Digital Communication and Networks

Network

In digital communications and networks, a network refers to a system of interconnected devices and transmission lines that are used to transmit and receive information between different locations. This can include wired or wireless networks, and can be used for various types of communication such as data, voice, and video.

A network can be classified by different characteristics such as its size, topology, and architecture. For example, a local area network (LAN) is a network that connects devices within a limited geographic area, such as a single building or campus. A wide area network (WAN) is a network that connects devices over a larger geographic area, such as across multiple cities or countries. Other types of networks include metropolitan area networks (MANs), storage area networks (SANs), and personal area networks (PANs).

In digital communication and networks, the communication between devices is done through the use of protocols, which are sets of rules that govern how devices communicate with each other. Examples of protocols include TCP/IP, which is the foundation for the Internet, and Ethernet, which is a common LAN protocol.

Data communication are the exchange of data between two devices via some form of transmission medium such as a wire cable. The effectiveness of digital communication system depends on four fundamental characteristics: delivery, accuracy, timelines and jitter.

1. **Delivery** the system must deliver data to the correct destination. Data must received by the intended device or user and only by the device or user.
2. **Accuracy** the system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timelines** the system must delivered the data in a timely manner. Data delivered late are useless in the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. **Jitter** jitter refers to the variation in the packet arrival time . it means uneven delay in the delivery of audio and video packets.

What is a network topology?

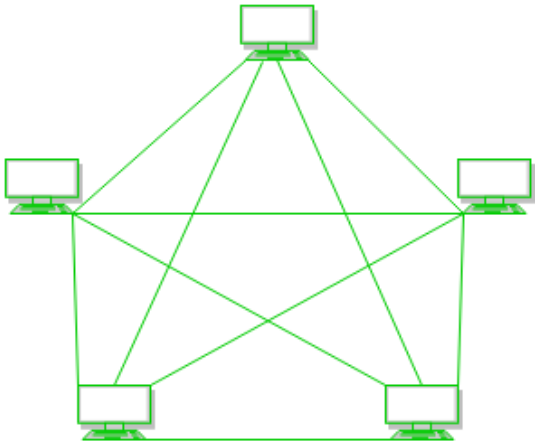
A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph. **A Network Topology is the arrangement with which computer systems or network devices are connected to each other.**

Types of network topologies

a. Mesh topology
b. Star topology
c. Bus topology
d. Ring topology
e. Tree topology

Mesh Topology:

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Every device is connected to another via dedicated channels. These channels are known as links.

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required=N*(N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is ${}^{N}C_{2}$ i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of mesh topology:

- Communication is very fast between the nodes.
- It is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

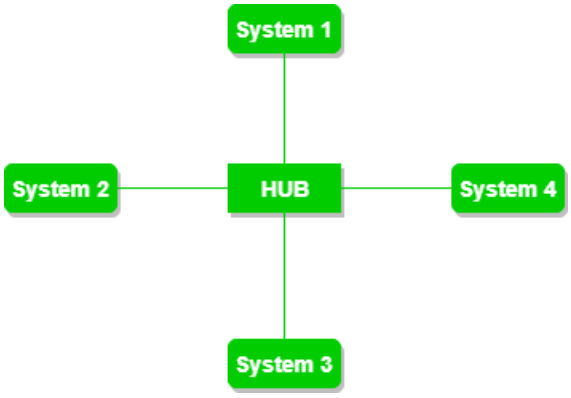
Disadvantages with mesh topology:

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

Star Topology:

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

A star topology having four systems connected to a single point of connection i.e. hub.



Advantages of star topology:

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

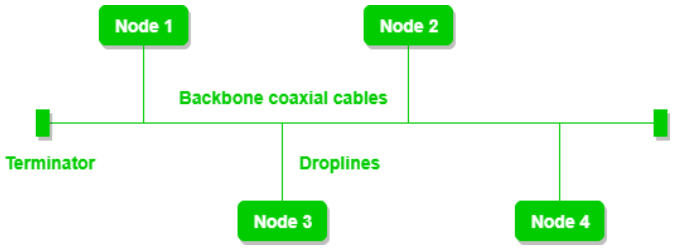
Problems with star topology:

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

Bus Topology:

Bus topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.

A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.



Advantages of this topology:

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.

Problems with this topology:

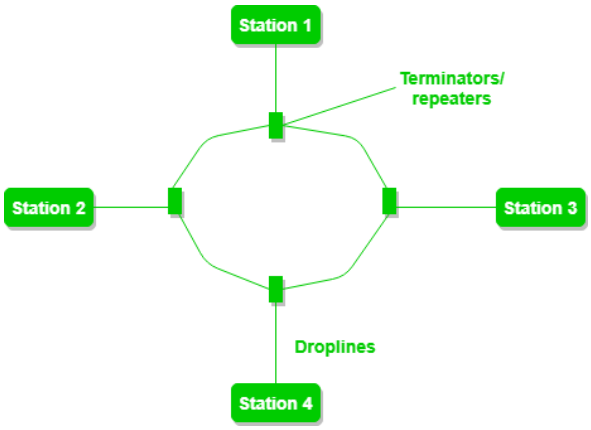
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

Ring Topology:

In this topology, it forms a ring connecting devices with exactly two neighboring devices.

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e.., it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



A ring topology comprises 4 stations connected with each forming a ring.

The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

The following operations take place in ring topology are :

1. One station is known as a **monitor** station which takes all the responsibility for performing the operations.
2. To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of ring topology:

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

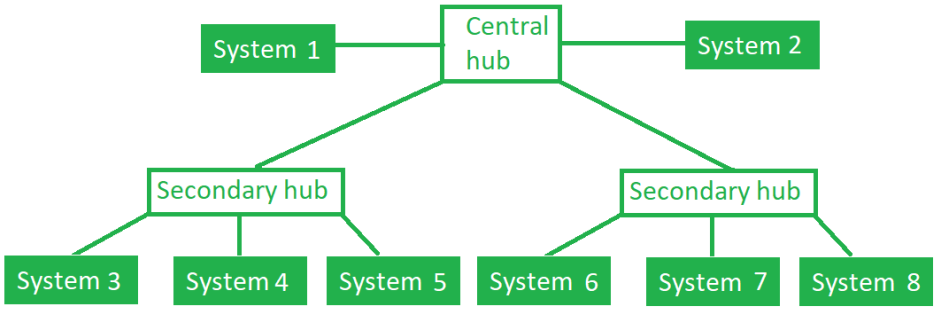
Problems with ring topology:

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.

- Less secure.

Tree Topology :

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of tree topology :

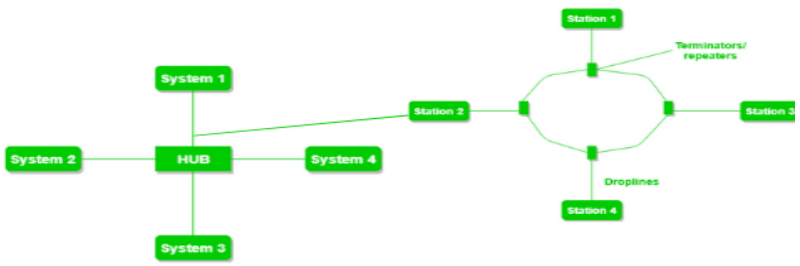
- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

Problems with this topology :

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

Hybrid Topology :

This topological technology is the combination of two or more than two topology. Called hybrid topology



Advantages of hybrid topology :

- This topology is **very flexible**.
- The size of the network can be easily expanded by **adding new devices.**

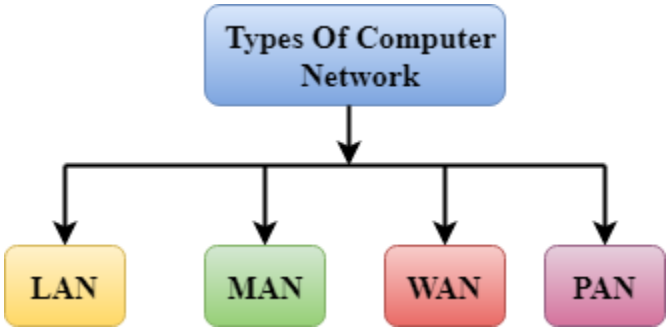
Problems with hybrid topology :

- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**.

Classifications of Network

Network classifications refer to different types of computer networks that are categorized based on their size, geographical area, and the types of services they provide. Some common network classifications include:

A **computer network** is mainly of **four types**:



- **LAN(Local Area Network)**
- **MAN(Metropolitan Area Network)**
- **WAN(Wide Area Network)**
- **PAN(Personal Area Network)**

LAN(Local Area Network)

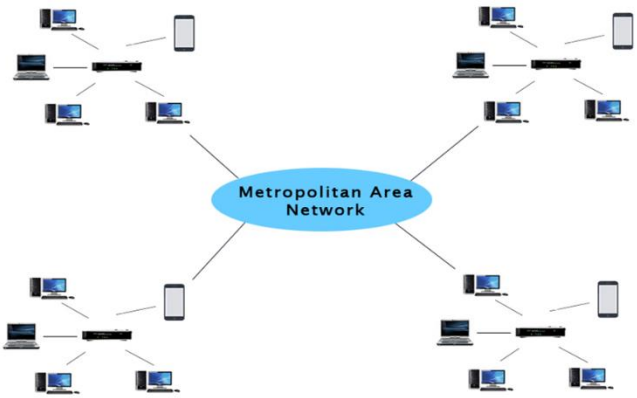
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

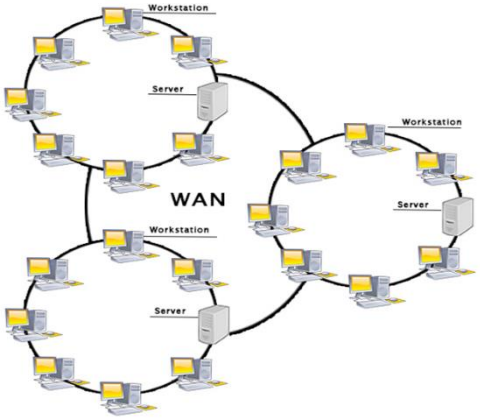


WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.

Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.



Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Network Protocol

Network protocols are a set of rules and standards that govern how data is transmitted over a network. They define the format of the data, the way it is addressed, and the rules for error checking and correction.

