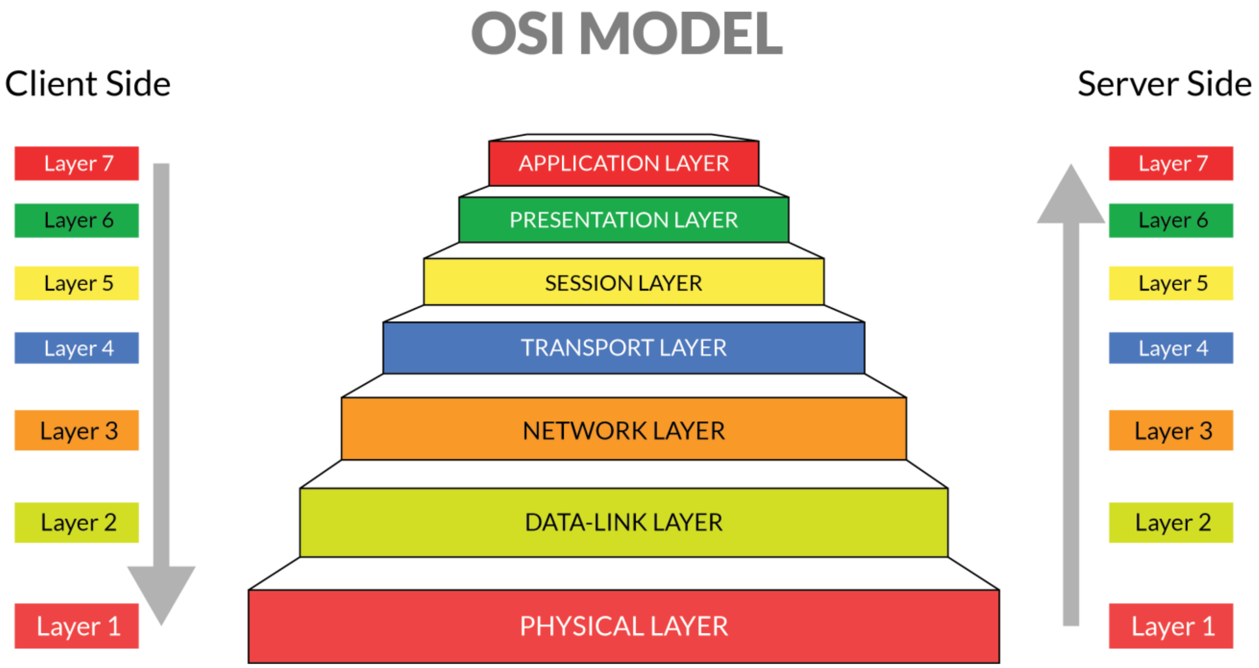
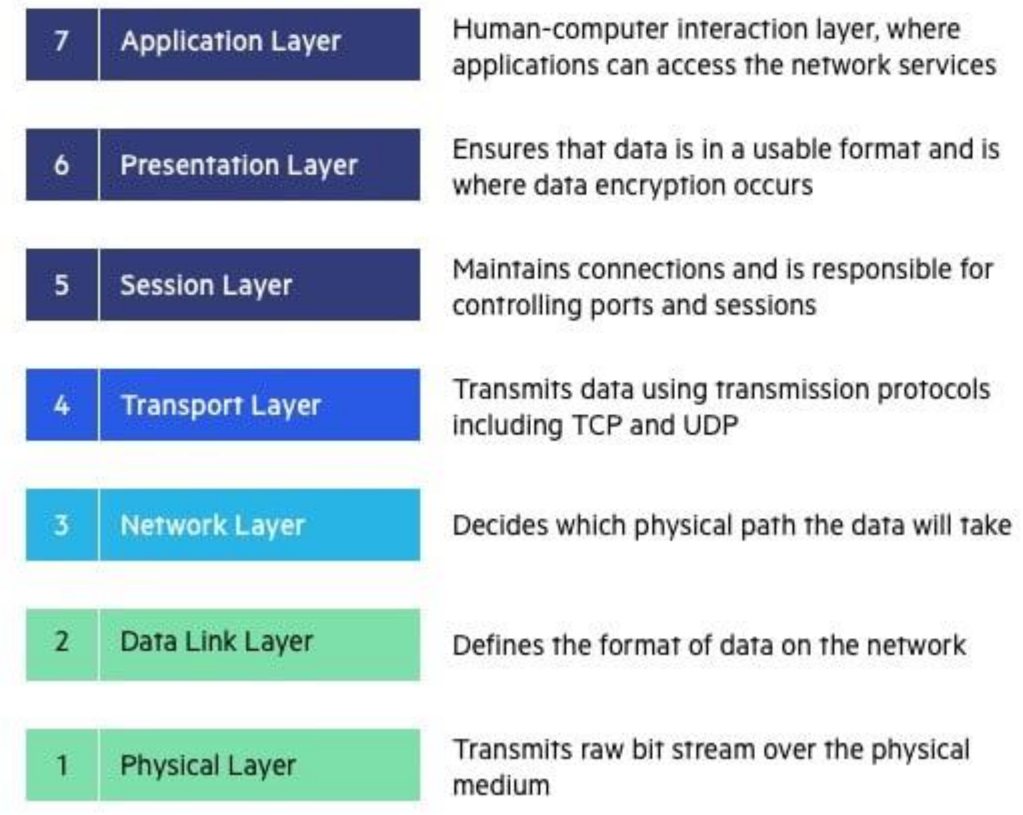
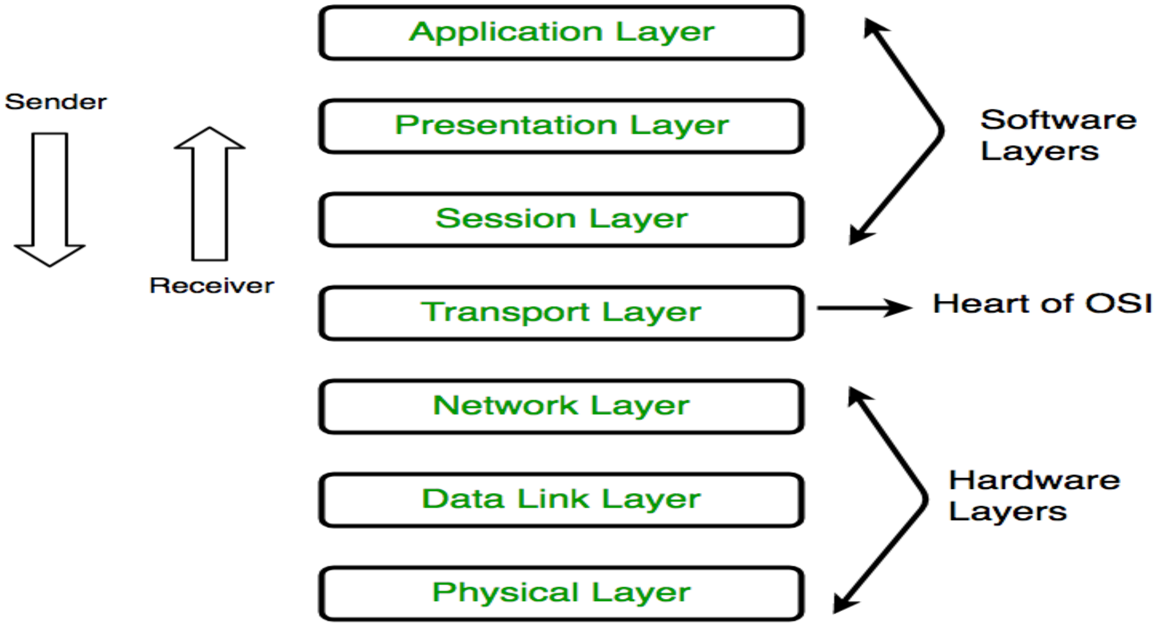
Unit: 1

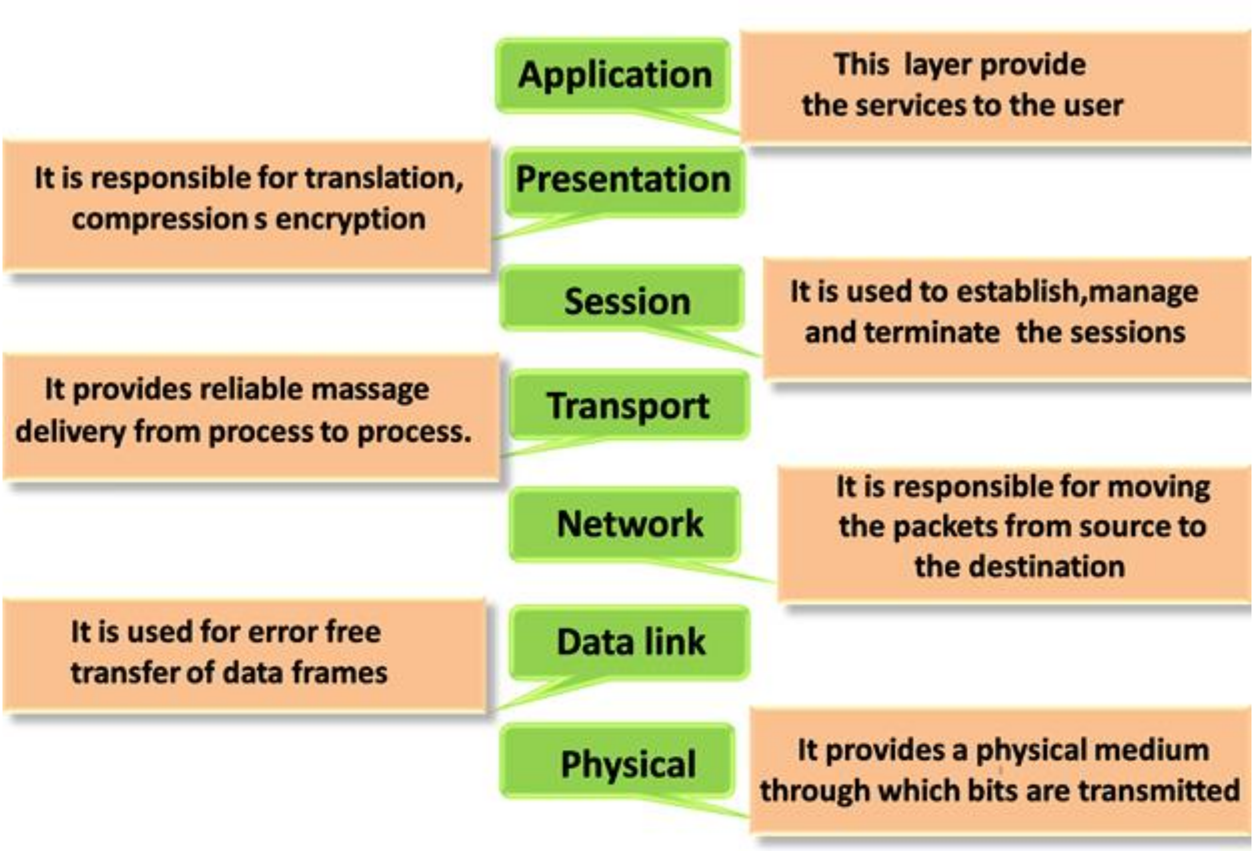




7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

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





This layer provide the services to the user

It is responsible for translation, compression s encryption

It is used to establish,manage and terminate the sessions

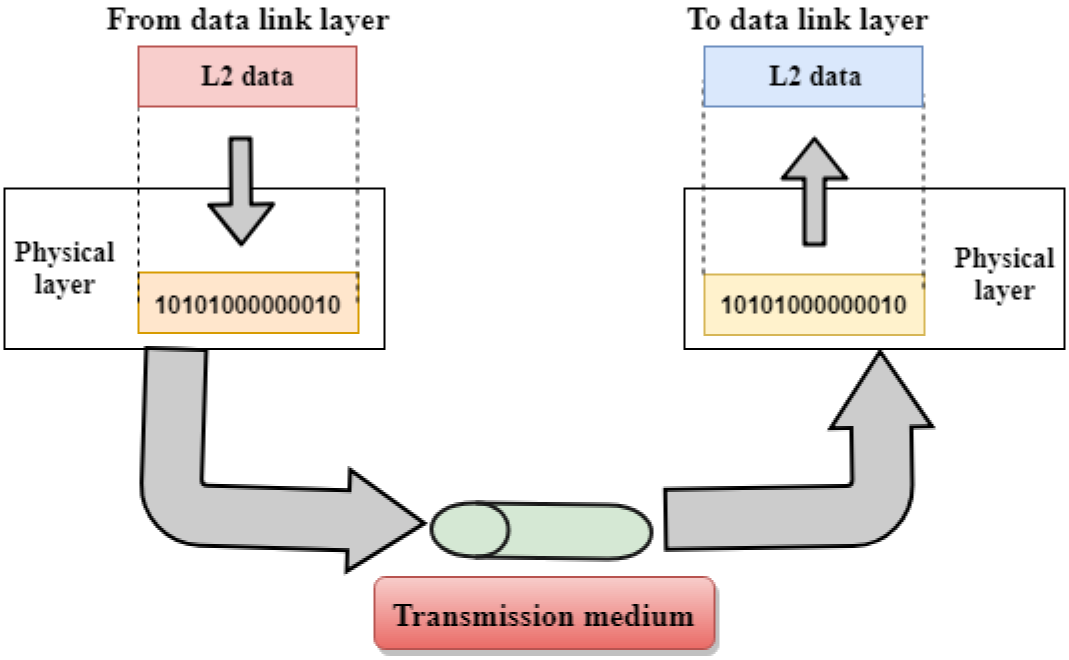
It provides reliable massage delivery from process to process.

It is responsible for moving the packets from source to the destination

It is used for error free transfer of data frames

It provides a physical medium through which bits are transmitted

1. Physical layer

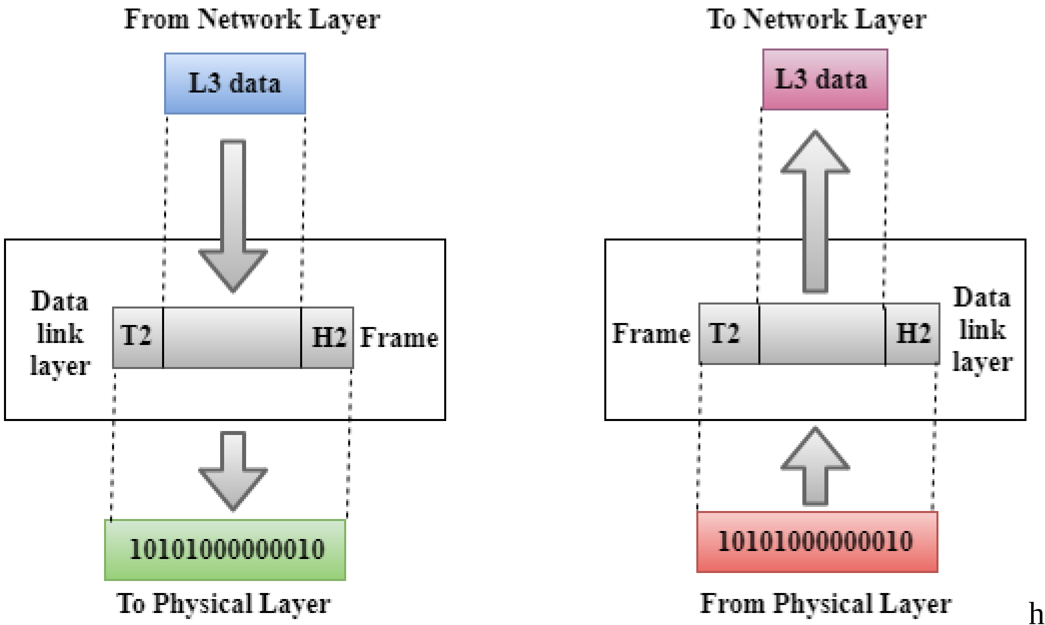


- ○ The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- ○ It is the lowest layer of the OSI model.
- ○ It establishes, maintains and deactivates the physical connection.
- ○ It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- ○ **Line Configuration:** It defines the way how two or more devices can be connected physically.
- ○ **Data Transmission**: It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- ○ **Topology**: It defines the way how network devices are arranged.
- ○ **Signals:** It determines the type of the signal used for transmitting the information.

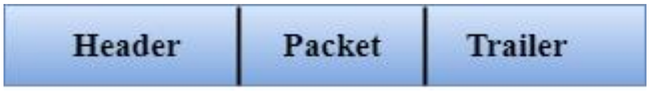
2. Data-Link Layer



- his layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - **Logical Link Control Layer**
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.
        - It also provides flow control.
    - **Media Access Control Layer**
        - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
        - It is used for transferring the packets over the network.

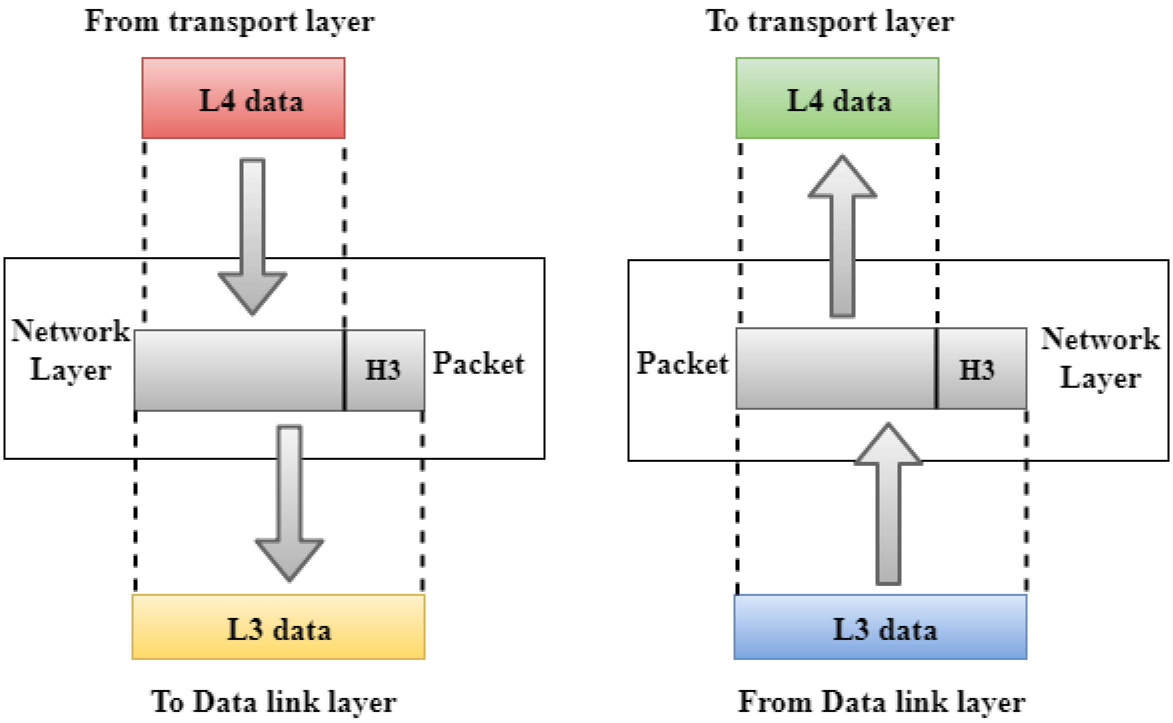
Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.



- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3. Network Layer



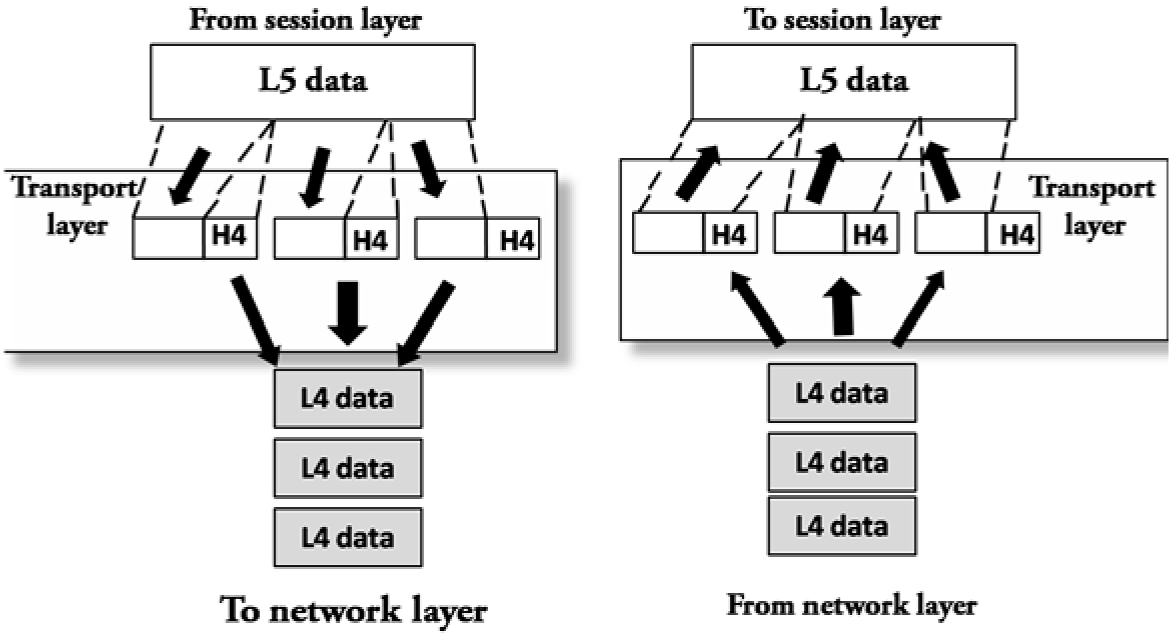
- It is a layer 3 that manages device addressing, tracks the location of devices on the network.

- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4. Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
    - It is a standard protocol that allows the systems to communicate over the internet.
    - It establishes and maintains a connection between hosts.
    - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
    - User Datagram Protocol is a transport layer protocol.
    - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

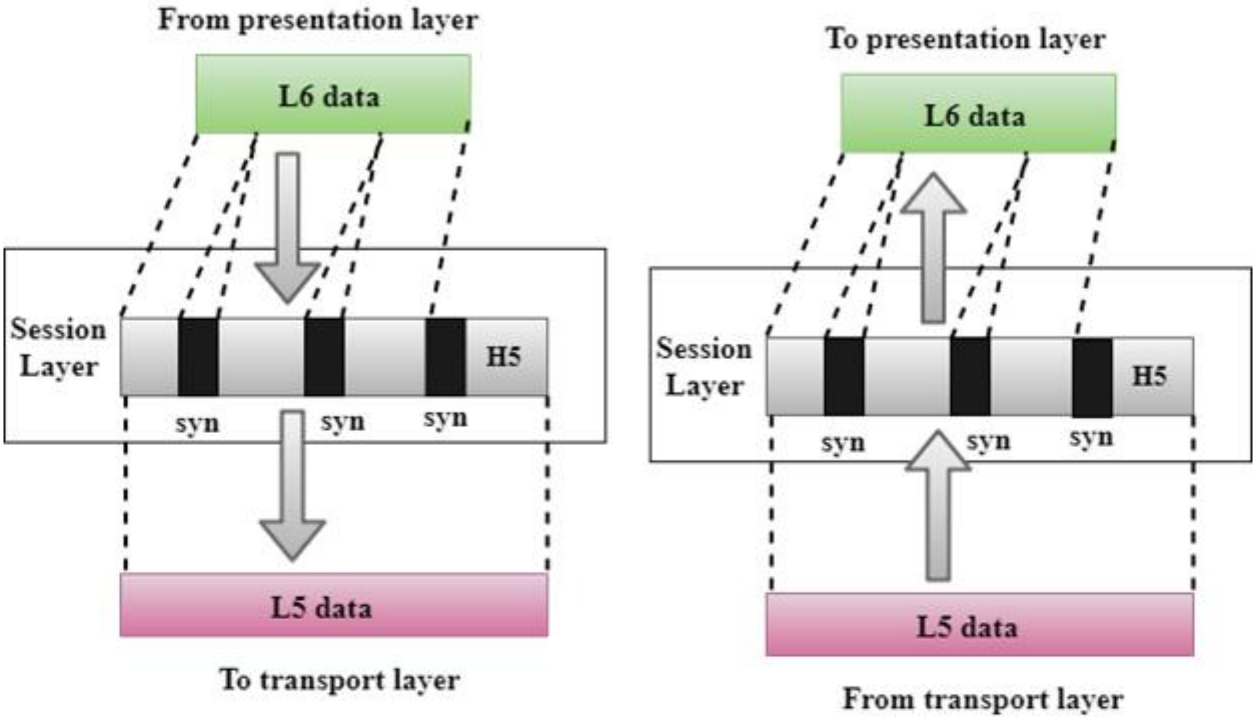
Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has

arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5. Session Layer

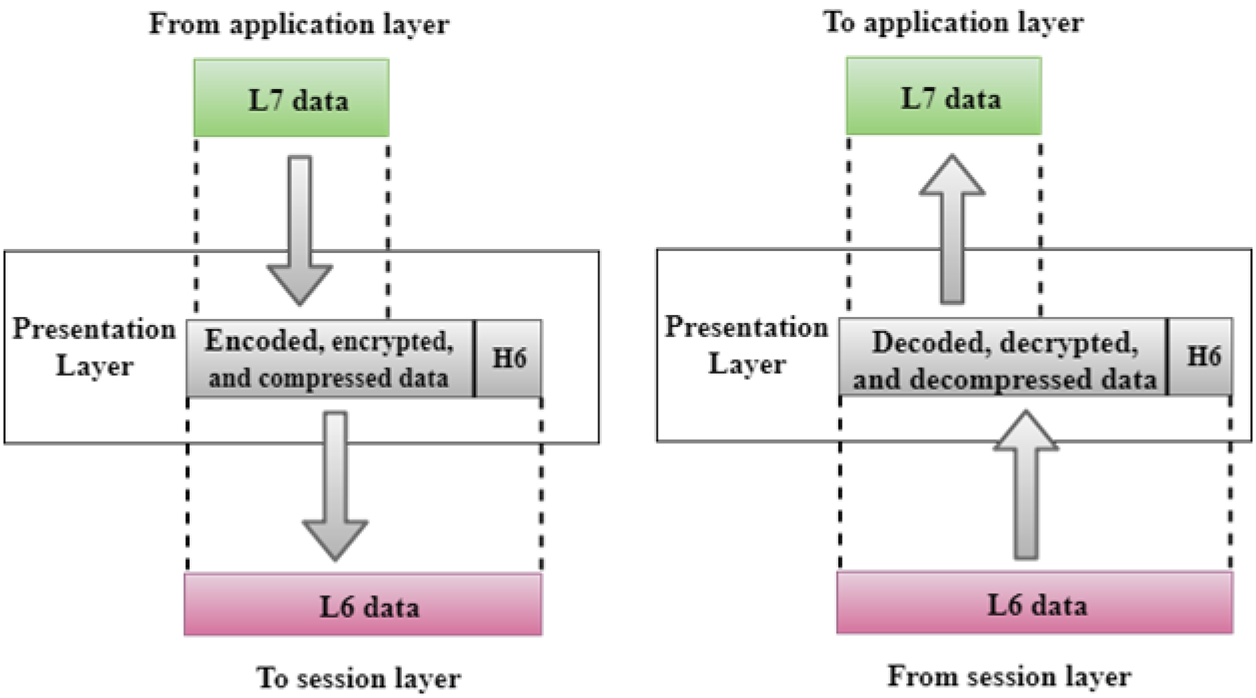


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6. Presentation Layer



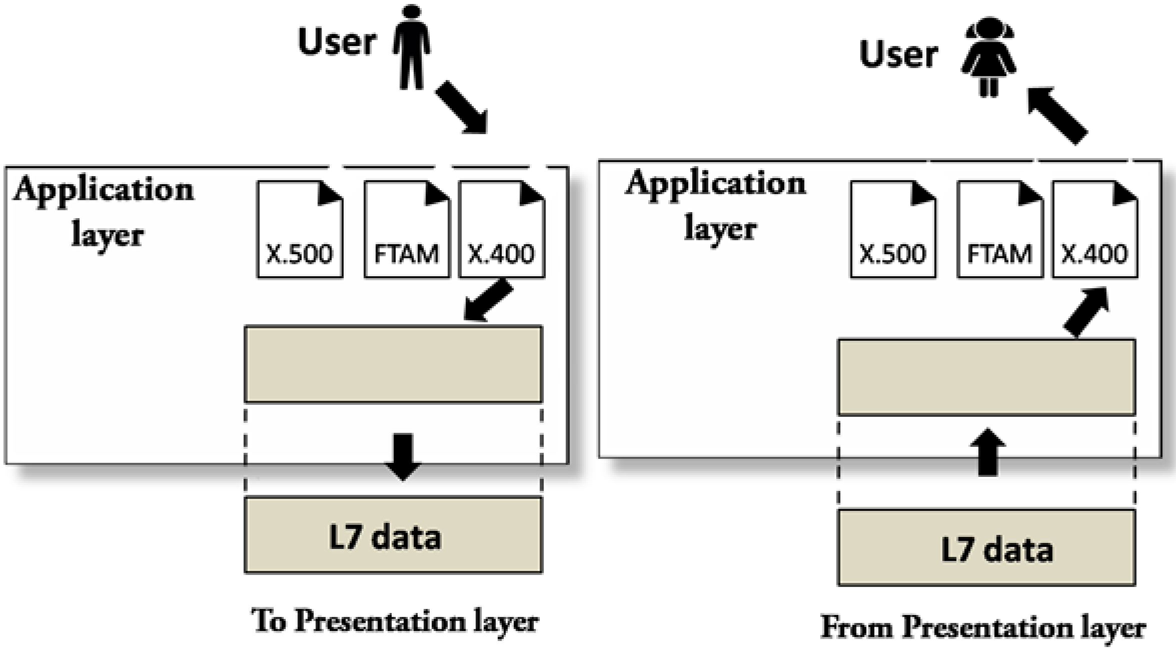
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7. Application Layer



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

Physical Layer is the bottom-most layer in the **Open System Interconnection (OSI) Model** which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, receivers, cable types, etc. Physical Layer sends data bits from one device(s) (like a computer) to another device(s). Physical Layer defines the types of encoding (that is how the 0's and 1's are encoded in a signal). Physical Layer is responsible for the communication of the unstructured raw data streams over a physical medium.

