MAC ADDRESS

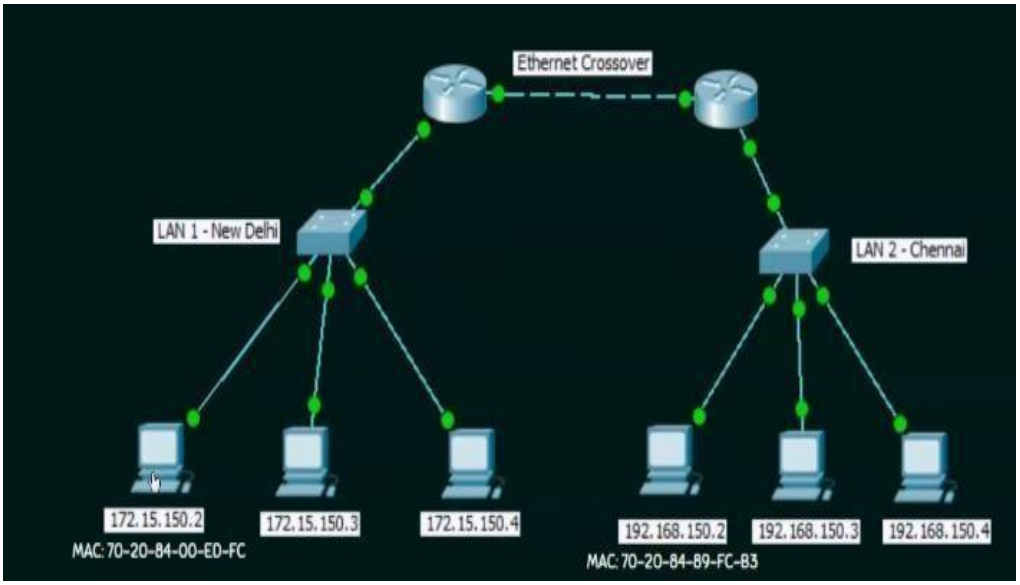
- MAC stands for Medium Access Control.
- Every node in the LAN is identified with the help of MAC Address.
- IP Address = Location of a person
- MAC Address = Name of the person.
- IP Addresses are router friendly addresses
- MAC Addresses are used by switches to deliver the data to the rightdestination.
- Unique
- Can't be changed.
- Assigned by the manufacturer.
- Represented in hexadecimal.
- Ex: 70-20-84-00-DE-AB (48 bits).
- Separator: hyphen (-), period (.), and colon (:)

PORT ADDRESS

Reaching our city = Reaching our network. (IP Address) Reaching our Apartment =

Reaching the host. (MAC Address)

Reaching our right person = Reaching the right process. (Port Address)



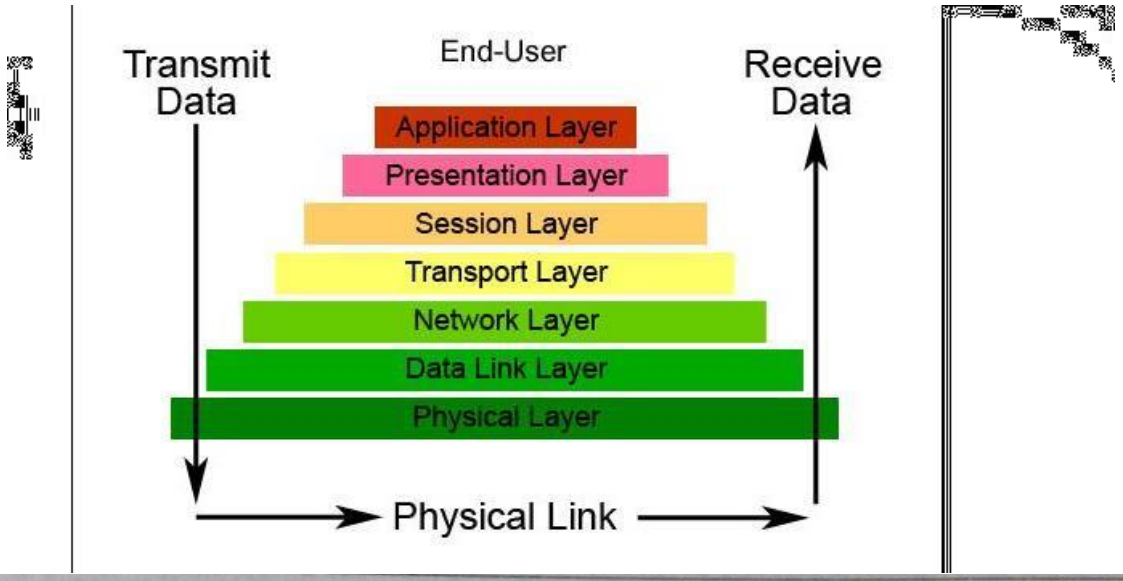
LAYERING

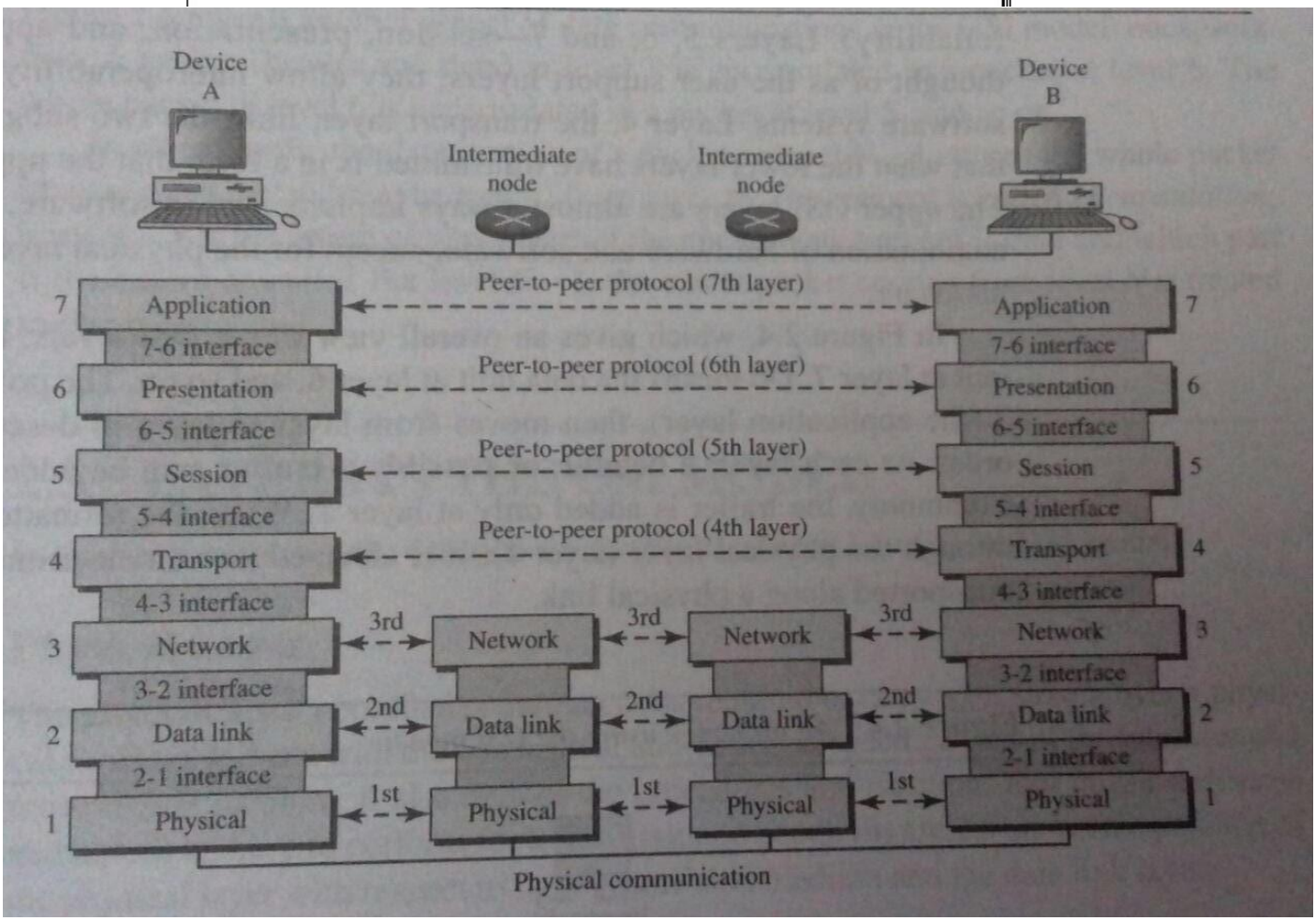
- Layering means decomposing the problem of building a network into more manageable components (Layers).
- Helps to more modular design and easy to troubleshoot.

OSI Model

The purpose of the OSI Model is to facilitate communication between different systems without requiring changes to the logic of the underlying Hardware and Software.

Layers in the OSI Reference Model





1. Application – “My message”
2. Presentation – 0dfpds321pQsljf*pthoi
3. Session - 0dfpds321pQsljf*pthoi
4. Transport – TL INFO - 0dfpds321pQsljf*pthoi
5. Network – NL INFO - TL INFO - 0dfpds321pQsljf*pthoi

6. Data Link – DL INFO - NL INFO - TL INFO - 0dfpds321pQsljf*pthoi
7. Physical – 10010110101001001101

APPLICATION LAYER

It enables the user to access the network resources.

For instance, device A wants to send the data to device B, there is an application (which sends the data to device B) that enables the user of device A to access the network resources.

Services provided by Application Layer

- **File Transfer and Access Management (FTAM)**. (Allows to send the data to remote computer or receive the data from the remote computer).
- **Mail Services** (allows to access email services).
- **Directory Services** (provides access to the data globally).

PRESENTATION LAYER

It is concerned with the **syntax** and **semantics** of the information exchanged between twosystems.

Syntax means the structure or the format of the message that is being sent. For instance, 16 bit of data is transmitting, what does the first 8-bit represent and what's the second 8-bit represent?

Semantics means, it refers to the meaning of each section. For instance, if the message has 3 sections, what is the meaning of the first section, second section and all the meaning of the section of the bits that are being transmitting.

Services provided by Presentation Layer

- Translation (Converting the data that is send by the sender into a common format which is acceptable by all devices)
- Encryption (Converting the message into some unreadable text)
- Compression (It means reducing the no. of bits contained in the information(multimedia messages))

SESSION LAYER

It establishes, maintains and synchronized the interaction among communicating devices. (It allows two systems to enter into a dialog).

Services provided by Presentation Layer

- Dialog control (Communication between two process to take place either in a Simplex way or half duplex mode or full duplex way).
- Synchronization

It means, the session layer allows a process to add checkpoints or synchronization points. For instance the information that is sending is a big file of 2000 pages and it is advisable to insert a checkpoint after every 100 pages to ensure that 100 pages unit is received and acknowledged independently. In this case, if a crash happens during a transmission of a particular page, only that page can be resent.

TRANSPORT LAYER

It is responsible for process-to-process delivery of the entire message.
(Each Application is assigned to process members by OS and that process is going to communicate with the internet then the OS will assigns PORT number. For instance, device A is sending the message then the port no. of A will be assigned to the message by OS)

Services provided by Transport Layer

- **Port addressing**
  process is identified with the help of port numbers.
- **Segmentation and Reassembly**

(Breaks the big message into smaller messages, where each messages can be numbered. And after reached the destination device B, B will reassemble all the messages and construct the original message)

- **Connection control**
  (Between the two nodes, whether there is going to be a **connection-oriented service** (before sending the data connection will be established) or **connection less** (Connection will not be established and the message will be sent just like that.

- **End-to-End Flow Control**
  (If the sender is a fast sender and the receiver is slow receiver, so the receiver can't handle that speed. For that the sender and the receiver agree upon a common speed matching mechanisms. So that the data send by the receiver will not be loss by the receiver.)

- **Error Control**
  (Whatever transport layer constructs, that data will be checked for errors)

NETWORK LAYER

It is responsible for delivery of data from the original source to the destination network.

Services provided by Transport Layer

- **Logical Addressing**
  (It helps to the router to take decision. i.e., When a packet is received by the router, it will have source and destination IP addresses. So that router knows what is the source and the destination of that packet.)

- **Routing -** finding the best route for the packet to be transmitted. For finding the best routes it uses IP Address.

DATA LINK LAYER

It is responsible for moving data (frames) from one node to another node.

Services provided by Transport Layer

- **Framing**
  The data link layer of the node, it groups the bits of zeros and ones and we call that grouping as frames.
- **Physical Addressing**
- **Flow Control**
- **Error Control**
- **Access Control**
  When 2 or more devices are connected to the common link, then data link layer protocolsare necessary to determine which node has control over the link at a given time.

  After the time is over, then it is the turn of other computer to use it.

PHYSICAL LAYER

It is responsible for transmitting bits over a medium. And also provides electrical and mechanical specifications.

After creating the frame, it is the responsibility of the physical layer to place that frames on the medium.

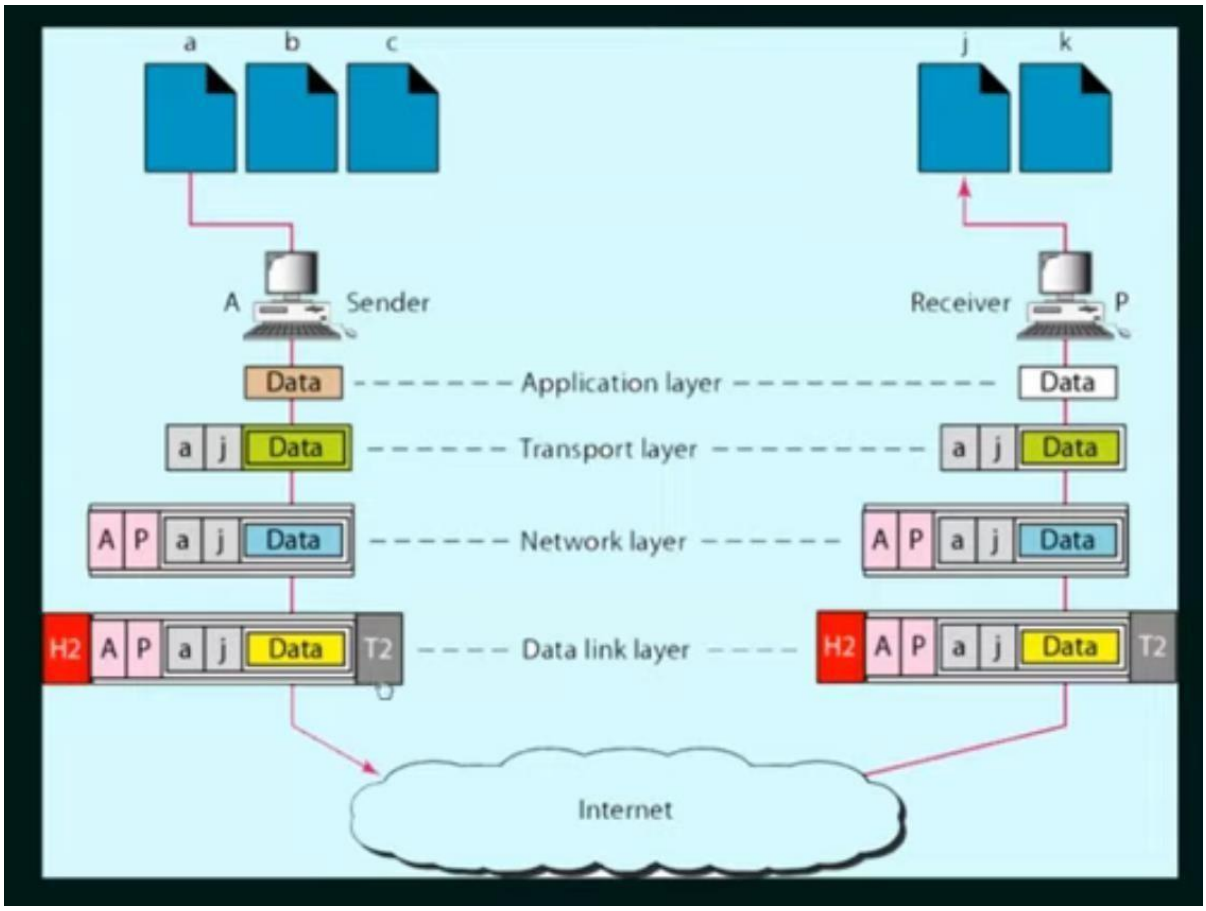
There are 2 kinds of medium: Wired and Wireless.