Some common network protocols include:

1. **TCP (Transmission Control Protocol):** A transport layer protocol that ensures reliable data transfer over a network by establishing a virtual connection between two computers and acknowledging the receipt of data.
2. **IP (Internet Protocol):** A network layer protocol that is responsible for routing data packets over a network. It provides addressing and routing services to allow data to be transmitted between computers on different networks.
3. **HTTP (Hypertext Transfer Protocol):** An application layer protocol that is used for transmitting data over the internet. It is the foundation of the World Wide Web and is used to request and receive web pages.
4. **FTP (File Transfer Protocol):** An application layer protocol that is used to transfer files between computers over a network.

5. **DNS (Domain Name System):** An application layer protocol that is used to translate domain names into IP addresses, allowing users to access websites using human-readable names instead of IP addresses.
6. **SMTP (Simple Mail Transfer Protocol)** is an application layer protocol for sending email messages between servers.
7. **DHCP (Dynamic Host Configuration Protocol)** is a protocol that allows a server to automatically assign IP addresses to devices on a network.
8. **SSH (Secure Shell)** is a protocol that allows secure remote login and other secure network services over an insecure network.

These are some of the common protocols that are used in networks, however, there are many other protocols that are specific to different types of networks and services.

Layered Network Architecture

Layered network architecture is a way of organizing the components of a network into different layers, with each layer providing a specific set of functions. The most common layered network architecture is the OSI (Open Systems Interconnection) model, which consists of seven layers:

1. Physical Layer: This layer deals with the physical connections between devices, such as cables and connectors.
2. Data Link Layer: This layer deals with the transmission of data between devices on the same network segment, such as error checking and flow control.
3. Network Layer: This layer deals with routing and addressing of data packets, allowing them to be transmitted between different networks.
4. Transport Layer: This layer provides end-to-end communication between devices, ensuring that data is delivered reliably and in the correct order.
5. Session Layer: This layer establishes and manages sessions between devices, allowing them to communicate over a period of time.
6. Presentation Layer: This layer deals with the formatting and representation of data, allowing it to be transmitted in a way that can be understood by different devices and systems.
7. Application Layer: This layer provides the interface to the user and applications, allowing them to access the network and its services.

Each layer communicates with the layer above and below it using a set of protocols and interfaces, allowing the different components of the network to work together. Layered network architecture allows for the separation of concerns, making the network more modular, and easy to troubleshoot and modify.

Another common layered network architecture is the TCP/IP (Transmission Control Protocol/Internet Protocol) model which is widely used in the Internet and other networks. It has four layers: **Data Link Layer, Internet Layer, Transport Layer and Application Layer.**

OSI Model

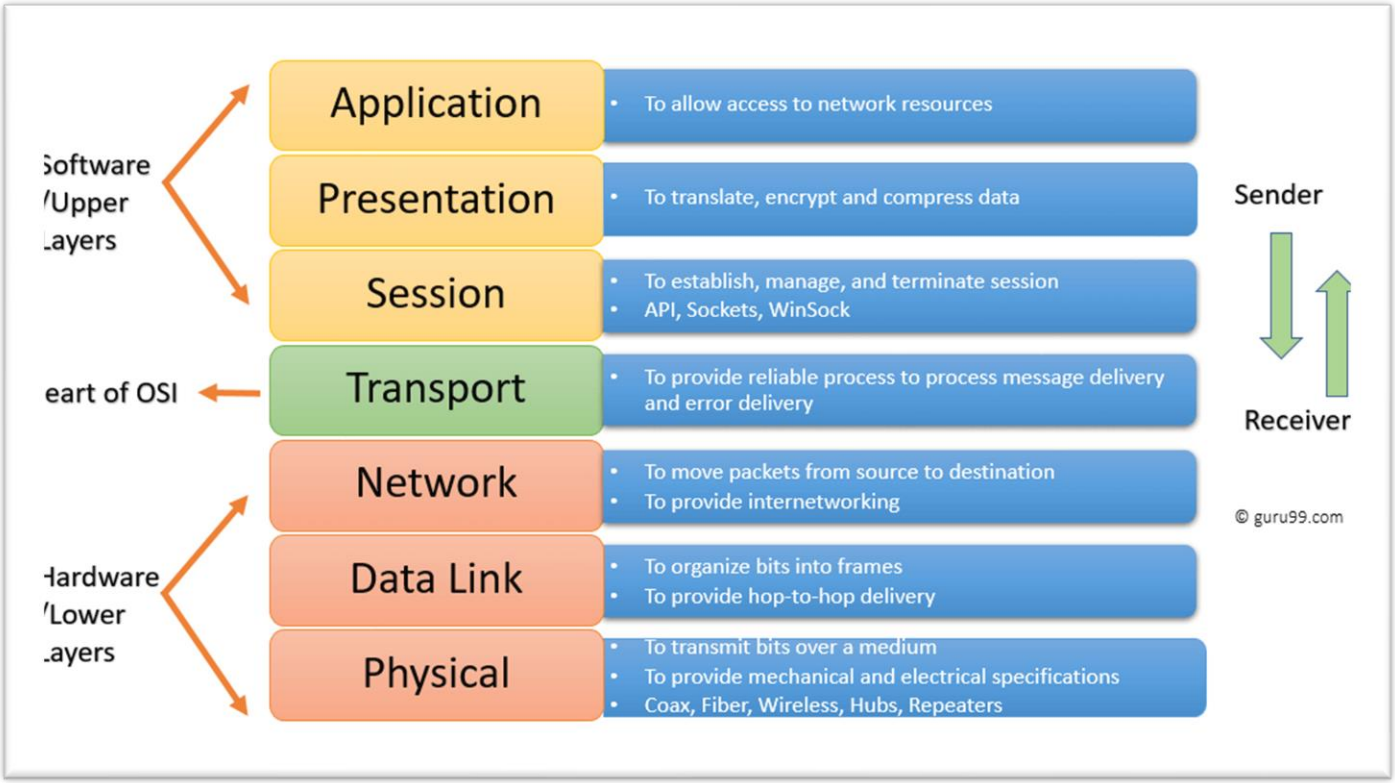
International standard organization (ISO) proposed an open system interconnection (ISO) model. OSI model allows two system to communicate regardless of their architecture.

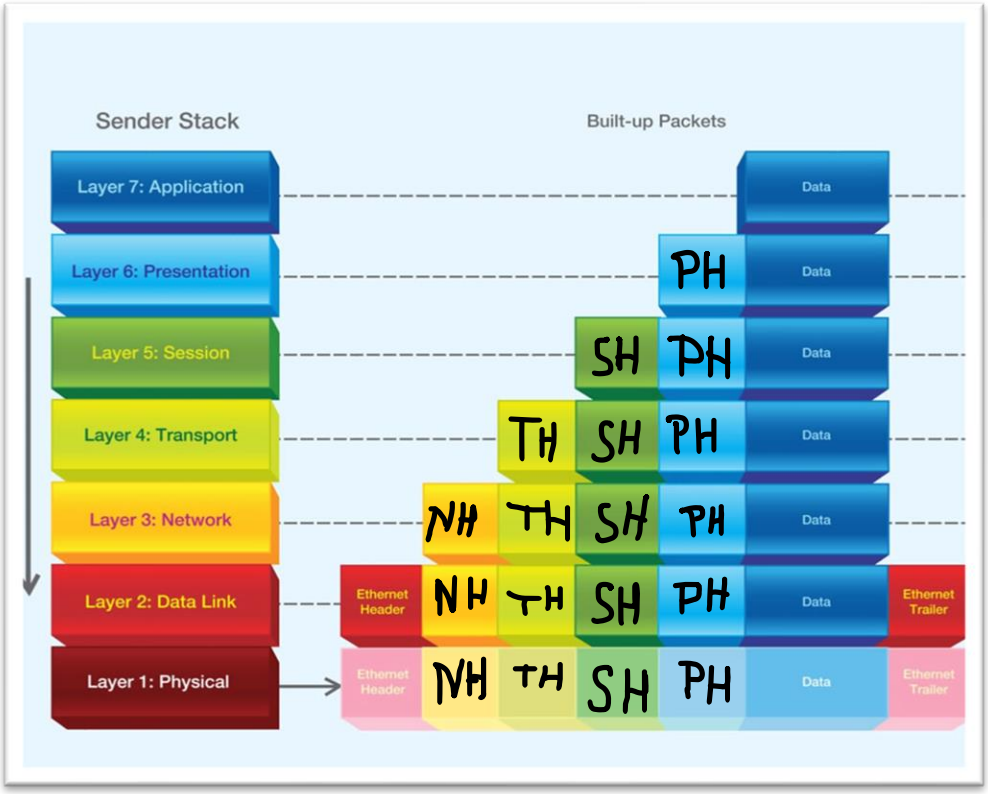
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of OSI model is to show how facilitate communication between different systems without requiring changes to the logic underlaying hardware and software

