Computer Network Unit 1 part 1

B.tech (Dr. A.P.J. Abdul Kalam Technical University)

COMPUTER NETWORK

Definition of Computer Network

A network is a set of devices often referred to as nodes connected by media links.

A node can be a computer, or a printer or a mobile phone or any other device capable of sending or receiving data generated by other nodes on the network. Also, the links connecting the devices are called communication channels.

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term telecommunication, which includes telephony, telegraphy, and television means communication at a distance (tele is a Greek word for **far**).

The word data refers to facts, concepts, and instructions presented in whatever form is agreed upon by parties creating and using data.

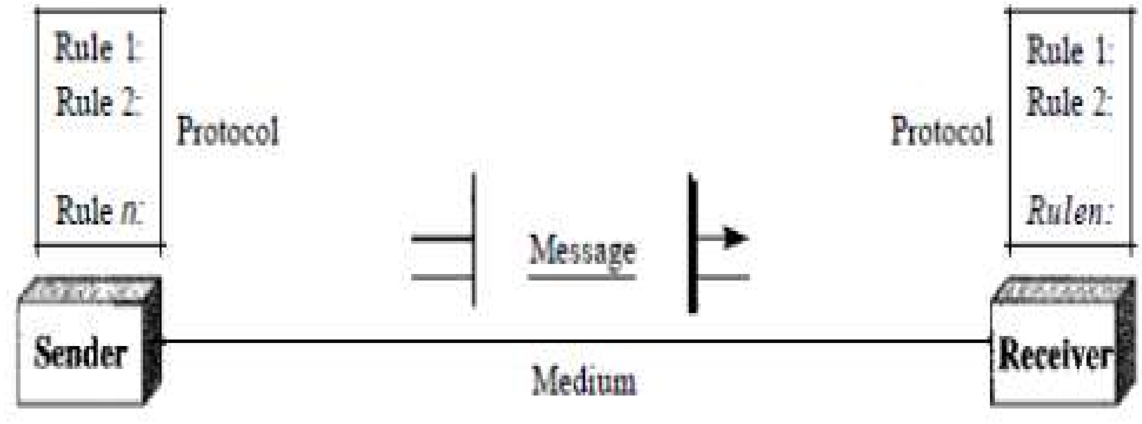
Data is represented by bits (0s and 1s)

Data communication is the exchange of data between two devices via some form of transmission (such as a wire cable).

Effectiveness of data Communication depends on four fundamental characteristics

1. **Delivery** – The system must deliver data to the correct destination. Data must be received by the intended devices or user and only by that device or user.
2. **Accuracy** – The system must deliver data accurately.
3. **Timeliness** – The system must deliver data in a timely manner because data delivered late is useless only in a real-time transmission.
4. **Jitter** – refers to small intermittent delays during data transfers. It can be caused by a number of factors including network congestion, collisions, and signal interference. So you have to remove jitter.

Components: A data communications system has five components.



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.

Network Criteria - A network must be able to meet a certain number of criteria. The most important of these are **performance, reliability, and security**.

Performance: Performance can be measured in many ways, including transit time and response time. **Transit time** is the amount of time required for a message to travel from one device to another. **Response time** is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: **throughput** and **delay**. We often need more throughputs and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability: In addition to the accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

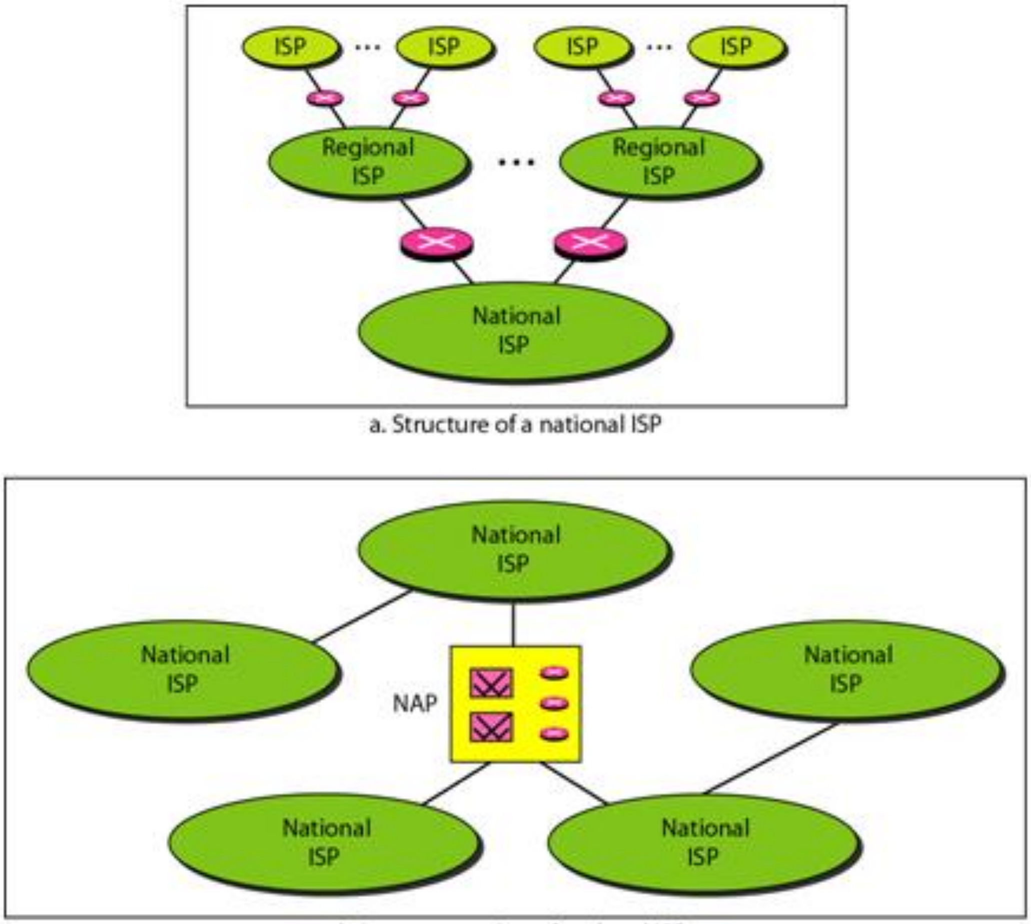
Applications

1. Marketing and sales
2. Financial Services
3. Electronic Messaging
4. Information Services
5. Electronic Data Interchange (EDI) – EDI allows business information (including documents such as purchase order and invoices) to be transferred without using paper.
6. Teleconferencing
7. Cellular phones
8. Cable television

INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

Internet Today



a. Structure of a national ISP

b. Interconnection of national ISPs

PROTOCOLS AND STANDARDS

Protocols: In computer networks, communication occurs between **entities or nodes** in different systems. An entity or node is anything capable of sending or receiving information.

However, two entities cannot simply send bitstreams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are **syntax**, **semantics**, and **timing**.

Example – A person from Bengal is talking to a person in Kerala on phone. They use their own languages, and no person understands, what the other person said. So no communication will occur between the two.

If they use a protocol, it means if both person understands English or Hindi, then the communication will occur because both person understands what the other person says.

Syntax - The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the **first 8 bits of data to be the address of the sender**, the **second 8 bits to be the address of the receiver**, and the **rest of the stream to be the message itself.**

Semantics - The word semantics refers to the meaning of each section of bits. How are a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

Timing - The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards

Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

De facto - Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

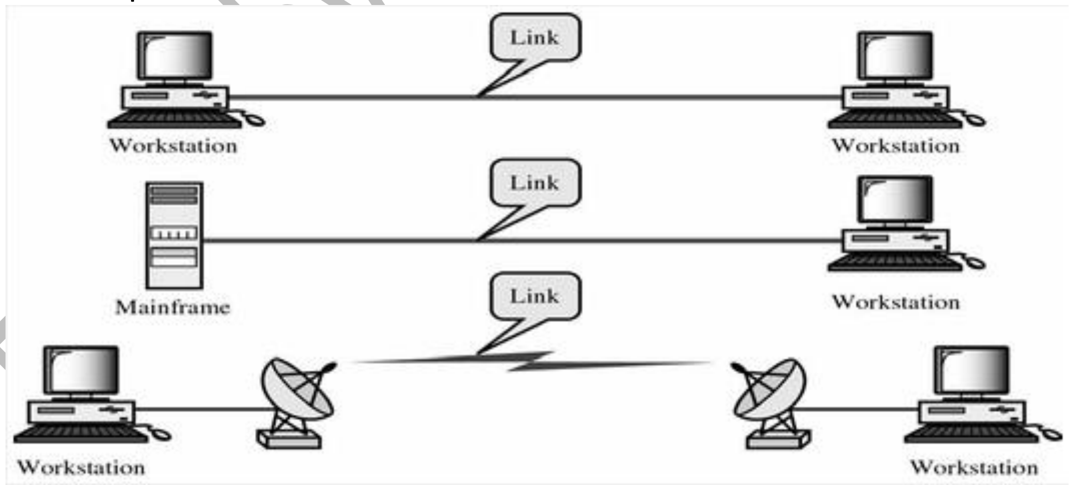
De jure - Those standards that have been legislated by an officially recognized body are de jure standards.

Line Configurations

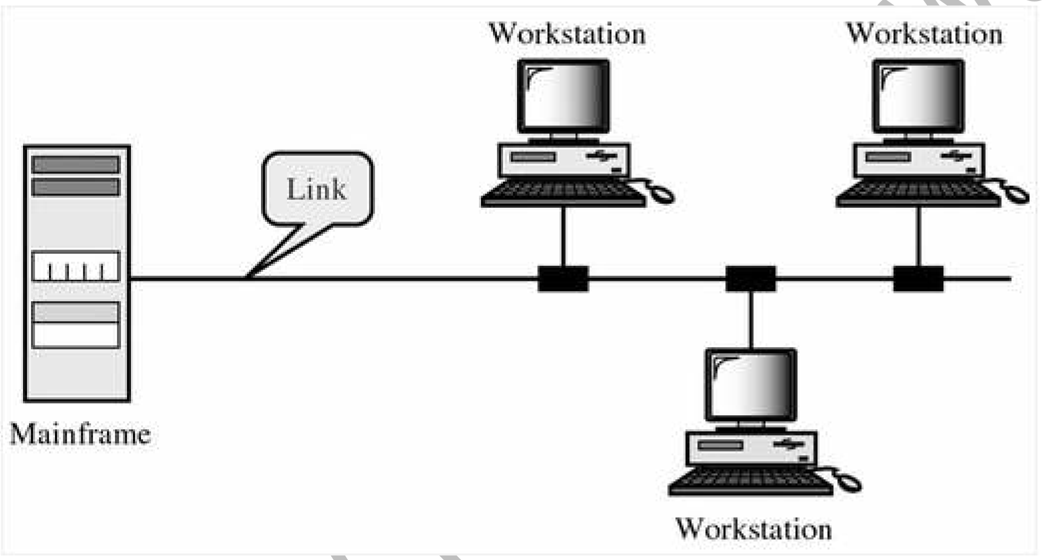
Line configuration refers to the way two or more communication devices attached to a link. A link is the physical communication pathway that transfers data from one device to another.

There are two possible line configurations

1. Point-to-Point – This provides a dedicated link between two devices. The entire capacity of the channel is reserved for transmission between those two devices.
   Most point-to-point line configurations use an actual length of wire or cable to connect two ends, but other options, such as microwave or satellite link, are also possible.



2. Multipoint or Multidrop - A multipoint line configuration is one in which more than two specific devices share a single link.
   In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
   Spatial Sharing: If several devices can share the link simultaneously, it's called spatially shared line configuration
   Temporal (Time) Sharing: If users must take turns using the link, then it's called temporally shared or Time Shared Line Configuration.