Functions Performed by Physical Layer :

Following are some important and basic functions that are performed by the Physical Layer of the OSI Model –

1. Physical Layer maintains the data rate (how many bits a sender can send per second).
2. It performs Synchronization of bits.
3. It helps in Transmission Medium decision (direction of data transfer).
4. It helps in Physical Topology (Mesh, Star, Bus, Ring) decision (Topology through which we can connect the devices with each other).
5. It helps in providing Physical Medium and Interface decisions.
6. It provides two types of configuration Point to Point configuration and Multi-Point configuration.
7. It provides an interface between devices (like PC's or computers) and transmission medium.
8. It has a protocol data unit in bits.
9. Hubs, Ethernet, etc. device is used in this layer.
10. This layer comes under the category of Hardware Layers (since the hardware layer is responsible for all the physical connection establishment and processing too).
11. It provides an important aspect called Modulation, which is the process of converting the data into radio waves by adding the information to an electrical or optical nerve signal.

12. It also provides Switching mechanism wherein data packets can be forward from one port (sender port) to the leading destination port.

Physical Topologies :

Physical Topology or Network Topology is the Geographical Representation of Linking devices. Following are the four types of physical topology-

1. **Mesh Topology:** In a mesh topology, each and every device should have a dedicated point-to-point connection with each and every other device in the network. Here there is more security of data because there is a dedicated point-to-point connection between two devices. Mesh Topology is difficult to install because it is more complex.
2. **Star Topology:** In star topology, the device should have a dedicated point-to-point connection with a central controller or hub. Star Topology is easy to install and reconnect as compared to Mesh Topology. Star Topology doesn't have Fault Tolerance Technique.
3. **Bus Topology:** In a bus topology, multiple devices are connected through a single cable that is known as backbone cable with the help of tap and drop lines. It is less costly as compared to Mesh Topology and Star Topology. Re-connection and Re-installation are difficult.
4. **Ring Topology:** In a ring topology, each device is connected with repeaters in a circle-like ring that's why it is called Ring Topology. In Ring topology, a device can send the data only when it has a token, without a token no device can send the data, and a token is placed by Monitor in Ring Topology.

Point to Point configuration : In Point-to-Point configuration, there is a line (link) that is fully dedicated to carrying the data between two devices.

Multi-Point configuration : In Multi-Point configuration, there is a line (link) through which multiple devices are connected.

Modes of Transmission Medium :

1. **Simplex mode:** In this mode, out of two devices, only one device can transmit the data, the other device can only receive the data. Example- Input from keyboards, monitors, TV broadcasting, Radio broadcasting, etc.
2. **Half Duplex mode:** In this mode, out of two devices, both devices can send and receive the data but only one at a time not simultaneously. Example- Walkie-Talkie, Railway Track, etc.
3. **Full-Duplex mode:** In this mode, both devices can send and receive the data simultaneously. Example- Telephone System, Chatting applications, etc.

Physical layer is the lowest layer of the OSI reference model. It is responsible for sending bits from one computer to another. This layer is not concerned with the meaning of the bits and deals with the setup of physical connection to the network and with transmission and reception of signals.

Functions of Physical Layer

Following are the various functions performed by the Physical layer of the OSI model.

1. **Representation of Bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.

2. **Data Rate:** This layer defines the rate of transmission which is the number of bits per second.

3. **Synchronization:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.

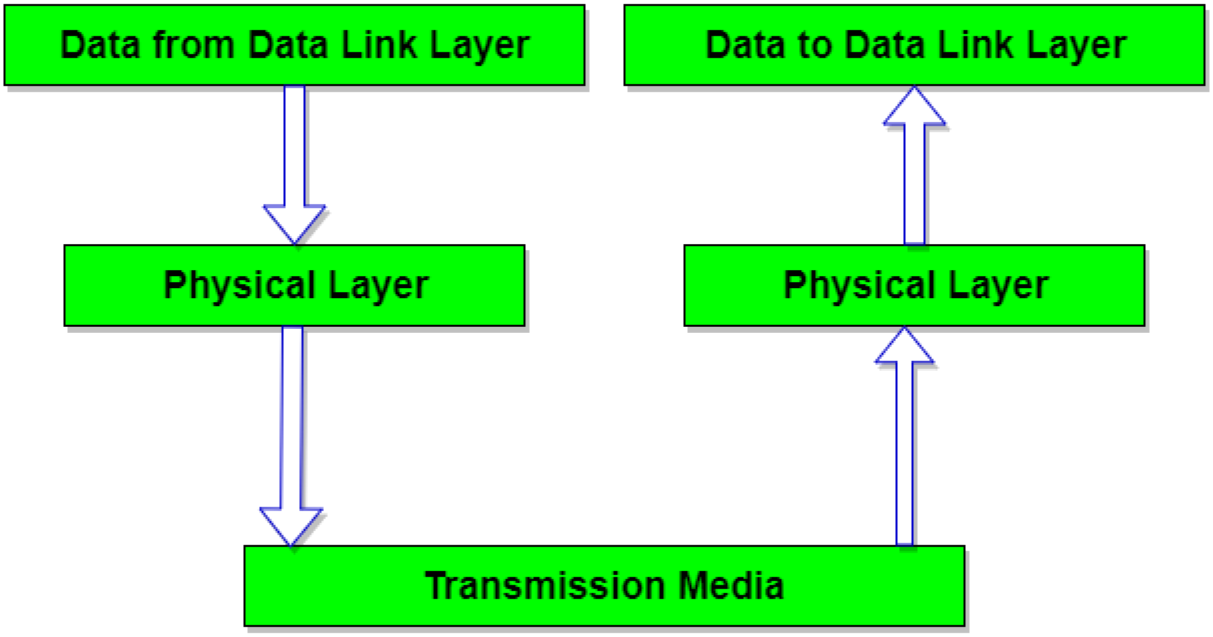
4. **Interface:** The physical layer defines the transmission interface between devices and transmission medium.

5. **Line Configuration:** This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.

6. **Topologies:** Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.

7. **Transmission Modes:** Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.

8. Deals with baseband and broadband transmission.

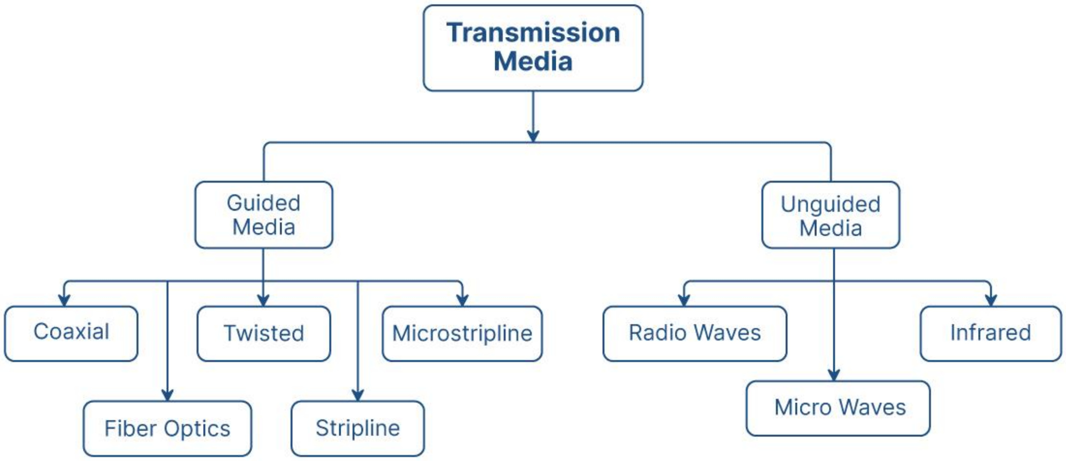


Design Issues with Physical Layer

- The Physical Layer is concerned with transmitting raw bits over a communication channel.

- The design issue has to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit and not as a 0 bit.

Transmission Media in Computer Network



A transmission medium is a route that transmits information from a source to a receiver. Transmission mediums lie underneath the physical layer and the physical layer regulates them. Communication channels are another name for transmission medium.

There are 2 types of transmission media:

- Guided
- Unguided

1. Guided Transmission Media:

Bounded media and wired media are other names for guided transmission media. They consist of cables or wires that transfer data. They go by the name "guided" because they act as a physical link between the transmitter and recipient devices. The physical limitations of the medium limit the signal flowing via these mediums. They are:

- Secure high-speed links.
- Generally used for shorter distances.

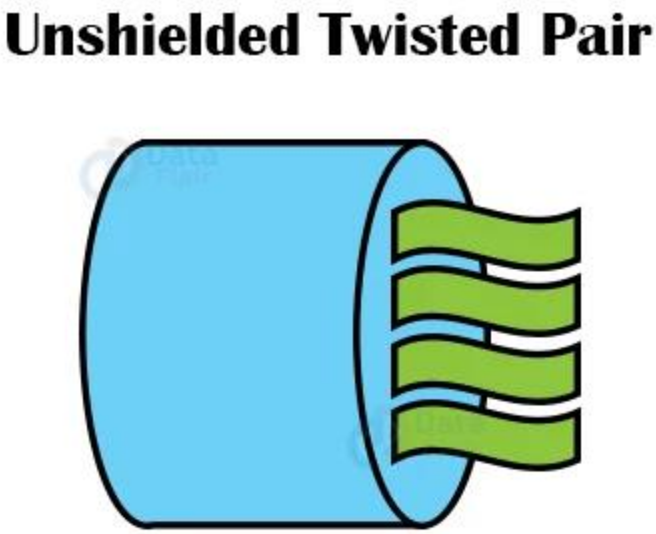
Some of these most popular guided transmission media are:

a. Twisted Pair Cable:

This is the most widely used transmission medium cable. It consists of two distinct insulated conductor wires coiled around each other. Several similar pairs are usually packed together in a protective sheath.

There are 2 broad types of twisted-pair cables:

i. Unshielded Twisted Pair:



- Provides a high speed link.
- The most affordable.
- Simple to set up.
- External interference is a possibility.
- When compared to Shielded Twisted Pair, it has a lower capacity and performance.

Unshielded Twisted Pair categories:

- **Category 1:** Category 1 twisted pair cables find use in low-speed telephone data transmission.
- **Category 2:** It has a maximum bandwidth of 4Mbps.
- **Category 3:** It has a maximum bandwidth of 16Mbps.
- **Category 4:** It has a maximum bandwidth of 20Mbps. As a result, it is suitable for long-distance communication.
- **Category 5:** It has a maximum bandwidth of 200Mbps.

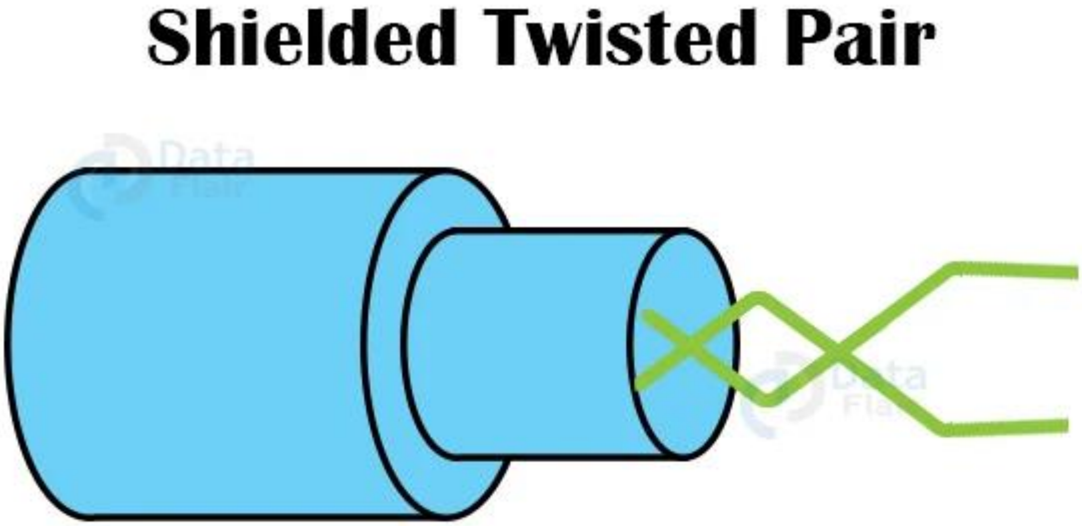
Advantages:

- It is inexpensive.
- The unshielded twisted pair is simple to install.
- It is suitable for high-speed LAN.

Disadvantages:

- Because of attenuation, this cable finds use in connectivity solutions for short distances.

ii. Shielded Twisted Pair:



- Installation and manufacturing are both somewhat challenging.
- Pricier.
- When compared to Unshielded Twisted Pair, it performs better at greater data rates.
- Faster in comparison.

Characteristics:

- The price of insulated twisted pair cable is neither extremely expensive nor very low.
- It has greater attenuation.
- Its insulation allows for a greater data transmission rate.

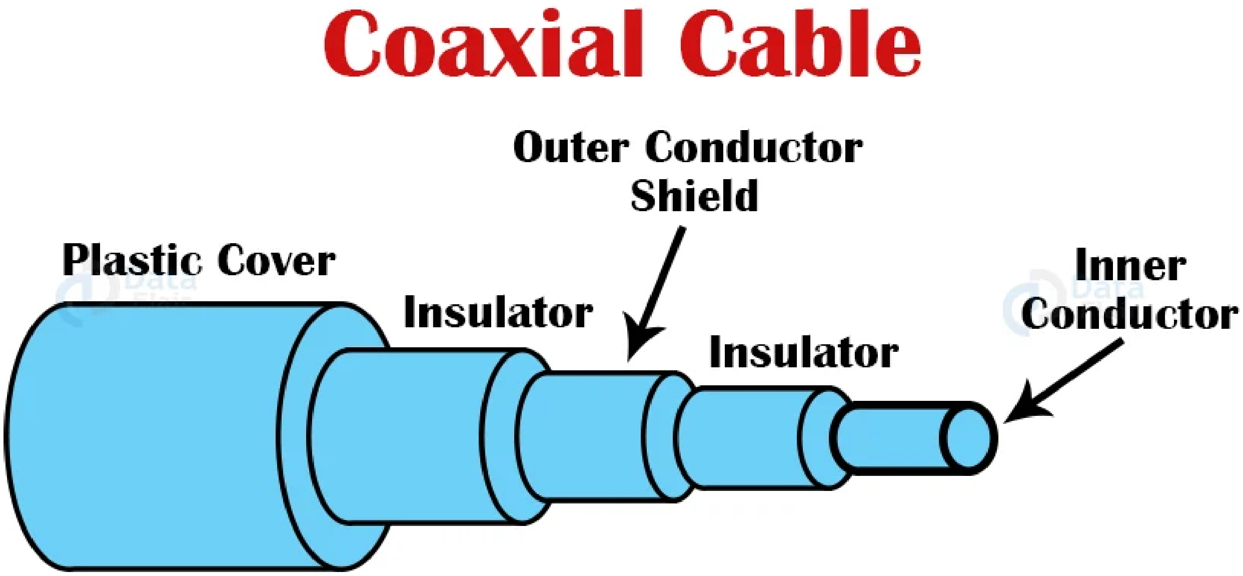
Advantages:

- STP installation is simple.
- It has a larger capacity than unshielded twisted pair cable.
- Higher rate of transmission.

Disadvantages:

- It is more costly than UTP and coaxial cable.
- It has a greater rate of attenuation.
- **Applications:**
- Local Area Networks
- Telephone Lines

b. Coaxial Cable:



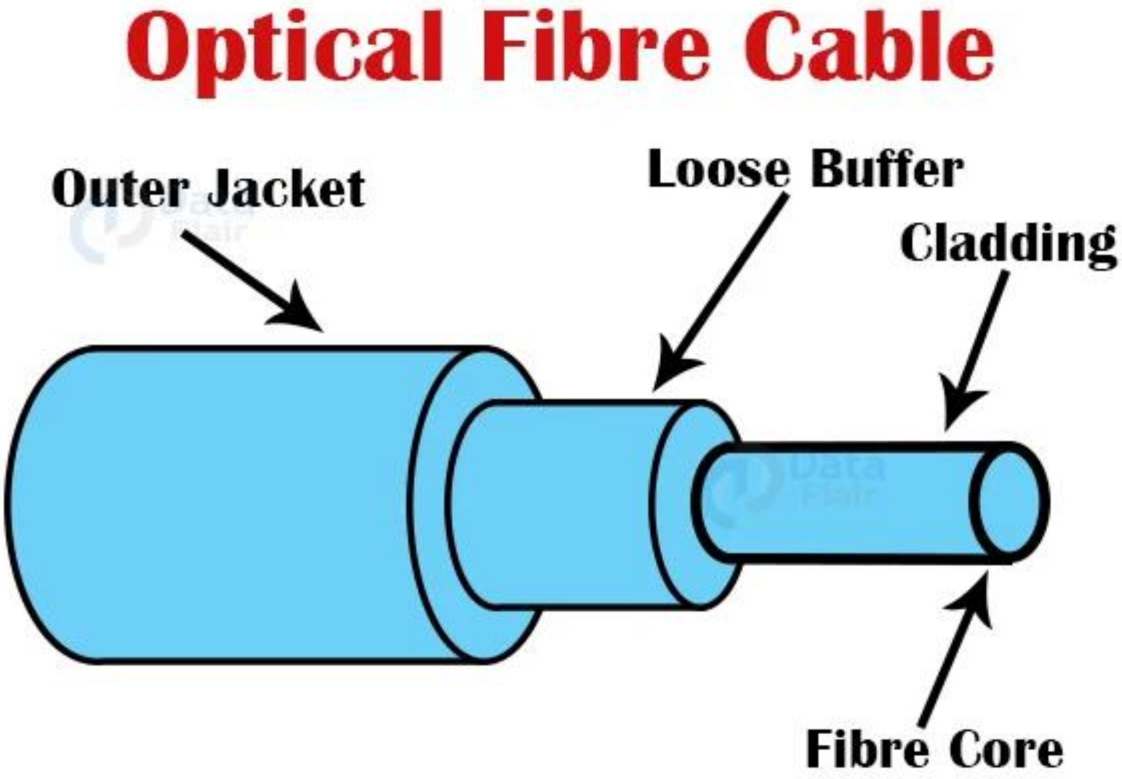
It features an exterior plastic covering and two parallel conductors, each with its own insulated protective cover. It operates in 2 ways: baseband and broadband.
Applications: Coaxial cables are commonly used in cable TV and analogue television networks.
i. Advantages:

- High bandwidth.
- Less susceptible to noise.
- Very cheap to install.
- Easy to install and upgrade.

ii. Disadvantages

- If there is a failure of the cable, the whole network may fail.

c. Optical Fibre Cable



It works on the principle of light reflection through a core composed of glass or plastic. The cladding surrounds the core, and the cladding is a less thick glass or plastic covering. It finds use in large-volume data transfer.
It is possible for the cable to be unidirectional or bidirectional.

Advantages and Disadvantages of optical fibre cable:

i. Advantages:

- Does not rust or corrode since there is no metal.
- Can transmit data at very high speed.
- Supports high bandwidth.
- There is less signal attenuation.
- Resistance to electromagnetic interference.

ii. Disadvantages:

- Installing and maintaining it is difficult.
- Fragile and expensive.

iii. Elements of optical fiber cable:

- **Core**: The core of an optical fiber is a small strand of glass or plastic. A core is the part of the fibre that transmits light. The amount of light transferred into the fibre depends upon the area of the core.
- **Cladding**: Cladding refers to the concentric layer of glass. The primary function of the cladding is to produce a lower refractive index at the core interface, causing reflection within the core and allowing light waves to pass through the fibre.

- **Jacket**: A jacket is a type of protective layer made of plastic. The primary function of a jacket is to retain fibre strength, absorb stress, and provide further fibre protection.

Applications of Fibre Optic cables:

- Backbone Networks
- Some local area networks and cable networks.

d. Stripline cable:

It is also known as a waveguide and it transmits high-frequency waves using a conducting substance.
This conductive substance is placed between two ground plane layers that are often short-circuited to offer EMI immunity.

e. Microstripline cable:

A dielectric layer separates the conducting material from the ground plane in this case.

f. Power Lines:

Layer-1 (Physical Layer) technology that uses power cables to transmit data signals is known as power line communication (PLC). Modulated data is sent over the cables in a PLC. The data is de-modulated and interpreted by the receiver on the other end.

g. Magnetic Media:

Even before networking, one of the most convenient ways to transfer data from one computer to another was to save it on storage media and physically transfer it from one station to another. Magnetic media is useful when the amount of data to be transferred is very large.

2. Unguided Transmission Media:

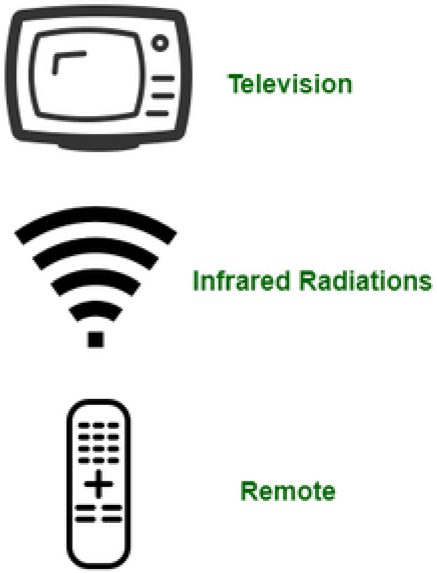
Electromagnetic signals can also be transmitted without the use of a physical medium. These are also known as wireless or unbounded transmission media.

Some properties of unguided media are:

- Less secure than guided media.
- Used for longer distances.

Types of UnGuided Transmission Media:

a. *Infrared:*



When there is a need for very short-range communication, infrared waves are used. However, they fail to penetrate any walls/obstacles in the way of the signal.

The frequency ranges from 300 GHz to 400 THz.

Characteristics of infrared transmission:

- It has a large bandwidth, thus the data rate will be quite high.
- Infrared waves are unable to permeate the walls. As a result, infrared communication in one room cannot be disrupted by surrounding rooms.
- Infrared communication is more secure and also causes less interference.
- Outside the building, infrared communication is unreliable because the sun's rays interfere with the infrared radiation.

Advantages:

- Cost-effective and cheap.
- Large bandwidth.
- Easy to install.
- Can be operated without any licence.

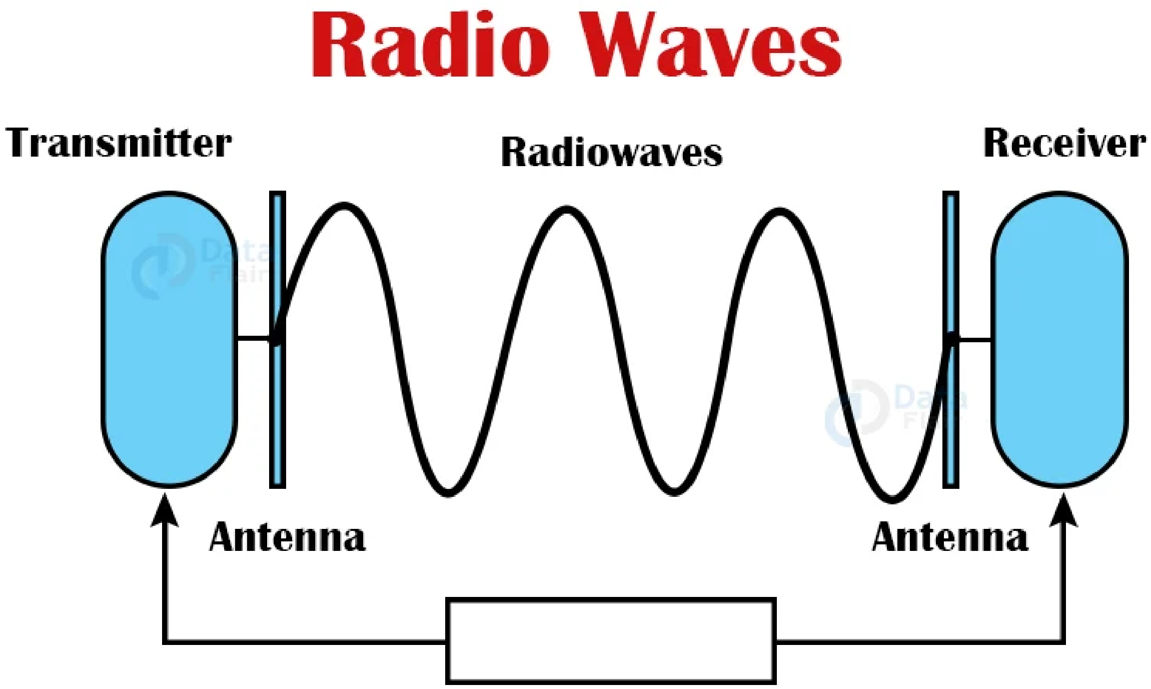
Disadvantages:

- Cannot cross barriers.
- Long-range communication is not possible.

Applications:

- Short-range communication
- Communication between keyboards, PCs and mouse.

b. Radio waves:



Very commonly used and very simple to generate. These types of waves can pass through obstacles easily. Two antennas are used, one for the transmitting station and one for the receiving station (these antennas need not be aligned).

The frequency ranges from 3 kHz to 1GHz.

Advantages of Radio Transmission:

- Radio transmission is mostly utilised for wide area networks and mobile phones.
- Radio waves may penetrate barriers and cover a broad area.
- Faster transmission speed.

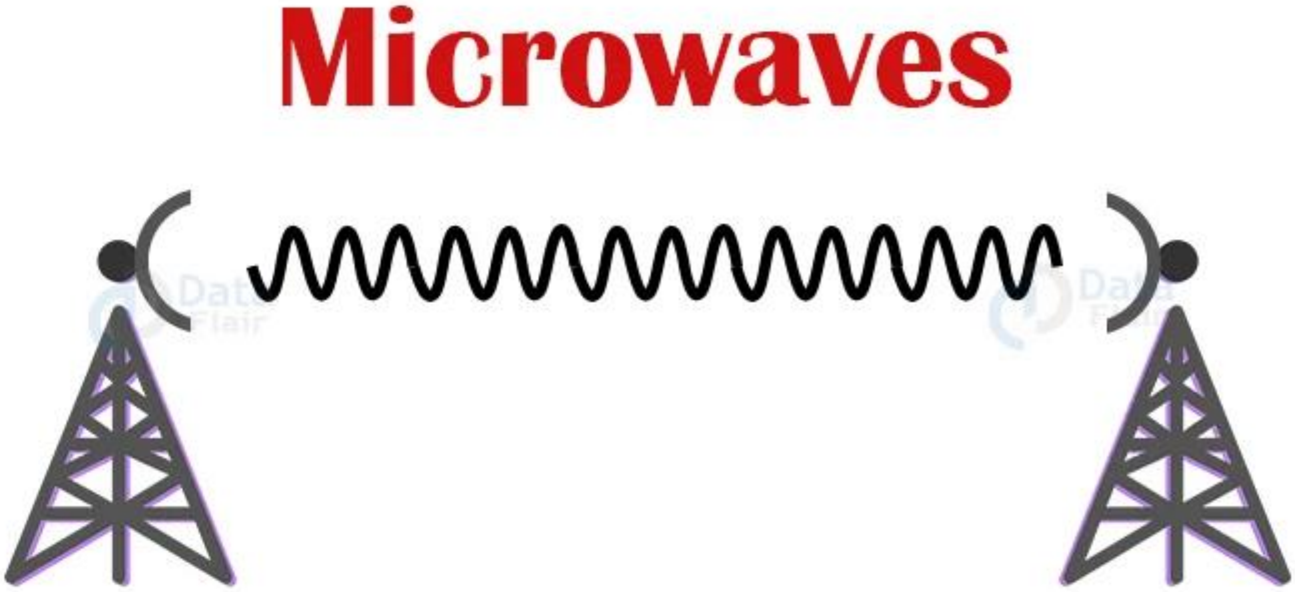
Disadvantages:

- Regulation of radio spectrum, thus it is expensive to buy.
- Cannot permeate matter very well.
- Cannot travel above the horizon because of the curvature of the earth.

Applications:

- AM and FM Radio
- Cordless phones

c. Microwaves:



It is a line-of-sight transmission, which means that the transmitting and receiving antennas must be correctly aligned. The distance reached by the signal is proportional to the antenna's height. These are mostly utilised for mobile phone communication and television broadcasting.

The frequency ranges from 1 GHz to 300GHz.

Characteristics of microwave:

- Frequency range: 4 to 23 GHz.
- Bandwidth: It provides bandwidths ranging from 1 to 10 Mbps.
- Short distance: Suitable for short distance communication.
- Long distance: It is costly since a larger tower is required for a longer distance.
- Attenuation: Weakening of a signal is referred to as attenuation. Antenna size can change attenuation.

Advantage of microwave transmission:

- Microwave transmission is cheaper than cable transmission.
- It does not necessitate the acquisition of land since the installation of cables does not necessitate the acquisition of land.
- Microwaves are more convenient in places where installing cables is difficult.
- Microwave transmission can be used to communicate across seas.

Disadvantages of microwave transmission:

- Eavesdropping: Eavesdropping makes communication unsafe. Any rogue user with its own antenna can capture the signal in the air.
- Out of phase signal: Signal may shift out of phase.
- Weather condition: Any environmental disturbance may cause the signal distortion.
- Bandwidth allocation: Less bandwidth is available.

