Unit 1

B230503T Data and Communication Networks

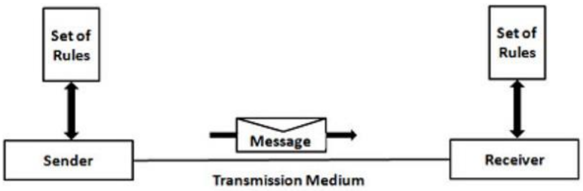
Basic Concepts:

Components of data communication, distributed processing, standards and organizations. Line configuration, topology, Transmission model and categories of networks. OSI and TCP/IP Models. Layers and their functions, comparison of models.Dig1tal Transmission: Interfaces and Modems• DTE-DCE Interfaces Modems, Cable modems.

Components of data communication: Data communication is nothing but the exchange of data between any two devices via transmission media.

Components:

There are five main components of data communication and they are explained below :



1. Message: This is the most valuable asset of a system for data communication. The message actually refers to data that is to be shared or a piece of information. A message is in any form, like a text file, an audio file, a video file, and so on.

2. Sender: Someone who can play the role of a source must be there to pass messages from source to destination. The sender plays a part of the data communication device root. A device that sends data messages is easy. The node can be a computer, mobile device, telephone, laptop, video camera, workstation, etc.

3. Receiver: It is the destination where messages sent by the source have finally arrived. It is a message-receiving system. The receiver is in the form of a computer, cell phone, workstation, etc., identical to the sender.

4. Transmission Medium: There must be something in the entire data communication process that could act as a bridge between sender and receiver. The transmission is the physical path from the sender to the recipient where the information or message passes.

The examples of transmission medium are twisted pair cable, fibre optic cable, radio waves, microwaves, etc. The transmission medium could be guided (with wires) or unguided (without wires).

5. Protocol: Different sets of rules have already been designed by the designers of communication systems to control data communication, reflecting a sort of agreement between communicating devices. These are characterized as protocols.

The protocol is also called as a set of rules regulating data communication. If two separate devices are connected, but there is no protocol between them, there will be no contact between the two devices of any sort.

Distributed Processing: Distributed processing is a setup in which multiple individual central processing units (CPU) work on the same programs, functions and systems to provide more capability for a computer and other device.

Originally, conventional microprocessors involved just one CPU on a chip. As microprocessor engineering evolved, manufacturers discovered that to speed up processes, more than one processor could be combined on a single unit. Many modern processors involve a multi-core design, such as a quad-core design pioneered by companies like Intel, where four separate processors offer extremely high speeds for program execution and logic.

Distributed processing also can be used as a rough synonym for parallel processing, in which programs are made to run more quickly with multiple processors. With the strategy of including more than one processor on a microprocessor chip, hardware users also can string multiple computers together to implement parallel processing with applications known as distributed processing software.

The distributed processing concept goes along with Moore's law, which posits that the number of transistors on an individual integrated circuit (IC) doubles every two years. As this theory has largely proven correct over the last four decades, engineering strategies like distributed processing also have added to the speed of logical devices for some amazing advances in the ability of computers to perform functional tasks.

Standards and Organizations: Data Communication is a phase of swapping data or information. This process contains a communication system that is created from hardware and software. The hardware part contains the sender and receiver devices and the intermediate devices through which the data moves. The software element includes specific rules which determine what is to be connected, how it is to be connected, and when. It is also referred to as a Protocol.

The primary standards organizations for data communication are as follows:

International Standard Organization (ISO): ISO is the international organization for standardization on a broad range of subjects. It includes mainly members from the standards committee of several administrations throughout the world.

It is important for developing models which support a high level of system compatibility, quality development, improved productivity, and decreased costs. The ISO is also responsible for supporting and integrating the work of the different standards organizations.

International Telecommunications Union-Telecommunication Sector (ITU-T): ITU-T is one of the four permanent parts of the International Telecommunications Union located in Geneva, Switzerland. It has created three sets of descriptions: the V series for modem integrating and data transmission over telephone lines, the X series for data transmission over public digital networks, email, and directory services.

The I and Q series for Integrated Services Digital Network **(ISDN)** and its continuation Broadband ISDN. ITU-T membership includes government authorities and representatives from several countries and it is the present standards organization for the United Nations.

Institute of Electrical and Electronics Engineers (IEEE): IEEE is an international professional organization established in the United States and is composed of electronics, computer, and communications engineers. It is presently the world's largest professional society with over 200,000 members. It creates communication and data processing standards with the basic goal of advancing theory, creativity, and product quality in any area associated with electrical engineering.

American National Standards Institute (ANSI): ANSI is the authorized standards agency for the United States and is the U.S voting characteristics for the ISO. ANSI is a private, non-profit organization of supplied manufacturers and users of data processing equipment and services. ANSI membership is composed of people from professional societies, market associations, governmental and regulatory bodies, and user goods.

Electronics Industry Association (EIA): EIA is a non-profit U.S. trade association that creates and recommends modern standards. EIA activities involve standards development, boosting public awareness, and promoting and it is responsible for developing the RS (recommended standard) sequence of standards for records and communications.

Telecommunications Industry Association (TIA): TIA is the leading trade association in the communications and data technology industry. It supports business development opportunities through industry development, trade promotion, trade shows, and standards development. It defines manufacturers of communications and data technology products and also supports the convergence of new communications networks.

Internet Engineering Task Force (IETF): The IETF is a large international community of network designers, operators, vendors, and researchers concerned with the development of the Internet architecture and continuous services of the Internet.

Internet Research Task Force (IRTF): The IRTF promotes research of importance to the evolution of the future Internet by generating focused, long-term and small research groups working on topics associated with Internet protocols, software, architecture, and technology.

Consultative Committee for International Telephony and Telegraphy (CCITT): CCITT is now standard organization for the United States. CCITT developer's recommended set of rules and standards for telephone and telegraph communication.

It has developed 3 set of specifications :

1. V Series for Modern Interfacing.

2. X series for Data Communication.

3. Q series for Integrated Services Digital Network(ISDN).

Standard Council of Canada (SCC): It is an official Standard Agency for Canada . It has Similar responsibilities as ANSI.

Line configuration: A network is two or more devices connected through a link. A link is a communication pathway that transfer data from one device to another. Devices can be a computer, printer or any other device that is capable to send and receive data. For visualization purpose, imagine any link as a line drawn between two points.