The physical layer knows what kind of the medium it has and it sends the data over that medium.If the medium is a wired, it converts the entire frames into signals.

For eg: If medium is an Ethernet cable – converts into electrical signals.Fiber optic cable – light signals

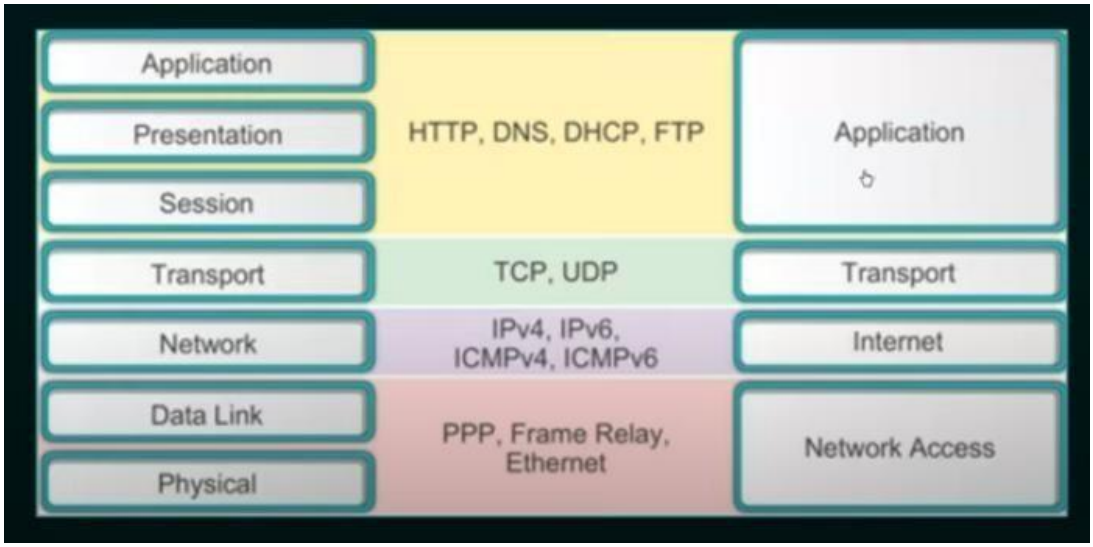
Services provided by Physical Layer

- **Physical characteristics of the media**
  What kind of media was connected.
- **Representation of bits**
  means encoding- the type of encoding, i.e., how those zeros and ones are converted into signals.
- **Data rate (Transmission Rate)**
  The number of bits sent each second.
- **Synchronization of bits**
  The clock between the sender and the receiver must also be synchronized.
- **Line Configuration**
  It is about whether "Point to Point" communication or "Point-to-Multipoint" Communication.
  Point-to-Point: only one medium between the 2 nodes.
  Point-to-Multipoint: common channel or a medium is accessed or shared by many nodes.
- **Physical topology**
  How devices are connected to make the network.
- **Transmission Mode**
  Simplex, half duplex and full duplex



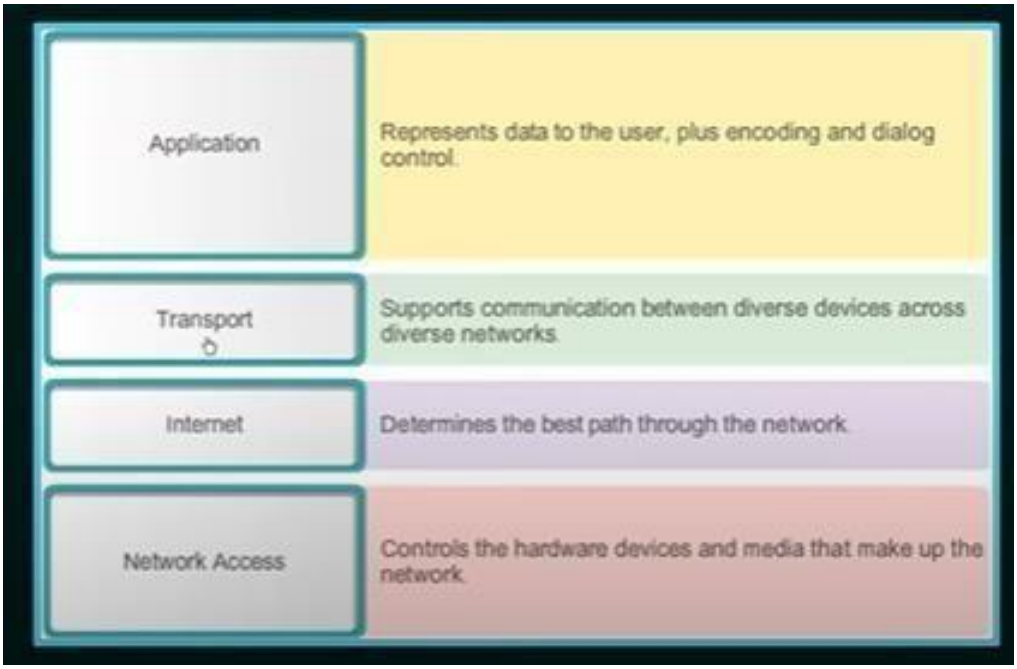
- a, b, c, j and k – port address of those particular processes
- A and P – represented IP Addresses of two nodes
- H2 (Header part) – source and destination MAC Adresses
- T2 (Trailer part) – Error control related part

OSI Reference Model Vs TCP/IP Model

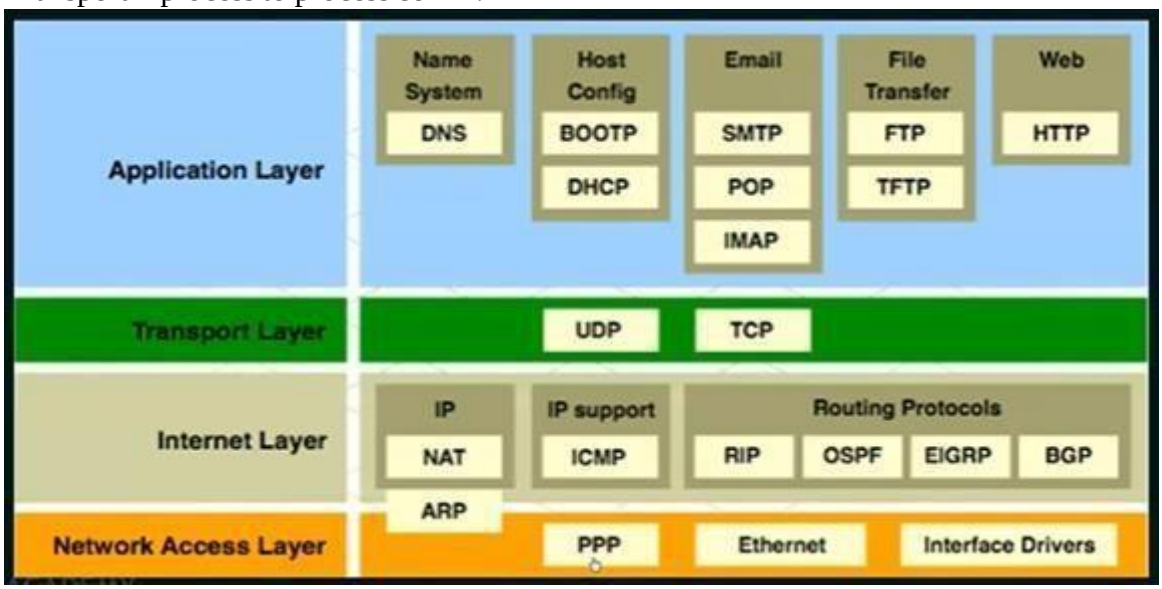


- The TCP/IP model was developed prior to the OSI model.

TCP/IP Model



Transport – process to process comm.



Network Access Layer

PPP – Point to Point Protocol
Ethernet – popular for LAN Technology to be précised for WLAN technology
Interface Drivers – (Physical Layer – Hubs, Cables, Modem, Repeaters & **Data Link Layer –** Bridges, Switch)

Internet Layer

Following are the protocols used in this layer are:

- **IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing**: This protocol implements logical host addresses known as IP addresses.

The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.

- **Host-to-host communication**: It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting**: An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:**
- **Routing:** the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP

ARP stands for Address Resolution Protocol.

- ARP is a network layer protocol which is used to find the physical address from the IP address.

The two terms are mainly associated with the ARP Protocol:

- **ARP request**: When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

- **ARP reply**: Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header.

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
  - **ICMP Test:** ICMP Test is used to test whether the destination is **reachable or not.**
  - **ICMP Reply:** ICMP Reply is used to check whether the destination **device is responding or not**.

Transport Layer

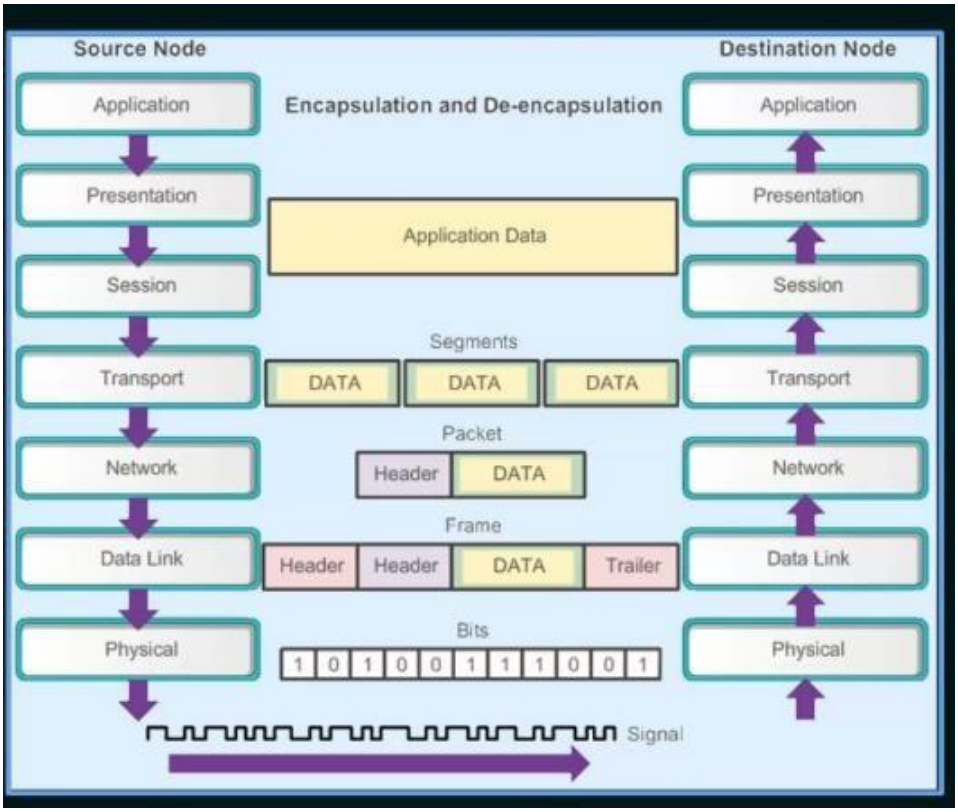
UDP – User Datagram Protocol TCP –Transport Layer Protocol

Any application will use either UDP or TCP

Protocol Data Unit (PDU) – PDUs are named according to the protocols of the TCP/IP suite: data, segment, packet, frame and bits**.**

Application Layer – Data **Transport Layer –** Segment**Network Layer –** Packet **Data Link Layer –** Frame **Physical Layer –** Bits

Physical Layer –Introduction to physical layer



In Transport Layer, if it is a big data, it is broken into smaller pieces and appended with the transport layer header (either UDP or TCP).

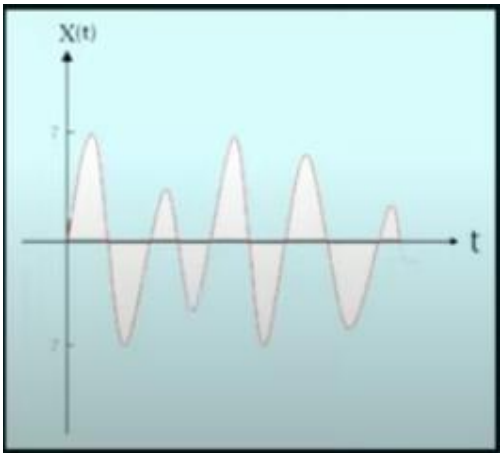
Data and Signals

Signals: It is a function that represents the variation of a physical quantity with respect to time.Two type of signals are Analog Signal and Digital Signal.

Analog signals have continuous electrical signals, while Digital signals have non-continuous electrical signals.

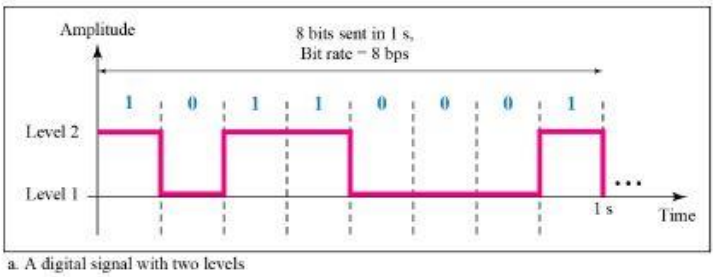
Analog Signal

- It is the signal that can take any value in the defined range.
- All real-life signals are analog in nature.Eg: Human voice
  For example, x(t) can take any value between -7 to +7.

