MALLA REDDY ENGINEERING COLLEGE (AUTONOMOUS)

Maisammaguda, Dhulapally (post via kompally), Secunderabad – 500100

Department of Computer Science and Engineering

COMPUTER NETWORKS

UNIT-1

MODULE I: Basics of Networking and Physical layer Basics of Networking - Components – Direction of Data flow – Networks – Components and Categories – Types of Connections – Topologies –Protocols and Standards – ISO / OSI model, TCP/IP model. Physical layer - Digital transmission, Multiplexing, Transmission Media, Switching, Circuit Switched Networks, Datagram Networks, Virtual Circuit Networks.

DATA COMMUNICATION

- Data Communication is a process of exchanging data or information
- In case of computer networks this exchange is done between two devices over a transmission medium.
- This process involves a communication system which is made up of hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes. The software part involves certain rules which specify what is to be communicated, how itis to be communicated and when. It is also called as a Protocol.
- The following sections describe the fundamental characteristics that are important for the effective working ofdata communication process and are followed by the components that make up a data communications system.

Characteristics of Data Communication

The effectiveness of any data communications system dependsupon the following four fundamental characteristics:

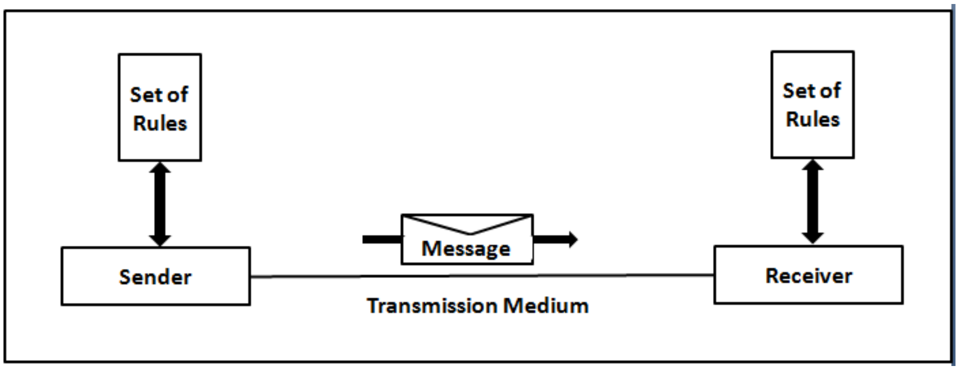
1. **Delivery**: The data should be delivered to the correct destination and correct user.
2. **Accuracy**: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the

delivered data.

3. **Timeliness**: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
4. **Jitter**: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

Components of Data Communication

A Data Communication system has five components as



shown in the diagram below:

1. Message
Message is the information to be communicated by the sender to the receiver.

2. Sender
The sender is any device that is capable of sending the data (message).

3. Receiver
The receiver is a device that the sender wants to communicate the data (message).

4. Transmission Medium

It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.

5. Protocol

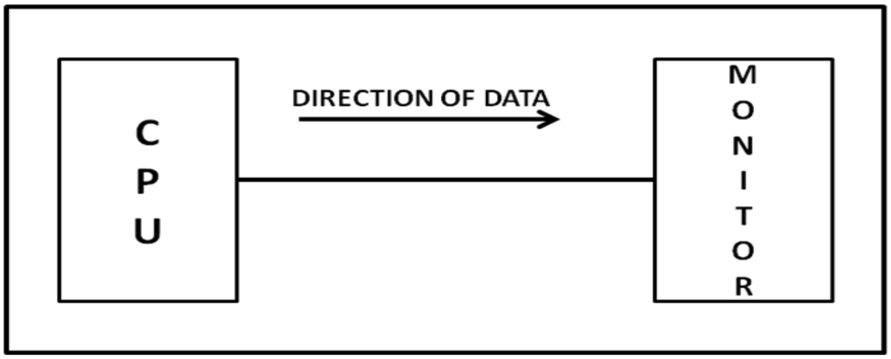
It is an agreed upon set or rules used by the sender and receiver to communicate data. A protocol is a set of rules that governs data communication. A Protocol is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language

DATA FLOW

Two devices communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways.

1. Simplex
2. Half Duplex
3. Full Duplex

Simplex



- In Simplex, communication is unidirectional
- Only one of the devices sends the data and the other oneonly receives the data.
- Example: in the above diagram: a cpu send data while amonitor only receives data.

Half Duplex

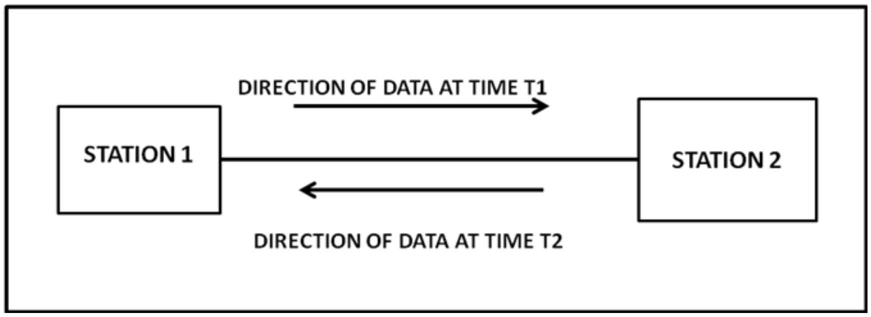


Figure: Half Duplex Mode of Communication

- In half duplex both the stations can transmit as well as receive but not at the same time.
- When one device is sending other can only receive and vice-versa (as shown in figure above.)
  - Example: A walkie-talkie

Full Duplex

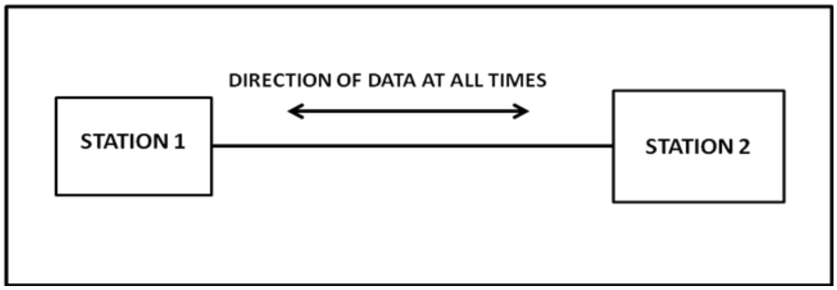


Figure: Full Duplex Mode of Communication

- In Full duplex mode, both stations can transmit and receiveat the same time.
- Example: mobile phones