Topology

The term “**Topology**” refers to the way in which the endpoints or stations/computer systems, attached to the networks, are interconnected. We have seen that topology is essentially a stable geometric arrangement of computers in a network. If you want to select a topology for doing networking, you have to take attention to the following points.

- Application S/W and protocols.
- Types of data communicating devices.
- Geographic scope of the network.
- Cost.
- Reliability.

Depending on the requirement there are different Topologies to construct a network.

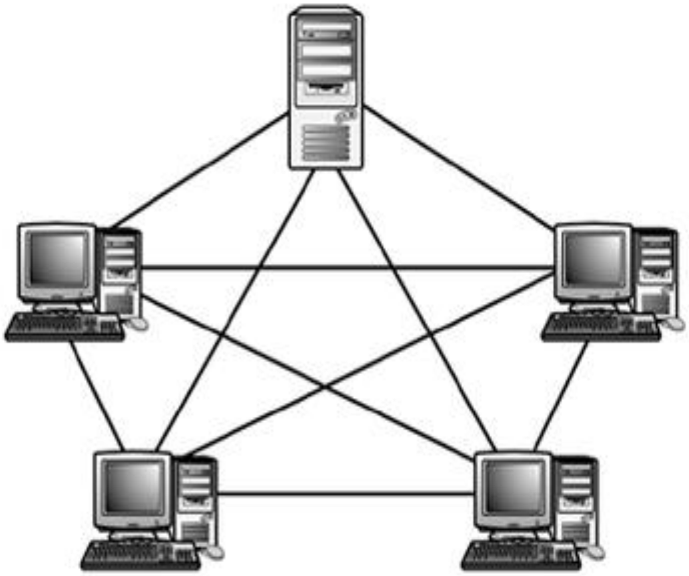
(1) Mesh topology.
(2) Star topology.
(3) Tree (Hierarchical) topology.
(4) Bus topology.
(5) Ring topology.
(6) Cellular topology.

- Ring and mesh topologies are felt convenient for peer to peer transmission.
- Star and tree are more convenient for client-server.
- Bus topology is equally convenient for either of them.

Mesh Topology

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by **Reed's Law**.
Reed's law is the assertion of David P. Reed that the utility of large networks, particularly social networks, can scale exponentially with the size of the network.

The number of connections in a full mesh = n(n - 1) / 2

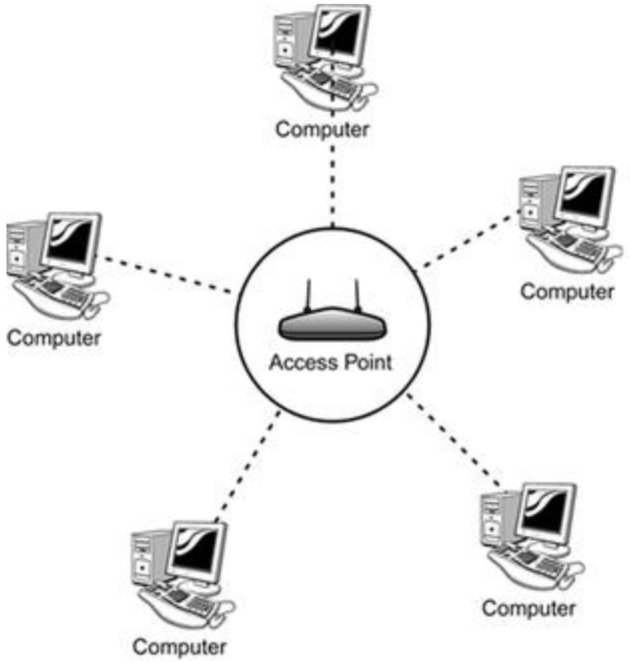


ADVANTAGE:
Robust.
Fault diagnosis is easy.
Provide security and privacy.
Each connection can carry its own load.

DISADVANTAGE:
Cabling cost is more.
Installation and configuration are difficult.

Star Topology

In a star topology, cables run from every computer to a centrally located device called a HUB. Star topology networks require a central point of connection between the media segment. These central points are referred to as Hubs. Hubs are special repeaters that overcome the electromechanical limitations of a media. Each computer on a star network communicates with a central hub that resends the message either to all the computers (In a broadcast network) or only the destination computer. (In a switched network). Ethernet 10 base T is a popular network based on the star topology. 10BASE-T, one of several physical media specified in the IEEE 802.3 standard for Ethernet local area networks (LANs), is ordinary telephone twisted-pair wire. 10BASE-T supports Ethernet's 10 Mbps transmission speed.



ADVANTAGES:

Easy to diagnose network fault.
Good performance.
Scalable, easy to set up and to extend.
Use of multiple cable types in the same network with a hub.

DISADVANTAGES:

Totally depend on a single hub.
Expensive to install.

Tree (Hierarchical) topology

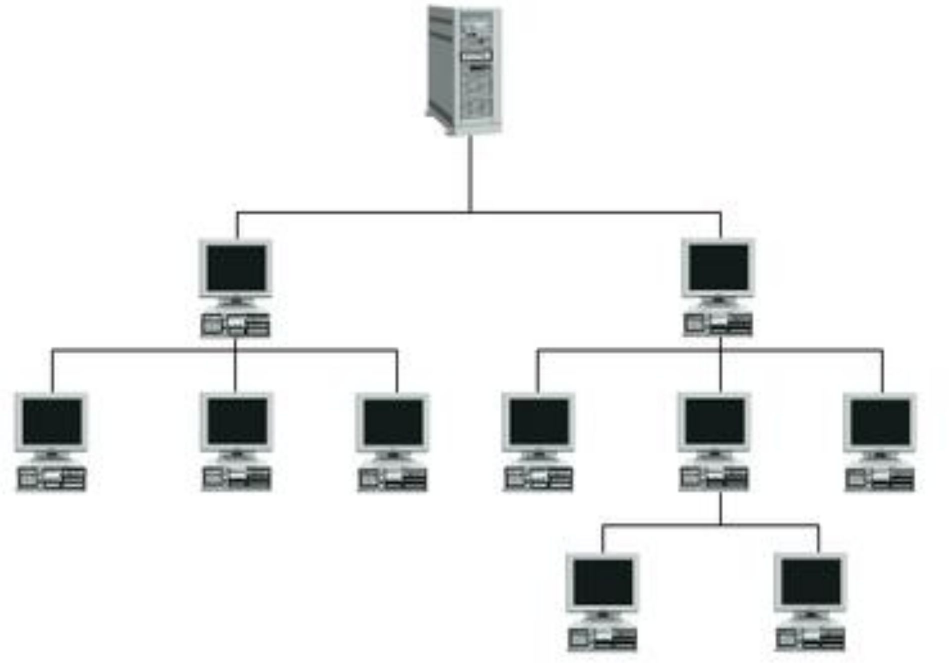
It is similar to the star network, but the nodes are connected to the secondary hub that in turn is connected to the central hub.

The central hub is the active hub.

The active hub contains the repeater, which regenerates the bits pattern it receives before sending them out.

The secondary hub can be either active or passive.

A passive hub provides a simple physical connection between the attached devices.



ADVANTAGE:

Easily managed and maintained.

Error detection is easily done.

The expansion of nodes is possible and easy.

Extension of bus and star topologies.

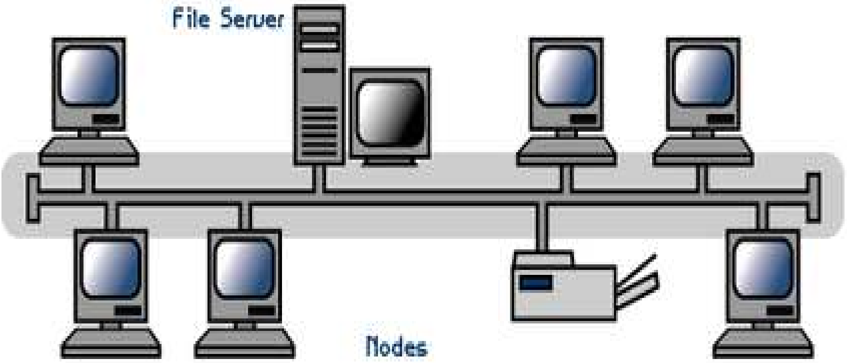
DISADVANTAGE:

Heavily cabled.

Central hub fails network fails.

Bus topology

A bus topology connects computers along a single or more cable to connect linearly. A network that uses a bus topology is referred to as a "bus network" which was the original form of Ethernet networks. Ethernet 10Base2 (also known as thinnet) is used for bus topology.



ADVANTAGES:

Easy to implement and extend.
Less expensive because it requires the least amount of cable to connect the computers together.
Suitable and easy to use for small or temporary networks.
For extension, a repeater can also be used.

DISADVANTAGES:

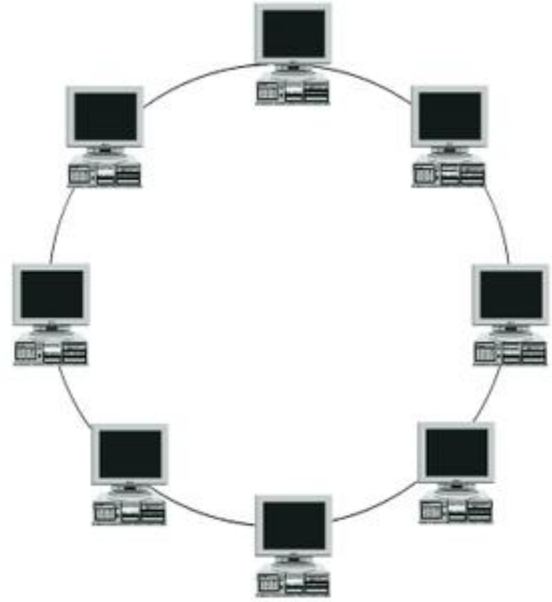
Heavy network traffic can slow a bus.
Proper termination is required.
Fault in the bus cable stops all transmission.
Difficult to administer.

Ring topology

In a ring topology, each device has a dedicated point-to-point line configuration only with two devices on either side of it.
A signal is passed along the ring in one direction, from device to device until it reaches its destination.

Each device in the ring has a repeater. When the devices receive the signal intended for the other node, it just regenerates the bits and passes them along. Ring network passes a token.

A token is a short message with the electronic address of the receiver. Each network interface card is given a unique electronic address, which is used to identify the computer on the network. **Early token release** releases the token just after the transmitting the data and **Delay token release** releases the token after the acknowledgement is received from the receiver.



ADVANTAGES:

It offers high performance for a small number of workstations or for large networks where each station has a similar workload.

Easy to extend.

DISADVANTAGE:

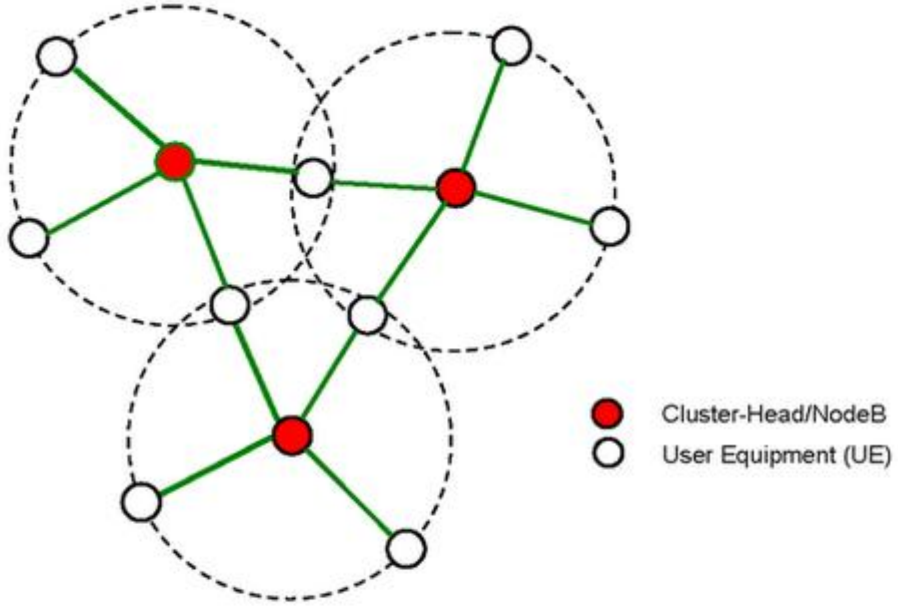
Adding and removing disrupt the network.