Applications;

- Satellite Networks

- Cell phones

d. Light Transmission:

Light or optical signalling is the most powerful electromagnetic spectrum that may be utilised for data transmission. LASER is used to do this.

Because of the frequency at which light travels, it tends to move in a straight path.

As a result, the transmitter and receiver must be in direct line of sight. Because laser transmission is unidirectional, the laser and photodetector must be deployed at both ends of the connection. Because laser beams are typically 1mm broad, aligning two distant receptors, each pointed to the laser's source, is a precise task.

Analog Transmission

To send the digital data over an analog media, it needs to be converted into analog signal.There can be two cases according to data formatting.

Bandpass: The filters are used to filter and pass frequencies of interest. A bandpass is a band of frequencies which can pass the filter.

Low-pass: Low-pass is a filter that passes low frequencies signals.

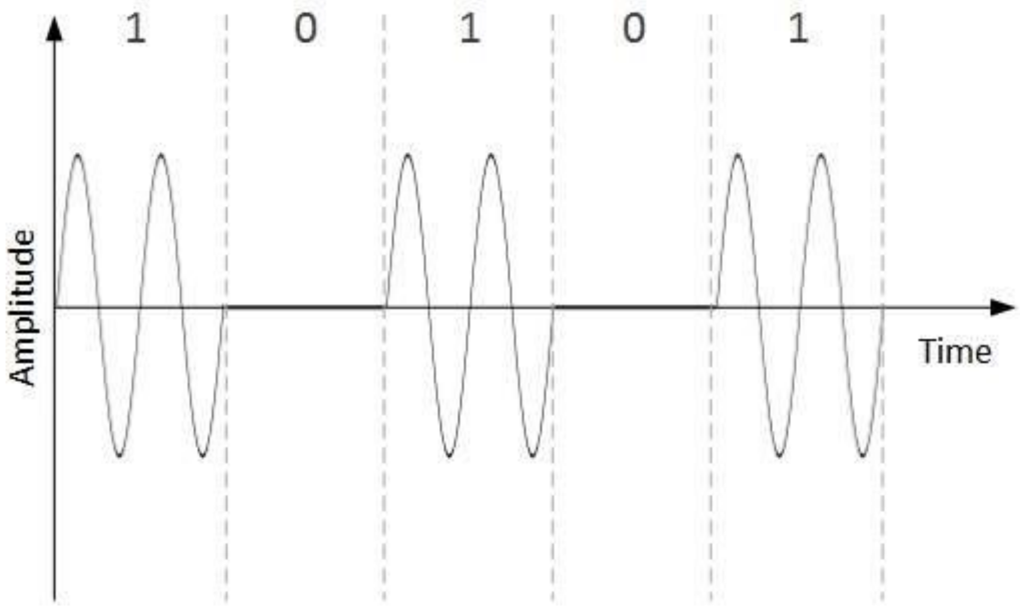
When digital data is converted into a bandpass analog signal, it is called digital-to-analog conversion. When low-pass analog signal is converted into bandpass analog signal, it is called analog-to-analog conversion.

Digital-to-Analog Conversion

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

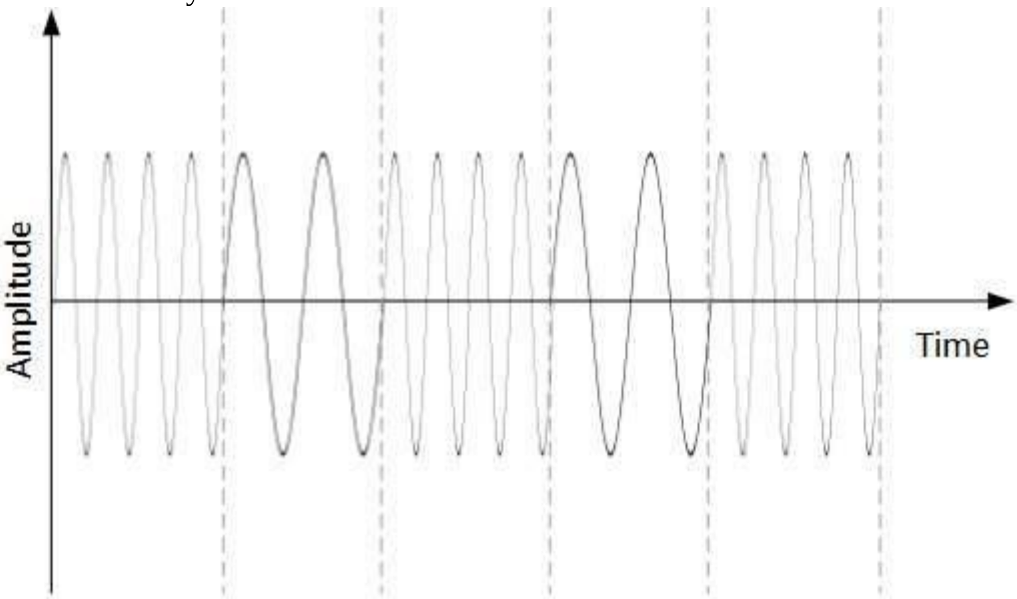
- **Amplitude Shift Keying**
  In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

- **Frequency Shift Keying**

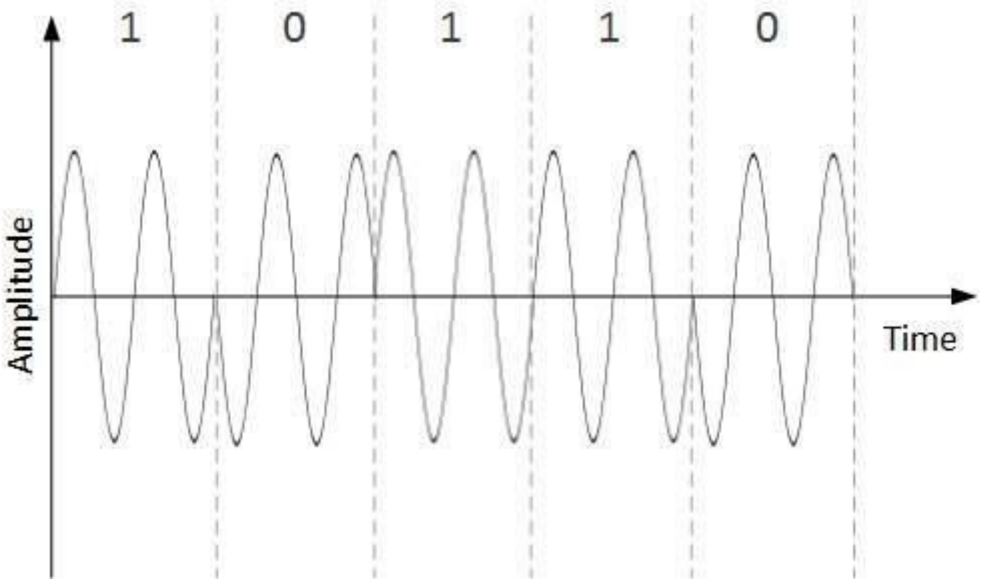
  In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



  This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

- **Phase Shift Keying**

  In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.

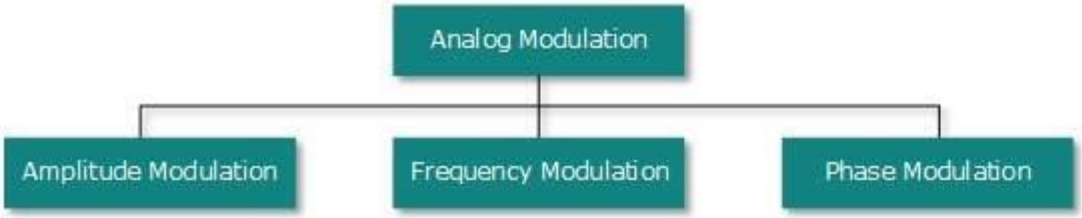


When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

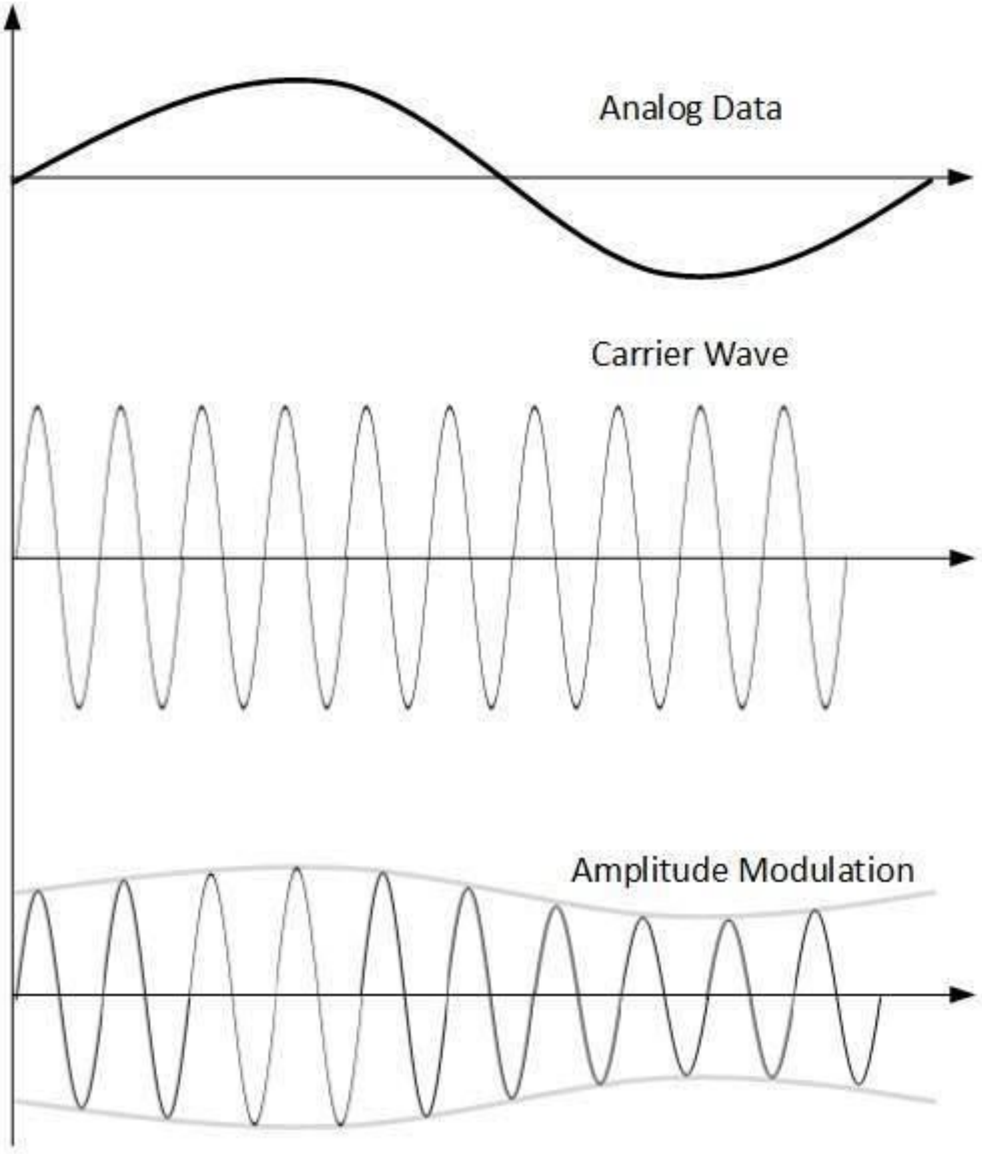
- **Quadrature Phase Shift Keying**
  QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

Analog-to-Analog Conversion

Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways:



- **Amplitude Modulation**
  In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.

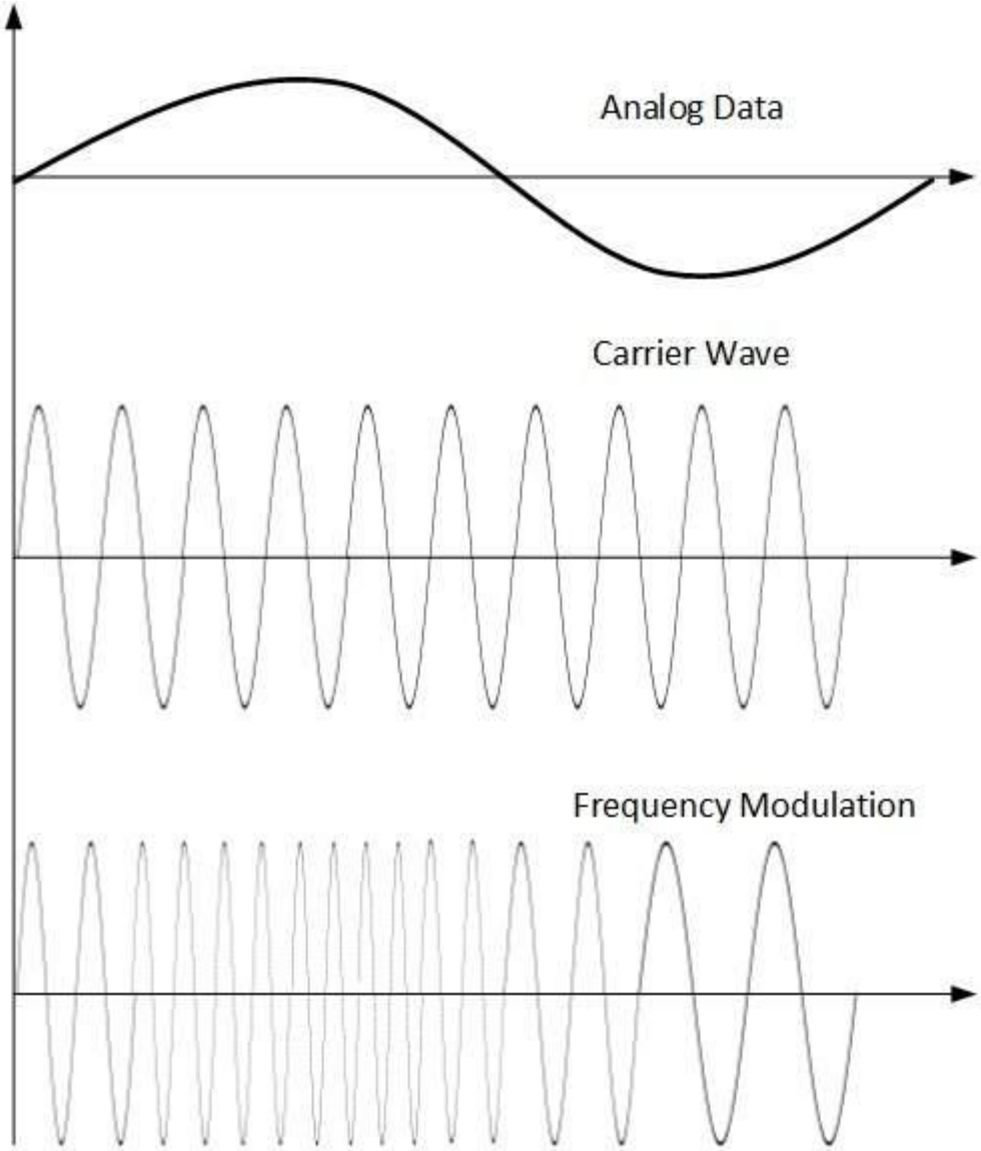


Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.

The frequency and phase of carrier signal remain unchanged.

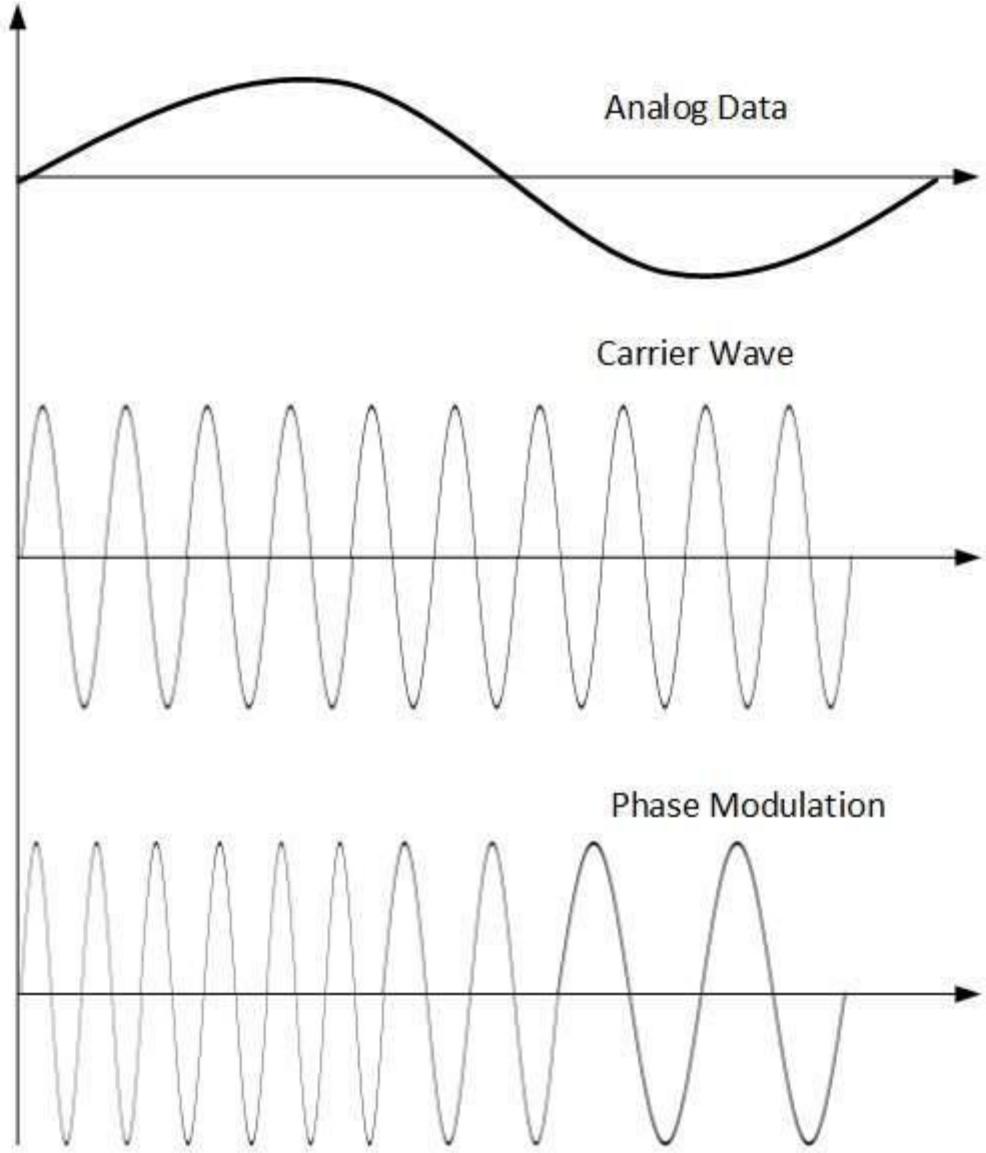
- **Frequency Modulation**

  In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).



The amplitude and phase of the carrier signal are not altered.

- **Phase Modulation**
  In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.



Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

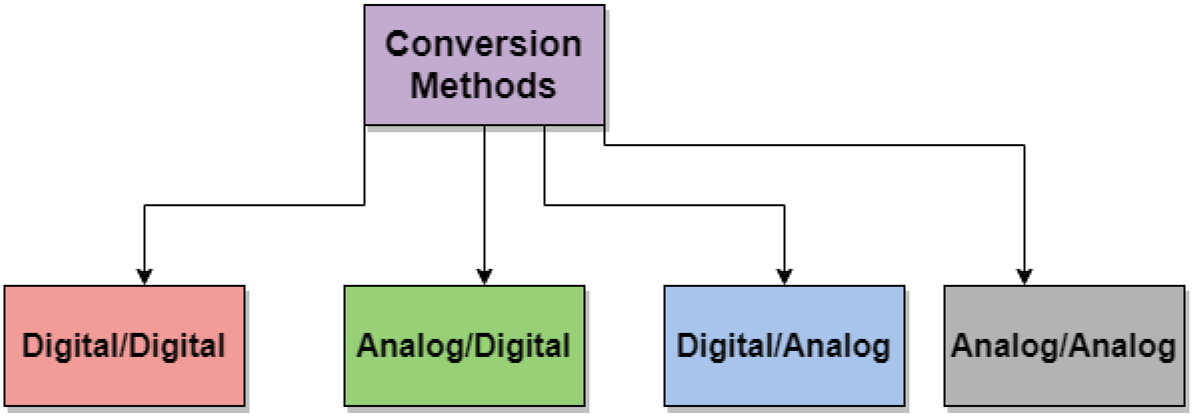
Digital Transmission

data is represented in two forms either analog or digital. The Computer can only understand the binary language that is of the form of 0 or 1 and also stores the information in the digital form.

Thus we need to convert the data into digital form so that it can be understood by the computer.

Given below are the conversion methods used for data transmission:

- Digital-to-Digital Conversion
- Analog-to-Digital Conversion
- Digital-to-Analog Conversion
- Analog-to-Analog Conversion



As we want to convert our data into digital form. Thus we will cover **Digital-to-Digital Conversion** and **Analog-to-Digital Conversion**

1.Digital-to-Digital Conversion

As we have already told you that data can either be in analog form or in digital form. So let us learn how can we represent digital data in the form of digital signals.

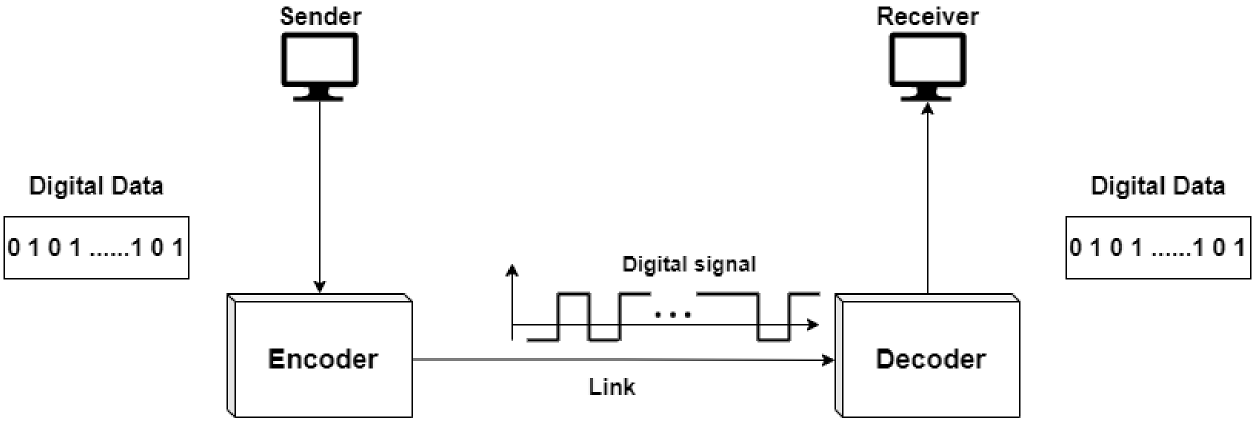
Three techniques used for this conversion are as follows:

- Line Coding
- Block Coding
- Scrambling

Line Coding

It is the process used to convert digital data to digital signals. Let us assume that data is in the form of text, numbers, audio, or video and it is stored in the form of a sequence of bits in the computer. Thus Line coding process converts the sequence of bits to a digital signal.

On the sender side, the digital data are encoded into digital signals, and on the receiver side, digital data is recreated by decoding the digital signal.



The above Figure shows Line Coding and Decoding

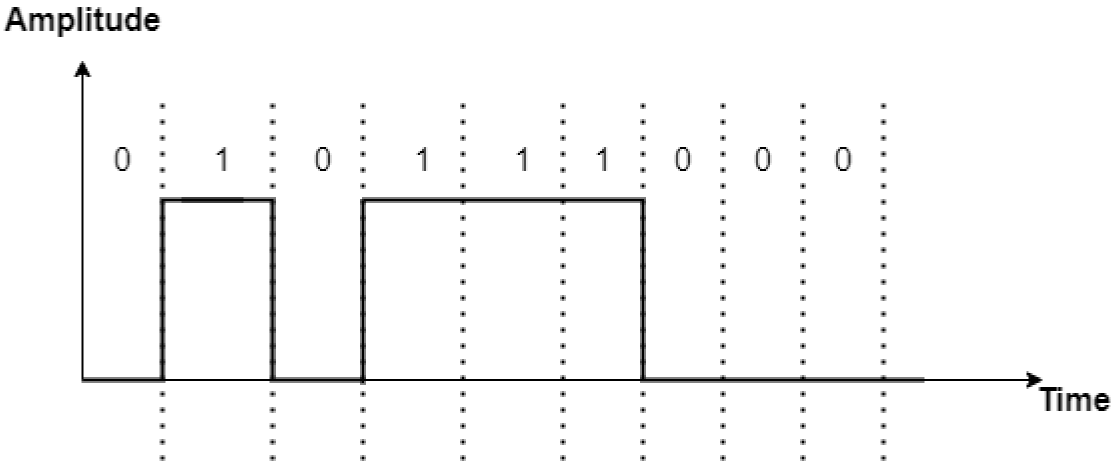
Line Coding schemes can be broadly classified into five categories:

- Unipolar
- Polar
- Bipolar
- Multilevel
- Multi Transition

Unipolar Scheme

In this line coding scheme, all the signal levels are on one side of the time axis. It can be either Above or Below. Basically, Unipolar Scheme was designed as a **Non-Return-to-Zero(NRZ)** scheme where **positive voltage defines bit 1** and zero voltage defined bit 0.

The unipolar scheme makes uses only one voltage level. It is called **NRZ** because the signal does not return to zero in the middle of the bit.



Unipolar NRZ Scheme

This coding scheme is inexpensive and is simple to implement.

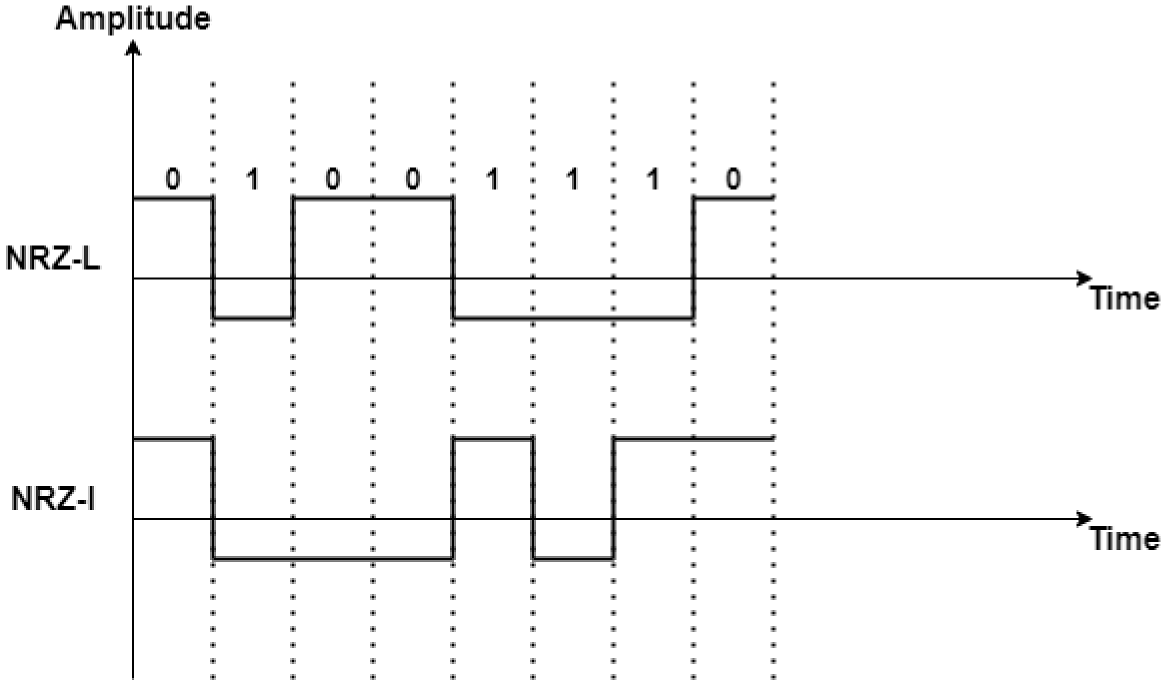
Polar Scheme

In this line coding scheme, the voltages are on both sides of the time axis. Let us take an example for this: the voltage level for 0 can be positive and the voltage level for 1 can be negative.

Thus in Polar NRZ encoding, we make use of two levels of voltage amplitude.

There are two versions of Polar NRZ:

- **NRZ-L(NRZ-level)** In this, the level of voltage mainly determines the value of the bit. Thus the level of the signal depends upon the value of the bit.
- **NRZ-I(NRZ-Invert)** In this, the change in the level of the voltage mainly determines the value of the bit. Suppose if there is no change then the bit is 0; and in case if there is a change the bit is 1.



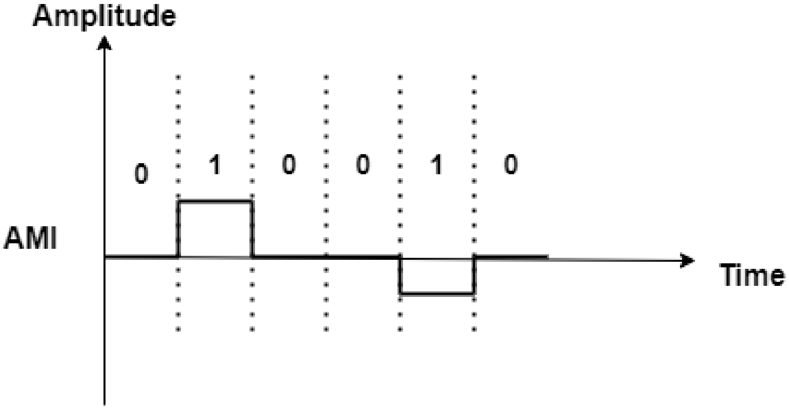
In the above diagram, If the next bit is 0 then there will be no inversion. But if the next bit is 1 then there will be Inversion

Bipolar schemes

In the Bipolar scheme, there are three voltage levels: positive, zero, and negative. In this, the voltage level for one data element is at 0 while the voltage level for other elements alternates between positive and negative.