Computer Network Components

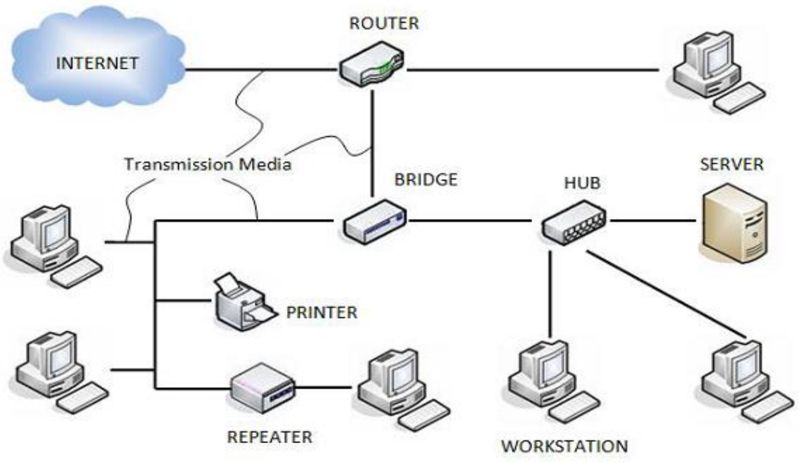
Computer Networks are used for data communications

Definition:

A computer network can be defined as a collection of nodes. A node can be any device capable of transmitting or receiving data. The communicating nodes have to be connected by communication links.

Computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.

The following figure shows a network along with its components –

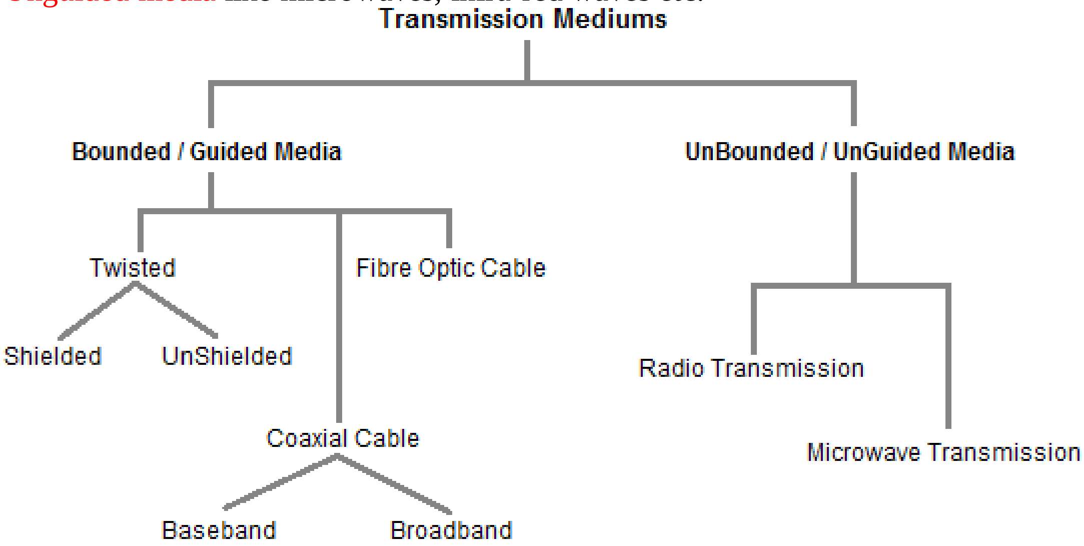


COMPUTER NETWORK COMPONENTS

Hardware Components

- **Servers** −Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.
- **Clients** − Clients are computers that request and receive service from the servers to access and use the network resources.
- **Peers** − Peers are computers that provide as well as receive services from other peers in a workgroup network.
- **Transmission Media** − Transmission media are the channels through which data is transferred from one device to another in a network.
  Transmission media may be
  Guided media like coaxial cable, fibre optic cables etc;

Or maybe
Unguided media like microwaves, infra-red waves etc.



- **Connecting Devices** − Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:
  a. Routers
  b. Bridges
  c. Hubs
  d. Repeaters
  e. Gateways
  f. Switches

Software Components:

- **Networking Operating System** − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
- **Protocol Suite** − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are −
  - a. OSI Model (Open System Interconnections)
  - b. TCP / IP Model

Types of Computer Networks

A computer network is a cluster of computers over a shared communication path that works for the purpose of sharing resources from one computer to another, provided by or located on the network nodes.

Some of the uses of computer networks are the following:

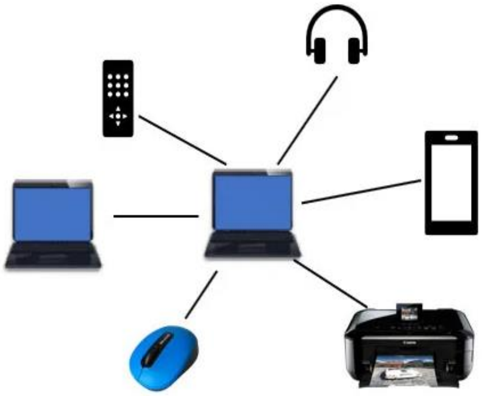
- Communicating using email, video, instant messaging, etc.
- Sharing devices such as printers, scanners, etc.
- Sharing files
- Sharing software and operating programs on remote systems
- Allowing network users to easily access and maintain information

Types of Computer Networks

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Wide Area Network (WAN)
4. Wireless Local Area Network (WLAN)
5. Campus Area Network (CAN)
6. Metropolitan Area Network (MAN)
7. Storage Area Network (SAN)
8. System-Area Network (SAN)
9. Passive Optical Local Area Network (POLAN)
10. Enterprise Private Network (EPN)
11. Virtual Private Network (VPN)
12. Home Area Network (HAN)

1. PAN (Personal Area Network)

PAN is expanded as Personal Area Network is configured in a person in range of approximately ten meters and is mostly employed for connecting internet range for personal usage. It has the coverage range to thirty meters. Personal equipment includes desktop, laptop, smart phones, game stations, electronic gadgets, and music players.

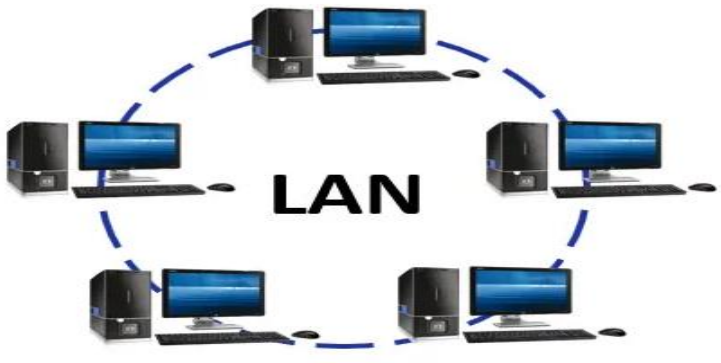


There are two types of Personal Area Network:

- Wireless Personal Area Network
- Wired Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is configured is based on wireless technologies like Bluetooth and Wi-Fi which falls over a limited range network.