Troubleshooting is difficult.

Parameters	BUS	STAR	RING	MESH	TREE
Installation	easy	easy	difficult	difficult	easy
Cost	inexpensive	expensive	moderate	expensive	less
Flexible	Yes	Yes	No	no	yes
Reliability	moderate	High	High	High	moderate
Extension	Easy	Easy	Easy	Poor	Easy
Robust	No	Yes	No	Yes	No

Cellular topology

The cellular topology is applicable only in the case of wireless media that does not require a cable connection.
In wireless media, each point transmits in a certain geographical area called a cell. Each cell represents a portion of the total network area.
Devices that are in the cell communicate through a central hub. Hubs in different cells are interconnected. The route data across the network and provide a complete network infrastructure.
The data is transmitted in the cellular digital packet data (CDPD) format.



Transmission Mode

A given transmission on a communications channel between two machines can occur in several different ways. The transmission is characterized by:

- the direction of the exchanges
- the transmission mode: the number of bits sent simultaneously
- synchronization between the transmitter and receiver

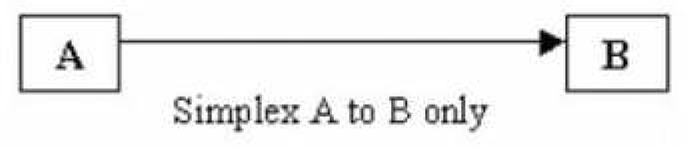
Types of Transmission mode

- Simplex
- Half Duplex
- Full Duplex

Simplex

A simplex connection is a connection in which the data flows in only one direction, from the transmitter to the receiver. This type of connection is useful if the data do not need to flow in both directions (for example, from your computer to the printer or from the mouse to your computer...).

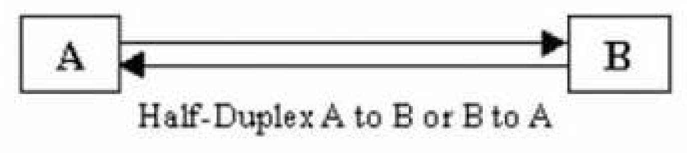
Example – Radio



Half Duplex

A half-duplex connection (sometimes called an *alternating connection* or *semi-duplex*) is a connection in which the data flows in one direction or the other, but not both at the same time. With this type of connection, each end of the connection transmits in turn. This type of connection makes it possible to have bidirectional communications using the full capacity of the line.

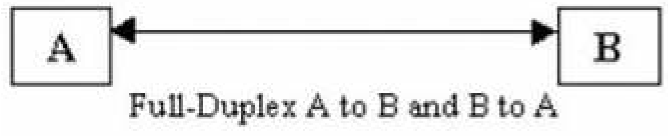
Example – Walkie-Talkie



Full Duplex

A full-duplex connection is a connection in which the data flow in both directions simultaneously. Each end of the line can thus transmit and receive at the same time, which means that the bandwidth is divided into two for each direction of data transmission if the same transmission medium is used for both directions of transmission.

Example – Phone



Categories of Network

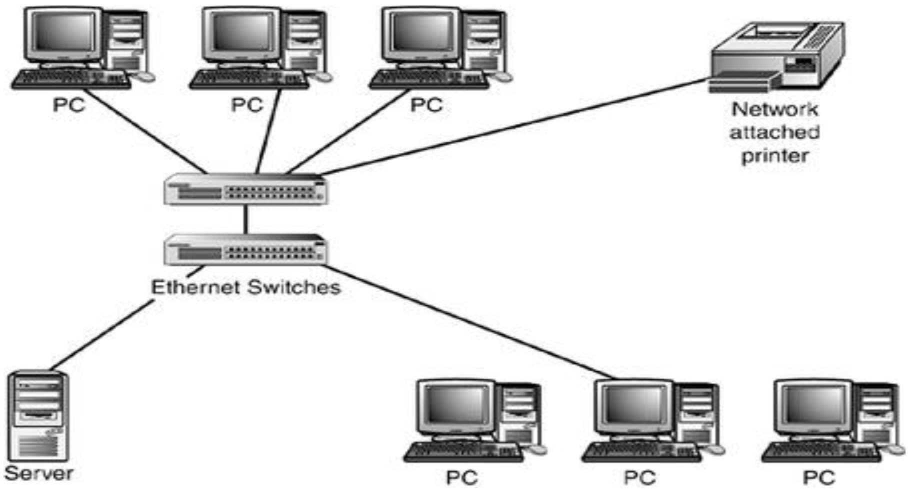
One way to categorize the different types of computer network designs is by their **scope** or **scale**. For historical reasons, the networking industry refers to nearly every type of design as some kind of *area network*. Common examples of area network types are:

- LAN - Local Area Network
- WLAN - Wireless Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network

Local Area Network

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet. In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

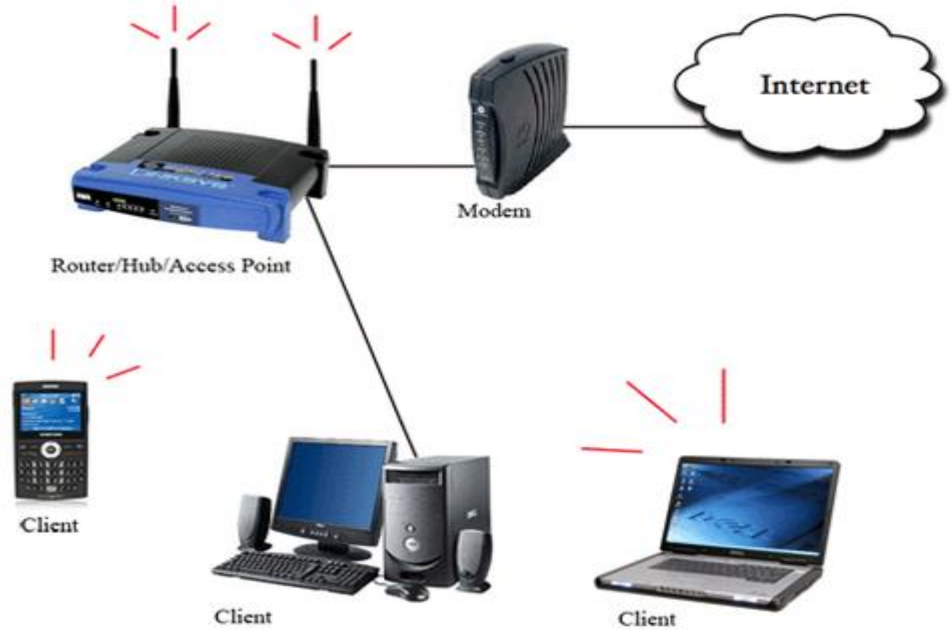
Ethernet - a system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.



Token Ring - a local area network in which a node can only transmit when in possession of a sequence of bits (the token), which is passed to each node in turn.

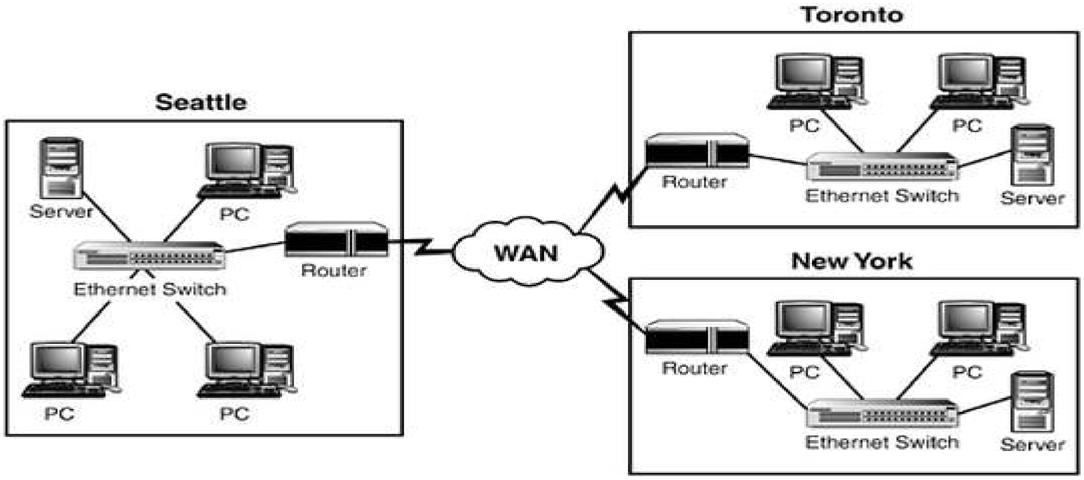
Wireless Local Area Network

A **wireless LAN** (**WLAN**) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building. This gives users the ability to move around within the area and remain connected to the network.



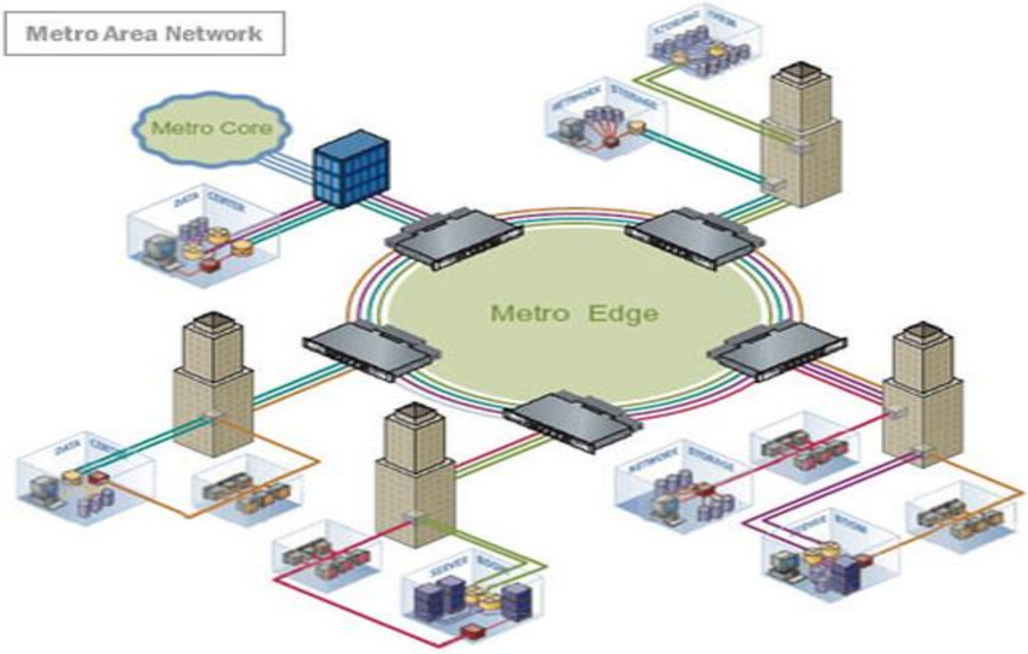
Wide Area Network

A WAN is a network that spans more than one geographical location often connecting separated LANs. WANs are slower than LANs and often require additional and costly hardware such as routers, dedicated leased lines, and complicated implementation procedures.