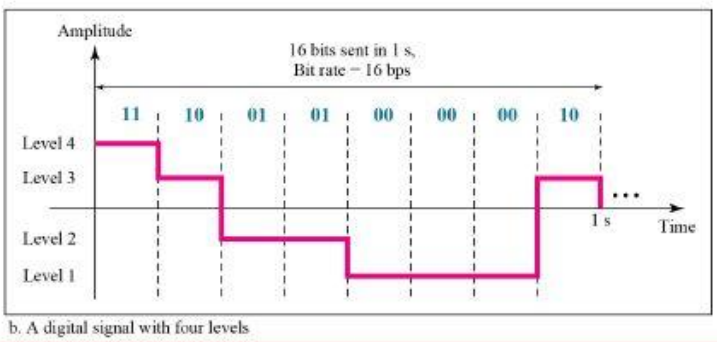


Digital Signal

It is the signal that can take on of the finite values at any given time.In case of digital signals, we discretize both time and magnitude.
Eg: Files in a disc



a. A digital signal with two levels

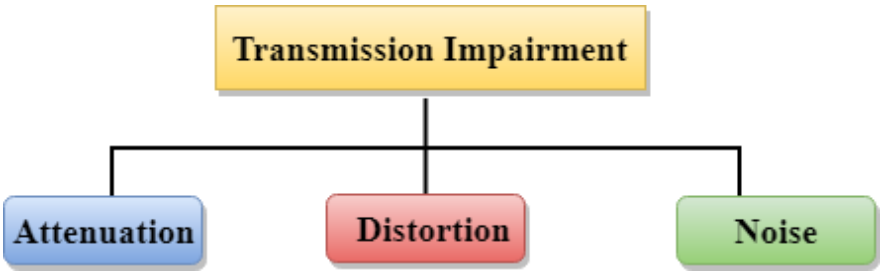


b. A digital signal with four levels

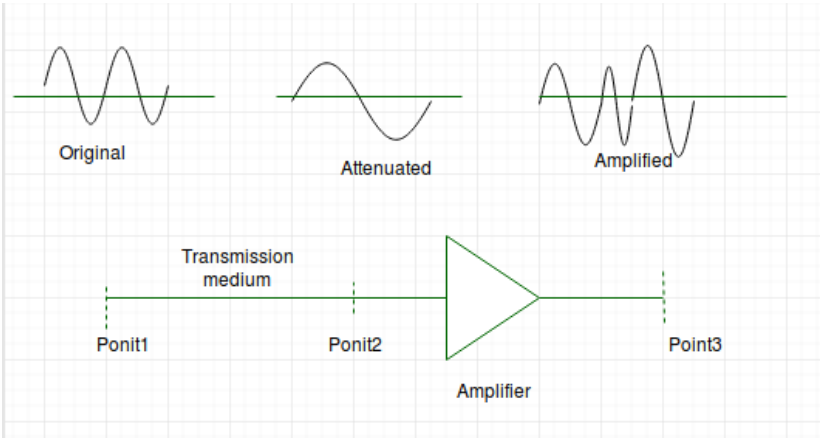
Transmission impairment: When the received signal is not identical to the transmitted one due to the

transmission impairment. The quality of the signals will get destroyed due to transmission impairment.

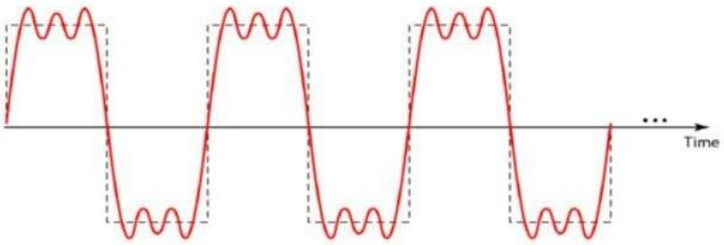
Causes Of Transmission Impairment:



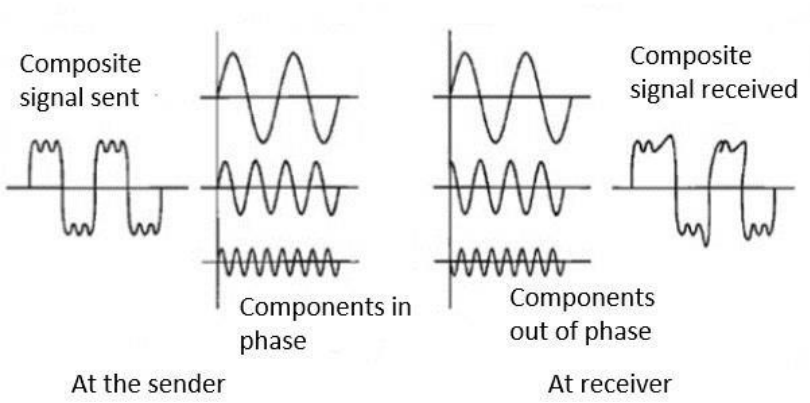
Attenuation – It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back and compensate for this loss.



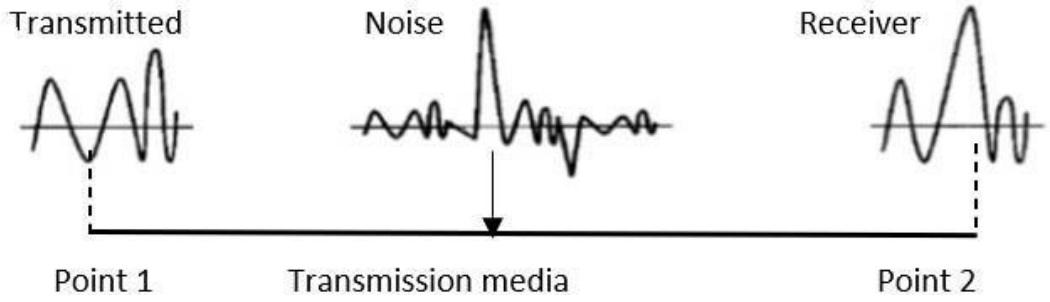
According to Fourier analysis, any composite signal is a combination of simple sine waves with different frequencies, amplitudes, and phases



- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delaydistortion.



- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to itwhich creates the noise.



Data rate refers to the speed of data transfer through a channel. It is generally computed in bits per second (bps). Higher data rates are expressed as Kbps ("Kilo" bits per second, i.e.1000 bps), Mbps ("Mega" bits per second, i.e.1000 Kbps), Gbps ("Giga" bits per second, i.e. 1000 Mbps) and Tbps ("Tera" bits per second, i.e. 1000 Gbps).

One of the main objectives of data communications is to increase the data rate. There are three factors that determine the data rate of a channel:

1. Bandwidth of the channel
2. Number of levels of signals that are used
3. Noise present in the channel

Data rate can be calculated using two theoretical formulae:

- Nyquist Bit Rate – for noiseless channel
- Shannon's Capacity – for noisy channel

For a Noiseless Channel, the Nyquist bit rate formula defines the theoretical maximum bit rate The theoretical formula for the maximum bit rate (the number of bits transferred every second) is:maximum bit rate = $2 \times \text{Bandwidth} \times \log_2 V$

Here, maximum bit rate is calculated in bps

- Bandwidth (the difference between the maximum frequency and the minimum frequency) is the bandwidth of the channel
- V is the number of discrete levels in the signal

For example, if there is a noiseless channel with a bandwidth of 4 KHz that is transmitting a signal with4 discrete levels, then the maximum bit rate will be computed as, maximum bit rate = 2 × 4000 × log24 = 16,000 bps = 16 kbps

Called the Shannon Capacity, to determine the theoretical highest data rate **for a noisy channel**:

Capacity = Bandwidth × $\log_2$(1+SNR)

Here, Capacity is the maximum data rate of the channel in bpsBandwidth is the bandwidth of the channel

SNR is the signal – to – noise ratio

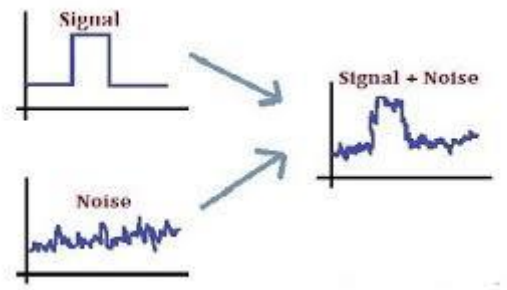
For example, if the bandwidth of a noisy channel is 4 KHz, and the signal to noise ratio is 100, then the maximum bit rate can be computed as:

Capacity = 4000 × log2(1+100) = 26,633 bps = 26.63 kbps

Signal – to – Noise Ratio

SNR is actually the ratio of what is wanted (signal) to what is not wanted (noise). A high SNR means the signal is less corrupted by noise; a low SNR means the signal is more corrupted by noise.

SNR = Avg. Signal power / Avg. Noise power



Performance: The examination and review of collective network information and review of collective network information to describe the quality of services delivered by the underlying computer network is known as "network performance".

Hence, to measure the performance of a network, here are the major factors to be considered:

Transit time: The total time a node takes to transmit a message from the beginning until the last character of the message. Transit stands for Transmission.

Response time: The total time a node takes to process an inquiry or a request from another node/ device and respond. It is the time between the inquiry's end and the response's beginning.

Throughput: Throughput measures how much data is transferred successfully from the sender node to the receiver node in a particular time frame. It is measured in bits per second or data per second.

The Throughput is a measure of how fast we can actually send data through a Network. (Actual amount of data that passes through the medium.)

Bandwidth: The maximum possible throughput capacity of the Network. We can measure it in bits, megabits, or gigabits per second. It defines the highest limit.

The Bandwidth of a Network is given by the no. of bits that can be transmitted over the network in a certain period of time. (Maximum amount of data that can be transmitted per second.)

Bandwidth in bps

Bandwidth = Capability.

Eg: Gigabit Ethernet can provide a bandwidth of 1Gbps.

Bandwidth in Hertz

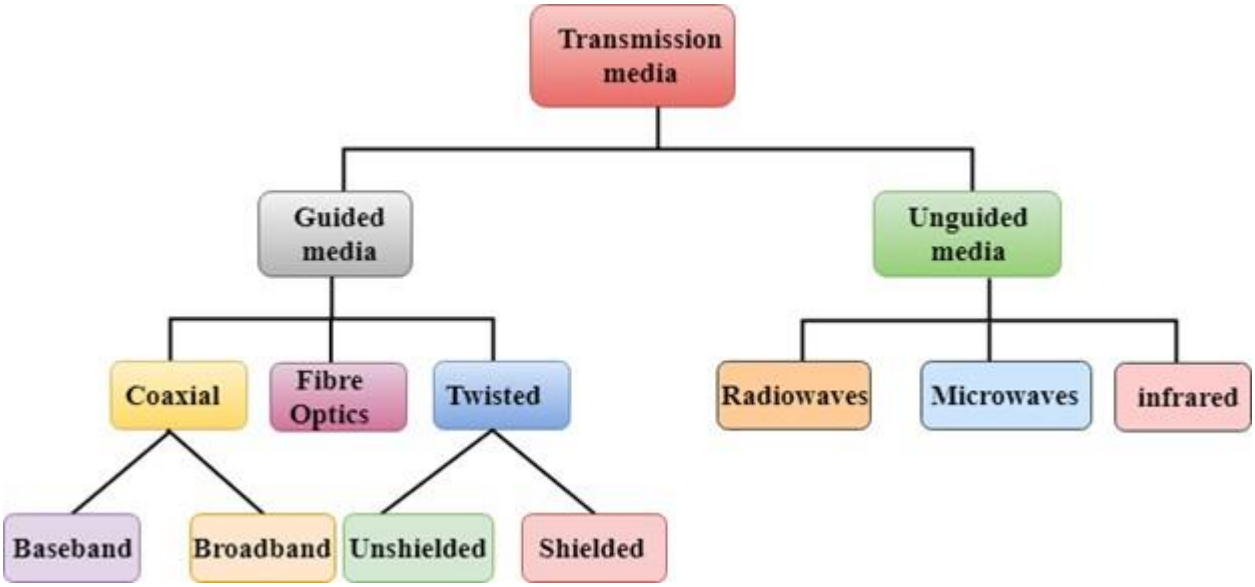
A range of frequencies used to transmit signals which is measured in hertz.

A link may have a bandwidth of 'B' bps, but we can only send 'T' bps through this link with T<B always.

Delay/ Latency: As we discussed, Throughput is the number of data packets successfully delivered in a given time. Delay is the measure of time taken to do the delivery.

The Latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

Introduction to Guided Media Classification Of Transmission Media:



Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

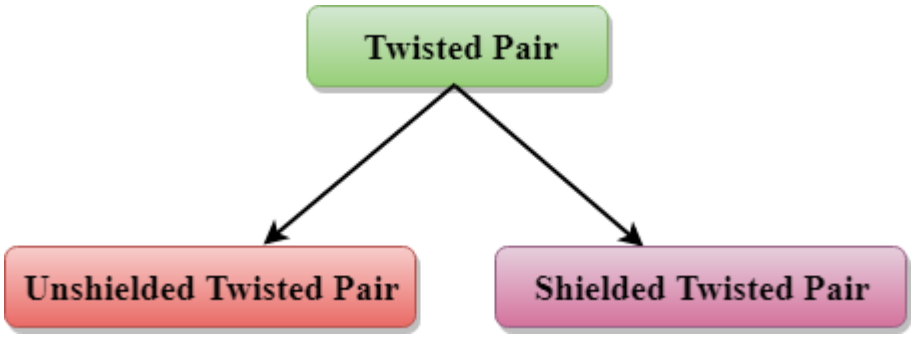
- High Speed
- Secure
- Used for comparatively shorter distances

Types Of Guided media:

Twisted pair: Copper wires are the most common wires used for transmitting signals because of good performance at low costs. They are most commonly used in telephone lines. However, **if two or more**

wires are lying together, they can interfere with each other's signals. To reduce this electromagnetic interference, pair of copper wires are twisted together in helical shape like a DNA molecule. Such twisted copper wires are called twisted pair. To reduce interference between nearby twisted pairs, the twist rates are different for each pair.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.



UTP is an **unshielded twisted pair** cable used in computer and telecommunications mediums. Its frequency range is suitable for transmitting both data and voice via a UTP cable. Therefore, it is widely used in the telephone, computers, etc. It is a pair of insulated copper wires twisted together to reduce noise generated by external interference. It is a wire with no additional shielding, like aluminium foil, to protect its data from the exterior.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.
- Lower capacity and performance in comparison to STP

A **shielded twisted pair** is a type of twisted pair cable that contains an extra wrapping foil or copper braid jacket to protect the cable from defects like cuts, losing bandwidth, noise, and signal to the interference. It is a cable that is usually used underground, and therefore it is costly than UTP. It supports the higher data transmission rates across the long distance. We can also say it is a cable with metal sheath or coating that surround each pair of the insulated conductor to protect the wire from external users and prevent electromagnetic noise from penetrating.

Advantages of the STP cable

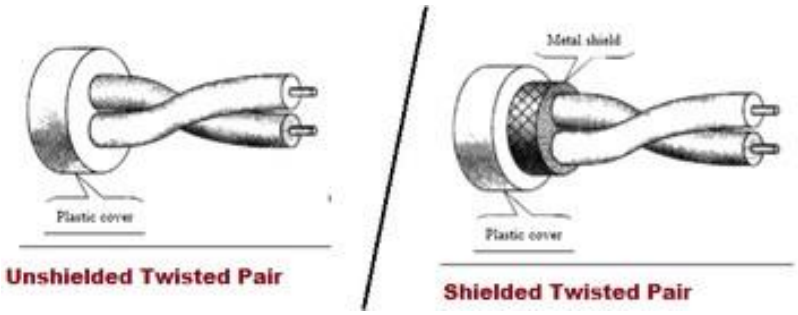
- It has lower noise and attenuation than UTP.
- It is shielded with a plastic cover that protects the STP cable from a harsh environment and

increases the data transmission rate.