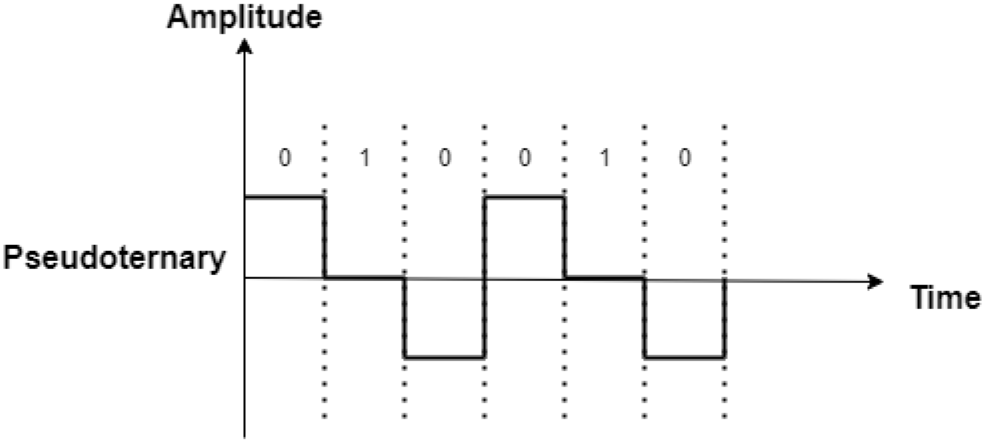
Given Below are two variations of Bipolar Encoding:

- **AMI(Alternate Mark Inversion)** It simply means alternate 1 inversion. In this neutral zero voltage represents binary 0 while binary 1s are represented by alternating positive and negative voltages.



The figure shows Bipolar AMI Encoding

- **Pseudoternary** In this 1 bit is encoded as zero voltage while 0 bit is encoded as alternating positive and negative voltages



The figure shows the Bipolar Pseudoternary Scheme

Multilevel Scheme

The Multilevel Coding scheme is also known as **mBnL**;

where:

m indicates the length of the Binary pattern.

B denotes the binary data

n indicates the length of the signal pattern

L indicates the number of levels in the signaling.

Three different versions of this scheme are:

- 2B1Q
- 8B6T
- 4D-PAM5

Multi Transition(MLT-3)

This technique uses three levels(+V,0,-V) and it also uses more than three transition rules in order to move between the levels.

Rules are:

- If the next bit is 0, then there is no transition.
- If the next bit is 1 and the current level is not 0, then the next level will be 0.
- If the next bit is 1 and also the current level is 0, then the next level is the opposite of the last non-zero level.

This technique does not perform self-synchronization for long 0s.

Block Coding

The main problem with line coding is Redundancy. The Block Codes mainly operates on a block of bits. They make use of the preset algorithm, takes the group of bits, and then add a coded part to them in order to make them a large block.

This large block is then checked at the receiver after that receiver makes the decision about the validity of the received sequence.

Thus the block coding changes the block of m bits into the block of n bits where **n>m.**

This block coding technique is also referred to as mB/nB encoding.

This technique overcomes the drawback of line coding and gives better performance.

Different versions of Block Coding are as follows:

- 4B/5B
- 8B/10B

Scrambling

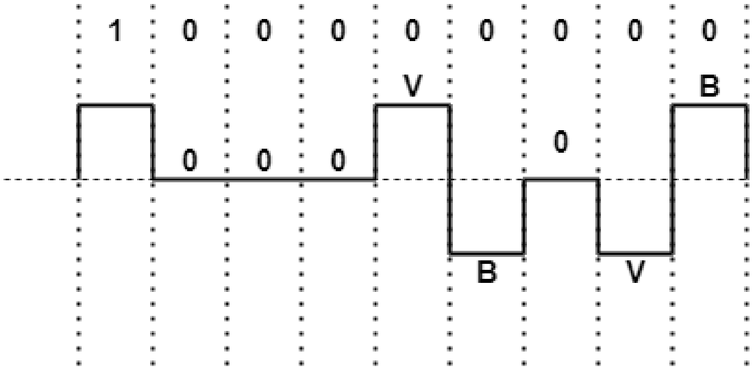
We can modify the line and block coding by including scrambling. It is important to note that scrambling as opposed to block coding is mainly done at the time of encoding.

Mainly the system needs to insert the required pulses on the basis of the scrambling rules.

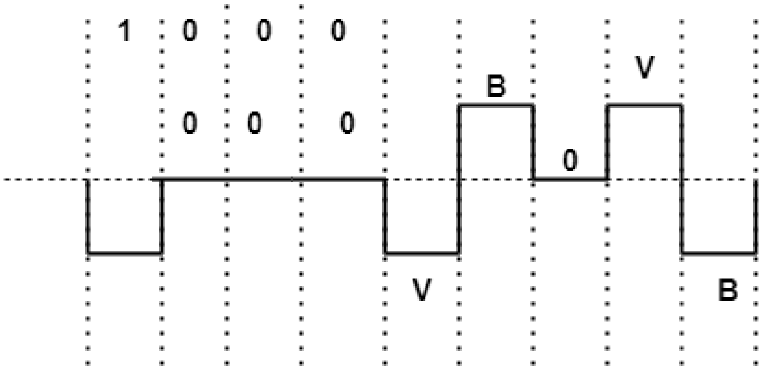
Given below are the two common techniques used for scrambling:

- **B8ZS(Bipolar with 8-zero substitution)** With this technique, eight consecutive zero-level voltages are replaced by the sequence of **000VB0VB**. In this sequence V mainly denotes violation and this is basically a nonzero voltage that breaks the AMI rule of encoding. The B in the given sequence denotes Bipolar which simply means nonzero voltage level according to the AMI rule.

Given below figure shows two cases of **the B8ZS** scrambling technique:



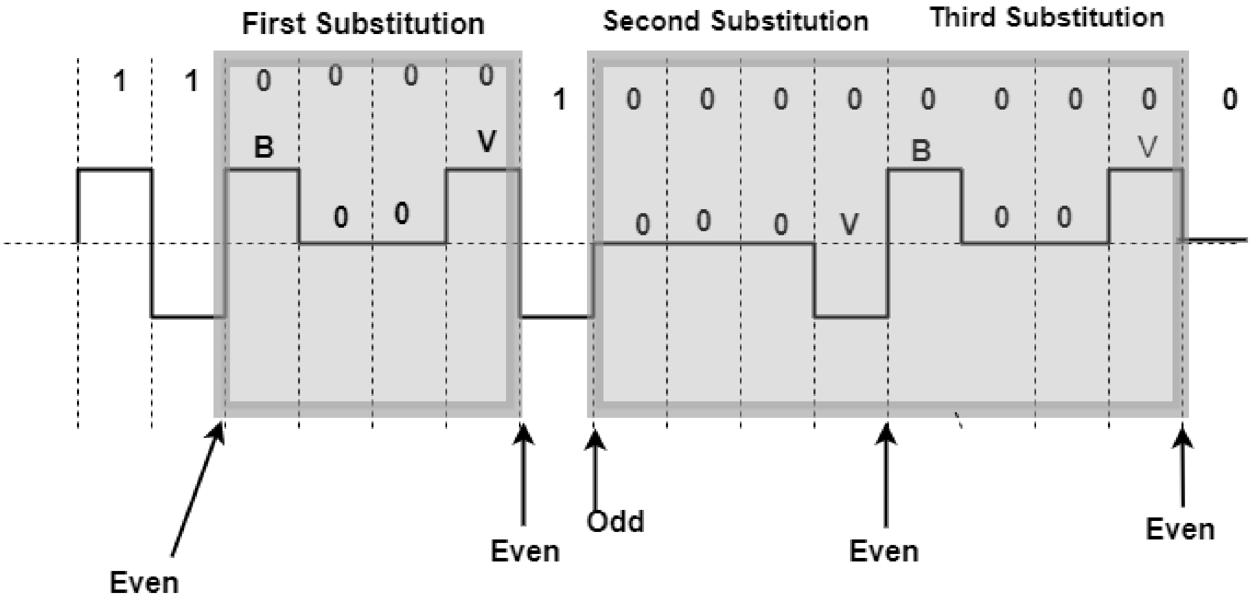
IN the above diagram previous level is positive



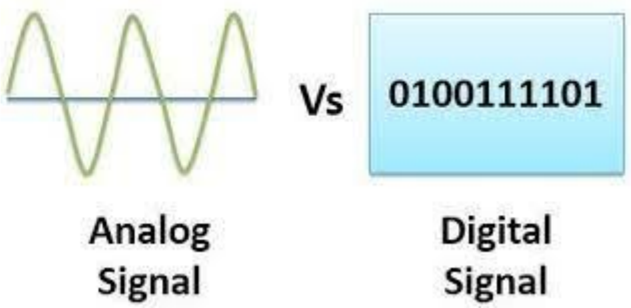
IN the above diagram previous level is negative

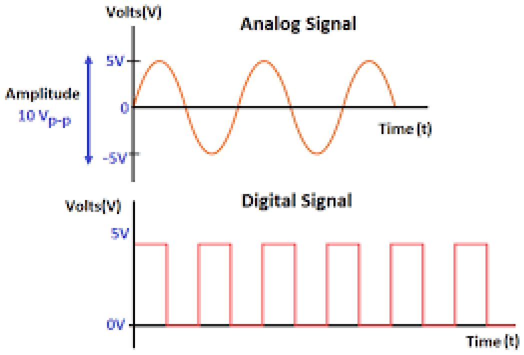
- **HDB3(High-Density Bipolar 3-zero** This technique is more conservative than B8ZS and in this four consecutive zero-level voltages are replaced with a sequence of 000V or B00V. The main reason for two different substitutions is just to maintain the even number of nonzero pulses after each substitution. Here are two rule for this purpose and these are as follows: 1. If the number of nonzero pulses after the **last substitution is odd**, then we will use the **000V** substitution pattern and it then makes the **total number of nonzero pulses even.** 2**.** If the number of nonzero pulses after the **last substitution is even**, then we will use the **B00V** substitution pattern and it then makes the **total number of nonzero pulses even.**

Given below figure shows different situations in the **HDB3** scrambling technique:



	Analog signal transmission	Digital signal transmission
signal	Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation.
Waves	Denoted by sine waves	Denoted by square waves
Representation	Uses continuous range of values to represent information	Uses discrete or discontinuous values to represent information
Example	Human voice in air, analog electronic devices.	Computers, CDs, DVDs, and other digital electronic devices.
Technology	Analog technology records waveforms as they are.	Samples analog waveforms into a limited set of numbers and records them.
Data transmissions	Subjected to deterioration by noise during transmission and write/read cycle.	Can be noise-immune without deterioration during transmission and write/read cycle.
Response to Noise	More likely to get affected reducing accuracy	Less affected since noise response are analog in nature.





Integrated Services Digital Network

ISDN stands for Integrated Services Digital Network. It is used to bridge the Central Office's local loop and the premise connection (home). ISDN uses the existing wiring so that no new cabling is required. It is a digital service that restores the analog plain old telephone set.

An Integrated Digital Network (ISDN) is a network in which digital switching connections are used to transmit digital signals. Integrated Services refers to ISDNs ability to deliver two simultaneous connections, in any merging of data, voice, video and fax, over an individual line. Multiple devices can be connected to the line and sent as needed.

An ISDN is a network, in general evolving from telephony ISDN, which provides end-to end digital connectivity to provide a broad range of services such as voice and non-voice services, to which customers have to create by a limited set of standard multipurpose user network interfaces.

Advantages

- ISDN is a mature technology, and it has been around since the late 1980s. It has been tried, tested and works.
- A worldwide set of standards governs it.

- It offers symmetrical transfer rates– the transmit rate is the same as the receiving rate.
- It has consistent transfer rates. If you have a 64 Kbps bearer channel, then it is the speed that you transfer at.
- It is a competitive price compared to other technologies.

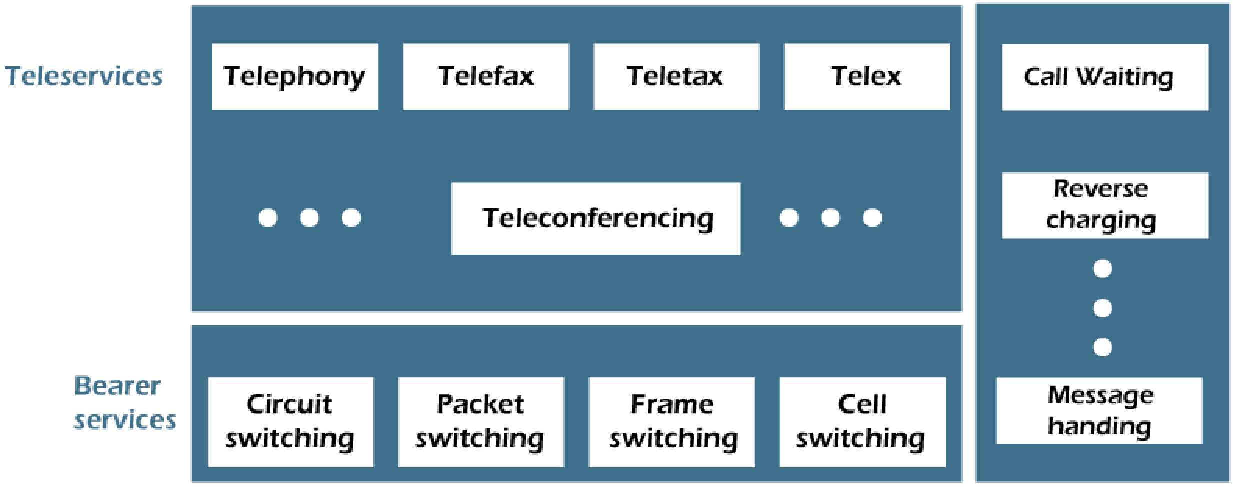
Disadvantages

- An external power supply is required. The telecommunication doesn't supply power for ISDN lines. If the power fails, the mobile phones won't work.
- Unique digital phones are necessary or a terminal adapter to talk to the existing plain old telephone set devices.
- It is costly to upgrade a central office switch ($500,000+) to ISDN.
- If the ISDN fails-the phone fails.

Introduction:

ISDN is a set of protocols that is based on high-speed fully digitized telephone service. The main aim of ISDN is to provide a fully integrated digital service to the users.

In ISDN there are following three types of ISDN services:



Bearer Services

This type of services is used to transfer information such as voice, data, and video between the users without manipulating the content of the network information. It belongs to the first 3 layers of the OSI reference model.

Tele Services:

In these types of services, the network may change the contents of the data. It belongs to the last 4 layers of the OSI reference model. It includes telephony, tele box, fax, and teleconferencing etc.

Supplementary Services:

It provides additional functionality to the bearer services and teleservices. Some of the examples of supplementary services are reverse charging, call waiting, and message handling.

Principles of ISDN:

Following are the principles of ISDN are:

- It supports both circuit switching & packet switching with the connections at 64 kbps.
- In ISDN layered protocol architecture is used for specification.
- ISDN services provides maintenance.
- ISDN services includes some network management functions.
- In ISDN network several configurations are possible for implementing.

ISDN SERVICES:

Following are the two types of services associated with ISDN:

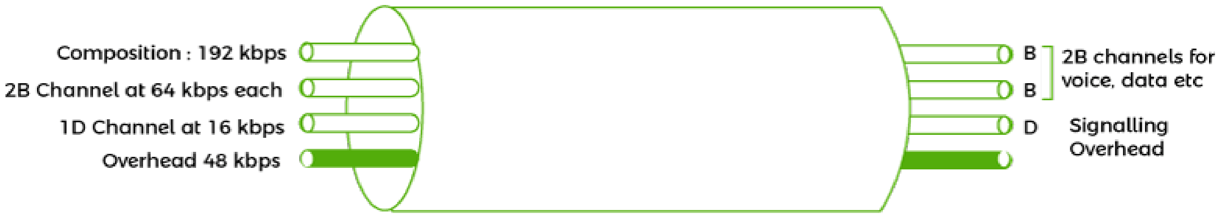
Basic Rate Interface (BRI)
ISDN Services
Primary Rate Interface (PRI)

Basic Rate Interface:

In the Basic Rate Interface digital pipe consists of 2 B channels and a 1 D channel. Therefore it is denoted as "2B + 1 D". These two B channels have a data rate of 64 kbps each, and the D channel have a data rate of 16 kbps. It has also a usable bandwidth of 144 kbps.

Basic Rate Interface allows the concurrent use of voice and various data applications such as packet-switched access, a link to a central alarm service, video, tax, etc. The signaling information for the two channels is sent onto the D channel. The two B channels can be used for one 128 kbps connection or two independent connections on the two channels.

The following figure shows the basic structure of the frame in the Basic Rate Interface is:



Basic Rate Interface (BRI)

This service is used to meet the needs of most individual users, including residential and small offices. In this case, the two B channels and the D channel are multiplexed with overhead bits in the form of the frame structure. The overhead bits include framing, DC balancing, and other bits.

The 48 bit frame consists of

- 16 bits of B1 Channel
- 16 bits of B2 Channel
- 4 bits of D channel
- 12 overhead bits

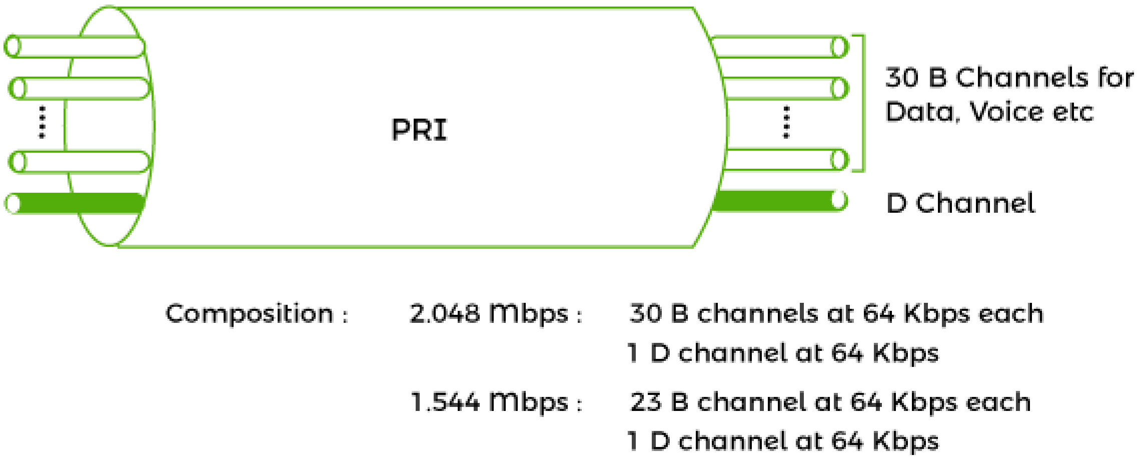
The frame is transmitted in 250 µsec, which results in the following bit rates:

- In frame each B channel = 16 / 250 µsec = 64 kbps
- In frame D channel = 4 / 250 µsec = 16 kbps
- In frame Overhead Bits = 12 / 250 µsec = 48 kbps
- In frame Overall Bit rate = 48 / 250 µsec = 192 kbps

Primary Rate Interface:

Primary Rate Interface consists of either 23 B channels or 30 B channels and a one 64 Kbps D channel. In North America and the Japan, 23 B channels and one D channel are used. It is also denoted by '23 B + 1 D'. In addition, the Primary Rate Interface service itself uses 8 kbps of overhead. Therefore 23D + 1D requires a data rate of 1.544 Mbps. In the case of 30 B channels and one D channel, the total bit rate is 2.048 Mbps.

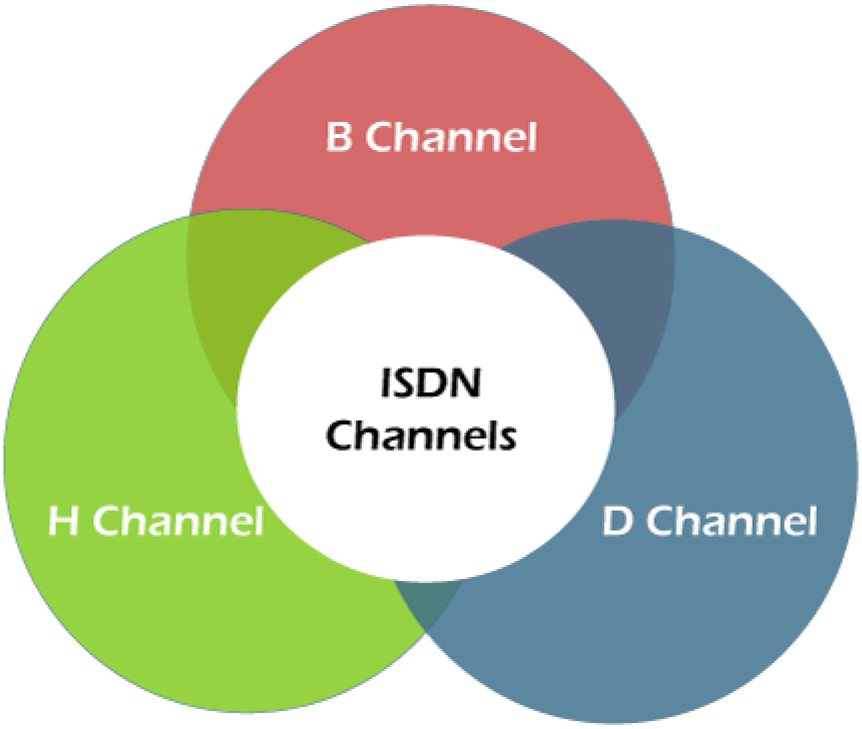
The following figure shows the basic structure of the frame in the Primary Rate Interface is:



ISDN CHANNELS:

ISDN structure have a central ISDN office in which all the users are linked to this through a digital pipe. This digital pipe have different capacities and have a different data transfer rates and these are organized into multiple channels of different sizes.

ISDN standard have the following three types of channels:



B Channel:

It stands for Bearer channel. It has a 64 kbps standard data rate. It is a basic user channel and can carry any digital information in full-duplex mode. In this transmission rate does not exceed 64 kbps. It can carry digital voice, digital data, and any other low data rate information.

D Channel:

It stands for Data Channel. This channel carry control signal for bearer services. This channel is required for signaling or packet-switched data and all-controlling signals such as establishing calls, ringing, call interrupt, etc.

H Channel:

It stands for Hybrid Channel. It provides user information at higher bit rates.

There are 3 types of Hybrid Channel depending on the data rates. Following are the hybrid channels types:

- Hybrid Channel 0 with 384 kbps data rate.
- Hybrid Channel 11 with 1536 kbps data rate.
- Hybrid Channel 12 with 1920 kbps data rate.

ISDN Devices:

Following are the types of ISDN devices:

TE1: Terminal equipment type (TE1) are specialized ISDN terminals. It includes digital telephone instruments such as FAX, or data terminal equipment. All these devices have an S-bus ISDN interface.

TE2: Terminal equipment type (TE2) is Non-ISDN compatible is connected through a Terminal Adapter. It includes analog phones and 3270 terminal Fax.

TA: It stands for Terminal Adapter. This device acts as an intermediary device for non-ISDN terminal devices. It converts the non-ISDN interface of these devices to the ISDN interface. The ISDN terminal Adapter can be either a standalone device or a board inside the Terminal equipment type 2. Some of the examples of Terminal adapter are EIA/TIA-232-C, V.24 etc.

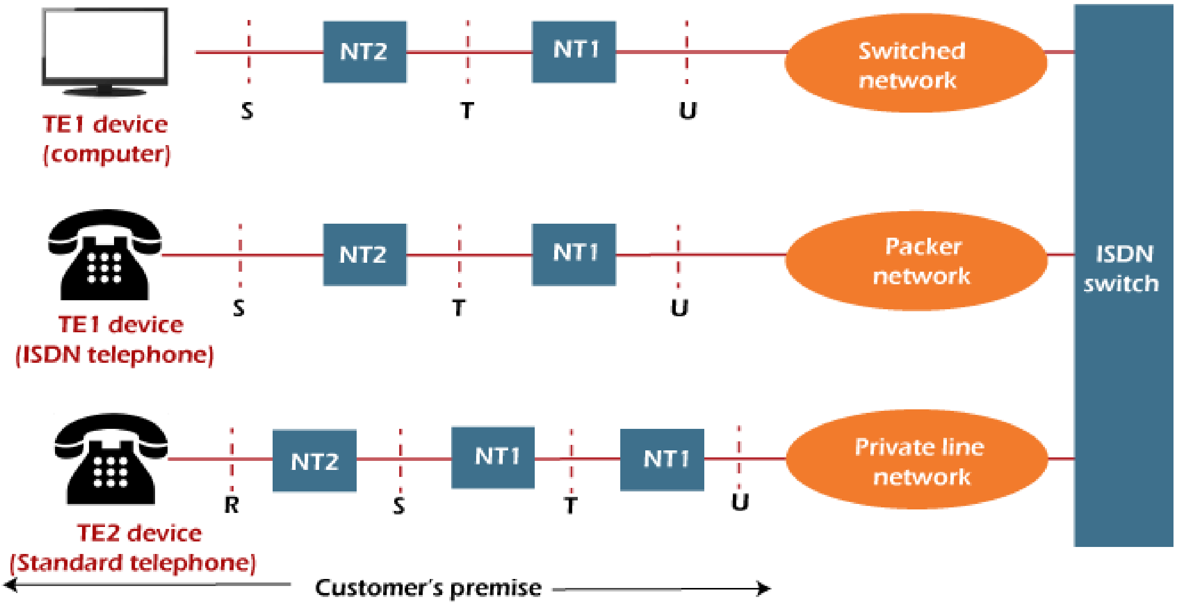
NT1: It stands for Network termination type 1. It provides a line termination at the customer's premise. They can also provide line monitoring, power feeding, error statistics, and proper timing.

NT2: It stands for Network termination type 2. It provides a switching, multiplexing, concentrating, or distributing information for the customer's premises. Some examples of Network termination type 2 are this could be a LAN server or Private Branch Exchange etc.

ISDN Reference Points:

It specifies the number of reference points that provide interfaces between the adjacent devices.

Following Figure displays the working of ISDN reference points:



In the above figure it shows an ISDN configuration in which 3 devices attached to an ISDN switch at the central office. In which 2 devices are ISDN compatible and they are attached through the S reference point to Network termination type 2 devices. Out of these third device is a standard non-ISDN telephone and is attached to a Terminal Adapter through an R reference point.

These reference points are R, S, T, and U.

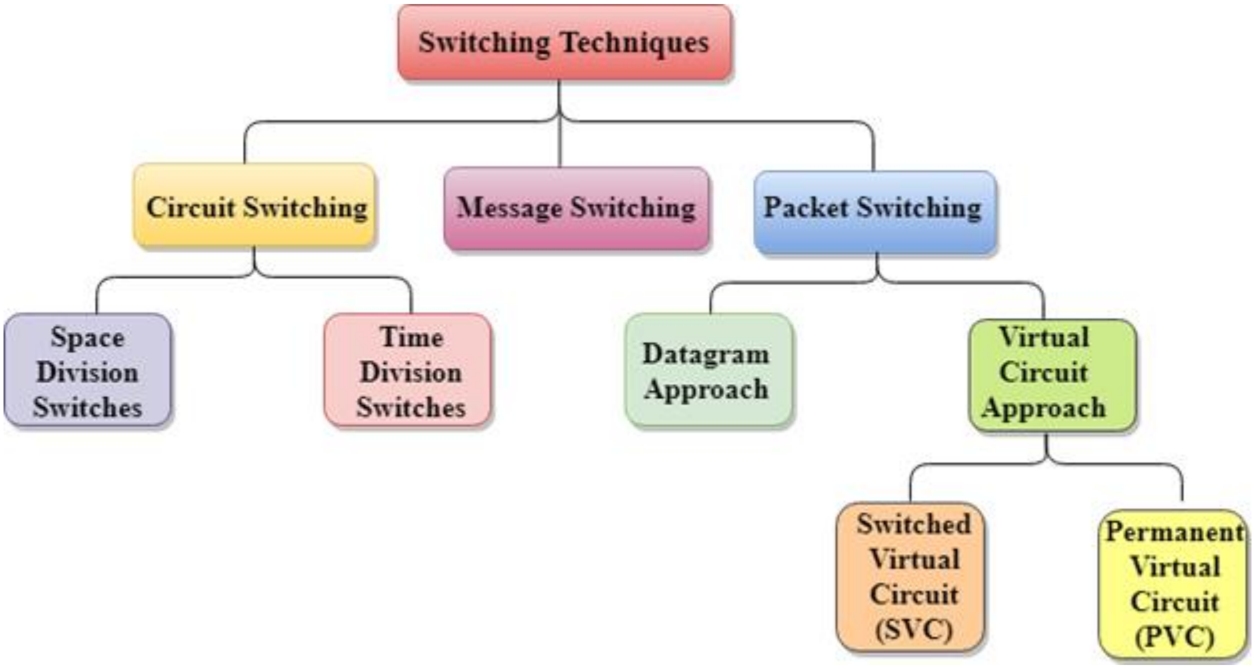
- **R:**It stands for Rate transfer point. It is an interface for non-ISDN devices and therefore is the reference point between non-ISDN equipment and a Terminal Adapter. It can be RS-232-C, V, or X series of ITU-T standard or ordinary telephone interface with two wires.
- **S:**It stands for System transfer point. The interface between the user terminal and NT2. It is a four-wire balanced to which upto eight ISDN terminals can be connected. The physical connector for S - interface on terminals and NT1 is an 8-pin RJ-45 connector.
- **T:**It stands for Terminal transfer point. It is the interface between Network termination type 1 and Network termination type 2
- **U:** It is the interface between Network termination type 1 device and the line termination equipment in the carrier network. The U interface is the local copper pair of the access network. The same pair is used for s signals.