Metropolitan Area Network

A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned and operated by a single entity such as a government body or large corporation.



Distributed Queue Dual Bus (DQDB)

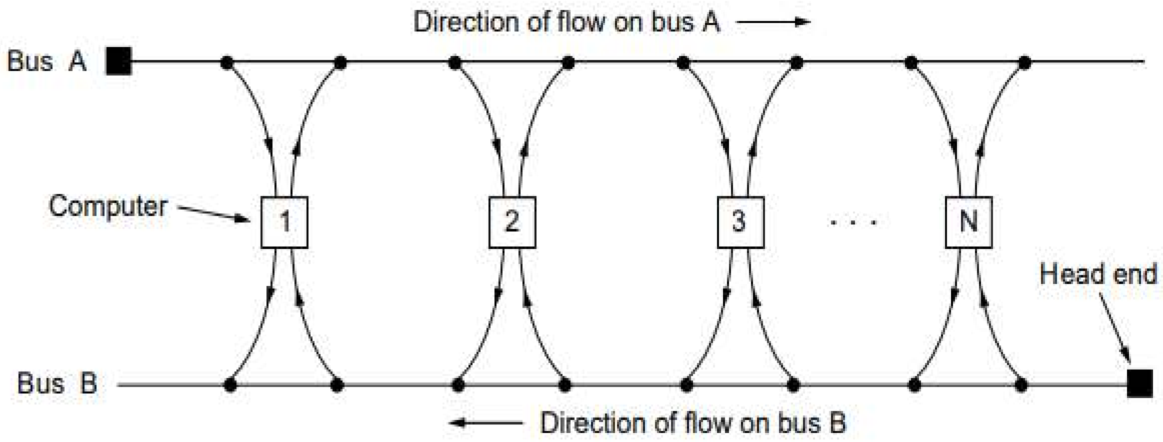
IEEE 802.3 to 802.5 protocols are only suited for “small” LANs. They cannot be used for very large but non-wide area networks.

IEEE 802.6 DQDB is designed for MANs. It can cover an entire city, it has ability to integerate individuals LANs by providing the interconnecting backbone structure.

The architecture consists of a slotted system using a unidirectional user system operating at 155 Mbit/s. The frame synchronizing signals are generated by the network by the network controller or **Head end** which is at one end of the system. Direction of flow on a bus points to downstream. Fixed-size **53-byte cells** with **44-byte payload** are used.

1 BYTE	52 BYTE
ACCESS CONTROL FIELD	PROTOCOL DATA UNIT (PDU)

Access control field contains 3 bits used for the purpose of **request**.
A station can queue a request to talk on a bus by putting a reservation on the other bus.



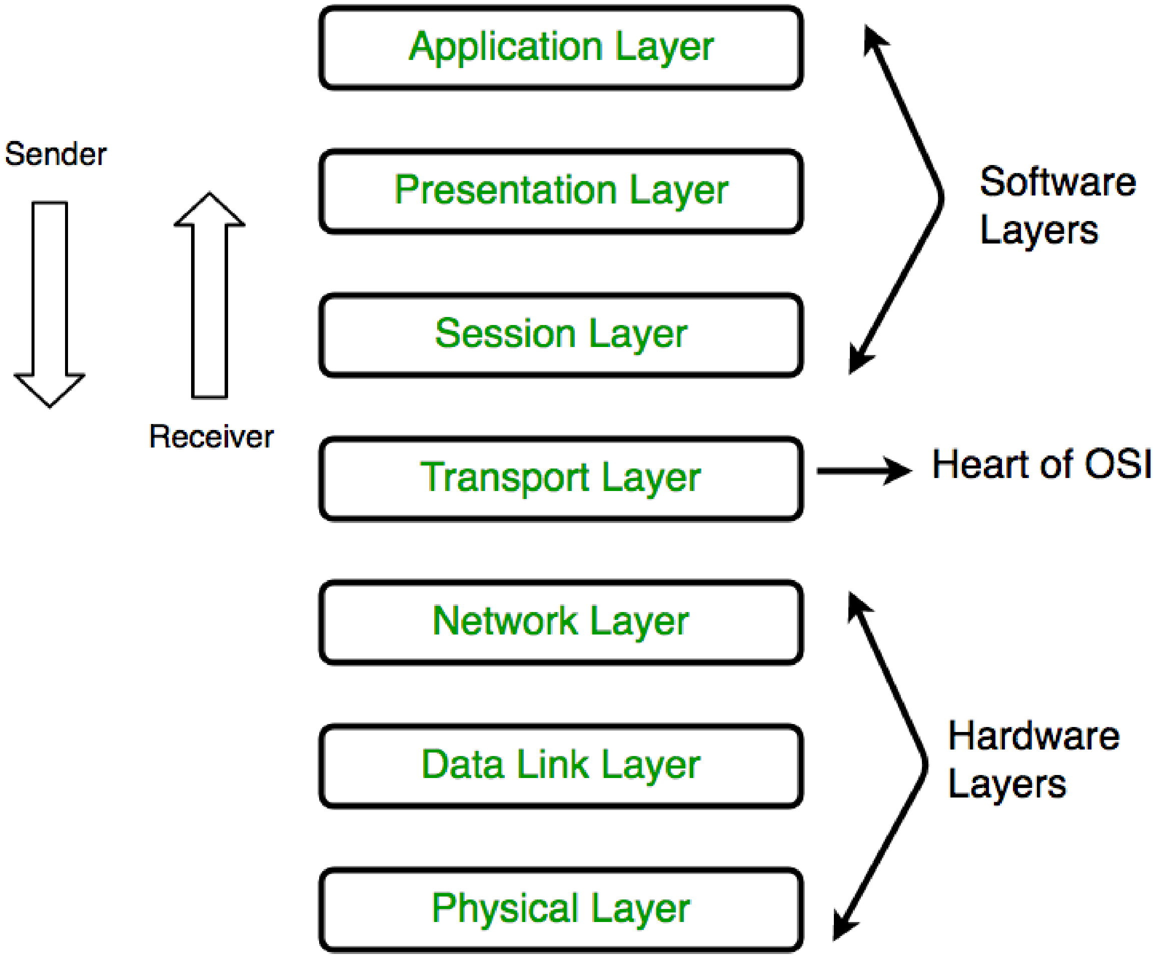
Every station has two count registers, one for each bus. A count register is incremented by 1 everytime an upstream station reservation is seen in a passing slot. This register is decremented by 1 for every empty slot which flows in the opposite direction on the other bus.
If a station is waiting to talk on a bus, then it makes a reservation on the other bus in the first free reservation field. Then a copy of request count register is made, and it is decremented for each empty slot passing by on the alternative bus. This process continues until this copied register contents reduce to zero. The next empty slot is then used. The request count register continues in a normal way and takes the requests made further.

The OSI Model

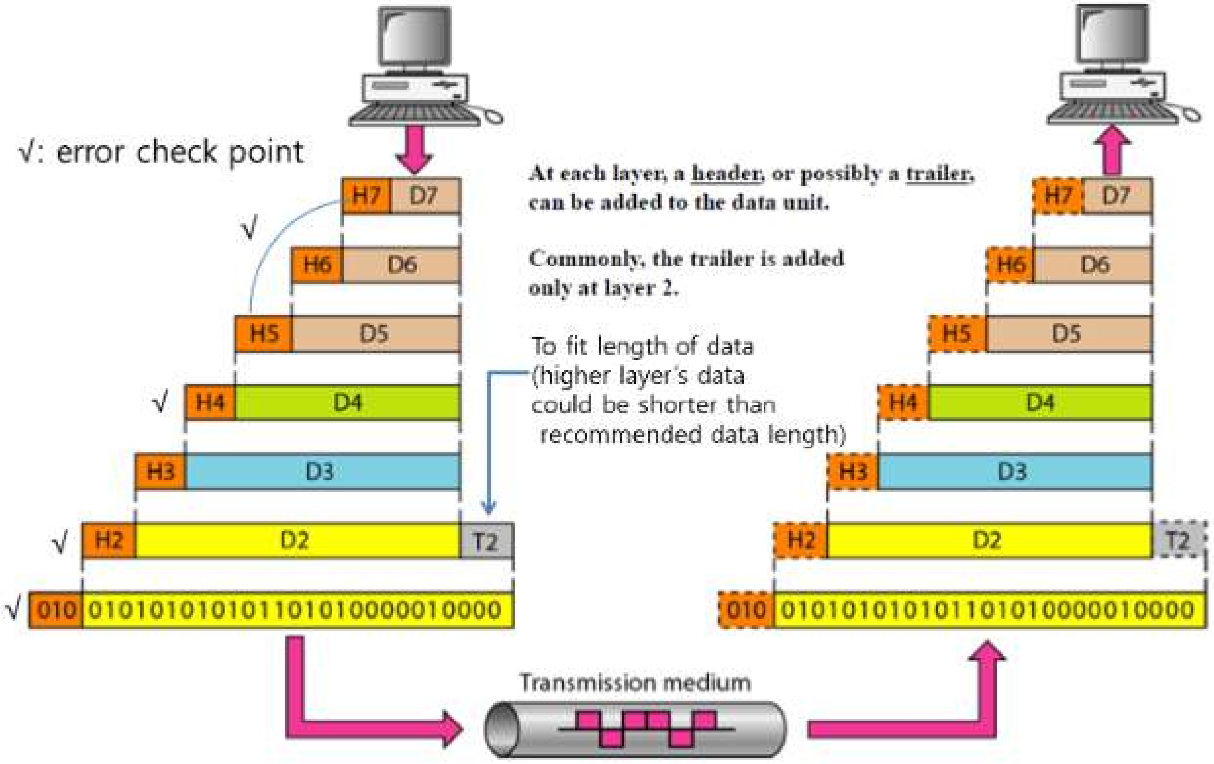
An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



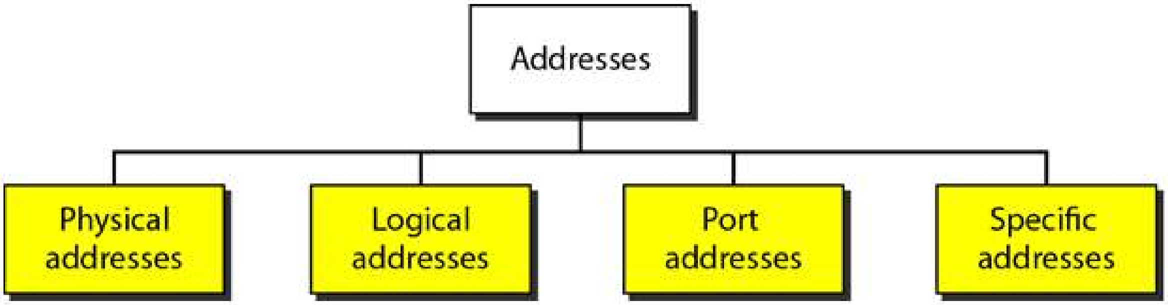
OSI Layers show **Headers** and **Trailers**


√: error check point
H7
D7
H6
D6
H5
D5
√
H4
D4
H3
D3
√
H2
D2
T2
√
010
0101010101011010100000100000
At each layer, a header, or possibly a trailer, can be added to the data unit.
Commonly, the trailer is added only at layer 2.
To fit length of data (higher layer's data could be shorter than recommended data length)
Transmission medium