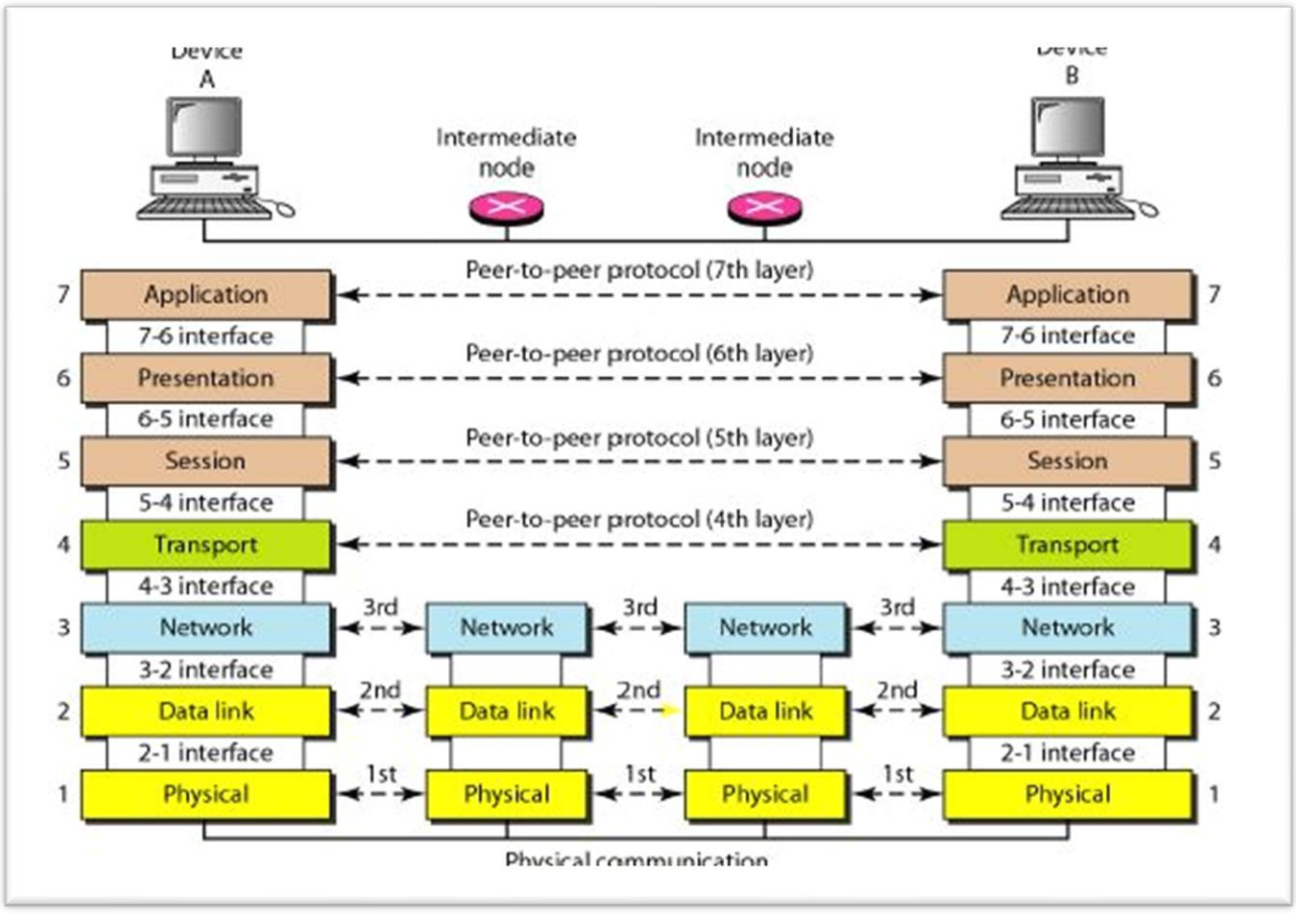
The OSI (Open Systems Interconnection) reference model is a seven-layer conceptual framework for networking that is used to describe how data is transmitted over a network. The seven layers are:

1. Physical Layer: Responsible for transmitting raw bits over a physical medium, such as a copper cable or wireless connection.
2. Data Link Layer: Responsible for providing reliable data transfer over the physical layer, through the use of error detection and correction.
3. Network Layer: Responsible for routing data packets through the network, determining the best path for data to travel.
4. Transport Layer: Responsible for ensuring end-to-end data integrity, through the use of flow control and error checking.
5. Session Layer: Responsible for establishing, maintaining and terminating sessions between applications.
6. Presentation Layer: Responsible for converting data into a standard format that can be understood by both the sender and the receiver.
7. Application Layer: Provides a interface between the network and the end-user application.

Each layer in the OSI model is responsible for a specific set of functions and communicates with the layers above and below it using a well-defined set of protocols. This modular approach allows different types of devices and protocols to be used at different layers, making it possible to create a wide variety of networks.




Sender Stack
Built-up Packets
Layer 7: Application
Layer 6: Presentation
Layer 5: Session
Layer 4: Transport
Layer 3: Network
Layer 2: Data Link
Layer 1: Physical
Data
PH
SH
TH
NH
Ethernet Header
Ethernet Trailer


Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication

TCP/IP Model

The TCP/IP model is a set of layers that describe the functions and protocols used in internet communication. It is a standard model used to understand and troubleshoot internet communication and networking. The model is based on a layered architecture, with each layer providing specific functionality and building on the functionality of the layers below it. The model has four layers:

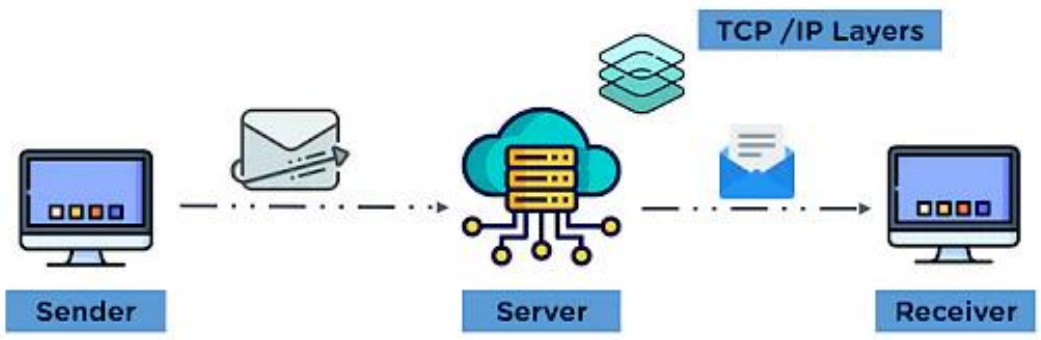
1. **The Application Layer:** This is the topmost layer and provides the interface between the application and the network. It is responsible for providing services to the application and handling the details of the underlying network communication. Examples of protocols at this layer include **HTTP, FTP, DNS, Telnet, and SMTP**.

2. **The Transport Layer:** This layer is responsible for end-to-end communication and error control. It is responsible for ensuring that the data is delivered reliably and correctly between the sender and receiver. **The main protocols at this layer are TCP and UDP.** TCP (Transmission Control Protocol) is a connection-oriented protocol that establishes a reliable connection between devices before transmitting data. It guarantees that data is delivered correctly. UDP (User Datagram Protocol) is a connectionless protocol that does not establish a connection before transmitting data. It is faster than TCP but does not guarantee that data will be delivered correctly.

3. **The Internet Layer: This layer handles the routing of data packets through the network.** The main protocol at this layer is IP (Internet Protocol). IP is responsible for addressing and routing packets of data to their correct destination. It determines the path that data should take through the network, based on the destination IP address.

4. **The Network Access Layer:** This is the bottom layer and **deals with the physical connection between devices.** It is responsible for communicating data between devices on the same network segment. Examples of protocols at this layer include Ethernet, WiFi, and PPP.

The TCP/IP model is designed to be independent of any specific hardware or software, making it a flexible and widely adopted standard for internet communication. It allows different devices and networks to communicate with each other by providing a common set of protocols and guidelines. Understanding the different layers and their functions can be helpful in troubleshooting communication issues and understanding how data is transmitted over the internet.



Network connecting devices

Hubs, repeaters, Bridges, Routers, Gateway, Switches

1. **Hubs:** A hub is a networking device that connects multiple devices together in a local area network (LAN). It is a central connection point that enables communication between devices connected to the network.

   A hub is essentially a multi-port repeater, which receives data on one port and then transmits it out to all other connected devices. Data is broadcast to all devices connected to the hub, regardless of whether the intended recipient is connected to the hub or not. This can lead to increased network traffic and can cause a bottleneck in the network.

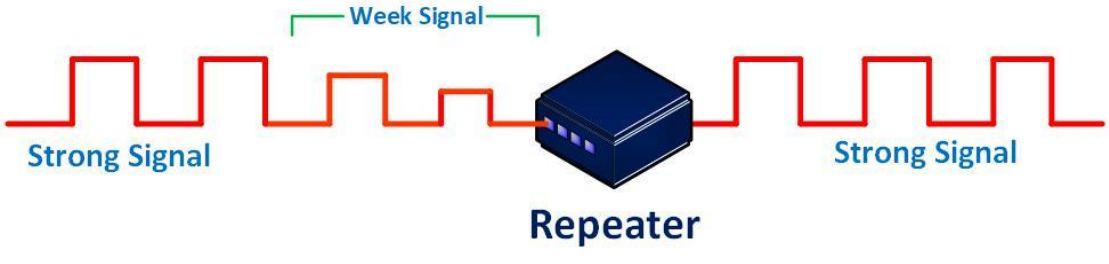
   There are two types of hubs: active hubs and passive hubs. An active hub contains a built-in power supply and can amplify the signal it receives, making it stronger and more reliable. Passive hubs, on the other hand, does not have a power supply and simply connects the devices together.

   Hubs are generally less expensive than other networking devices such as switches, but they are less efficient and less secure than switches and routers. They are also less common in modern networks, as they have been largely replaced by switches and routers, which provide more advanced features and better performance.

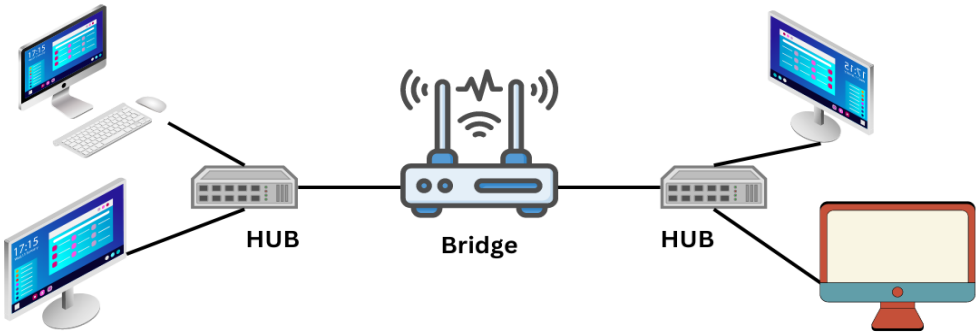
2. **Repeaters:** A repeater is a networking device that amplifies or regenerates signals in order to extend the distance over which data can be transmitted. It receives a signal on one network segment, amplifies it, and then sends it on to the next network segment. This allows for the signal to travel farther, enabling devices to be located at a greater distance from the central hub or router.

   Repeaters work at the physical layer (layer 1) of the OSI model, which means that they do not interpret or make decisions about the data that they are forwarding. They simply receive a signal, amplify it and retransmit it. They do not have the ability to filter or direct data traffic, and all data is broadcast to all devices connected to the repeater.

