Chapter 1: Introduction to Data Communication and Computer Networks

Sr. No.	Contents
1.1	Internet basics and network components. [Transmission Media- Guided, Unguided, Network Devices]
1.2	Various types of Networks (only overview)
1.2.1	Connection Oriented N/Ws Vs Connectionless N/Ws,
1.2.2	Ethernet- Ethernet standards ZigBee, WiFi, Access Technique - CSMA-CD, Negotiation technique Overview
1.2.3	. Wireless Network
1.3	Unified Communication –VOIP

Extra Reading: Switching Techniques, CSMA/CA, CSMA/CD, Unified Communication

1.1 Internet basics and network components.

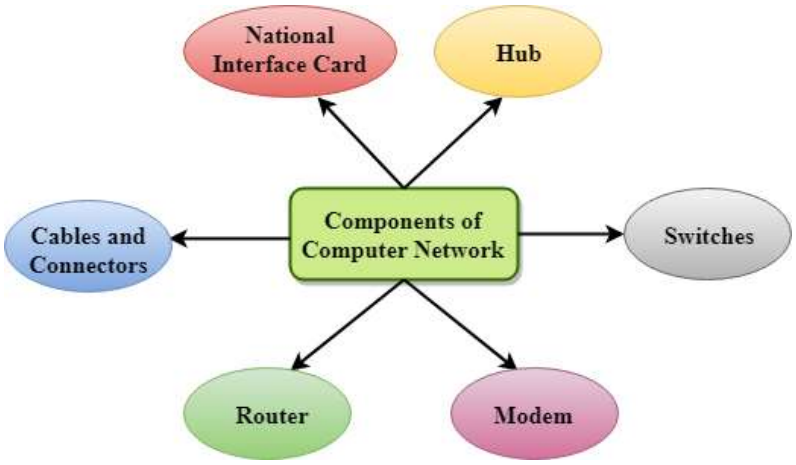
1.1.1 What is a Computer Network?

Computer Network is a group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network.

The aim of the computer network is the sharing of resources among various devices.

In the case of computer network technology, there are several types of networks that vary from simple to complex level.

Components of Computer Network:



Major components of a computer network are:

NIC (Network Interface Card)

NIC is a device that helps the computer to communicate with another device. The network interface card contains the hardware addresses; the data-link layer protocol uses this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC: wireless NIC and wired NIC.

Wireless NIC: All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the radio wave technology.

Wired NIC: Cables use the wired NIC to transfer the data over the medium.

Hub

Hub is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub. Hub distributes this request to all the interconnected computers.

Switches

Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

Cables and connectors

Cable is a transmission media that transmits the communication signals. There are three types of cables:

Twisted pair cable: It is a high-speed cable that transmits the data over 1Gbps or more.

Coaxial cable: Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair cable, but it provides the high data transmission speed.

Fiber optic cable: Fiber optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive as compared to other cables, so it is installed at the government level.

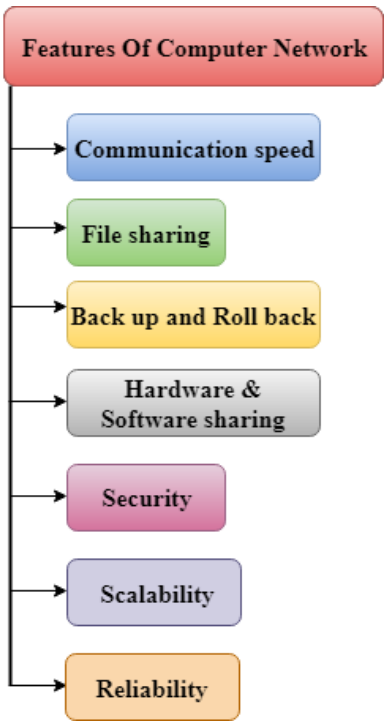
Router

Router is a device that connects the LAN to the internet. The router is mainly used to connect the distinct networks or connect the internet to multiple computers.

Modem

Modem connects the computer to the internet over the existing telephone line. A modem is not integrated with the computer motherboard. A modem is a separate part on the PC slot found on the motherboard.

1.1.2 Features of Computer network



1.1.3 Computer Network Architecture (Categories of Network)

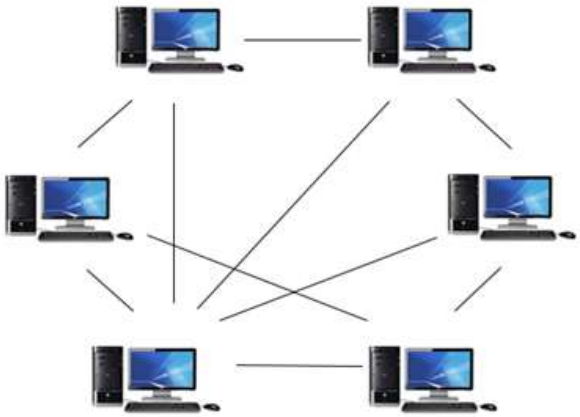
Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

Network can be divided in to two main categories:

- Peer-to-peer.
- Server – based.

o In peer-to-peer networking there are no dedicated servers or hierarchy among the computers. All of the computers are equal and therefore known as peers.
o Normally each computer serves as Client/Server and there is no one assigned to be an administrator responsible for the entire network.
o Peer-To-Peer network is useful for small environments, usually up to 10 computers.

- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages of Peer-To-Peer Network:

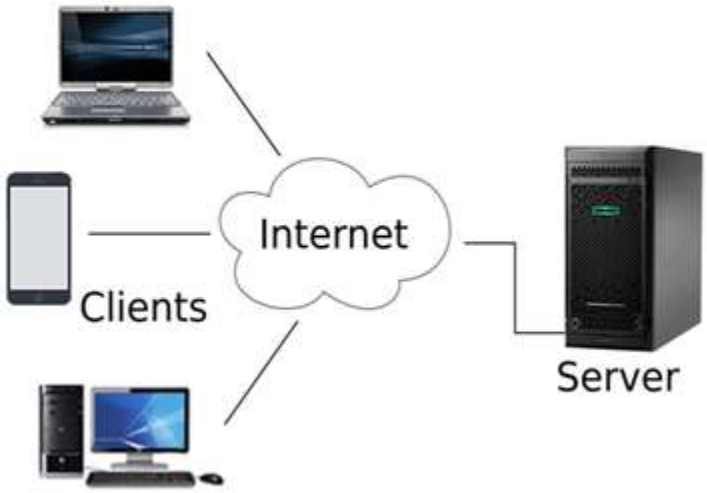
- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.
- Peer-to-peer networks are good choices for needs of small organizations where the users are allocated in the same general area, security is not an issue and the organization and the network will have limited growth within the foreseeable future.

The term Client/server refers to the concept of sharing the work involved in processing data between the client computer and the most powerful server computer.

The client/server network is the most efficient way to provide:

- Databases and management of applications such as Spreadsheets, Accounting, Communications and Document management.
- Network management.
- Centralized file storage.
- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.

All the clients communicate with each other through a server. For example, if client -1 wants to send some data to client -2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages of Client/Server network:

- A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

1.1.4 Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.

- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Why Switching Concept is required?

Switching concept is developed because of the following reasons:

Bandwidth: It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.

Collision: Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

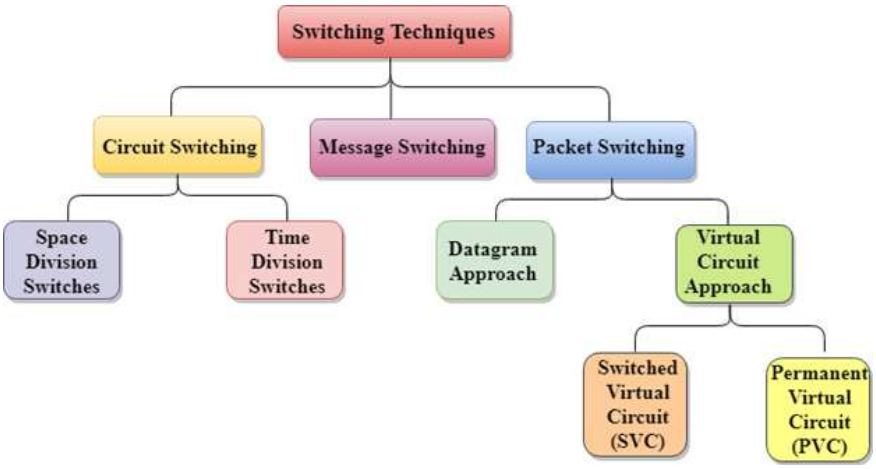
- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification of Switching Techniques

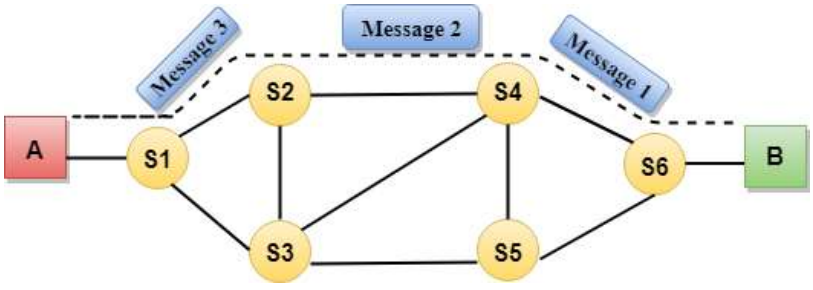


Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Advantages of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.

