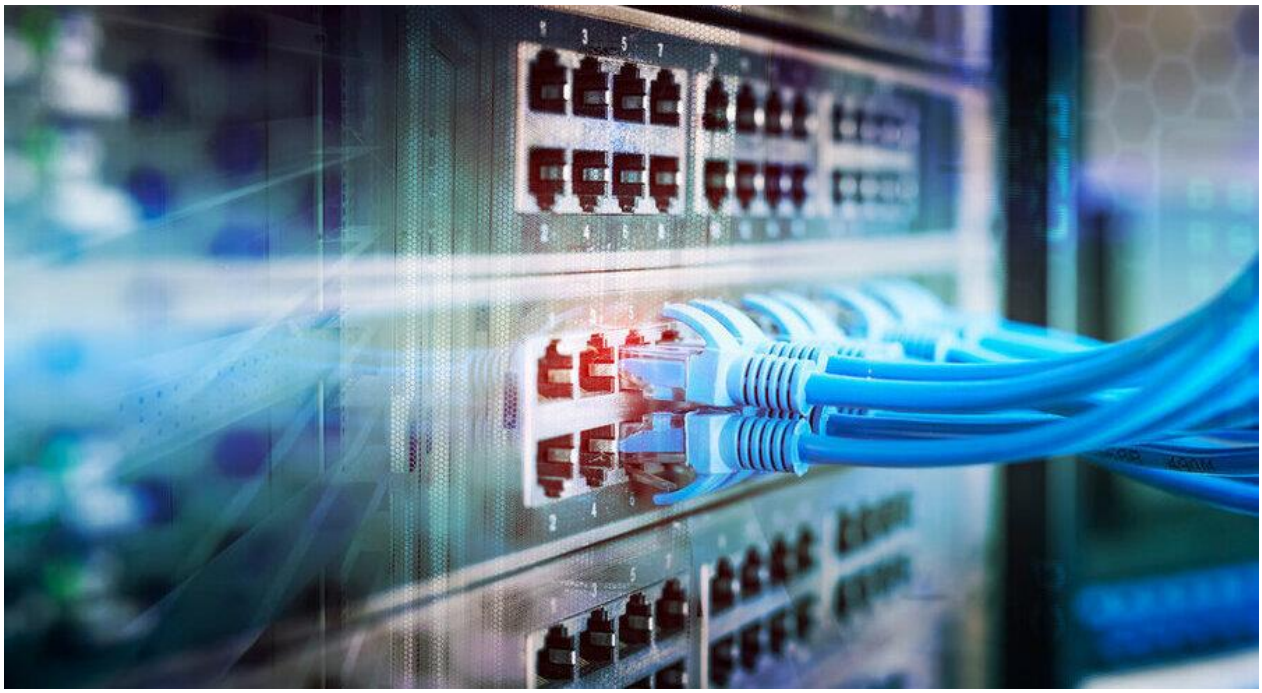


Communication Network

Computer Network

1. Communication Network Fundamentals:

1.1 Definition:

Communication network is a set of nodes connected by communication links. A node can be any intelligent device such as computer, printer or any other device capable of sending and receiving data generated by other nodes in the network. Communication link can be wired or wireless link and it carries the data information.

1.2 Characteristics of communication network:

- Fault tolerance: Fault tolerance is the property that enables the network to continue working without interruption when one or more of its components fail. And ensure no loss of the service.

- Scalability: is the ability of growing based on the needs and have good performance after growth.

- Quality of service: a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity.

- Security: is the ability to prevent unauthorized access, missus and forgery. And the ability to provide confidentiality, integrity and availability.

1.3 Protocols and Data communications:

1.3.1 Data communications:

the exchange of data between two nodes via some form of link (transmission medium) such as cable or wireless.

1.3.2 Data flow:

Data flow is the way that data can flow from one node to another, there are three ways:

- Simplex: provides a unidirectional communication of two devices, one device can transmit and the other device will receive (ex. Keyboard, Traditional monitors etc.…)
- Half Duplex: provides a communication in both directions but not at the same time, if one device is sending, the other can only receive, and vice versa (ex. Walkie-Talkie)
- Duplex or Full Duplex: provides a communication in both directions simultaneously, both devices can receive and send at the same time (ex. Telephone line)

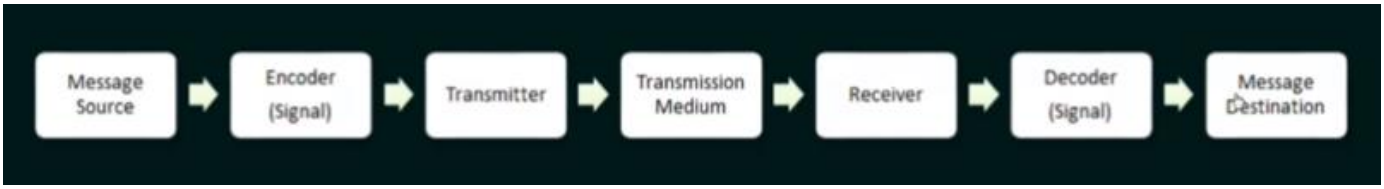
1.3.3 Protocols:

1.3.3.1 Protocols definition:

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.

1.3.3.2 Protocols elements:

- Message encoding: messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted. The destination host receives and decodes the signals in order to interpret the message.



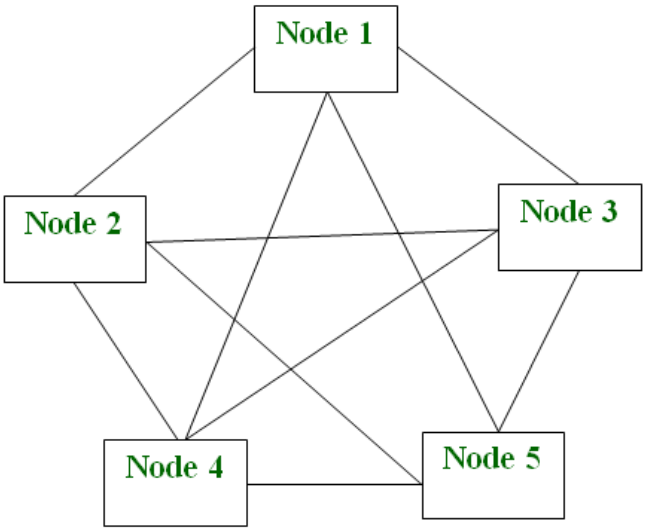
- Message formatting and Encapsulation: a message that is sent over a computer network follows specific format rules for it to be delivered and processed. Just as a letter is encapsulated in an envelope for delivery, so too are computer messages encapsulated. Each computer message is encapsulated in a specific format, called a frame, before it is sent over the network. A frame acts like an envelope; it provides the address of the intended destination and the address of the source host and other information.

Destination (physical / hardware address)	Source (physical / hardware address)	Start Flag (start of message indicator)	Recipient (destination identifier)	Sender (source identifier)	Encapsulated Data (bits)	End of Frame (end of message indicator)
Frame Addressing		Encapsulated Message				

- Message size: is the process of breaking up a long message into individual pieces before being sent over the network.
- Message timing: is a process that manage timing, flow control and response timeout (for example computer determines when to start sending a message and how to respond when there is occurrence of error).
- Message delivery options: There are different delivery options like Unicast, Multicast, Broadcast. Sending information to a single person is referred to as a one-to-one delivery and is called unicast which implies that there is only one destination (single destination). To communicate information to more than one person (Group of people at the same time) is referred to as one-to-many and is called multicast which implies that one sender to multiple destinations/recipients for the same message. Sometimes information is to be communicated to every person in the same area. This is referred to as one-to-all and is called broadcast which implies that one sender sends a message to all connected recipients.

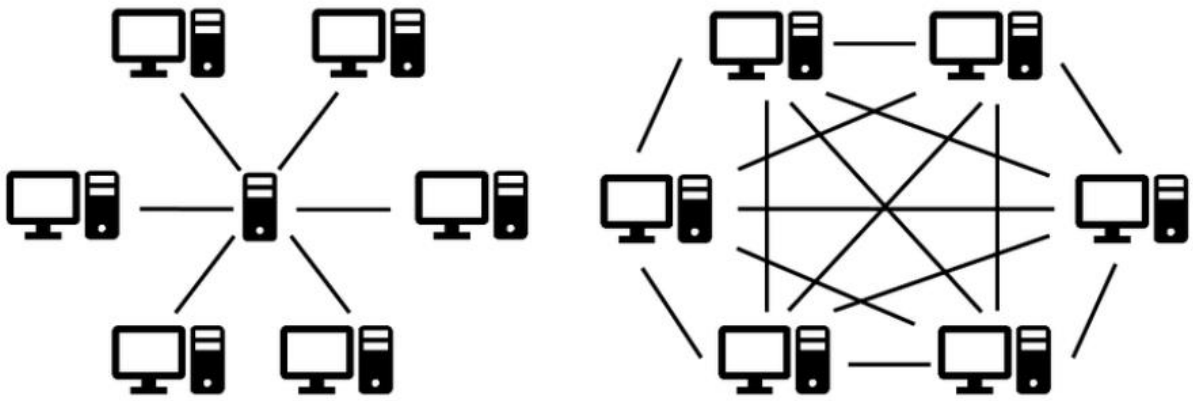
1.3.4 Peer-To-Peer Network (P2P):

A peer-to-peer network is a simple network of computers connected with no centralized administration. Here each computer acts as a node for file sharing within the formed network. And each node acts as a server and thus there is no central server to the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.



1.3.5 Client server network:

Client-server networks are computer networks that use a dedicated computer (server) to store data, manage/provide resources and control user access. The server acts as a central point on the network upon which the other computers connect to. A computer that connects to the server is called a client and it have ability to request server then receive a response from the server. A client-server network is usually preferred over a peer-to-peer network that doesn't have a central server to manage the network.



Client-Server network

P2P network

1.3.6 Network types:

1.3.6.1 Local Area Network (LAN):

Local Area Network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

- LAN devices are: Wired LAN ex. Ethernet – Hub, Switch, Wireless LAN ex. Wi-Fi

1.3.6.2 Metropolitan Area Network (MAN):

Is a computer network that interconnects users with computer resources in a geographic region of the size of metropolitan area (city). It's the interconnection of multiples LANs.

- MAN devices ex. Switches or Hub, Routers or Bridges

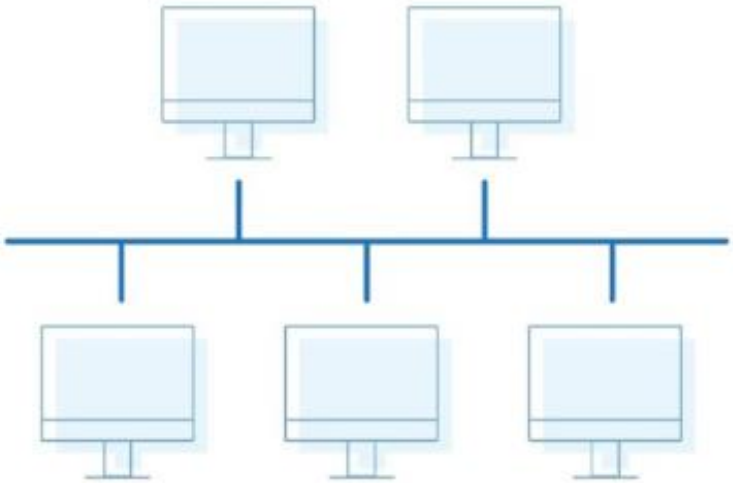
1.3.6.3 Wide Area Network (WAN):

Is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking. It's the interconnection of WANs and LANs all together and on different region in the entire world.

- WAN devices ex. Internet network

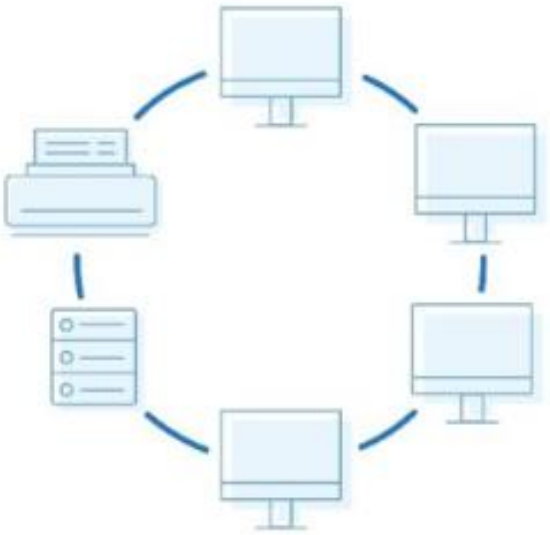
1.3.7 Network Topologies

1. **Bus:** all data transmitted between nodes in the network is transmitted over a common transmission medium and is able to be received by all nodes in the network simultaneously. A signal containing the address of the intended receiving machine travels from a source machine in both directions to all

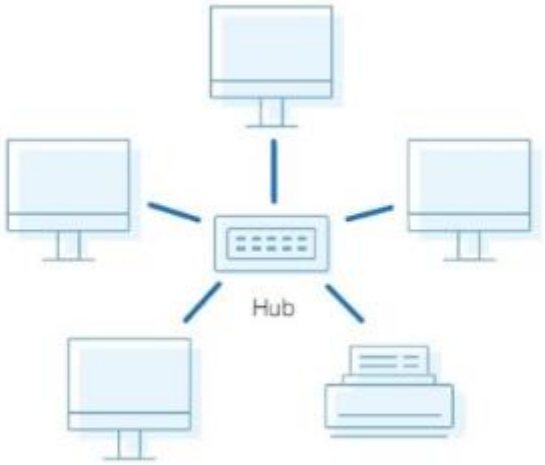


machines connected to the bus until it finds the intended recipient.
- Advantages: only one wire and less expensive, suited for temporary network, nodes failures does not affect others.
- Disadvantages: not fault tolerant (No redundancy), Limited cable length, No security.