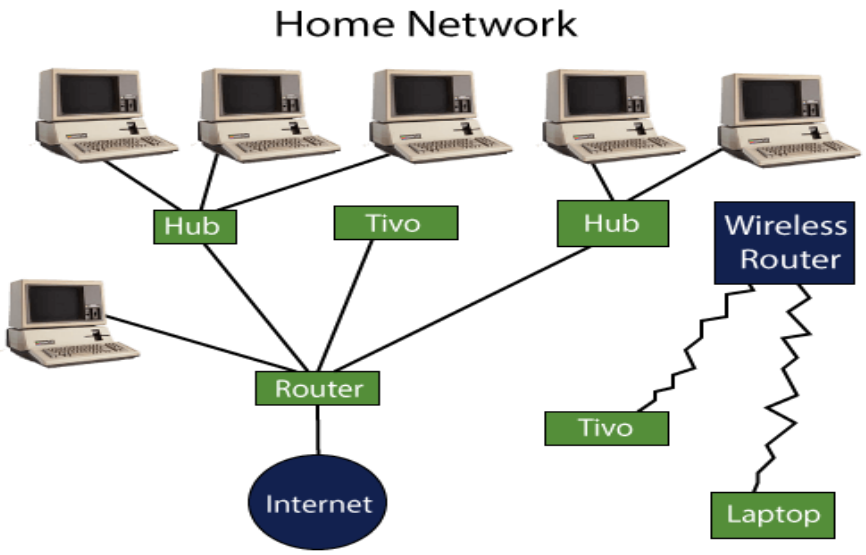
   Repeaters are generally used in wired networks, such as Ethernet networks, and they can be used to extend the distance of a network cable up to 100 meters. With the advancement of wireless networks, the use of repeaters in wireless networks is also common. However, repeaters can also introduce some issues such as increased collision and increased latency on the network.



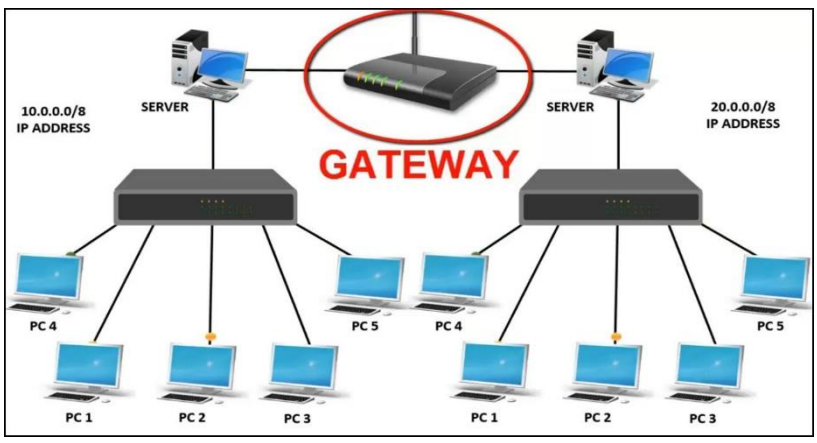
3. **Bridges:** In computer networks, a bridge is a device that connects two separate network segments, allowing data to flow between them. Bridges operate at the data link layer (layer 2) of the OSI model and use MAC addresses to forward packets between network segments. This helps to reduce network traffic and improve network performance by breaking up large networks into smaller segments. Bridges are often used in LANs (local area networks) to connect different subnets or to connect LANs to other networks, such as the Internet.



4. **Routers:**



5. **Gateway:** Gateway is a hardware or software device that is use to connect two dissimilar or similar type of network.
   - In a computer network, a gateway is a device that acts as an entry point to another network. It connects two networks together, allowing communication between them. A gateway can also be a software program that allows a computer to connect to another network or to the Internet. It translates between different protocols and provides security features such as firewalling and VPN support.



6. Switches: A switch is a networking device that connects devices together on a computer network. It forwards data packets between devices on a LAN (Local Area Network) using MAC addresses to determine the destination device. Switches operate at the data link layer (Layer 2) of the OSI model, which means they are responsible for forwarding packets based on the MAC addresses of devices. They use a process called "switching" to forward packets to their intended destinations, allowing multiple devices on a network to communicate with each other simultaneously. This is in contrast to a hub, which simply broadcasts packets to all devices on the network regardless of whether or not they are the intended recipients.

Unit- 2

Analog Signal

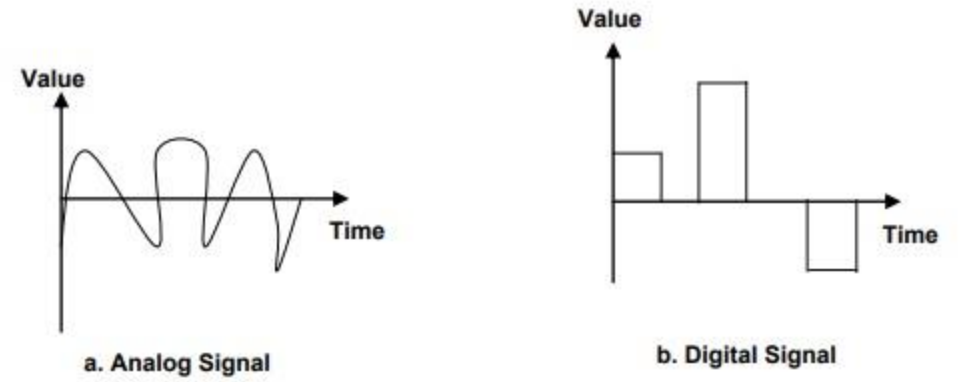
Analog signals have infinitely so many levels of intensity over a period of time. When the wave moves from value A to value B, it passes through and it includes an infinite number of values along its path.

Digital Signal

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

The easiest way to show signals is by plotting them on a pair of perpendicular axes.

- The vertical axis represents the value or strength of a signal.
- The horizontal axis represents time.



The above figure shows the Analog signal and a digital signal. The curve represents the Analog signal through an infinite number of points. The vertical lines of the digital signal, however, demonstrate the sudden jump that the signal makes from value to value.

Data-rate: Data Rate: Data Rate is defined as **the amount of data transmitted during a specified time period over a network**. It is the speed at which data is transferred from one device to another or between a peripheral device and the computer. It is generally measured in Mega bits per second(Mbps) or Megabytes per second(MBps).

Bandwidth is a measure of the capacity of a communication channel, and it refers to the amount of data that can be transferred over that channel in a certain amount of time. It is typically measured in bits per second (bps) or bytes per second (Bps).

For example, a network connection with a bandwidth of 100Mbps (Mega bits per second) can transfer 100 million bits of data every second. Similarly, a network connection with a bandwidth of 10Gbps (Giga bits per second) can transfer 10 billion bits of data every second.

Bandwidth can be affected by various factors such as the type of connection, distance, and number of users sharing the connection.

In summary, bandwidth is the capacity of a network or internet connection to transfer data in a given period of time and is measured in bits per second (bps) or bytes per second (Bps). It is an important factor that determines the performance of a network and the maximum rate at which data can be transferred.

Data-rate limits: In a computer network, a data rate limit refers to the maximum amount of data that can be transmitted over a network connection within a certain period of time. This limit is often expressed in terms of bits per second (bps) or bytes per second (Bps). Data rate limits are used to regulate network traffic and prevent congestion, ensuring that all devices on the network have fair access to bandwidth. They can be set at various levels, such as at the router, switch, or individual device level.

Line coding

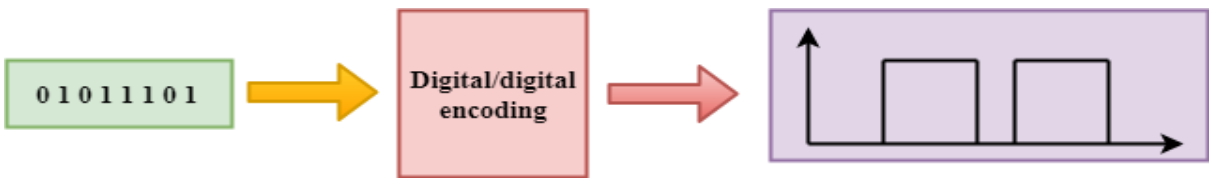
Line coding refers to the process of converting digital data into digital signals. Whenever we transmit data it is in the form of digital signals, so with the help of line coding, we can convert a sequence to bits (or encoding) into a digital signal which then again converted into bits by the receiver (or can be said as decoded by the receiver). For all this to happen we need line coding schemes which could also be able to avoid overlapping and distortion of signals.

Some necessary characteristics of line coding schemes:

- Less complexity.
- Should have noise and interference tolerance.
- No DC component (or say low-frequency component) should be there because it can't be transferred to larger distances.
- Least baseline wandering should be there (baseline wander: low-frequency noise having nonlinear and non-stationary nature).
- Should have error detection capability.
- Should be self-synchronized.

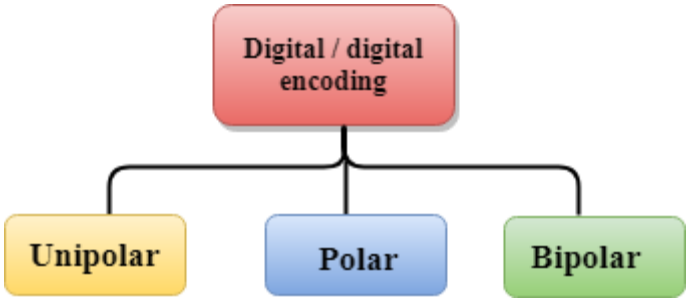
DIGITAL-TO-DIGITAL CONVERSION

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.



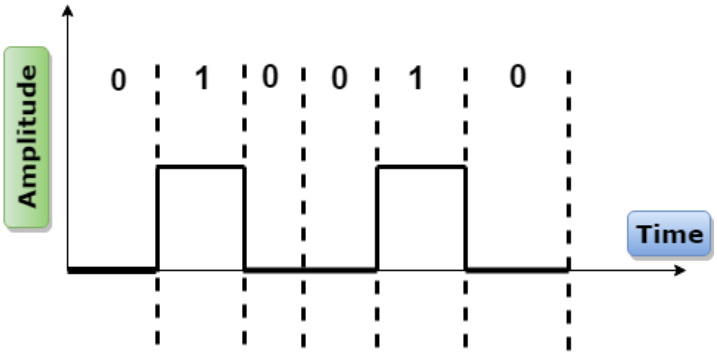
Digital-to-digital encoding is divided into three categories:

- 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.

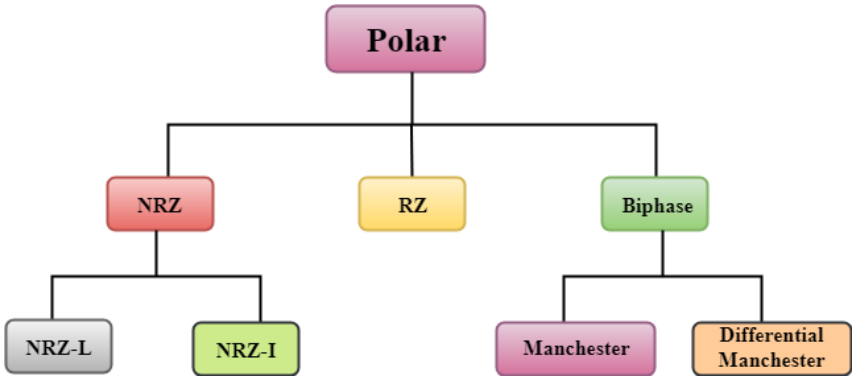


Unipolar encoding has two problems that make this scheme less desirable:

- 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.