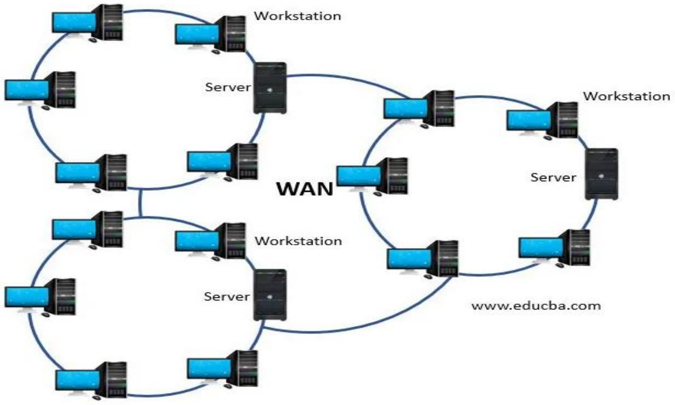
2. LocalAreaNetwork(LAN):
LAN is the most frequently used network. A LAN is a computer network that connects computers together through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi.
Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



2. Wide Area Network (WAN)

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other.

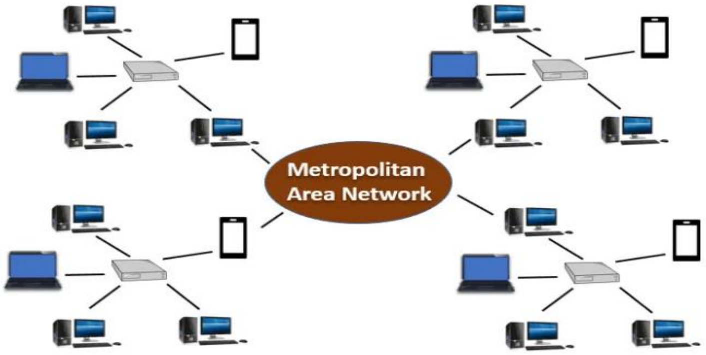
The most common example of WAN is the Internet.



Metropolitan Area Network (MAN) :

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town or metropolitan area.

Examples of MAN are networking in towns, cities, a single large city, large area within multiple buildings, etc.

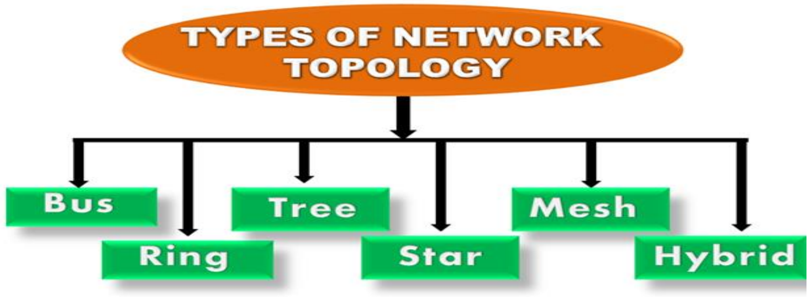


Topologies

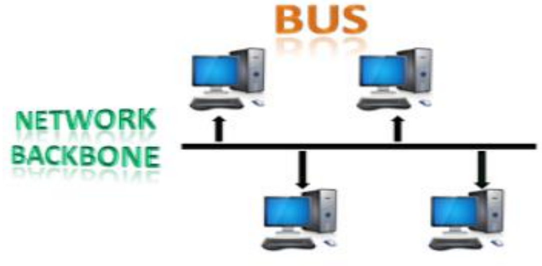
The arrangement with which computer systems or network devices are connected to each other.

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.

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.

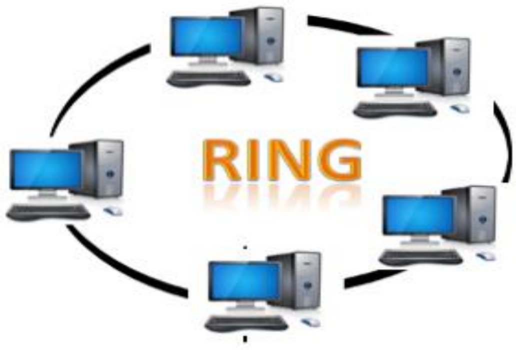
Difficult troubleshooting: It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.

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 move 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:

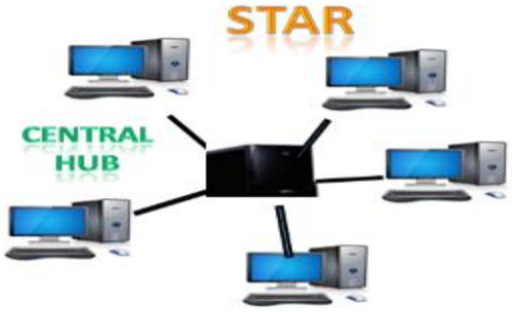
Difficult troubleshooting: It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.

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.

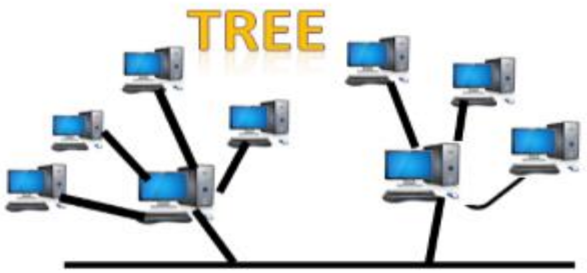
High data speeds: It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

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.

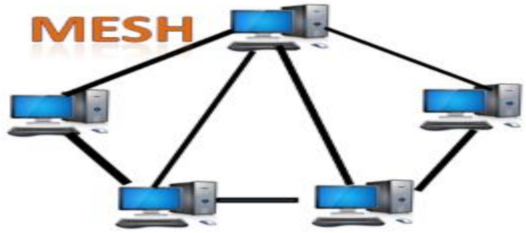
Cable: Sometimes cable routing becomes difficult when a significant amount of routing is required.

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.

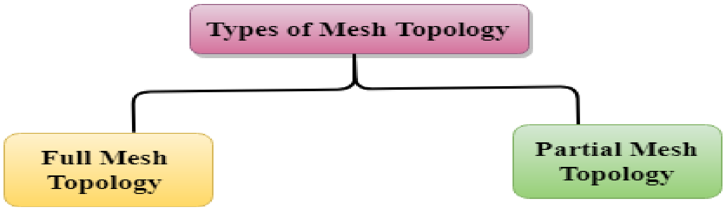
Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;**

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.