Switching techniques

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

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

Classification Of Switching Techniques



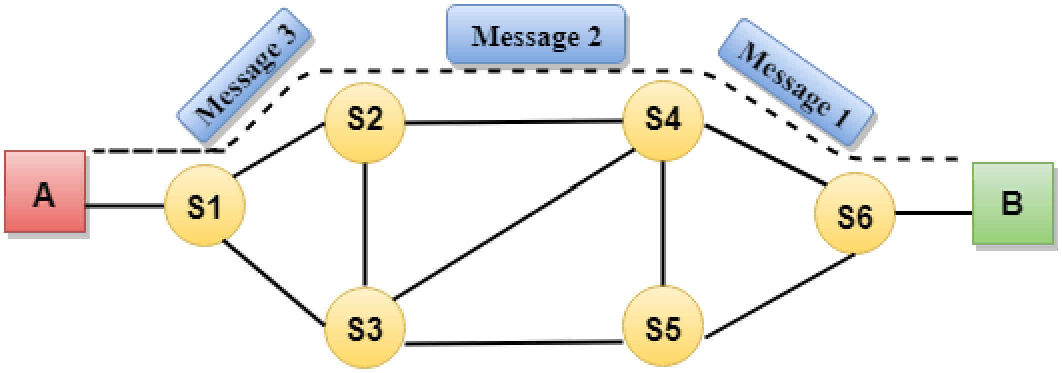
Circuit Switching

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

- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.
- The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.
- Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- **Crossbar Switch**
- **Multistage Switch**

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

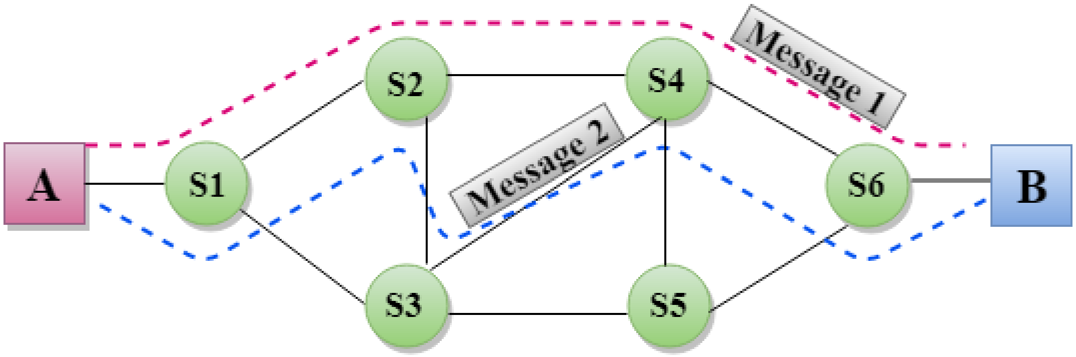
Disadvantages Of Circuit Switching:

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

Message Switching

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

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



Advantages Of Message Switching

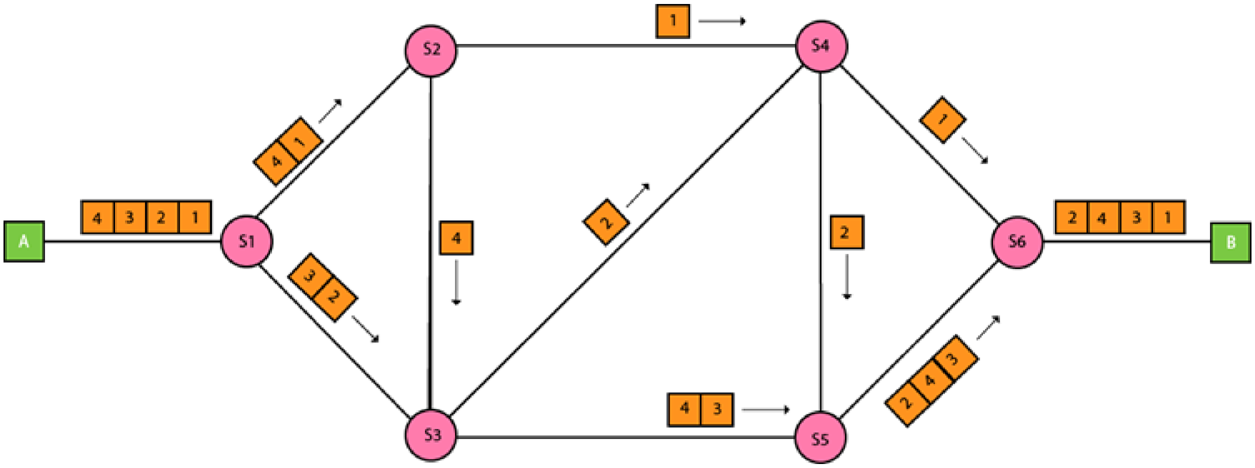
- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

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

Packet Switching

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



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

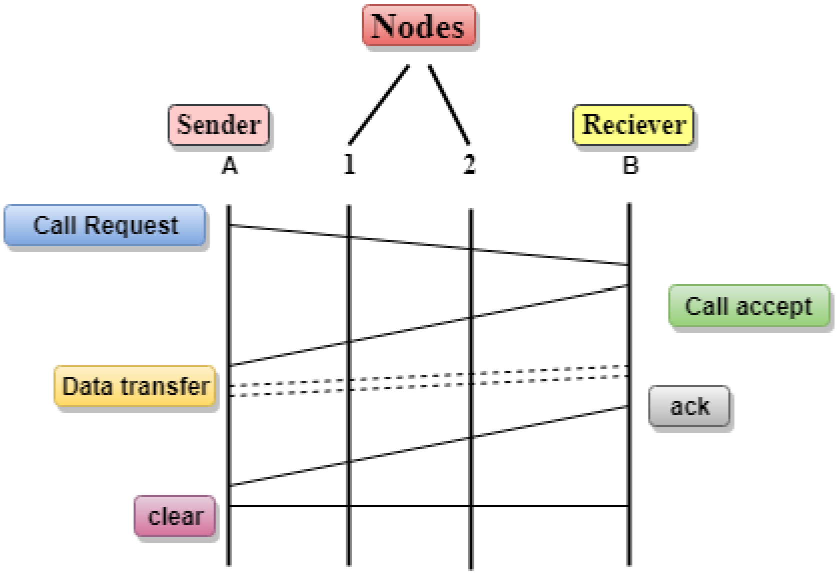
Datagram Packet switching:

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

- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

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



- 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.

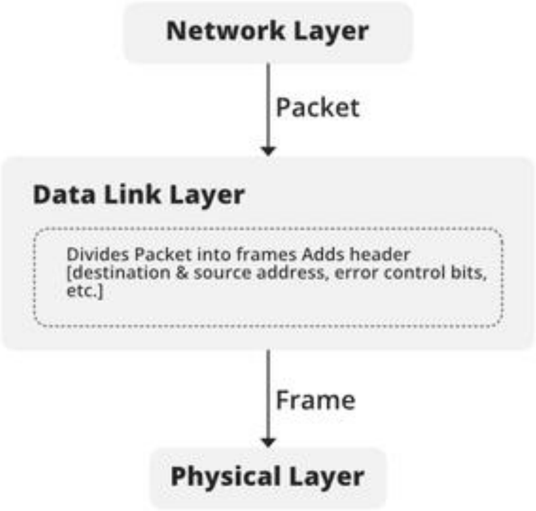
Disadvantages Of Packet Switching:

- 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.

Data Link Layer

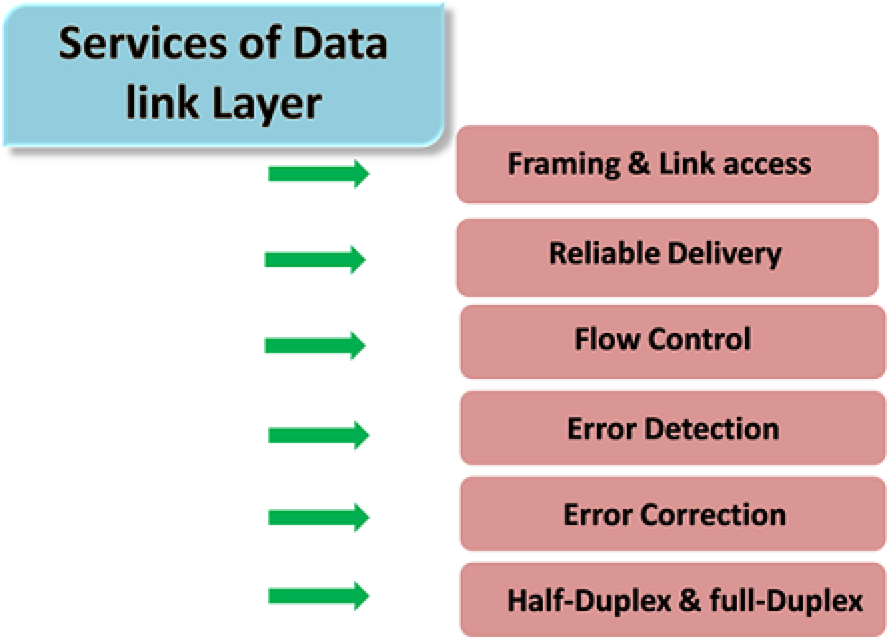
- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.

- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.
- The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link.


Network Layer
Packet
Data Link Layer
Divides Packet into frames Adds header [destination & source address, error control bits, etc.]
Frame
Physical Layer

-

Following services are provided by the Data Link Layer:



- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.

- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Data-link layer is the second layer after the physical layer. The data link layer is responsible for maintaining the data link between two hosts or nodes.
Before going through the design issues in the data link layer. Some of its sub-layers and their functions are as following below.

The data link layer is divided into two sub-layers :

1. **Logical Link Control Sub-layer (LLC)** –
   Provides the logic for the data link, Thus it controls the synchronization, flow control, and error checking functions of the data link layer. Functions are –
   - **(i)** Error Recovery.
   - **(ii)** It performs the flow control operations.
   - **(iii)** User addressing.

2. **Media Access Control Sub-layer (MAC)** –
   It is the second sub-layer of data-link layer. It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card.
   Functions are –
   - **(i)** To perform the control of access to media.
   - **(ii)** It performs the unique addressing to stations directly connected to LAN.
   - **(iii)** Detection of errors.

Design issues with data link layer are :

1. **Services provided to the network layer –**
   The data link layer act as a service interface to the network layer. The principle service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).
2. **Frame synchronization** –
   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.
3. **Flow control –**
   Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.
4. **Error control –**
   Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Error Detection in Computer Networks

Error

A condition when the receiver’s information does not match with the sender’s information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Error Detecting Codes (Implemented either at Data link layer or Transport Layer of OSI Model)

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.

Some popular techniques for error detection are:

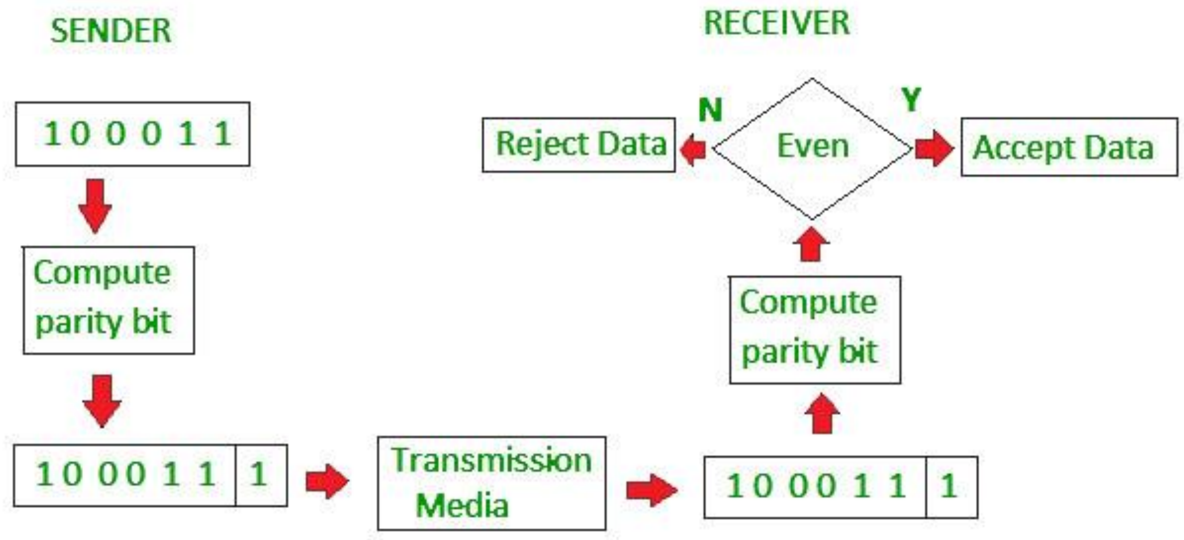
1. Simple Parity check
2. Two-dimensional Parity check
3. Checksum
4. Cyclic redundancy check

1. Simple Parity check

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

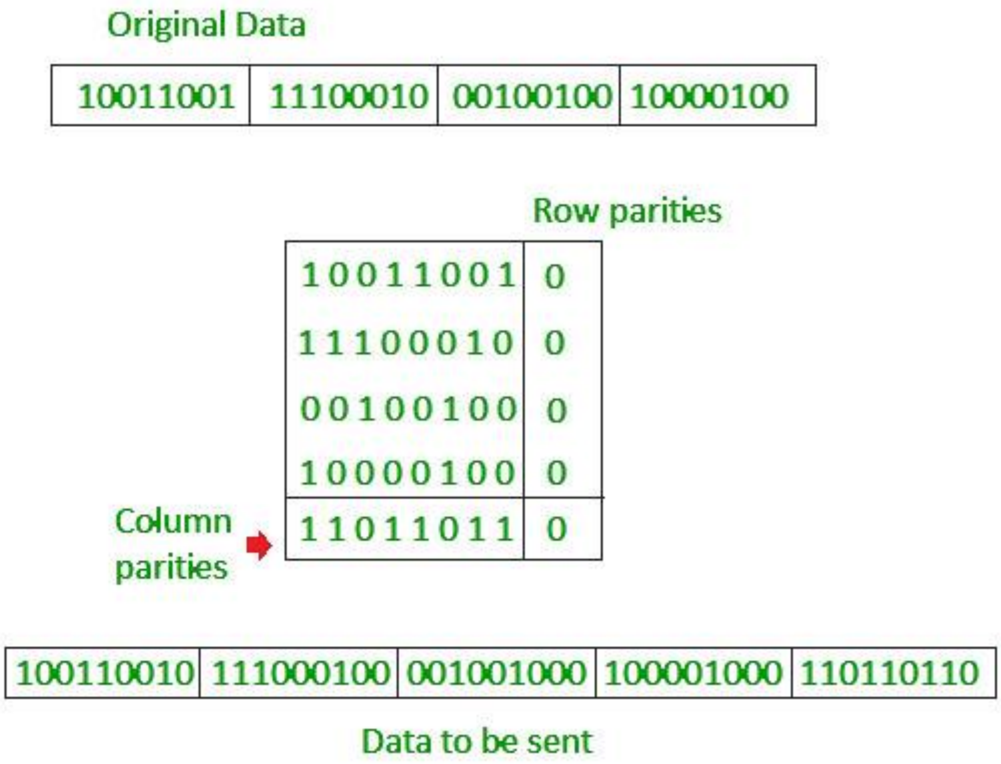
- 1 is added to the block if it contains odd number of 1's, and
- 0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.



2. Two-dimensional Parity check

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.



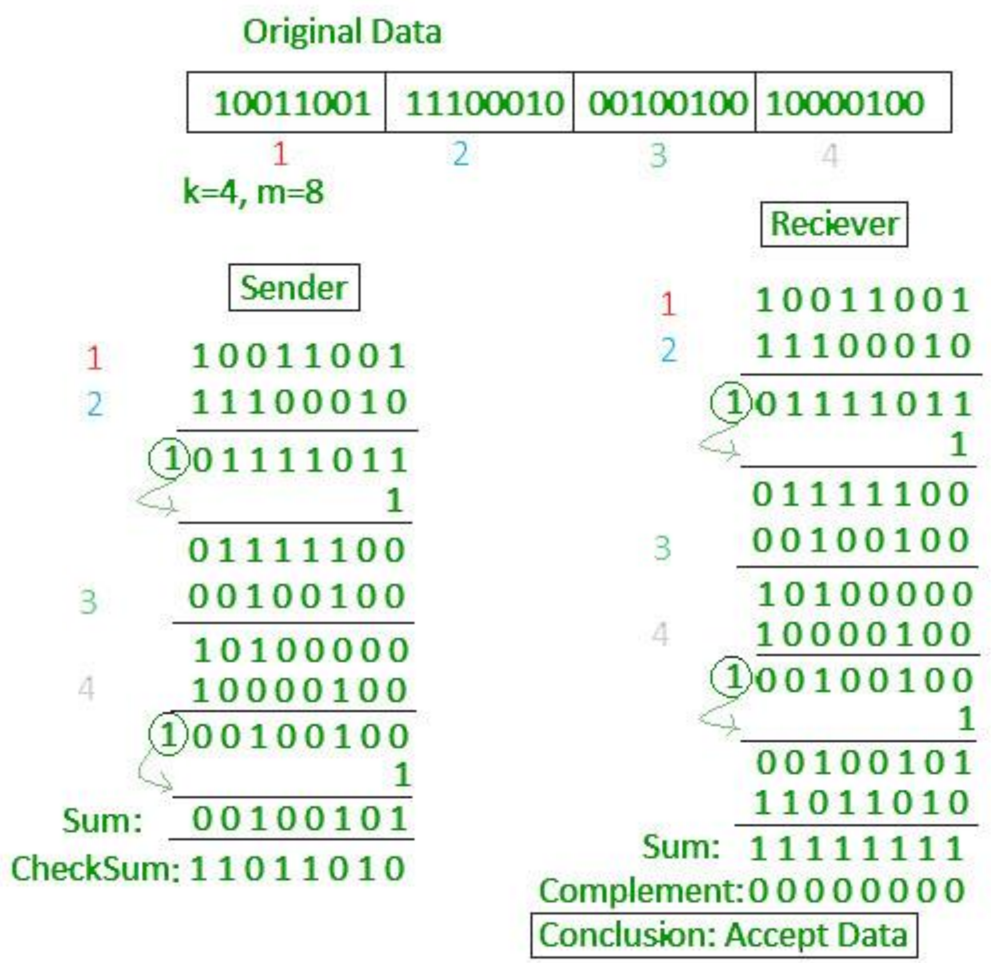
10011001	11100010	00100100	10000100

10011001	0
11100010	0
00100100	0
10000100	0
11011011	0

100110010	111000100	001001000	100001000	110110110

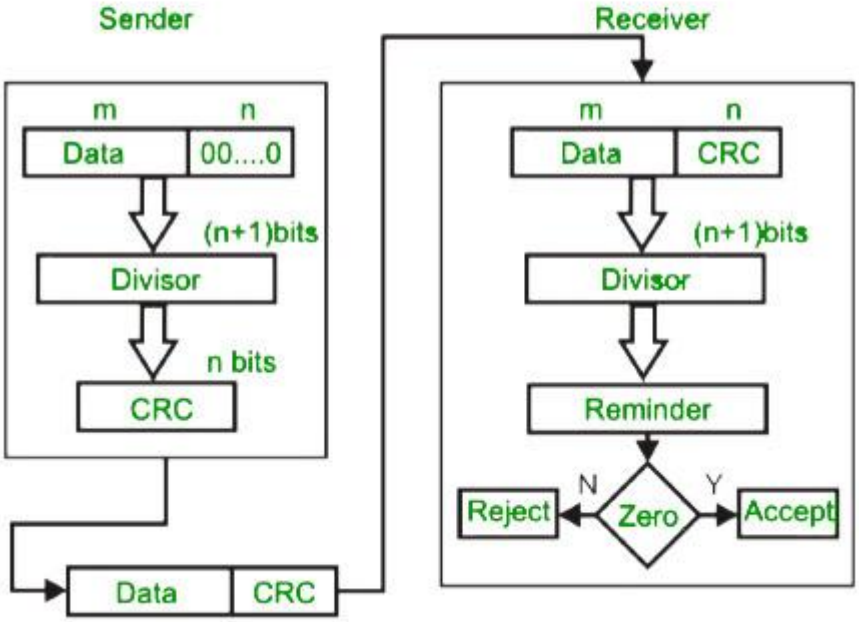
3. Checksum

- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.



4. Cyclic redundancy check (CRC)

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



Data-link layer uses error control techniques to ensure that frames, i.e. bit streams of data, are transmitted from the source to the destination with a certain extent of accuracy.

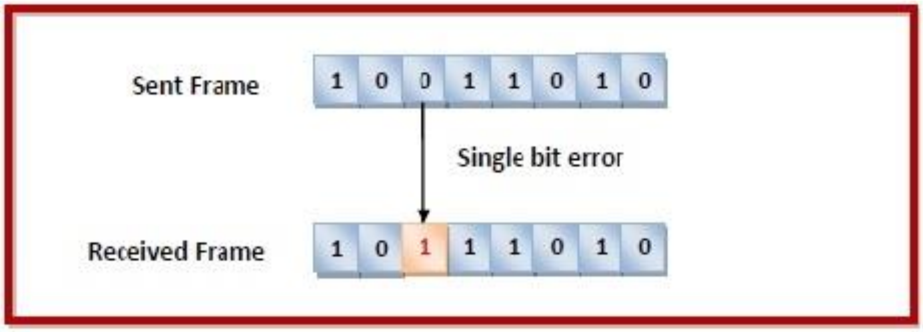
Errors

When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits leads to spurious data being received by the destination and are called errors.

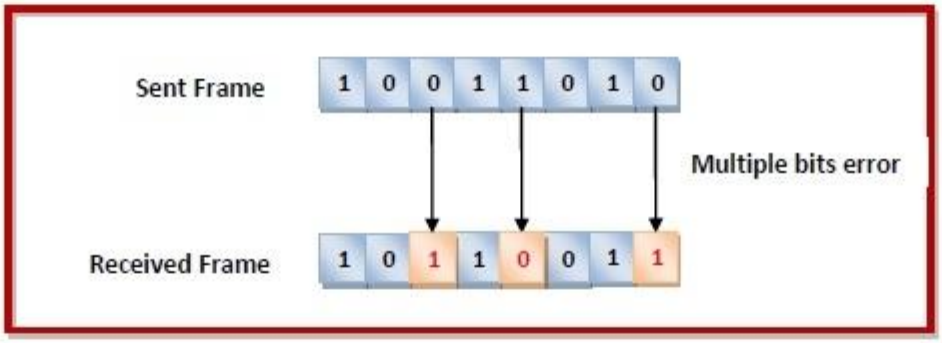
Types of Errors

Errors can be of three types, namely single bit errors, multiple bit errors, and burst errors.

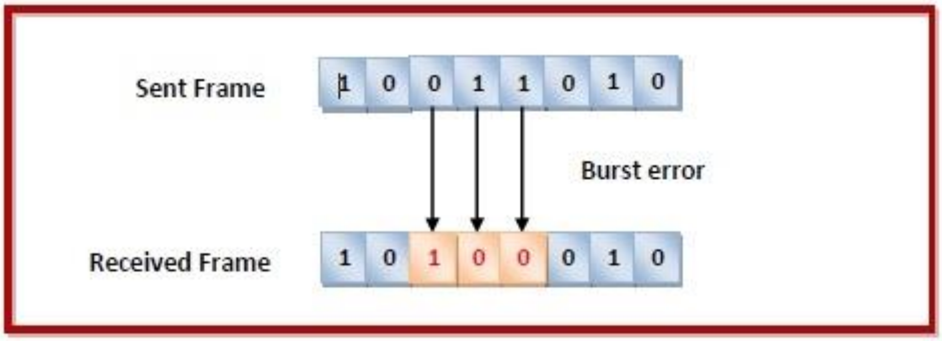
- **Single bit error** − In the received frame, only one bit has been corrupted, i.e. either changed from 0 to 1 or from 1 to 0.



- **Multiple bits error** − In the received frame, more than one bits are corrupted.



- **Burst error** − In the received frame, more than one consecutive bits are corrupted.



Error Control

Error control can be done in two ways

- **Error detection** − Error detection involves checking whether any error has occurred or not. The number of error bits and the type of error does not matter.
- **Error correction** − Error correction involves ascertaining the exact number of bits that has been corrupted and the location of the corrupted bits.

For both error detection and error correction, the sender needs to send some additional bits along with the data bits. The receiver performs necessary checks based upon the additional redundant bits. If it finds that the data is free from errors, it removes the redundant bits before passing the message to the upper layers.

Error Detection Techniques

There are three main techniques for detecting errors in frames: Parity Check, Checksum and Cyclic Redundancy Check (CRC).

Parity Check

The parity check is done by adding an extra bit, called parity bit to the data to make a number of 1s either even in case of even parity or odd in case of odd parity.

While creating a frame, the sender counts the number of 1s in it and adds the parity bit in the following way

- In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.
- In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.

On receiving a frame, the receiver counts the number of 1s in it. In case of even parity check, if the count of 1s is even, the frame is accepted, otherwise, it is rejected. A similar rule is adopted for odd parity check.

The parity check is suitable for single bit error detection only.

Checksum

In this error detection scheme, the following procedure is applied

- Data is divided into fixed sized frames or segments.
- The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
- The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.
- If the result is zero, the received frames are accepted; otherwise, they are discarded.

Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC) involves binary division of the data bits being sent by a predetermined divisor agreed upon by the communicating system. The divisor is generated using polynomials.

- Here, the sender performs binary division of the data segment by the divisor. It then appends the remainder called CRC bits to the end of the data segment. This makes the resulting data unit exactly divisible by the divisor.
- The receiver divides the incoming data unit by the divisor. If there is no remainder, the data unit is assumed to be correct and is accepted. Otherwise, it is understood that the data is corrupted and is therefore rejected.

Error Correction Techniques

Error correction techniques find out the exact number of bits that have been corrupted and as well as their locations. There are two principle ways

- **Backward Error Correction (Retransmission)** − If the receiver detects an error in the incoming frame, it requests the sender to retransmit the frame. It is a relatively simple technique. But it can be efficiently used only where retransmitting is not expensive as in fiber optics and the time for retransmission is low relative to the requirements of the application.

Forward Error Correction − If the receiver detects some error in the incoming frame, it executes error-correcting code that generates the actual frame. This saves bandwidth required for retransmission. It is inevitable in real-time systems. However, if there are too many errors, the frames need to be retransmitted.

A single additional bit can detect the error, but cannot correct it.

For correcting the errors, one has to know the exact position of the error. For example, If we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits

-

The four main error correction codes are

- Hamming Codes
- Binary Convolution Code
- Reed – Solomon Code
- Low-Density Parity-Check Code

Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using the formula:

$2^r >= d+r+1$

The value of r is calculated by using the above formula. For example, if the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

To determine the position of the bit which is in error, a technique developed by R.W Hamming is Hamming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Hamming Code

Parity bits: The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity bit is 1.

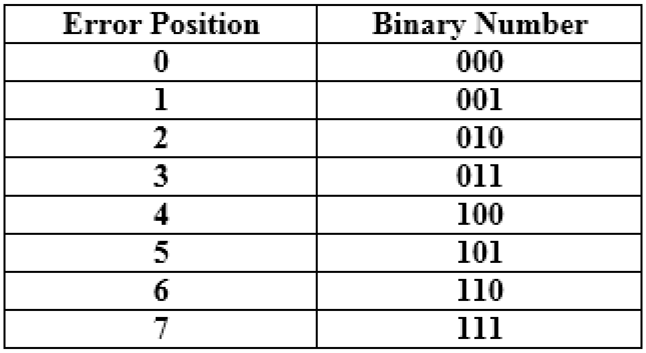
Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

Algorithm of Hamming code:

- An information of 'd' bits are added to the redundant bits 'r' to form d+r.
- The location of each of the (d+r) digits is assigned a decimal value.
- The 'r' bits are placed in the positions 1,2,.....2^{k-1}.

- At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

Relationship b/w Error position & binary number.



Error Position	Binary Number
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Let's understand the concept of Hamming code through an example:

Suppose the original data is 1010 which is to be sent.

Total number of data bits 'd' = 4

Number of redundant bits r : $2^r >= d+r+1$

$2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

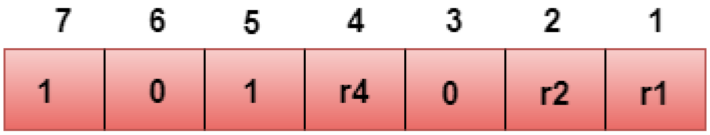
Total number of bits = d+r = 4+3 = 7;

Determining the position of the redundant bits

The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits is calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are **1, 2^1, 2^2**.