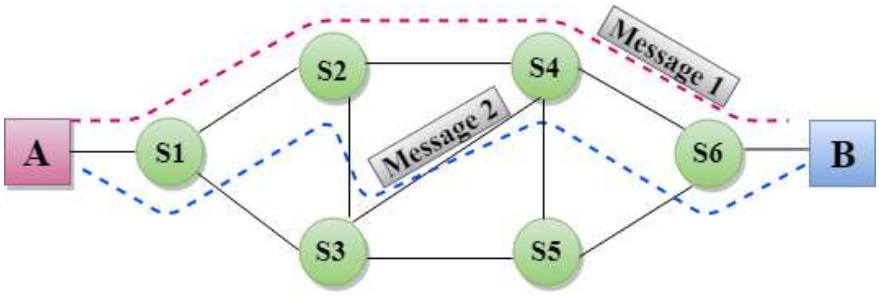
- It has fixed bandwidth.

Disadvantages of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as store and forward network.
- Message switching treats each message as an independent entity.



Advantages of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.

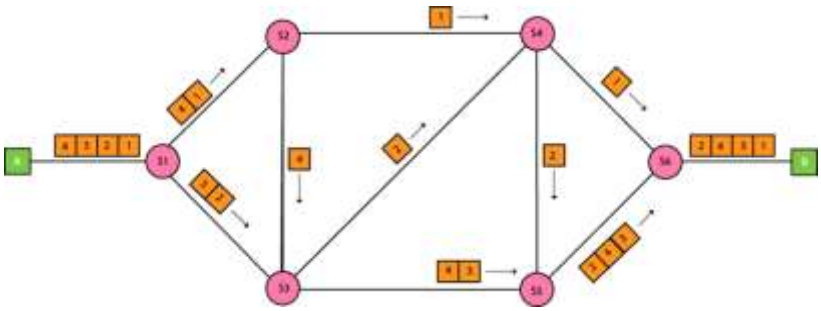
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches of Packet Switching:

There are two approaches to Packet Switching:

Datagram Packet switching:

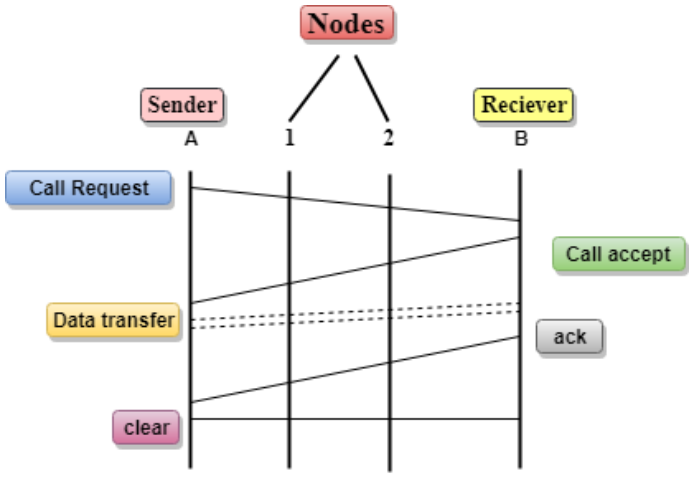
- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.

- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages of Packet Switching:

- Cost-effective: In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- Reliable: If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- Efficient: Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

1.1.5 What is Multiplexing?

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (MUX) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

De-multiplexing is achieved by using a device called De-multiplexer (DEMUX) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that de-multiplexing follows the one-to-many approach.

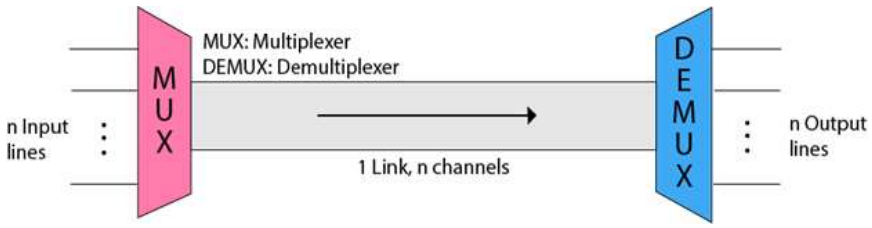
Why Multiplexing?

- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.

History of Multiplexing

- Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.
- Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.
- George Owen Squier developed the telephone carrier multiplexing in 1910.

Concept of Multiplexing



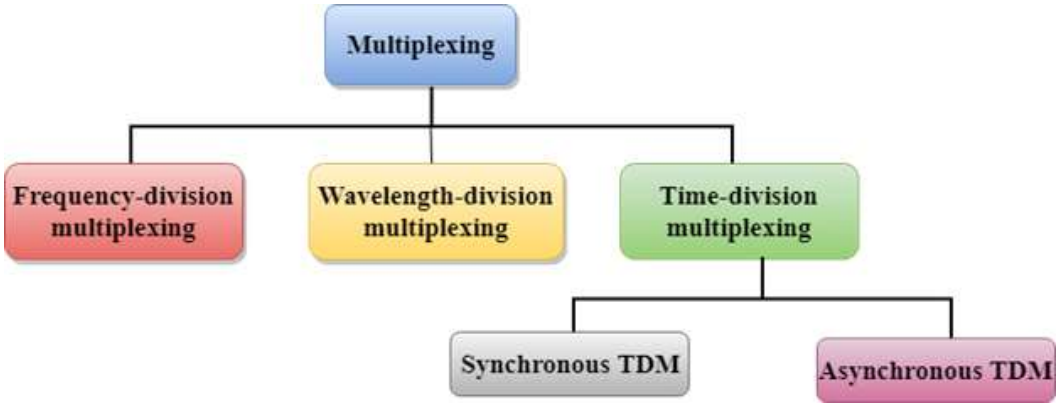
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a De-multiplexer and de-multiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

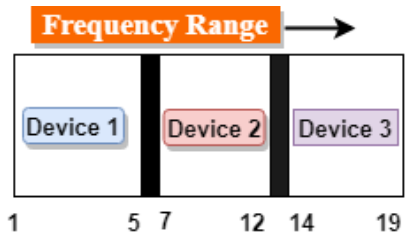
Multiplexing Techniques

Multiplexing techniques can be classified as:

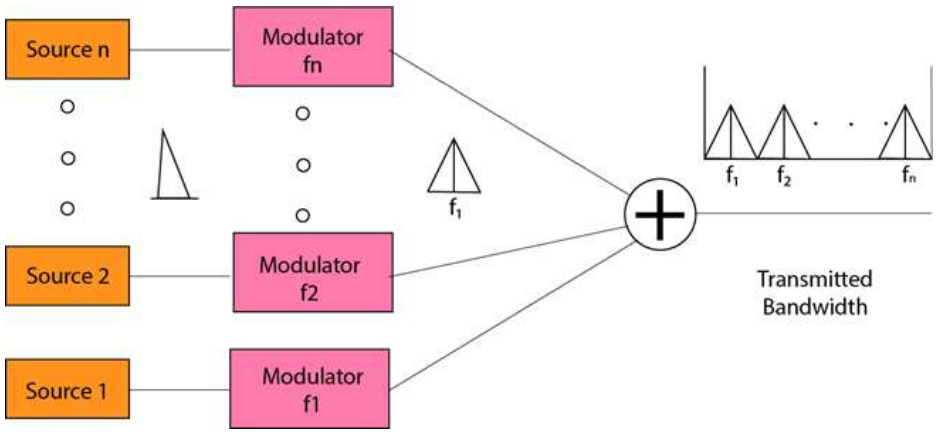


Frequency-division Multiplexing (FDM)

- It is an analog technique.
- Frequency Division Multiplexing is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as sub-carriers. They are represented as f1,f2..fn.
- FDM is mainly used in radio broadcasts and TV networks.



Advantages of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

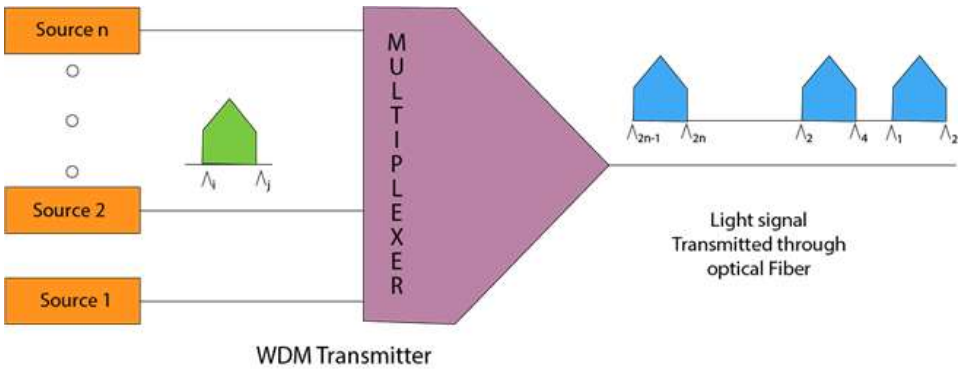
Disadvantages of FDM:

- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

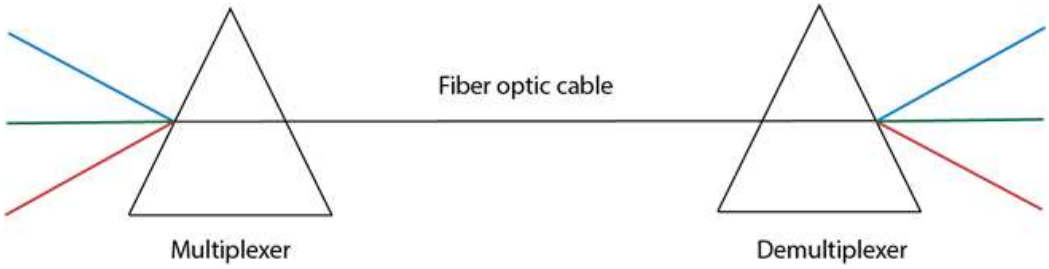
Applications of FDM:

- FDM is commonly used in TV networks.
- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fiber optic cable.
- WDM is used on fiber optics to increase the capacity of a single fiber.
- It is used to utilize the high data rate capability of fiber optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, de-multiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and De-multiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fiber optical cable.
- Prism also performs a reverse operation, i.e., de-multiplexing the signal.