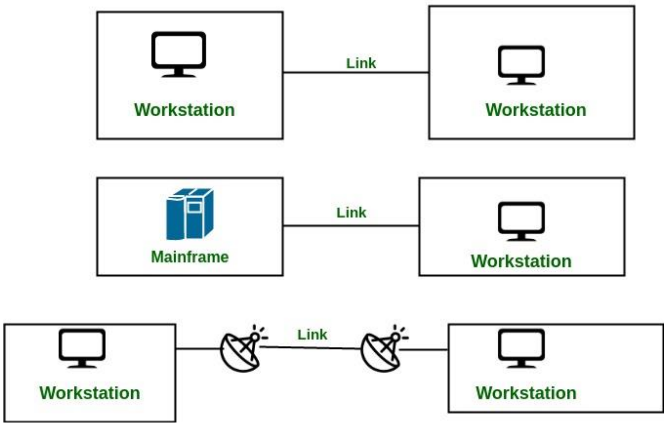
For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections:

1. Point-to-Point Connection

2. Multipoint Connection

1. Point-to-Point Connection: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use a actual length of wire or cable to connect the two end, but other options such as microwave or satellite links are also possible. Point to point network topology is considered to be one of the easiest and most conventional network topologies.

It is also the simplest to establish and understand.



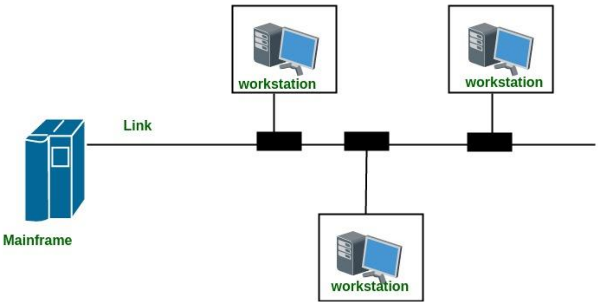
Example: Point-to-Point connection between remote control and Television for changing the channels.

2. Multipoint Connection: It is also called Multidrop configuration. In this connection two or more devices share a single link.

More than two devices share the link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line configuration:

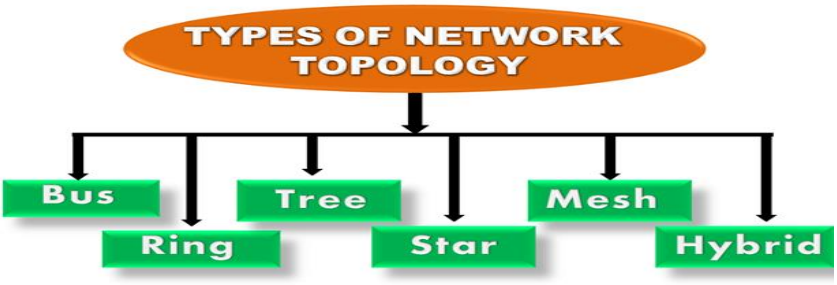
1. Spatial Sharing: If several devices can share the link simultaneously, its called Spatially shared line configuration.

2 Temporal (Time) Sharing: If users must take turns using the link , then its called Temporally shared or Time Shared Line configuration.

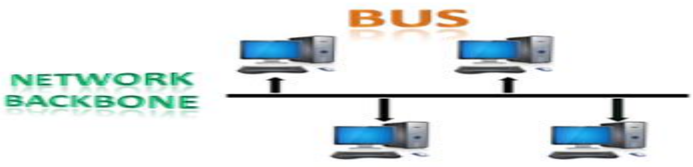


Topology: Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Computer Network Topologies: Physical topology is the geometric representation of all the nodes in a network.



Bus Topology:



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA: CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media

becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

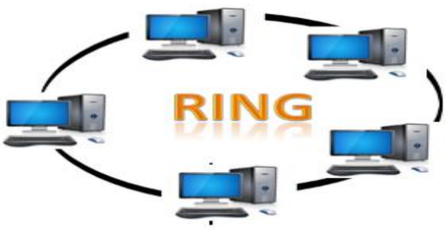
Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology:



- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.

- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
    - **Token passing:** It is a network access method in which token is passed from one node to another node.
    - **Token:** It is a frame that circulates around the network.

Working of Token passing:

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

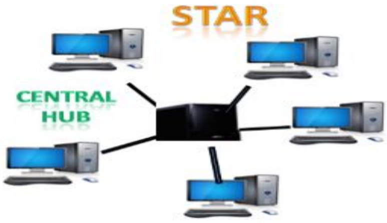
Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology:



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- **Star topology is the most popular topology in network implementation.**

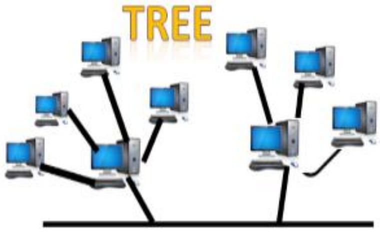
Advantages of Star topology:

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology:

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree topology:



- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

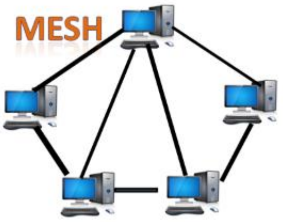
Advantages of Tree topology:

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology:

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

Mesh topology:

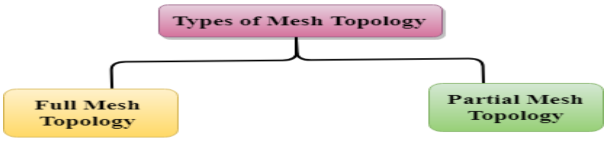


- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;**

Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology



- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

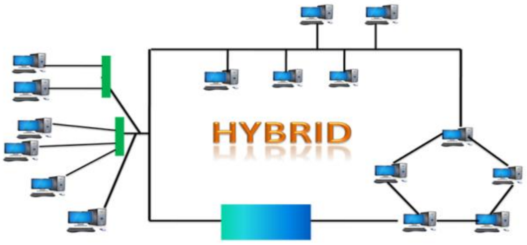
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology:

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology:



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology:

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

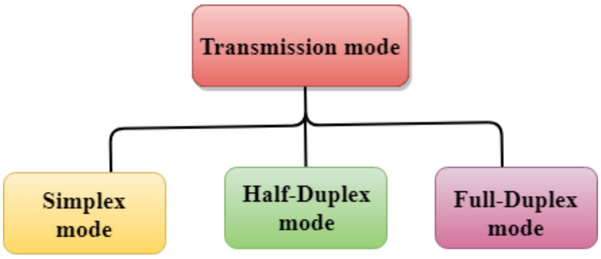
Disadvantages of Hybrid topology:

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Transmission model and categories of networks:

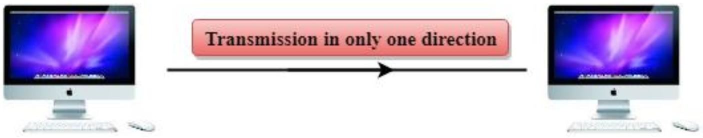
- The way in which data is transmitted from one device to another device is known as **transmission mode**.
- The transmission mode is also known as the communication mode.
- Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The transmission mode is defined in the physical layer.

The Transmission mode is divided into three categories:



- Simplex mode
- Half-duplex mode
- Full-duplex mode

Simplex mode:



- In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.

- This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.
- The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
- Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.
- The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.

