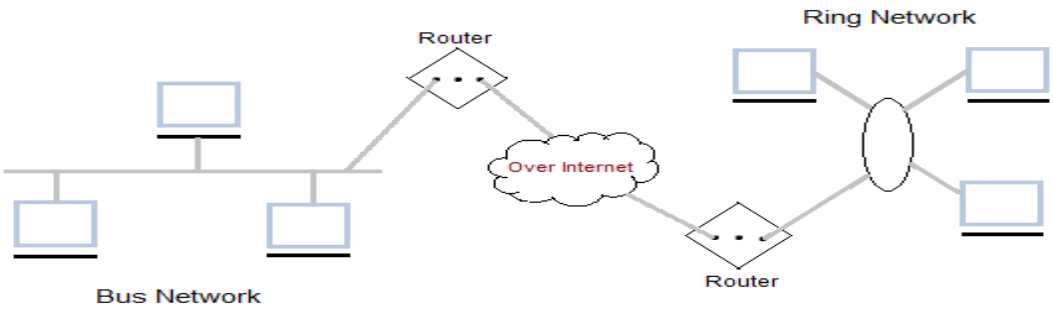


Fig.2: Metropolitan area network based on cable TV.

A MAN is implemented by a standard called DQDB (Distributed Queue Dual Bus) or IEEE 802.16. DQDB has two unidirectional buses (or cables) to which all the computers are attached.

Wide Area Network:

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design. In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links.



In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one router to another via

one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet. Nearly all wide area networks (except those using satellites) have store-and-forward subnets. When the packets are small and all the same size, they are often called cells. The principle of a packet-switched WAN is so important. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process. A stream of packets resulting from some initial message is illustrated in Fig.

In this figure, all the packets follow the route ACE, rather than ABDE or ACDE. In some networks all packets from a given message must follow the same route; in others each acked is routed separately. Of course, if ACE is the best route, all packets may be sent along it, even if each packet is individually routed.

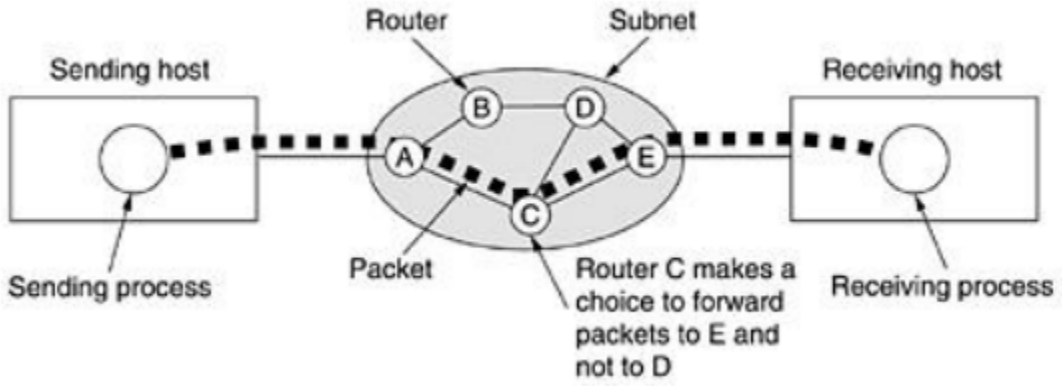
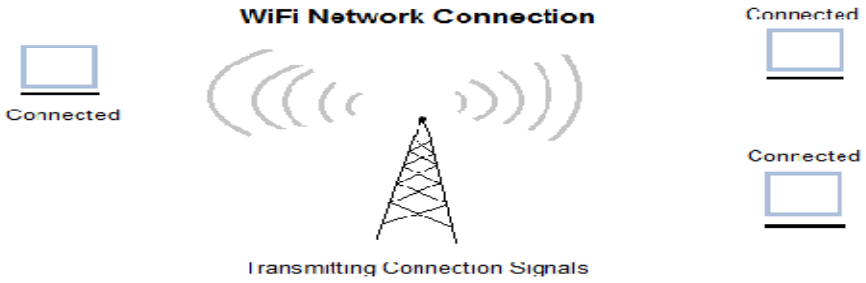


Fig.3.1: A stream of packets from sender to receiver.