- It reduces the chances of crosstalk and protects from external interference.

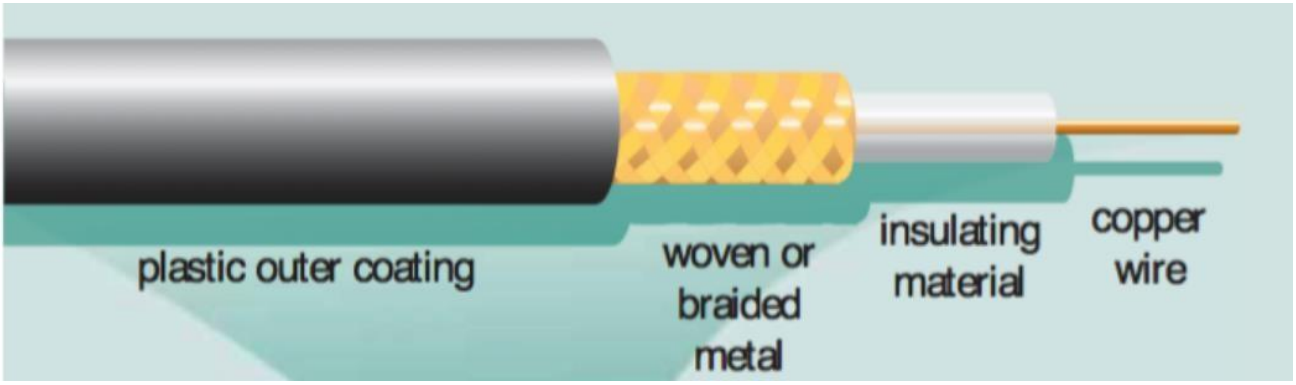
Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.



Coaxial cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- It consists of a single copper wire surrounded by at least three layers: (1) an insulating material, (2) a woven or braided metal, and (3) a plastic outer coating



Coaxial cable is of two types:

- **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
- **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

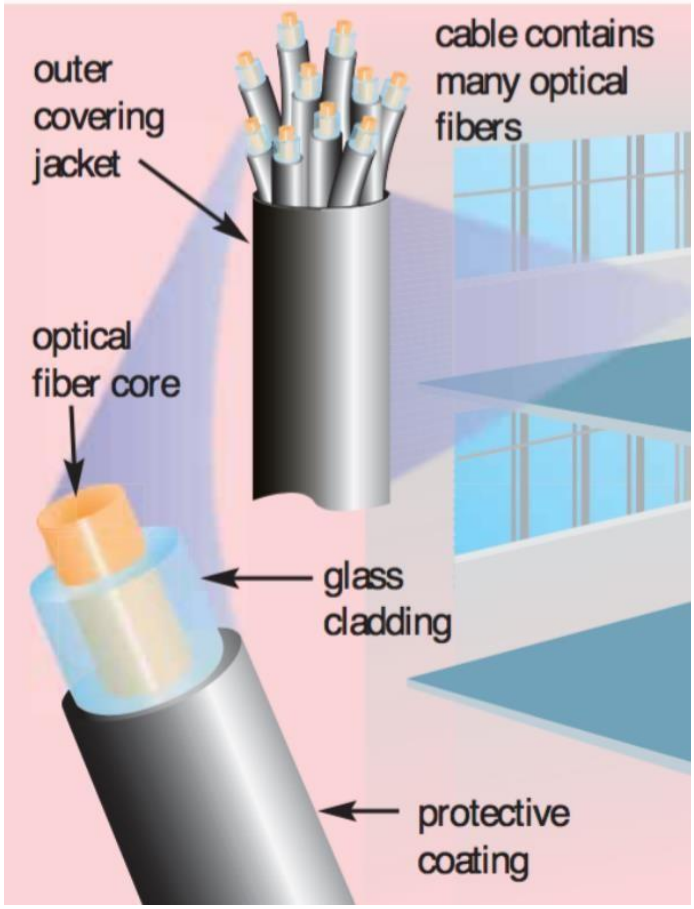
Disadvantages Of Coaxial cable:

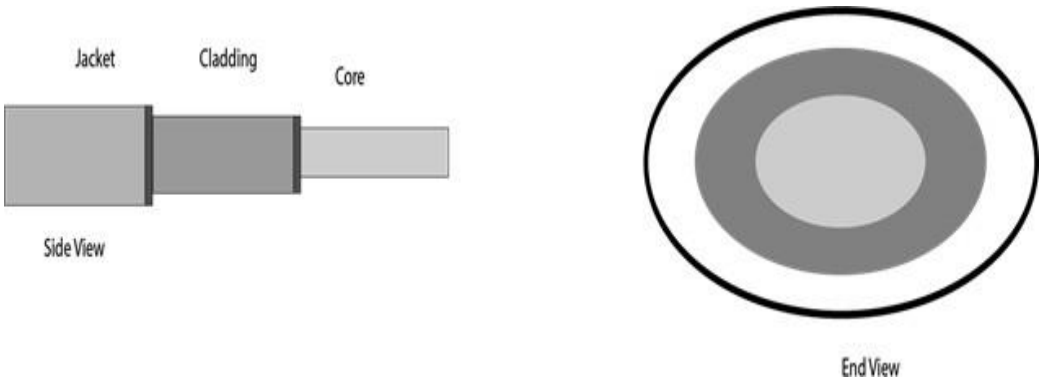
- It is more expensive as compared to twisted pair cable.

- If any fault occurs in the cable causes the failure in the entire network.

Fibre-Optic cable

The core of a fiber-optic cable consists of dozens or hundreds of thin strands of glass or plastic that use light to transmit signals. Each strand, called an optical fiber, is as thin as a human hair. Inside the fiber-optic cable, an insu- lating glass cladding and a protective coating surround each optical fiber (Figure 8-26).





- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core isa light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.

- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Advantages

- Capability of carrying significantly more signals than wire cables
- Faster data transmission
- Less susceptible to noise (interference) from other devices such as a copy machine
- Better security for signals during transmission because they are less susceptible to noise
- Smaller size (much thinner and lighter weight)

Disadvantages

Fiber-optic cables are it costs more than twisted-pair or coaxial cable and can be difficult to install and modify.

Unguided Media:

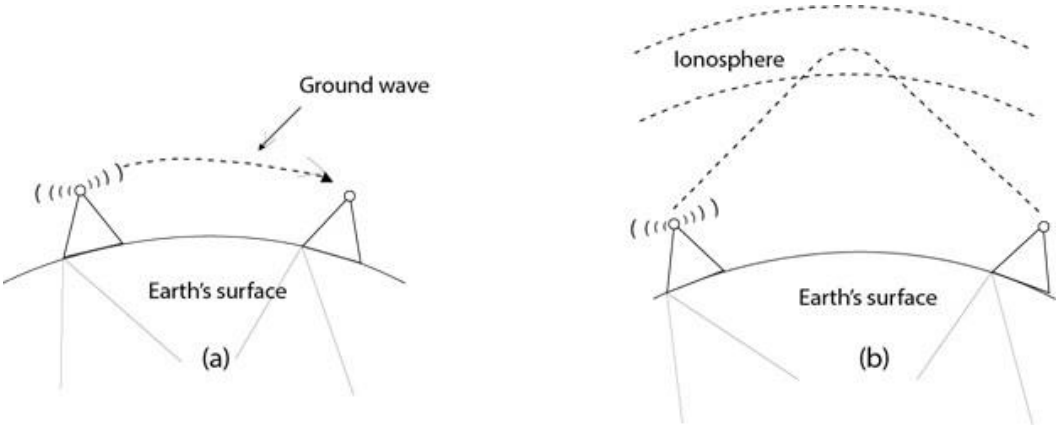
Wave: It is a transfer of energy, usually through a form of matter called a Medium.

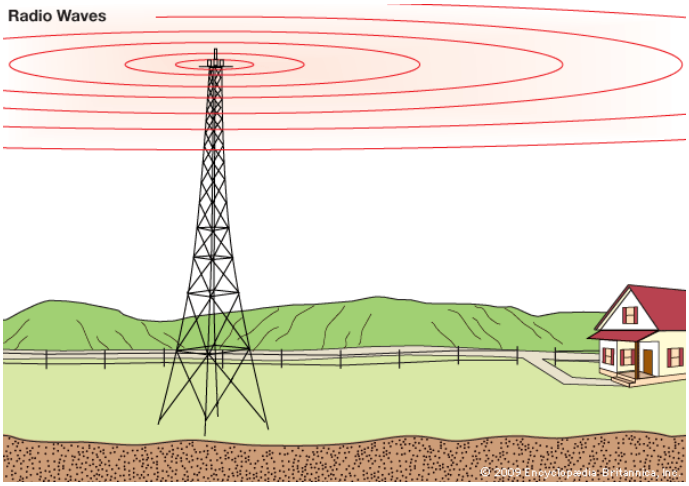
There is a special type of wave that can travel without a medium, called Electromagnetic Waves (EM Waves), which are waves like Radio Waves, Microwaves.

Electromagnetic waves are formed when an **electric field** comes in contact with a **magnetic field.** They are hence known as EM Waves.

Radio Waves:

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.





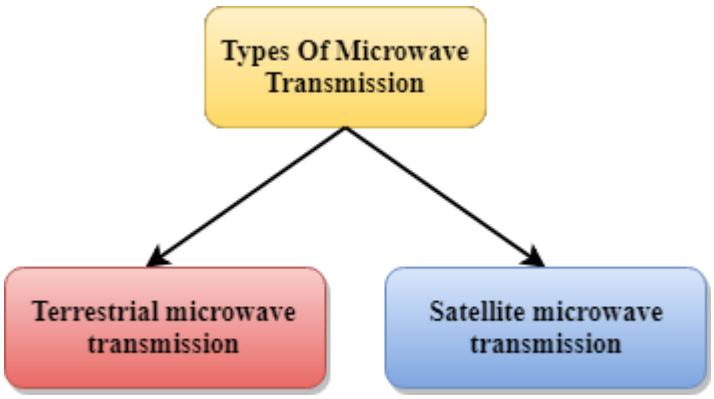
Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

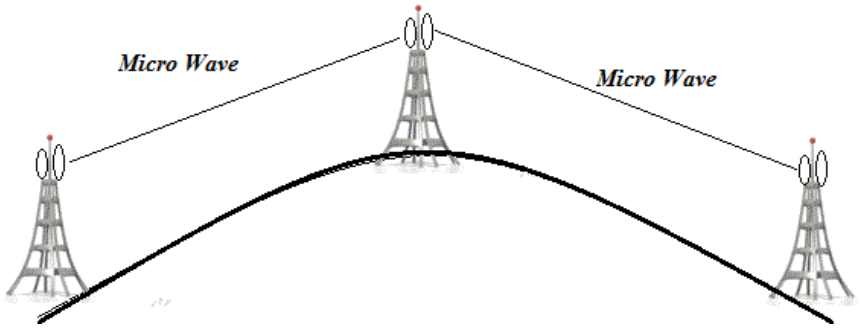
- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves



Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.



Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

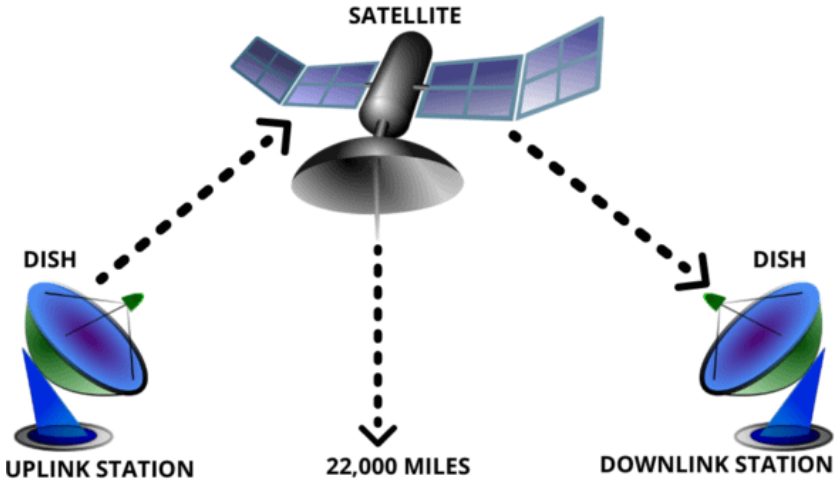
Disadvantages of Microwave transmission:

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.

- **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.



How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.

- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

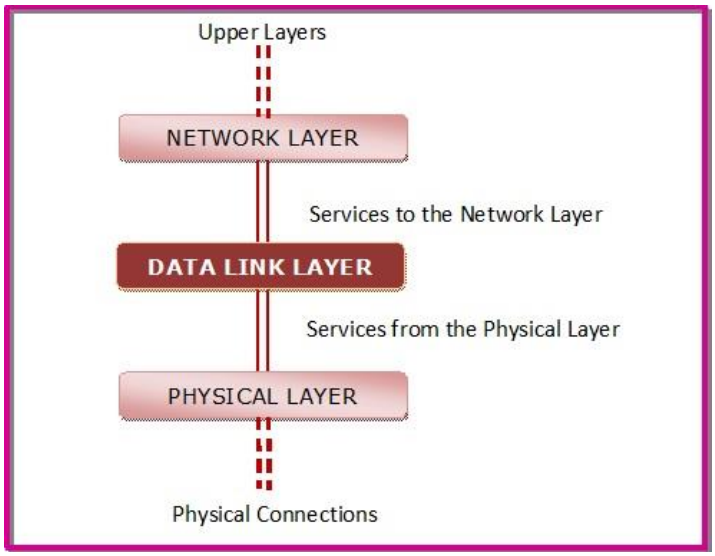
Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Data Link Layer

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.

The primary function of the data link layer is to provide a well-defined service interface to the network layer above it.

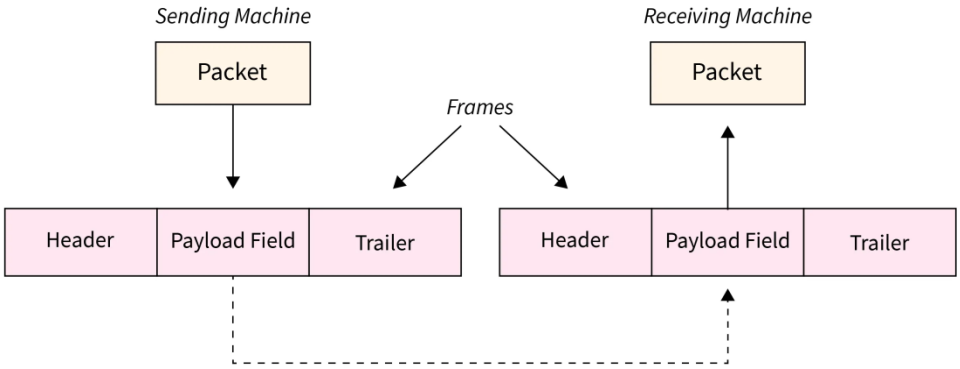


Data Link Layer Design Issues

Physical layer delivers bits of information to and from data link layer. The **functions of Data Link Layer** are:

1. Providing a well-defined service interface to the network layer.
2. Dealing with transmission errors.
3. Regulating the flow of data so that slow receivers are not swamped by fast senders.