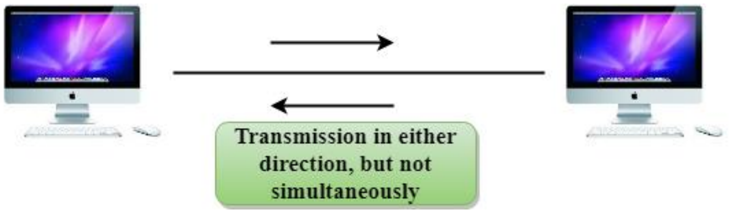
Advantage of Simplex mode:

- In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

Disadvantage of Simplex mode:

- Communication is unidirectional, so it has no inter-communication between devices.

Half-Duplex mode:



- In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
- Messages flow in both the directions, but not at the same time.
- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
- A **Walkie-talkie** is an example of the Half-duplex mode. In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.

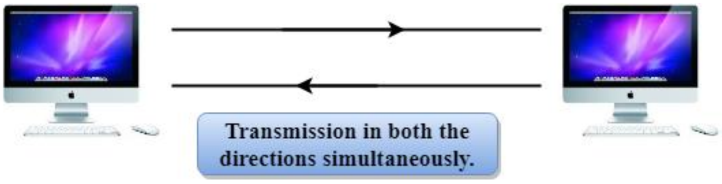
Advantage of Half-duplex mode:

- In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

- In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

Full-duplex mode:



- In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.
- Both the stations can send and receive the message simultaneously.
- Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
- The Full-duplex mode is the fastest mode of communication between devices.
- The most common example of the full-duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

Advantage of Full-duplex mode:

- Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

- If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

Differences b/w Simplex, Half-duplex and Full-duplex mode:

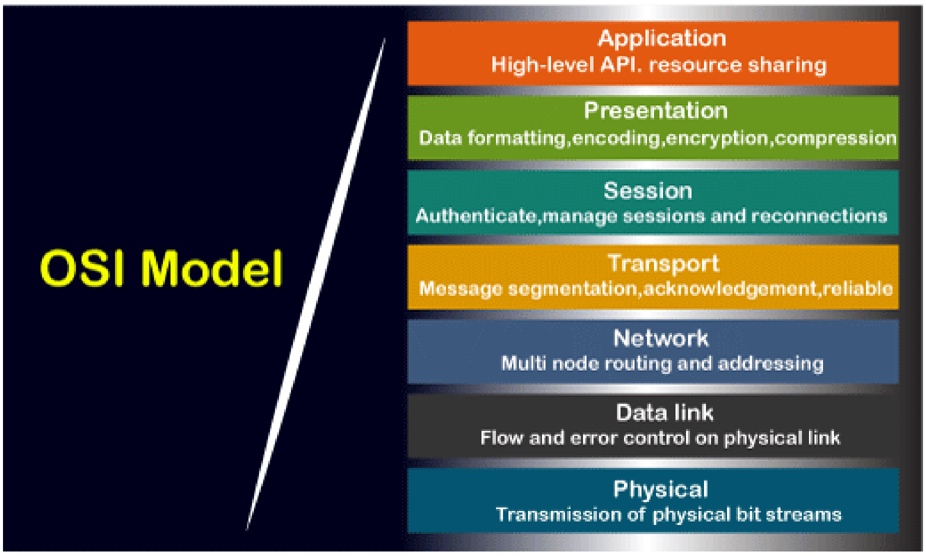
Basis for comparison	Simplex mode	Half-duplex mode	Full-duplex mode

Direction of communication	In simplex mode, the communication is unidirectional.	In half-duplex mode, the communication is bidirectional, but one at a time.	In full-duplex mode, the communication is bidirectional.
Send/Receive	A device can only send the data but cannot receive it or it can only receive the data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
Performance	The performance of half-duplex mode is better than the simplex mode.	The performance of full-duplex mode is better than the half-duplex mode.	The Full-duplex mode has better performance among simplex and half-duplex mode as it doubles the utilization of the capacity of the communication channel.
Example	Examples of Simplex mode are radio, keyboard, and monitor.	Example of half-duplex is Walkie-Talkies.	Example of the Full-duplex mode is a telephone network.

OSI and TCP/IP Models. Layers and their functions, comparison of models:

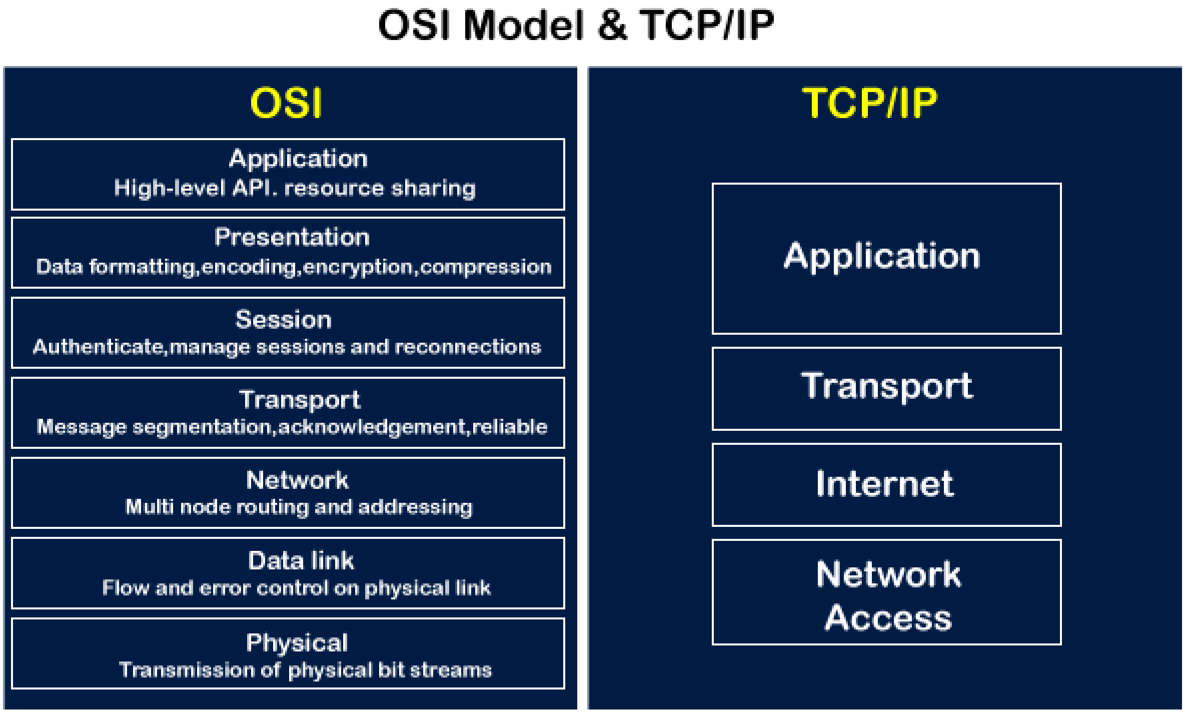
What is OSI model?