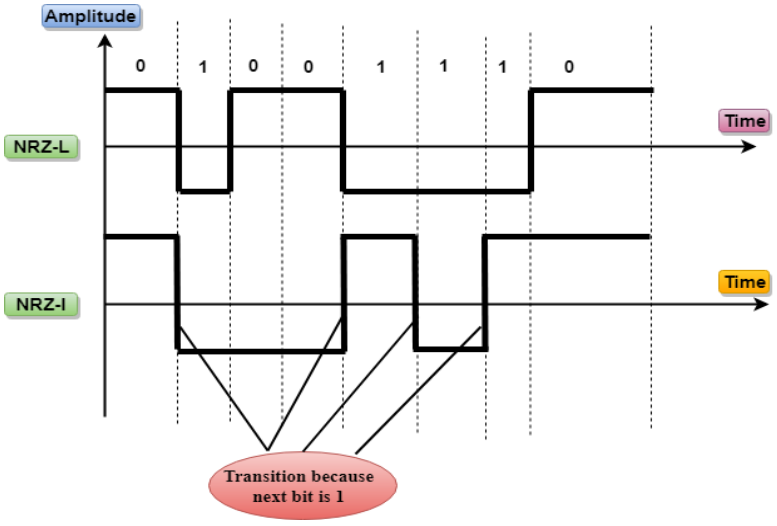
NRZ

- 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:

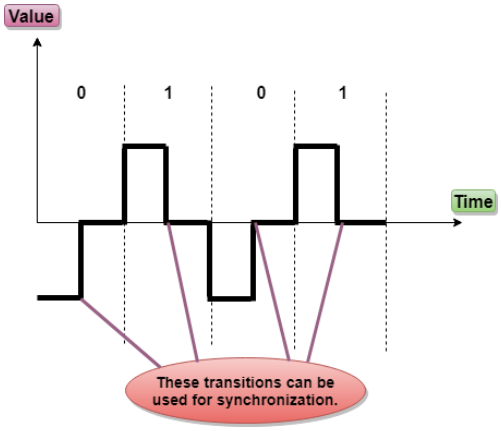
NRZ-L: In NRZ-L encoding, the level of the signal depends on the type of the bit that it represents. If a bit is 0 or 1, then their voltages will be positive and negative respectively. Therefore, we can say that the level of the signal is dependent on the state of the bit.

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.

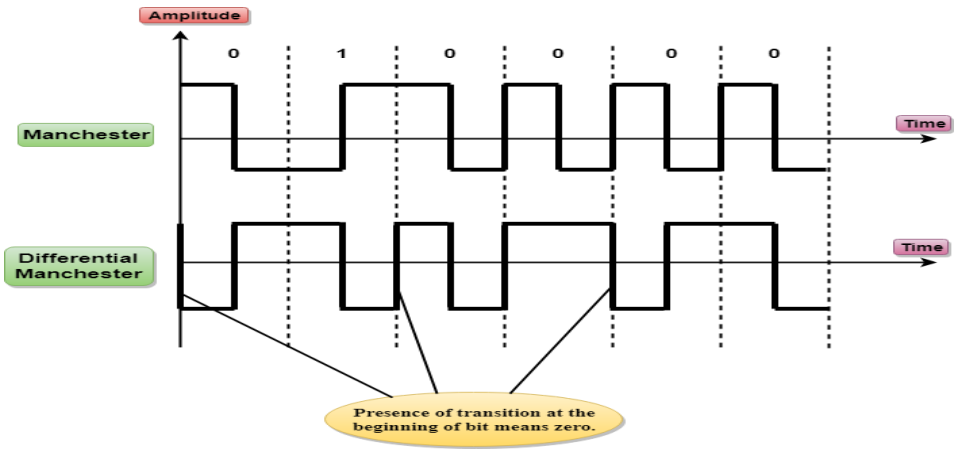
Biphase encoding is implemented in two different ways:

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

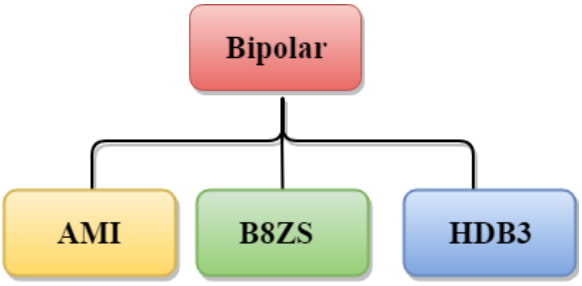
- It changes the signal at the middle of the bit interval for synchronization, but the presence or absence of the transition at the beginning of the interval determines the bit. A transition means binary 0 and no transition means binary 1.
- In Manchester Encoding scheme, two signal changes represent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

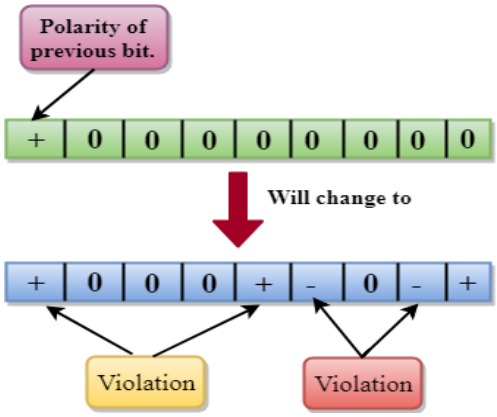
Disadvantage:

- 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.

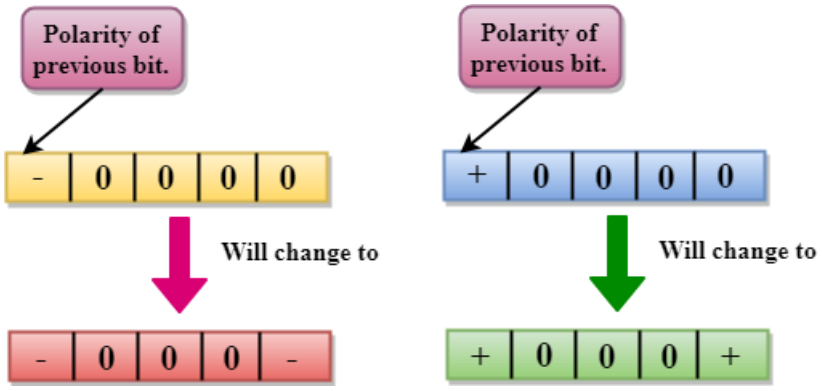
- If the polarity of previous 1 bit is negative, then the eight 0s will be encoded as zero, zero, zero, negative, positive, zero, positive, negative.



HDB3

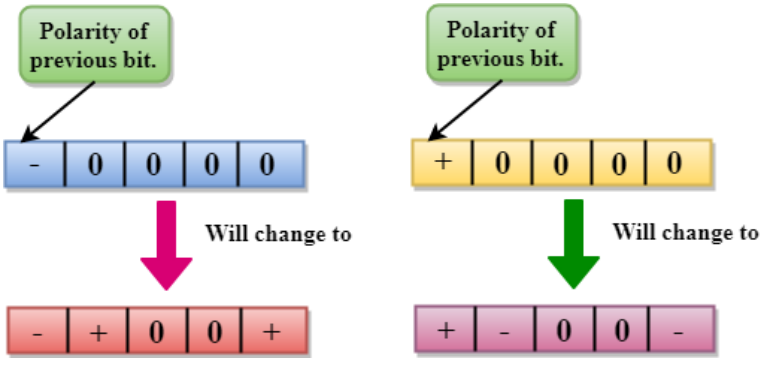
- HDB3 stands for **High-Density Bipolar 3**.
- HDB3 technique was first adopted in Europe and Japan.
- HDB3 technique is designed to provide the synchronization of a long sequence of 0s bits.
- In the HDB3 technique, the pattern of violation is based on the polarity of the previous bit.
- When four 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.



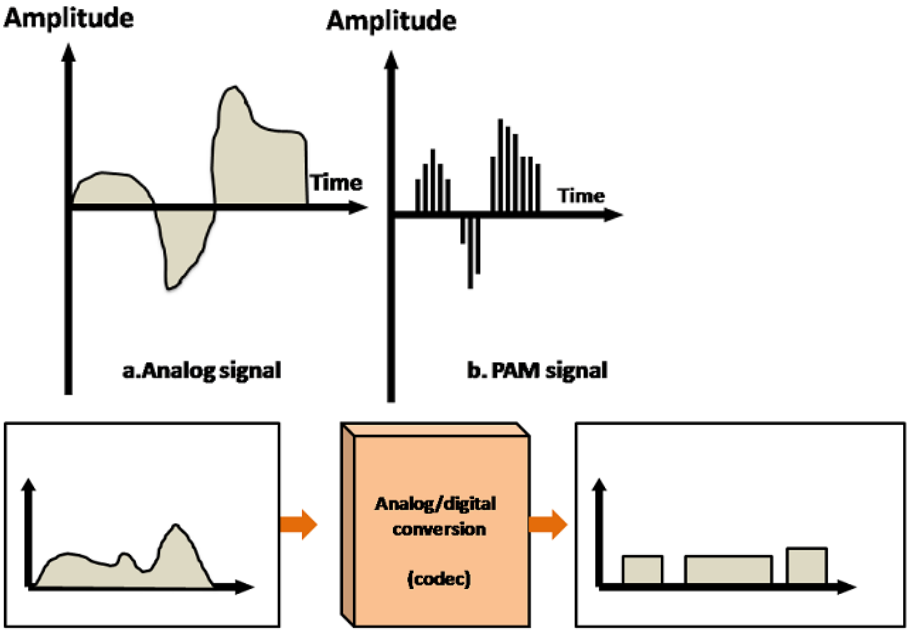
ANALOG-TO-DIGITAL CONVERSION

- 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

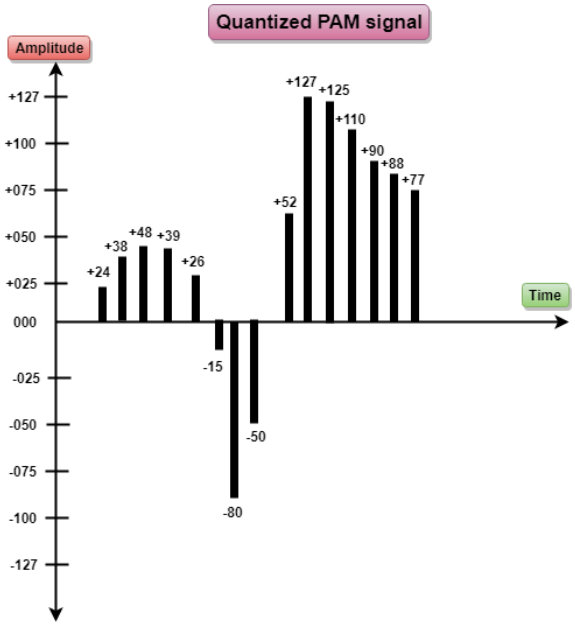
PAM

- 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.