Time Division Multiplexing

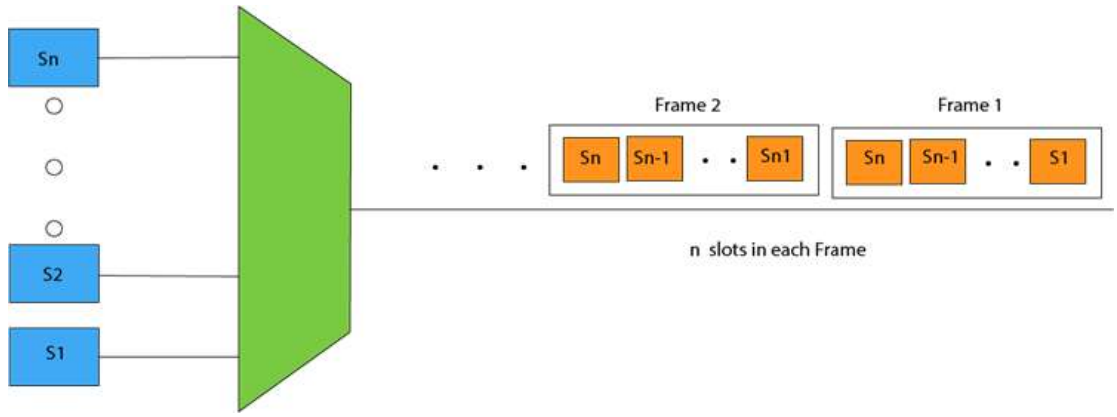
- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In Time Division Multiplexing technique, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

There are two types of TDM:

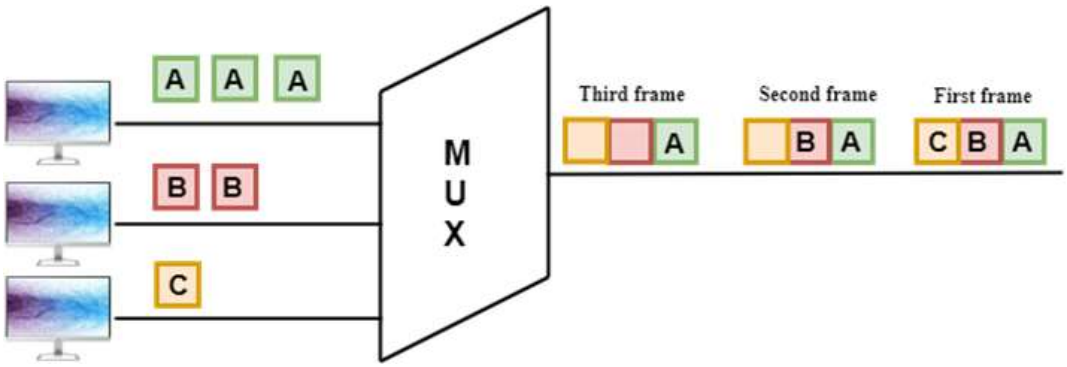
- Synchronous TDM
- Asynchronous TDM

Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.



Concept of Synchronous TDM



In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Disadvantages of Synchronous TDM:

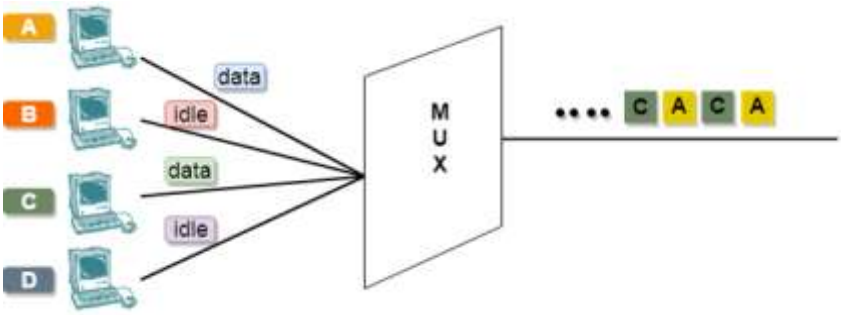
- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.
- The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

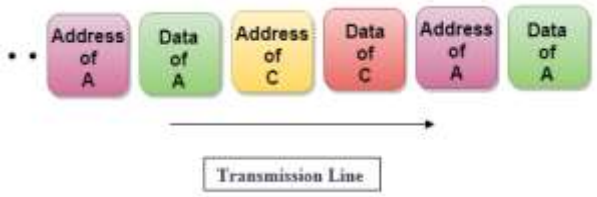
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (m<n).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept of Asynchronous TDM



In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Frame of above diagram can be represented as:



The above figure shows that the data part contains the address to determine the source of the data.

1.2 Transmission media

Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

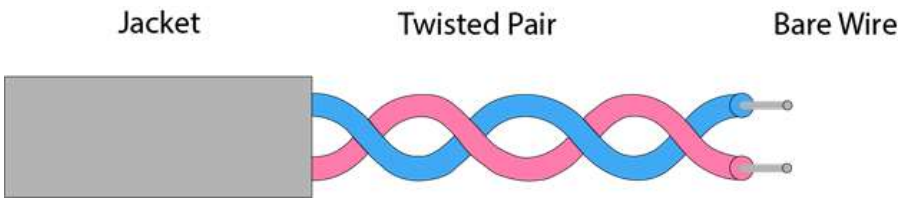
Types of Guided media:

Twisted pair:

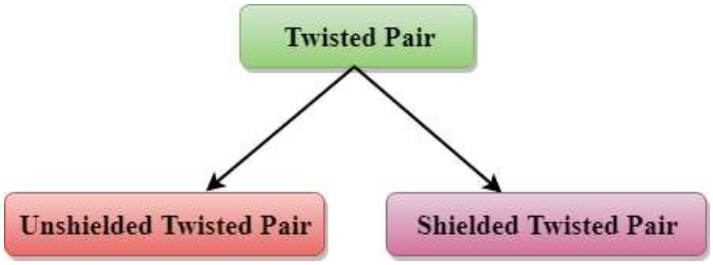
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- Category 1: Category 1 is used for telephone lines that have low-speed data.
- Category 2: It can support upto 4Mbps.
- Category 3: It can support upto 16Mbps.
- Category 4: It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- Category 5: It can support upto 200Mbps.

Advantages of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics of Shielded Twisted Pair:

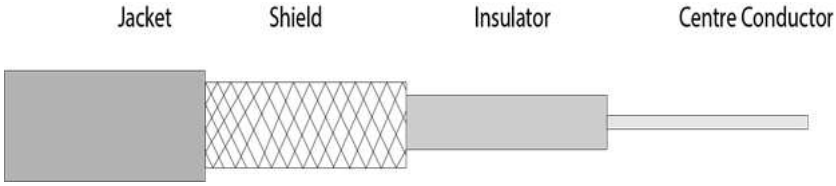
- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI(Electromagnetic interference).



Coaxial cable is of two types:

1. Baseband transmission: It is defined as the process of transmitting a single signal at high speed.
2. Broadband transmission: It is defined as the process of transmitting multiple signals simultaneously.

Advantages of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

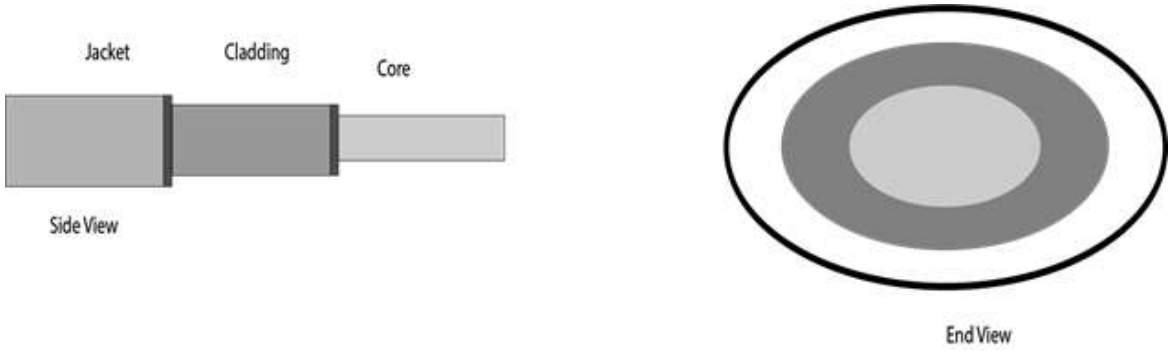
Disadvantages of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

Fiber Optic

- Fiber optic cable is a cable that uses electrical signals for communication.
- Fiber optic is a cable that holds the optical fibers coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibers from heat, cold, electromagnetic interference from other types of wiring.
- Fiber optics provide faster data transmission than copper wires.

Diagrammatic representation of fiber optic cable:



Basic elements of Fiber optic cable:

- Core: The optical fiber consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fiber. The more the area of the core, the more light will be transmitted into the fiber.
- Cladding: The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fiber.
- Jacket: The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fiber strength, absorb shock and extra fiber protection.