1. The position of r1 = 1
2. The position of r2 = 2
3. The position of r4 = 4

Representation of Data on the addition of parity bits:

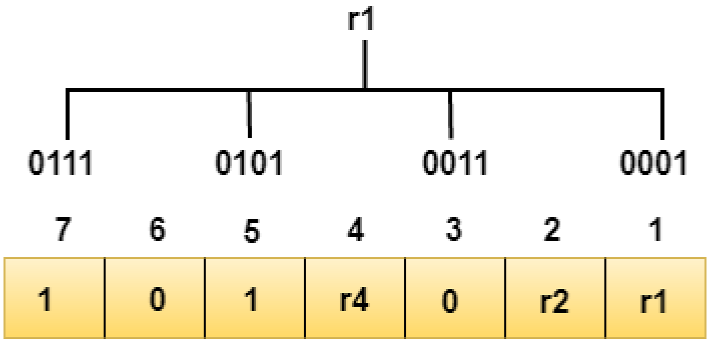


7	6	5	4	3	2	1
1	0	1	r4	0	r2	r1

Determining the Parity bits

Determining the r1 bit

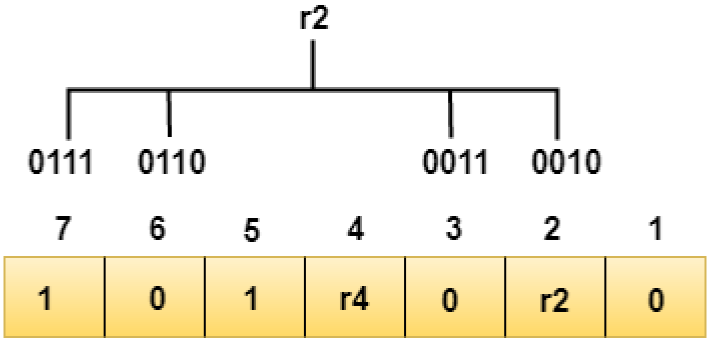
The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r1 is **even, therefore, the value of the r1 bit is 0**.

Determining r2 bit

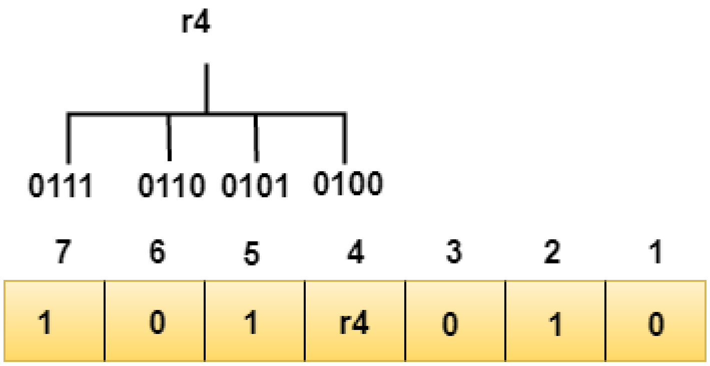
The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



We observe from the above figure that the bit positions that includes 1 in the second position are **2, 3, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r2 is **odd, therefore, the value of the r2 bit is 1**.

Determining r4 bit

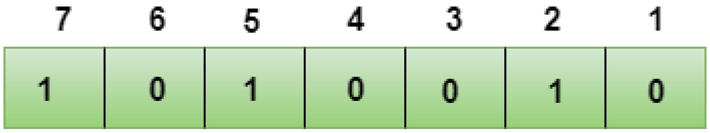
The r4 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position.



7	6	5	4	3	2	1
1	0	1	r4	0	1	0

We observe from the above figure that the bit positions that includes 1 in the third position are **4, 5, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r4 is **even, therefore, the value of the r4 bit is 0**.

Data transferred is given below:

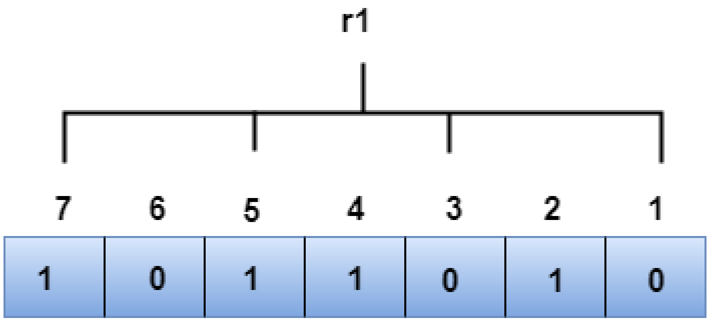


7	6	5	4	3	2	1
1	0	1	0	0	1	0

Suppose the 4th bit is changed from 0 to 1 at the receiving end, then parity bits are recalculated.

R1 bit

The bit positions of the r1 bit are 1,3,5,7

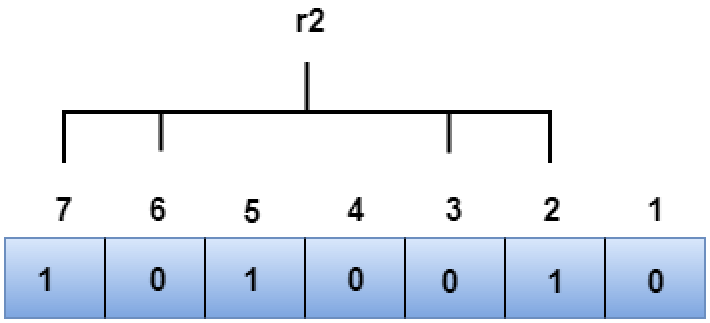


7	6	5	4	3	2	1
1	0	1	1	0	1	0

We observe from the above figure that the binary representation of r1 is 1100. Now, we perform the even-parity check, the total number of 1s appearing in the r1 bit is an even number. Therefore, the value of r1 is 0.

R2 bit

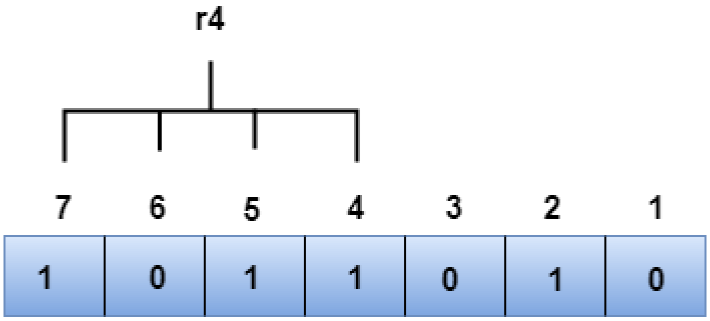
The bit positions of r2 bit are 2,3,6,7.



We observe from the above figure that the binary representation of r2 is 1001. Now, we perform the even-parity check, the total number of 1s appearing in the r2 bit is an even number. Therefore, the value of r2 is 0.

R4 bit

The bit positions of r4 bit are 4,5,6,7.



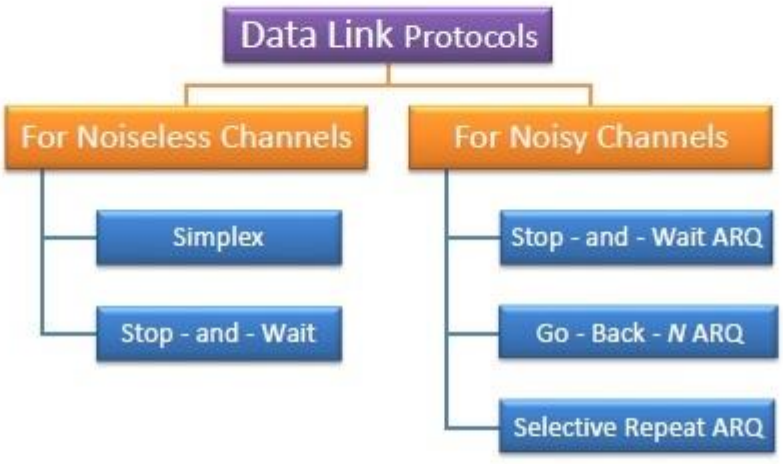
We observe from the above figure that the binary representation of r4 is 1011. Now, we perform the even-parity check, the total number of 1s appearing in the r4 bit is an odd number. Therefore, the value of r4 is 1.

Elementary Data Link Protocols

Protocols in the data link layer are designed so that this layer can perform its basic functions: framing, error control and flow control. Framing is the process of dividing bit - streams from physical layer into data frames whose size ranges from a few hundred to a few thousand bytes. Error control mechanisms deals with transmission errors and retransmission of corrupted and lost frames. Flow control regulates speed of delivery and so that a fast sender does not drown a slow receiver.

Types of Data Link Protocols

Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.



Simplex Protocol

The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong. It has distinct procedures for sender and receiver. The sender simply sends all its data available onto the channel as soon as they are available its buffer. The receiver is assumed to process all incoming data instantly. It is hypothetical since it does not handle flow control or error control.

Stop – and – Wait Protocol

Stop – and – Wait protocol is for noiseless channel too. It provides unidirectional data transmission without any error control facilities. However, it provides for flow control so that a fast sender does not drown a slow receiver. The receiver has a finite buffer size with finite processing speed. The sender can send a frame only when it has received indication from the receiver that it is available for further data processing.

Stop – and – Wait ARQ

Stop – and – wait Automatic Repeat Request (Stop – and – Wait ARQ) is a variation of the above protocol with added error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires or a negative acknowledgement is received, the frame is retransmitted. If a positive acknowledgement is received then the next frame is sent.

Go – Back – N ARQ

Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.

Selective Repeat ARQ

This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

Elementary Data Link protocols are classified into three categories, as given below −

- Protocol 1 − Unrestricted simplex protocol

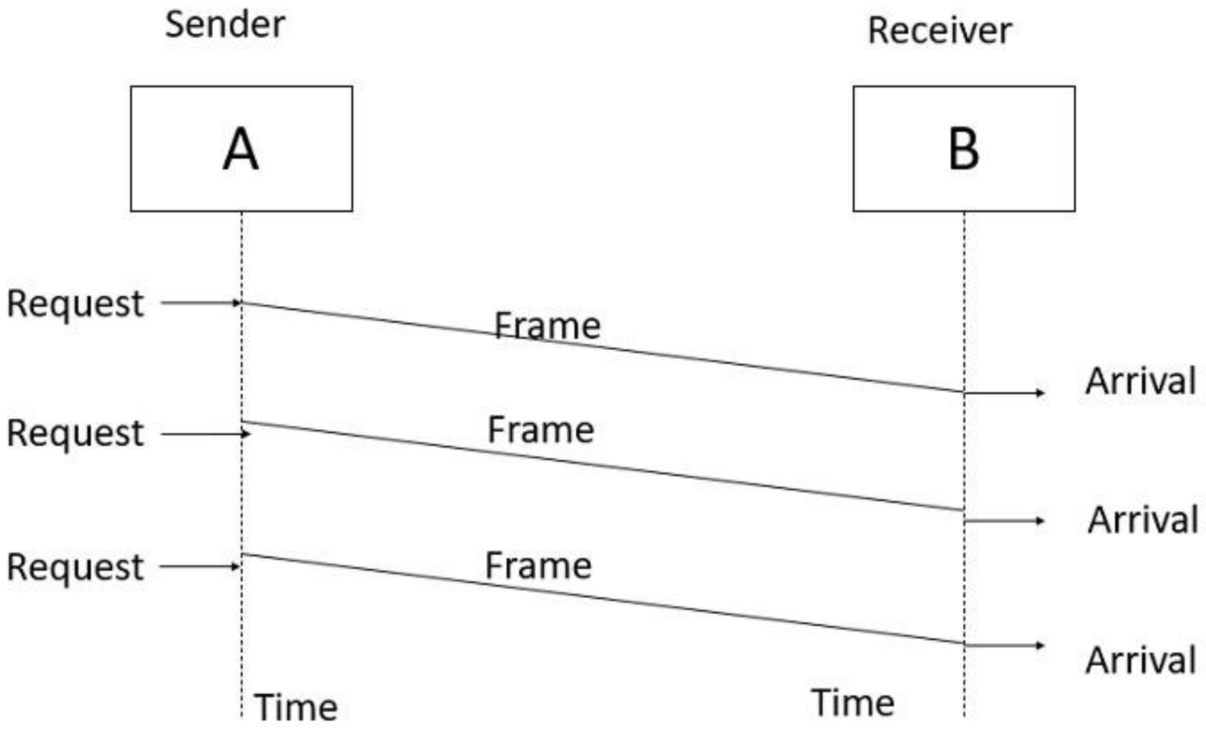
- Protocol 2 − Simplex stop and wait protocol
- Protocol 3 − Simplex protocol for noisy channels.

Let us discuss each protocol one by one.

Unrestricted Simplex Protocol

Data transmitting is carried out in one direction only. The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored. In this protocol, infinite buffer space is available, and no errors are occurring that is no damage frames and no lost frames.

The Unrestricted Simplex Protocol is diagrammatically represented as follows −



Simplex Stop and Wait protocol

In this protocol we assume that data is transmitted in one direction only. No error occurs; the receiver can only process the received information at finite rate. These assumptions imply that the transmitter cannot send frames at rate faster than the receiver can process them.

The main problem here is how to prevent the sender from flooding the receiver. The general solution for this problem is to have the receiver send some sort of feedback to sender, the process is as follows −

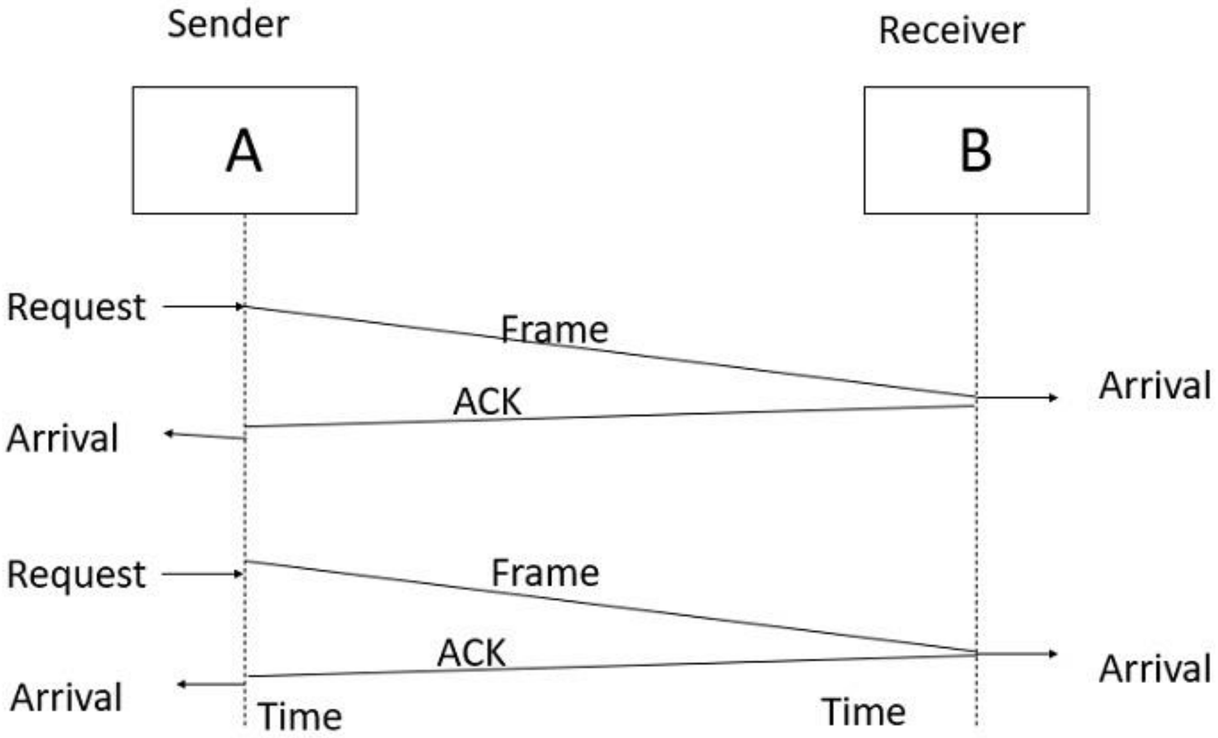
Step1 − The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.

Step 2 − Permission to send the next frame is granted.

Step 3 − The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.

This protocol is called Simplex Stop and wait protocol, the sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.

The Simplex Stop and Wait Protocol is diagrammatically represented as follows −

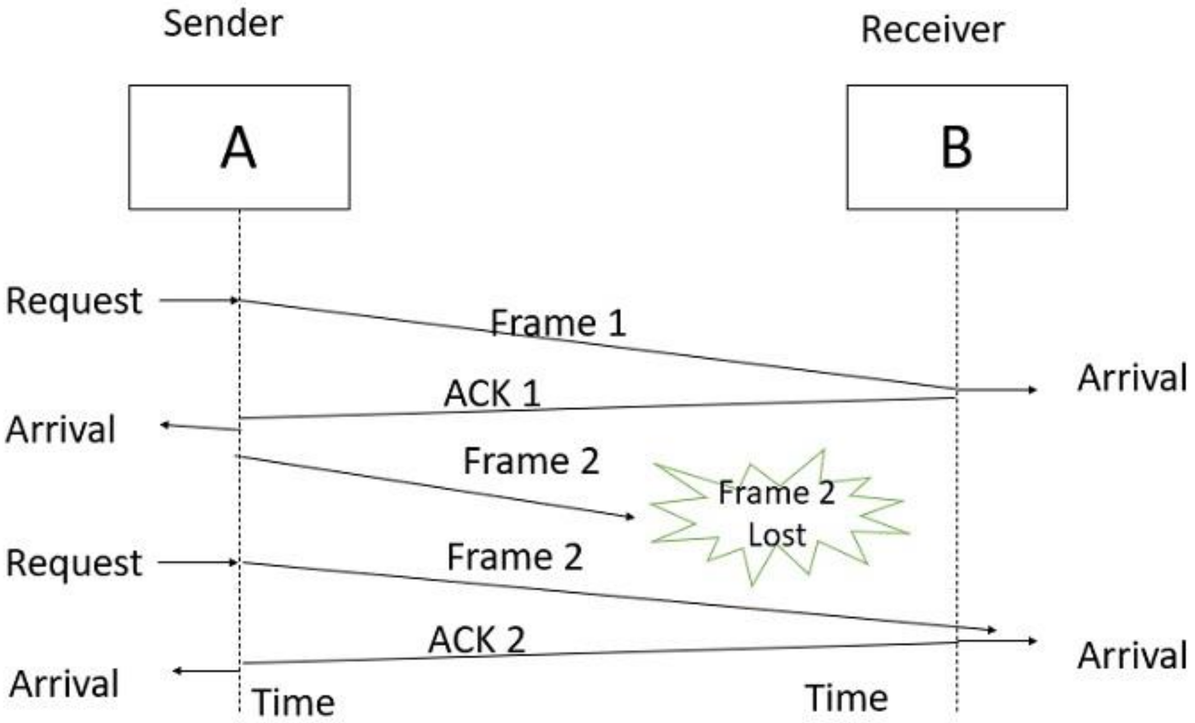


Simplex Protocol for Noisy Channel

Data transfer is only in one direction, consider separate sender and receiver, finite processing capacity and speed at the receiver, since it is a noisy channel, errors in data frames or acknowledgement frames are expected. Every frame has a unique sequence number.

After a frame has been transmitted, the timer is started for a finite time. Before the timer expires, if the acknowledgement is not received , the frame gets retransmitted, when the acknowledgement gets corrupted or sent data frames gets damaged, how long the sender should wait to transmit the next frame is infinite.

The Simplex Protocol for Noisy Channel is diagrammatically represented as follows −



Sliding Window Protocol

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol)

.

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocol

Sliding window protocol has two types:

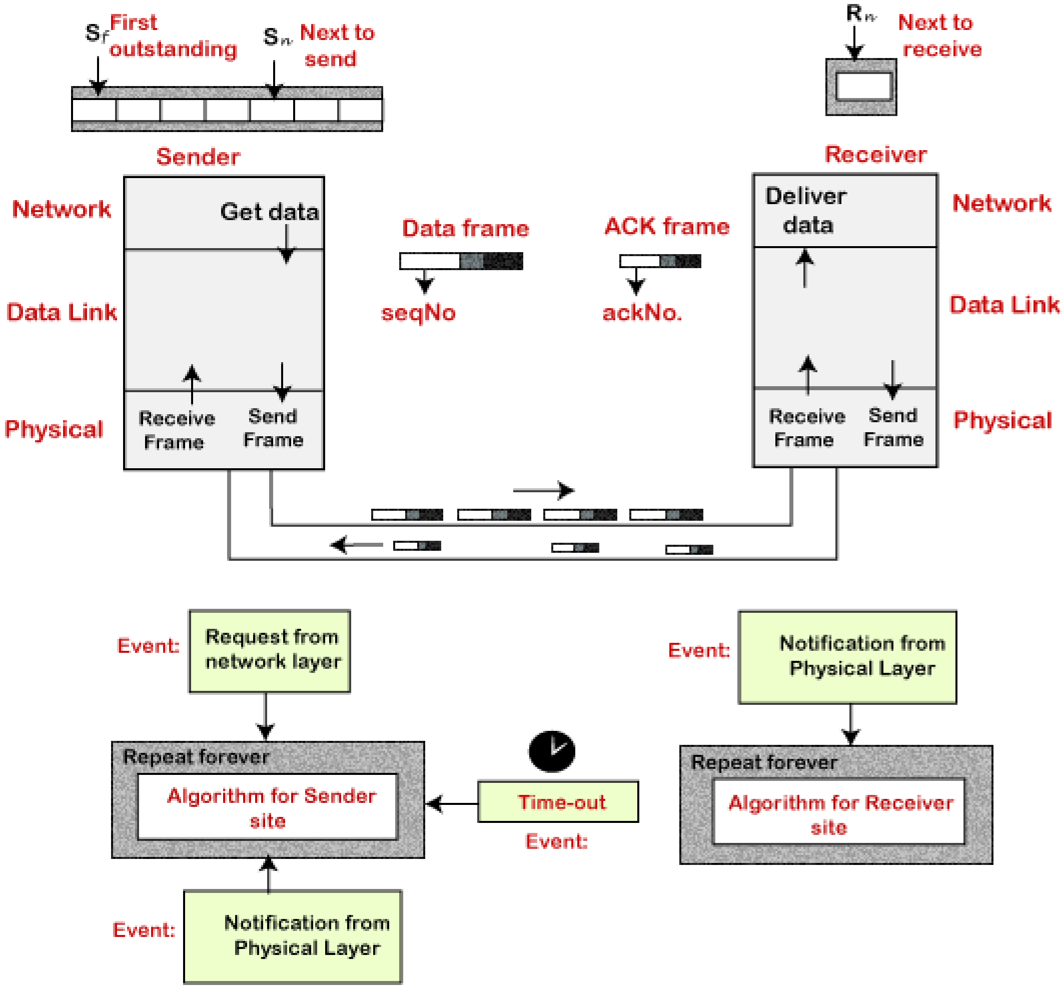
1. Go-Back-N ARQ
2. Selective Repeat ARQ

Go-Back-N ARQ

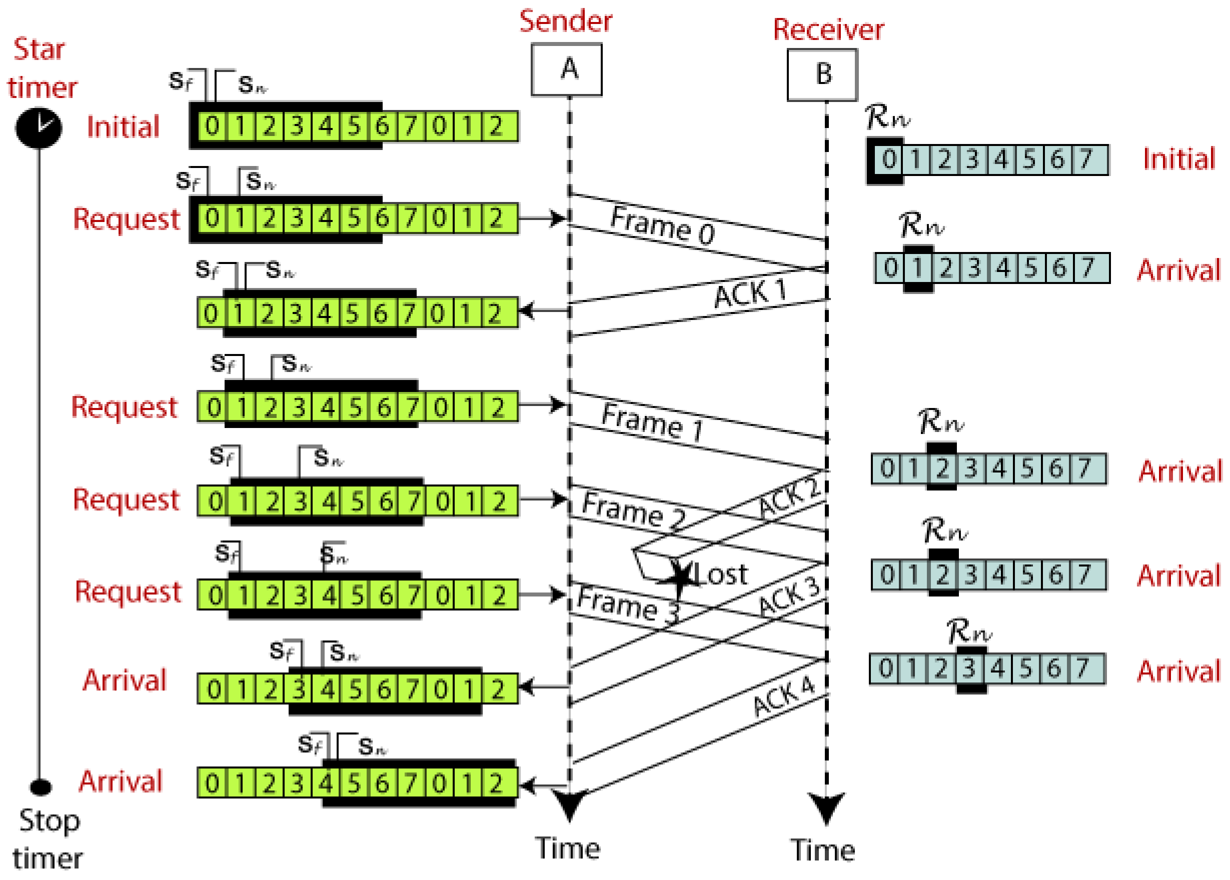
Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.



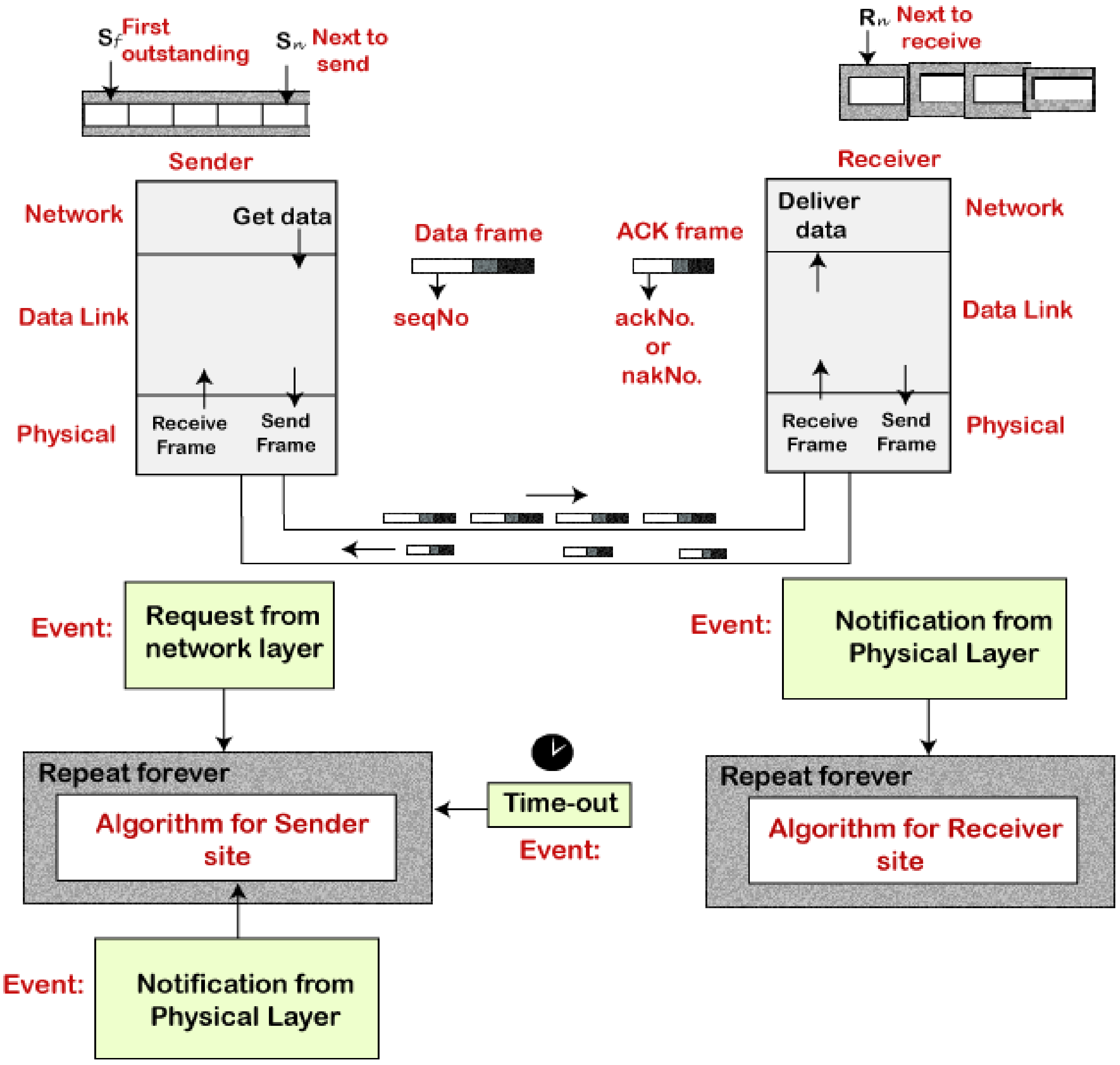
The example of Go-Back-N ARQ is shown below in the figure.