   To accomplish these goals, the data link layer **takes the packets from the Network Layer** and **encapsulates them into frames** for transmission.



Each frame contains a frame header for storing the information of Source Address, Destination Address, a payload field for holding the packet, and a frame trailer for Error Detection and Correction.

Design Issues of Data Link Layer

1. Services Providing services to the network layer

2. Framing
3. Error Control
4. Flow Control

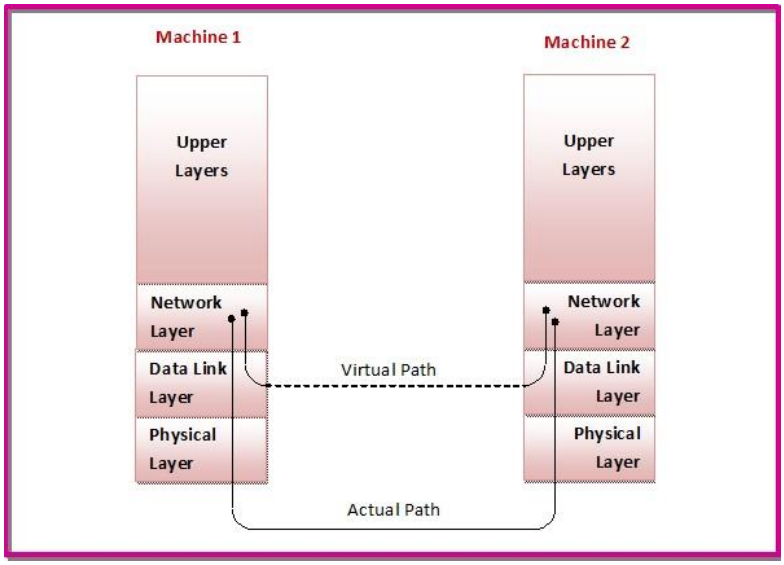
1. Services Providing services to the network layer

Virtual Communication versus Actual Communication

The main service provided is to transfer data packets from the network layer on the sending machine to the network layer on the receiving machine. Data link layer of the sending machine transmits accepts data from the network layer and sends them to the data link layer of the destination machine which hands them to the network layer there.

In actual communication, the data link layer transmits bits via the physical layers and physical medium. However virtually, this can be visualized as the two data link layers communicating with each other using a data link protocol.

The processes are depicted in the following diagram −



Types of Services

The data link layer offers three types of services.

Unacknowledged connectionless service − Here, the data link layer of the sending machine sends independent frames to the data link layer of the receiving machine. **The receiving machine does not acknowledge receiving the frame**. **No logical connection is set up between the host machines**. Error and data loss is not handled in this service. This is applicable in Ethernet services and voice communications.

Acknowledged connectionless service − Here, **no logical connection is set up between the host machines, but each frame sent by the source machine is acknowledged by the destination machine** on receiving. If the source does not receive the acknowledgment within a stipulated time, then it resends the frame. This is used in Wifi (IEEE 802.11) services.

Acknowledged connection-oriented service − This is the best service that the data link layer can offer to the network layer. A logical connection is set up between the two machines and the data is

transmitted along this logical path. The frames are numbered, that keeps track of loss of frames and also ensures that frames are received in correct order.

2. Framing:

- To provide service to the network layer the data link layer must use the service provided to it by physical layer.
- Stream of data bits provided to data link layer by the Physical Layer is not guaranteed to be without errors.
- Some bits may have different values and the number of bits received may be less than, equal to, or more than the number of bits transmitted. It is up to the data link layer to detect and, if necessary, correct errors.
- The usual approach is for the data link layer to break up the bit stream into discrete frames, compute a short token called a checksum for each frame, and include the checksum in the frame when it is transmitted.
- When a frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it.

Types of Framing

1. Fixed Length Framing

- Here the size of the frame is fixed and so the frame length acts as delimiter of the frame.
- Consequently, it doesn't require additional boundary bits to identify the start and end of the frame.
- Eg: 200 bits of data to be transmitted

  20 X 10 frames = 200 bits

2. Variable-size Framing

- Here, the size of each frame to be transmitted may be different.
- So the additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

Methods of Framing:

1. Byte count (Character Count)
2. Flag bytes with byte stuffing.
3. Flag bits with bit stuffing.
4. Physical layer coding violations.

Byte count (Character Count)

The first framing method uses a field in the header to specify the number of bytes in the frame. When the data link layer at the destination sees the byte count, it knows how many bytes follow and hence where the end of the frame is. This technique is shown in Fig. 3-3(a) for four small example frames of sizes 5, 5, 8, and 8 bytes, respectively.

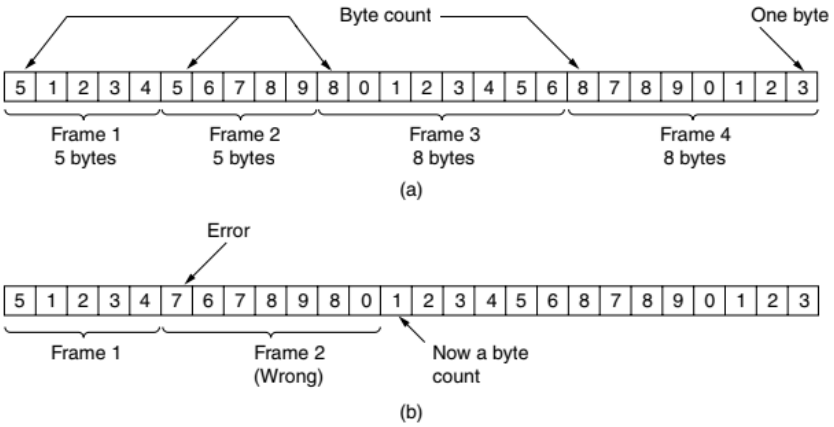


Figure 3-3. A byte stream. (a) Without errors. (b) With one error.

The trouble with this algorithm is that the count can be garbled by a transmission error. For example, if the byte count of 5 in the second frame of Fig. 3-3(b) becomes a 7 due to a single bit flip, the destination will get out of synchronization. Even if the checksum is incorrect so the destination knows that the frame is bad.

Flag bytes with byte stuffing

This methods gets around the boundary detection of the frame by having each appended by the frame start and frame end special bytes. If they are the same (beginning and ending byte in the frame) they are called flag byte. This byte is shown in Fig. 3-4(a) as FLAG.

However, there is a still a problem we have to solve. It may happen that the flag byte occurs in the data, especially when binary data such as photographs or songs are being transmitted. One way to solve this problem is to have the sender's data link layer insert a special escape byte (ESC) just before each ''accidental'' flag byte in the data.

The data link layer on the receiving end removes the escape bytes before giving the data to the network layer. This technique is called byte stuffing. If an escape byte occurs in the middle of the data, it too, is stuffed with an escape byte.

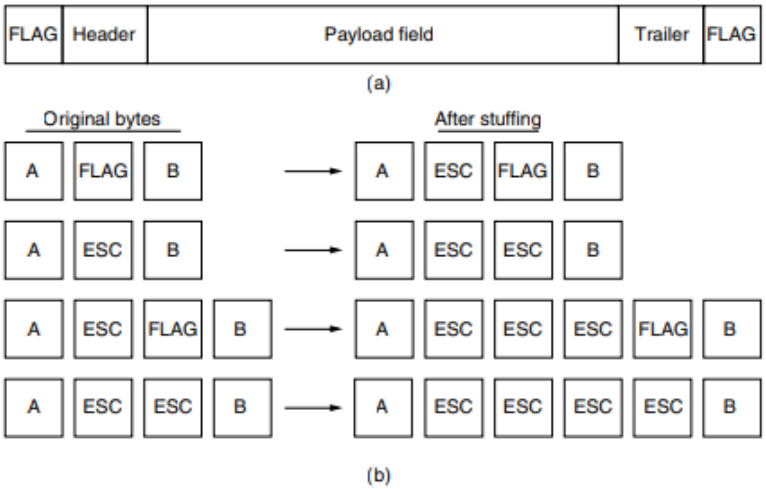


Figure 3-4. (a) A frame delimited by flag bytes. (b) Four examples of byte sequences before and after byte stuffing.

Flag bits with bit stuffing

This method achieves the same thing as Byte Stuffing method by using Bits (1) instead of Bytes (8 Bits). It was developed for High-level Data Link Control (HDLC) protocol. Each frame begins and ends with a special bit pattern, 01111110 or 0x7E in hexadecimal. This pattern is a flag byte. Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit. If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110. Figure 3-5 gives an example of bit stuffing.

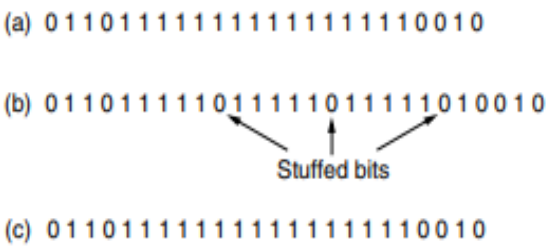


Figure 3-5. Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

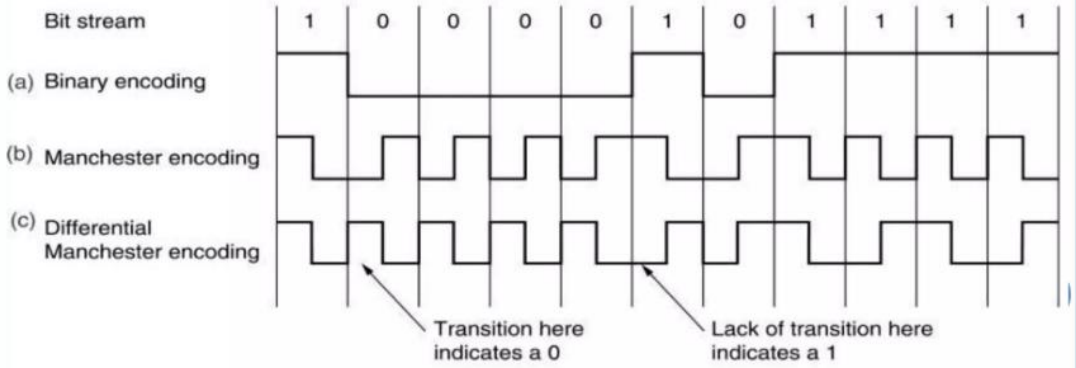
Physical layer coding violations

The last method of framing is only applicable to networks in which the encoding on the physical medium contains some redundancy. For Example, some LANs encode 1 bit of data using 2 physical bits. Normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair.

The combinations of high-high and low-low are not used for data but are used for delimiting frames in some protocols.

PHYSICAL LAYER CODING VIOLATIONS

- This Framing Method is used only in those networks in which Encoding on the Physical Medium contains some redundancy.
- Some **LANs** encode each bit of data by using two Physical Bits i.e. Manchester coding is Used. Here, Bit **1** is encoded into high-low(10) pair and Bit **0** is encoded into low-high(01) pair.
- The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries. The combinations high-high and low-low are not used for data but are used for delimiting frames in some protocols.

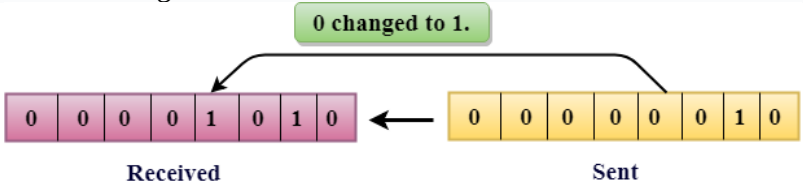


3. Error Control:

- Error Control is a **combination of both error detection and error correction**. It ensures that the data received at the receiver end is the same as the one sent by the sender.
- Error detection is the process by which the receiver informs the sender about any erroneous frame (damaged or lost) sent during transmission.
- DLL follows the technique ARQ (Automatic Repeat Request) to detect an error and take action i.e. retransmit the frame.
- **Phases in Error Control**:
  - Detection of Error
  - Acknowledgment
    - Positive Acknowledgment
    - Negative Acknowledgment
  - Retransmission
- Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal; leads to an error in data transmission.
- **Types of Errors**

i. Single-Bit Error

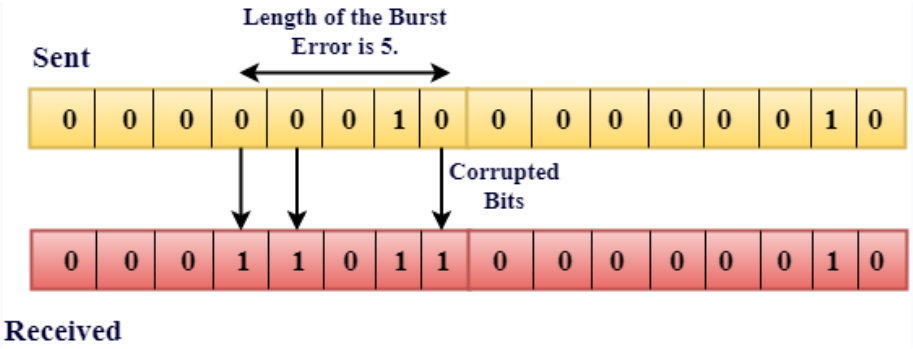
The term single-bit error means that only one bit of a given data unit (such as a byte, character, data unit, or packet) is changed from 1 to 0 or from 0 to I. In a single-bit error, only one bit in the data unit has changed.



In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

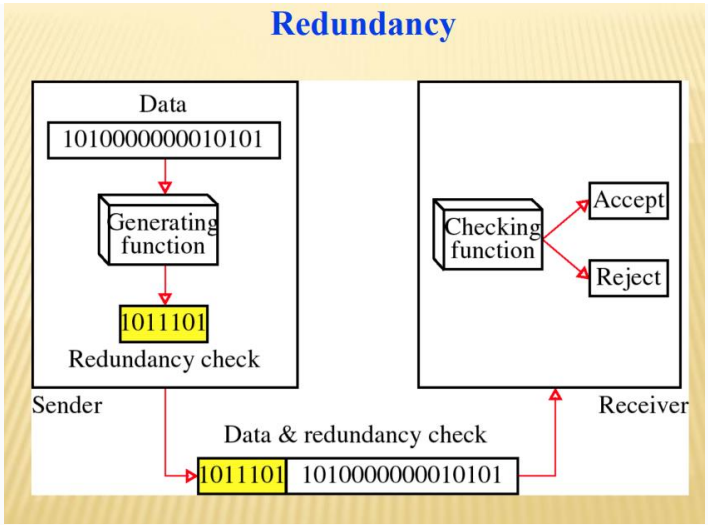
ii. Burst Error

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.
The Burst Error is determined from the first corrupted bit to the last corrupted bit.