2. **Ring:** is a bus topology in a closed loop, it's a peer-to-peer LAN topology and unidirectional.
- Advantages: better in performance than bus topology, all nodes with equal access.
- Disadvantages: unidirectional, single point of failure will affect the whole network, No security.



3. **Star:** here every node is connected to a central node (hub or switch) with a centralized management, and all the traffic must pass through a hub or a switch.



- Advantages: easy to design and implement, centralized administration, scalable.
- Disadvantages: Single point of failure affect the whole network, increase the cost due to switch and hub.

4. **Hybrid:** is the combination of all topologies.

1.3.8 Addresses:

1.3.8.1 Ip Address: An Internet Protocol address (IP address) is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions network interface identification and location addressing. Every node in the computer network is identified with the help of IP address, IP address can change based on the location of the device. IP addresses are represented in decimal and it has 32 bits.

1.3.8.2 Mac Address: A media access control address is a unique identifier assigned to each intelligent device connected to the internet network, it's used as a network address in communications within a network segment. MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator. MAC addresses are primarily assigned by device manufacturers.

1.3.8.3 Port Addressing: is a port number that represent a process, every process in a node is uniquely identified using a port number, for example in operating system many processes will be running in the same time and data which are sent or received must reach the right process, the port address provides this process's address. It's an integer number (between 0 and 65535).

MAC addresses represent the name of the device and IP addresses represent the location of the device and port address represent the right prosses.

1.4 Computer Network Technologies:

1.4.1 Nodes: includes end nodes and intermediary nodes

End devices: End devices are either the source or destination of data transmitted over the network. In order to distinguish one end device from another, each end device on a network is identified by an address. When an end device initiates communication, it uses the address of the destination end device to specify where the message should be sent.

For example, a server is an end device that has software installed that enables it to provide information, like email or web pages, to other end devices on the network. An example of server end device is Google servers.

And the client's device is an end device that has software installed to enable it to request and display the information obtained from a server. An example of a client end device is smartphone.

Intermediary network devices: Intermediary devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network. Intermediary devices connect the individual hosts to the network and can connect multiple individual networks to form an internet network. An examples of intermediary network devices are: switches and wireless access points, routers, firewalls.

- Switches:

A network switch (also called switching hub, bridging hub, and, by the IEEE, MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

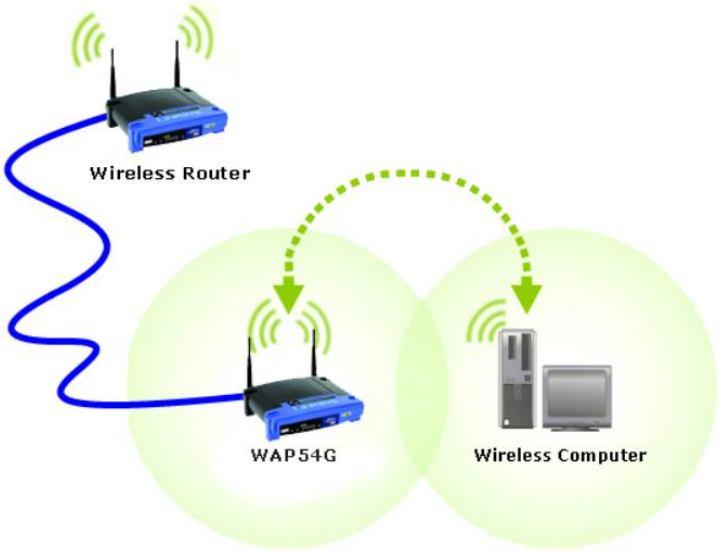
A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model (we will talk about OSI model later in this papers). Some switches can also

forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

Unlike repeater hubs, which broadcast the same data out of each port and let the devices pick out the data addressed to them, a network switch learns the identities of connected devices and then only forwards data to the port connected to the device to which it is addressed.

- Wireless access point:

In computer networking, a wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. As a standalone device, the AP may have a wired connection to a router, but, in a wireless router, it can also be an integral component of the router itself. An AP is differentiated from a hotspot which is a physical location where Wi-Fi access is available.



- Routers:

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the

form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.

A router is connected to two or more data lines from different IP networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet header to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

The most familiar type of IP routers are home and small office routers that simply forward IP packets between the home computers and the Internet.

The different between switches and router is that router is a layer 3(Network layer) device and it stores routing IP addresses table and switches are layer 2 (Data Link) devices and stores MAC addresses.

- Security Devices (firewall):

Network security is a system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

- Bridges:

A network bridge is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments. This function is called network bridging. Bridging is distinct from routing. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. In the OSI model, bridging is performed in the data link layer (layer 2).If one or more segments of the bridged network are wireless, the device is known as a wireless bridge.

Bridges have the same ability of a repeater with some additional functionalities such as it can reading Mac address. It also used to connect two local area networks but on the same protocol.

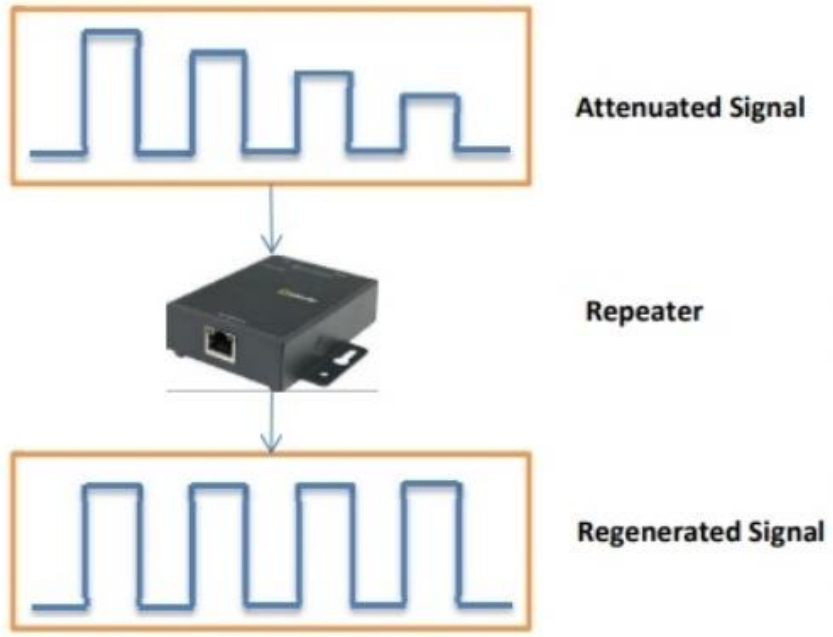
The difference between bridge and router is that these two devices can connect LANs but, the bridge is layer 2 device and it works with only two LANs and with the same protocol, whereas router is layer 3 device and it works at least with two LANs and it doesn't require the same protocol for LANs to communicate.

- **Hubs:**

A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices. It's a physical layer device and used to set up LANs. And it works only in star topology.

- Repeaters:

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



- Cell Tower:

Also known as cell sites, are where electric communications equipment and antennae are mounted, allowing the surrounding large area to use wireless communication devices like telephones and radios. Cell towers are usually built by a tower company or a wireless carrier when they expand their network coverage or capacity, providing a better reception signal in that area.

1.4.2 Media:

- **Wired medium (guided medium):**
  - Ethernet straight-through cable
  - Ethernet cross over cable
  - Fiber optic cable
  - USB cable

- **Wireless medium (unguided medium)**
  - Infrared
  - Radio
  - Microwaves
  - Satellite

1.4.3 Services: includes: e-mail, Storage services, file sharing, instant messaging, online game, voice over IP, video telephony, World wide web.

1.5 Switching techniques:

Switching techniques helps in deciding the best route for data transmission if there are multiple paths in a larger network. It provides one to one connection. There are multiple switching techniques such as circuit switching and message switching and packet switching.

Circuit switching:

This technique provides a dedicated path established between the sender and the receiver before data transfer, for example telephone network.

3 phases in circuit switching: 1. Connection establishment. 2. Data transfer. 3. Connection Disconnection.

Message switching:

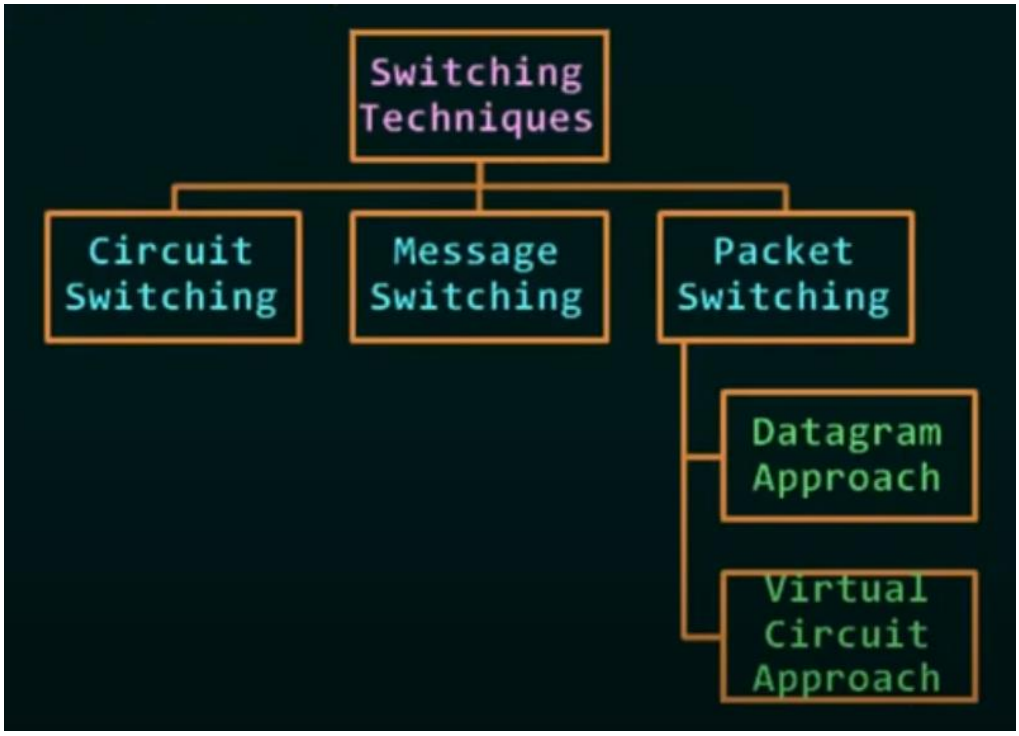
This technique provides store and forward mechanism, message transferring as a complete unit and forwarded using store and forward mechanism at the intermediary node. This technique not suited for streaming and real-time applications.

Packet switching:

In this technique message will be broken into individual chunks called packets, and each packets sent individually with a source and IP address and an additional sequence of numbers.

Sequence of numbers help the receiver to reorder the packets and detect missing packets and send acknowledgments.

- **Datagram Approach:** it sends data packet with its order information for each packet, the transmission path is not fixed so the receiver need to reorder the packets with using the order information of each packet.
- **Virtual Circuit Approach:** in this case a preplanned route is established before the messages are sent. A call request and call accept are used to establish the connection between sender and receiver. Then the path must be fixed for a duration of a logical connection.



2.Layering in computer Network:

Layering means decomposing the problem into more manageable component (layers). So, it provides more modular design and easy to troubleshoot. There are protocols in each layer governs the activities of the data communication.

2.1 layered architecture:

- **The OSI Reference Model:** stands for open system interconnection, it's a model for understanding and designing a network architecture. The OSI is not a protocol, it's a guideline and hence it's referred as OSI reference model.
  The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- **The TCP/IP Model:** (Transmission Control Protocol/Internet protocol) is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.