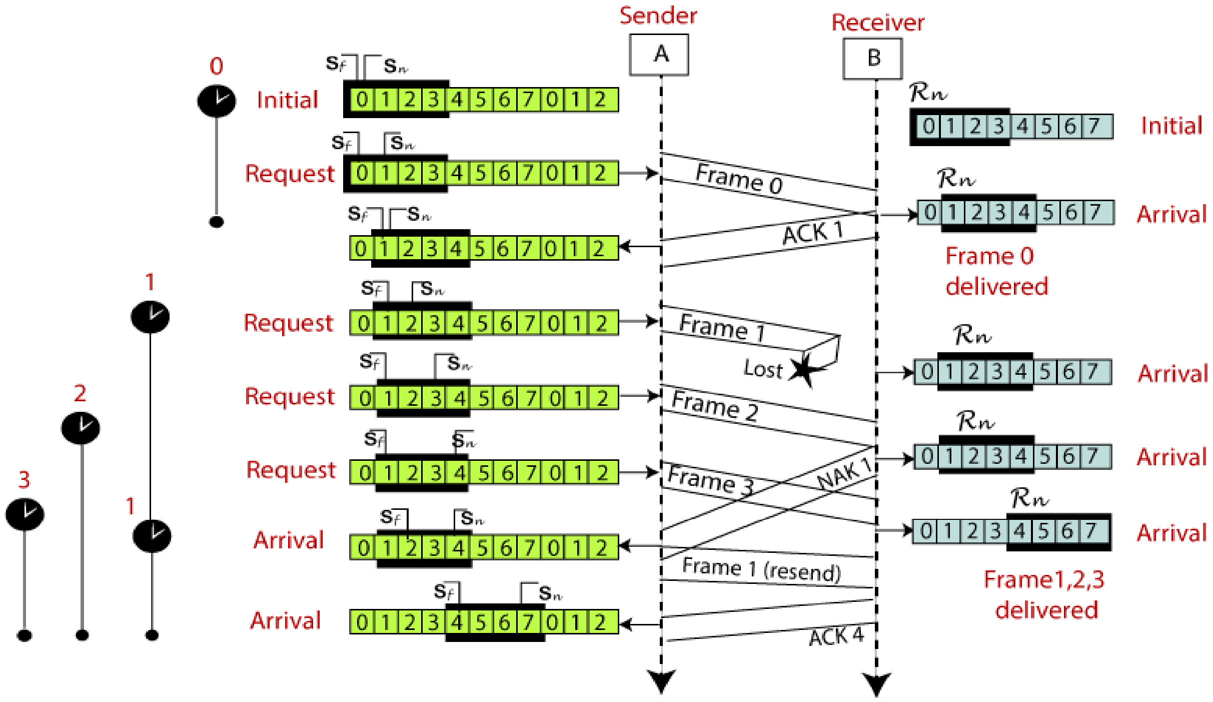
Selective Repeat ARQ

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame. The design of the Selective Repeat ARQ protocol is shown below.



The example of the Selective Repeat ARQ protocol is shown below in the figure.



Difference between the Go-Back-N ARQ and Selective Repeat ARQ?

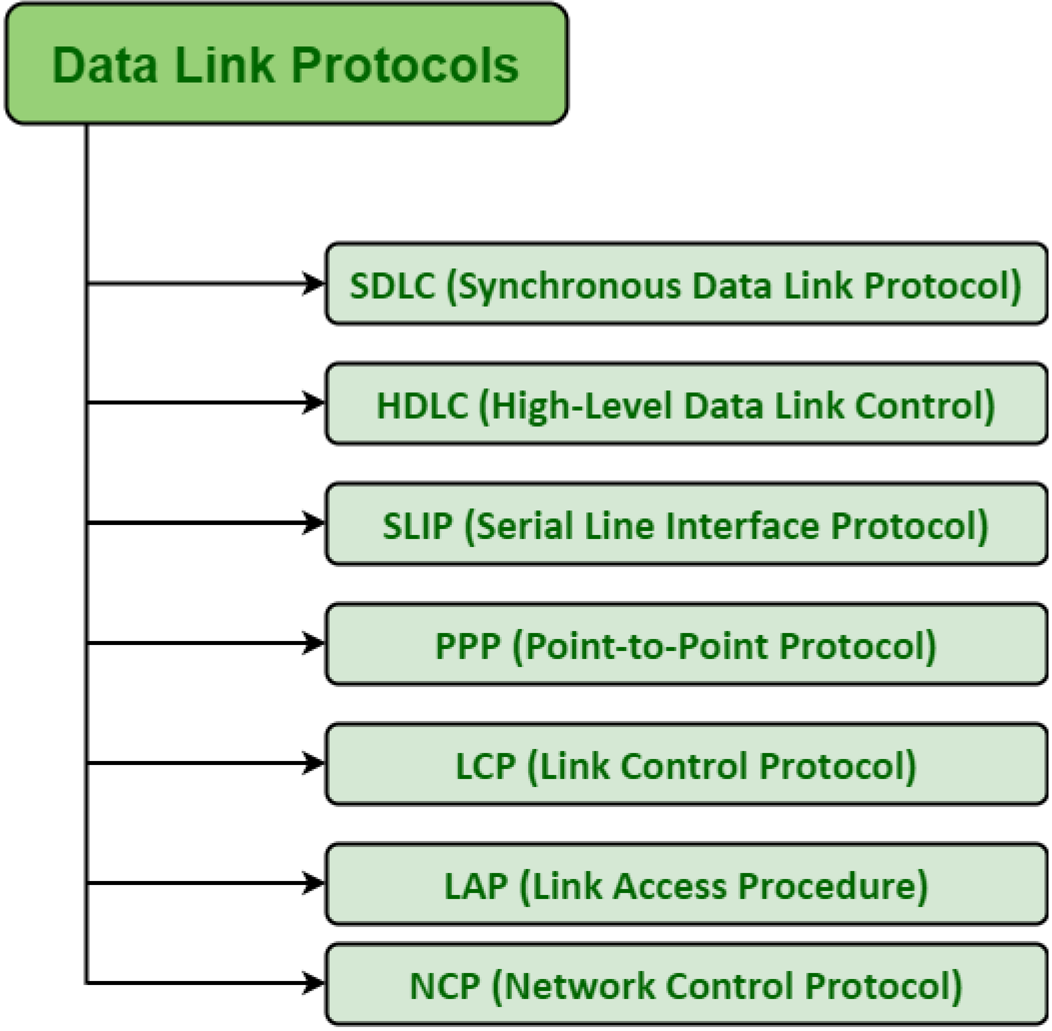
Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is more complex because it has to do sorting and searching as well. And it also requires more storage.
It does not require sorting.	In this, sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed in it.
It is used more.	It is used less because it is more complex.

Data Link Layer **protocolsS**

Data Link Layer protocols are generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to the bits and bytes being transferred. It is basically a set of specifications that are used for implementation of data link layer just above the physical layer of the Open System Interconnections (OSI) Model.

Some Common Data Link Protocols :

There are various data link protocols that are required for Wide Area Network (WAN) and modem connections. Logical Link Control (LLC) is a data link protocol of Local Area Network (LAN). Some of data link protocols are given below :


Data Link Protocols
SDLC (Synchronous Data Link Protocol)
HDLC (High-Level Data Link Control)
SLIP (Serial Line Interface Protocol)
PPP (Point-to-Point Protocol)
LCP (Link Control Protocol)
LAP (Link Access Procedure)
NCP (Network Control Protocol)

1. Synchronous Data Link Protocol (SDLC) –
   SDLC is basically a communication protocol of computer. It usually supports multipoint links even error recovery or error correction also. It is usually used to carry SNA (Systems Network Architecture) traffic and is present precursor to HDLC. It is also designed and developed by IBM in 1975. It is also used to connect all of the remote devices to mainframe computers at central locations may be in point-to-point (one-to-one) or point-to-multipoint (one-to-many) connections. It is also used to make sure that the data units should arrive correctly and with right flow from one network point to next network point.

2. High-Level Data Link Protocol (HDLC) –
   HDLC is basically a protocol that is now assumed to be an umbrella under which many Wide Area protocols sit. It is also adopted as a part of X.25 network. It was originally created and developed by ISO in 1979. This protocol is generally based on SDLC. It also provides best-effort unreliable service and also reliable service. HDLC is a bit-oriented protocol that is applicable for point-to-point and multipoint communications both.

3. Serial Line Interface Protocol (SLIP) –
   SLIP is generally an older protocol that is just used to add a framing byte at end of IP packet. It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user over a dial-up link. It is an encapsulation of the TCP/IP especially designed to work with over serial ports and several router connections simply for communication. It is some limitations like it does not provide mechanisms such as error correction or error detection.
4. Point to Point Protocol (PPP) –
   PPP is a protocol that is basically used to provide same functionality as SLIP. It is most robust protocol that is used to transport other types of packets also along with IP Packets. It can also be required for dial-up and leased router-router lines. It basically provides framing method to describe frames. It is a character-oriented protocol that is also used for error detection. It is also used to provides two protocols i.e. NCP and LCP. LCP is used for bringing lines up, negotiation of options, bringing them down whereas NCP is used for negotiating network-layer protocols. It is required for same serial interfaces like that of HDLC.

5. **Link Control Protocol (LCP) –**
   It was originally developed and created by IEEE 802.2. It is also used to provide HDLC style services on LAN (Local Area Network). LCP is basically a PPP protocol that is used for establishing, configuring, testing, maintenance, and ending or terminating links for transmission of data frames.

6. **Link Access Procedure (LAP) –**
   LAP protocols are basically a data link layer protocols that are required for framing and transferring data across point-to-point links. It also includes some reliability service features. There are basically three types of LAP i.e. LAPB (Link Access Procedure Balanced), LAPD (Link Access Procedure D-Channel), and LAPF (Link Access Procedure Frame-Mode Bearer Services). It is actually originated from IBM SDLC, which is being submitted by IBM to the ISP simply for standardization.

7. **Network Control Protocol (NCP) –**
   NCP was also an older protocol that was implemented by ARPANET. It basically allows users to have access to use computers and some of the devices at remote locations and also to transfer files among two or more computers. It is generally a set of protocols that is forming a part of PPP. NCP is always available for each and every higher-layer protocol that is supported by PPP. NCP was replaced by TCP/IP in the 1980s.

Examples of data link protocols are **Ethernet, Point-to-Point Protocol (PPP), HDLC and ADCCP**.

The network layer

The network layer or layer 3 of the OSI (Open Systems Interconnection) model is concerned delivery of data packets from the source to the destination across multiple hops or links. It is the lowest layer that is concerned with end − to − end transmission. The designers who are concerned with designing this layer needs to cater to certain issues. These issues encompasses the services provided to the upper layers as well as internal design of the layer.

The design issues can be elaborated under four heads −

- Store − and − Forward Packet Switching
- Services to Transport Layer
- Providing Connection Oriented Service
- Providing Connectionless Service

Store − and − Forward Packet Switching

The network layer operates in an environment that uses store and forward packet switching. The node which has a packet to send, delivers it to the nearest router. The packet is stored in the router until it has fully arrived and its checksum is verified for error detection. Once, this is done, the packet is forwarded to the next router. Since, each router needs to store the entire packet before it can forward it to the next hop, the mechanism is called store − and − forward switching.

Services to Transport Layer

The network layer provides service its immediate upper layer, namely transport layer, through the network − transport layer interface. The two types of services provided are −

- Connection − Oriented Service − In this service, a path is setup between the source and the destination, and all the data packets belonging to a message are routed along this path.
- Connectionless Service − In this service, each packet of the message is considered as an independent entity and is individually routed from the source to the destination.

The objectives of the network layer while providing these services are −

- The services should not be dependent upon the router technology.
- The router configuration details should not be of a concern to the transport layer.
- A uniform addressing plan should be made available to the transport layer, whether the network is a LAN, MAN or WAN.

Providing Connection Oriented Service

In connection − oriented services, a path or route called a **virtual circuit** is setup between the source and the destination nodes before the transmission starts. All the packets in the message are sent along this route. Each packet contains an identifier that denotes the virtual circuit to which it belongs to. When all the packets are transmitted, the virtual circuit is terminated and the connection is released. An example of connection − oriented service is MultiProtocol Label Switching (MPLS).

Providing Connectionless Service

In connectionless service, since each packet is transmitted independently, each packet contains its routing information and is termed as datagram. The network using datagrams for transmission is called datagram networks or datagram subnets. No prior setup of routes are needed before transmitting a message. Each datagram belong to the message follows its own individual route from the source to the destination. An example of connectionless service is Internet Protocol or IP.

Network layer is majorly focused on getting packets from the source to the destination, routing error handling and congestion control.

Before learning about design issues in the network layer, let’s learn about it’s various functions.

- **Addressing:**
  Maintains the address at the frame header of both source and destination and performs addressing to detect various devices in network.
- **Packeting:**
  This is performed by Internet Protocol. The network layer converts the packets from its upper layer.
- **Routing:**
  It is the most important functionality. The network layer chooses the most relevant and best path for the data transmission from source to destination.
- **Inter-networking:**
  It works to deliver a logical connection across multiple devices.

Network layer design issues:
The network layer comes with some design issues they are described as follows:
1. Store and Forward packet switching:
The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called “Store and Forward packet switching.”
2. Services provided to Transport Layer:
Through the network/transport layer interface, the network layer transfers it’s services to the transport layer. These services are described below.
But before providing these services to the transfer layer following goals must be kept in mind :-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

Based on the connections there are 2 types of services provided :

- **Connectionless –** The routing and insertion of packets into subnet is done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service:

Packet are termed as "datagrams" and corresponding subnet as "datagram subnets". When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via. a few protocol.Each data packet has destination address and is routed independently irrespective of the packets.

4. Implementation of Connection Oriented service:

To use a connection-oriented service, first we establishes a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.

It can be done in either two ways :

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

Routing is the process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes that data packets follow. Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

Classification of Routing Algorithms: The routing algorithms can be classified as follows:

1. Adaptive Algorithms –

These are the algorithms that change their routing decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as the traffic of the network. Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops, and estimated transit time.

Further, these are classified as follows:

- **(a) Isolated –** In this method each, node makes its routing decisions using the information it has without seeking information from other nodes. The sending nodes don't have information about the status of a particular link. The disadvantage is that packets may be sent through a congested network which may result in delay. Examples: Hot potato routing, backward learning.

- **(b) Centralized –** In this method, a centralized node has entire information about the network and makes all the routing decisions. The advantage of this is only one node is required to keep the information of the entire network and the disadvantage is that if the central node goes down the entire network is done. The link state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.

- **(c) Distributed –** In this method, the node receives information from its neighbors and then takes the decision about routing the packets. A disadvantage is that the packet may be delayed if there is a change in between intervals in which it receives information and sends packets. It is also known as a decentralized algorithm as it computes the least-cost path between source and destination

2. Non-Adaptive Algorithms –
These are the algorithms that do not change their routing decisions once they have been selected. This is also known as static routing as a route to be taken is computed in advance and downloaded to routers when a router is booted.
Further, these are classified as follows:

- **(a) Flooding –** This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in a loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count, and spanning trees.

- **(b) Random walk –** In this method, packets are sent host by host or node by node to one of its neighbors randomly. This is a highly robust method that is usually implemented by sending packets onto the link which is least queued.

Classes of Routing Protocols

Routing is a process in which the layer 3 devices (either router or layer 3 switches) find the optimal path to deliver a packet from one network to another. Dynamic routing protocols use metric, cost, and hop count to identify the best path from the path available for the destination network. There are mainly 3 different classes of routing protocols:

1. Distance Vector Routing Protocol :
These protocols select the best path on the basis of hop counts to reach a destination network in a particular direction. Dynamic protocol like RIP is an example of a distance vector routing protocol. Hop count is each router that occurs in between the source and the destination network. The path with the least hop count will be chosen as the best path.
Features –

- Updates of the network are exchanged periodically.
- Updates (routing information) is not broadcasted but shared to neighbouring nodes only.
- Full routing tables are not sent in updates but only distance vector is shared.
- Routers always trust routing information received from neighbor routers. This is also known as routing on rumors.

Disadvantages –

- As the routing information is exchanged periodically, unnecessary traffic is generated which consumes available bandwidth.
- As full routing tables are exchanged, therefore it has security issues. If an **un-authorized** person enters the network, then the whole topology will be very easy to understand.
- Also, the broadcasting of the network periodically creates unnecessary traffic.

2. Link State Routing Protocol :
These protocols know more about Internetwork than any other distance vector routing protocol. These are also known as SPF (Shortest Path First) protocol. OSPF is an example of link-state routing protocol.
Features –

- Hello, messages, also known as keep-alive messages are used for neighbor discovery and recovery.
- Concept of triggered updates is used i.e updates are triggered only when there is a topology change.
- Only that many updates are exchanged which is requested by the neighbor router.

Link state routing protocol maintains three tables namely:

1. **Neighbor table-** the table which contains information about the neighbors of the router only, i.e, to which adjacency has been formed.
2. **Topology table-** This table contains information about the whole topology i.e contains both best and backup routes to a particular advertised networks.
3. **Routing table-** This table contains all the best routes to the advertised network.

Advantages –

- As it maintains separate tables for both the best route and the backup routes (whole topology) therefore it has more knowledge of the internetwork than any other distance vector routing protocol.
- Concept of triggered updates is used therefore no more unnecessary bandwidth consumption is seen like in distance vector routing protocol.
- Partial updates are triggered when there is a topology change, not a full update like distance vector routing protocol where the whole routing table is exchanged.

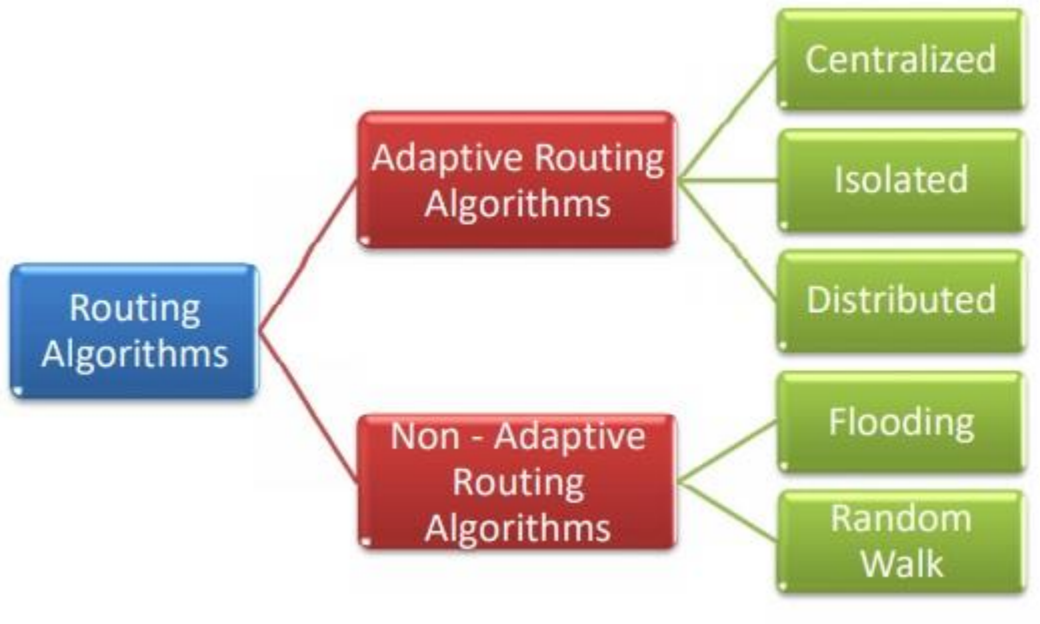
3. Advanced Distance vector routing protocol :
It is also known as hybrid routing protocol which uses the concept of both distance vector and link-state routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an example of this class of routing protocol. EIGRP acts as a link-state routing protocol as it uses the concept of Hello protocol for neighbor discovery and forming an adjacency. Also, partial updates are triggered when a change occurs. EIGRP acts as a distance-vector routing protocol as it learned routes from directly connected neighbors.

What is a Routing Algorithm in Computer Network?

A routing algorithm is a procedure that lays down the route or path to transfer data packets from source to the destination. They help in directing Internet traffic efficiently. After a data packet leaves its source, it can choose among the many different paths to reach its destination. Routing algorithm mathematically computes the best path, i.e. “least – cost path” that the packet can be routed through.

Types of Routing Algorithms

Routing algorithms can be broadly categorized into two types, adaptive and nonadaptive routing algorithms. They can be further categorized as shown in the following diagram −



Adaptive Routing Algorithms

Adaptive routing algorithms, also known as dynamic routing algorithms, makes routing decisions dynamically depending on the network conditions. It constructs the routing table depending upon the network traffic and topology. They try to compute the optimized route depending upon the hop count, transit time and distance.

The three popular types of adaptive routing algorithms are −

- **Centralized algorithm** − It finds the least-cost path between source and destination nodes by using global knowledge about the network. So, it is also known as global routing algorithm.
- **Isolated algorithm** − This algorithm procures the routing information by using local information instead of gathering information from other nodes.
- **Distributed algorithm** − This is a decentralized algorithm that computes the least-cost path between source and destination iteratively in a distributed manner.

Non – Adaptive Routing Algorithms

Non-adaptive Routing algorithms, also known as static routing algorithms, construct a static routing table to determine the path through which packets are to be sent. The static routing table is constructed based upon the routing information stored in the routers when the network is booted up.

The two types of non – adaptive routing algorithms are −

- **Flooding** − In flooding, when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on. Flooding may be uncontrolled, controlled or selective flooding.
- **Random walks** − This is a probabilistic algorithm where a data packet is sent by the router to any one of its neighbours randomly.

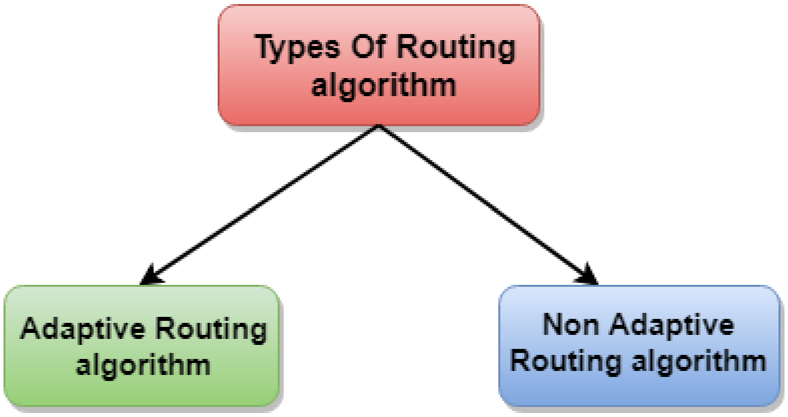
Routing algorithm

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm


Types Of Routing algorithm
Adaptive Routing algorithm
Non Adaptive Routing algorithm

Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.

- The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
- **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

What is Congestion Control Algorithm?

Congestion causes choking of the communication medium. When too many packets are displayed in a method of the subnet, the subnet's performance degrades. Hence, a network's communication channel is called congested if packets are traversing the path and experience delays mainly over the path's propagation delay.

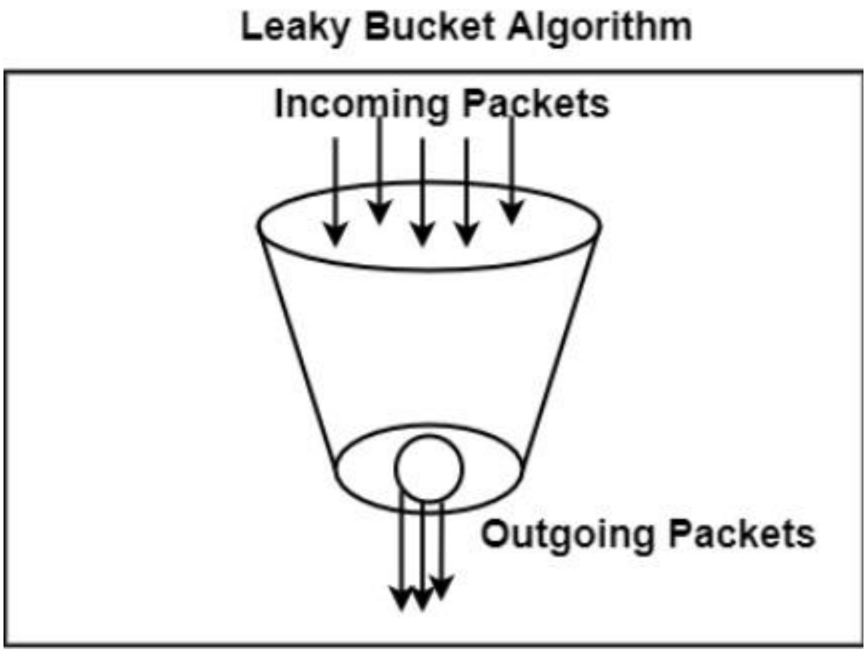
There is two congestion control algorithm which is as follows:

Leaky Bucket

The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting. The algorithm allows controlling the rate at which a record is injected into a network and managing burstiness in the data rate.

A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms. This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.

The figure shows the leaky bucket algorithm.



In this algorithm, a bucket with a volume of, say, b bytes and a hole in the Notes bottom is considered. If the bucket is null, it means b bytes are available as storage. A packet with a size smaller than b bytes arrives at the bucket and will forward it. If the packet's size increases by more than b bytes, it will either be discarded or queued. It is also considered that the bucket leaks through the hole in its bottom at a constant rate of r bytes per second.

The outflow is considered constant when there is any packet in the bucket and zero when it is empty. This defines that if data flows into the bucket faster than data flows out through the hole, the bucket overflows.

The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources. The leak rate is a fixed parameter. In the case of the traffic, volume is deficient, the large area of network resources such as bandwidth is not being used effectively. The leaky-bucket algorithm does not allow individual flows to burst up to port speed to effectively consume network resources when there would not be resource contention in the network.

Token Bucket Algorithm

The leaky bucket algorithm has a rigid output design at the average rate independent of the bursty traffic. In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.

It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket. The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.

When tokens are shown, a flow to transmit traffic appears in the display of tokens. No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

Thus, the token bucket algorithm adds a token to the bucket each 1 / r seconds. The volume of the bucket is b tokens. When a token appears, and the bucket is complete, the token is discarded. If a packet of n bytes appears and n tokens are deleted from the bucket, the packet is forwarded to the network.

When a packet of n bytes appears but fewer than n tokens are available. No tokens are removed from the bucket in such a case, and the packet is considered non-conformant. The non-conformant packets can either be dropped or queued for subsequent transmission when sufficient tokens have accumulated in the bucket.

They can also be transmitted but marked as being non-conformant. The possibility is that they may be dropped subsequently if the network is overloaded.

What is **congestion**?
A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

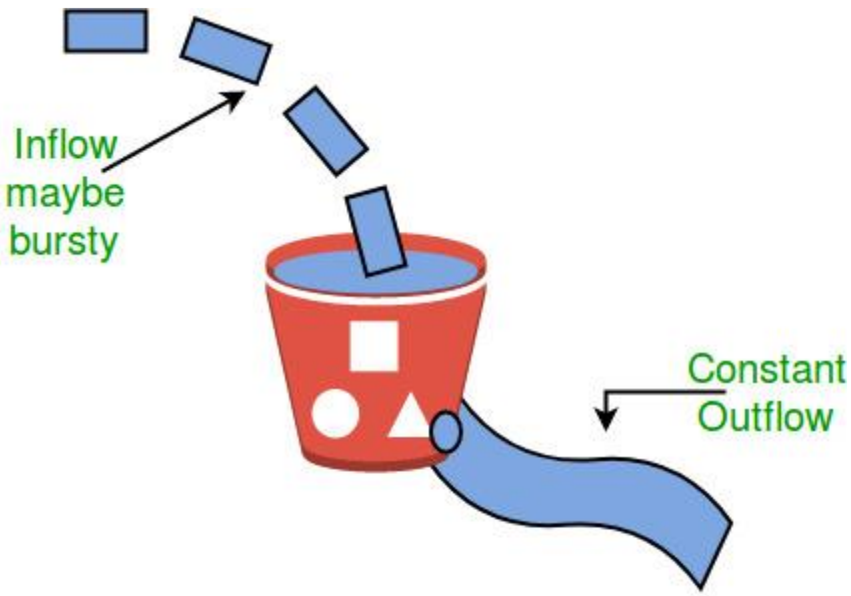
Congestion control algorithms

- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.
- There are two congestion control algorithm which are as follows:

- **Leaky Bucket Algorithm**
- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
- This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
- The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

- **Token bucket Algorithm**
- The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.
- In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.
- It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
- The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
- When tokens are shown, a flow to transmit traffic appears in the display of tokens.
- No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

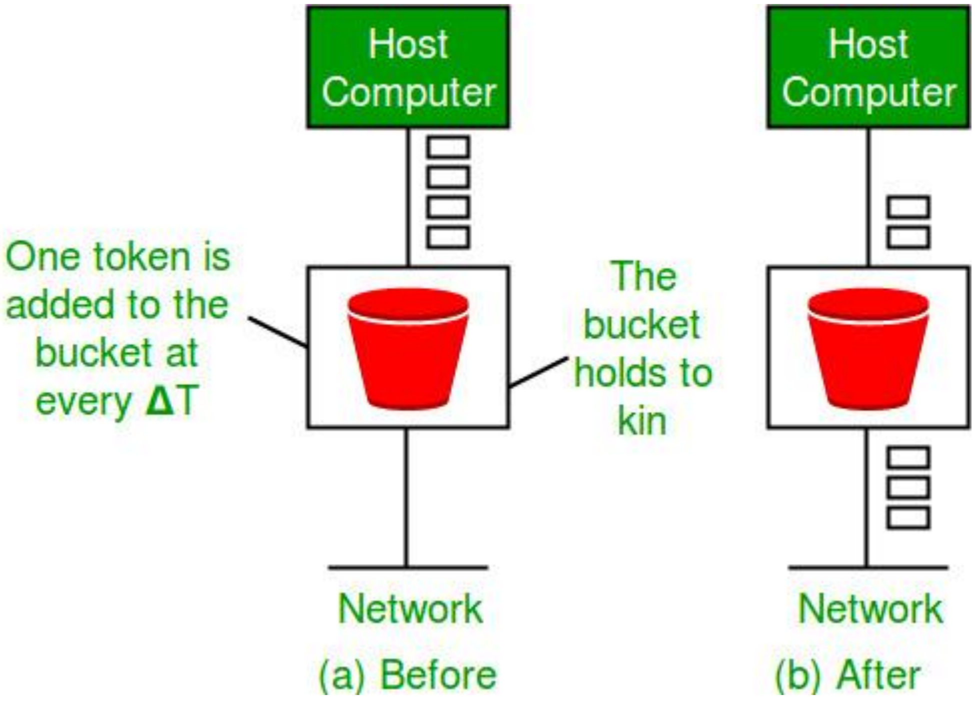
Need of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket. ƒ
2. The bucket has a maximum capacity. ƒ

3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.