The OSI stands for Open System Interconnection, which was developed in 1980s. It is a conceptual model used for network communication. It is not implemented entirely, but it is still referenced today. This OSI model consists of seven layers, and each layer is connected to each other. The data moves down the OSI model, and each layer adds additional information. The data moves down until it reaches the last layer of the OSI model. When the data is received at the last layer of the OSI model, then the data is transmitted over the network. Once the data is reached on the other side, then the process will get reversed.


OSI Model
Application
High-level API. resource sharing
Presentation
Data formatting,encoding,encryption,compression
Session
Authenticate,manage sessions and reconnections
Transport
Message segmentation,acknowledgement,reliable
Network
Multi node routing and addressing
Data link
Flow and error control on physical link
Physical
Transmission of physical bit streams

What is TCP/IP model?

The TCP model stands for **Transmission Control Protocol,** whereas IP stands for **Internet Protocol**. A number of protocols that make the internet possibly comes under the TCP/IP model. Nowadays, we do not hear the name of the TCP/IP model much, we generally hear the name of the IPv4 or IPv6, but it is still valid. This model consists of 4 layers. Now, we will look at the diagrammatic representation of the TCP/IP model.


OSI Model & TCP/IP
OSI
Application
High-level API. resource sharing
Presentation
Data formatting,encoding,encryption,compression
Session
Authenticate,manage sessions and reconnections
Transport
Message segmentation,acknowledgement,reliable
Network
Multi node routing and addressing
Data link
Flow and error control on physical link
Physical
Transmission of physical bit streams
TCP/IP
Application
Transport
Internet
Network Access

As shown in the above diagram, the TCP/IP model has 4 layers, while the OSI model consists of 7 layers. Diagrammatically, it looks that the 4 layers of the TCP/IP model exactly fit the 7 layers of the OSI model, but this is not reality. The application layer of the TCP/IP model maps to the first three layers, i.e., application, session, and presentation layer of the OSI model. The transport layer of the TCP maps directly to the transport layer of the OSI model. The internet layer of the TCP/IP model maps directly to the network layer of the OSI model. The last two layers of the OSI model map to the network layer of the TCP/IP model. TCP/IP is the most widely used model as compared to the OSI model for providing communication between computers over the internet.

Similarities between the OSI and TCP/IP model:

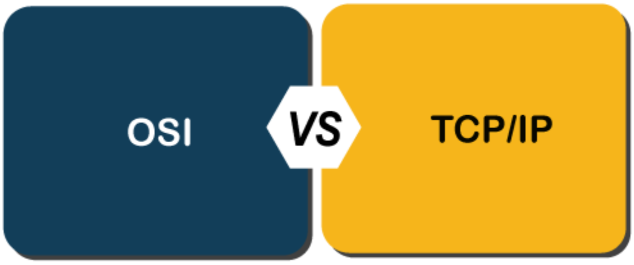
The following are the similarities between the OSI and TCP/IP model:

- **Share common architecture:** Both the models are the logical models and having similar architectures as both the models are constructed with the layers.
- **Define standards:** Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.
- **Simplified troubleshooting process:** Both models have simplified the troubleshooting process by breaking the complex function into simpler components.

- **Pre-defined standards:** The standards and protocols which are already pre-defined; these models do not redefine them; they just reference or use them. For example, the Ethernet standards were already defined by the IEEE before the development of these models; instead of recreating them, models have used these pre-defined standards.

- **Both have similar functionality of 'transport' and 'network' layers:** The function which is performed between the **'presentation'** and the **'network'** layer is similar to the function performed at the **transport** layer.

Differences between the OSI and TCP/IP model:



Let's see the differences between the OSI and TCP/IP model in a tabular form:

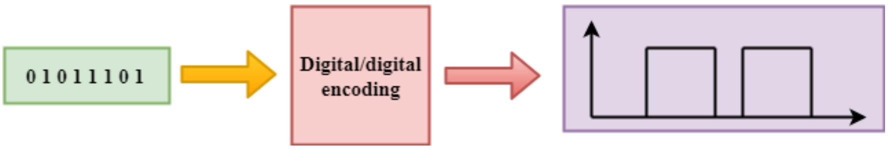
OSI Model	TCP/IP Model
It stands for **Open System Interconnection.**	It stands for **Transmission Control Protocol.**
OSI model has been developed by ISO (International Standard Organization).	It was developed by ARPANET (Advanced Research Project Agency Network).
It is an independent standard and generic protocol used as a communication gateway between the network and the end user.	It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts.
In the OSI model, the transport layer provides a guarantee for the delivery of the packets.	The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.
This model is based on a vertical approach.	This model is based on a horizontal approach.
In this model, the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool.	It is an implemented model of an OSI model.
In this model, the network layer provides both connection-oriented and connectionless service.	The network layer provides only connectionless service.

Protocols in the OSI model are hidden and can be easily replaced when the technology changes.	In this model, the protocol cannot be easily replaced.
It consists of 7 layers.	It consists of 4 layers.
OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent.	In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent.
The usage of this model is very low.	This model is highly used.
It provides standardization to the devices like router, motherboard, switches, and other hardware devices.	It does not provide the standardization to the devices. It provides a connection between various computers.

Digital Transmission: Data can be represented either in analog or digital form. The computers used the digital form to store the information. Therefore, the data needs to be converted in digital form so that it can be used by a computer.

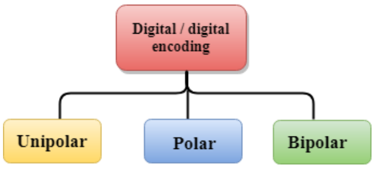
DIGITAL-TO-DIGITAL CONVERSION:

Digital-to-digital encoding is the representation of digital information by a digital signal. When binary 1s and 0s generated by the computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process is known as digital-to-digital encoding.



Digital-to-digital encoding is divided into three categories:

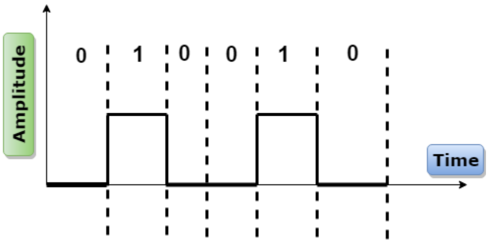
- Unipolar Encoding
- Polar Encoding
- Bipolar Encoding



Unipolar:

- Digital transmission system sends the voltage pulses over the medium link such as wire or cable.

- In most types of encoding, one voltage level represents 0, and another voltage level represents 1.
- The polarity of each pulse determines whether it is positive or negative.
- This type of encoding is known as Unipolar encoding as it uses only one polarity.
- In Unipolar encoding, the polarity is assigned to the 1 binary state.
- In this, 1s are represented as a positive value and 0s are represented as a zero value.
- In Unipolar Encoding, '1' is considered as a high voltage and '0' is considered as a zero voltage.
- Unipolar encoding is simpler and inexpensive to implement.