Redundancy Error Detection:

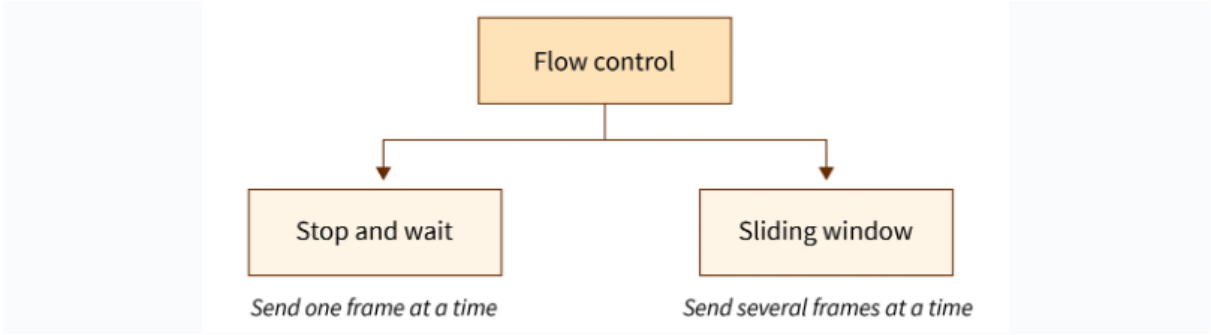
One error detection mechanism that would appends extra bits for detecting errors at the destination.



4. Flow control

It is a set of procedures that restrict the amount of data a sender should send before it waits for some acknowledgment from the receiver.

- Flow Control is an essential function of the data link layer.
- It determines the amount of data that a sender can send.
- It makes the sender wait until an acknowledgment is received from the receiver's end.
- Methods of Flow Control are Stop-and-wait, and Sliding window.

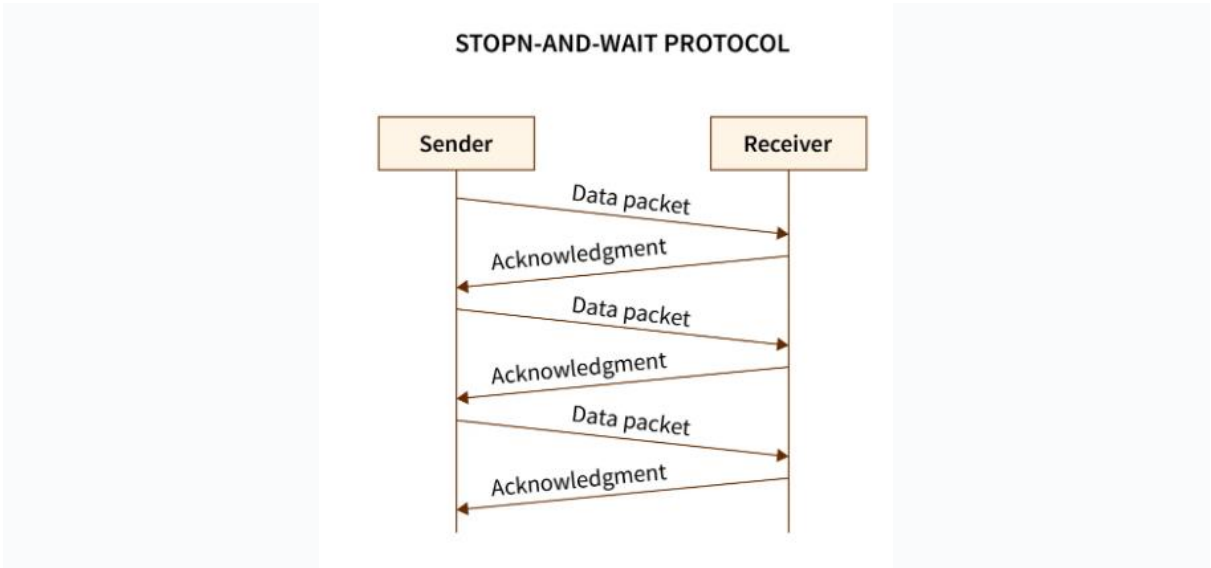


Stop-and-wait Protocol

Stop-and-wait protocol works under the assumption that the communication channel is **noiseless** and transmissions are **error-free**.

Working:

- The sender sends data to the receiver.
- The sender stops and waits for the acknowledgment.
- The receiver receives the data and processes it.
- The receiver sends an acknowledgment for the above data to the sender.
- The sender sends data to the receiver after receiving the acknowledgment of previously sent data.
- The process is unidirectional and continues until the sender sends the **End of Transmission (EoT)** frame.



Sliding Window Protocol

The sliding window protocol is the **flow control protocol** for noisy channels that allows the sender to send multiple frames even before acknowledgments are received. It is called a **Sliding window** because the sender slides its window upon receiving the acknowledgments for the sent frames.

Two peers in the network maintain a buffer of frames sent across the network. Sending multiple frames simultaneously is the task, and the sliding window is the technique to be followed while sending each of the frames. Once the receiver has received a frame, an acknowledgement is sent to the sender of the frame to process for the other frame in the buffer array of frames. Multiple frames can be transmitted from sender to receiver without needing to have an acknowledgement. The sliding window is just a

drawn up name to refer to the frame holding capacity at both ends. It does make use of transmission control protocol.

Working:

- The sender and receiver have a "window" of frames. A window is a space that consists of multiple bytes. The size of the window on the receiver side is always 1.
- The sliding window mentions the criteria for several frames that can be sent until being acknowledged by the receiver.
- Frames will get acknowledged even when the window is not filled up on the receiver side.
- Frames can be transferred from the senders' side without the need to be filled up.
- The frames are numbered modulo-n which signifies the size of the window. If n is the window size, the frames are numbered from 0 to n-1
- The receiver also sends the number of expected frames to receive along with every acknowledgement. When an acknowledgement is being sent with the number 8, all 7 frames have been received, and the 8th one is to be acknowledged. This concept of acknowledgement being sent is termed **piggybacking**.

Let us look at both sender's side and receiver's size functionalities.

Sender side

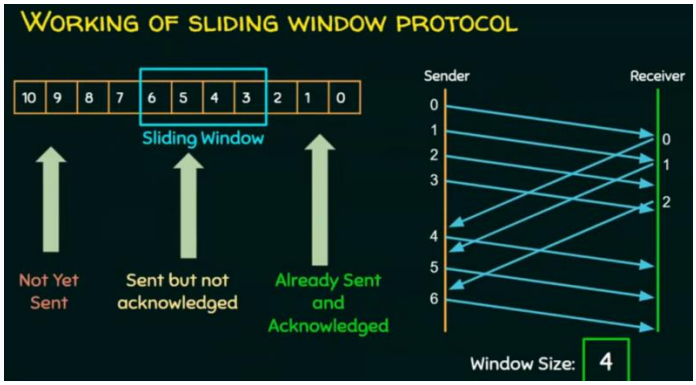
- The sender window maintains a well-sized array to sequentially attack identity to each frame.
- For k bits being allowed by the frame's header, the sequence number lies between 0 to 2k-1.

Receiver side

The receiver window size is always kept at one. The receiver can receive all n frames one by one and send an acknowledgement to all of them.

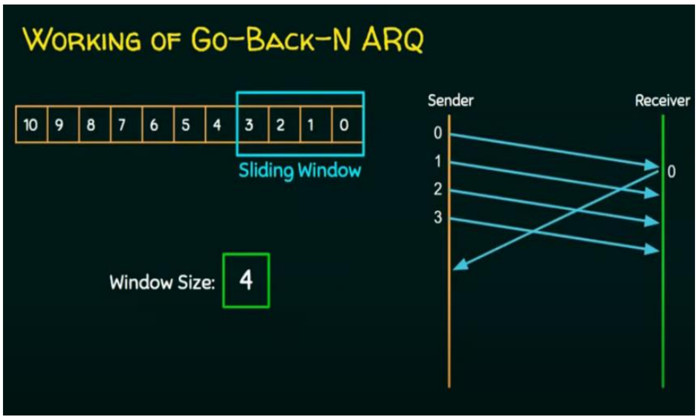
When received 1,2 frames, the window will hold on to acknowledgement frame 3 until it arrives, then the receiver will send this acknowledgement to the sender to confirm that all three frames have been received. This way, the sender gets to know which frame to send next.

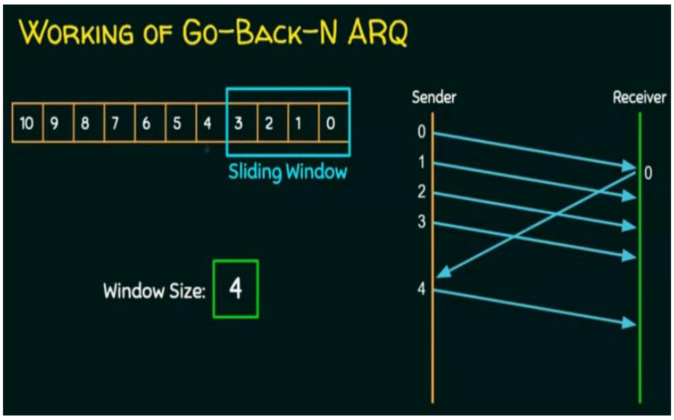
- Each frame is sequentially numbered from 0 to n - 1, where n is the window size at the sender side.
- The sender sends as many frames as would fit in a window.
- After receiving the desired number of frames, the receiver sends an acknowledgment. The acknowledgment (ACK) includes the number of the next expected frame.

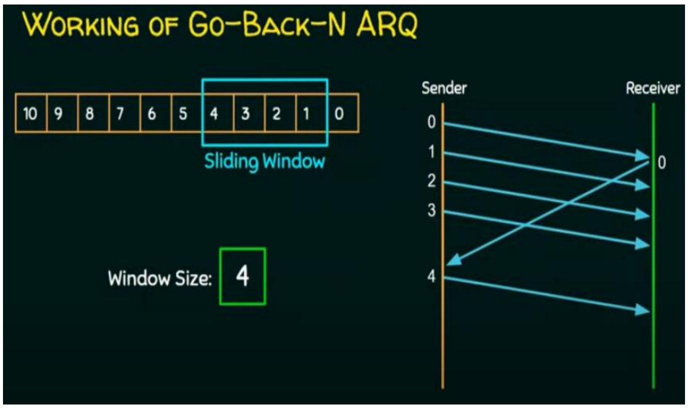


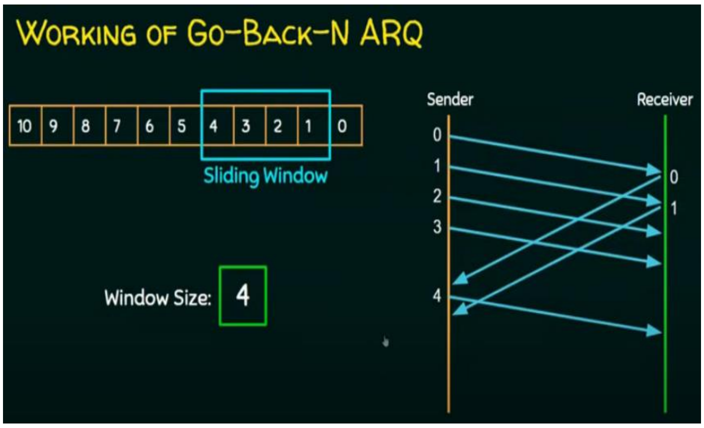
Go Back-N ARQ

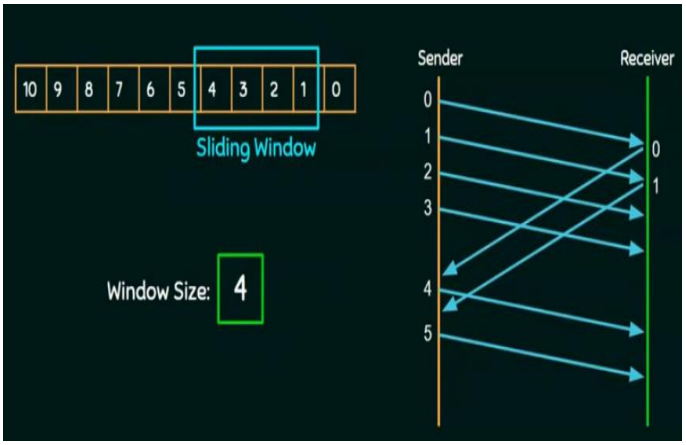
- **'N'** is the sender window size.
- **Go Back-N ARQ** uses the concept of protocol pipelining i.e. the sender can send multiple frames before receiving the acknowledgment for the first frame.
- There are finite number of frames and the frames are numbered in a sequential manner.
- The number of frames that can be sent depends on the window size of the sender.
- If the acknowledgment of a frame is not received within an agreed upon time period, **all frames in the current window are transmitted.**
- The size of the sending window determines the sequence number of the outbound frames.
- For example, if the sending window size (i.e. **'N'**) is 4 (2^2), then the sequence numbers will be 0,1,2,3,0,1,2,3,0,1 and so on.
- The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

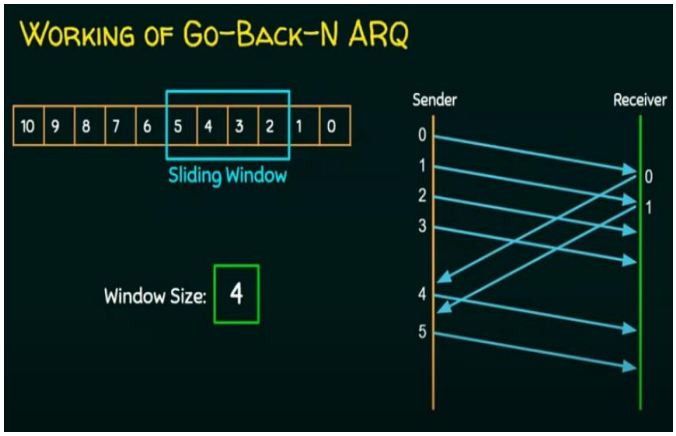


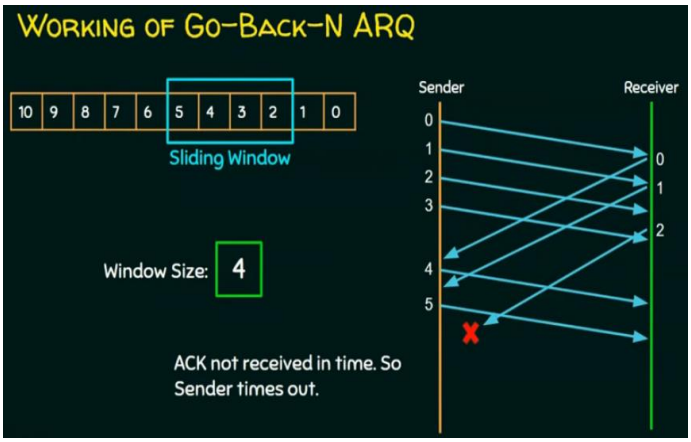


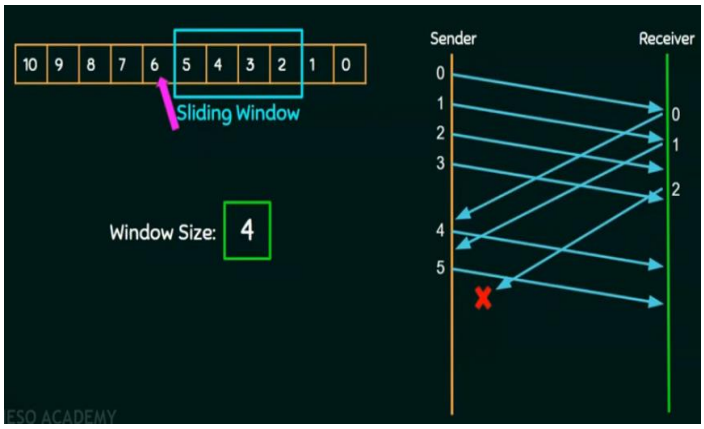


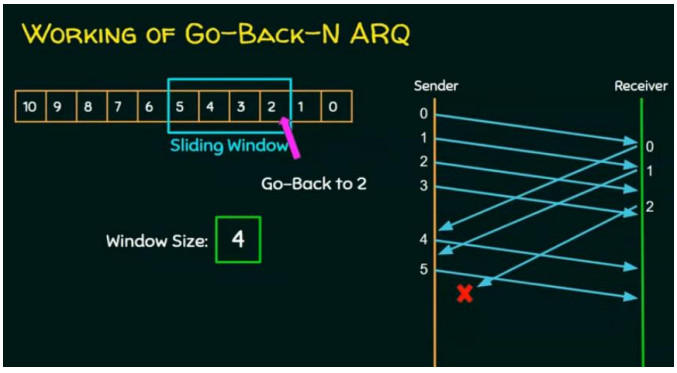



10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0 1 2 3 4 5
0 1


Working of Go-Back-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0 1 2 3 4 5
0 1


Working of Go-Back-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
ACK not received in time. So
Sender times out.
Sender
Receiver
0 1 2 3 4 5
0 1 2


10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0 1 2 3 4 5
0 1 2


Working of Go-Back-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Go-Back to 2
Window Size: 4
Sender
Receiver
0 1 2 3 4 5
0 1 2


Working of Go-Back-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Go-Back to 2
Window Size: 4
Sender
Receiver
0 1 2 3 4 5 2 3 4 5
0 1 2


Working of Go-Back-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Go-Back to 2
Window Size: 4
Sender
Receiver
0 1 2 3 4 5 2 3 4 5
0 1 2

Error Detection and Correction

Errors are introduced into the binary data transmitted from the sender to the receiver due to noise during transmission. The error can be a single-bit error, multi-bit error, or burst error.