Network layer

- transport segment from sending to receiving host
- on sending side encapsulates segments into datagrams
- on receiving side, delivers segments to transport layer
- network layer protocols in *every* host, router
- router examines header fields in all IP datagrams passing through it

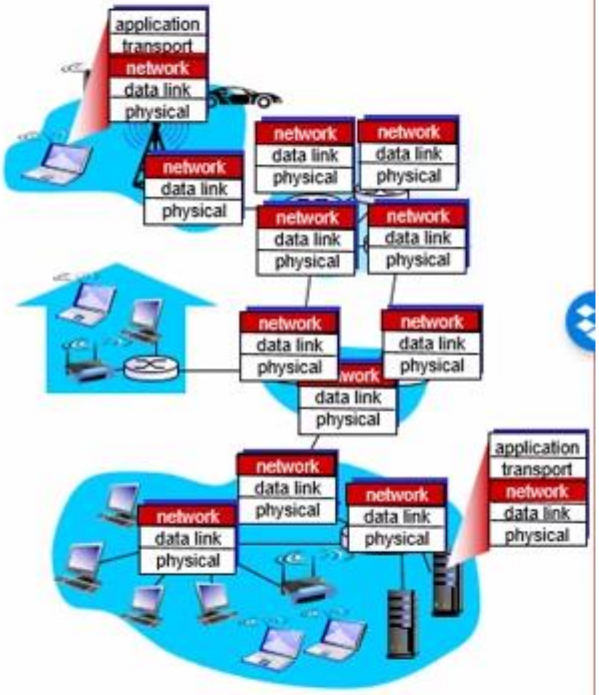


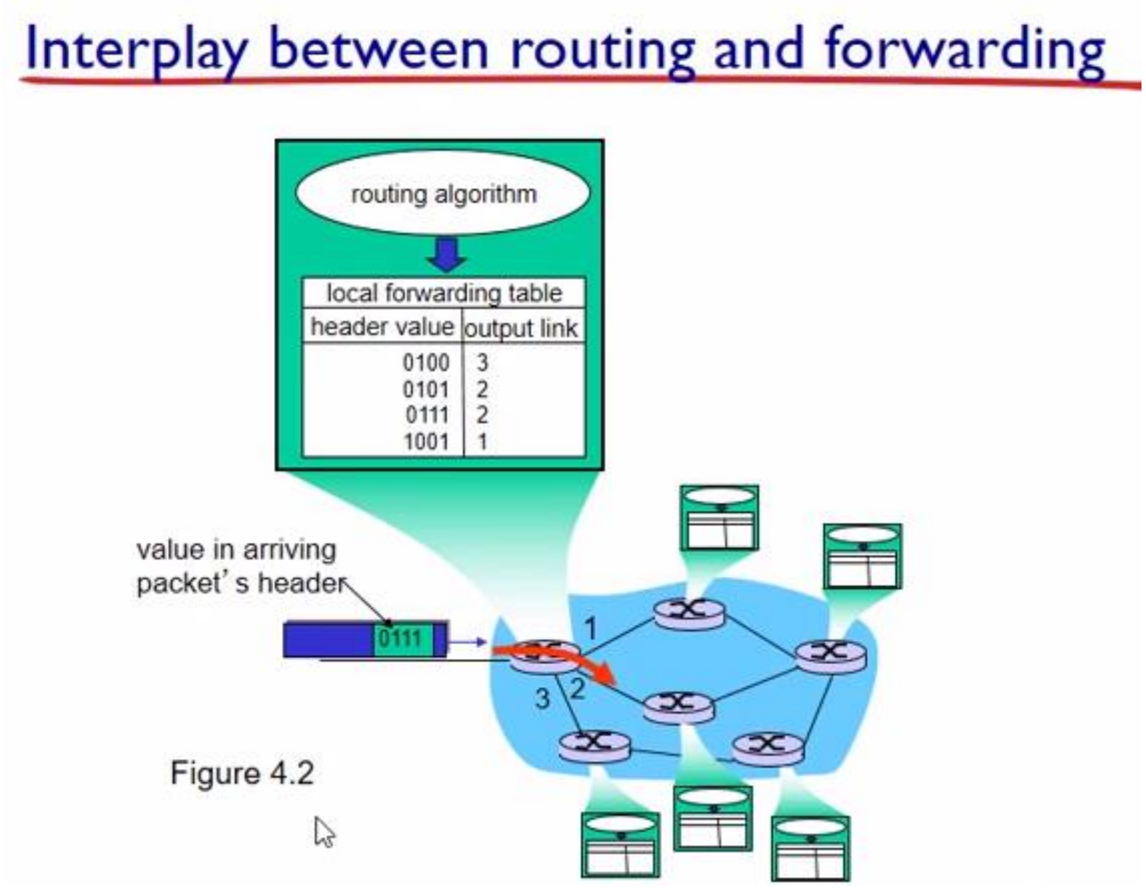
Figure 4.1

Two key network-layer functions

- *forwarding:* move packets from router's input to appropriate router output
- *routing:* determine route taken by packets from source to dest.
  - *routing algorithms*

analogy:

- *routing:* process of planning trip from source to dest
- *forwarding:* process of getting through single interchange

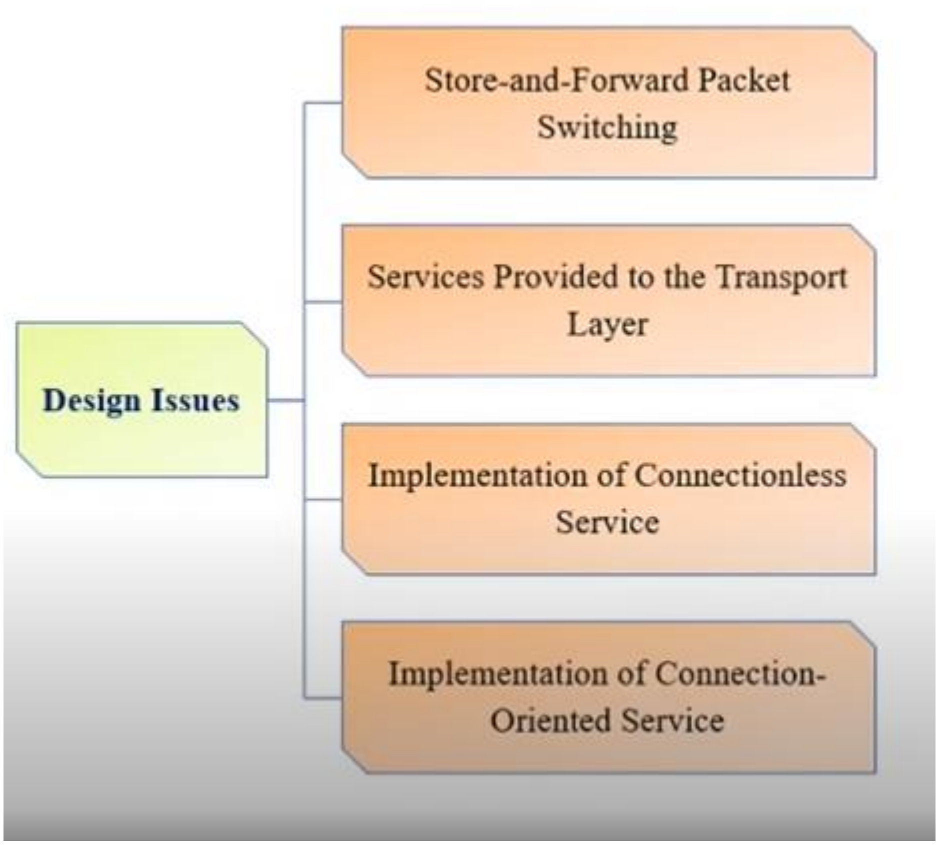


Interplay between routing and forwarding

local forwarding table	
header value	output link
0100	3
0101	2
0111	2
1001	1

value in arriving packet's header

Figure 4.2



Design Issues

- Store-and-Forward Packet Switching
- Services Provided to the Transport Layer
- Implementation of Connectionless Service
- Implementation of Connection-Oriented Service

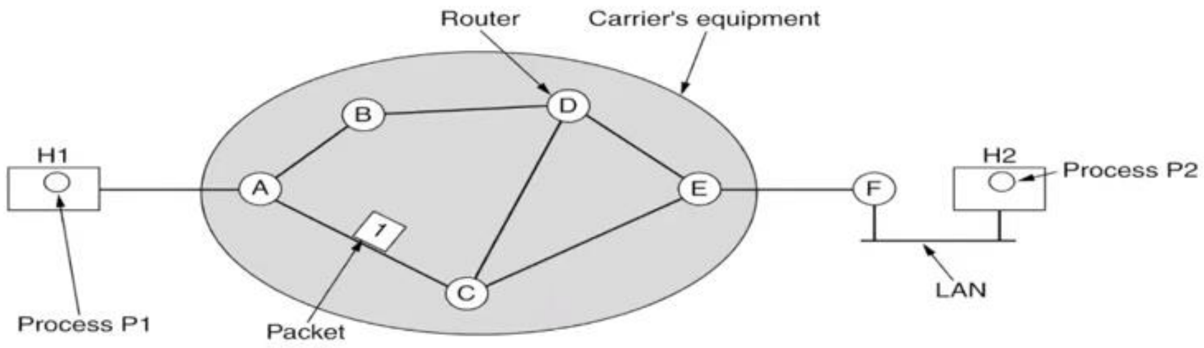
Store-and-Forward Packet Switching

Services Provided to the Transport Layer

Implementation of Connectionless Service

Implementation of Connection-Oriented Service

Comparison of Virtual-Circuit and Datagram Subnets



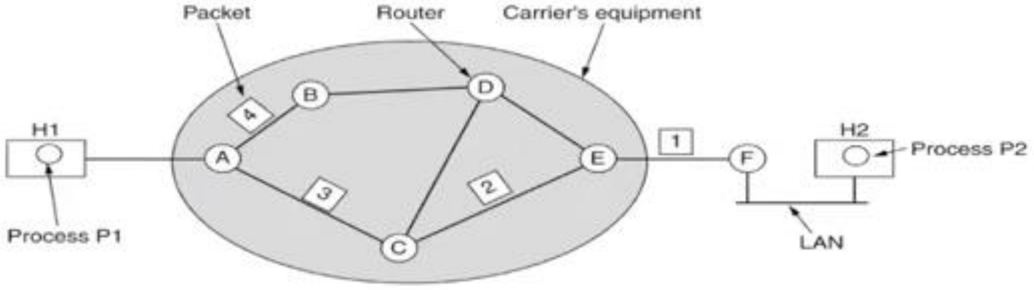
The environment of the network layer protocols.

Services Provided to the Transport Layer

The services should be independent of the router technology.

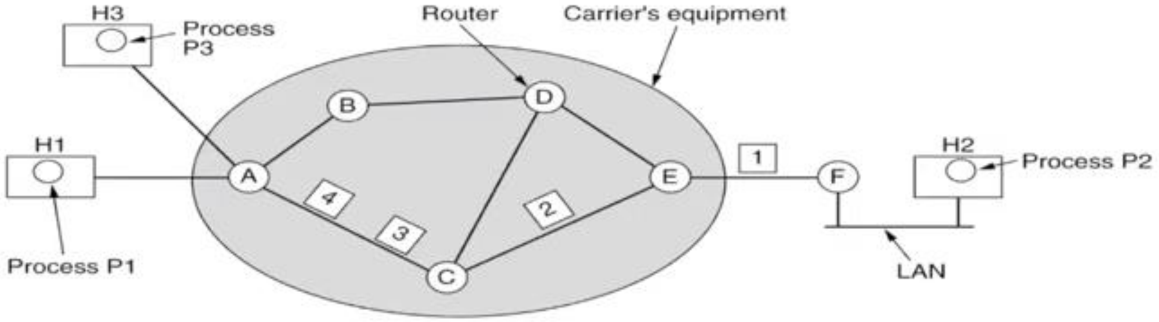
The transport layer should be shielded from the number, type, and topology of the routers present.

The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.



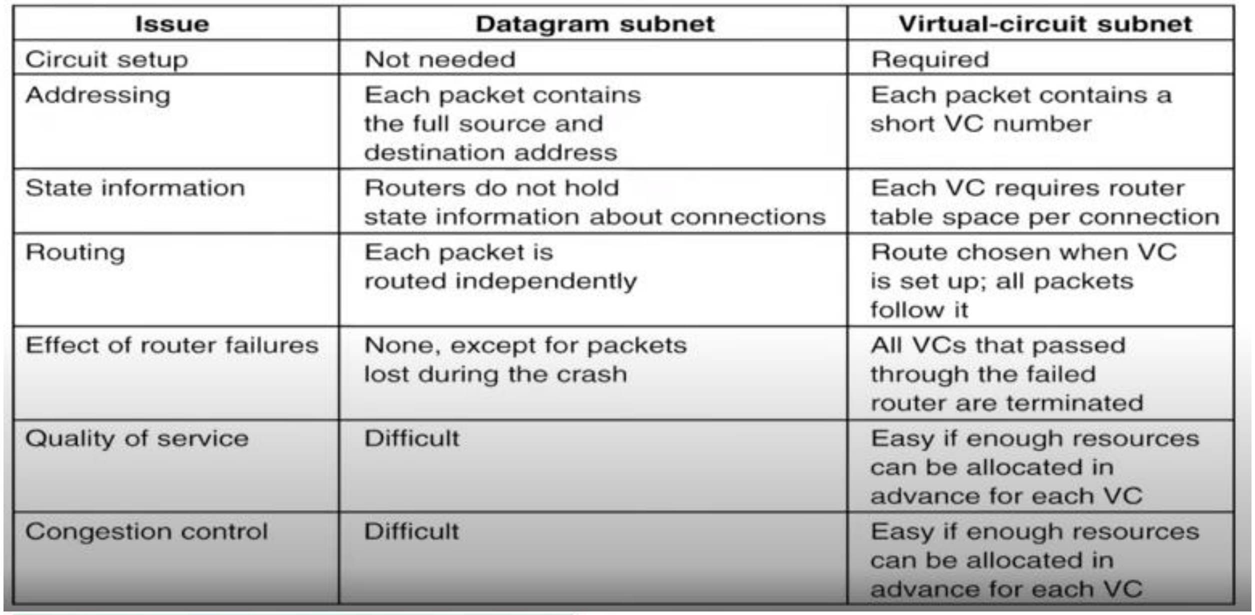
A's table							
initially		later		C's table		E's table	
A	–	A	–	A	A	A	C
B	B	B	B	B	A	B	D
C	C	C	C	C	–	C	C
D	B	D	B	D	D	D	D
E	C	E	B	E	E	E	–
F	C	F	B	F	E	F	F
Dest.	Line						

Routing within a diagram subnet.



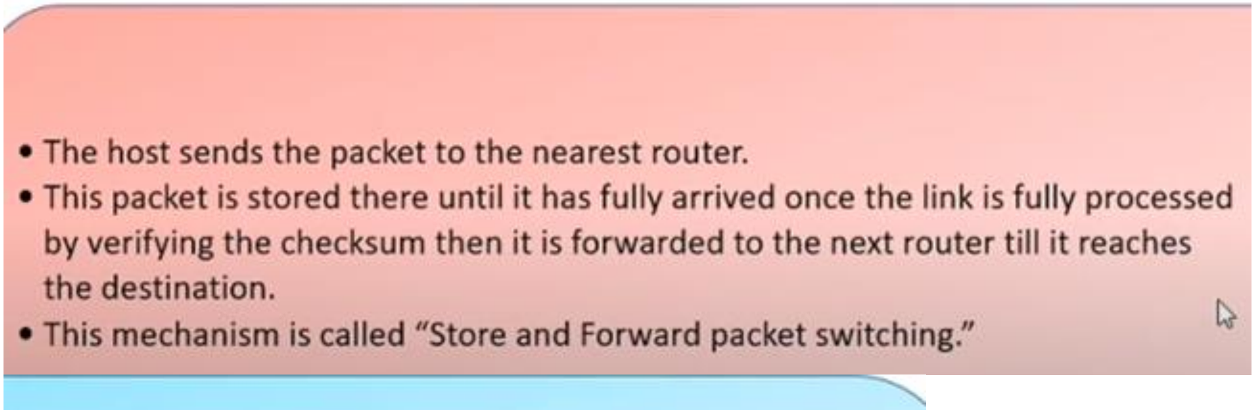
A's table				C's table				E's table			
H1	1	C	1	A	1	E	1	C	1	F	1
H3	1	C	2	A	2	E	2	C	2	F	2
In		Out									

Routing within a virtual-circuit subnet.

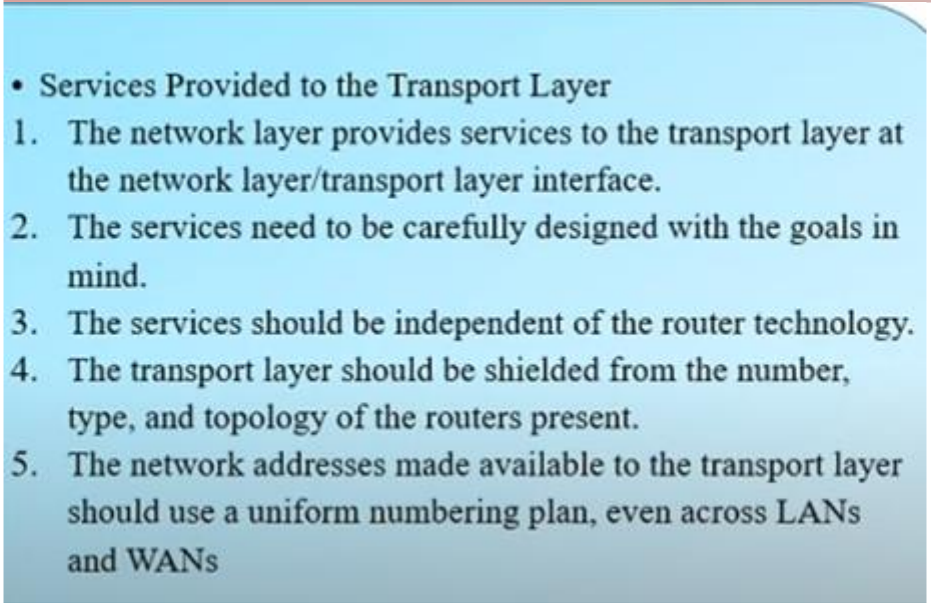


Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

- Store-and-Forward Packet Switching



- The host sends the packet to the nearest router.
- This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination.
- This mechanism is called “Store and Forward packet switching.”

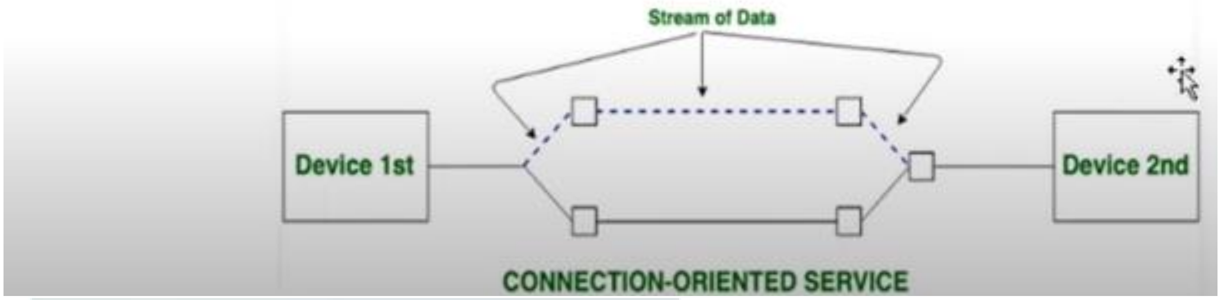


- Services Provided to the Transport Layer

1. The network layer provides services to the transport layer at the network layer/transport layer interface.
2. The services need to be carefully designed with the goals in mind.
3. The services should be independent of the router technology.
4. The transport layer should be shielded from the number, type, and topology of the routers present.
5. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs

Connection Oriented Service

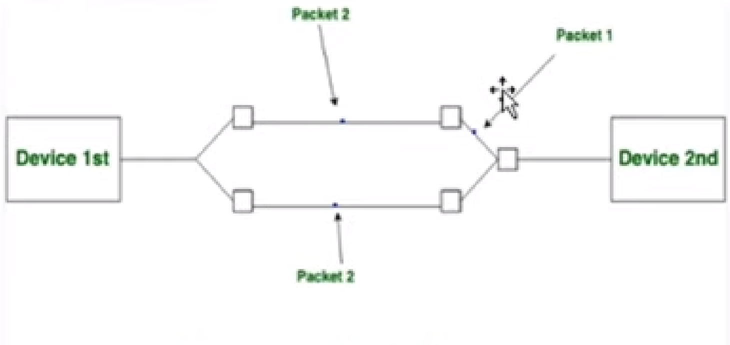
- Connection is established beforehand.
- Message is broken into packets and routed over the established route.
- Reliable data transmission.



CONNECTION-ORIENTED SERVICE

Implementation of Connectionless Service

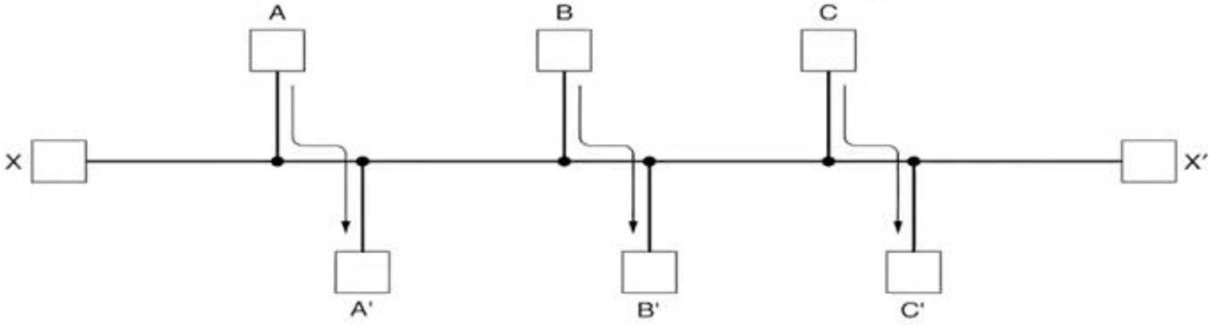
- No connection setup
- Message is broken into packets and Each packet is individually routed
- Routers decides line based on routing table
- Packets may follow different paths
- Not guaranteed to arrive in order



CONNECTIONIESS SERVICE

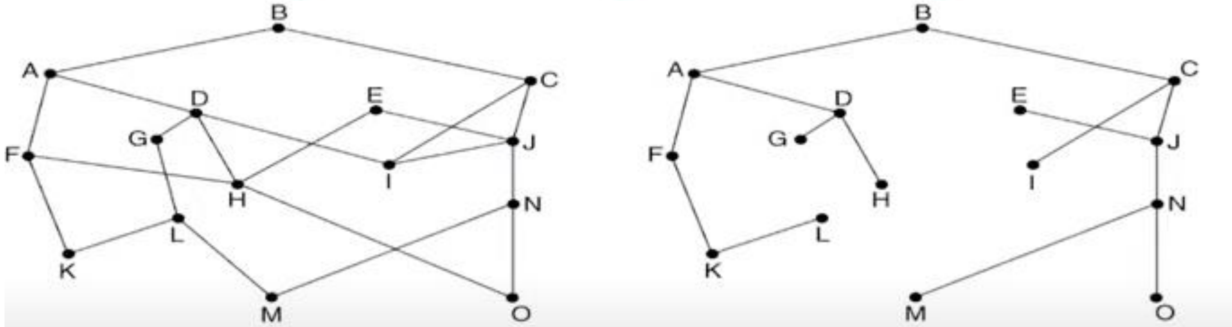
Routing Algorithms

- The Optimality Principle
- Shortest Path Routing
- Flooding
- Distance Vector Routing



Conflict between fairness and optimality.

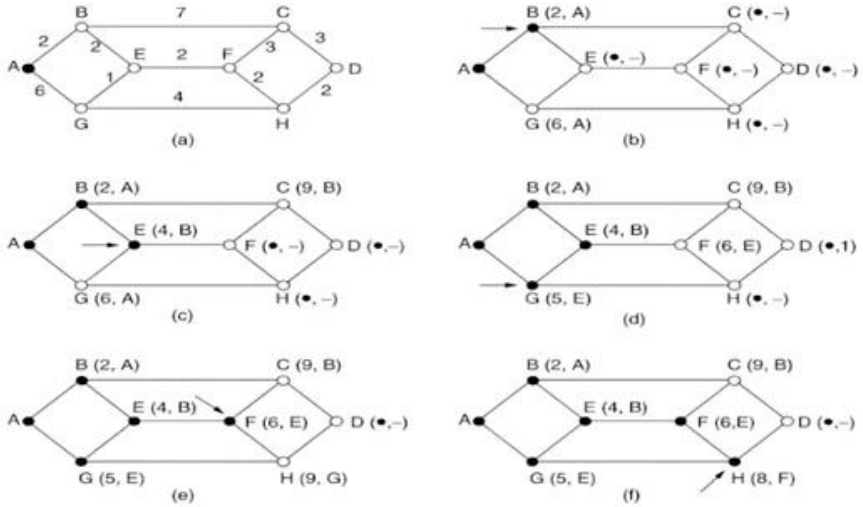
The Optimality Principle



(a) (b)

(a) A subnet. (b) A sink tree for router B.

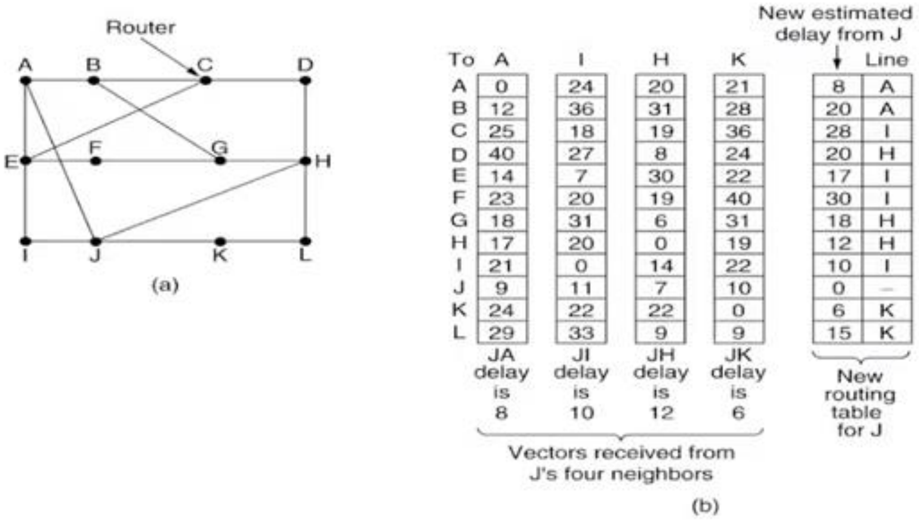
Shortest Path Routing



[he first 5 steps used in computing the shortest path from A to D. The arrows indicate the working node.

Flooding

Distance Vector Routing



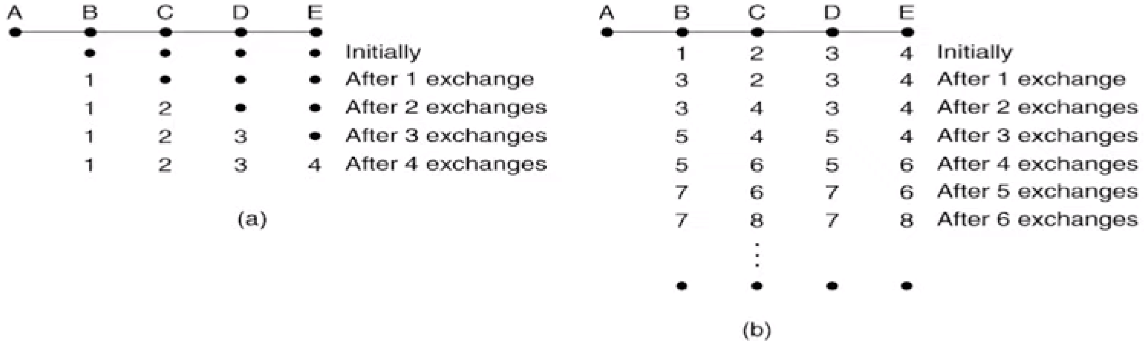
To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J	

Vectors received from J's four neighbors

(b)

(a) A subnet. (b) Input from A, I, H, K, and the new routing table for J.

Distance Vector Routing (2)



B	C	D	E	
•	•	•	•	Initially
1	•	•	•	After 1 exchange
1	2	•	•	After 2 exchanges
1	2	3	•	After 3 exchanges
1	2	3	4	After 4 exchanges

(a)

B	C	D	E	
1	2	3	4	Initially
3	2	3	4	After 1 exchange
3	4	3	4	After 2 exchanges
5	4	5	4	After 3 exchanges
5	6	5	6	After 4 exchanges
7	6	7	6	After 5 exchanges
7	8	7	8	After 6 exchanges
	⋮			
•	•	•	•	

(b)

The count-to-infinity problem.