Following are the advantages of fiber optic cable over copper:

- Greater Bandwidth: The fiber optic cable provides more bandwidth as compared copper. Therefore, the fiber optic carries more data as compared to copper cable.
- Faster speed: Fiber optic cable carries the data in the form of light. This allows the fiber optic cable to carry the signals at a higher speed.
- Longer distances: The fiber optic cable carries the data at a longer distance as compared to copper cable.
- Better reliability: The fiber optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- Thinner and Sturdier: Fiber optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

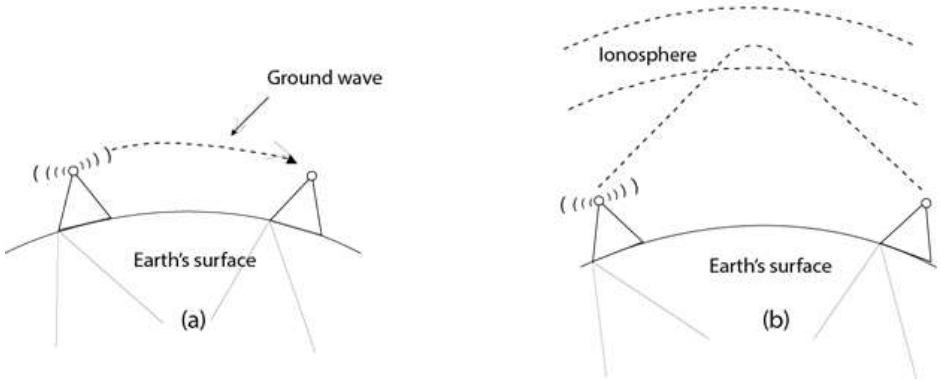
Un-Guided Transmission

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore, it is also known as wireless transmission.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is FM radio.



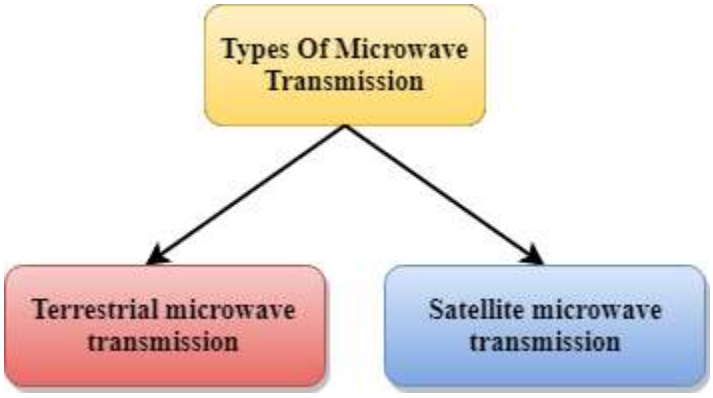
Applications of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves



Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focused.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- Frequency range: The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- Bandwidth: It supports the bandwidth from 1 to 10 Mbps.
- Short distance: It is inexpensive for short distance.
- Long distance: It is expensive as it requires a higher tower for a longer distance.
- Attenuation: Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- Eavesdropping: An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- Out of phase signal: A signal can be moved out of phase by using microwave transmission.
- Susceptible to weather condition: A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- Bandwidth limited: Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fiber optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

1.3 Types of Networks:

LANs (Local Area Networks)

A network is any collection of independent computers that communicate with one another over a shared network medium. LANs are networks usually confined to a geographic area, such as a single building or a college campus. LANs can be small, linking as few as three computers, but often link hundreds of computers used by thousands of people. The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business and educational organizations.

WANs (Wide Area Networks)

Wide area networking combines multiple LANs that are geographically separate. This is accomplished by connecting the different LANs using services such as dedicated leased phone lines, dial-up phone lines (both synchronous and asynchronous), satellite links, and data packet carrier services. Wide area networking can be as simple as a modem and remote access server for employees to dial into, or it can be as complex as hundreds of branch offices globally linked using special routing protocols and filters to minimize the expense of sending data sent over vast distances.

Internet

The Internet is a system of linked networks that are worldwide in scope and facilitate data communication services such as remote login, file transfer, electronic mail, the World Wide Web and newsgroups.

With the meteoric rise in demand for connectivity, the Internet has become a communications highway for millions of users. The Internet was initially restricted to military and academic institutions, but now it is a full-fledged conduit for any and all forms of information and commerce. Internet websites now provide personal, educational, political and economic resources to every corner of the planet.

Intranet

With the advancements made in browser-based software for the Internet, many private organizations are implementing intranets. An intranet is a private network utilizing Internet-type tools, but available only within that organization. For large organizations, an intranet provides an easy access mode to corporate information for employees.

MANs (Metropolitan area Networks)

The refers to a network of computers with in a City.

VPN (Virtual Private Network)

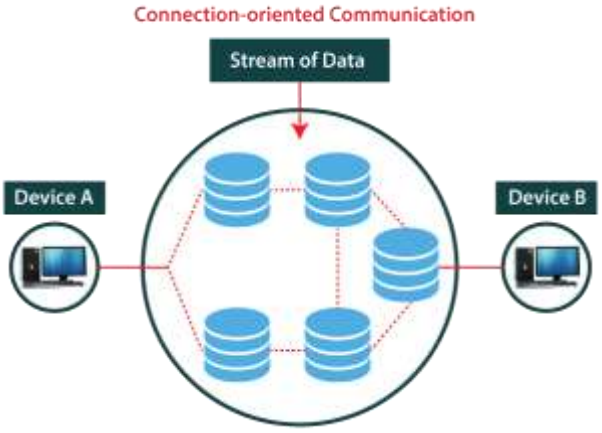
VPN uses a technique known as tunneling to transfer data securely on the Internet to a remote access server on your workplace network. Using a VPN helps you save money by using the public Internet instead of making long–distance phone calls to connect securely with your private network. There are two ways to create a VPN connection, by dialing an Internet service provider (ISP), or connecting directly to Internet.

1.4 Connection Oriented N/W Vs Connectionless N/W

Data communication is a telecommunication network to send and receive data between two or more computers over the same or different network. There are two ways to establish a connection before sending data from one device to another, that are Connection-Oriented and Connectionless Service. Connection-oriented service involves the creation and termination of the connection for sending the data between two or more devices. In contrast, connectionless service does not require establishing any connection and termination process for transferring the data over a network.

Connection-Oriented Service

A connection-oriented service is a network service that was designed and developed after the telephone system. A connection-oriented service is used to create an end to end connection between the sender and the receiver before transmitting the data over the same or different networks. In connection-oriented service, packets are transmitted to the receiver in the same order the sender has sent them. It uses a handshake method that creates a connection between the user and sender for transmitting the data over the network. Hence it is also known as a reliable network service.



Suppose, a sender wants to send data to the receiver. Then, first, the sender sends a request packet to a receiver in the form of an SYN packet. After that, the receiver responds to the sender's request with an (SYN-ACK) signal/packets. That represents the confirmation is received by the receiver to start the communication between the sender and the receiver. Now a sender can send the message or data to the receiver.

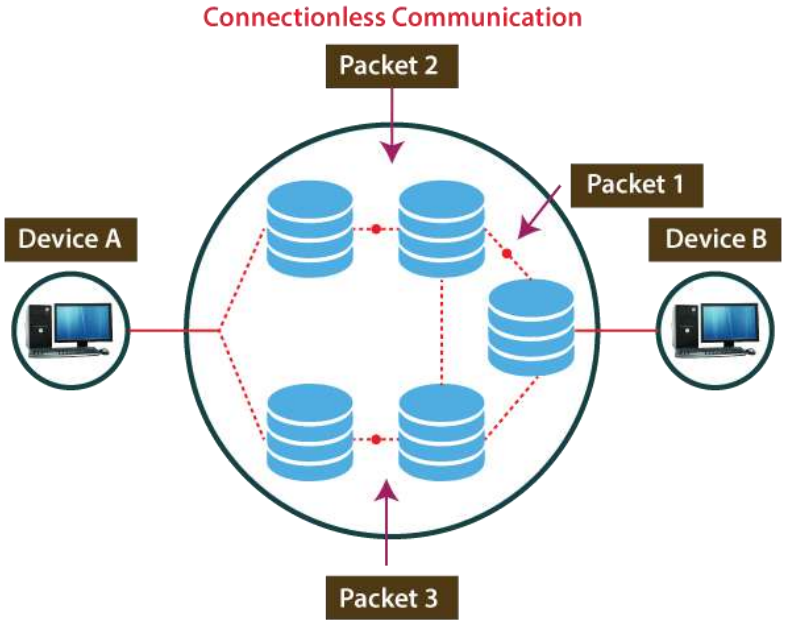
Similarly, a receiver can respond or send the data to the sender in the form of packets. After successfully exchanging or transmitting data, a sender can terminate the connection by sending a signal to the receiver. In this way, we can say that it is a reliable network service.

What is a TCP?

TCP (Transmission Control Protocol) is a connection-oriented protocol that allows communication between two or more computer devices by establishing connections in the same or different networks. It is the most important protocol that uses internet protocol to transfer the data from one end to another. Hence, it is sometimes referred to as TCP/IP. It ensures that the connection is established and maintained until the data packet is transferring between the sender and receiver is complete.

Connectionless Service

A connection is similar to a postal system, in which each letter takes along different route paths from the source to the destination address. Connectionless service is used in the network system to transfer data from one end to another end without creating any connection. So it does not require establishing a connection before sending the data from the sender to the receiver. It is not a reliable network service because it does not guarantee the transfer of data packets to the receiver, and data packets can be received in any order to the receiver. Therefore we can say that the data packet does not follow a defined path. In connectionless service, the transmitted data packet is not received by the receiver due to network congestion, and the data may be lost.



For example, a sender can directly send any data to the receiver without establishing any connection because it is a connectionless service. Data sent by the sender will be in the packet or data streams containing the receiver's address. In connectionless service, the data can be travelled and received in any order. However, it does not guarantee to transfer of the packets to the right destination.

What is UDP?