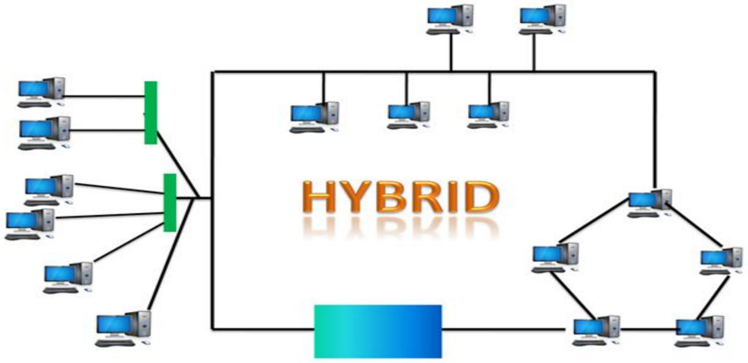
Fast Communication: Communication is very fast between the nodes.

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

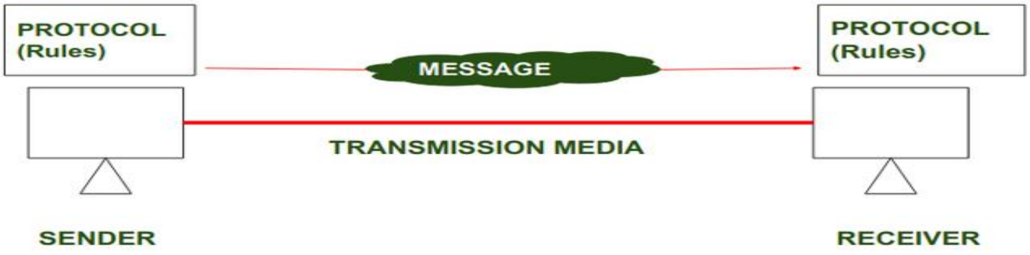


The combination of various different topologies is known as **Hybrid topology**.
A Hybrid topology is a connection between different links and nodes to transfer the data.
When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with 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.

Protocol and Standard in Computer Networks

In Order to make communication successful between devices, some rules and procedures should be agreed upon at the sending and receiving ends of the system. Such rules and procedures are called as Protocols. Different types of protocols are used for different types of communication.

1. Syntax
2. Semantics
3. Timing



Standards:

- A protocol is basically a synonym for the rule. In Computer Networks, basically, A Protocol is a set of rules that mainly govern data communications. The protocol mainly defines what is communicated, how it is communicated, and when it is communicated.
- Standards are the set of rules for data communication that are needed for exchange of information among devices. It is important to follow Standards which are created by various Standard Organization like IEEE, ISO, and ANSI etc.

Types of Standards:

1. De Facto Standard.
2. De Jure Standard.

De Facto Standard: The meaning of the work" De Facto" is" By Fact" or "By Convention". These are the standard s that have not been approved by any Organization, but have been adopted as Standards because of its widespread use. Also, sometimes these standards are often established by Manufacturers.

For example: Apple and Google are two companies which established their own rules on their products which are different. Also they use some same standard rules for manufacturing for their products.

De Jure Standard: The meaning of the word "De Jure" is "By Law" or "By Regulations" . Thus, these are the standards that have been approved by officially recognized body like ANSI, ISO, and IEEE etc. These are the standard which is important to follow if it is required or needed.

For example : All the data communication standard protocols like SMTP , TCP , IP , UDP etc. are important to follow the same when we needed them.

Why of OSI Model? (All People Seem To Need Data Processing)

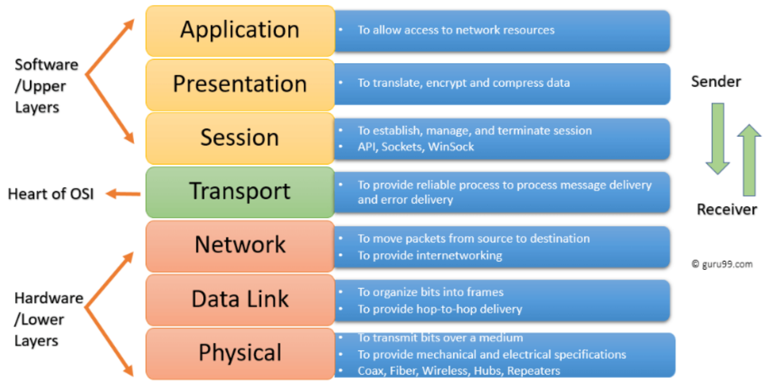
- Helps you to understand communication over a network
- Troubleshooting is easier by separating functions into different network layers.
- Helps you to understand new technologies as they are developed.
- Allows you to compare primary functional relationships on various network layers.

History of OSI Model

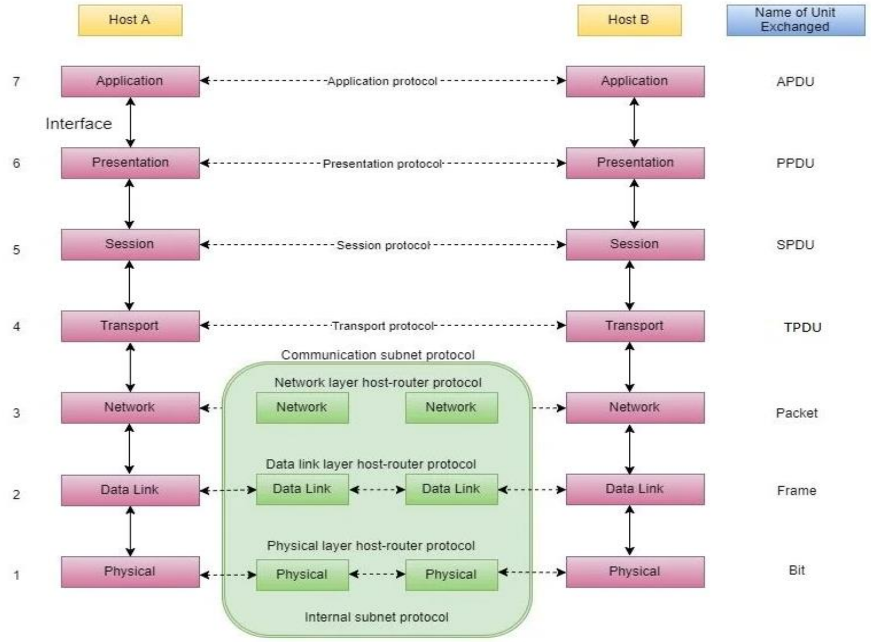
Here are essential landmarks from the history of OSI model:

- In the late 1970s, the ISO conducted a program to develop general standards and methods of networking.
- In 1973, an Experimental Packet Switched System in the UK identified the requirement for defining the higher-level protocols.
- In the year 1983, OSI model was initially intended to be a detailed specification of actual interfaces.
- In 1984, the OSI architecture was formally adopted by ISO as an international standard

7 Layers of the OSI Model


Software
/Upper
Layers
Heart of OSI
Hardware
/Lower
Layers
Application
Presentation
Session
Transport
Network
Data Link
Physical
• To allow access to network resources
• To translate, encrypt and compress data
• To establish, manage, and terminate session
• API, Sockets, WinSock
• To provide reliable process to process message delivery and error delivery
• To move packets from source to destination
• To provide internetworking
• To organize bits into frames
• To provide hop-to-hop delivery
• To transmit bits over a medium
• To provide mechanical and electrical specifications
• Coax, Fiber, Wireless, Hubs, Repeaters
Sender
Receiver
© guru99.com

Network Layers Diagram



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 transmitting individual bits from one node to the next. 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 as follows:

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 topology.
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**.

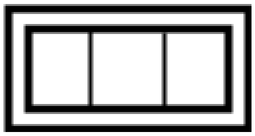
2. Data Link Layer (DLL) (Layer 2) :

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 sublayers:

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

The packet received from the 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, the Data link layer adds physical addresses (MAC address) of the 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 the amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

** Packet in Data Link layer is referred to 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.

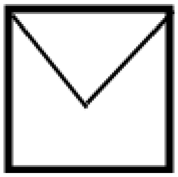
3. Network Layer (Layer 3) :

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

* *Segment* in Network layer is referred to as **Packet**.



** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

The transport layer provides services to the application layer and takes services from the 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. The transport layer also provides the acknowledgement 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 numbers in its header and forwards the segmented data to the Network Layer.

Note: *The sender needs 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 ports 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 as follows:

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments 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 the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

A. Connection-Oriented Service: It is a three-phase process that includes
– Connection Establishment
– Data Transfer
– Termination / disconnection

In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

B. Connectionless 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 connectionless 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):

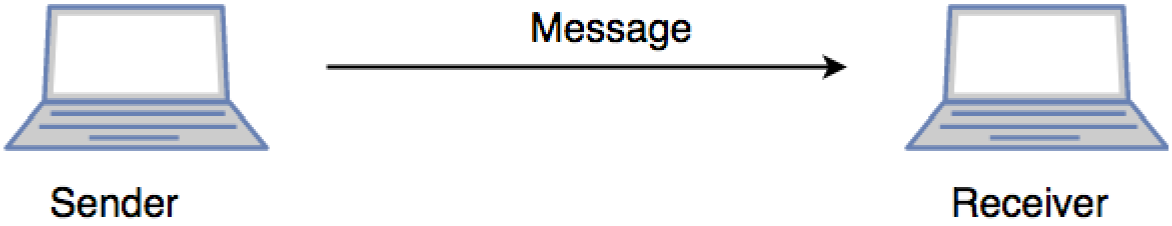
This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.
The functions of the session layer are :

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 synchronization points into the data. These synchronization points 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 the 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 us 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):

The 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:

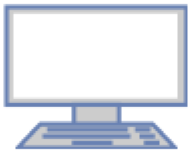
- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** 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 the 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.

Example: Application – Browsers, Skype Messenger, etc.

***Application Layer is also called Desktop Layer.*

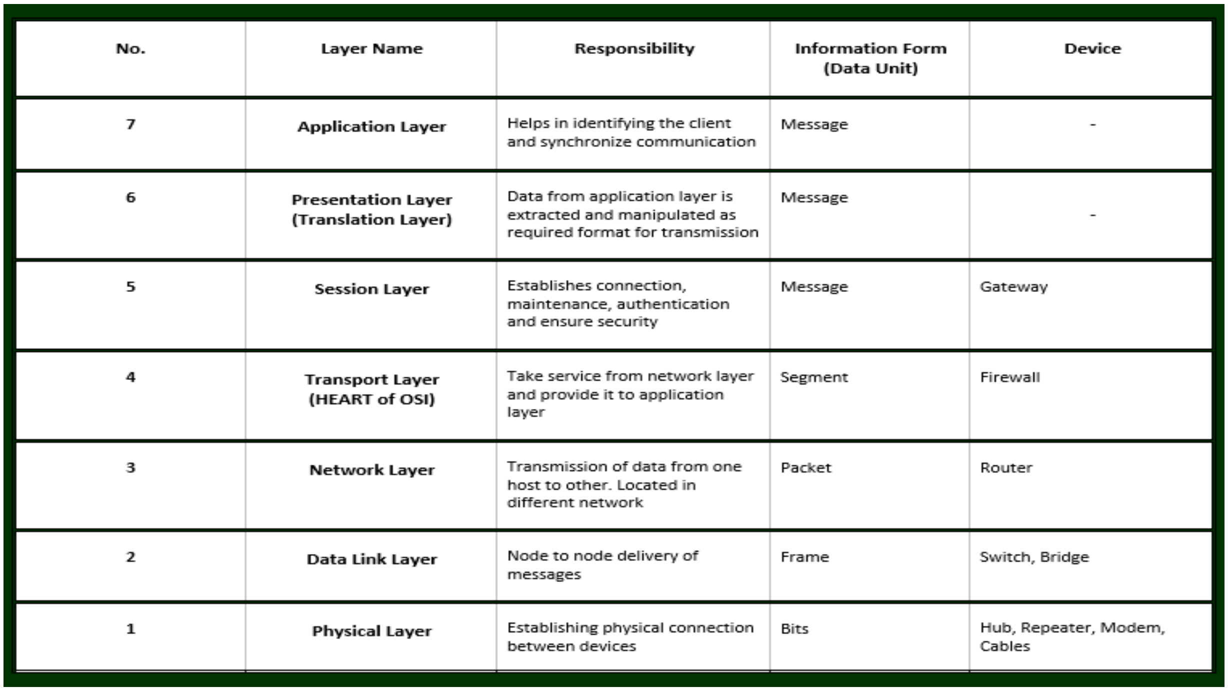


The functions of the Application layer are :

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 on the Internet because of its late invention. The current model being used is the TCP/IP model.