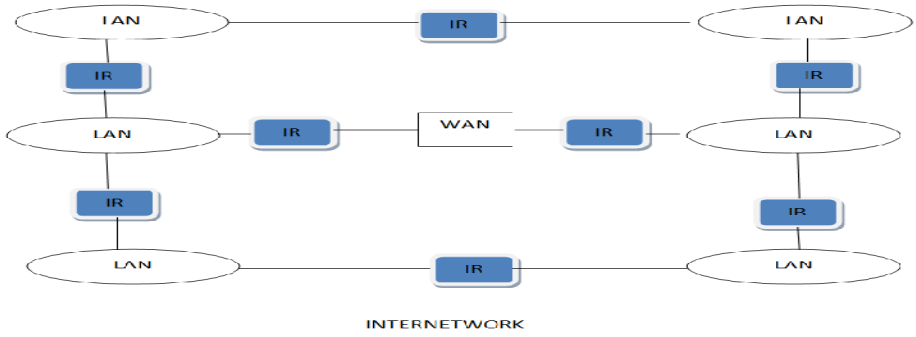
Not all WANs are packet switched. A second possibility for a WAN is a satellite system. Each router has an antenna through which it can send and receive. All routers can hear the output from the satellite, and in some cases they can also hear the upward transmissions of their fellow routers to the satellite as well. Sometimes the routers are connected to a substantial point-to-point subnet, with only some of them having a satellite antenna. Satellite networks are inherently broadcast and are most useful when the broadcast property is important.

WIRELESS WAN'S:

Modern digital wireless systems have better performance. Wireless networks provide connection communication links such as infrared, radio frequency, microwaves links etc. these types of networks allow mobile devices to move freely which are completely wireless.



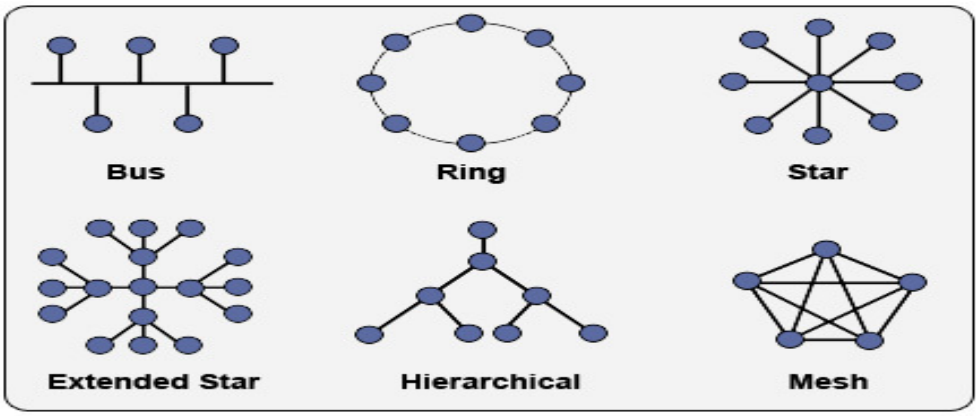
Inter network: when we are connect two or more networks then they are called internetwork or internet. We can join two or more individual networks forms internetwork through devices like routers gateways, bridges.



NETWORK TOPOLOGIES:

Topology: Topology refers to the layout of connected devices on a network. Here, some logical layout of topology. Mesh, Star, Bus, Ring, Tree and Hybrid

Network Topology:

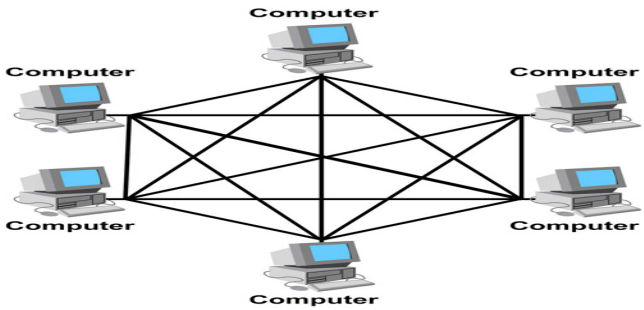


Mesh Topology

Here every device has a point to point link to every other device. Node 1 node must be connected with n-1 nodes. A fully connected mesh can have n(n-1)/2 physical channels to link n devices. It must have n-1 I/O ports.

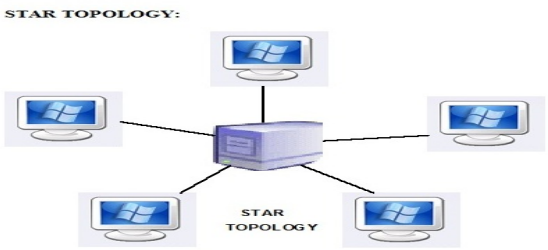
Advantages:

1. They use dedicated links so each link can only carry its own data load. So traffic problem can be avoided.
2. It is robust. If anyone link get damaged it cannot affect others.
3. It gives privacy and security.(Message travels along a dedicated link)
4. Fault identification and fault isolation are easy.