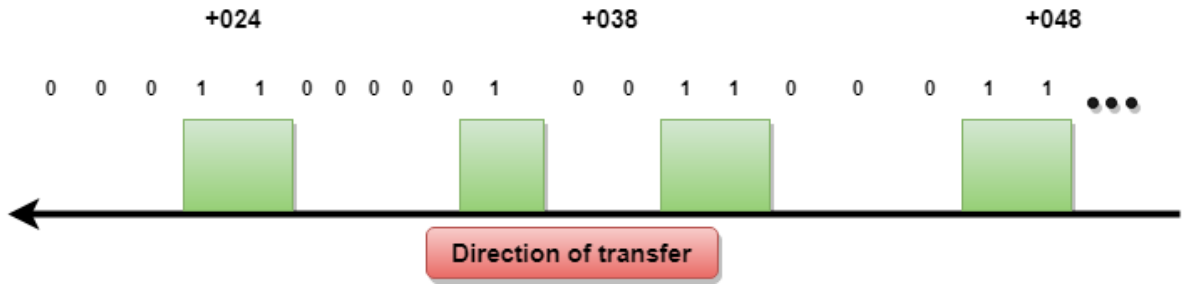


PCM

- 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.


Quantized PAM signal
Amplitude
+127
+100
+075
+050
+025
000
-025
-050
-075
-100
-127
+24
+38
+48
+39
+26
-15
-80
-50
+52
+127
+125
+110
+90
+88
+77
Time

PCM


+024
+038
+048
0 0 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0 0 1 1
Direction of transfer

Unit- 3

There are several types of errors that can occur in computer networks, including:

1. **Single-bit errors: These are errors that involve the alteration of a single bit** in the transmitted data. Single-bit errors can be caused by noise on the communication channel, or by a malfunctioning component in the network.

2. **Burst errors: These are errors that involve the alteration of multiple bits in a sequence**. Burst errors can be caused by a variety of factors, such as interference from other devices, or a malfunctioning component in the network.

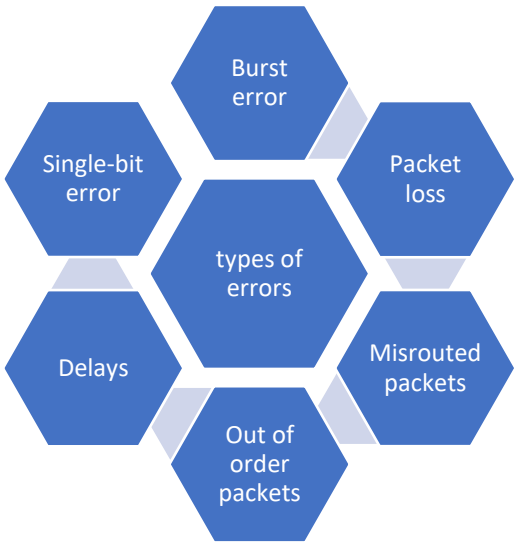
3. **Packet loss: This occurs when one or more packets of data are not successfully delivered to the destination.** This can be caused by network congestion, faulty network components, or a poor signal quality.

4. **Delays:** This occurs when packets take longer than expected time to reach their destination. This can be caused by network congestion, poor signal quality or routing loops.

5. **Out of order packets:** This occurs when packets arrive at the destination out of the order in which they were sent. This can be caused by routing loops, network congestion or poor signal quality.

6. **Misrouted packets: This occurs when packets are sent to the wrong destination.** This can be caused by a poor routing table, network congestion or faulty network components.

These errors can negatively impact the performance and functionality of the network, and can lead to data loss or corruption. Error detection and correction techniques are used to detect and correct these errors, helping to maintain the integrity and reliability of the network.



Error detection is a technique used in computer networks to detect and correct errors that occur during the transmission of data. The goal of error detection is to ensure that the data received by the receiver is the same as the data that was originally sent by the sender.

There are various error detection techniques that can be used in computer networks, some of the most common ones include:

1. **Parity checking:** Parity checking is a method used for error detection in data transmission or storage. It involves adding an extra bit, called a parity bit, to each group of data bits. The value of the parity bit is chosen so that the total number of 1's in the group (including the parity bit) is always even (or always odd). When the data is received or read, the parity of the bits is checked to ensure that no errors have occurred. If the parity is not correct, an error has occurred and the data can be corrected or retransmitted.

2. **Cyclic Redundancy Check (CRC):** This is a more sophisticated method of error detection that uses a mathematical algorithm to generate a checksum for each data unit. The receiver can then compare the received checksum with the one that was sent to detect any errors.

3. **Checksum:** It is the sum of all the data unit added together and sent along with the data. At the receiver, if the sum of the received data unit is same as the received checksum, the data is considered to be correct otherwise it is considered to be in error

4. **Hamming Code:** It is a method of error correction, which uses extra bits called parity bits to detect and correct errors in the data.

These techniques are used to detect errors in the data and request for retransmission of data if errors are detected, which helps to maintain the integrity of the data transmitted over the network.

Data-link layer

The Data Link Layer is the second layer of the OSI (Open Systems Interconnection) model, which is used to define the various aspects of computer networking. **This layer is responsible for providing a reliable link between two devices on a network by ensuring that data is transmitted correctly and in the correct order.** It also provides error detection and correction to ensure that data is transmitted without errors.

The Data Link Layer is divided into two sub-layers: the **Media Access Control (MAC)** layer and the **Logical Link Control (LLC)** layer.

The MAC sub-layer is responsible for controlling access to the physical medium, such as a network cable or wireless connection. It assigns a unique address, called a MAC address, to each device on the network, and uses this address to ensure that data is transmitted only to the intended recipient. The MAC sub-layer also controls the flow of data to prevent collisions, where multiple devices attempt to transmit data at the same time.

The LLC sub-layer provides a way for the network layer to communicate with the MAC sub-layer, and it also provides error checking and correction. It also controls the flow of data to make sure packets are sent in the correct order.

In summary, The Data Link Layer is responsible for creating a reliable link between two devices on a network by providing error detection and correction, controlling the flow of data and managing

access to the physical medium through MAC addresses. It also includes protocols such as Ethernet and Wi-Fi.

Data Link Layer Frame

A frame is a unit of communication in the data link layer. Data link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

Fields of a Data Link Layer Frame

A data link layer frame has the following parts:

- **Frame Header**: It contains the source and the destination addresses of the frame and the control bytes.
- **Payload field**: It contains the message to be delivered.
- **Trailer**: It contains the error detection and error correction bits. It is also called a Frame Check Sequence (FCS).
- **Flag**: Two flag at the two ends mark the beginning and the end of the frame.

Frame Header

A frame header contains the destination address, the source address and three control fields *kind*, *seq*, and *ack* serving the following purposes:

- *kind*: This field states whether the frame is a data frame or it is used for control functions like error and flow control or link management etc.
- *seq*: This contains the sequence number of the frame for rearrangement of out – of – sequence frames and sending acknowledgments by the receiver.
- *ack*: This contains the acknowledgment number of some frame, particularly when piggybacking is used.

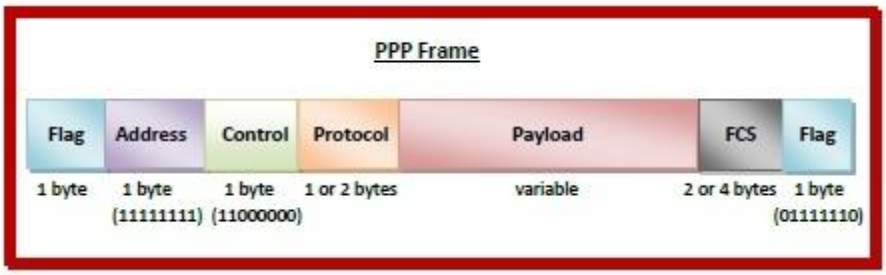
Specific Data Link Layer Frames

The structure of the data link layer frame may be specialized according to the type of protocol used. Let us study the frame structure used in two protocols: Point – to – Point Protocol (PPP) and High-level Data Link Control (HDLC).

Point – to – Point Protocol

Point – to – Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. The fields of a PPP frame are:

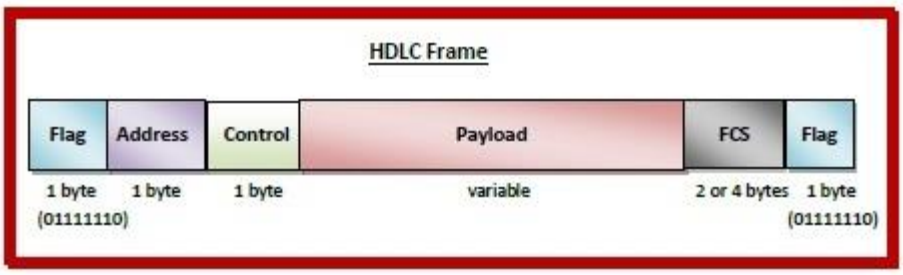
- **Flag**: It is of 1 byte that with bit pattern 01111110.
- **Address**: 1 byte which is set to 11111111 in case of the broadcast.
- **Control**: 1 byte set to a constant value of 11000000.
- **Protocol**: 1 or 2 bytes that define the type of data contained in the payload field.
- **Payload**: This carries the data from the network layer. The maximum length of the payload field is 1500 bytes.
- **FCS**: It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code).