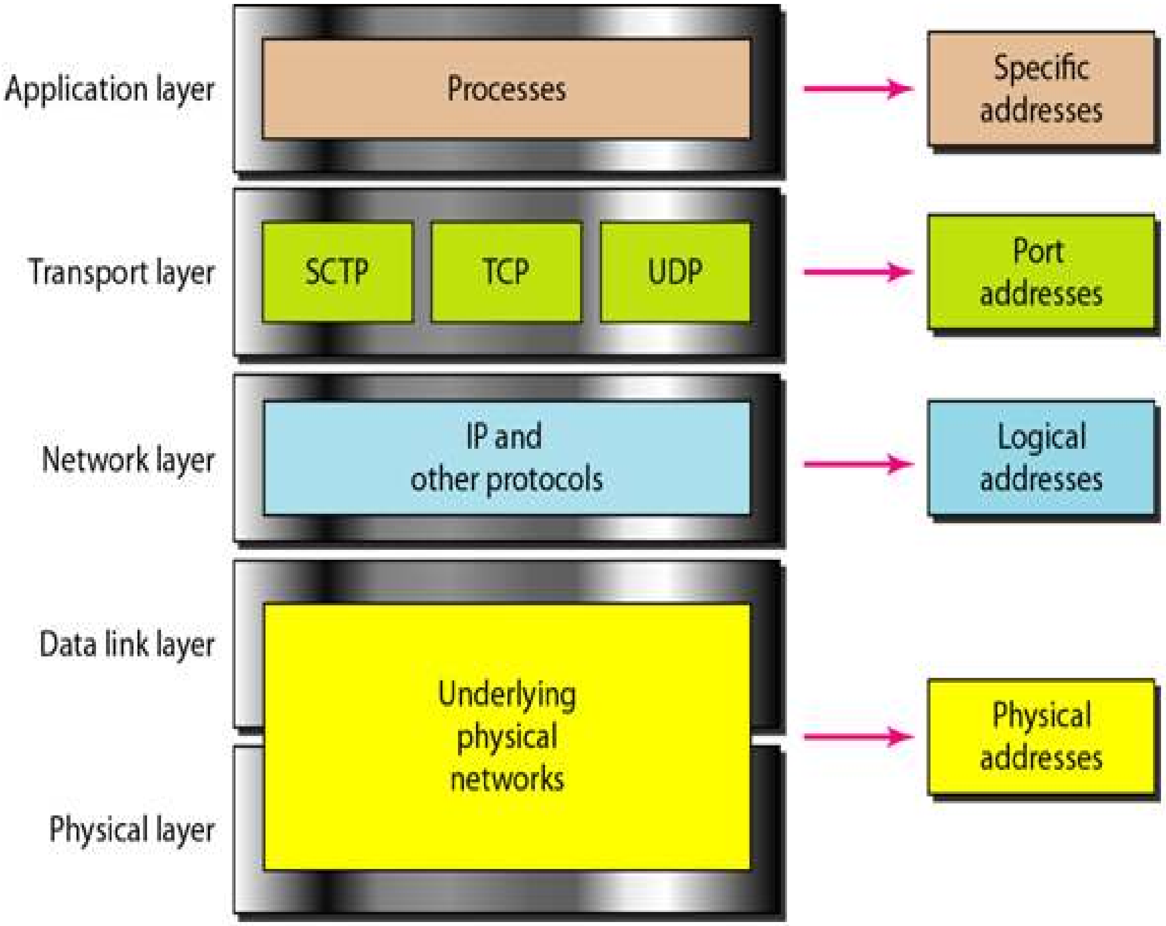
TCP/IP Layer Protocol

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

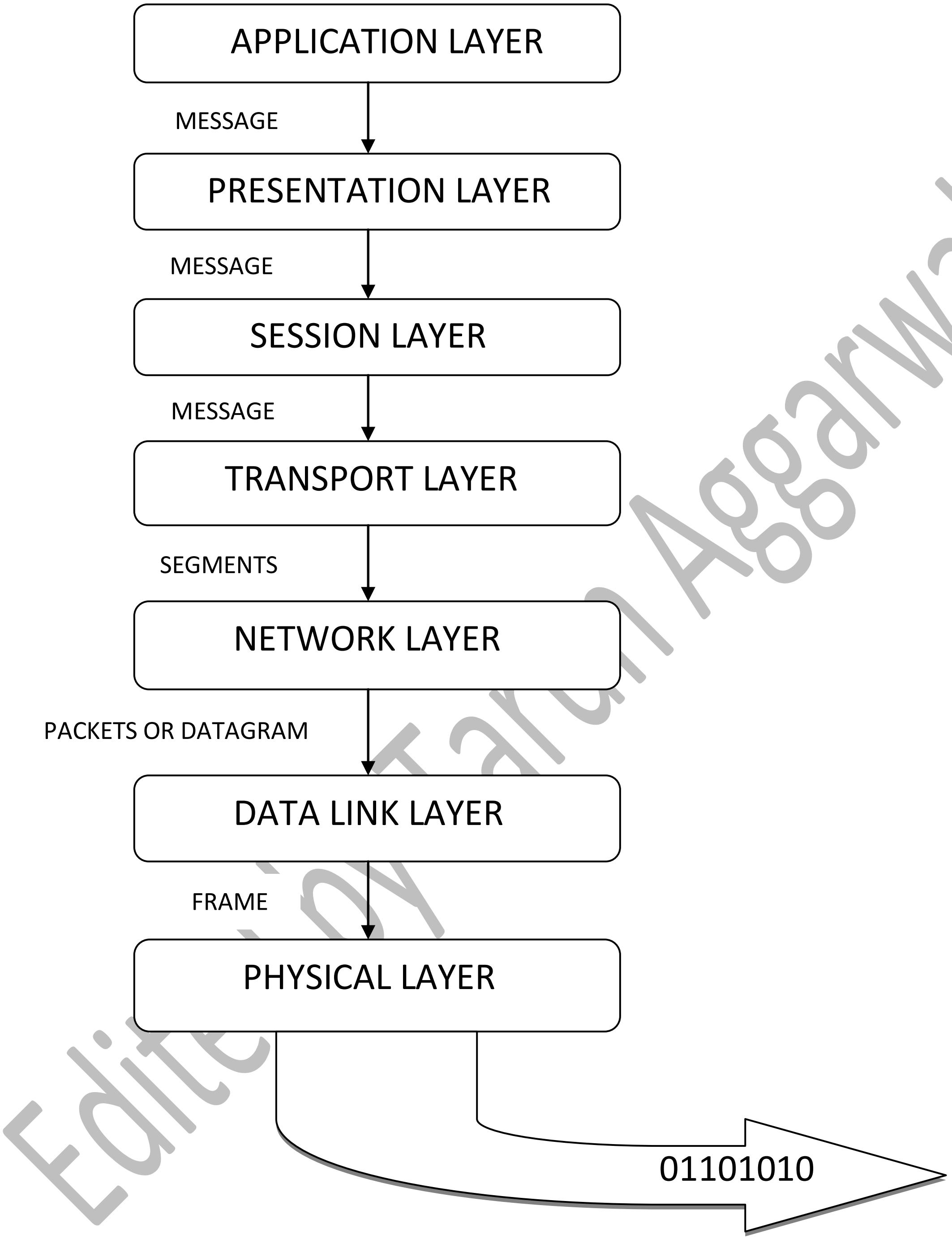
Four levels of addresses are used in an internet employing TCP/IP protocol.



Socket Address (Logical Address) = Port address + IP address



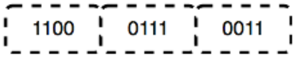
OSI Layers Connection in b/w two Computers or Devices



STREAM OF BITS

1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for the actual physical connection between the devices. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

1. **Bit synchronization**: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control**: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies**: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. **Transmission mode**: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

Hub, Repeater, Modem, Cables are Physical Layer devices. Network Layer, Data Link Layer and Physical Layer are also known as Lower Layers or Hardware Layers.

2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address. Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The functions of the data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

Packet in Data Link layer is referred as **Frame**.
Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
Switch & Bridge are Data Link Layer devices.

3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer. The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.

2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

Segment in Network layer is referred as **Packet**.
Network layer is implemented by networking devices such as **routers**.

4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

• At sender's side:
Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer. Note: The sender need to know the port number associated with the receiver's application.
Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

• At receiver's side:
Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.
The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.

2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service:** It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

Data in the Transport Layer is called as **Segments**.

Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls. Transport Layer is called as **Heart of OSI** model.

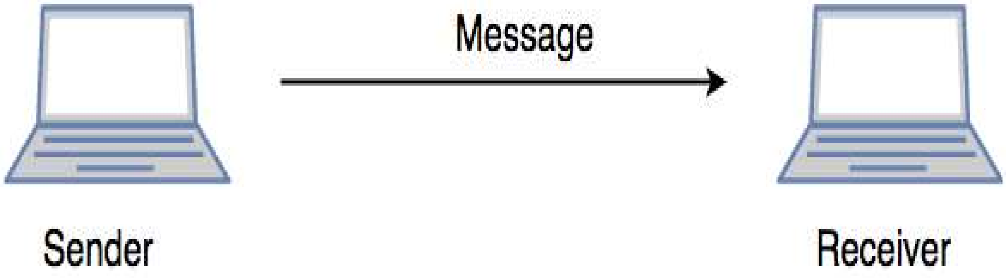
5. Session Layer (Layer 5) :

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

All the below 3 layers(including Session Layer) are integrated as a single layer in TCP/IP model as “Application Layer”.
Implementation of these 3 layers is done by the network application itself. These are also known as ***Upper Layers*** or ***Software Layers***.
SCENARIO:
Let’s consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0’s and 1’s) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

1. **Translation :** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
Ex: Application – Browsers, Skype Messenger etc.
Application Layer is also called as Desktop Layer.
The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in Internet because of its late invention. Current model being used is the TCP/IP model.

Switching

A network consists of many switching devices. In order to connect multiple devices, one solution could be to have a point to point connection in between pair of devices. But this increases the number of connection. The other solution could be to have a central device and connect every device to each other via the central device which is generally known as Star Topology. Both these methods are wasteful and impractical for very large network. The other topology also can not be used at this stage. Hence a better solution for this situation is SWITCHING. A switched network is made up of a series of interconnected nodes called switches.

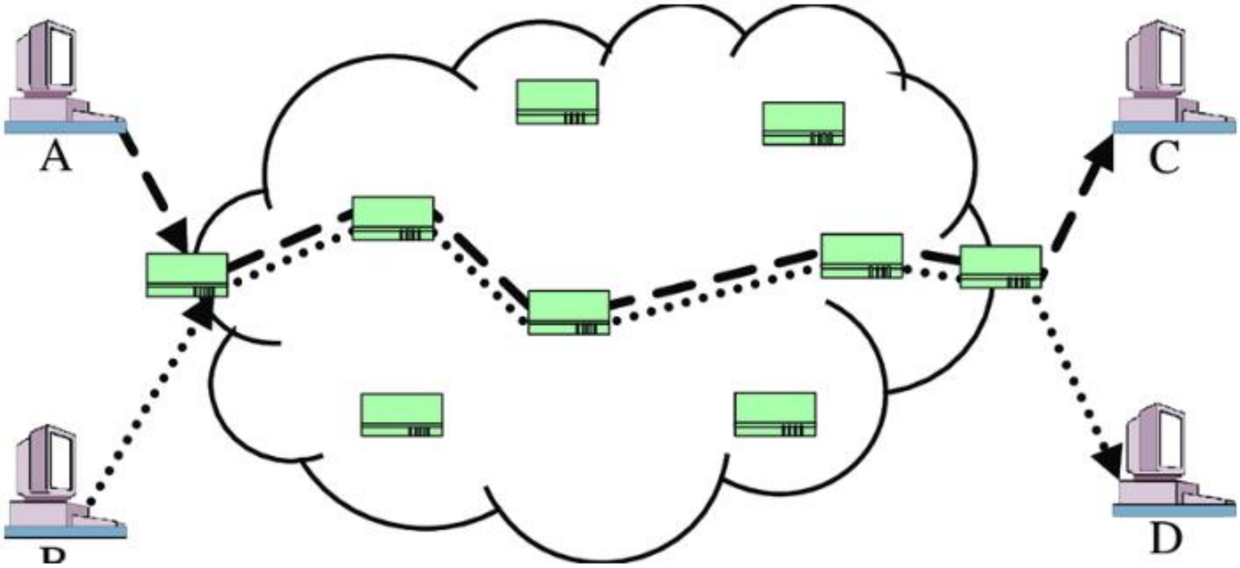
Types of Switching Techniques

There are basically three types of switching methods are made available. Out of three methods, circuit switching and packet switching are commonly used but the message switching has been opposed out in the general communication procedure but is still used in the networking application.