Star Topology:

- Here each device has a dedicated point-to-point link to the central controller called "Hub"(Act as a Exchange).
- There is no direct traffic between devices.
- The transmissions are occurred only through the central "hub".



- When device 1 wants to send data to device 2; first sends the data to hub. This then relays the data to the other connected device.

Advantages:

1. Less expensive then mesh since each device is connected only to the hub.
2. Installation and configuration are easy.
3. Less cabling is need then mesh.
4. Robustness.(if one link fails, only that links is affected. All other links remain active)
5. Easy to fault identification & to remove parts. No disruptions to the network then connecting(or) removing devices

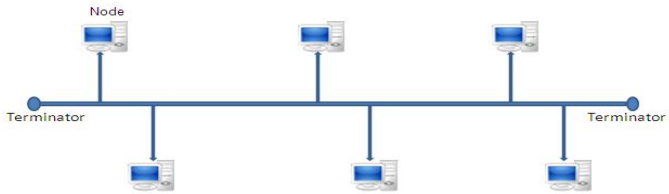
Bus Topology:

- A bus topology is multipoint.
- Here one long cable act as a backbone to link all the devices are connected to the backbone by drop lines and taps.
- Drop line- is the connection b/w the devices and the cable.
- Tap- is the splitter that cut the main link.

- This allows only one device to transmit at a time.

Advantages:

1. Ease of installation
2. Less cabling

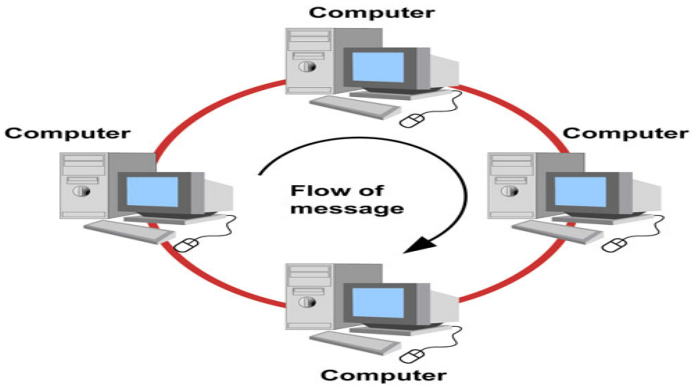


Disadvantages:

1. Difficult reconfiguration and fault isolation.
2. Difficult to add new devices.
3. Signal reflection at top can degradation in quality. If any fault in backbone can stops all transmission

Ring topology

- Here each device has a dedicated connection with two devices on either side.
- The signal is passed in one direction from device to device until it reaches the destination and each device have repeater.
- When one device received signals instead of intended another device, its repeater then regenerates the data and passes them along.



- To add or delete a device requires changing only two connections.

Advantages:

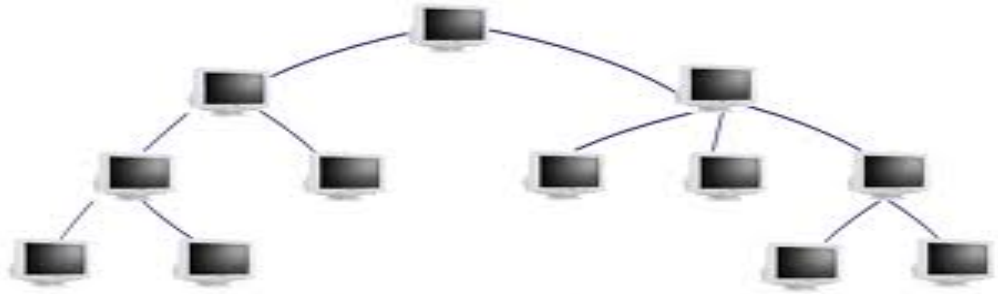
1. Easy to install.
2. Easy to reconfigure.
3. Fault identification is easy.