OSI model in a nutshell



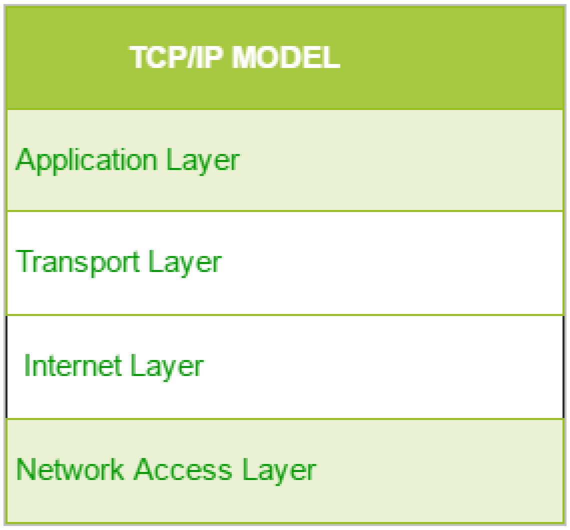
No.	Layer Name	Responsibility	Information Form (Data Unit)	Device
7	**Application Layer**	Helps in identifying the client and synchronize communication	Message	-
6	**Presentation Layer (Translation Layer)**	Data from application layer is extracted and manipulated as required format for transmission	Message	-
5	**Session Layer**	Establishes connection, maintenance, authentication and ensure security	Message	Gateway
4	**Transport Layer (HEART of OSI)**	Take service from network layer and provide it to application layer	Segment	Firewall
3	**Network Layer**	Transmission of data from one host to other. Located in different network	Packet	Router
2	**Data Link Layer**	Node to node delivery of messages	Frame	Switch, Bridge
1	**Physical Layer**	Establishing physical connection between devices	Bits	Hub, Repeater, Modem, Cables

TCP/IP Model

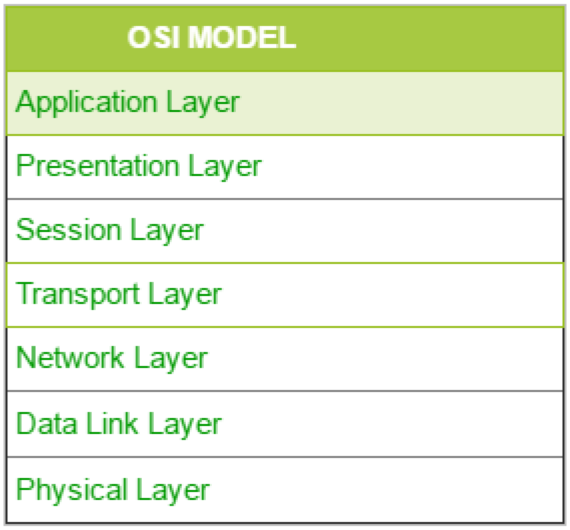
The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.

TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

Digital Transmission in Computer Network

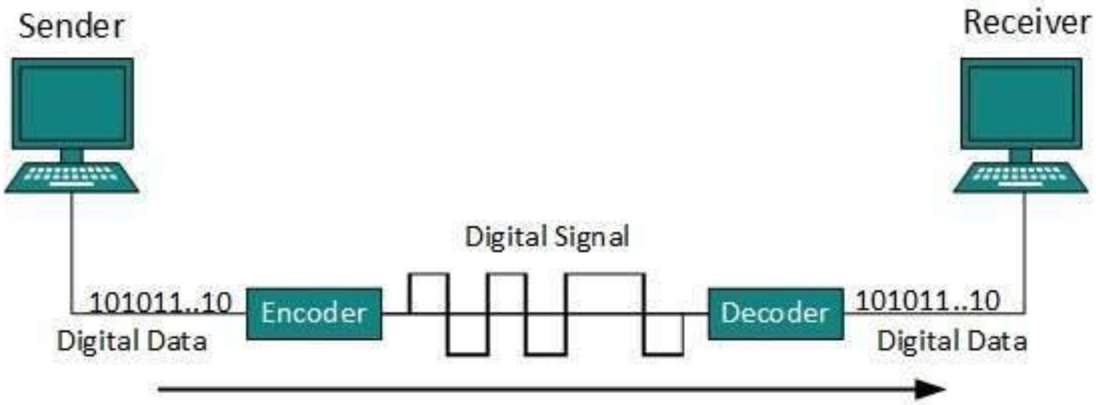
Data or information can be stored in two ways, analog and digital. For a computer to use the data, it must be in discrete digital form. Similar to data, signals can also be in analog and digital form. To transmit data digitally, it needs to be first converted to digital form.

Digital-to-Digital Conversion

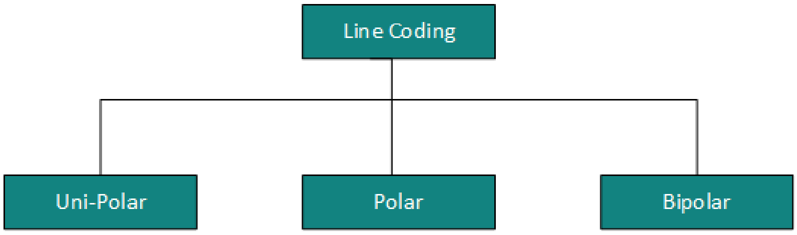
This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s.

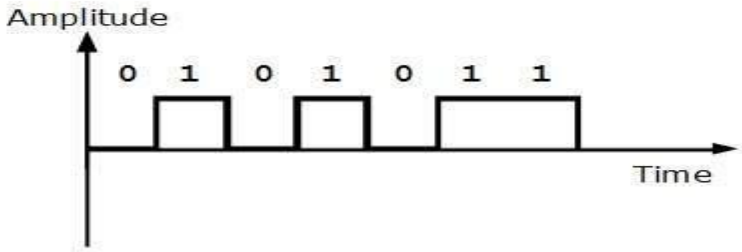


Digital signal is denoted by discreet signal, which represents digital data.There are three types of line coding schemes available:



Uni-polar Encoding

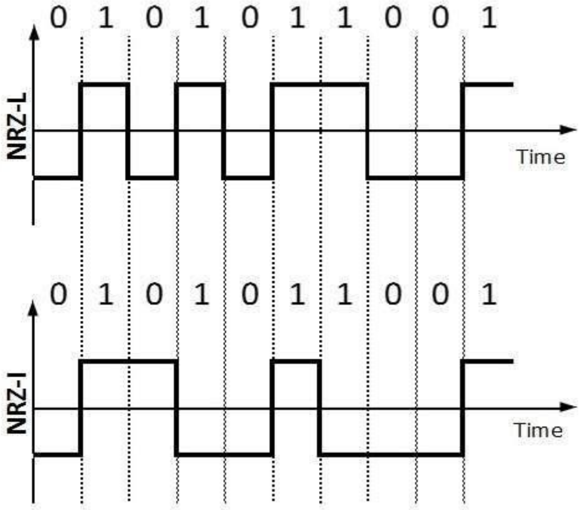
Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.