High-level Data Link Control

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. The fields of an HDLC frame are:

- **Flag**: It is an 8-bit sequence with bit pattern 01111110.
- **Address**: It contains the address of the receiver. The address field may be from 1 byte to several bytes.
- **Control**: It is 1 or 2 bytes containing flow and error control information.
- **Payload**: This carries the data from the network layer. Its length may vary from one network to another.
- **FCS**: It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

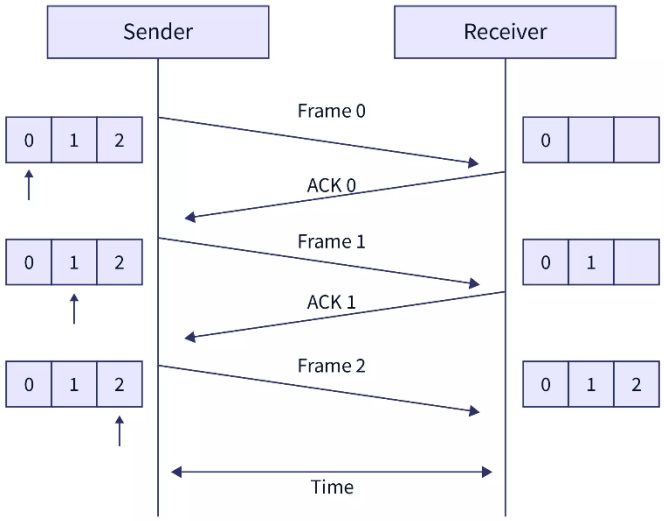


error recovery protocols- stop and wait ARQ

Error recovery protocols are methods used to detect and correct errors that occur during data transmission. One such protocol is Stop-and-Wait ARQ (Automatic Repeat Request). In this protocol, the sender sends a single data packet and waits for an acknowledgement (ACK) from the receiver before sending the next packet. If the sender does not receive an ACK, it retransmits the packet until an ACK is received or a maximum number of retransmissions is reached. This protocol helps ensure that the receiver receives all packets without errors, but it also results in a slower data transfer rate.

The stop and wait ARQ is one of the Sliding Window Protocol strategies that is used where reliable in-order delivery of the data frames is required. The stop and wait ARQ is used for noisy channels or links and it manages the flow and error control between the sender and the receiver.

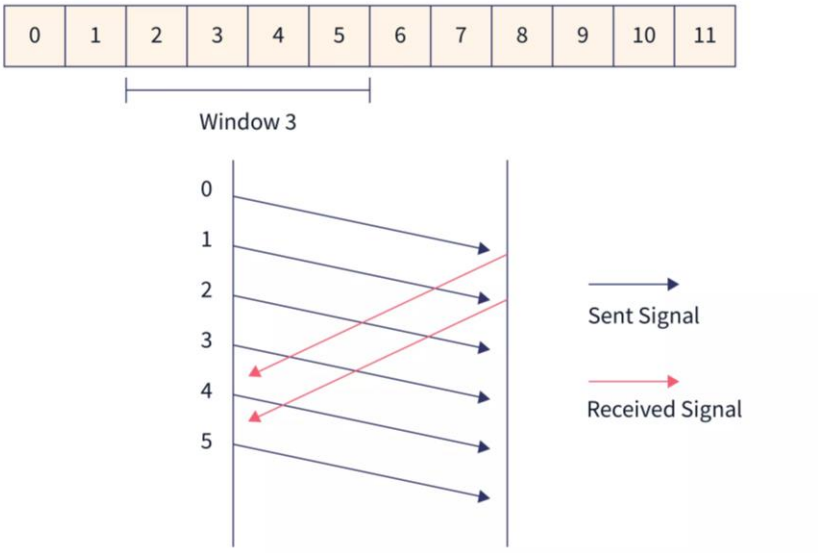
The stop and wait ARQ protocol sends a data frame and then waits for an acknowledgment or ACK from the receiver. The ACK means that the receiver has successfully received the data frame. After the sender receives the ACK from the receiver, it sends the next data frame. So, there is a wait and then the next data frame is transmitted so the name came **Stop and Wait ARQ** protocol.



Go Back N ARQ

Go Back N ARQ is a **sliding window protocol** which is used for flow control purposes. Multiple frames present in a single window are sent together from sender to receiver.

Pipelining is allowed in the Go Back N ARQ protocol. **Pipelining means sending a frame before receiving the acknowledgment for the previously sent frame.**

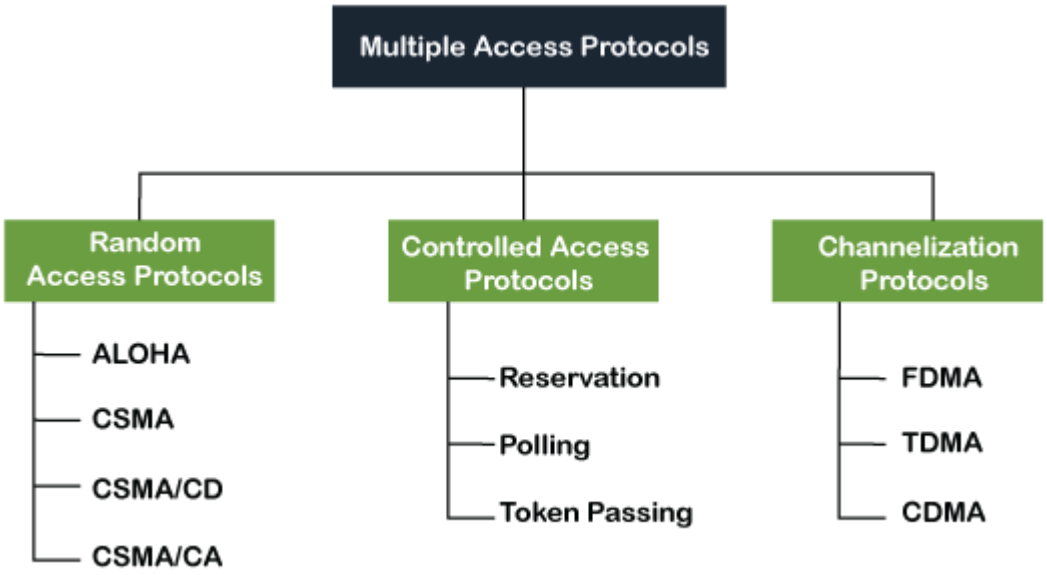


Multiple Access Control

Data link layer divided into two sub-layers Logical link control and Media Access Control. Media Access Control is responsible for Multiple Access Protocols.

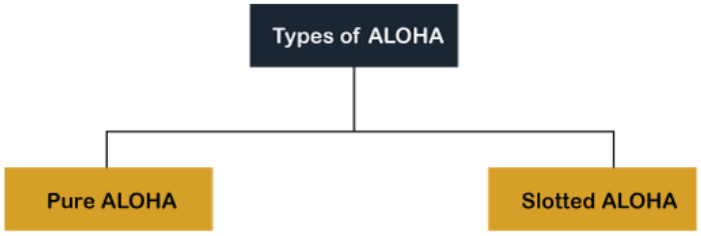
Multiple Access Protocols are used in wireless communication networks to control how multiple devices share the same communication channel.

following are the types of multiple access protocol that is subdivided into the different process as:



A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on each other nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver at the end.



 # Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. **In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not**, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not

acknowledge the receiver end within the specified time, (the station waits for a random amount of time, called the backoff time (Tb)). then the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver end.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

ALOHA is considered a simple and easy-to-implement protocol, but it has low efficiency and low throughput due to the high probability of collisions. It has been mainly used as a reference point and inspiration for more advanced MAC protocols, such as **CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).**

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

Ethernet LANs

Ethernet LANs (Local Area Networks) are networks that use Ethernet technology to connect computers and other devices together in a localized area, such as a home, office, or building. Ethernet is a widely-used standard for local area networking, and is defined by the IEEE 802.3 standard. Ethernet LANs can be either wired or wireless. Wired Ethernet LANs use cables, such as twisted pair or fiber optic cables, to connect devices together. Wireless Ethernet LANs use wireless technology, such as Wi-Fi, to connect devices without the need for physical cables. Ethernet LANs can be used to connect a variety of devices, including computers, printers, and servers, and are commonly used to share resources such as internet access, files, and printers among the devices on the network.

 # Connecting LANs

Connecting LANs (Local Area Networks) refers to the process of connecting multiple separate LANs together to form a larger network. This allows devices on one LAN to communicate and share resources with devices on another LAN. There are several methods for connecting LANs, including the use of routers, switches, and bridges.

- Routers: Routers are devices that connect multiple networks together and forward data packets between them. They use routing tables and protocols to determine the best path for data to travel between networks.
- Switches: Switches are network devices that connect multiple devices together on a LAN. They can also be used to connect multiple LANs together by creating virtual LANs (VLANs).
- Bridges: Bridges are devices that connect two LANs together by forwarding data between them at the data link layer (layer 2) of the OSI model.

Another way to connect LANs is using VPN (Virtual Private Network) that allows devices on one LAN to securely communicate with devices on another LAN over a public network, such as the internet.

Connecting LANs together allows for better communication and resource sharing between devices on different networks. This is particularly useful in large organizations with multiple office locations, as it allows employees to access resources and communicate with each other as if they were all on the same LAN.

Unit- 4

Switching techniques

Network switching is a method used in computer networking to forward data packets between devices on a LAN (Local Area Network). It is performed at the data link layer.

When a device on a network sends a packet of data, the switch receives the packet and examines the destination address. The switch then forwards the packet to the appropriate device on the network. This is called packet switching.

it only forwards packets to the intended destination device, rather than broadcasting to all devices on the network. This reduces network congestion and improves overall network performance.