Disadvantages:

1. Unidirectional traffic. Break in a single ring can break entire network.

Tree Topology:

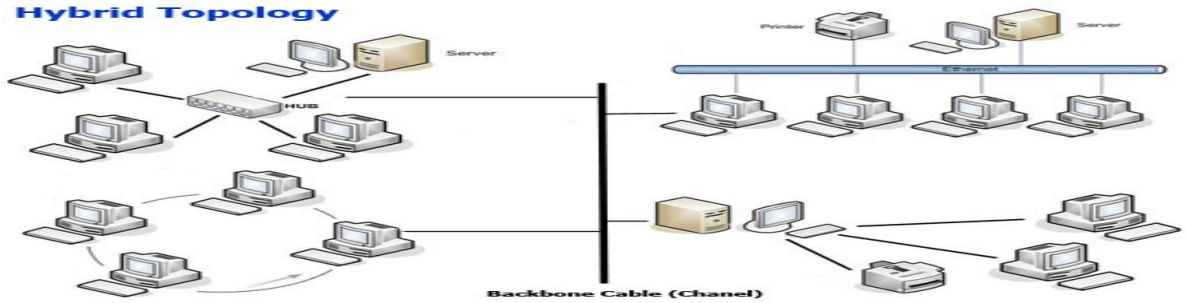
- Alternatively referred to as a star bus topology.
- Tree topology is one of the most common network setups that is similar to a bus topology and a star topology.
- A tree topology connects multiple star networks to other star networks. Below is a visual example of a simple computer setup on a network using the star topology.



Digram - Tree Topology

Hybrid Topology:

A network which contain all type of physical structure and connected under a single backbone channel.



A" protocol" is a set of rules governing the format and the meaning of the frames or messages that are exchanged by the peer entities within the layer. Entities use their protocols in order to implement their service definitions

The OSI Reference Model:

The OSI model 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. 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.

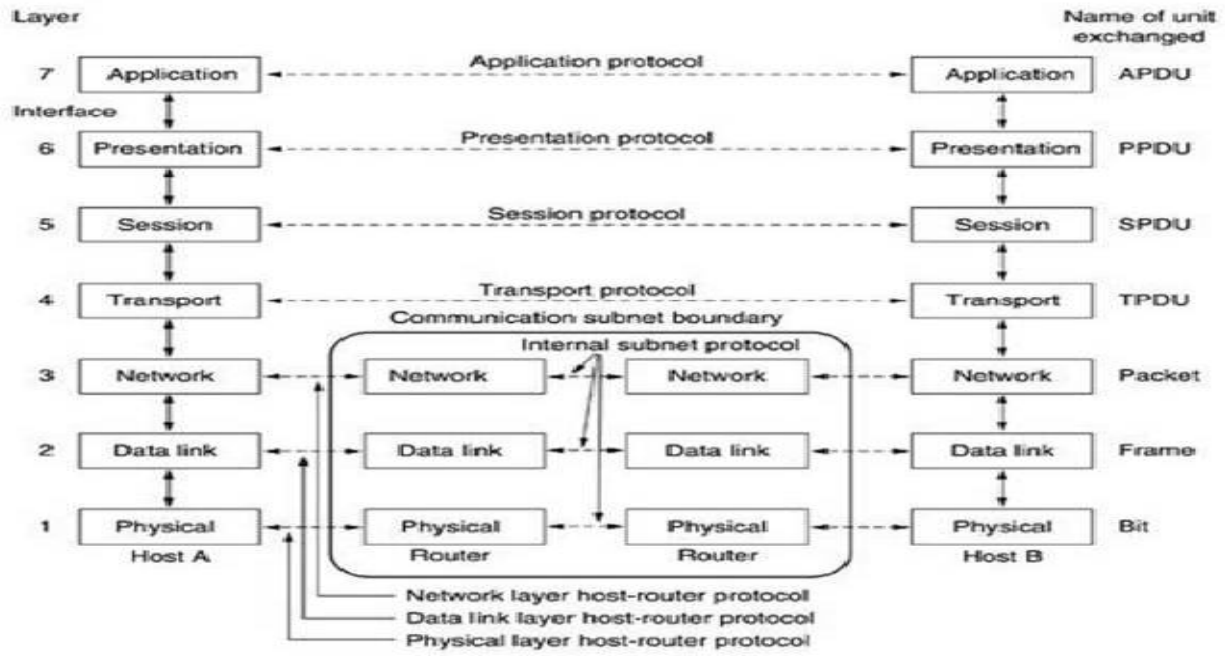


Fig.: The OSI reference model.

The Physical Layer:

Function : Defines electrical and mechanical standards. deals with timing interfaces.

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:

Function : Framing error detection and flow control.

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:

Function : Routing Qos and congestion control.