Polar Encoding

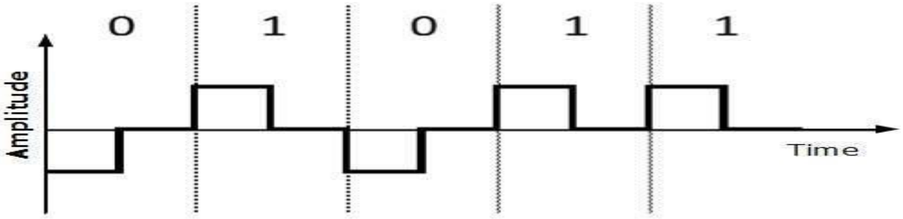
Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

- Polar Non-Return to Zero (Polar NRZ)
  It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.
  NRZ scheme has two variants: NRZ-L and NRZ-I.



  NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

- Return to Zero (RZ)
  Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver’s clock are not synchronized.

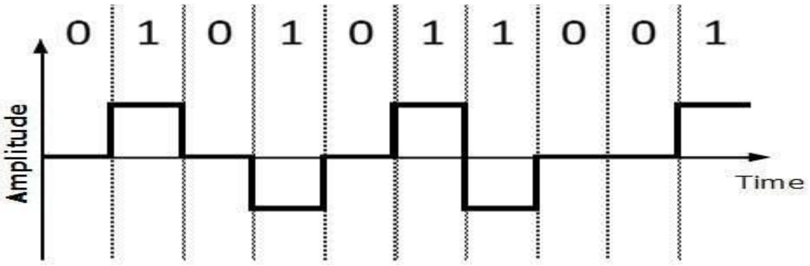


RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

- Manchester
  This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.
- Differential Manchester
  This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Block Coding

To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.

Block coding is represented by slash notation, mB/nB.Means, m-bit block is substituted with n-bit block where n > m. Block coding involves three steps:

- Division,
- Substitution
- Combination.

After block coding is done, it is line coded for transmission.

Analog-to-Digital Conversion

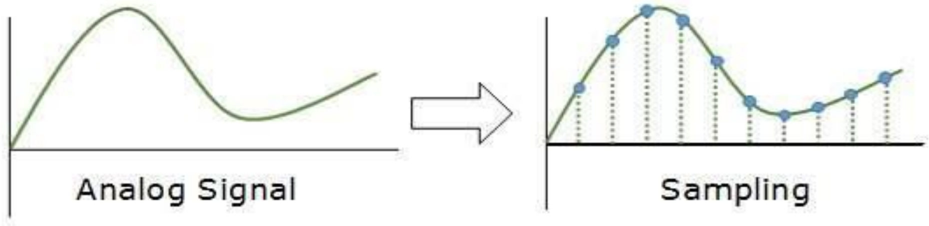
Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog to digital conversion.

Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To convert analog wave into digital data, we use Pulse Code Modulation (PCM).

PCM is one of the most commonly used method to convert analog data into digital form. It involves three steps:

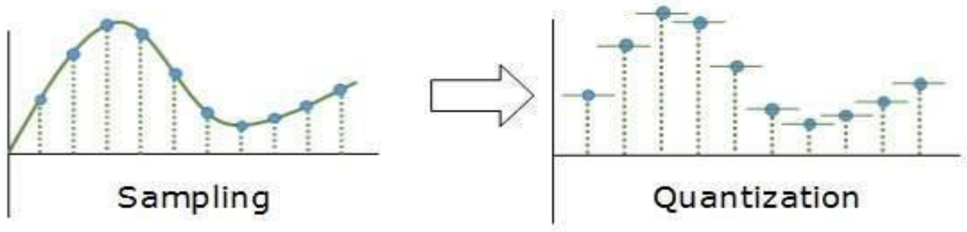
- Sampling
- Quantization
- Encoding.

Sampling



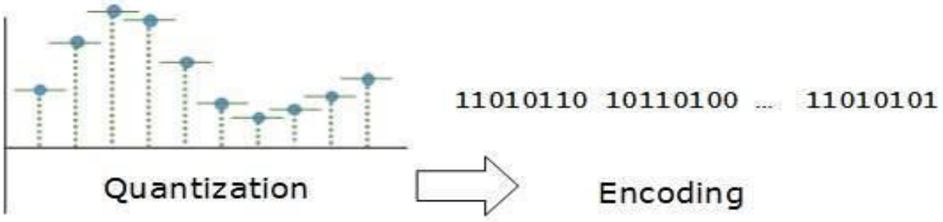
The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

Quantization



Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

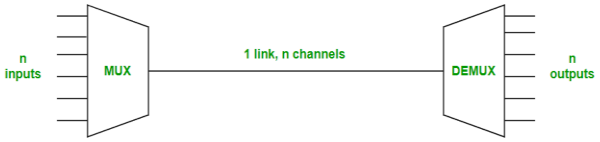
Encoding



In encoding, each approximated value is then converted into binary format.

Multiplexing

Multiplexing is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.



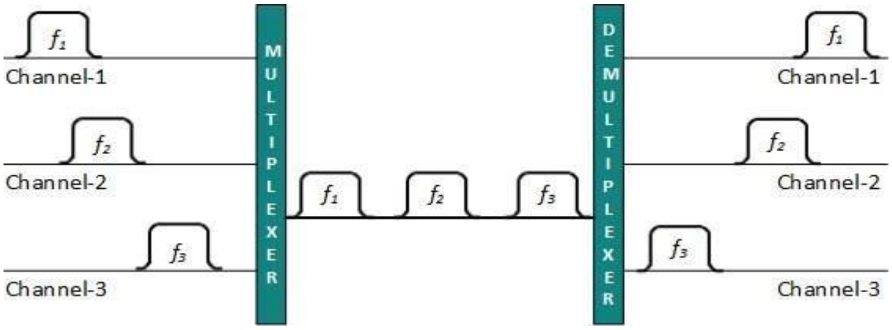
Types of Multiplexing

There are three types of Multiplexing :

1. Frequency Division Multiplexing (FDM)
2. Time-Division Multiplexing (TDM)
3. Wavelength Division Multiplexing (WDM)

Frequency Division Multiplexing

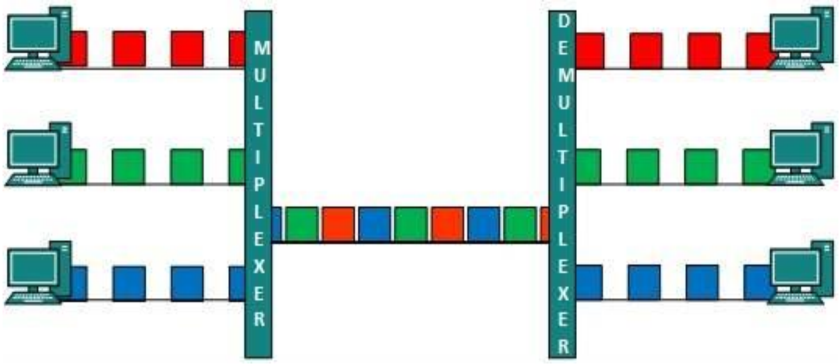
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