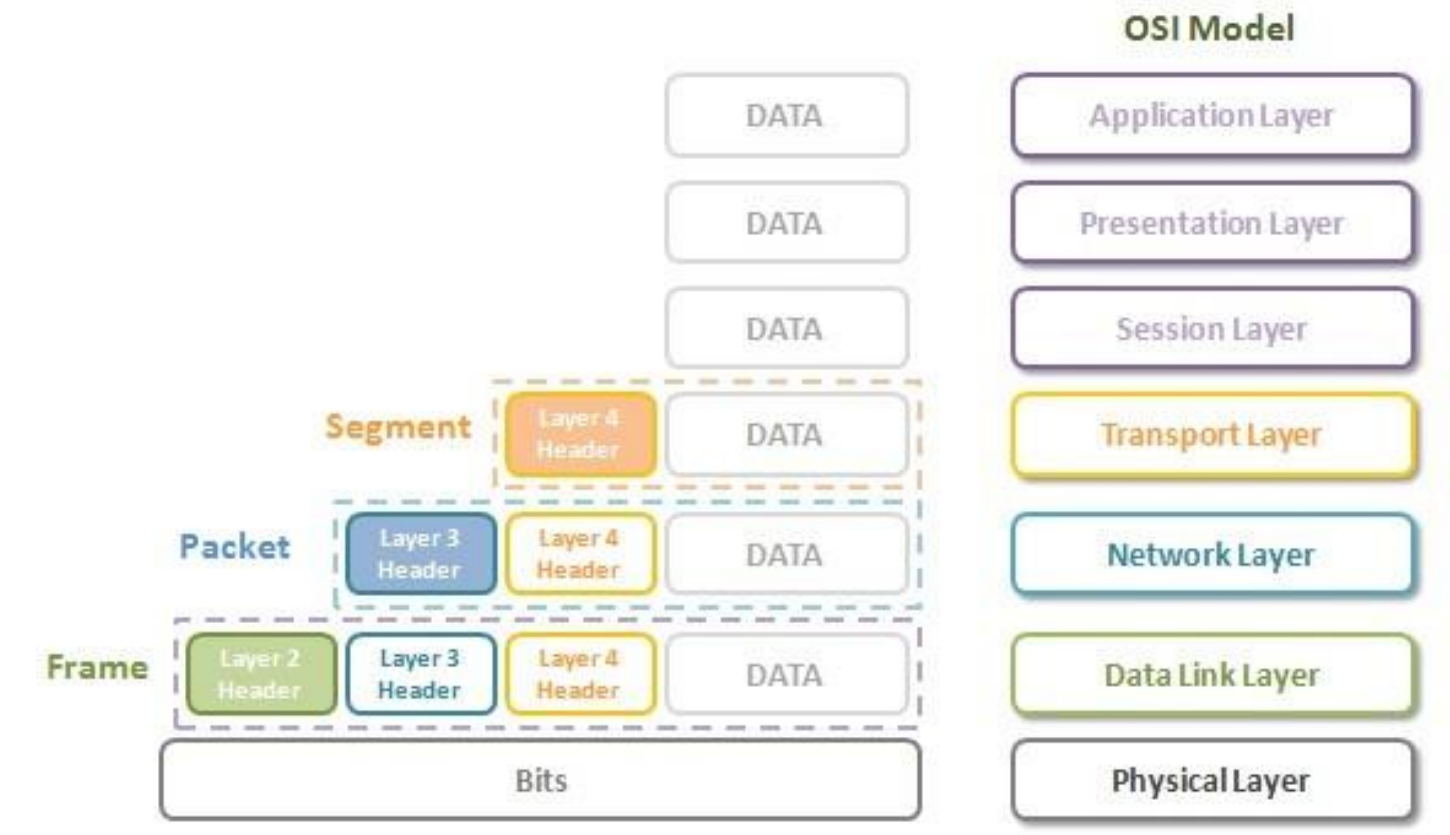
2.2 Layers in the OSI Reference Model:

- Application Layer: it enables the user to access the network resources such as file transfer mail services and directory services.
- Presentation Layer: it's concerned with the syntax and semantics of the information exchanged between two systems such as translation, encryption and compression.
- Session Layer: it establishes and maintains and synchronizes the interaction among communicating devices such as dialog control and synchronization.
- Transport Layer: it's responsible for process-to-process delivery of the entire message. The services that are provided by this layer are port addressing, segmentation and reassembly, connection control, end-to-end flow control and error control.
- Network Layer: it's responsible for delivery of data from the original source to the destination network. The services that are provided by this layer are logical addressing and routing.
- Data Link Layer: it's responsible for moving data(frames) from one node to another node. The services that are provided by this layer are framing, physical addressing, flow control, error control, access control.

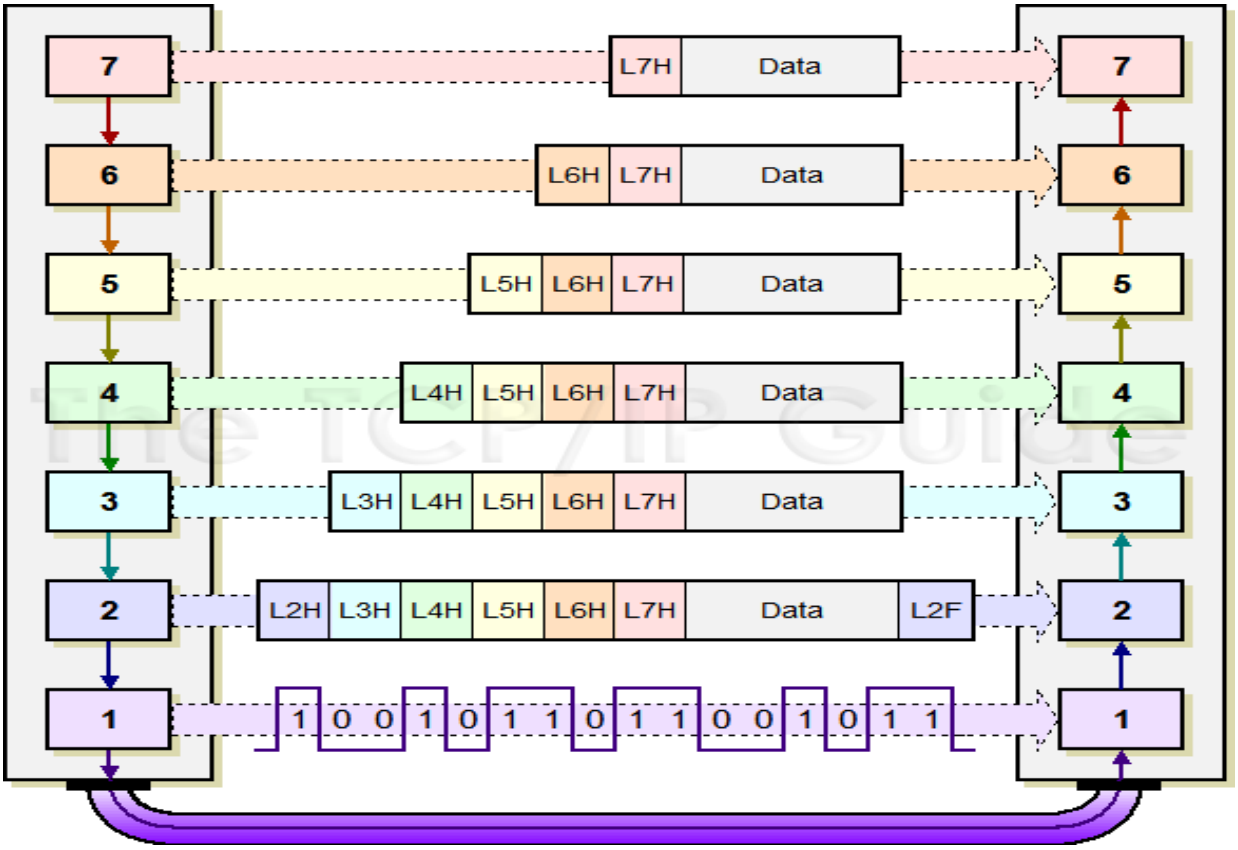
- Physical Layer: it's responsible for transmitting bits over a medium. It also provides electrical and mechanical specifications. The services that are provided by this layer are physical characteristics of the media, representation of bits, Data rate, Synchronization of bits, Line configuration, physical topology.

Example:

These layers are applied on Data from the top to the bottom, this model encode data to a segment then to packet then it will be a frame and the final state is a digital signal, after that it will be an analog signal ready for physical transmission.

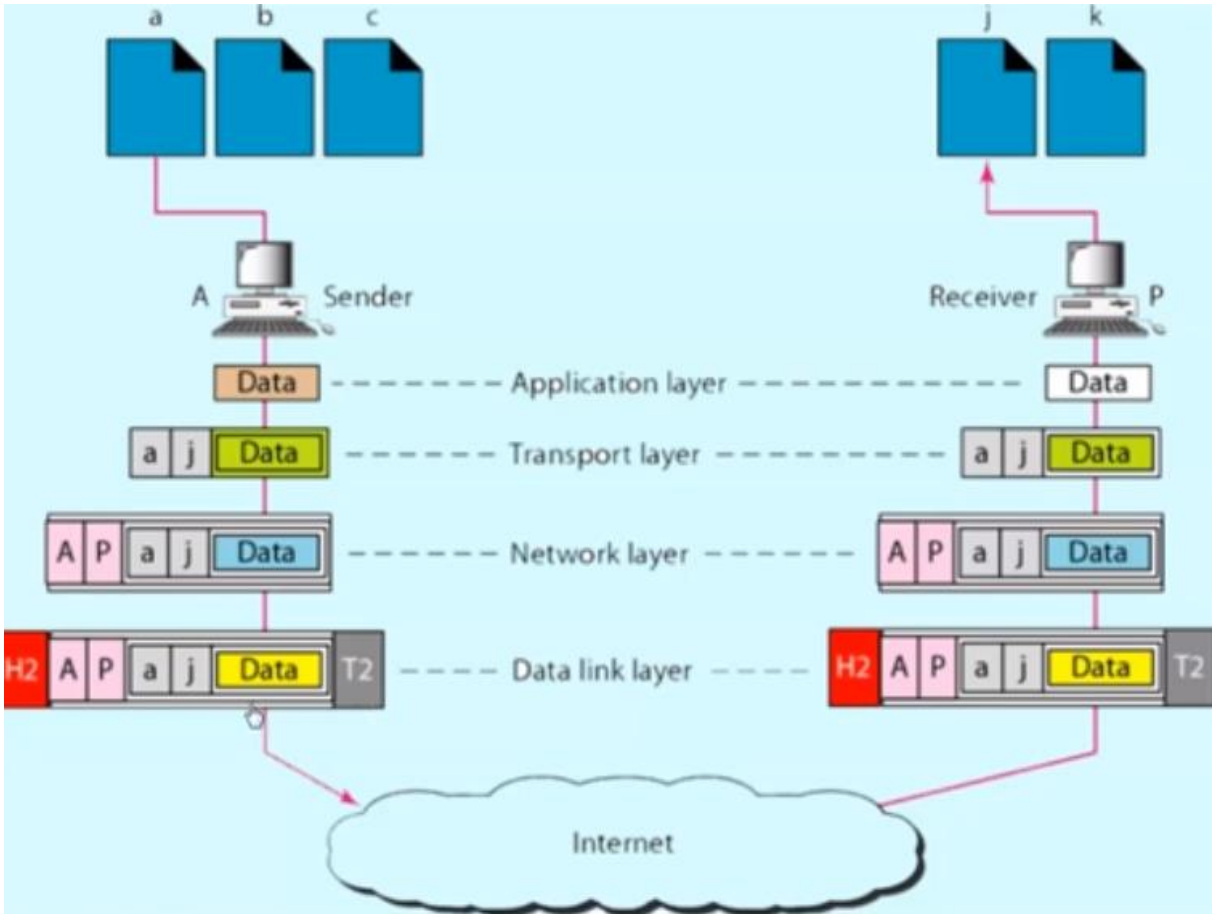


The receiver will apply the same layers from the bottom to the top to decoding the received Data.

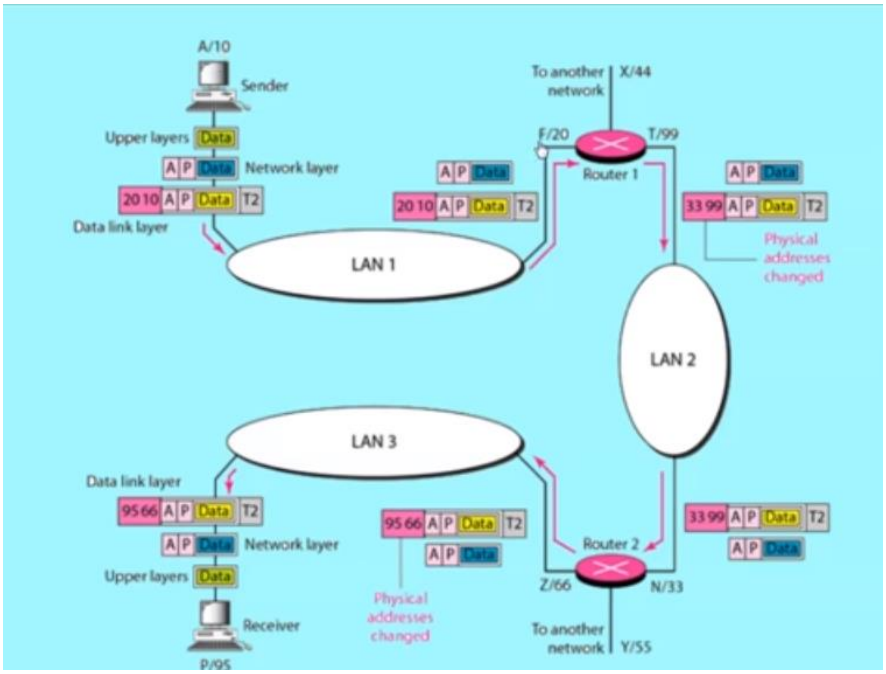


2.3 Addressing:

Addressing is adding sender and receiver addresses to the transmission Data so they can communicate using theses addresses. First, transport layer adds port address of sender plus port address of receiver as a header to the data, then the network layer adds IP addresses of the sender and the receiver, finally Data link layer adds MAC addresses. (in this paragraph we talk only about addressing other information will be described in the next papers).