Error detection methods are used to check whether the receiver has received correct data or corrupted data. And error correction is used to correct the detected errors during the transmission of data from sender to receiver.

When the information received at the receiver end does not match the sent data. At the time of transmission, errors are introduced into the binary data sent from the sender to the receiver due to noise during transmission. This means that a bit having a 0 value can change to 1 and a bit having a 1 value can change to 0.

Error Detection:

It means to decide whether the received data is correct or not without having a copy of the original message.

To detect or correct errors, we need to send some extra bits with the data. The extra bits are called as redundant bits.

Error Correction:

- Receiver can have the sender retransmit the entire data unit.
- The Receiver can use an error-correcting code, which automatically corrects certain errors.

Error Detecting Codes:

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

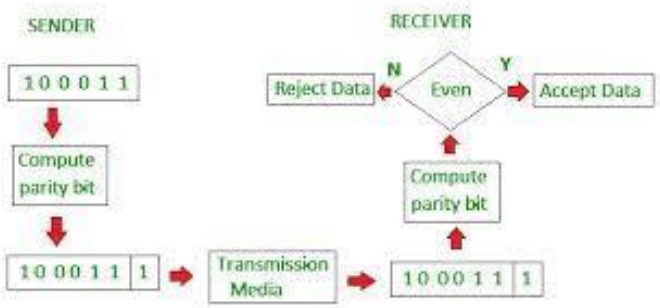
Three different error-detecting codes

1. Parity
2. Checksums
3. Cyclic Redundancy Checks (CRCs)

1. Parity Check

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.

- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking



2. Checksum at Sender Side

- Checksum is used for error detection.
- Checksum is the redundant bits that are attached with actual data.
- Sometimes, a Checksum is also considered as a hash sum or hash value.
- On the sender's side, this method uses a checksum generator to generate a Checksum. On the receiving end, a checksum checker is used to validate whether the correct data is received.
- Checksum is an error detection algorithm that can be applied to any length message.
- Checksum provides information to the receiver about the transmission to ensure that the full range of data is delivered successfully.

Note :
The Checksum is an error detection algorithm that appends redundant bits in a message for error detection and can work on any message length.

Working: The sender divides data into blocks of equal size and then adds the data of every block 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.

At sender side steps of generation of the Checksum are given below :

Step 1 :
First of all, break the given data into "k" an equal number of blocks, i.e., "N" bits in all the "K" blocks of the message.
Step 2 :
Perform addition of all the "k" divisions
Step 3 :
If there is a carry bit, add it.
Step 4 :

Now find the 1's complement of the sum. For finding 1's complement of any binary number, just replace every zero with one and replace everyone with zero(e.g., 10001 - 1's Complement 01110) This complemented sum is known as Checksum.

Step 5 :

Checksum is appended to the message to be sent to the receiver.

Now the data appended with Checksum is ready to send.

Checksum at Receiver Side

The receiver receives data
Checksum and passes it to the checksum validator. The following steps are used to validate the Checksum at the receiver end.

Step 1 :

Perform addition on all "K" data blocks

Step 2 :

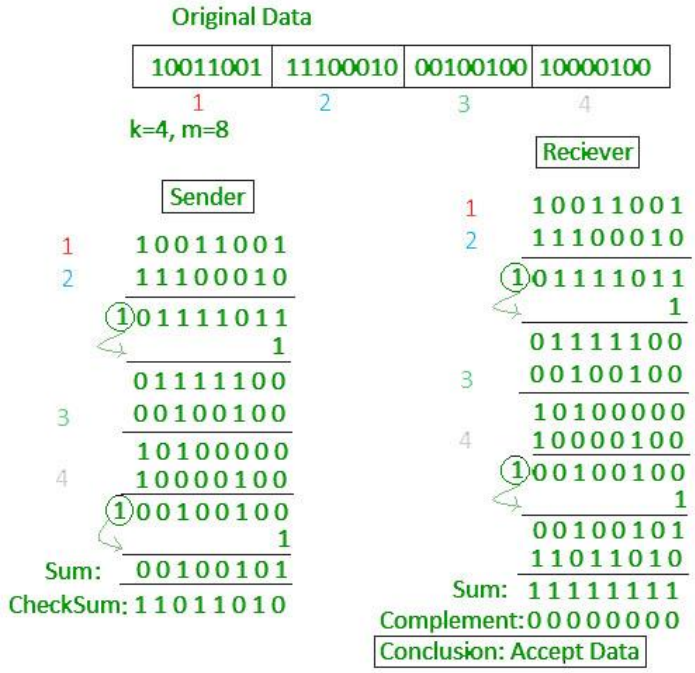
If there is a carry bit, add it.

Step 3 :

Find the 1's complement of the sum.

Step 4 :

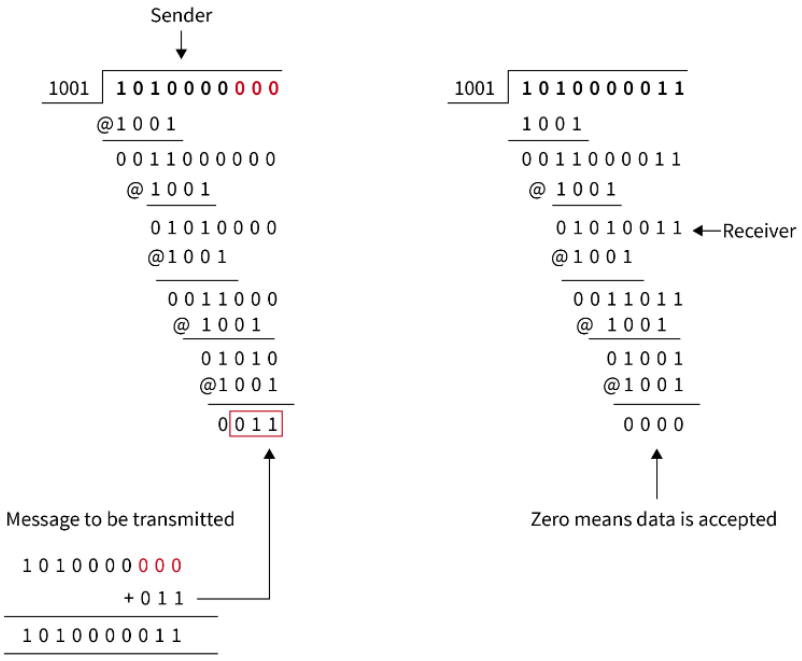
If we got a result that contains only 0, then ACCEPT the data, otherwise, REJECT the data.



3. Cyclic Redundancy Checks (CRCs)

- Given a k-bit frame or message, the transmitter generates an n-bit sequence, known as a frame check sequence (FCS), so that the resulting frame, consisting of (k+n) bits, is exactly divisible by some predetermined number.
- The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error.
- The receiving data units on the receiver's side need to be divided by the same number. These data units are accepted and found to be correct only on the condition of the remainder of this

division is zero. The remainder shows that the data is not correct. So, they need to be discarded.



Error Correcting Codes

Hamming codes

- It can be applied to data units of any length
- It is used to detect and correct Single Bit errors.
- In this coding method, the source encodes the message by inserting redundant bits within the message. These redundant bits are extra bits that are generated and inserted at specific positions in the message itself to enable error detection and correction. When the destination receives this message, it performs recalculations to detect errors and find the bit position that has error.

Hamming Code Structure

The bits that are powers of 2 (1, 2, 4, 8, 16, etc.) are check bits. The rest (3, 5, 6, 7, 9, etc.) are filled up with the m data bits.

D 7	D 6	D 5	P 4	D 3	P 2	P 1

Determine the value of Parity Bits

Rule: The value of parity bit is determined by the Sequence of bits that is alternatively **checks and skips.**

Ex: The sender's data is 1101

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

For P1: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit,….

(1, 3, 5, 7, 9, …)

For P2: check 2 bit, skip 2 bit, check 2 bit, skip 2 bit,….

(2, 3, 6, 7, 10, 11 …)

For P4: check 4 bit, skip 4 bit, check 4 bit, skip 4 bit,….

(4, 5, 6, 7, 12, 13, 14, 15, …)

P1 D3 D5 D7 **P1** 1 0 1 **P1=0**	**P2 D3 D6 D7** **P2** 1 1 1 **P2=1**	**P4 D5 D6 D7** **P4** 0 1 1 **P4=0**

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

Detecting Error:

Consider a 7bit Hamming Code: D7 D6 D5 P4 D3 P2 P1

At receiver end, bits are (1,3,5,7), (2,3,6,7) and (4,5,6,7) are checked for even parity.

Ex: P1=0, P2=0, P3 =0, then there are no errors.

Problem: A 7 bit Hamming Code is received as 1011011. Assume even parity and state whether the received code is correct or wrong, if wrong locate the bit in error.

s	D 6	D 5	P 4	D 3	P 2	P 1
1	0	1	1	0	1	1

Detecting Errors:

Step1: Analysing bits 1, 3, 5, 7

We have P1 D3 D5 D7 = 1011, (Odd Parity means Error exists)

i.e., p1 = 1

Step2: Analysing bits 2, 3, 6, 7

We have P2 D3 D6 D7 = 1001, (Even Parity means No Error)

i.e., p2 = 0

Step3: Analysing bits 4, 5, 6, 7

We have P4 D5 D6 D7 = 1101, (Odd Parity means Error exists)

i.e., p4 = 1

P4 and P1 are not equal to zero, so receiver's code is wrong.

Correcting Errors:

Error Word E

P4	P2	P1
1	0	1

Decimal Value E= 5, which shows that the 5^{th} bit is error. So, we write the correct word by simply inverting the 5^{th} bit.

Therefore, Correct word = 1001011

UNIT 3

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes:

1. Static Channel Allocation in LANs and MANs
2. Dynamic Channel Allocation.

Static Channel Allocation

- In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user. For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.
- This scheme is also referred as fixed channel allocation or fixed channel assignment.
- In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel. However, it is not suitable in case of a large number of users with variable bandwidth requirements.
- Two common static channel allocation techniques are TDMA and FDMA.

1. Time Division Multiple Access (TDMA)

Time Division Multiple Access (TDMA) is a digital cellular telephone communication technology. It facilitates many users to share the same frequency without interference. Its technology divides a signal into different timeslots, and increases the data carrying capacity.

2. Frequency Division Multiple Access (FDMA)

FDMA is an abbreviation for ***"Frequency Division Multiple Access".*** It is a form of channelization protocol. In this system, the bandwidth is separated into different frequency bands. Each station is assigned a band to transmit data, and that band is always reserved for that station.

The performance of static channel allocation depends on:

1. The variation in the number of users over time.
2. The nature of the traffic sent by the user.

- **The poor performance of static channel allocation can be calculated by the formula**

$$T = 1/(\mu C-\lambda).$$

Where T is mean time delay

Channel of capacity = C

Average arrival rate = $1/\mu$

Frame arrival rate is =λ

Assumptions for Dynamic Channel Allocation

In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.

This allocation scheme optimises bandwidth usage and results is faster transmissions.

Underlying all the work done in this area are the following five key assumptions:

1. Independent Traffic. The model consists of N independent stations (e.g., computers, telephones), each with a program or user that generates frames for transmission. The expected number of frames generated in an interval of length Δt is $\lambda \Delta t$, where λ is a constant (the arrival rate of new frames). Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

2. Single Channel. A single channel is available for all communication. All stations can transmit on it and all can receive from it. The stations are assumed to be equally capable, though protocols may assign them different roles (e.g., priorities).

3. Observable Collisions. If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled. This event is called a collision. All stations can detect that a collision has occurred. A collided frame must be transmitted again later. No errors other than those generated by collisions occur.

4. Continuous or Slotted Time. Time may be assumed continuous, in which case frame transmission can begin at any instant. Alternatively, time may be slotted or divided into discrete intervals (called slots). Frame transmissions must then begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

5. Carrier Sense or No Carrier Sense. With the carrier sense assumption, stations can tell if the channel is in use before trying to use it. No station will attempt to use the channel while it is sensed as busy. If there is no carrier sense, stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.