1) Circuit Switching
2) Packet Switching
3) Message Switching

Circuit Switching

Circuit Switching is generally used in the public networks. It come into existence for handling voice traffic in addition to digital data. How ever digital data handling by the use of circuit switching methods are proved to be inefficient. The network for Circuit Switching is shown in figure.



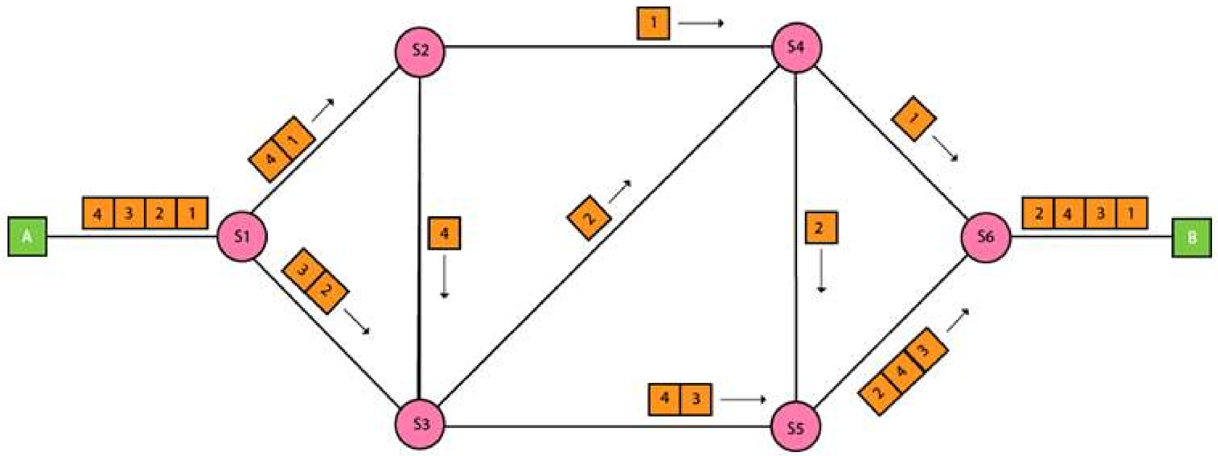
Circuit Switching Network

- Here the network connection allows the electrical current and the associated voice with it to flow in between the two respective users. The end to end communication was established during the duration of call.
- In circuit switching the routing decision is made when the path is set up across the given network. After the link has been sets in between the sender and the receiver then the information is forwarded continuously over the provided link.
- In Circuit Switching a dedicated link/path is established across the sender and the receiver which is maintained for the entire duration of conversation.

Packet Switching

In Packet Switching, messages are broken up into packets and each of which includes a header with source, destination and intermediate node address information. Individual Packets in packet switching technique take different routes to reach their respective destination. Independent routing of packets is done in this case for following reasons:

- **Bandwidth** is reduces by the splitting of data onto different routes for a busy circuit.
- For a certain link in the network, the link goes down during transmission. The remaining packet can be sent through the another route.

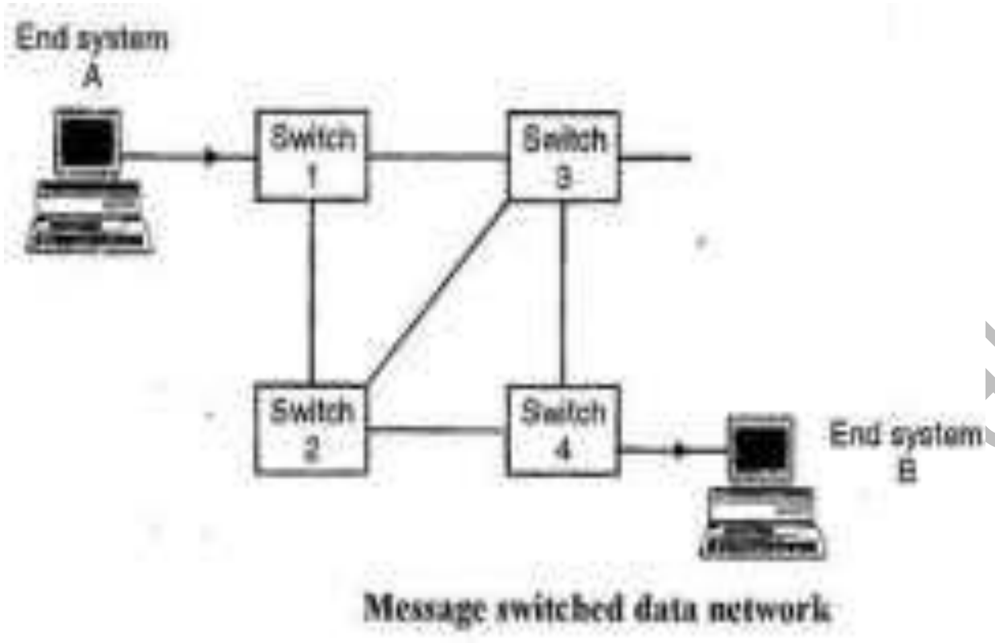


Packet Switching Network

- The major advantage of Packet switching is that they are used for performing data rate conversion.
- When traversing the network switches, routers or the other network nodes then the packets are buffered in the queue, resulting in variable delay and throughput depending on the network's capacity and the traffic load on network.
- Packet switching contrasts with another principal networking paradigm, circuit switching, a method which sets up a limited number of dedicated connections of constant bit rate and constant delay between nodes for exclusive use during the communication session.
- In cases where traffic fees are charged, for example in cellular communication, packet switching is characterized by a fee per unit of information transmitted.

Message Switching

In case of Message Switching it is not necessary to established a dedicated path in between any two communication devices. Here each message is treated as an independent unit and includes its own destination source address by its own. Each complete message is then transmitted from one device to another through internetwork.



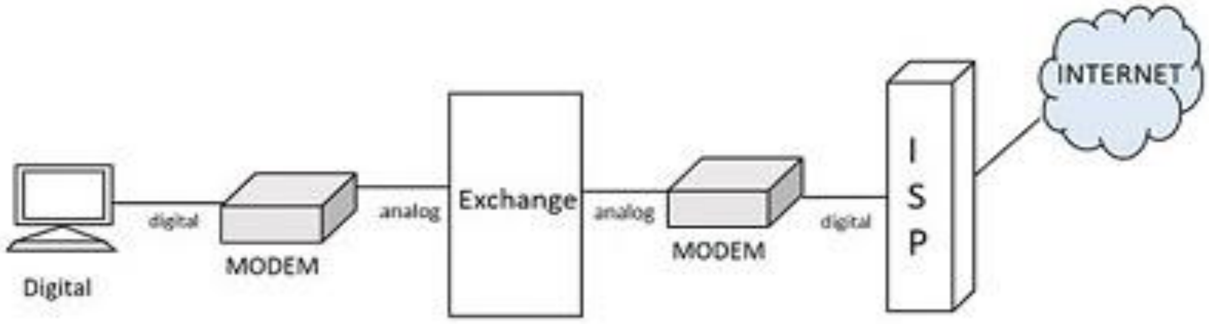
Message Switching Data Network

- Each intermediate device receive the message and store it until the next device is ready to receive it and then this message is forwarded to the next device. For this reason a message switching network is sometimes called as **Store and Forward** Switching.
- Message switches can be programmed with the information about the most efficient route as well as information regarding to the near switches that can be used for forwarding the present message to their required destination.
- The storing and Forwarding introduces the concept of delay. For this reasons this switching is not recommended for real time applications like voice and video.

ISDN (Integerated Services of Digital Networking)

Earlier, the transmission of data and voice both were possible through normal POTS, **Plain Old Telephone Systems**. With the introduction of Internet came the advancement in telecommunication too. Yet, the sending and receiving of data along with voice was not an easy task. One could use either the Internet or the Telephone. The invention of ISDN helped mitigate this problem.

The process of connecting a home computer to the Internet Service Provider used to take a lot of effort. The usage of the modulator-demodulator unit, simply called the MODEM was the essential thing to establish a connection. The following figure shows how the model worked in the past.



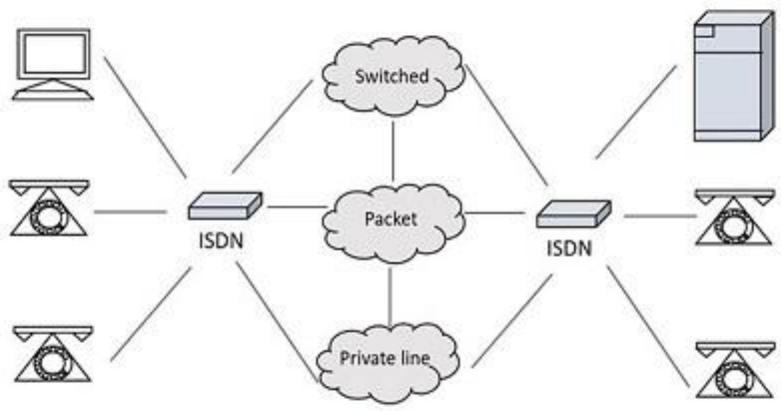
The above figure shows that the digital signals have to be converted into analog and analog signals to digital using modem during the whole path. What if the digital information at one end reaches to the other end in the same mode, without all these connections? It is this basic idea that lead to the development of **ISDN.**

As the system has to use the telephone cable through the telephone exchange for using the Internet, the usage of telephone for voice calls was not permitted. The introduction of ISDN has resolved this problem allowing the transmission of both voice and data simultaneously. This has many advanced features over the traditional PSTN, **Public Switched Telephone Network**.

ISDN

ISDN was first defined in the CCITT red book in 1988.The **Integrated Services of Digital Networking**, in short ISDN is a telephone network based infrastructure that allows the transmission of voice and data simultaneously at a high speed with greater efficiency. This is a circuit switched telephone network system, which also provides access to Packet switched networks.

The model of a practical ISDN is as shown below.



ISDN supports a variety of services. A few of them are listed below –

- Voice calls
- Facsimile
- Videotext
- Teletext
- Electronic Mail
- Database access
- Data transmission and voice
- Connection to internet
- Electronic Fund transfer
- Image and graphics exchange
- Document storage and transfer
- Audio and Video Conferencing
- Automatic alarm services to fire stations, police, medical etc.

Types of ISDN

Among the types of several interfaces present, some of them contains channels such as the **B-Channels** or Bearer Channels that are used to transmit voice and data simultaneously; the **D-Channels** or Delta Channels that are used for signaling purpose to set up communication.

The ISDN has several kinds of access interfaces such as −

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)
- Narrowband ISDN
- Broadband ISDN

Basic Rate Interface (BRI)

The Basic Rate Interface or Basic Rate Access, simply called the **ISDN BRI Connection** uses the existing telephone infrastructure. The BRI configuration provides **two data** or bearer channels at **64 Kbits/sec** speed and one control or delta channel at **16 Kbits/sec**. This is a standard rate.