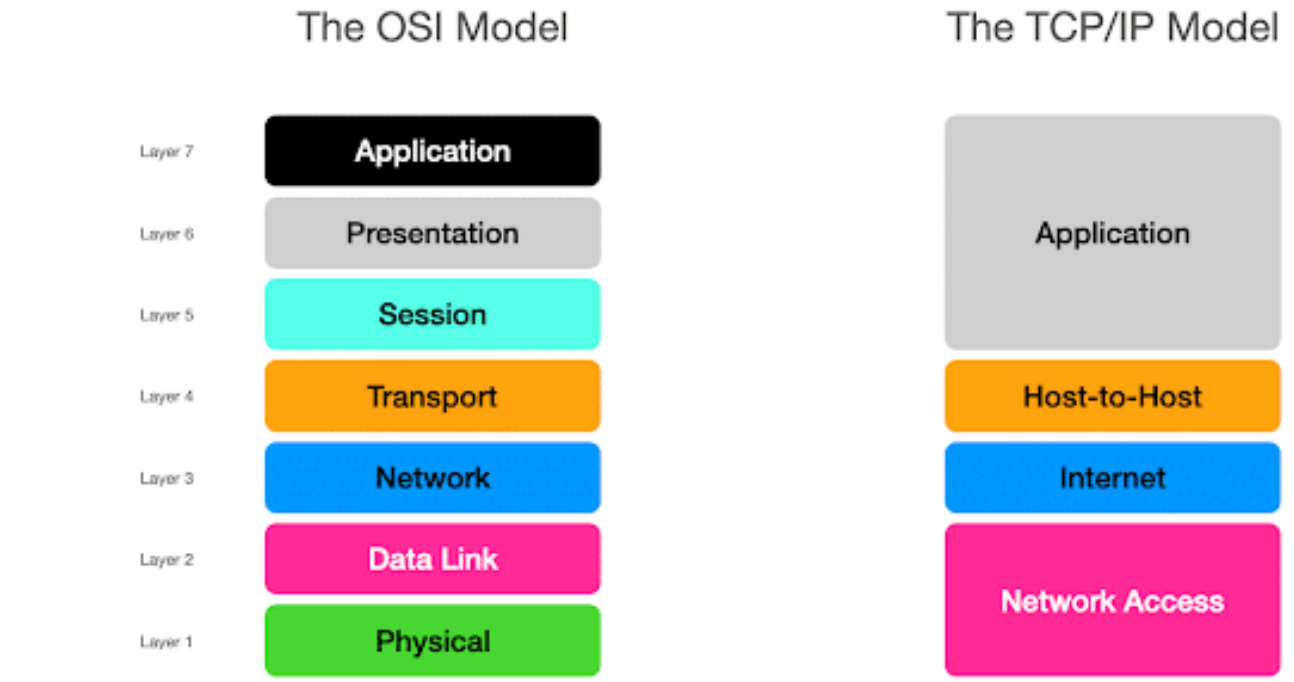
Now we will focus only on MAC and IP addresses of data header in transmission network, in this figure we have an example of transmission network from a node to another. First, we have A (IP address of the sender) and P (IP address of the receiver). Second, on the Data link layer of each node we have MAC address of the sender and the target MAC address of the local node receiver. it means that MAC addresses are used to help defining path between LANs and with help of IP address it can reach the final destination.

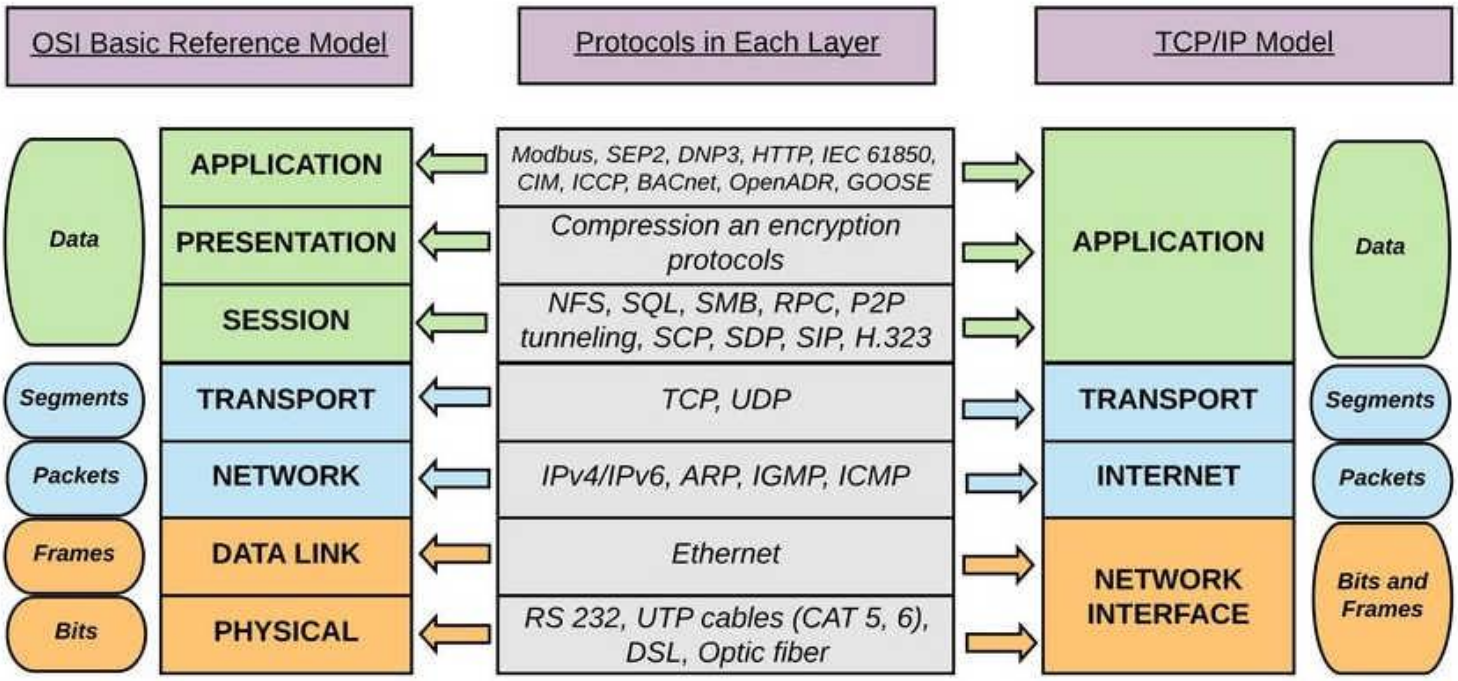


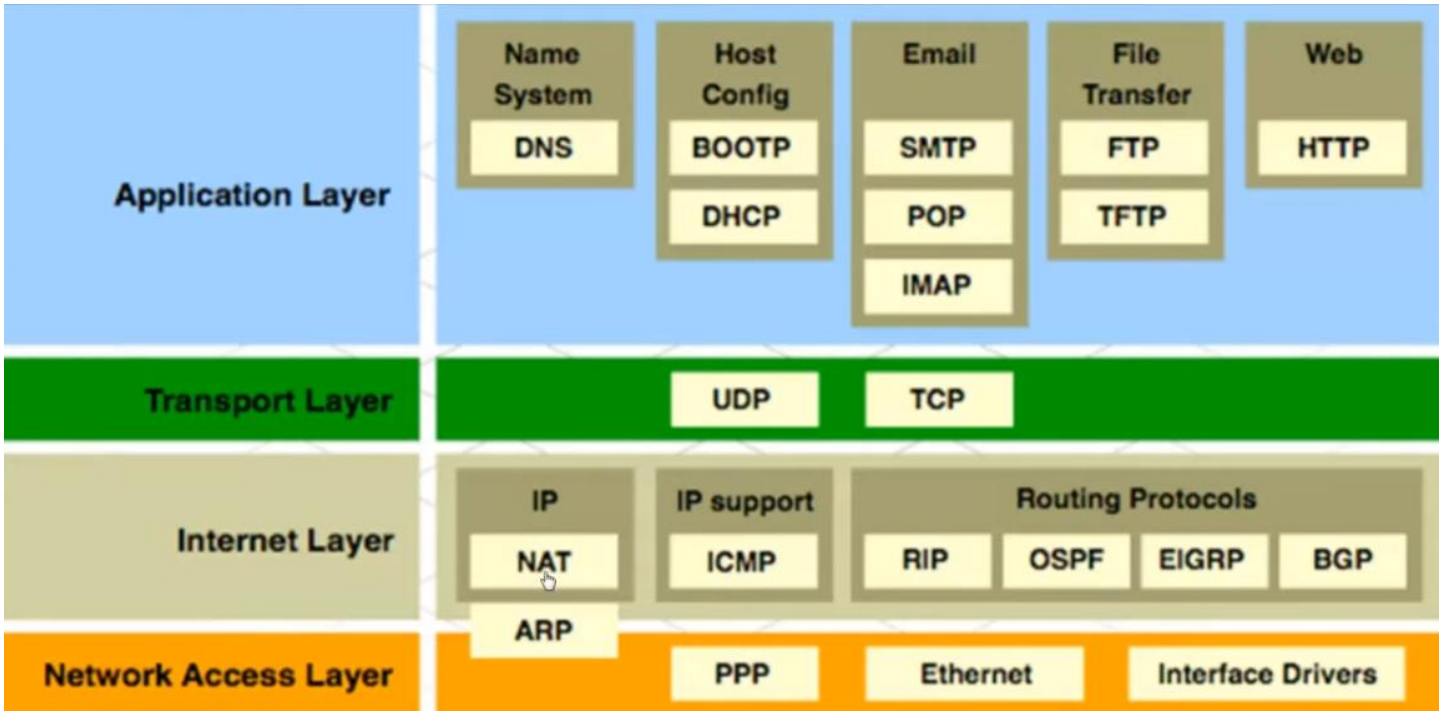
2.4 TCP/IP Model

The TCP/IP layers are not compatible with OSI model, TCP/IP model was developed prior to the OSI model and therefore it does not match with OSI model. TCP/IP is more popular, OSI is just a guideline.

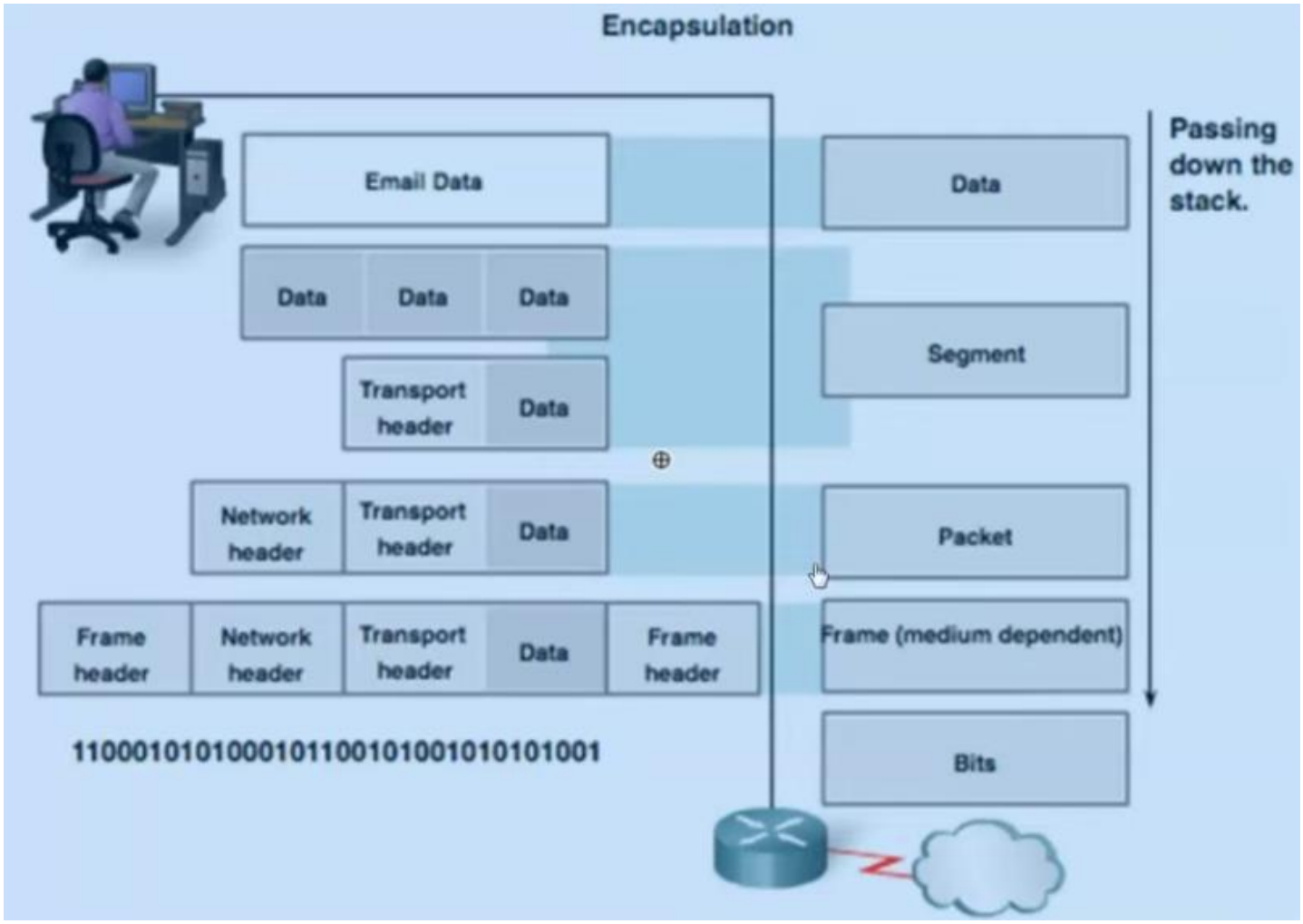
In some resources you will find 5 layers on TCP/IP, it just because sometimes they splits network access layers onto Data link layer and Physical layer.