Time Division Multiplexing

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

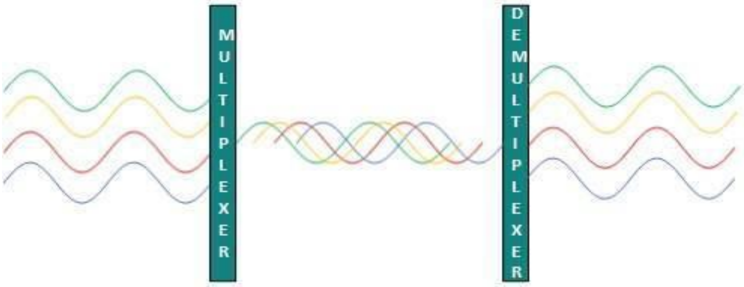
TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.



When channel A transmits its frame at one end,the De-multiplexer provides media to channel A on the other end.As soon as the channel A’s time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.

Wavelength Division Multiplexing

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.



Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

Code Division Multiplexing

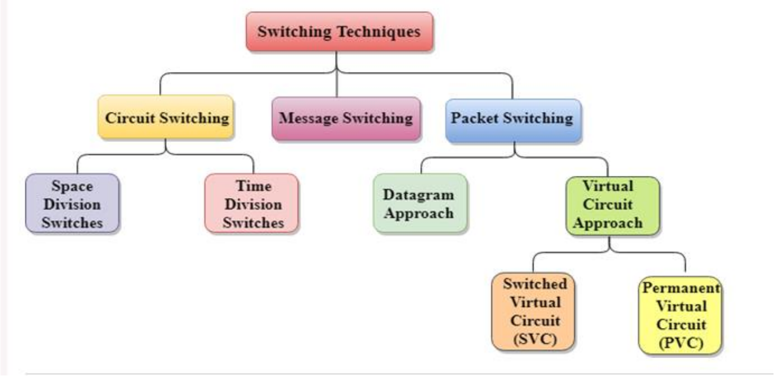
Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique code. CDM uses orthogonal codes to spread signals.

Each station is assigned with a unique code, called chip. Signals travel with these codes independently, inside the whole bandwidth.The receiver knows in advance the chip code signal it has to receive.

Network Switching

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

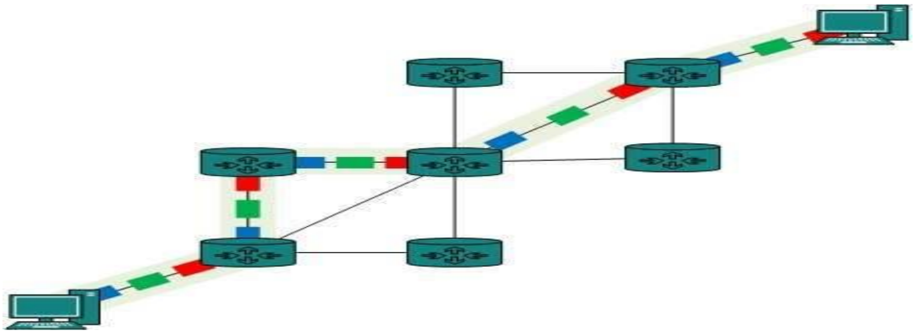


Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.There 'is a need of pre-specified route from which data will travels and no other data is permitted.In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

- Establish a circuit
- Transfer the data
- Disconnect the circuit

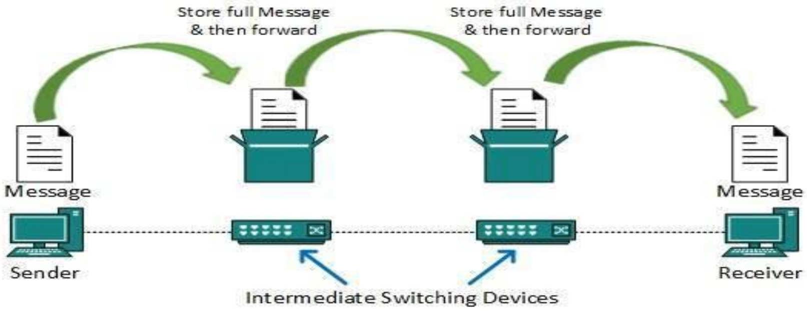


Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.



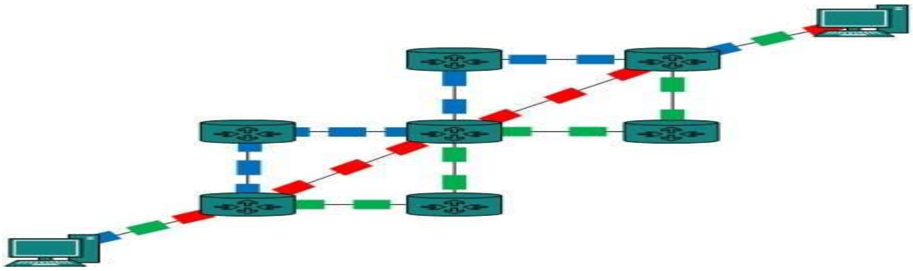
This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.



Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

Approaches of Packet Switching:

There are two approaches to Packet Switching:

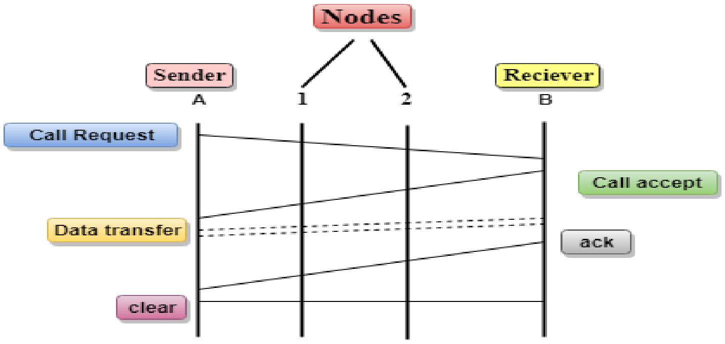
Datagram Packet switching:

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

Virtual Circuit Switching

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

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



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

Mr. D. SYAM KUMAR