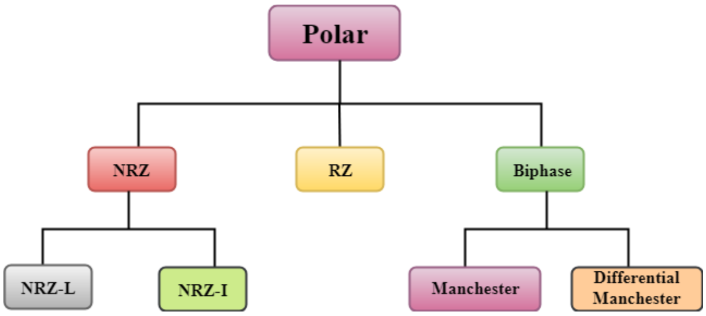


Unipolar encoding has two problems that make this scheme less desirable:

- DC Component
- Synchronization

Polar:

- Polar encoding is an encoding scheme that uses two voltage levels: one is positive, and another is negative.
- By using two voltage levels, an average voltage level is reduced, and the DC component problem of unipolar encoding scheme is alleviated.



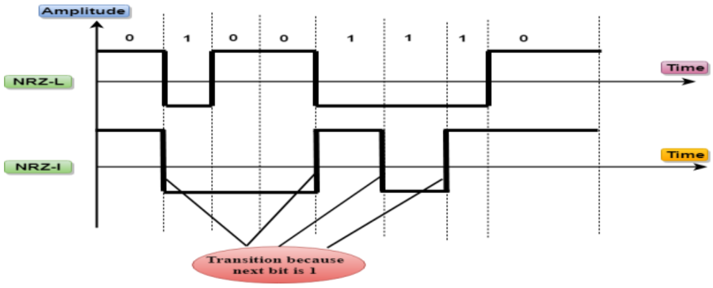
NRZ:

- NRZ stands for Non-return zero.
- In NRZ encoding, the level of the signal can be represented either positive or negative.

The two most common methods used in NRZ are:

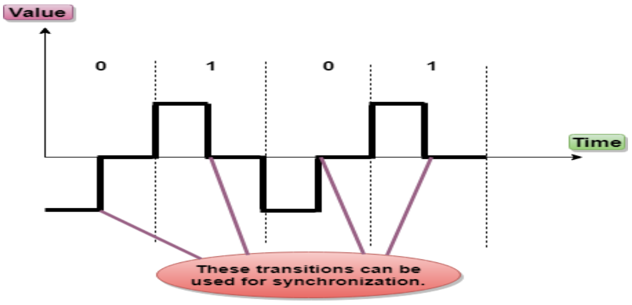
NRZ-L: In NRZ-L encoding, the level of the signal depends on the type of the bit that it represents. If a bit is 0 or 1, then their voltages will be positive and negative respectively. Therefore, we can say that the level of the signal is dependent on the state of the bit.

NRZ-I: NRZ-I is an inversion of the voltage level that represents 1 bit. In the NRZ-I encoding scheme, a transition occurs between the positive and negative voltage that represents 1 bit. In this scheme, 0 bit represents no change and 1 bit represents a change in voltage level.



RZ

- RZ stands for Return to zero.
- There must be a signal change for each bit to achieve synchronization. However, to change with every bit, we need to have three values: positive, negative and zero.
- RZ is an encoding scheme that provides three values, positive voltage represents 1, the negative voltage represents 0, and zero voltage represents none.
- In the RZ scheme, halfway through each interval, the signal returns to zero.
- In RZ scheme, 1 bit is represented by positive-to-zero and 0 bit is represented by negative-to-zero.



Disadvantage of RZ:

It performs two signal changes to encode one bit that acquires more bandwidth.

Biphase

- Biphase is an encoding scheme in which signal changes at the middle of the bit interval but does not return to zero.

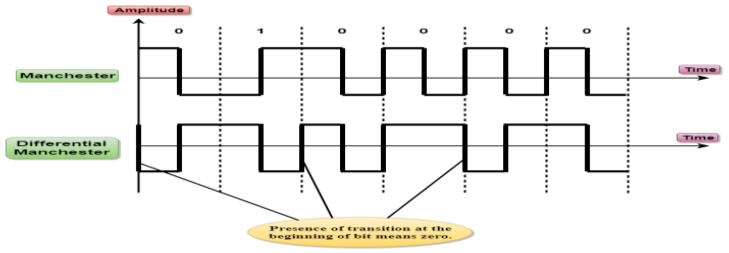
Biphase encoding is implemented in two different ways:

Manchester:

- It changes the signal at the middle of the bit interval but does not return to zero for synchronization.
- In Manchester encoding, a negative-to-positive transition represents binary 1, and positive-to-negative transition represents 0.
- Manchester has the same level of synchronization as RZ scheme except that it has two levels of amplitude.

Differential Manchester:

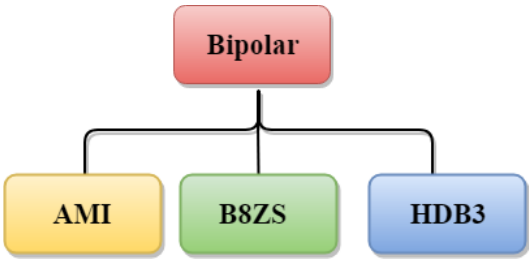
- It changes the signal at the middle of the bit interval for synchronization, but the presence or absence of the transition at the beginning of the interval determines the bit. A transition means binary 0 and no transition means binary 1.
- In Manchester Encoding scheme, two signal changes represent 0 and one signal change represent 1.



Bipolar:

- Bipolar encoding scheme represents three voltage levels: positive, negative, and zero.
- In Bipolar encoding scheme, zero level represents binary 0, and binary 1 is represented by alternating positive and negative voltages.
- If the first 1 bit is represented by positive amplitude, then the second 1 bit is represented by negative voltage, third 1 bit is represented by the positive amplitude and so on. This alternation can also occur even when the 1bits are not consecutive.

Bipolar can be classified as:



AMI:

- AMI stands for ***alternate mark inversion*** where mark work comes from telegraphy which means 1. So, it can be redefined as **alternate 1 inversion**.
- In Bipolar AMI encoding scheme, 0 bit is represented by zero level and 1 bit is represented by alternating positive and negative voltages.

Advantage:

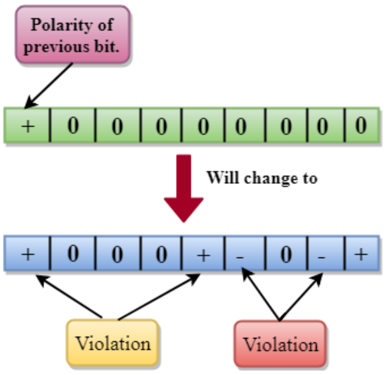
- DC component is zero.
- Sequence of 1s bits are synchronized.

Disadvantage:

- This encoding scheme does not ensure the synchronization of a long string of 0s bits.