The OSI Model
The TCP/IP Model
Layer 7
Application
Layer 6
Presentation
Layer 5
Session
Layer 4
Transport
Layer 3
Network
Layer 2
Data Link
Layer 1
Physical
Application
Host-to-Host
Internet
Network Access


OSI Basic Reference Model
Protocols in Each Layer
TCP/IP Model
Data
APPLICATION
Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE
PRESENTATION
Compression an encryption protocols
SESSION
NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323
APPLICATION
Data
Segments
TRANSPORT
TCP, UDP
TRANSPORT
Segments
Packets
NETWORK
IPv4/IPv6, ARP, IGMP, ICMP
INTERNET
Packets
Frames
DATA LINK
Ethernet
NETWORK INTERFACE
Bits and Frames
Bits
PHYSICAL
RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber



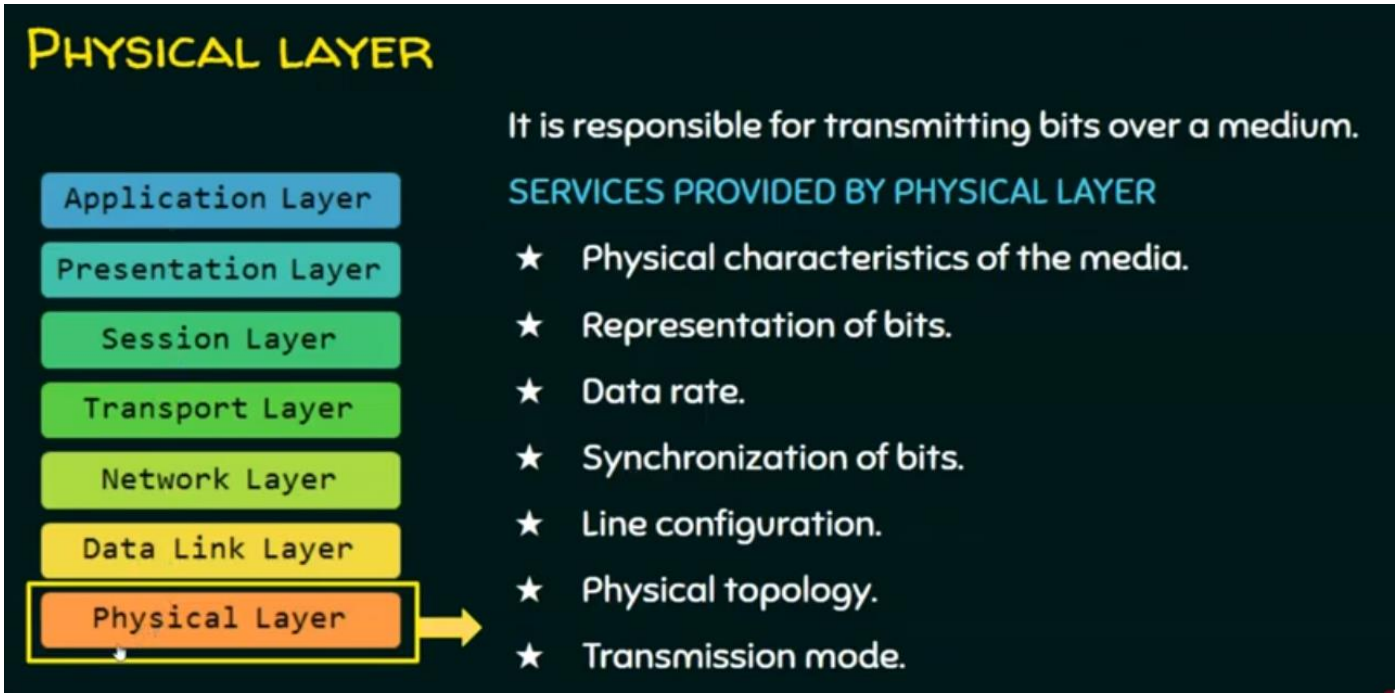
2.4.2 Protocol Data Unit (PDU): is the encapsulation of data from the first layers with the origin format of data to the format of bits.



2.5 Layers:

2.5.1 Physical Layer:

Data that outputs by the PDU have a format of bits, and physically bits are a digital signal. For physical medium transmission (physical media), digital signals are not required. It requires an analog signal and for that we have to convert the output signal. The most popular physical medias are: copper cable, fiber optic cable and wireless media.



2.5.1.1 Copper cable (wired)

Copper has been used in electrical wiring since the invention of the electromagnet and the telegraph in the 1820s. The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

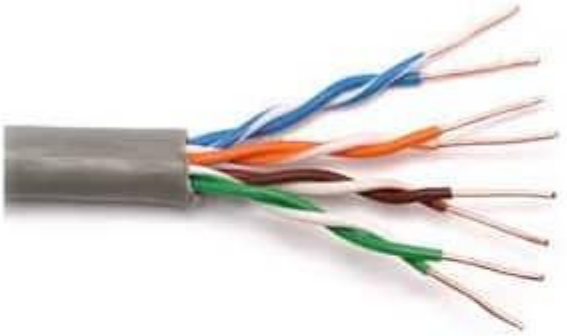
Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment.

Copper cable conducts an electromagnetic signal. The physical components that are used for copper cable are USP/STP, coaxial, connectors, NICs, ports/interfaces.

There are lot of types of copper wired media cables:

1. **Ethernet cable – Unshielded twisted pair (UTP)**
2. **Ethernet cable – Shielded twisted pair (STP)**

There are two types of ethernet cables shielded and unshielded, the differences between these two types are the cost but STP have less effect of the electromagnetic interferences (EMI) and radio frequency interferences (RFI) then UTP, this effect called crosstalk it can be limited on UTP cable by varying the number of twists per wire pair.



UTP Cable

STP Cable

2.5.1.2 Fiber optic cable (wired)

Fiber-optic cable, also known as an optical-fiber cable, is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable is used.

Fiber optic conducts light pulses (a light pulse equal 1 and no light equal 0). The physical components that are used for fiber optic cables are single-mode fiber, multimode fiber, connectors, NICs and interfaces, Lasers and LEDs.

The difference between copper and fiber optic cables:

Implementation Points	Copper	Fiber Optic
Bandwidth Supported	10 Mbps – 10 Gbps	10 Mbps – 100 Gbps
Range	Relatively short (upto 100 meters)	Relatively High (upto 100,000 meters)
Immunity To EMI And RFI	Low	High (Completely immune)
Immunity To Electrical Hazards	Low	High (Completely immune)
Media And Connector Costs	Lowest	Highest
Installation Skills Required	Lowest	Highest
Safety	Lowest	Highest

2.5.1.3 Wireless Media

This type of conductors, no physical media is required for the transmission, data can transfer through the air, and it can travel large distances but it also less secure.

Wireless media conducts radio waves. The physical components that are used for wireless medias are: Access points, NICs, Radio, Antenna.

There are four types of wireless media:

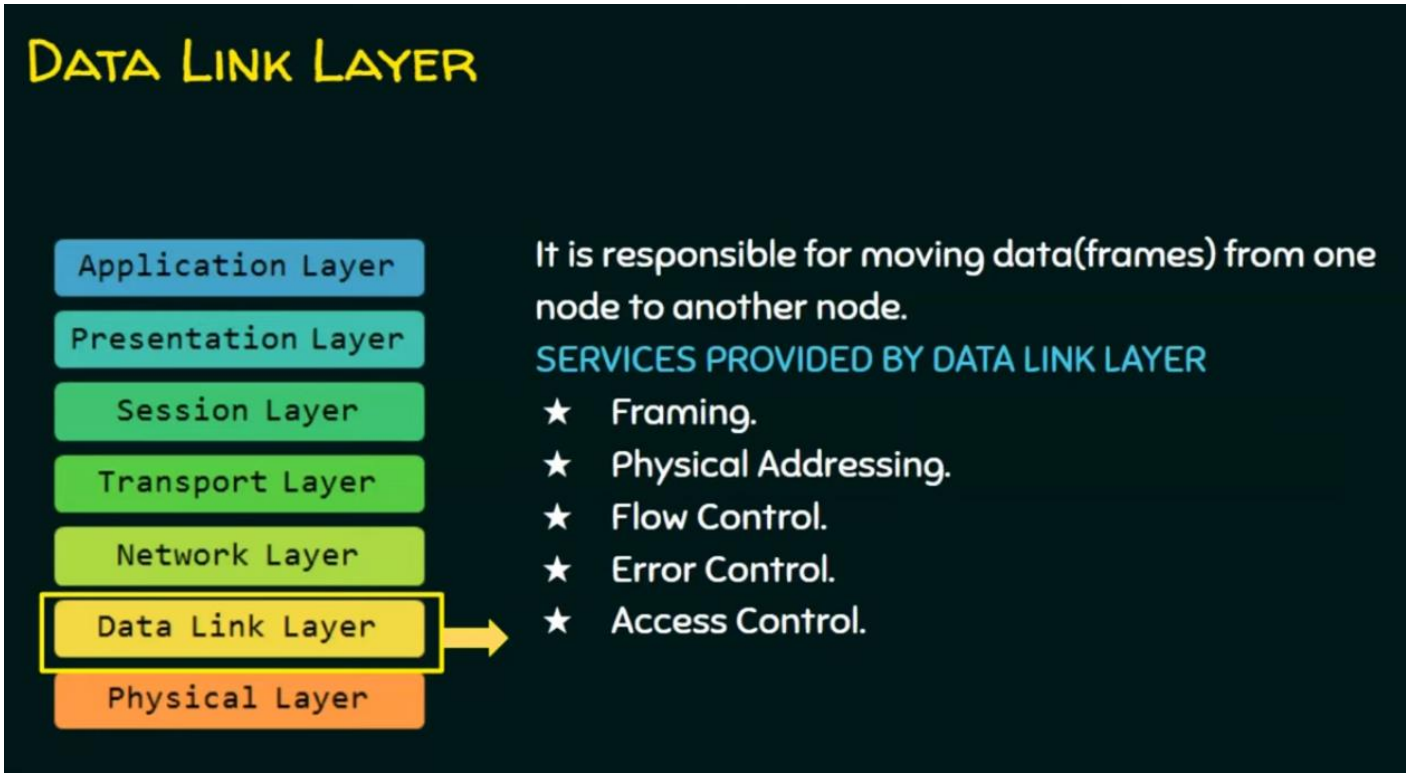
1. **Bluetooth:** have a shorter converge area.
2. **Wi-Fi:** have a medium converge area.
3. **Cellular technology:** have a large converge area.
4. **Satellite:** have the biggest geographical area.

2.5.1.4 Line configuration

Line configuration service provide by the physical layer, it ensures that two nodes must be connected to the same link at the same time. There are two type of line configuration: One-to-one connection and Multi-point connection.

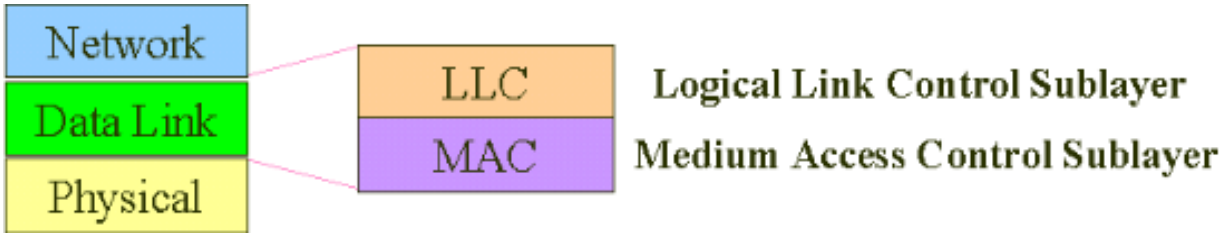
2.5.2 Data Link Layer:

Data link layer is the second layer on the OSI reference, it guaranteed the transmission of data from node to another with control of errors.



2.5.2.1 Data Link Sub-layers:

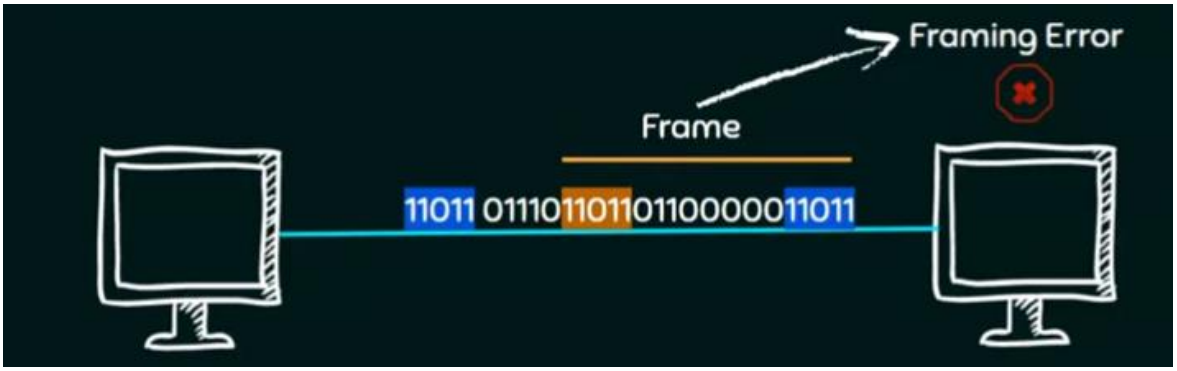
Data link Layer have two Sub-layers Logical Link Control and Medium Access Control.



2.5.2.2 Data Link Services:

- **Framing**

  - **Definition:**
    Framing protocol takes the data packet from the previous layer (network layer) and adds header and trailer to separate between frames and define the start and the end of the frame transmitted by the sender, the receiver will be able to detect the size of data frame with these informations. The sender and receivers must define the rules of framing (for example. This code 110011 is the header and trailer) before the transmission.
  - **Framing error:**
    It is when the rules code appears in the transmitted data frame, in this case it uses framing approaches protocols Bit Oriented and Byte Oriented and Clock based framing.



- **Bit Oriented protocol**

It views the frame as a collection of bits, data is transmitted as a sequence of bits that can be interpreted in the upper layers both as text as well as multimedia data. The popular bit-oriented protocol is: High-level Data Link Control (HDLC).

- ❖ **HDLC:** the beginning sequence and the ending sequence are the HDLC header and trailer.

- The header contains the MAC address and control field.
- CRC contain the Cyclic Redundancy check (error detection).

Types of HDLC frames:

- I-frame: when the 1st bit is 0 it means that the frame handles an information.