The UDP (User Datagram Protocol) is a connectionless protocol that allows communication between two or more devices without establishing any connection. In this protocol, a sender sends the data packets to the receiver that holds the destination address. A UDP does not ensure to deliver the data packets to the correct destination, and it does not generate any acknowledgment about the sender's data. Similarly, it does not acknowledge the receiver about the data. Hence, it is an unreliable protocol.

Connection-Oriented Vs Connectionless Service

S. No	Comparison Parameter	Connection-oriented Service	Connection Less Service
1.	Related System	It is designed and developed based on the telephone system.	It is service based on the postal system.
2.	Definition	It is used to create an end to end connection between the senders to the receiver before transmitting the data over the same or different network.	It is used to transfer the data packets between senders to the receiver without creating any connection.
3.	Virtual path	It creates a virtual path between the sender and the receiver.	It does not create any virtual connection or path between the sender and the receiver.
4.	Authentication	It requires authentication before transmitting the data packets to the receiver.	It does not require authentication before transferring data packets.
5.	Data Packets Path	All data packets are received in the same order as those sent by the sender.	Not all data packets are received in the same order as those sent by the sender.

6.	Bandwidth Requirement	It requires a higher bandwidth to transfer the data packets.	It requires low bandwidth to transfer the data packets.
7.	Data Reliability	It is a more reliable connection service because it guarantees data packets transfer from one end to the other end with a connection.	It is not a reliable connection service because it does not guarantee the transfer of data packets from one end to another for establishing a connection.
8.	Congestion	There is no congestion as it provides an end-to-end connection between sender and receiver during transmission of data.	There may be congestion due to not providing an end-to-end connection between the source and receiver to transmit of data packets.
9.	Examples	Transmission Control Protocol (TCP) is an example of a connection-oriented service.	User Datagram Protocol (UDP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP) are examples of connectionless service.

1.5 ETHERNET-

(ETHERNET STANDARDS, ZIGBEE, WIFI, ACCESS TECHNIQUE - CSMA-CD, NEGOTIATION TECHNIQUE OVERVIEW)

Ethernet:

Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

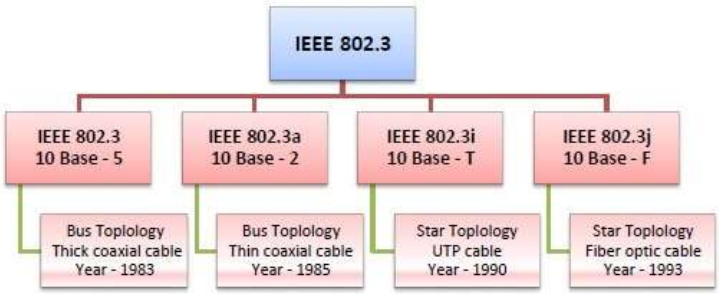
Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used. Most varieties of classic Ethernet have become obsolete in present communication scenario.

A switched Ethernet uses switches to connect to the stations in the LAN. It replaces the repeaters used in classic Ethernet and allows full bandwidth utilization.

IEEE 802.3 Popular Versions

There are a number of versions of IEEE 802.3 protocol. The most popular ones are -

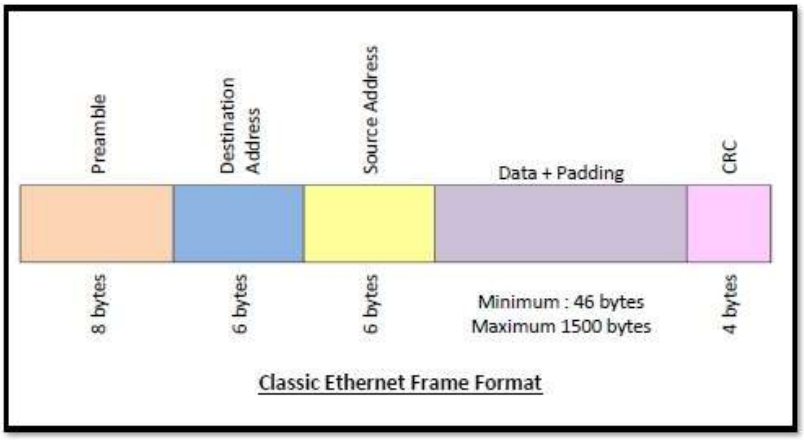
- IEEE 802.3: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.
- IEEE 802.3a: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- IEEE 802.3i: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.
- IEEE 802.3i: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.

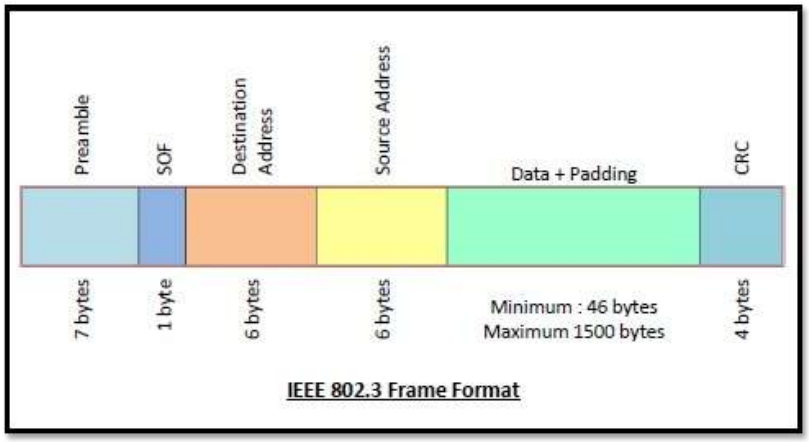


Frame Format of Classic Ethernet and IEEE 802.3

The main fields of a frame of classic Ethernet are -

- Preamble: It is the starting field that provides alert and timing pulse for transmission. In case of classic Ethernet it is an 8 byte field and in case of IEEE 802.3 it is of 7 bytes.
- Start of Frame Delimiter: It is a 1 byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- Destination Address: It is a 6 byte field containing physical address of destination stations.
- Source Address: It is a 6 byte field containing the physical address of the sending station.
- Length: It a 7 bytes field that stores the number of bytes in the data field.
- Data: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- Padding: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- CRC: CRC stands for cyclic redundancy check. It contains the error detection information.





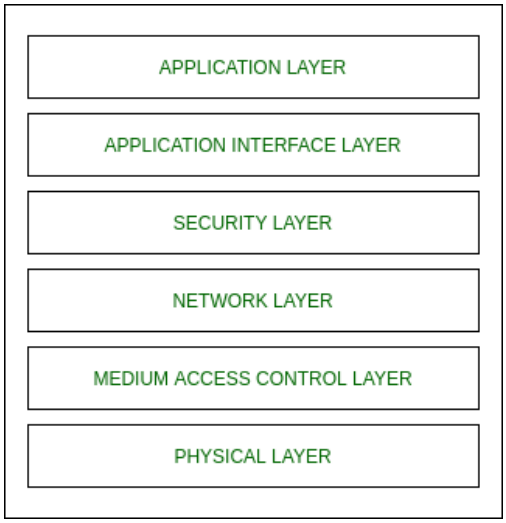
Zigbee:

ZigBee is a Personal Area Network task group with low rate task group 4. It is a technology of home networking. ZigBee is a technological standard created for controlling and sensor the network. As we know that ZigBee is Personal Area network of task group 4 so it is based on IEEE 802.14.4 and it is created by Zigbee Alliance.

Architecture of Zigbee:

Zigbee architecture is a combination of 6 layers.

1. Application Layer
2. Application Interface Layer
3. Security Layer
4. Network Layer
5. Medium Access Control Layer
6. Physical Layer



- The Application layer is present at the user level.
- The Application Interface Layer, Security Layer and Network Layer are the Zigbee Aliance and they are used to sore data and they uses stack.
- Medium Access control and the Physical layer are the IEEE 802.15.4 and they are hardware which are silicon means they accept only 0 and 1.

Types of ZigBee Devices:

1. Zigbee Coordinator Device – It communicate with routers. This device is used for connecting the devices.
2. Zigbee Router – It used for passing the data between devices.
3. Zigbee End Device – It is the device which is going to be controlled

Wi fi:

WiFi stands for Wireless Fidelity. WiFiIt is based on the IEEE 802.11 family of standards and is primarily a local area networking (LAN) technology designed to provide in-building broadband coverage.

Current WiFi systems support a peak physical-layer data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 feet.

WiFi has become the *de facto* standard for *last mile* broadband connectivity in homes, offices, and public hotspot locations. Systems can typically provide a coverage range of only about 1,000 feet from the access point.

WiFi offers remarkably higher peak data rates than do 3G systems, primarily since it operates over a larger 20 MHz bandwidth, but WiFiWiFi systems are not designed to support high-speed mobility.

One significant advantage of WiFi over WiMAX and 3G is its wide availability of terminal devices. A vast majority of laptops shipped today have a built-in WiFi interface. WiFi interfaces are now also

being built into a variety of devices, including personal data assistants (PDAs), cordless phones, cellular phones, cameras, and media players.

WiFi is Half Duplex

All WiFi networks are contention-based TDD systems, where the access point and the mobile stations all vie for use of the same channel. Because of the shared media operation, all WiFi networks are half duplex.

There are equipment vendors who market WiFi mesh configurations, but those implementations incorporate technologies that are not defined in the standards.

Channel Bandwidth

The WiFi standards define a fixed channel bandwidth of 25 MHz for 802.11b and 20 MHz for either 802.11a or g networks.

Wi-Fi - Working Concepts

Radio Signals

Radio Signals are the keys, which make WiFi networking possible. These radio signals transmitted from WiFi antennas are picked up by WiFi receivers, such as computers and cell phones that are equipped with WiFi cards. Whenever, a computer receives any of the signals within the range of a WiFi network, which is usually 300 — 500 feet for antennas, the WiFi card reads the signals and thus creates an internet connection between the user and the network without the use of a cord.