B8ZS:

- B8ZS stands for **Bipolar 8-Zero Substitution**.
- This technique is adopted in North America to provide synchronization of a long sequence of 0s bits.
- In most of the cases, the functionality of B8ZS is similar to the bipolar AMI, but the only difference is that it provides the synchronization when a long sequence of 0s bits occur.
- B8ZS ensures synchronization of a long string of 0s by providing force artificial signal changes called violations, within 0 string pattern.
- When eight 0 occurs, then B8ZS implements some changes in 0s string pattern based on the polarity of the previous 1 bit.
- If the polarity of the previous 1 bit is positive, the eight 0s will be encoded as zero, zero, zero, positive, negative, zero, negative, positive.

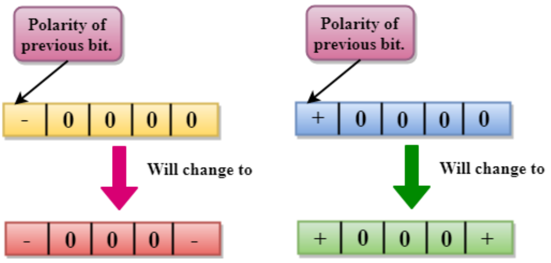


- If the polarity of previous 1 bit is negative, then the eight 0s will be encoded as zero, zero, zero, negative, positive, zero, positive, negative.

HDB3:

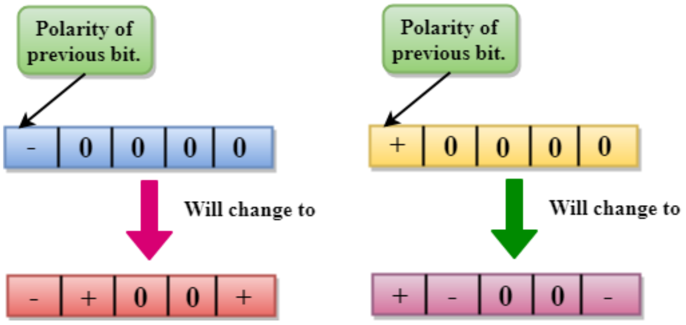
- HDB3 stands for **High-Density Bipolar 3**.
- HDB3 technique was first adopted in Europe and Japan.
- HDB3 technique is designed to provide the synchronization of a long sequence of 0s bits.
- In the HDB3 technique, the pattern of violation is based on the polarity of the previous bit.
- When four 0s occur, HDB3 looks at the number of 1s bits occurred since the last substitution.
- If the number of 1s bits is odd, then the violation is made on the fourth consecutive of 0. If the polarity of the previous bit is positive, then the violation is positive. If the polarity of the previous bit is negative, then the violation is negative.

If the number of 1s bits since the last substitution is odd.



If the number of 1s bits is even, then the violation is made on the place of the first and fourth consecutive 0s. If the polarity of the previous bit is positive, then violations are negative, and if the polarity of the previous bit is negative, then violations are positive.

If the number of 1s bits since the last substitution is even.



ANALOG-TO-DIGITAL CONVERSION:

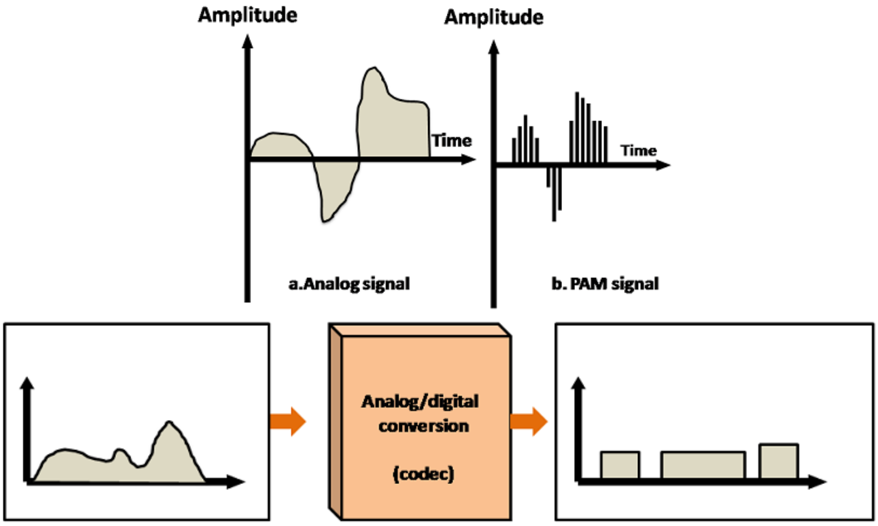
- When an analog signal is digitalized, this is called an analog-to-digital conversion.
- Suppose human sends a voice in the form of an analog signal, we need to digitalize the analog signal which is less prone to noise. It requires a reduction in the number of values in an analog message so that they can be represented in the digital stream.

- In analog-to-digital conversion, the information contained in a continuous wave form is converted in digital pulses.

Techniques for Analog-To-Digital Conversion:

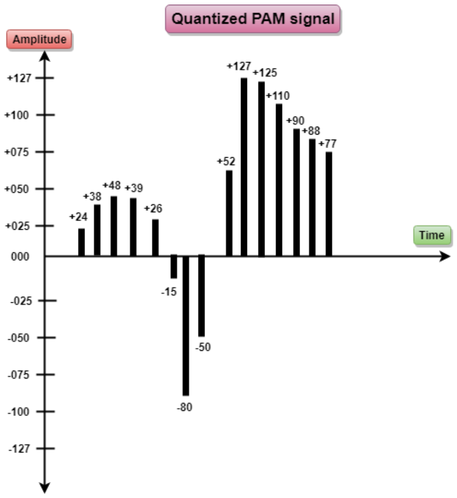
PAM:

- PAM stands for **pulse amplitude modulation**.
- PAM is a technique used in analog-to-digital conversion.
- PAM technique takes an analog signal, samples it, and generates a series of digital pulses based on the result of sampling where sampling means measuring the amplitude of a signal at equal intervals.
- PAM technique is not useful in data communication as it translates the original wave form into pulses, but these pulses are not digital. To make them digital, PAM technique is modified to PCM technique.

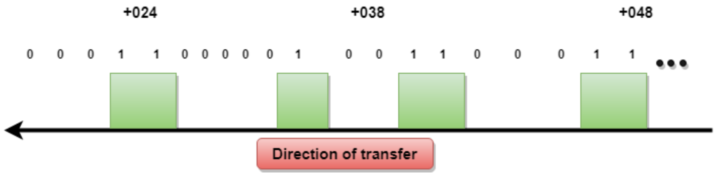


PCM

- PCM stands for **Pulse Code Modulation**.
- PCM technique is used to modify the pulses created by PAM to form a digital signal. To achieve this, PCM quantizes PAM pulses. Quantization is a process of assigning integral values in a specific range to sampled instances.
- PCM is made of four separate processes: PAM, quantization, binary encoding, and digital-to-digital encoding.