- S-frame: when 1st two bits are 10 it means that we have a supervisory frame, this case has some role in error control and flow control mechanism.

- U-frame: 1st two bits are 11 it means Un-numbered frame, it's for doing miscellaneous activities.

Bit stuffing protocol (on HDLC): this protocol solves the framing problem, the method is by adding 0's in the data after every N's ones (for example if the HDLC beginning and ending sequence is 01111110, this protocol will add 0 after every consecutive five ones by the sender and delete them by the receiver.

- **Byte Oriented protocol**

Here each frame is viewed as a collection of bytes (characters) rather than bits, It also known as characters oriented protocol. The popular byte-oriented protocols are: Binary synchronous communication protocol (BSCP) and Digital Data Communication Message Protocol (DDCMP) and Point-to-Point protocol (PPP).

Character stuffing protocol (used on BSCP and PPP) is the process that can solves the framing problem of adding one extra byte whenever there is a flag sequence appear in the payload.

Count field (used on DDCMP) is by sending how many byte are contained in the frame body, one danger with this approach is that if transmission error could corrupt the count field then the end of the frame would not be correctly detected by the receiver.

- **Clock Based Framing**
  The third approach to framing is the clock-based framing. We have Synchronous Optical Network protocol (SONet).

➢ **Physical Addressing**

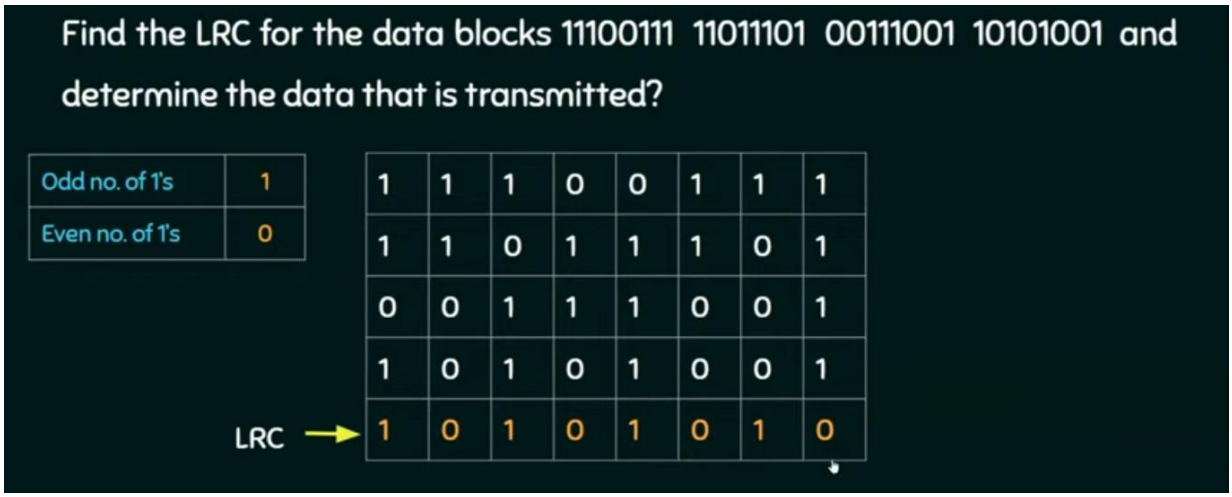
➢ **Error control**

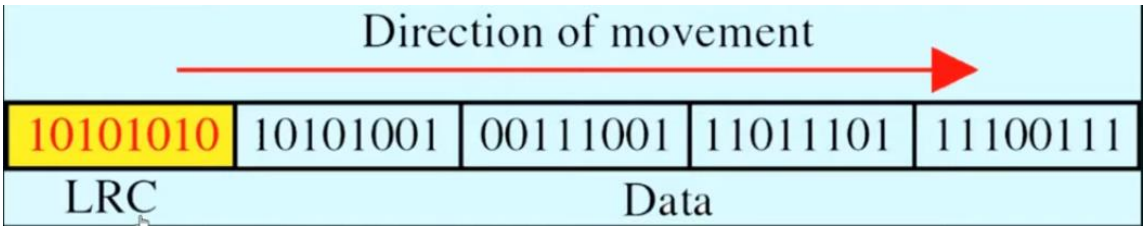
1. **Error detection**

Vertical Redundancy Check (VRC) it can detect only single bit error by sending header of 1 bit (if header is 1 it's mean that the number of 1's in data is odd and vice versa, so receiver can check data and detect the error).

Longitudinal Redundancy Check (LRC) it calculates the number of 1's in each bit position for each byte, if this number is odd w put 0 and vice versa until the last bit position of the LRC byte. This LRC byte will be sent as a header, and the receiver check errors using this header information.

We have this example of LRC:





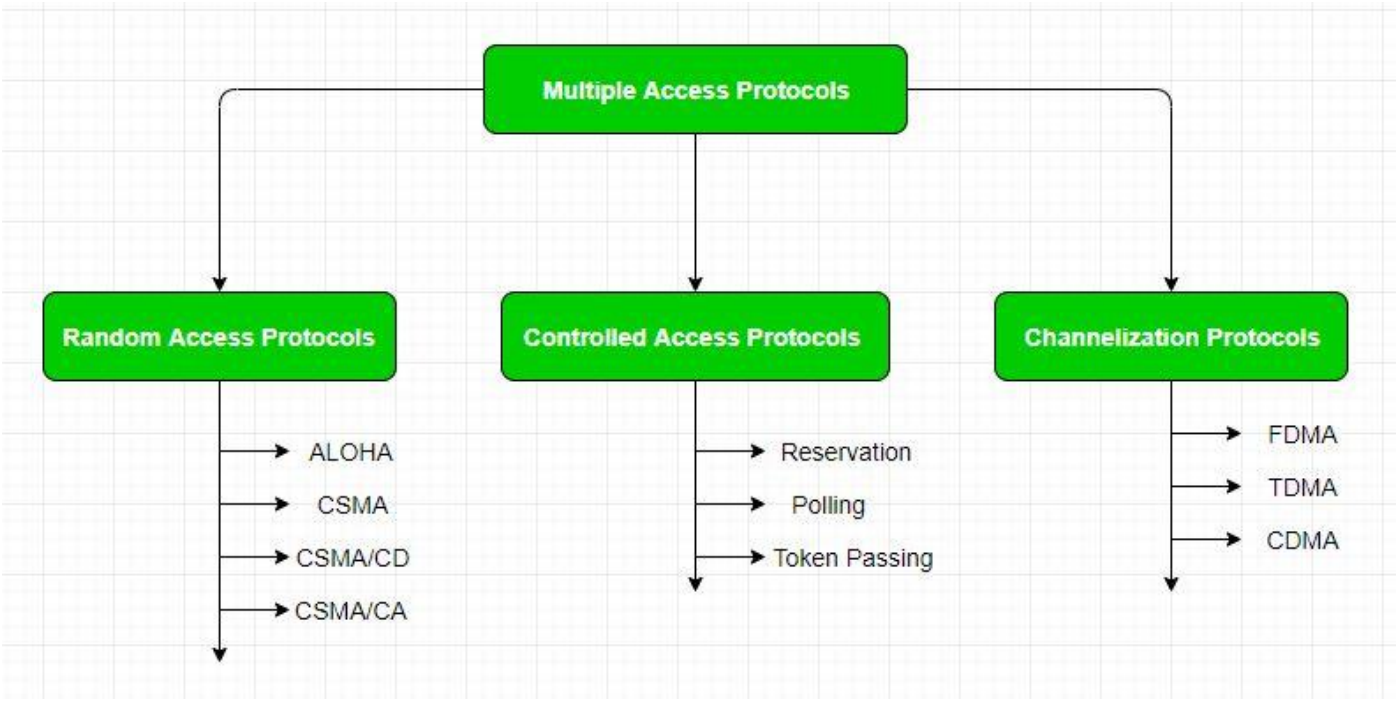
Checksum and Cyclic Redundancy Check (CRC) these two protocols are also using calculation functions to detect errors.

2. **Error correction**

➢ **Access control**

When two nodes sent data in the same time it leads to collision. Access control is used on controlling and managing accesses of sending and receiving to avoid data collision and ensure data transmission.

There are multiple access protocols:

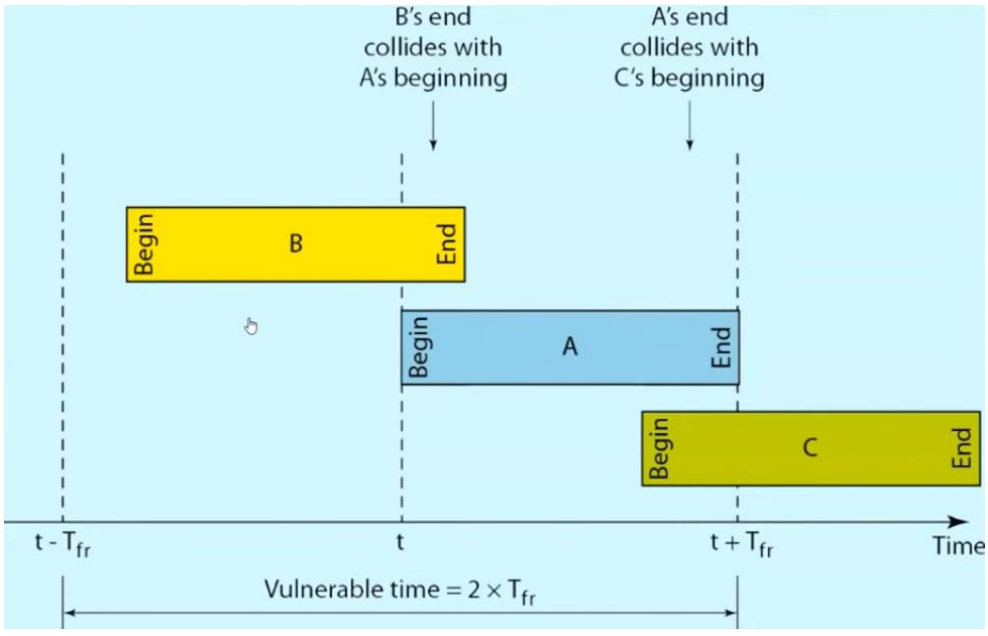


I. Random Access Protocols:

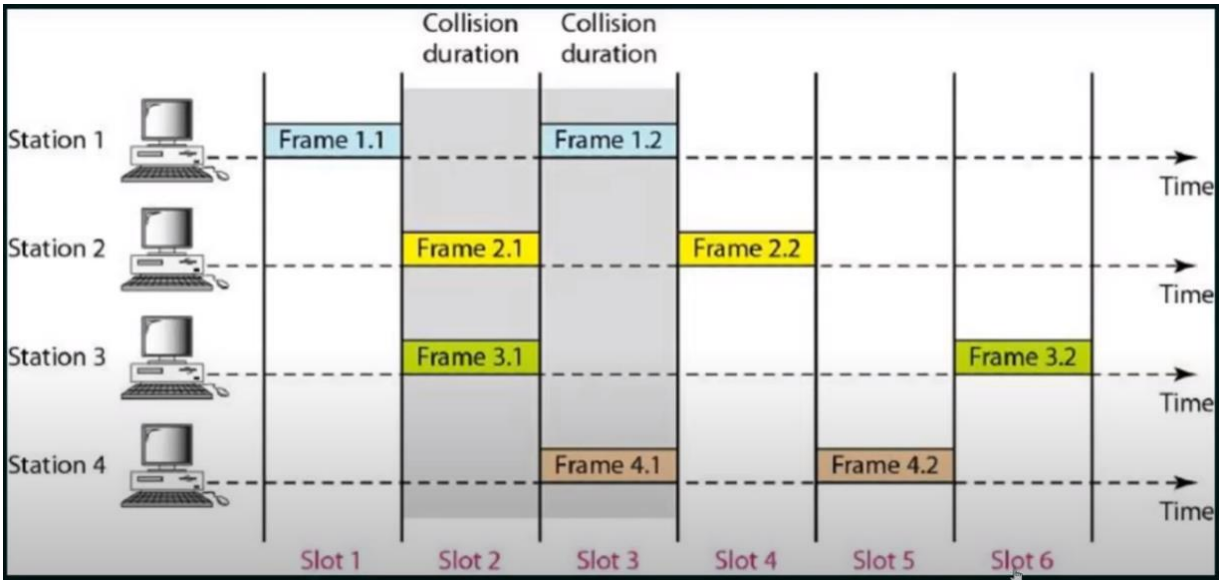
ALOHA

- **Pure ALOHA** allows stations to transmit whenever they have data to be sent. When a collision it happens (acknowledgement doesn't come), the station (sender) waits for a random amount of time called back-off time and re-sends the data. Since the different stations wait for different amount of time, the probability of further collision decreases.

Vulnerable time = **2* Tf**
where Tf is the time of transmission of one frame
Throughput = **G * exp(-2*G)**
where G is the number of stations wish transmits in the same time.



- **Slotted ALOHA** it was developed to improve the efficiency of pure ALOHA as the chances of collision in pure ALOHA are high. Slotted ALOHA have the same principle as Pure ALOHA but here the time of the shared channels is divided into discrete time intervals called slots. So, any station can transmit the data at the beginning of any time slot.