Access points, consisting of antennas and routers, are the main source that transmit and receive radio waves. Antennas work stronger and have a longer radio transmission with a radius of 300-500 feet, which are used in public areas while the weaker yet effective router is more suitable for homes with a radio transmission of 100-150 feet.

WiFi Cards

You can think of WiFi cards as being invisible cords that connect your computer to the antenna for a direct connection to the internet.

WiFi cards can be external or internal. If a WiFi card is not installed in your computer, then you may purchase a USB antenna attachment and have it externally connect to your USB port, or have an antenna-equipped expansion card installed directly to the computer (as shown in the figure given above). For laptops, this card will be a PCMCIA card which you insert to the PCMCIA slot on the laptop.

WiFi Hotspots

A WiFi hotspot is created by installing an access point to an internet connection. The access point transmits a wireless signal over a short distance. It typically covers around 300 feet. When a WiFi

enabled device such as a Pocket PC encounters a hotspot, the device can then connect to that network wirelessly.

Most hotspots are located in places that are readily accessible to the public such as airports, coffee shops, hotels, book stores, and campus environments. 802.11b is the most common specification for hotspots worldwide. The 802.11g standard is backwards compatible with .11b but .11a uses a different frequency range and requires separate hardware such as an a, a/g, or a/b/g adapter. The largest public WiFi networks are provided by private internet service providers (ISPs); they charge a fee to the users who want to access the internet.

Hotspots are increasingly developing around the world. In fact, T-Mobile USA controls more than 4,100 hotspots located in public locations such as Starbucks, Borders, Kinko's, and the airline clubs of Delta, United, and US Airways. Even select McDonald's restaurants now feature WiFi hotspot access.

Any notebook computer with integrated wireless, a wireless adapter attached to the motherboard by the manufacturer, or a wireless adapter such as a PCMCIA card can access a wireless network. Furthermore, all Pocket PCs or Palm units with Compact Flash, SD I/O support, or built-in WiFi, can access hotspots.

Some Hotspots require WEP key to connect, which is considered as private and secure. As for open connections, anyone with a WiFi card can have access to that hotspot. So in order to have internet access under WEP, the user must input the WEP key code.

1.6 ACCESS TECHNIQUE – CSMA/CD:

What is Carrier Sense Multiple Access (CSMA)?

Carrier Sense Multiple Access (CSMA) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and transmits if the channel is not busy. Using CMSA protocols, more than one users or nodes send and receive data through a shared medium that may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.

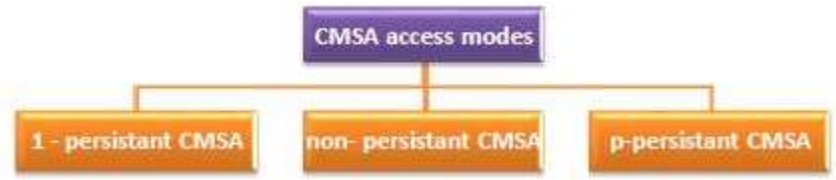
Working Principle

When a station has frames to transmit, it attempts to detect presence of the carrier signal from the other nodes connected to the shared channel. If a carrier signal is detected, it implies that a transmission is in progress. The station waits till the ongoing transmission executes to completion, and then initiates its own transmission. Generally, transmissions by the node are received by all other nodes connected to the channel.

Since, the nodes detect for a transmission before sending their own frames, collision of frames is reduced. However, if two nodes detect an idle channel at the same time, they may simultaneously initiate transmission. This would cause the frames to garble resulting in a collision.

CMSA Access Modes

The versions of CMSA access modes are−



Variations of CMSA protocol

There may be further additions to the basic CMSA protocols. This results is the various protocols as follows−

Multiple Access with Collision Avoidance (MACA)

Multiple Access with Collision Avoidance (MACA) is a medium access control (MAC) layer protocol used in wireless networks, with a view to solve the hidden terminal problem. It also provides solution to the exposed terminal problem. The MAC layer protocol IEEE 802.11 RTS/CTS has been adopted from MACA.

Working Principle

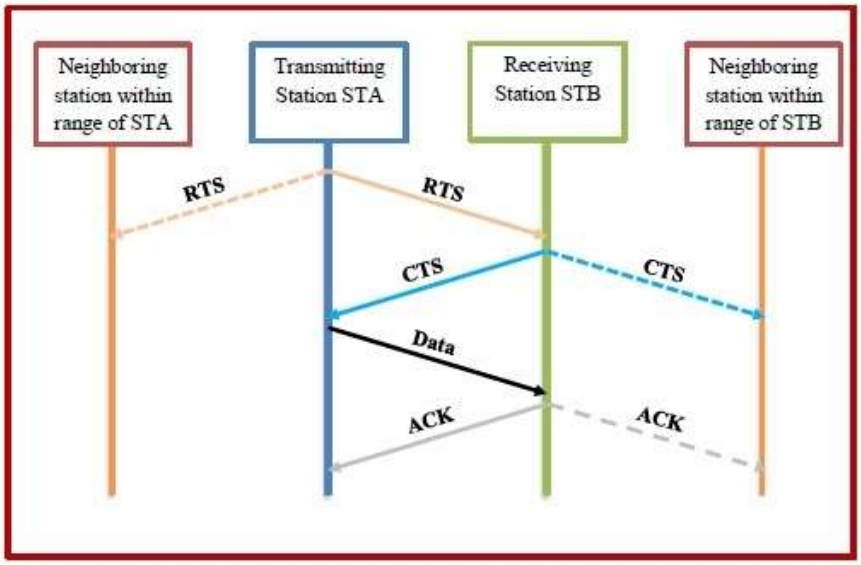
The MACA protocol works with the condition that the stations are synchronized and frame sizes and data speed are the same. It involves transmission of two frames called RTS and CTS prior to data transmission. RTS stands for Request to Send and CTS stands for Clear to Send.

Let us consider that a transmitting station STA has data frame to send to a receiving station STB. The operation works as follows:

- Station STA sends a RTS frame to the receiving station.

- On receiving the RTS, station STB replies by sending a CTS frame.
- On receipt of CTS frame, station STA begins transmitting its data frame.
- After successful receipt of the data frame, station STB sends an ACK frame (acknowledgement frame).

The sequence is illustrated as follows:



Any station than can hear RTS is close to the transmitting station and remains silent long enough for the CTS, or waits for a certain time period. If the RTS is not followed by a CTS, the maximum waiting time is the RTS propagation time.

Any station that can hear the CTS is close to the receiving station and remains silent during the data transmission. It attempts for transmission after hearing the ACK.

MACA is a non-persistent slotted protocol. This implies that if the medium is detected as busy, a station waits for a random time period after the beginning of a time slot and then it sends an RTS. This assures fair access to the medium.

CSMA with Collision Avoidance (CSMA/CA)

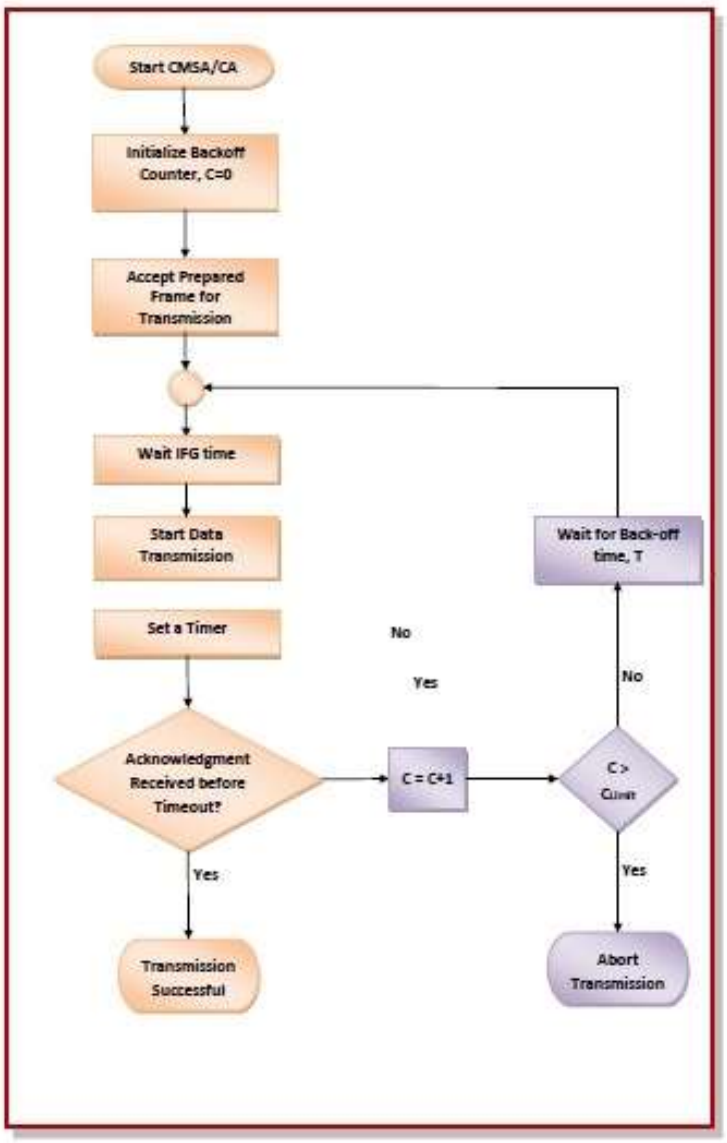
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. In contrast to CSMA/CD (Carrier Sense Multiple Access/Collision Detection) that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their occurrence.