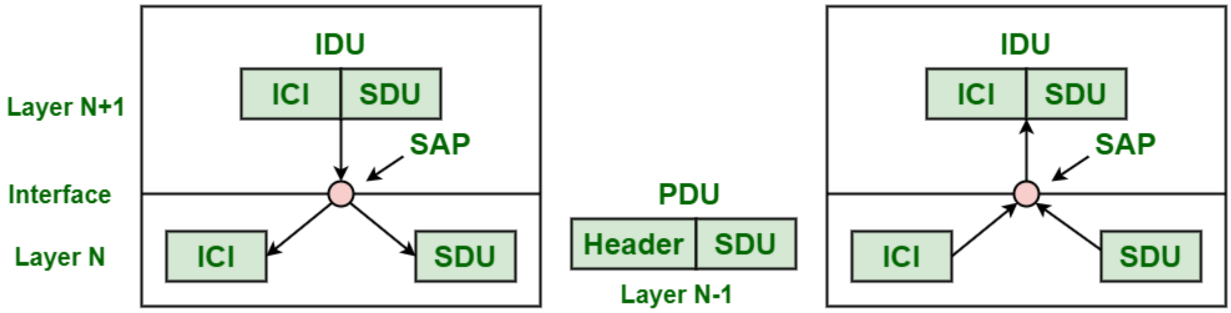


PCM:



Interfaces and Modems:

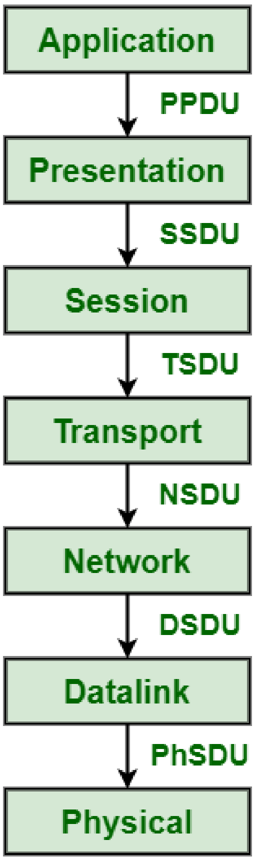
Interfaces and Services is a process that generally provides and gives a common technique for each layer to communicate with each other. Standard terminology basically required for layered networks to request and aim for the services are provided. Service is defined as a set of primitive operations. Services are provided by layer to each of layers above it. Below is diagram showing relation between layers at an interface. In diagram, layers N+1, N, and N-1 are involved and engaged in process of communication among each other.



Relationship Between Layers at an Interface

Components Involved and their Functions :

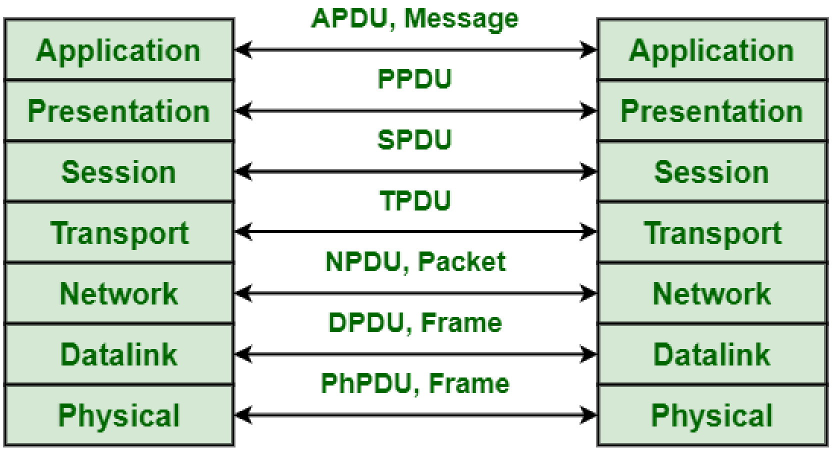
- **Service Data Unit (SDU) –** SDU is a piece of information or data that is generally passed by layer just above current layer for transmission. Unit of data or information is passed down to a lower layer from an OSI (Open System Interconnection) layer or sublayer. Data is passed with request to transmit data. SDU basically identifies or determines information that is been transferred among entities of peer layers that are not interpreted by supporting entities of lower-



Service Data Unit

layer.

- **Protocol Data Unit (PDU) –** PDU is a single unit of information or data that is transmitted or transferred among entities of peer layers of a computer network. When application data is passed down to protocol stack on its way to being transmitted all over network media, some of protocols add information and data to it at each and every level. PDU is used to represent and describe data is it gets transferred from one layer of OSI model to another



Protocol Data Unit

layer.

- **Interface Data Unit (IDU) –** IDU is used to have an agreed way of communication among two layers in a network layered architecture. It is passed from (N+1 to N).

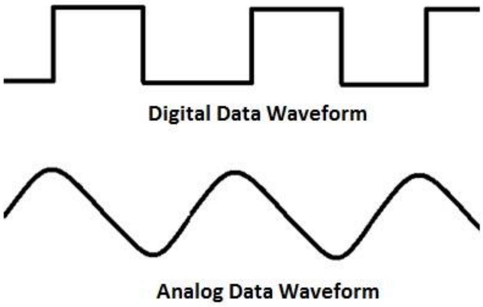
- **Service Access Point (SAP) –** SAP is generally used as an identifier label for endpoints of network in OSI networking or model. It is a data structure and identifier also for a buffer area in memory of system. It is a point in a layer of a layered architecture where a network is usually provided and where layer just above layer that provides service can probably have access to it.
- **Interface Control Information (ICI) –** ICI is a temporary parameter that is passed between N and N-1 layers to include service functions among two layers.

Benefits :

- **Increase in Compatibility –** Layered approach to networking and communication protocols generally provides and shows greater compatibility among all devices, systems, and networks that they deliver.
- **Less expensive –** Easy way of development and implementation converts to increase in an efficiency and even effectiveness that in turn converts into larger economic rationalization and very cheaper products while not compromising with quality.
- **Increase in Mobility –** Whenever we use layered and segmented strategies into architecture design, there will always be an increase in mobility.
- **Better Scalability –** Whenever we use a layered or hierarchical approach to networking protocol, design, and implementation scale much better than horizontal approach.

Modem

Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.



Digital Data Waveform

Analog Data Waveform

The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − **modulator** and **demodulator**. The **modulator** converts digital data into analog data when the data is being sent by the computer. The **demodulator** converts analog data signals into digital data when it is being received by the computer.

Types of Modem

Modem can be categorized in several ways like direction in which it can transmit data, type of connection to the transmission line, transmission mode, etc.

Depending on direction of data transmission, modem can be of these types −

- **Simplex** − A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).
- **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
- **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

RJ45 Connector

RJ45 is the acronym for **Registered Jack 45. RJ45 connector** is an 8-pin jack used by devices to physically connect to **Ethernet** based **local area networks (LANs)**. **Ethernet** is a technology that defines protocols for establishing a LAN. The cable used for Ethernet LANs are twisted pair ones and have **RJ45 connector pins** at both ends. These pins go into the corresponding socket on devices and connect the device to the network.