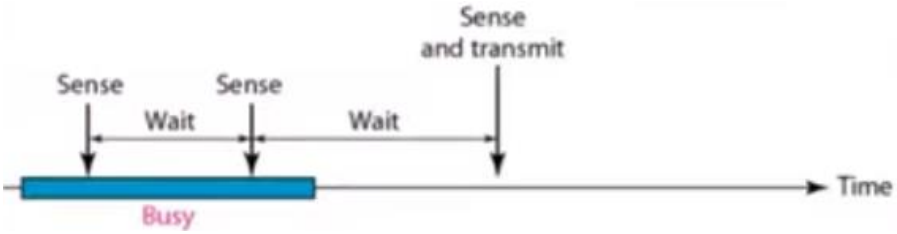
Vulnerable time = **frame transmission time**

Throughput = **G** * **exp**(-**G**)

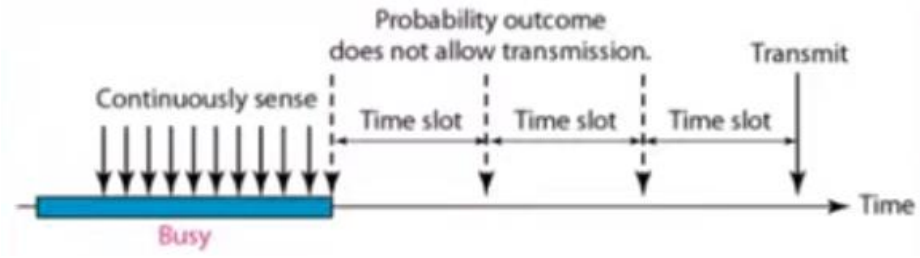
where G is the number of stations wish transmits in the same time.

- **CSMA:** it senses the transmission medium for idle or busy continuously and if the transmission is idle, it transmits data immediately.

- **CSMA/CD:** it senses the transmission medium if it's idle or busy and if the transmission is idle, it transmits data immediately. Otherwise, if it's busy it waits for a random period then check the transmission line, this cycle will be repeating again until it senses that the line is idle, then it transmits data. This protocol called 1-persistant because, after transmission applied immediately with a probability of 1.

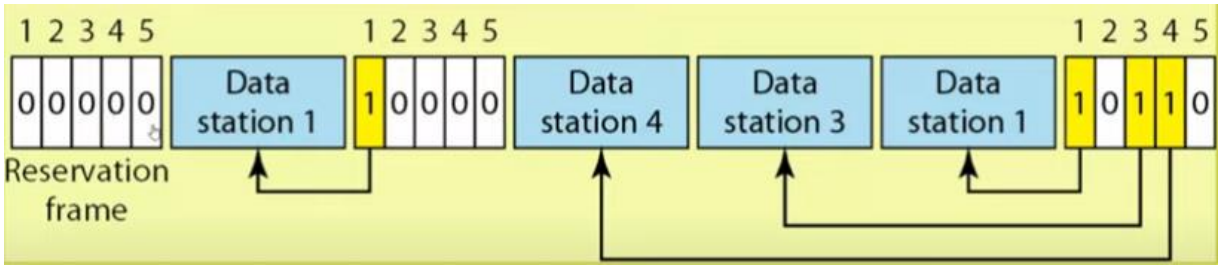


- **CSMA/CA:** The same protocol as CSMA/CD, the difference is the probability of transmitting, and this protocol is called P-persistent.

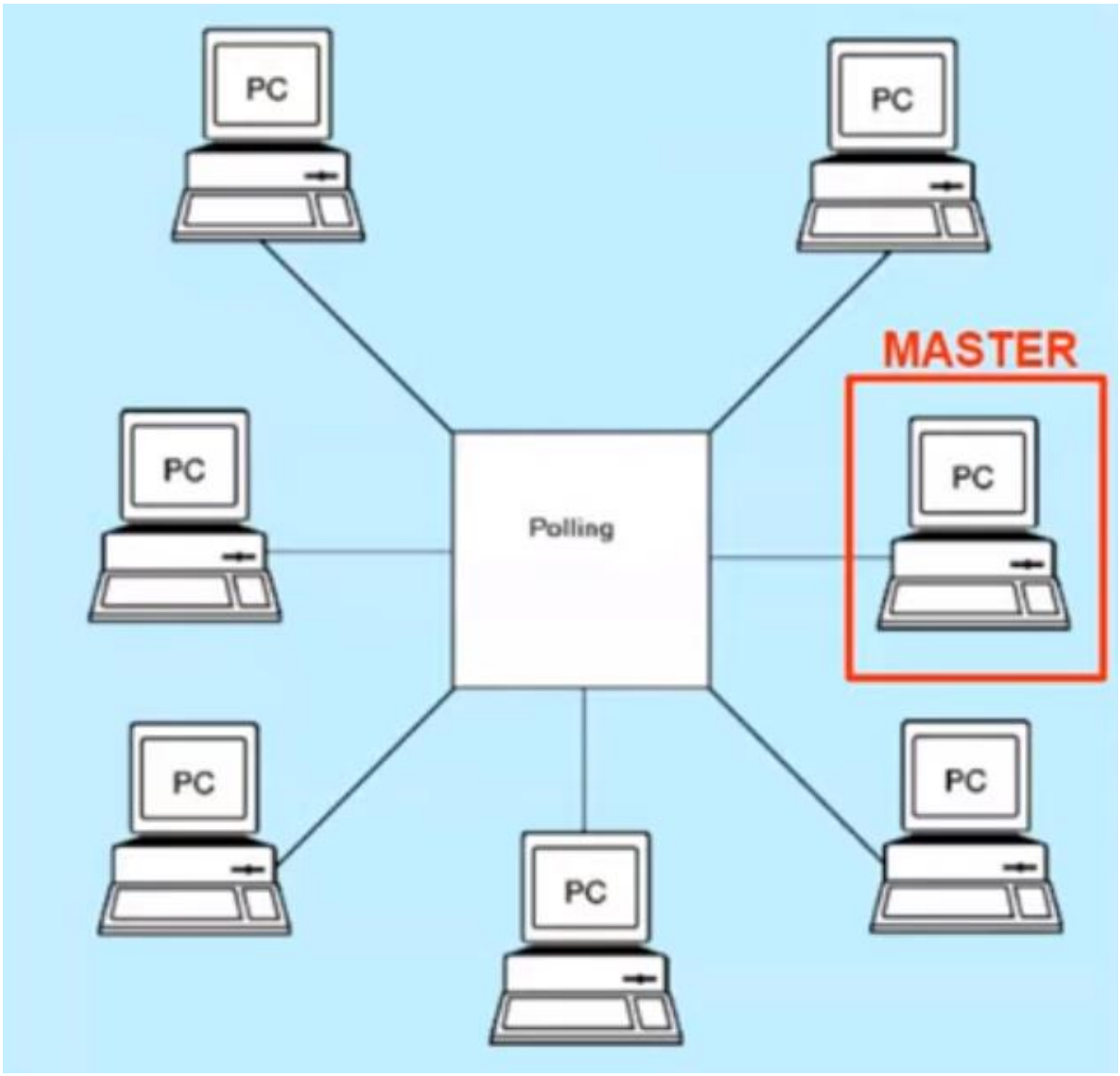


II. Controlled Access Protocols:

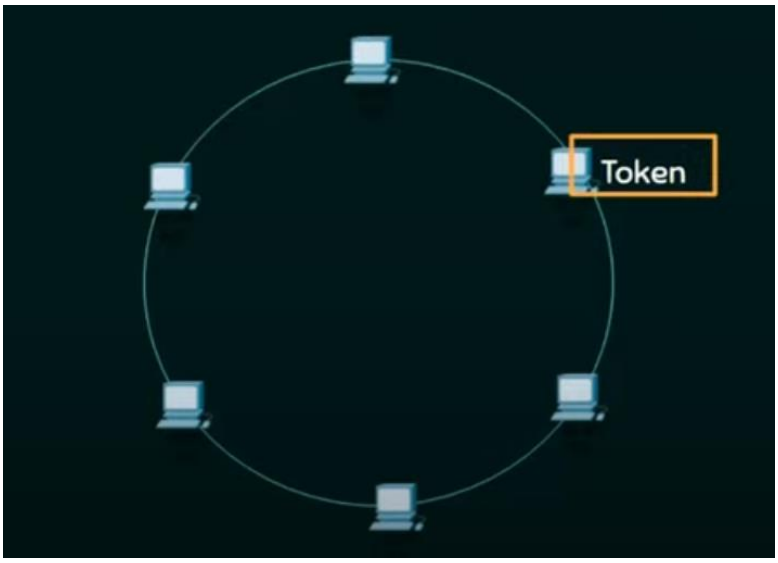
- **Reservation** every station needs to make a reservation before sending data.



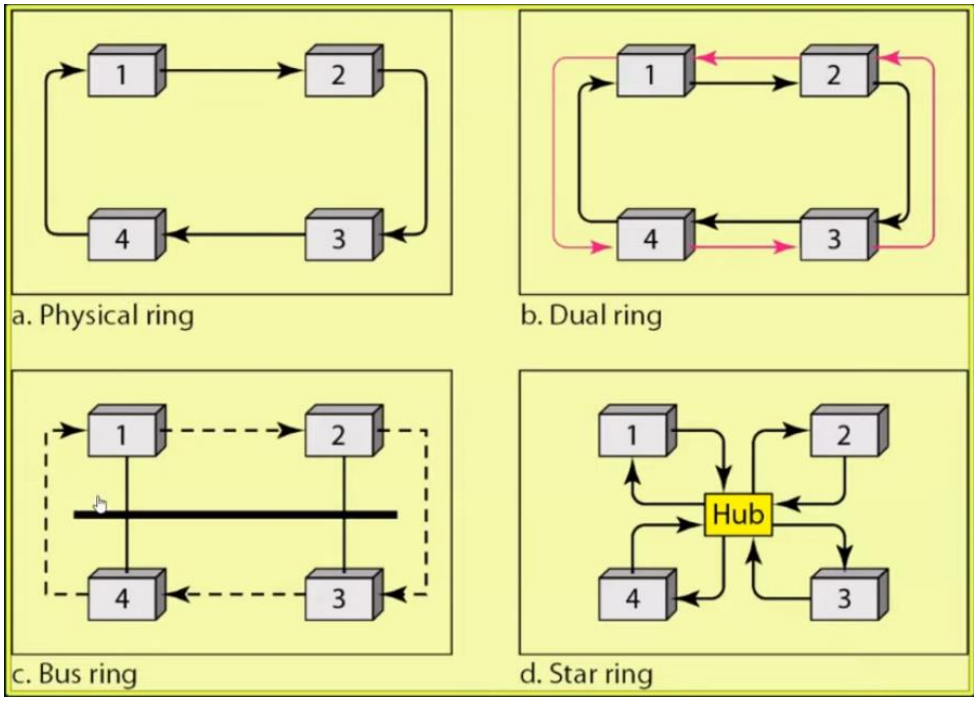
- **Polling** this protocol requires one of the nodes to be designed as a Master node (Primary station), the master manages and gives access to stations (one by one). This protocol eliminates the collision. But it increases the time because of the additional delay (to notify the node that it can transmit).



- **Token Passing:** it uses a packet called a token is passed between nodes to authorize that node to communicate. In contrast to polling access, there is no pre-defined "master" node.

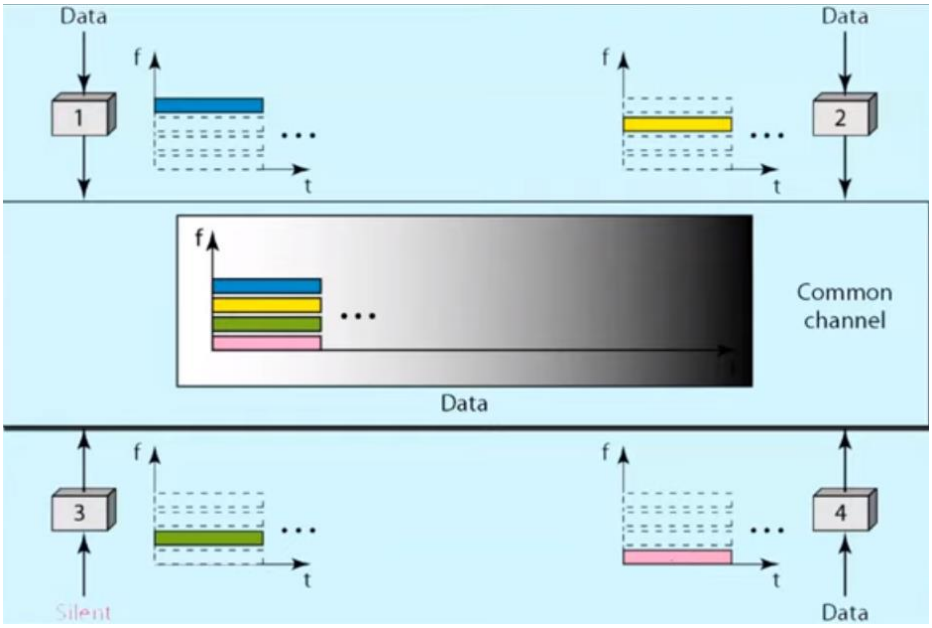


This protocol can applied on different topologies.