Algorithm

The algorithm of CSMA/CA is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
- After sending the frame, it sets a timer.
- The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
- Otherwise, it waits for a back-off time period and restarts the algorithm.

The following flowchart summarizes the algorithms:



Advantages of CMSA/CD

- CMSA/CA prevents collision.
- Due to acknowledgements, data is not lost unnecessarily.

- It avoids wasteful transmission.
- It is very much suited for wireless transmissions.

Disadvantages of CSMA/CD

- The algorithm calls for long waiting times.
- It has high power consumption.

CSMA with Collision Detection (CSMA/CD)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free. The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

Algorithms

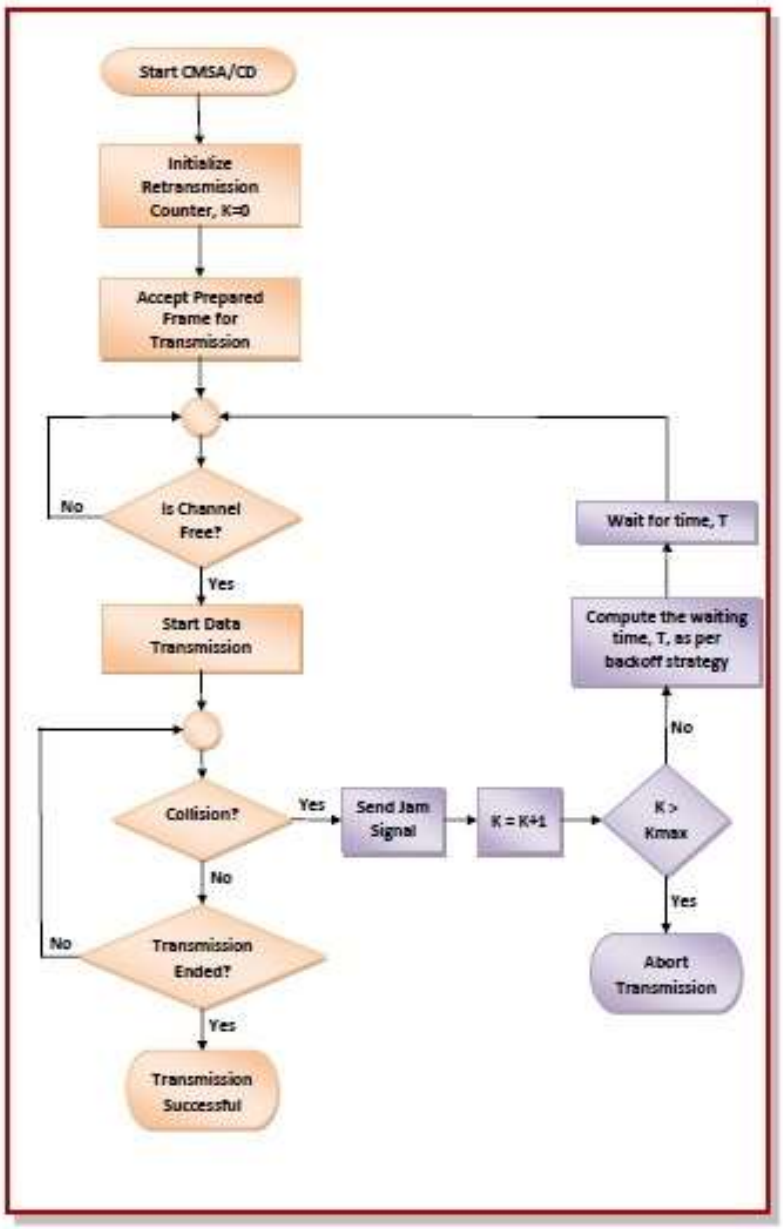
The algorithm of CSMA/CD is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
- If a collision is detected, the station starts the collision resolution algorithm.
- The station resets the retransmission counters and completes frame transmission.

The algorithm of Collision Resolution is:

- The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.
- The station increments the retransmission counter.
- If the maximum number of retransmission attempts is reached, then the station aborts transmission.
- Otherwise, the station waits for a backoff period which is generally a function of the number of collisions and restart main algorithm.

The following flowchart summarizes the algorithms:



- Though this algorithm detects collisions, it does not reduce the number of collisions.
- It is not appropriate for large networks performance degrades exponentially when more stations are added.
- The following are some of the important differences between CSMA/CA and CSMA/CD.

Sr. No.	Key	CSMA/CA	CSMA/CD
1	Effectiveness	CSMA/CA is effective before a collision.	CSMA/CD is effective after a collision.
2	Network Type	CSMA/CA is generally used in wireless networks.	CSMA/CD is generally used in wired networks.
3	Recovery Time	CSMA/CA minimizes the risk of collision.	CSMA/CD reduces recovery time.
4	Conflict Management	CSMA/CA initially transmits the intent to send the data, once an acknowledgment is received, the sender sends the data.	CSMA/CD resends the data frame in case a conflict occurs during transmission.
5	IEEE Standards	CSMA/CA is part of the IEEE 802.11 standard.	CSMA/CD is part of the IEEE 802.3 standard.
6	Efficiency	CSMA/CA is similar in efficiency as CSMA.	CSMA/CD is more efficient than CSMA.

1.7 Wireless Network

Computer networks that are not connected by cables are called wireless networks. They generally use radio waves for communication between the network nodes. They allow devices to be connected to the network while roaming around within the network coverage.

Types of Wireless Networks

- Wireless LANs − Connects two or more network devices using wireless distribution techniques.
- Wireless MANs − Connects two or more wireless LANs spreading over a metropolitan area.
- Wireless WANs − Connects large areas comprising LANs, MANs and personal networks.

Advantages of Wireless Networks

- It provides clutter-free desks due to the absence of wires and cables.
- It increases the mobility of network devices connected to the system since the devices need not be connected to each other.
- Accessing network devices from any location within the network coverage or Wi-Fi hotspot becomes convenient since laying out cables is not needed.
- Installation and setup of wireless networks are easier.
- New devices can be easily connected to the existing setup since they needn't be wired to the present equipment. Also, the number of equipment that can be added or removed to the system can vary considerably since they are not limited by the cable capacity. This makes wireless networks very scalable.
- Wireless networks require very limited or no wires. Thus, it reduces the equipment and setup costs.

Examples of wireless networks

- Mobile phone networks
- Wireless sensor networks
- Satellite communication networks
- Terrestrial microwave networks

1.8 Unified Communication –VOIP

Voice Over IP (VoIP)

If you've been looking at your business communication strategy lately, then you've probably already heard of "VoIP."

VoIP simply stands for "Voice over Internet Protocol." You might have seen it referred to as "Internet Telephony" or "IP Telephony" instead, as the defining feature of this calling method, is that it directs data over the internet.

VoIP is a way of making calls incredibly cost-effectively, and though it's still a relatively new technology in the comms world, it's achieved world-wide acceptance very rapidly. In fact, many businesses have replaced their "POTs" (Plain Old Telephones) with VoIP.

How Does VoIP Work?

Anyone with a reliable internet connection can access VoIP. Essentially, the system works by delivering a phone service through your internet connection, instead of using traditional wired connections from a local phone company. VoIP translates traditional analogue phone signals into digital signals that can move over the internet. You can access VoIP in several ways. For instance:

- **Using an ATA:** An analogue terminal adapter turns an ordinary phone into a VoIP phone
- **Using an IP Phone:** An IP Phone connects directly to the internet, instead of going through a landline service
- **Using a direct connection:** A VoIP service provider can directly connect you to another VoIP user

The Benefits of VoIP

The growth of the VoIP strategy today is like the internet revolution we saw back in the 90s. VoIP not only gives businesses additional features from their phone connections but also delivers serious cost savings too. The main benefits of VoIP include:

- **Cost savings:** Companies can save you on calls by making connections over the internet. Because VoIP and video works by sending and receiving digital packets of data over the web, you can enjoy cheaper calls to anywhere in the world. Additionally, there are none of the up-front costs associated with a fixed-line service
- **Better flexibility:** Unlike standard PSTN or ISDN lines, VoIP offers significantly greater flexibility to businesses. You can increase or decrease the number of channels or users using your services virtually instantly. What's more, you only pay for the services you use
- **Increased mobility:** Because you don't need to be tied to a specific landline to use VoIP, this opens the door for remote working and global employees. VoIP also provides a fitting solution for the huge percentage of deskless (on the field) employees in the community
- **Faster deployment:** VoIP is easy-to-use, quick to install and cheap. This means that companies of any shape or size can begin to reap the benefits without any up-front investment on line

installations or hardware. Many VoIP phones are plug-and-play systems that cause minimal disruption to daily operations

- **Rich feature sets:** Finally, VoIP works in collaboration with the various applications available on your computer or IP phone. This means that you can access more than just voice connections. VoIP telephony often comes with access to video calling, voicemail, click-to-call services on websites, recording services, messaging and presence information – among other things

Voice over IP is an efficient, cost-effective, and highly immersive way for today's companies to make the most of the power of the cloud and a solid internet connection

VoIP is exactly what the name indicates—sending voice (and video) over an IP-based network. This is completely different than the circuit-switched public telephone network that I grew up with. Circuit switching allocates resources to each individual call. Traditional telephony services are usually described by terms such as Signaling System 7, T carriers, plain old telephone service (POTS), the public switched telephone network (PSTN), tip and ring connections, dial up, local loops, circuit switching, and anything coming from the International Telecommunications Union. All of these refer to a system that has been used for decades to deliver reliable, low-bandwidth telephone calls with a high level of quality. A simple traditional topology might look like the one shown in Figure 1-1. This traditional operation will be covered in greater detail in Chapter 2.