Ethernet Card

Ethernet card, also known as **network interface card (NIC)**, is a hardware component used by computers to connect to **Ethernet LAN** and communicate with other devices on the LAN. The earliest **Ethernet cards** were external to the system and needed to be installed manually. In modern computer systems, it is an internal hardware component. The NIC has **RJ45 socket** where network cable is physically plugged in.

Ethernet card speeds may vary depending upon the protocols it supports. Old Ethernet cards had maximum speed of **10 Mbps**. However, modern cards support fast Ethernets up to a speed of **100 Mbps**. Some cards even have capacity of **1 Gbps**.

Router

A **router** is a **network layer** hardware device that transmits data from one LAN to another if both networks support the same set of protocols. So a **router** is typically connected to at least two LANs and the **internet service provider** (ISP). It receives its data in the form of **packets**, which are **data frames** with their **destination address** added. Router also strengthens the signals before transmitting them. That is why it is also called **repeater**.

Routing Table

A router reads its routing table to decide the best available route the packet can take to reach its destination quickly and accurately. The routing table may be of these two types −

- **Static** − In a static routing table the routes are fed manually. So it is suitable only for very small networks that have maximum two to three routers.
- **Dynamic** − In a dynamic routing table, the router communicates with other routers through protocols to determine which routes are free. This is suited for larger networks where manual feeding may not be feasible due to large number of routers.

Switch

Switch is a network device that connects other devices to **Ethernet** networks through **twisted pair** cables. It uses **packet switching** technique to **receive, store** and **forward data packets** on the network. The switch maintains a list of network addresses of all the devices connected to it.

On receiving a packet, it checks the destination address and transmits the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full duplex mode

Data transmission speed in switches can be double that of other network devices like hubs used for networking. This is because switch shares its maximum speed with all the devices connected to it. This helps in maintaining network speed even during high traffic. In fact, higher data speeds are achieved on networks through use of multiple switches.

Gateway

Gateway is a network device used to connect two or more dissimilar networks. In networking parlance, networks that use different protocols are **dissimilar networks**. A gateway usually is a computer with multiple **NICs** connected to different networks. A gateway can also be configured completely using software. As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.

Gateway uses **packet switching** technique to transmit data from one network to another. In this way it is similar to a **router**, the only difference being router can transmit data only over networks that use same protocols.

Wi-Fi Card

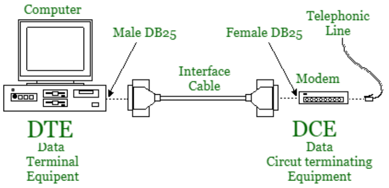
Wi-Fi is the acronym for **wireless fidelity. Wi-Fi technology** is used to achieve **wireless connection** to any network. **Wi-Fi card** is a **card** used to connect any device to the local network wirelessly. The physical area of the network which provides internet access through Wi-Fi is called **Wi-Fi hotspot**. Hotspots can be set up at home, office or any public space. Hotspots themselves are connected to the network through wires.

A **Wi-Fi card** is used to add capabilities like **teleconferencing, downloading** digital camera images, **video chat**, etc. to old devices. Modern devices come with their in-built **wireless network adapter**.

DTE-DCE Interfaces Modems:

1. Data Terminal Equipment (DTE): It includes any unit that functions either as a source of or as a destination for binary digital data. At physical layer, it can be a terminal, microcomputer, computer, printer, fax, machine or any other device that generates or consumes digital data. DTEs do not often communicate information but need an intermediary to be able to communicate.

2. Data Circuit Terminating Equipment (DCE): It includes any functional unit that transmit or receives data in form of an analog or digital signal through a network. At physical layer, a DCE takes data generated by a DTE, converts them to an appropriate signal, and then introduces signal onto telecommunication link. Commonly used DCEs at this layer include modems. In any network, a DTE generates digital data and passes them to a DCE. DCE converts that data to a form acceptable to transmission medium and sends converted signal to another DCE on network. The second DCE takes signal off line, converts it to a form usable by its DTE, and delivers it.

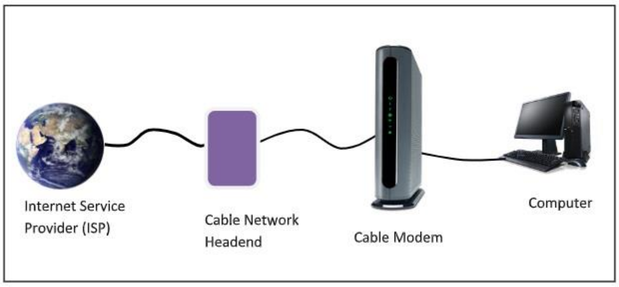


Difference between DTE and DCE :

SR.NO	DTE	DCE
1	DTE stands for Data Termination Equipment.	DCE stands for Data Communication Equipment.
2	It is a device that is an information source or an information sink.	It is a device used as an interface between a DTE.
3	DTE is concerned with source or destination of data.	DCE is concerned with communications aspect of data.
4	It produces data and transfers them to a DCE, with essential control characters.	It converts signals to a format appropriate to transmission medium and introduces it onto network line.
5	It is connected through help of a DCE network.	DCE network acts as a medium for two DTE networks.
6	Examples of DTE include computers, printers and routers, etc.	Examples of DCE include modem, ISDN adaptors, satellites and network interface cards, etc.

Cable modems: Cable modem is a hardware device that is used to connect the computer with the Internet Service Provider (ISP) through the local cable TV line. It has two interfaces – one to the cable TV network outlet and the other to a computer or television or set-top box.

Configuration: Cable modems used to be proprietary in the initial days and had to be installed by the cable company. Nowadays, cable modems of open standards are available that can be personally installed by the user. The standard is called Data over Cable Service Interface Spectrum (DOSCIS). The modem to computer interface is normally Ethernet or USB. The interface between the modem and the cable network outlet supports FDM, TDM, and CDMA so that the bandwidth of the cable can be shared among the subscribers.



Establishment of Connection: After a cable modem is plugged on to the cable TV network, it scans the downstream channels for a particular packet that is periodically sent over the network. On detecting it, the modem announces its presence over the network. If its authentication criteria are met, then it is assigned for both upstream and downstream communication.

Channels for Communication: For downstream data, 6HMz or 8MHz channels are used which are modulated using QAM-64. This gives the data rate of 36Mbps. For upstream data, there is more radio-frequency noise. Consequently, the data rate is around 9Mbps.

Communication Method: For sharing upstream data, time division multiplexing (TDM) is used. TDM divides the time in minislots, which are assigned to subscribers who want to send the data. When a computer has data to send, it sends data packets to the cable modem. The modem requests the number of minislots needed to send the data. If the request is granted, the modem receives an acknowledgment along with the allotted number of slots. The modem then transmits the data packets accordingly.