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:

Function: Connection management, flow control and error flow.

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 neighbors, and not between the ultimate source and destination machines, which may be separated by many routers.

The Session Layer:

Function: Session management, token management, dialog control and synchronization.

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:

Function: Encoding and decoding,encryption and decryption ,compression and decompression

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.

The TCP/IP Reference Model:

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

1. To connect multiple networks together so that they appear as a single network.
2. To survive after partial subnet hardware failures.
3. To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

1. Host-to-Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer

Application layer
Transport layer
Internet layer
Host to network layer

TCP/IP Reference model

Host-to-Network Layer:

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

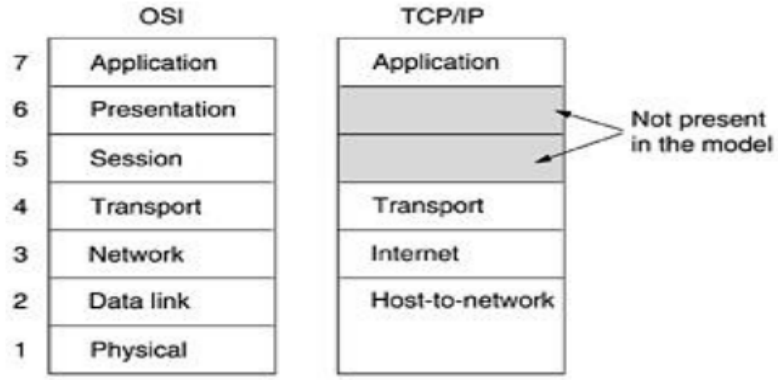
Internet Layer:

This layer, called the internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have they travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The internet layer defines an official packet format and protocol called IP (Internet Protocol). The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer.

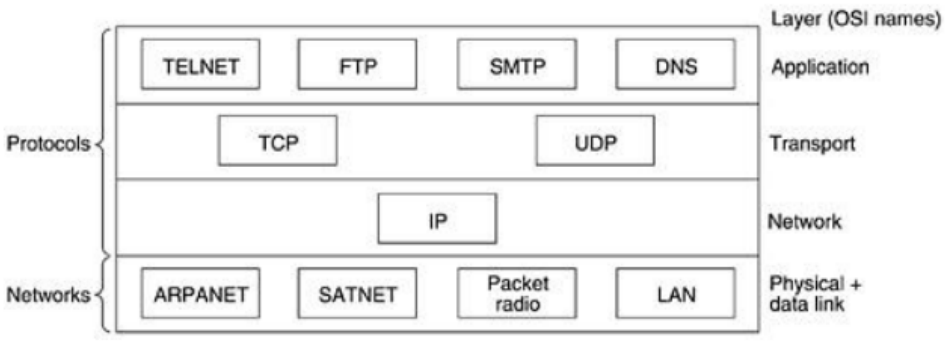
The Transport Layer:

The layer above the internet layer in the TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.



The TCP/IP reference model.

The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig. 6.2. Since the model was developed, IP has been implemented on many other networks.



Protocols and networks in the TCP/IP model initially.

The Application Layer:

The TCP/IP model does not have session or presentation layers. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP), as shown in Fig.6.2. The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it. Many other protocols have been added to these over the years: the Domain Name System (DNS) for mapping host names onto their network addresses, NNTP, the protocol for moving USENET news articles around, and HTTP, the protocol for fetching pages on the World Wide Web, and many others.

What is Internet?

It is a Global network of computers which may be server or client that exchanges information. It can be defined as a "network of networks" which can be linked through copper wires, wireless connections, and other technologies. This is the world-wide network of computers accessible to anyone who knows their Internet Protocol (IP) address.

The Internet: Development History

- Grew out of a research network originally funded by U.S. Department of Defense.
- Development of this network, known as the ARPANET after the Advanced Research Projects Agency (ARPA), began in 1969.
- As the network grew, it was used for applications beyond research, such as electronic mail.

In the early 1980s, the current versions of the core Internet protocols, TCP and IP, were introduced across the network. The term Internet comes from the word inter-network - an interconnected set of networks.

In 1992, the Center for European Nuclear Research (CERN) released the first versions of World Wide Web software.

- Subsequently, the number of Web servers has grown quickly.

What is Intranet?

The term Intranet is derived from two words: ‘Intra’ which means within and ‘net’ which means group of interconnected computers. It is a private computer network that uses Internet protocols and network connectivity to securely share any part of an organization's

information or operational systems with its employees. In short, an intranet is private network, similar to the Internet and using the same protocols and technology, contained within an enterprise or not-for-profit organization.