IP networks are packet switched, and each packet sent is semi-autonomous, has its own IP header, and is forwarded separately by routers. Chapters 3 through 7 will take us through the technical details regarding the operation of a VoIP system, but it turns out that understanding VoIP and its impetus is often a matter of understanding the effects of VoIP, which can be significant.

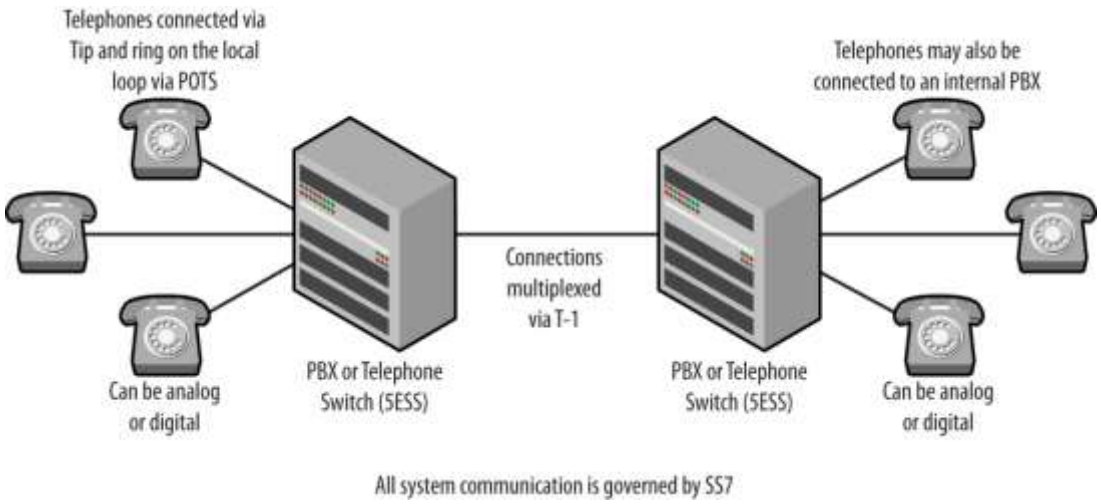


Figure: Simple traditional telephony topology

- Native VoIP systems do away with much of what is considered traditional telephony. Well, almost. A system like the one pictured in Figure 1-1 involves a lot of control signaling to accomplish the various tasks required. For example, telephone numbers are dialed, and those numbers have meaning. Sounds or tones such as busy and off-hook are also messages of a sort. Database lookups for 411 or 800 numbers require additional messages as do services like caller-

id, advanced features, and call routing. These signals are sent between the devices like the private branch exchange (PBX) before any human communication can occur.

- VoIP takes all of these signaling messages and places them inside IP packets. While traditional telephones can be used in conjunction with a VoIP system, it is often the case that they are not. After a pilot project, companies implementing a VoIP system commonly desire to roll out a single set of equipment in order to simplify support and maintenance. This also reduces cost. After this occurs, endpoints are not referred to as telephones anymore, just VoIP or Ethernet phones. The PBX name is retained, although it is now called an IP PBX, which really means it is a server running on a computer. Redrawing the topology, we might see something like the one shown in Figure 1-2. It is also worth mentioning that since the Internet Protocol can and does run over almost every single type of low-layer communication architecture, Voice over IP can as well.

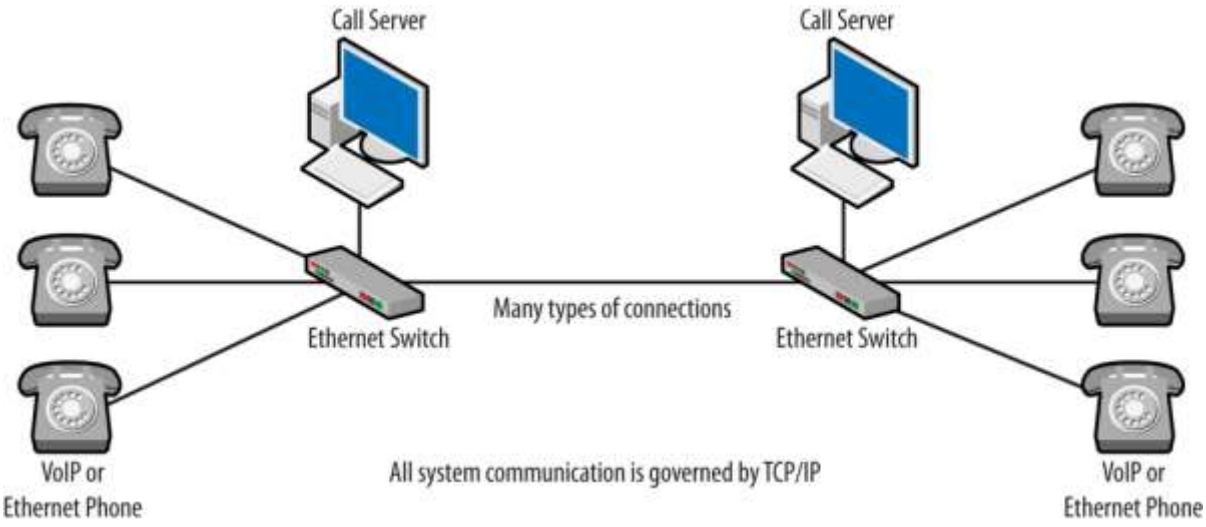


Figure: Basic VoIP architecture

- And this indicates just how big an understatement a simple definition of VoIP can be. The languages spoken by the two systems are completely different, with traditional systems using Signaling System 7 (SS7) and VoIP networks using Transmission Control Protocol/Internet Protocol or TCP/IP. This also explains why the Digium folks call VoIP disruptive. Everything about this system is different.
- To finish this section, let's take a quick look at the skill sets required to run the two systems. Figure 1-3 shows a side-by-side comparison of the topologies and a short list of the basic skills required to work on each. At first glance, the topologies do not seem all that different, especially as they are drawn. But, the equipment used in each, while serving the same functions, performs these functions differently and in fact operates using a completely different set of protocols.

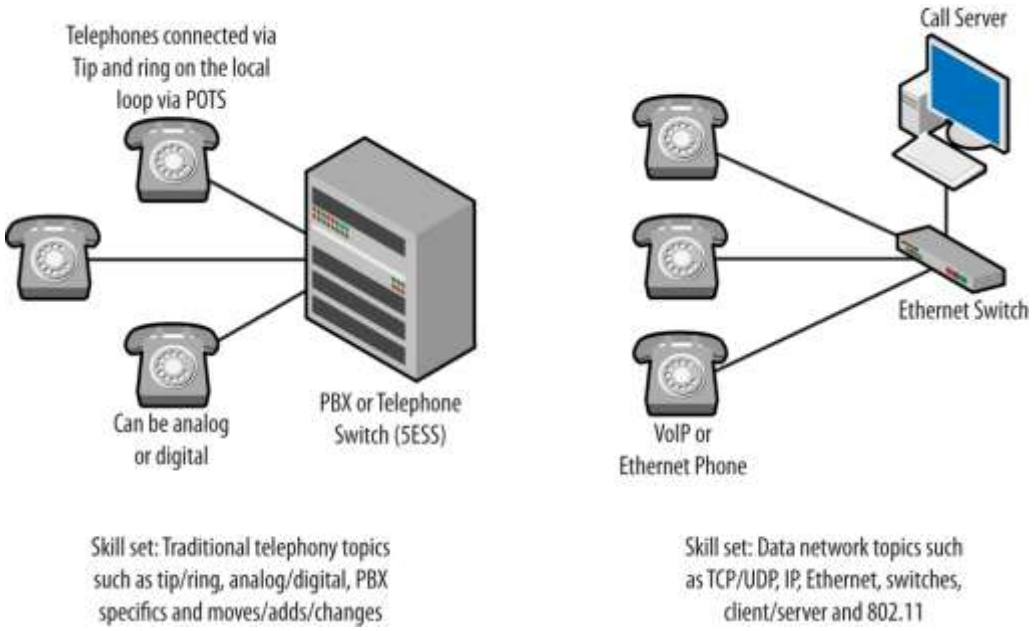


Figure: Skills needed for traditional telephony versus VoIP

- A Venn diagram comparing the skills for each topology would find very little intersection. Following this line of thought to the hiring or training activities in an organization, we have to conclude that there would be a different demand for someone knowledgeable in traditional telephony topics compared to someone possessing a data network background. When faced with the need to support a VoIP infrastructure, what would the two individuals have to learn? If we consider the typical deployment on the consumer side, the traditional telephony person may possess knowledge about dial plans, call routing, T-1s, and features but will not understand the operation of an IP-based wired/wireless network.
- A person possessing a data network background (Ethernet, 802.11, IP, TCP, UDP) would find that VoIP has migrated to the area of their expertise. They would be missing knowledge about the operation of a telephony system. However, many of the telephony skills would not be necessary. For example, moves or adds and changes are simply a matter of moving the phone and obtaining a new IP address. The debate over which individual would have an easier time transitioning has points on both sides, but there is no question that each side is missing something. This is somewhat mitigated by the proliferation of IP-based voice and location services, such as those offered by Google. It seems that we are all becoming a bit VoIP-ish whether we know it or not. Disruptive indeed.

Real-time Versus Non real-time Data

When you are downloading a file, delays are inconvenient and sometimes vexing, but they do not damage or prevent the transfer. Similarly, when visiting a website, if the page loads slowly, we are willing to give it a few seconds before navigating away. If some of the images from the page appear, we may be willing to wait even longer. These examples constitute transfers involving non real-time data. From a protocol standpoint, the transmission control protocol (TCP) is used to manage the connection, and all packets (or at least the bytes) are controlled via the associated sequence numbers. Lost or delayed data is retransmitted in order to ensure that the receiver has everything.