The ISDN BRI interface is commonly used by smaller organizations or home users or within a local group, limiting a smaller area.

Primary Rate Interface (PRI)

The Primary Rate Interface or Primary Rate Access, simply called the ISDN PRI connection is used by enterprises and offices. The PRI configuration is based on T-carrier or T1 in the US, Canada and Japan countries consisting of **23 data** or bearer channels and one control or delta channel, with 64kbps speed for a bandwidth of 1.544 M bits/sec. The PRI configuration is based on E-carrier or E1 in Europe, Australia and few Asian countries consisting of **30 data** or bearer channels and **two-control** or delta channel with 64kbps speed for a bandwidth of 2.048 M bits/sec.

The ISDN BRI interface is used by larger organizations or enterprises and for Internet Service Providers.

Narrowband ISDN

The Narrowband Integrated Services Digital Network is called the **N-ISDN**. This can be understood as a telecommunication that carries voice information in a narrow band of frequencies. This is actually an attempt to digitize the analog voice information. This uses 64kbps circuit switching.

The narrowband ISDN is implemented to carry voice data, which uses lesser bandwidth, on a limited number of frequencies.

Broadband ISDN

The Broadband Integrated Services Digital Network is called the **B-ISDN**. This integrates the digital networking services and provides digital transmission over ordinary telephone wires, as well as over other media. The CCITT defined it as, "Qualifying a service or system requiring transmission channels capable of supporting rates greater than primary rates."

The broadband ISDN speed is around 2 MBPS to 1 GBPS and the transmission is related to ATM, i.e., Asynchronous Transfer Mode. The broadband ISDN communication is usually made using the fiber optic cables.

As the speed is greater than 1.544 Mbps, the communications based on this are called **Broadband Communications**. The broadband services provide a continuous flow of information, which is distributed from a central source to an unlimited number of authorized receivers connected to the network. Though a user can access this flow of information, he cannot control it.

Advantages of ISDN

ISDN is a telephone network based infrastructure, which enables the transmission of both voice and data simultaneously. There are many advantages of ISDN such as −

- As the services are digital, there is less chance for errors.
- The connection is faster.
- The bandwidth is higher.
- Voice, data and video − all of these can be sent over a single ISDN line.

Disadvantages of ISDN

The disadvantage of ISDN is that it requires specialized digital services and is costlier.

However, the advent of ISDN has brought great advancement in communications. Multiple transmissions with greater speed are being achieved with higher levels of accuracy.

DATA AND SIGNALS

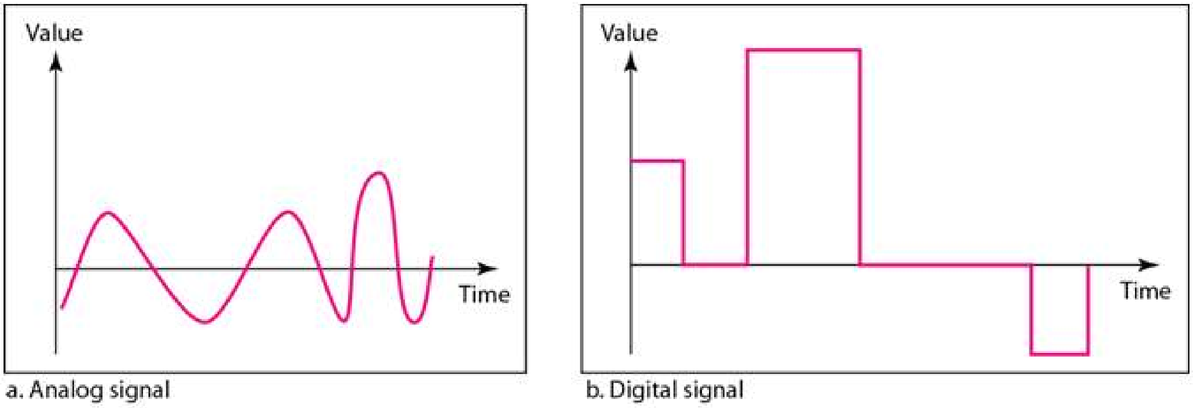
To be transmitted, data must be transformed into electromagnetic signals.

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.

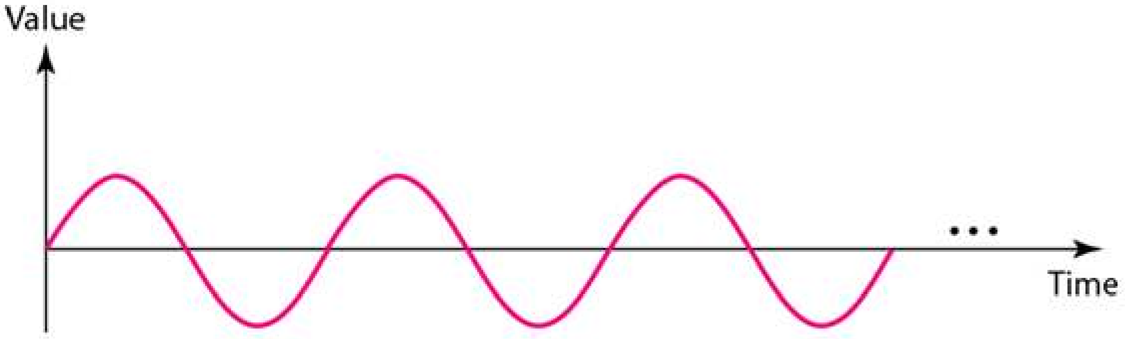


a. Analog signal

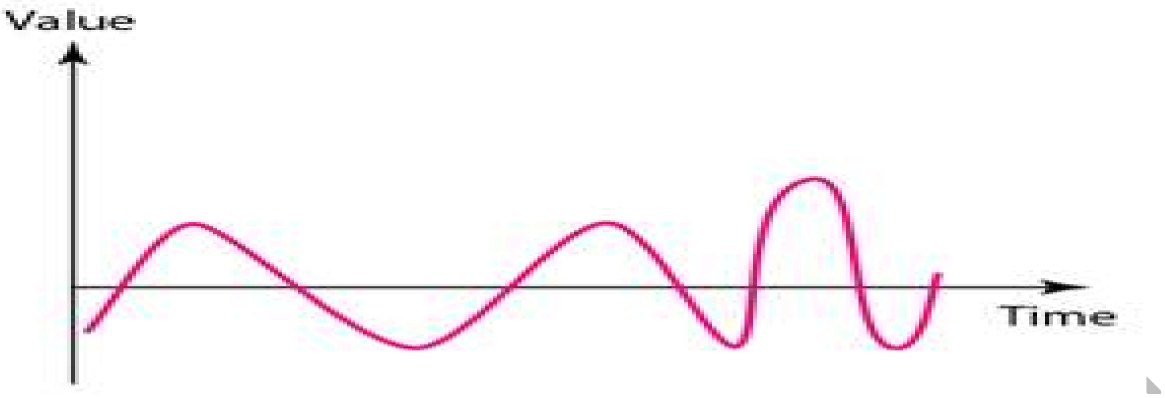
b. Digital signal

Periodic and Non-Periodic

Periodic Signals - A signals that repeats its pattern over a period is called **periodic** signals.
Example – A sine wave



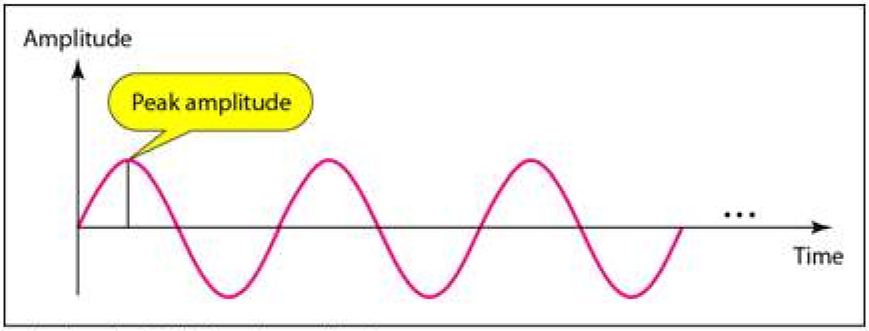
Non-Periodic Signals – A signal that does not repeat its pattern over a period is called **Non – Periodic** signals.



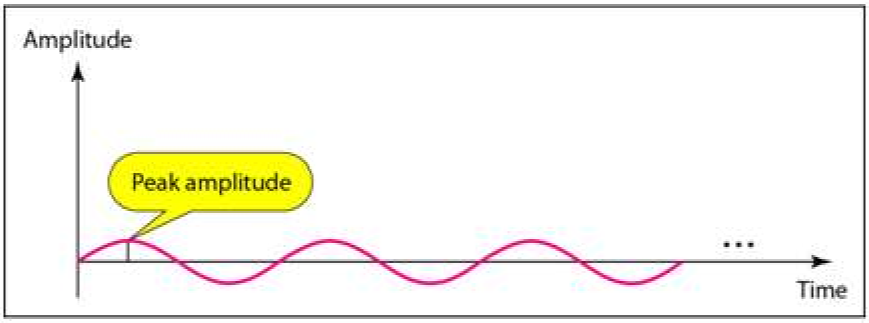
A wave can be represented by three parameters