What is Extranet?

It is an intranet for outside authorized users using same internet technologies. The outside users are trusted partners of the organization who have access to information of their interest & concern.It extends the intranet concept to provide a network that connects a company's network to the networks of its business partners, selected customers, or suppliers.

Types of Extranet:

Public Network Extranet

It exists when an organization allows the public to access its intranet from any public network. Security is an issue in this configuration, because a public network does not provide any security protection.

Private Network Extranet

It is a private, leased-line connection bet. Two companies that physically connects their intranets to one another. The single advantage of this is Security. The single largest drawback is Cost.

Virtual Private Network (VPN)

It is a network that uses public networks and their protocols to send sensitive data to partners, customers, suppliers, and employees by using system called "tunneling". Tunnels are private passage ways through the public internet that provide secure transmission from one extranet partner to another

Some uses of Internet

- ✓ Looking for jobs
- ✓ Learning a foreign language
- ✓ Making friends from any part of the world
- ✓ Participating in a discussion about your favorite TV show with similar minded people across the world,
- ✓ Send to a friend, an electronic birthday card that actually signs happy birthday to you'
- ✓ Go through the catalogue of a library situated across the globe and find a book you always wanted to read
- ✓ See the latest photographs of your movie stars.
- ✓ Download some interesting software and try it out.

- ✓ Make your own home page, which talks about yourself, your family, your pets and your hobbies.
- ✓ Chat with a friend working abroad and see him as you talk.

From home you can use Internet for following activities

- ✓ To exchange email with friends and family
- ✓ To participate in group discussions through public news groups or bulletin board
- ✓ To find educational tools around the world, access libraries, book stores etc.
- ✓ For entertainment
- ✓ To do shopping
- ✓ Leisure activities

For business the Internet is invaluable:

- ✓ Get technical support for products
- ✓ Distribute software
- ✓ Provide technical support, bug fixes, product information to customers etc.
- ✓ Publish information on any topic
- ✓ Communicate or collaborate on projects
- ✓ Market or sell products
- ✓ Access business while at home
- ✓ These services can be availed round the clock from anywhere in the world.
- ✓ At any given point of time, up-to-date information can be obtained.

The Internet Layered Architecture:

The Internet, as a network of connecting many small networks, consists of four layers:

- Application Layer (HTTP, SMTP..)
- Transport Layer (TCP, UDP)
- Network Layer (IP)
- Physical Layer

The Internet: Design Principles

The Internet has been successful because of some fundamental decisions about its design made early in its history.

- Interoperability:

Independent implementations of Internet protocols actually work together.

Interoperability means that systems can be assembled using client and server computers and software from different vendors.

In the context of Internet commerce, interoperability means that buyers and sellers do not have to buy and upgrade software simultaneously from the same vendors to conduct commerce.

- Layering:

Internet protocols are designed to work in layers, with each higher layer building on the facilities provided by lower layers.

- Simplicity:

One way to look at the layering of the Internet is that it grows both up and down from IP. IP is very simple, providing only addressing and formatting of packets.

Below the level of IP, there is the complexity of many different kinds of network hardware, topologies, and routers.

IP hides that complexity from applications and insulates application developers from:

- the complexities of different network devices
- the complexities of implementing low-level network protocols.

Above IP, higher-level protocols such as TCP offer service abstractions that are easy for application programmers to understand and use.

- Uniform naming and addressing:

The IP layer offers a uniform addressing structure that assigns a 32-bit address to each computer connected to the network.

Domain name system (DNS) offers a uniform way to translate human-readable names for computers, such as www.openmarket.com to the numeric address for that computer.

- End-to-end:

Internet is designed around end-to-end protocols. That is, the interpretation of the data happens on the sending and receiving systems, but nothing in the network needs to look at anything but the destination address for delivering the packet.

End-to-end protocols have several advantages:

- hide the internal structure of the network
- provide simple abstractions to programmers
- shielding them from such things as the messy details of recovering from lower-level errors.

The Internet Protocols

- **FTP**:(File transfer protocol)

One of the most oldest and probably the most popular protocol to be used to move files on the Internet.

- **TCP/IP**:(Transmission Control Protocol and Internet Protocol)

The low-level communications protocol that holds the Internet together.

It provides means to allows two software on difference machines on the Internet find each other, rendezvous, and transfer data.