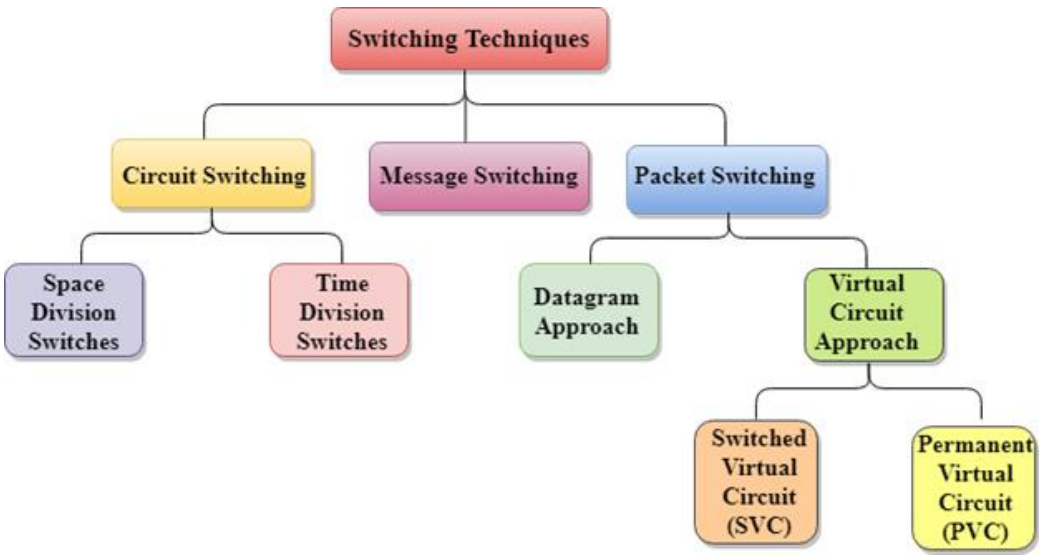
Switching can be done using both hardware and software. Hardware switches are physical devices that are typically built into routers or other networking equipment. Software switches, on the other hand, are virtual switches that are implemented through software.

Additionally, there are several types of switching techniques such as circuit switching, packet switching, and message switching. Each switching technique has its own advantages and disadvantages and is used in different applications

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

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

Classification Of Switching Techniques



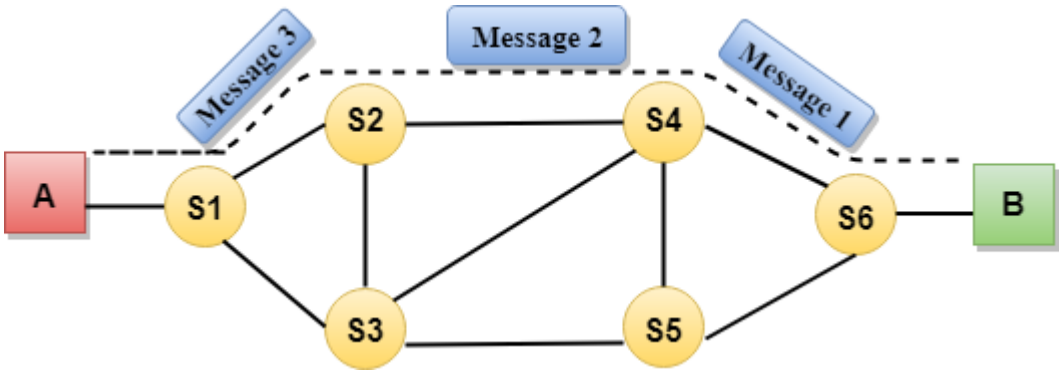
Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.

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

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit switching is a method of transmitting data on a network in which a dedicated physical path, or circuit, is established between two devices for the duration of their communication.

In circuit switching, a connection is established between the sender and receiver before any data is transmitted. This connection, or circuit, is reserved for the exclusive use of the two devices for the duration of the communication. Once the communication is finished, the circuit is broken and the resources are freed up for other devices to use.

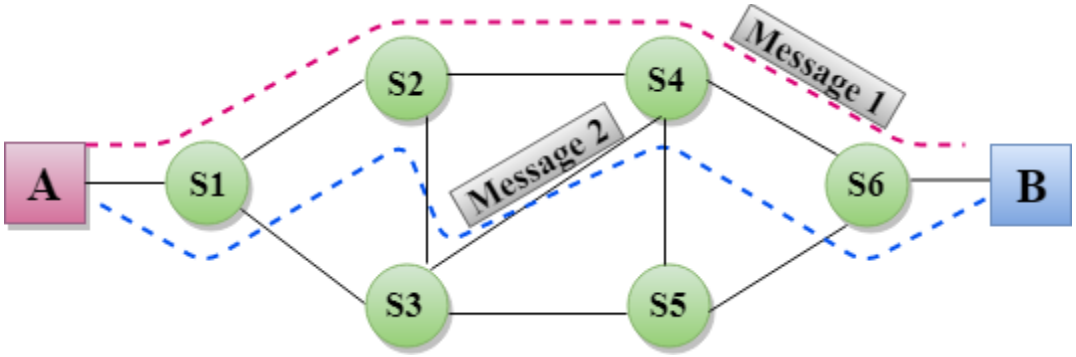
An example of circuit switching is a **traditional telephone system.** When you make a telephone call, a circuit is established between your phone and the person you are calling. The circuit remains open for the duration of the call and is then disconnected when you hang up.

In modern communication networks, packet switching is used more widely, as it allows for more efficient use of network resources.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.

- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Packet Switching

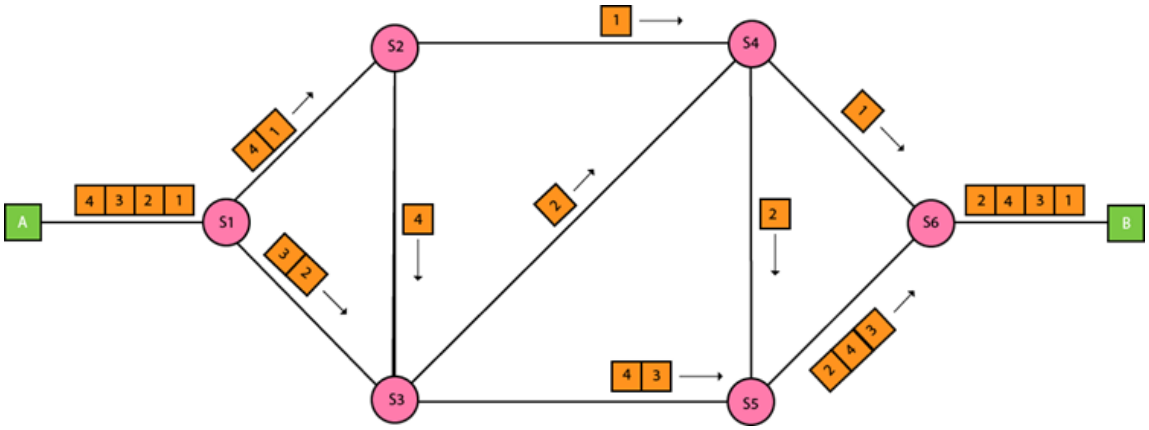
Packet switching is a method of transmitting data across a network in which data is divided into small packets, each with a header that contains routing information. The packets are sent independently through the network, with each node along the way forwarding the packet to the next node based on the routing information until it reaches its destination.

In packet switching, the data to be transmitted is divided into small packets, each with a header that contains routing information. The packets are then sent independently through the network, with each node along the way forwarding the packet to the next node based on the routing information until it reaches its destination.

The main advantage of packet switching is that it allows multiple transmissions to occur simultaneously, which increases network efficiency and allows for more efficient use of network resources.

Additionally, if a packet encounters an error, it can be re-transmitted without affecting the rest of the transmission. Also, if a node or link becomes unavailable, the packets can be routed around it, allowing the transmission to continue.

Packet switching is the primary method used in modern networks, including the internet. The most common protocol for packet switching is the Internet Protocol (IP).



Datagram Packet switching:

Datagram packet switching, also known as connectionless packet switching, is a method of packet switching in which each packet is treated as an independent unit, with its own destination address, and is routed through the network independently of other packets. This means that each packet is routed based on its own header information, rather than being part of a larger communication session or connection.

In datagram packet switching, each packet is sent with its own header that contains the destination address and any other necessary routing information. Each node in the network examines the header of the packet and forwards it to the next node based on the information in the header.

One of the main advantages of datagram packet switching is that it allows for more efficient use of network resources, since each packet can be routed independently of other packets. This allows for multiple transmissions to occur simultaneously, increasing network efficiency.

Additionally, if a packet encounters an error, it can be re-transmitted without affecting the rest of the transmission. Also, if a node or link becomes unavailable, the packets can be routed around it, allowing the transmission to continue.

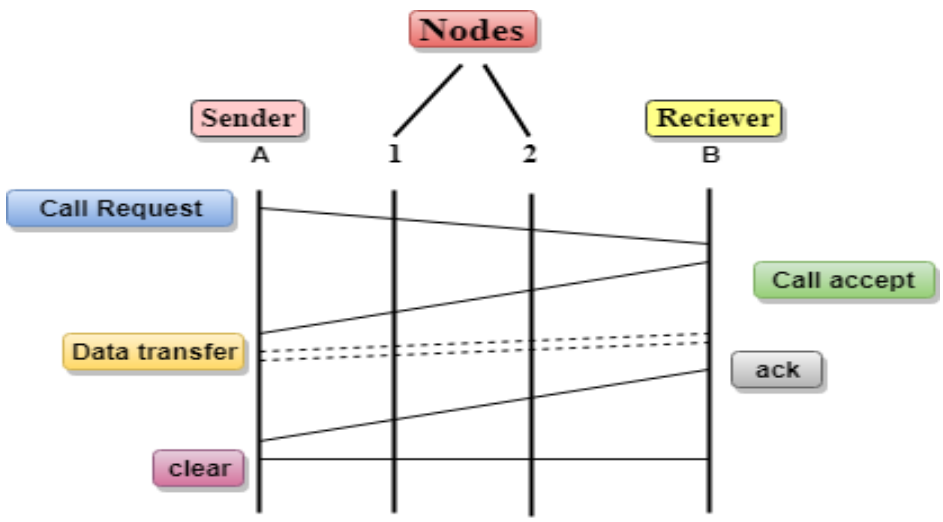
The most common protocol for datagram packet switching is the User Datagram Protocol (UDP).

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

Virtual Circuit Switching

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

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



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

Differences b/w Datagram approach and Virtual Circuit approach

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

Advantages Of Packet Switching:

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

Disadvantages Of Packet Switching:

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

Dial-up connection

Dial-up connection is a method of connecting to the internet that uses a telephone line. It works by using a modem, which is a device that converts the computer's digital signals into analog signals that can be transmitted over a telephone line. The modem at the other end of the connection then converts the analog signals back into digital signals that the computer can understand.

To establish a dial-up connection, the user must first connect their computer to a telephone line using a telephone cable. They then use software on the computer, such as a web browser or an internet service provider's (ISP) connection software, to initiate the connection. The software dials a telephone number provided by the ISP, and the modem at the other end of the line answers the call and establishes the connection.

Dial-up is the slowest form of internet connection, with speeds typically ranging from 56 kbps to about 114 kbps. It has largely been replaced by faster broadband connections such as DSL and cable, which offer much higher speeds and a more stable connection. Dial-up connection still exist and is used in remote rural areas where DSL or cable are not available.