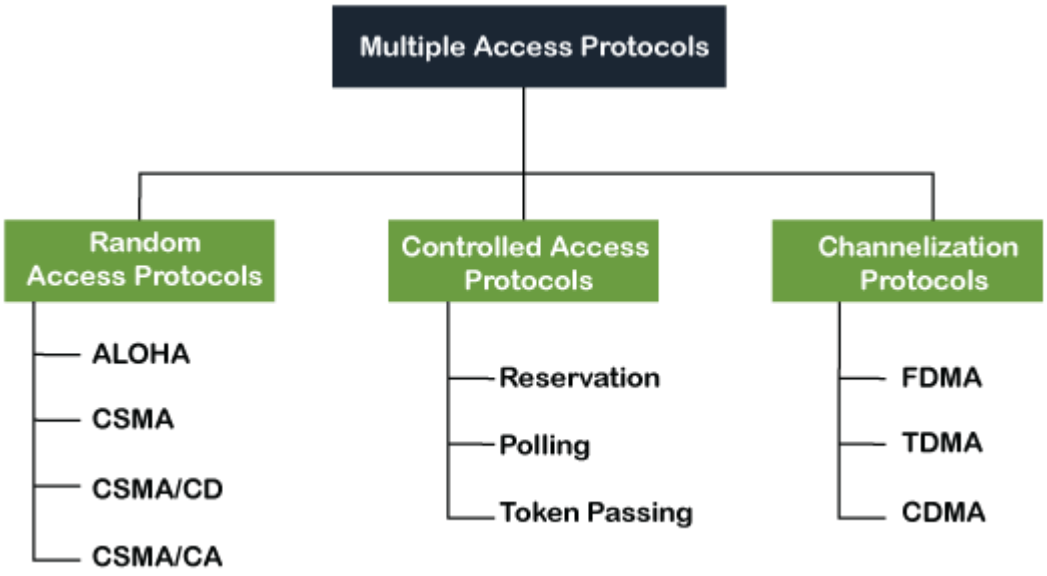
Multiple Access Protocols

If there is a dedicated link between the sender and the receiver the data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

Hence multiple access protocols are required to decrease collision and avoid crosstalk.

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



Random Access Protocol

In this, all stations have same superiority that is no station has more priority than another station. Any Station can send data depending on medium's state (idle or busy).

In a Random access method, each station has the right to the medium without being controlled by any other station.

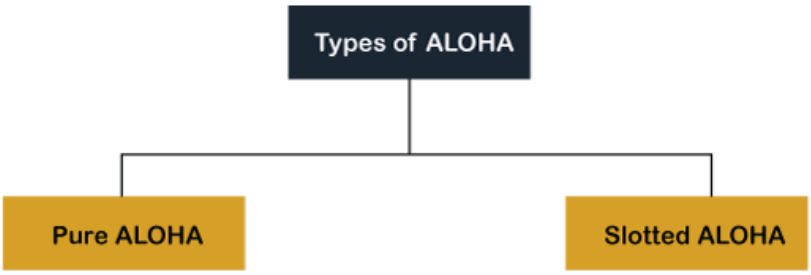
If more than one station tries to send, there is an access conflict (collision) and the frames will be either destroyed or modified.

To avoid access conflict, each station follows a procedure.

- When can the station access the medium?
- What can the station do if the medium is busy?
- How can the station determine the success or failure of the transmission?
- What can the station do if there is an access conflict?

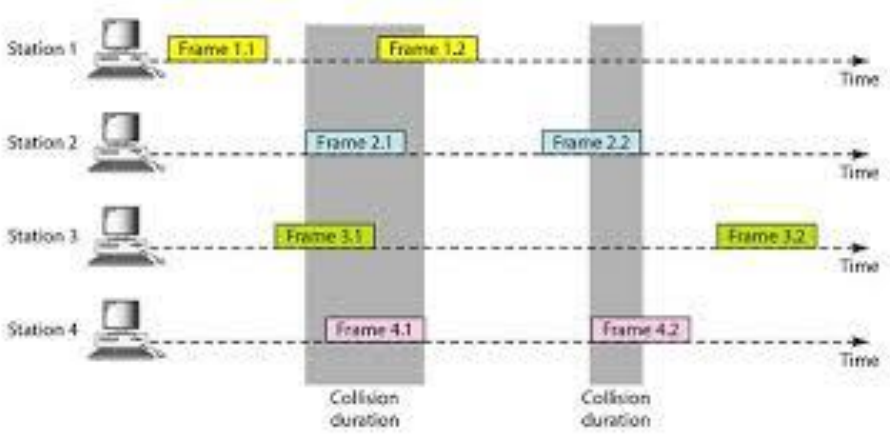
Aloha

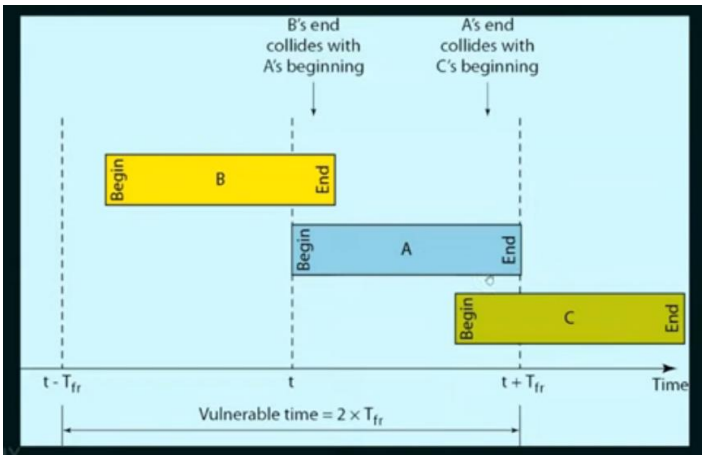
- Aloha is a random access protocol.
- It was actually designed for WLAN but it is also applicable for share medium.
- In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.



Pure Aloha

- Whenever data is available for sending over a channel at stations, we use Pure Aloha.
- In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost.
- When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment.
- If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb).
- And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.



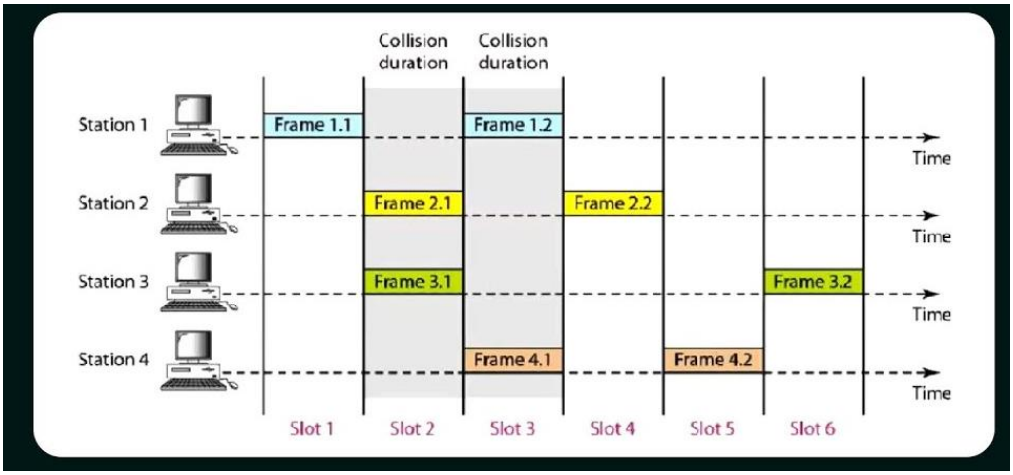


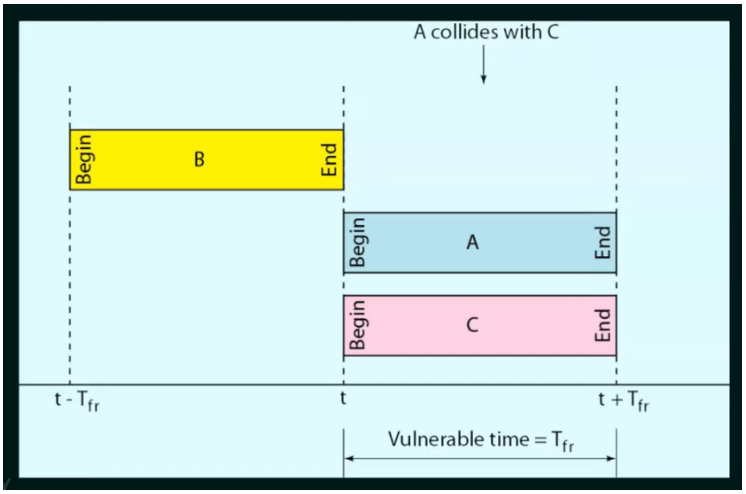
1. The total vulnerable time of pure Aloha is 2 * T_{fr}. (Frames Transmission Time)
2. Maximum throughput occurs when G = 1/2 that is 18.4%.

3. Successful transmission of data frame (Throughput) is $S = G * e^{-2G}$. (Where G is the number of stations wish to transmit in the same time.)

Slotted Aloha

- The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting.
- In slotted Aloha, the shared channel is divided into a fixed time interval called slots.
- So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot.
- If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.





1. Maximum throughput when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is $S = G * e^{-G}$. (Where G is the number of stations wish to transmit in the same time.)
3. Vulnerable Time = Frame Transmission Time (The total vulnerable time required in slotted Aloha is Tfr.)

CSMA Protocol

- Carrier Sense Protocol.
- To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- Principle of CSMA: “sense before transmit” or “listen before talk.”
- Carrier busy = Transmission is taking place.
- Carrier idle = No transmission currently taking place.
- The possibility of collision still exists because of propagation delay; a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.
- **Types of CSMA**

    1. **1-Persistent CSMA**

        In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

    2. **P-Persistent CSMA**

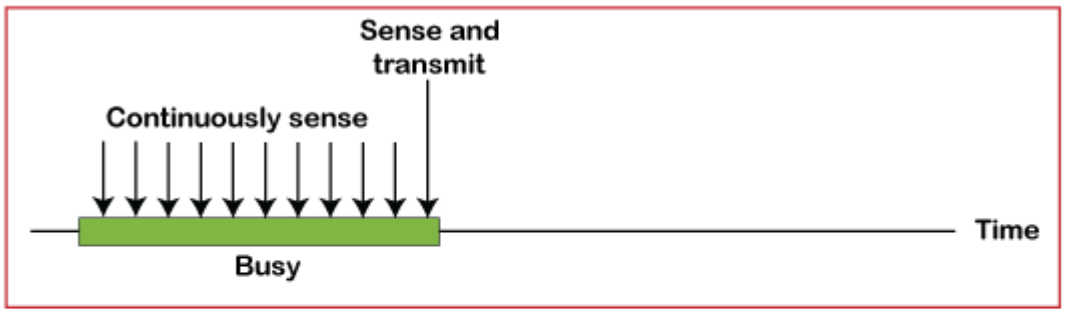
        It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

    3. **Non-Persistent CSMA**

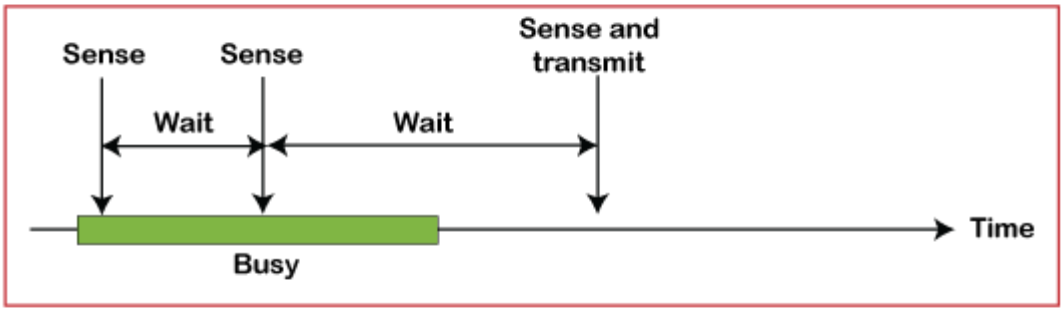
        It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

    4. **O-Persistent CSMA**

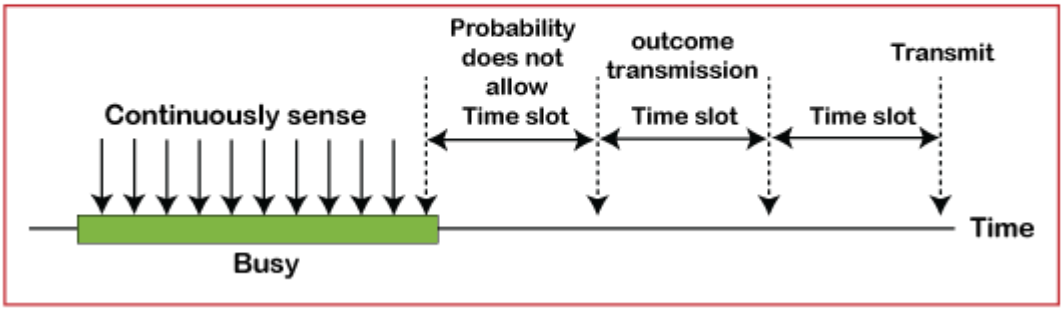
        It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent



b. Nonpersistent



c. p-persistent

CSMA/ CD

Carrier Sense Multiple Access/ Collision Detection

- It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer.
- Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful.
- If the frame is successfully received, the station sends another frame.
- If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission.
- After that, it waits for a random time before sending a frame to a channel.
- Quickly terminating damaged frames saves time and bandwidth.
- This protocol, known as CSMA/CD (CSMA with Collision Detection) is widely used on LANs in the MAC sublayer.
- Access method used by Ethernet: CSMA/CD.

- At the point marked t_0, a station has finished transmitting its frame.
- Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision.

- Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.
- After a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.
- Therefore, our model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.

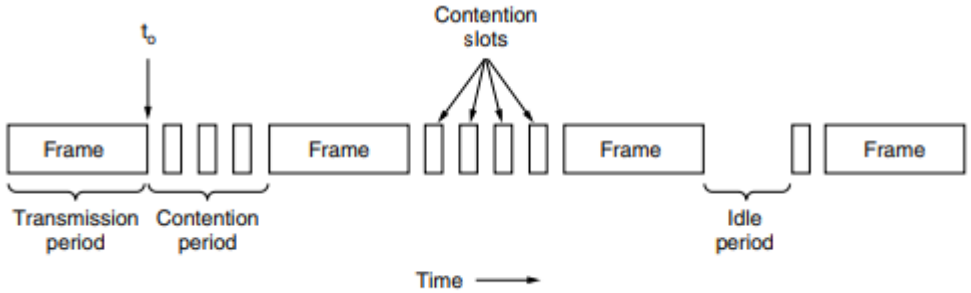


Figure 4-5. CSMA/CD can be in contention, transmission, or idle state.

CSMA/ CA

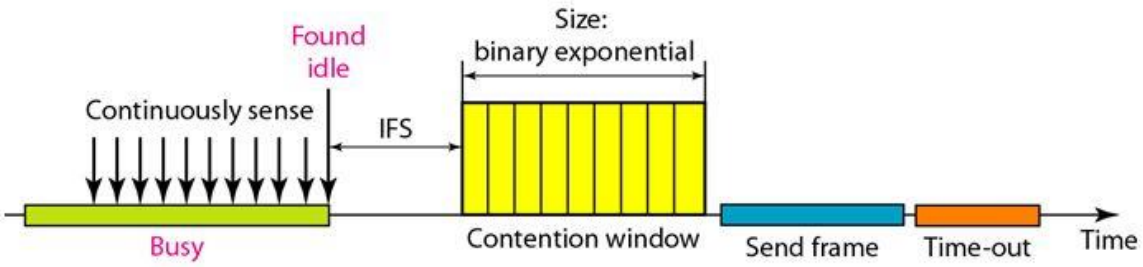
- It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer.
- When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear.
- If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel.
- Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the **CSMA/ CA** to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.


Found
idle
Size:
binary exponential
Continuously sense
IFS
Busy
Contention window
Send frame
Time-out
Time