It provides the essential service of making sure that each piece of data is transferred in the correct sequence and without error.

- **SMTP**: (the e-mail message protocol)

A protocol to allow two users to communicate through e-mail messages over the Internet.

- **NNTP**: (Net News Transfer Protocol)

A protocol, which can be used to access or transfer Usenet news over the Internet.

- **Telnet**: - The traditional teletype-style communications protocol for communicating with text-based information services.

The World Wide Web:

The Web: An infrastructure of information combined and the network software used to access it

Web page: A document that contains or references various kinds of data

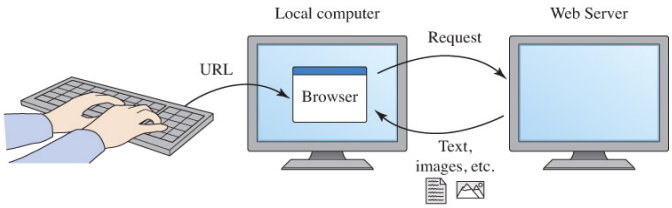
Links A connection between one web page and another

Website: A collection of related web pages

Web browser: A software tool that retrieves and displays eb pages

Web server: A computer set up to respond to requests for web pages

Uniform Resource Locator (URL): A standard way of specifying the location of a Web page, containing the hostname, "/", and a file.



Search Engine: A website that helps you finds other websites

Blog or Weblog : An online journal or newsletter that is frequently updated and intended for public consumption

Hypertext Markup Language (HTML) : The language used to create or build a Web page

Markup language : A language that uses tags to annotate the information in a document

Tags : The syntactic element in a markup language that indicates how information should be displayed

Introduction to World Wide Web

The World Wide Web is an information retrieval system based on hypertext. In hypertext selected words or areas on the screen are expandable, leading to more details about subject. A hypertext allows you to view information without using complex commands and without even using source of information. When a hyperlink is attached to text it is called hypertext

A browser is a client application used to access the information on www. The browser displays web pages and makes the connection necessary to follow hypertext links.

www is a global hypertext system that uses the Internet as its transmission medium.

The www enables you to access information on the Internet without the use of complicated commands. By linking resources throughout the Internet, the web brings a world of information to your doorstep. The www could be very simply defined as a universal database of knowledge. Information that is easily accessible to people around the world and links easily to other pieces of information. This allows any user to quickly find the things most important to themselves. It is an Internet resource where one can get information about different topics such as the latest trends in programming language.

Today there are thousands of web servers throughout the world. Web browsers, who are available for just about every type of computer made enable millions of people to use the www.

The two main uses of the World Wide Web are to retrieve resources and to publish information on the Internet. You can access almost any Internet resource using the www. You can publish your own hypertext documents on the World Wide Web. Web documents are written in HTML. HTML editors and file converters are available to simplify the task of creating documents that contain embedded links to other information.

The World Wide Web: History

- March, 1989, Tim Berners-Lee of Geneva s European Particle Physics Laboratory (CERN) circulated a proposal to develop a hypertext system for global information sharing in High Energy Physics community.

(http://info.cern.ch/hypertext/WWW/TheProject.html)

- The World Wide Web project began to take shape at the beginning of 1991.
- October 1991, the gateway for WAIS search (a crucial development for the Web s future as search as well as a browsing tool),
- Before the end of 1991, CERN announced the Web to the High Energy Physics community in general.
- Essentially, 1992 was a developmental year. In March of 1993, WWW traffic clocked in at 0.1 percent of total Internet backbone traffic.
- In July of 1994, CERN began to turn over the Web project to a new group called the W3 organization, a joint venture between CERN and MIT to develop the Web further.

Introduction to URL's :

Every web page or Internet resource accessible through the www has a unique name, this is URL (Uniform Resource Locator). The URL identifies and locates a resource so that a web browser can access it directly. A URL is type of Internet address. The language that Web clients and servers use to communicate with each other is called the Hyper Text Transfer Protocol (http). All the web clients and servers must be able to speak http in order to send and receive hypermedia documents. For this reason web servers are often called http servers.

A URL can point you to a single record in a database, the front-end of an Internet program, or a result of a query.

Example:

http://www.ibm.com/Features/Harlem/Harlem.html

Protocol / Host Indicator/ Server Name / Path Name / Resource Name

The World Wide Web: HTML

HTML is a simplified derivative of SGML, or Standard Generalized Markup language.