(1) The peak amplitude
(2) Frequency
(3) Phase

<u>The Peak Amplitude</u>



a. A signal with high peak amplitude

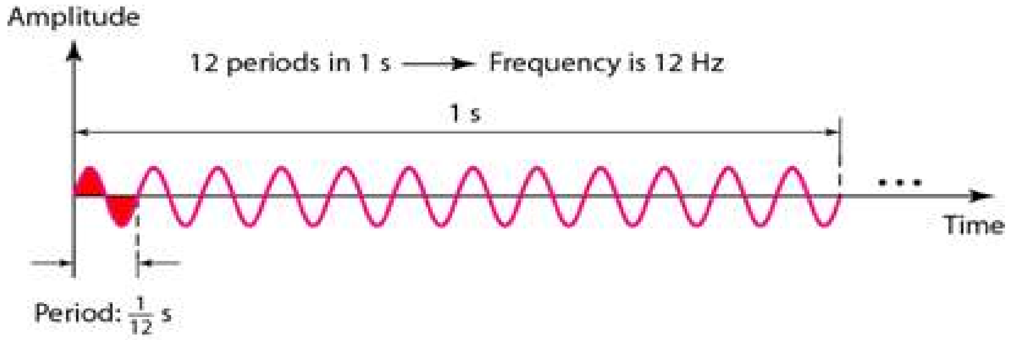


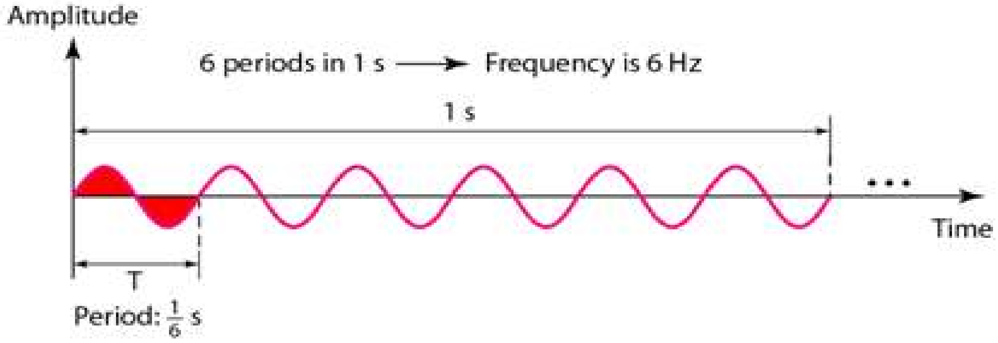
b. A signal with low peak amplitude

Frequency

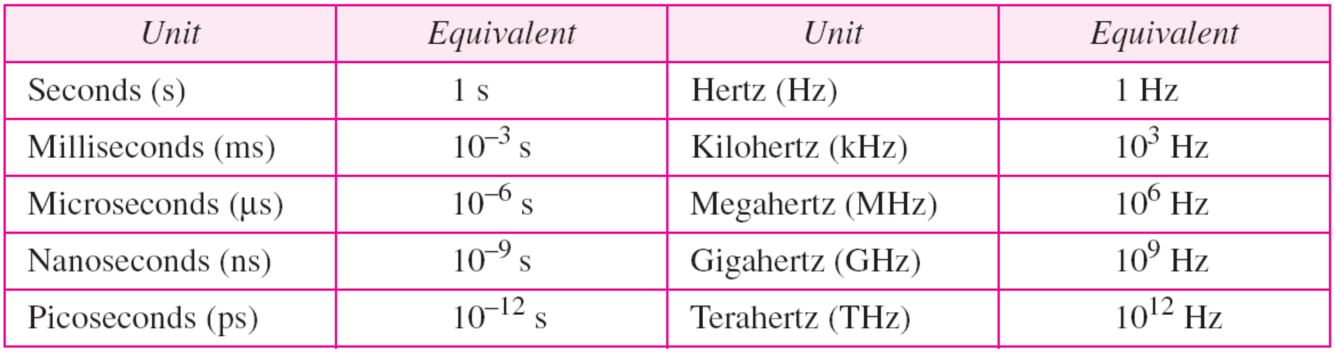
Frequency refers to the number of periods in 1 second. Period refers to the amount of time, in seconds, a signal need to complete 1 cycle.

Frequency and Period are the inverse of each other.





UNITS OF PERIOD AND FREQUENCY



Unit	*Equivalent*	*Unit*	*Equivalent*
Seconds (s)	1 s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3} s	Kilohertz (kHz)	10^{3} Hz
Microseconds (μs)	10^{-6} s	Megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10^{12} Hz

Exercise: The power we use at home has a frequency of 60 Hz. The period of this sine wave can be determined as follows

T = 1/f = 1/60 = 0.0166 s = 16.6 ms

Exercise: The period of signal is 100 ms. What is its frequency in kilohertz?

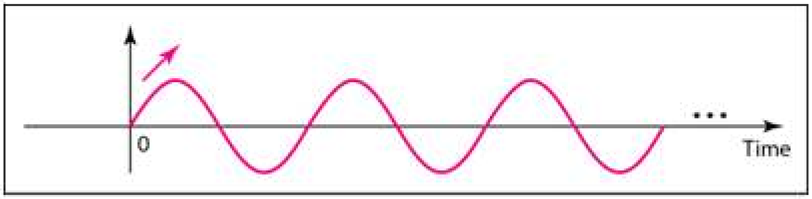
T = 1/f = 1/(100 ms) = 1/ (100 * 10^{-3} s) = 1/ (10^{-1} s) = 10 Hz = 10^{-2} KHz.

Frequency is the rate of change with respect to time. Change in a short span of time means high frequency. Change over a long span of time means low frequency.

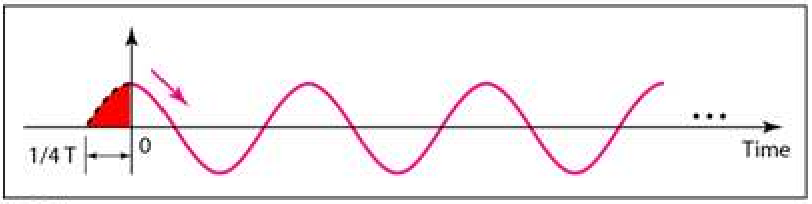
If a signal does not change at all, its frequency is zero. If a signal changes instantaneously, its frequency is infinite.

Phase

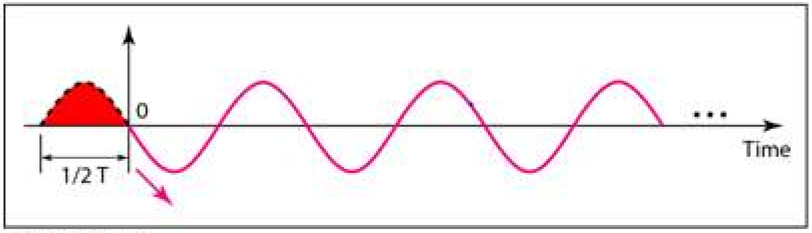
The term phase describes the position of the waveform relative to time 0. If we think of the wave as something that can be shifted backward or forward along the time axis, phase describes the amount of that shift. It indicates the status of the first cycle.



a. 0 degrees



b. 90 degrees



c. 180 degrees

Example - A sine wave is offset 1/6 cycle with respect to time 0. What is its phase in degrees and radians?

Solution - We know that 1 complete cycle is 360°.

Therefore, 1 cycle is 1/6 x 360 = 60^0 = 60 * 2 π/360 rad = π/3 rad = 1.046 radian

Composite Signal

A signal made up of many signals are called composite signals.

- If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies.
- If the composite signal is nonperiodic, the decomposition gives a combination of sine waves with continuous frequencies.

Bandwidth

- The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.

Exercise: If a periodic signal is decomposed into five sine waves with frequency of 100 Hz, 300 Hz, 500 Hz, 700 Hz and 900 Hz. Find the bandwidth?

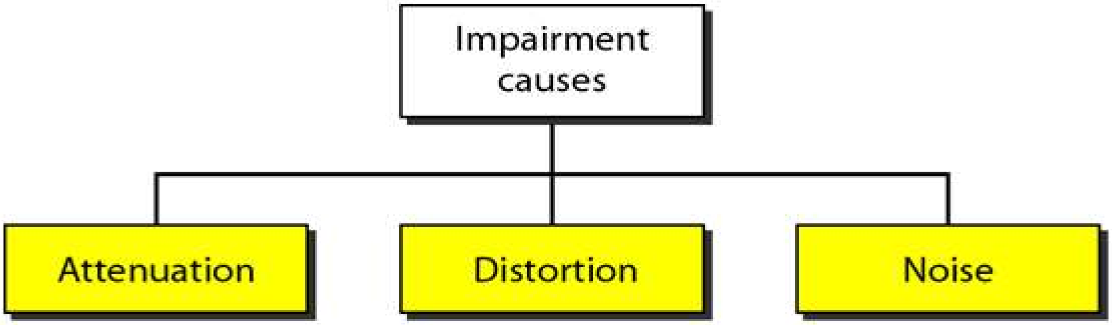
Sol – Highest frequency = 900 Hz
Lowest frequency = 100 Hz
Bandwidth = Highest frequency – lowest frequency = 900 – 100 = 800 Hz

Digital Signal

In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level.

Transmission Impairment

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are **attenuation, distortion, and noise.**



Attenuation

- Means loss of energy -> weaker signal
- When a signal travels through a medium it loses energy overcoming the resistance of the medium
- Amplifiers are used to compensate for this loss of energy by amplifying the signal.
- To show the loss or gain of energy the unit “decibel” is used.

$$dB = 10\log_{10}P_2/P_1$$

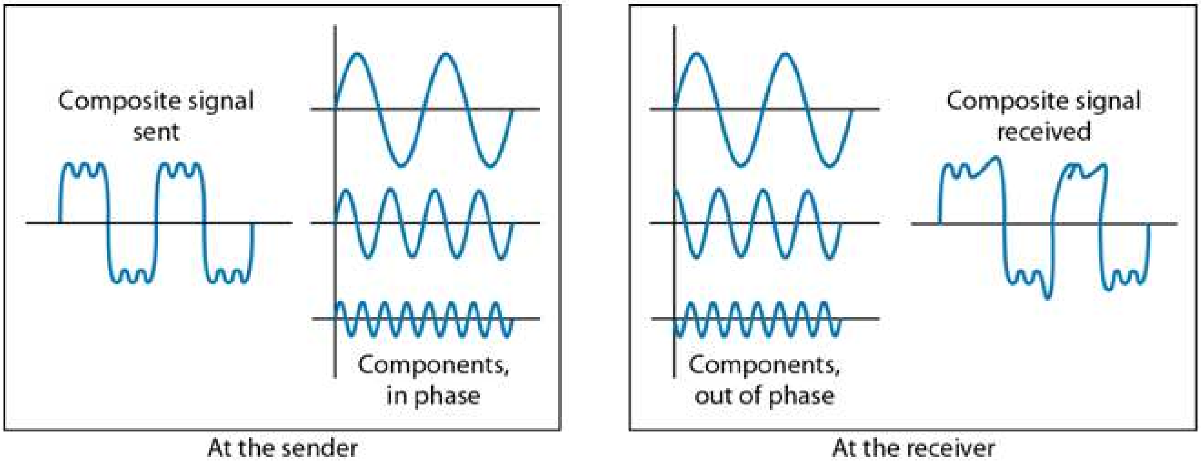
P_1 - input signal

P_2 - output signal

Distortion

- Means that the signal changes its form or shape
- Distortion occurs in composite signals
- Each frequency component has its own propagation speed traveling through a medium.
- The different components therefore arrive with different delays at the receiver.

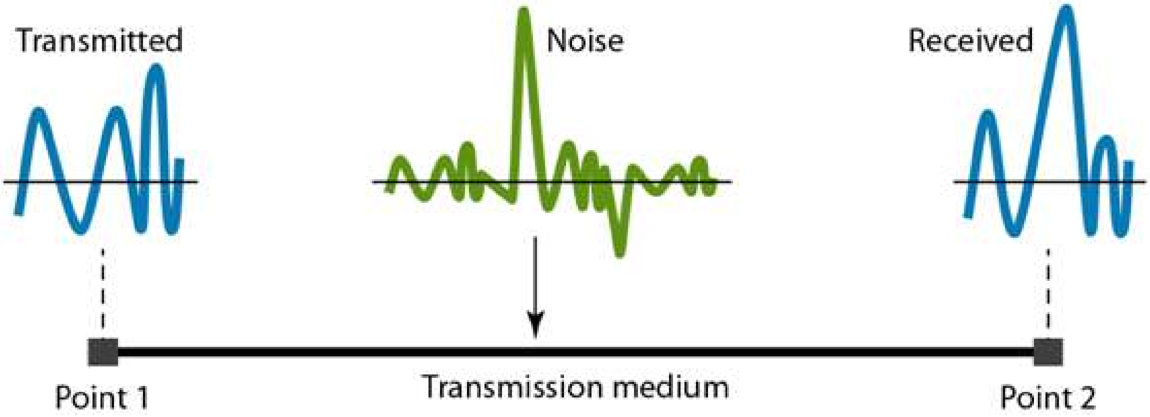
- That means that the signals have different phases at the receiver than they did at the source.



Noise

There are different types of noise

- Thermal - random noise of electrons in the wire creates an extra signal
- Induced - from motors and appliances, devices act are transmitter antenna and medium as receiving antenna.
- Crosstalk - same as above but between two wires.
- Impulse - Spikes that result from power lines, lighning, etc.



Signal to Noise Ratio (SNR)

- To measure the quality of a system the SNR is often used. It indicates the strength of the signal wrt the noise power in the system.
- It is the ratio between two powers.

It is usually given in dB and referred to as SNR_{dB}

$$SNR = \frac{average\ signal\ power}{average\ noise\ power}$$

For noise less channel

$$\text{SNR} = \frac{Signal\ \ power}{0} = \infty$$

$$\text{SNR}_{\text{dB}} = 10 \log_{10}\text{SNR} = 10 \log_{10}\infty = \infty$$