- Its code can be used to make documents readable across a variety of platforms and software.
- Like SGML, HTML operates through a series of codes placed within an ASCII doc. These codes are translated by a WWW client such as Lynx, Mosaic, Cello, Viola, or MacWeb into specific kinds of formats to be displayed on the screen.

- Items include in a HTML page are:
    - links, lists, headings, titles, images, forms, and maps.
- Due to the limitation of HTML documents, now more advanced technologies are introduced to enrich its functions, such as , JavaScript, ActiveX, VML, SVG

HTTP stands for HyperText Transfer Protocol.

- It is a simple data transfer protocol that binds the Web together.
- It supports the communications between a web client (browser) and its web server.
- It consists of a set of messages and replies for both servers and browsers.
- It treats documents, files, menus, and graphics as objects.
- It relies on the Universal resource identifier (URI), enclosed in the universal resource locator (URL), to identify files.
- It uses the Internet s TCP/IP network protocol.

(http://info.cern.ch/hypertext/WWW/Protocols/HTTP/HTTP2.html)

The World Wide Web: Protocols

- **Hypertext Transfer Protocol (HTTP):** HTTP is the original Web Communication protocol which supports the connectionless communications between a Web server and its clients above TCP layer.
- **Secure Sockets Layer (SSL):** Developed by: Netscape Communications Corp.,

It is the most widely used security protocol on the Internet.

Features: Encrypting the communications, digital certificates.

- **Secure HTTP (S-HTTP):** Developed by: Enterprise Integration Technologies (EIT). Not widely used.

Features: Clients and servers can specify authentication and privacy capabilities independently of one another.

The World Wide Web: Tools

- Web Browsers and Web Servers:

HTTP is the original Web Communication protocol which supports the connectionless communications between a Web server and its clients above TCP layer.

To support the client-server communications on the Web.

Web Browser: A web browser is used as a client on the Web to support the following functions:

- to process users requests
- to connect to a web server using URL information
- to send the request to the sever
- to format the responding information (from the server)
- to display the formatted information as a document

Web Sever: A web server plays as a server on the web:

- to listen for incoming requests from the browser
- to find the requested document, and transmit to the browser or
- to find the corresponding CGI program and execute it
- to send the responding information back to the browser

Web Search Tools and Search Directories:

They provides on-line subject guides for users to find the useful information over the Web.

Their major functions are:

- process users search requests

- conduct an information search according to a classified and well-structure index library (database).

- generate the search results

- display them to the users

- Web Authoring Tools:

- Group-ware Tools: Email, FTP, Online Chat,

- Administration Tools: Performance monitor, Trace log, Traffic Monitor

The World Wide Web: Applications

Distributing and Sharing Scientific Data:

Share scientific information (data, papers, databases) among scientists around the world

E-Commerce: Electronic marketing and advertising, online shopping (order/purchase, payment), online trading, online customer services.

Online Education and Training:

On-line courses, training program and information, distance learning Organization and Public

Service: Distributing public service information for organizations and government offices.

Online Publishing: Online books, magazines and journals, newspapers, Video, CD .

Online Banking and Trading: Support online bank transactions for banks and stockbrokerages

DNS:

The Domain Name System (DNS) is used to resolve human-readable hostnames like www.Dyn.com into machine-readable IP addresses like 204.13.248.115. DNS also provides other information about domain names, such as mail services.

IP Addresses

IP addresses are unique four octet numbers expressed either as binary dotted or decimal dotted.

e.g. 10101110.00001011.00010000.01000001 Binary-dotted

179.11.16.65 Decimal-dotted

Address Classes

There are five different classes of address designed to meet the needs of different organizations. The various classes are given as A, B, C, D and E. The classes are distinguished from each other by the decimal notation of the first octet. The class range is presented in the table below:

Class	First Octet	Net-ID	Default Subnet mask	Availability
A	1-126	First Octet	255.0.0.0	Available
B	128-191	First 2 Octet	255.255.0.0	Available
C	192-223	First 3 Octet	255.255.255.0	Available
D	224-239	N/A		Reserved for multicasting
E	240-255	N/A		Reserved

127 is reserved for loopback (127.0.0.1) for internal testing on the local machine. Web applications can be tested on the local machines using the loop back (local host) before deployment to the web.

Each system on a network or Internet is assigned a unique IP address by which it is identified. Furthermore, for easy identification and operations of the entire system, the domain name service (DNS), maintains a database of computer names and IP addresses corresponding to each of them. That is, the DNS is responsible for translating domain names to IP addresses and vice versa as occasions demand between the users and the systems