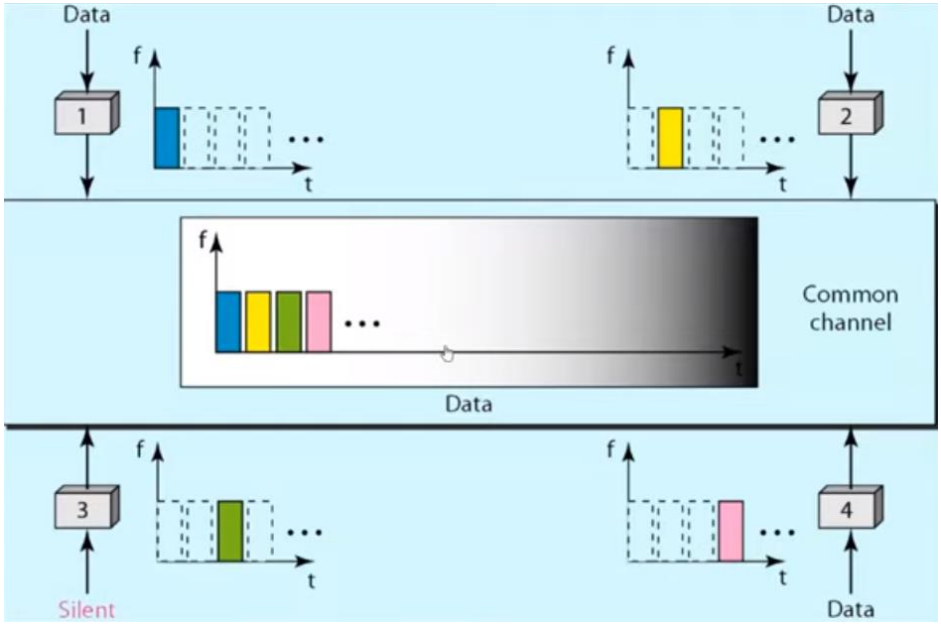


III. **Channelization** is a multi-access method in which the available bandwidth of a link is shared in time, frequency or code between different stations.
Multiplexing: or sharing the bandwidth of a link, in another sense multiple signals are combined together thus travel simultaneously in a shared medium.

- **FDMA (Frequency Division Multiple Access)** the available bandwidth of the common channel is divided into bands that are separated by guard bands, and shared by all the stations. The FDMA is a data link layer protocol that uses FDM at the physical layer.



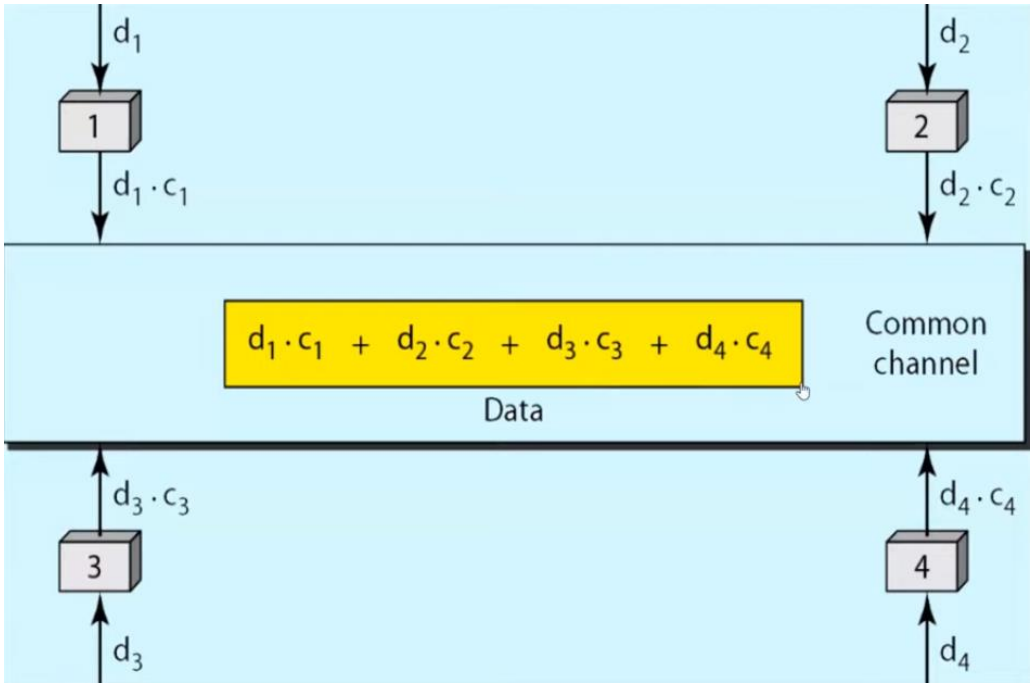
TDMA (Time Division Multiple Access) The bandwidth is just one channel that is time shared between different stations.



CDMA (Code Division Multiple Access) one channel carries all transmission simultaneously. There is no time sharing and all stations can send data simultaneously, and only one frequency channel occupies the entire bandwidth of the link.

The protocol is by multiply a code by a signal and this code must have the following properties:

1. If we multiply each code by another, we get 0.
2. if we multiply each code by itself, we get the number of stations.



Example: Data of the station 1 = (d1*c1 + d2*c2 + d3*c3 + d4*c4) * c1 = 4*d1

- **Flow control**

Flow control is a speed matching mechanism that coordinate the amount of data that can be sent before receiving an acknowledgement, receiver has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. Receiver must inform the sender before the limits are reached and request the transmitter to send fewer frames or stop temporarily. Flow control uses two types of protocols Noiseless channels and Noisy channels.

- **Noiseless channels protocols**
  - **Simplest**
  - **Stop-and-wait**

  It provides unidirectional data transmission with flow control facilities but without error control facilities, the sender transmits one frame, then it waits for an acknowledgement from the receiver before transmitting the next frame. The receiver receives and consume data packet then it must send an acknowledgment to the sender.

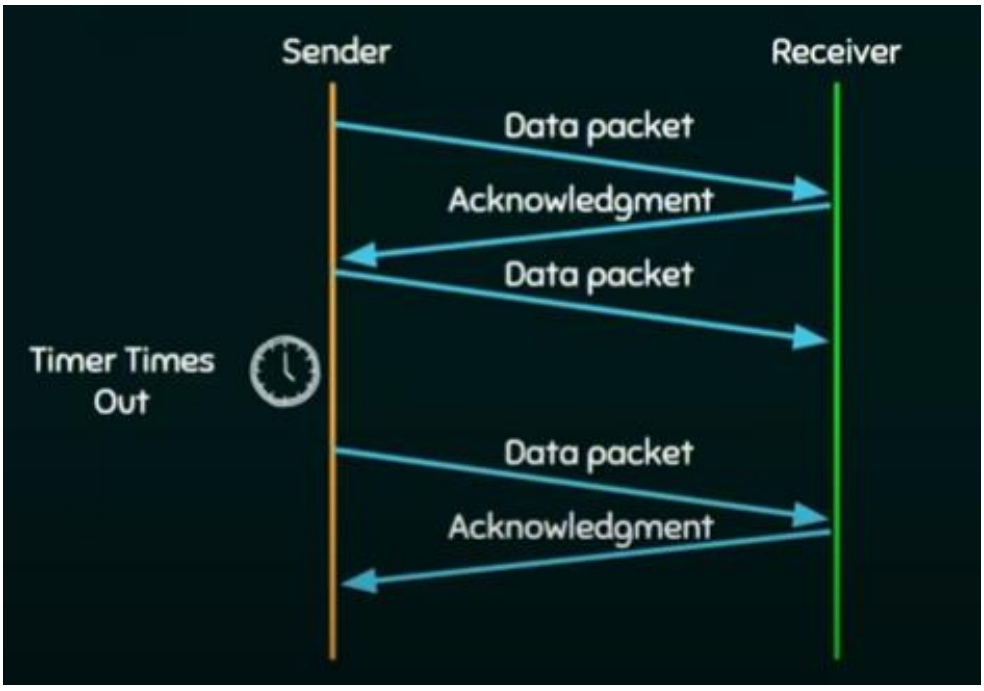
  There are some problems with this protocol:

  - Sender or receiver waits for acknowledgement for an infinite amount of time due to lost of data.

- **Noisy channels protocols**

- **Stop-and-wait ARQ**

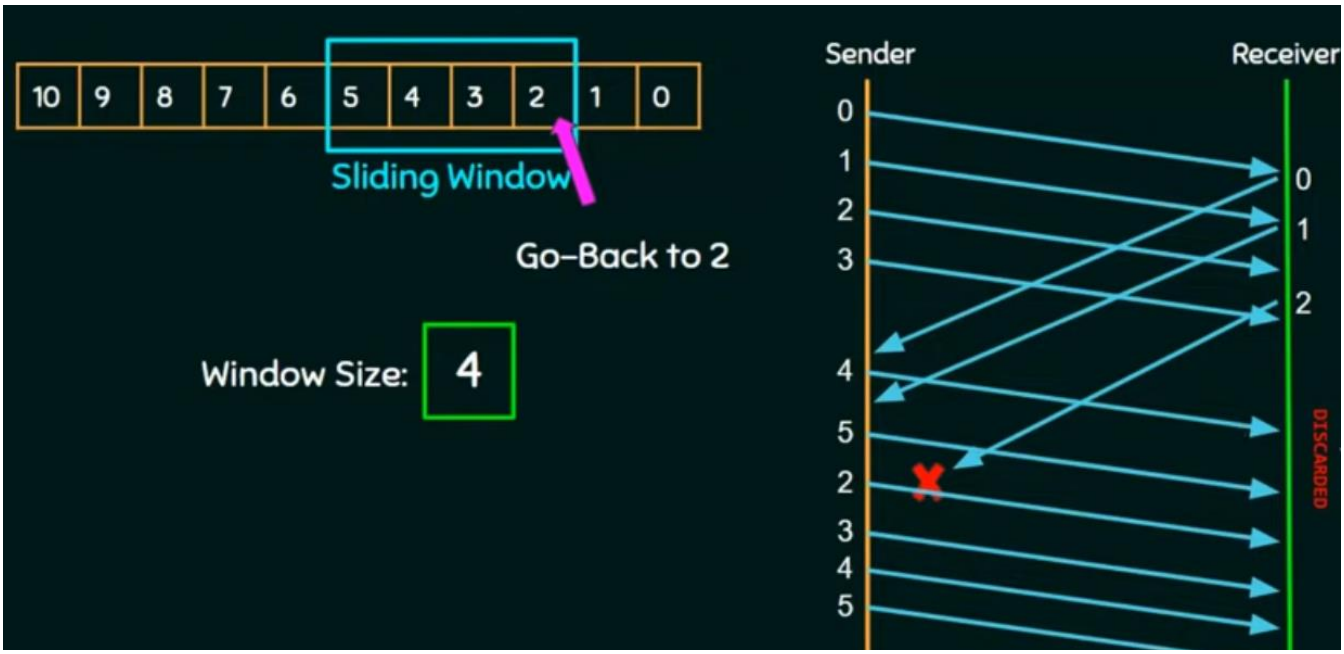
  In this protocol, after transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame. if the acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the original frame.



  Drawbacks of this method are: One frame at a time, poor utilization of bandwidth, poor performance.

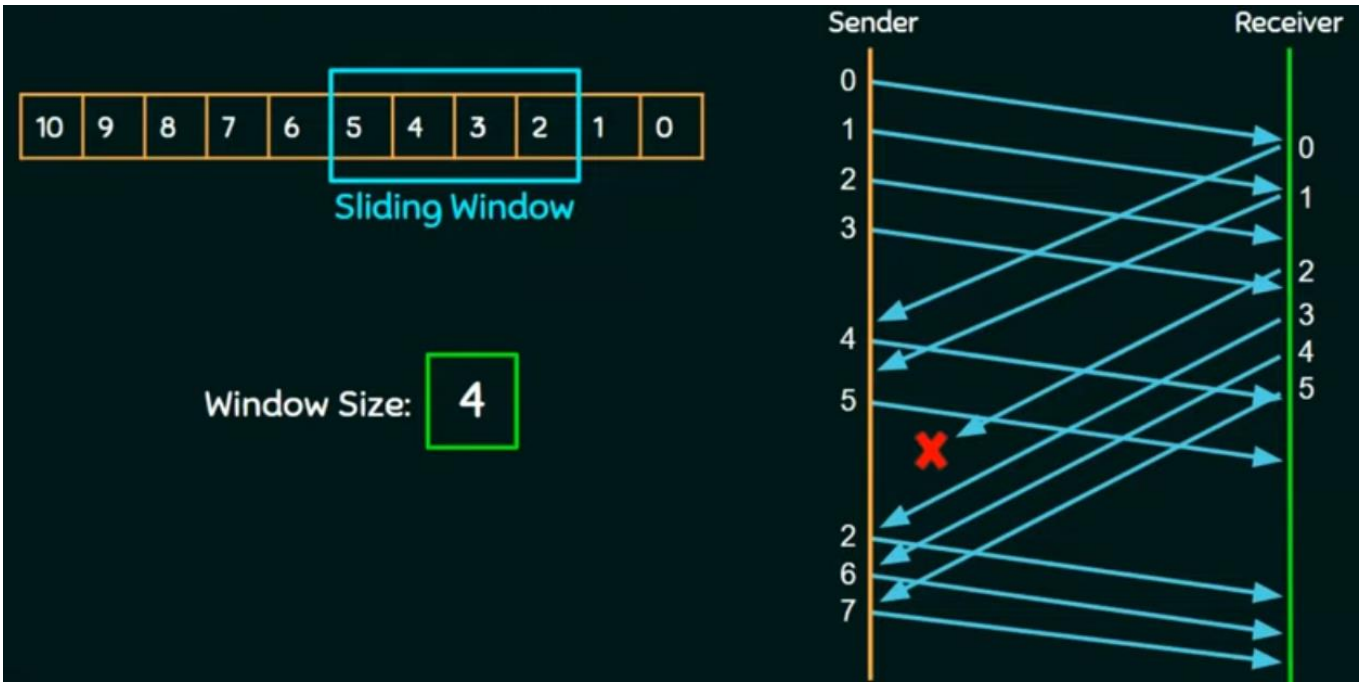
- **Go-back-N-ARQ**

The sender can send multiple frames before receiving the first acknowledgement. The number of frames that can be sent depends on the window size (N is the window size) of the sender. If the ack of a frame is not received within an agreed upon time, the sender retransmit all the frames in the current window.



- **Selective Repeat ARQ**

In this protocol, only the erroneous or lost frames are retransmitted, while correct frames are received and buffered. The receiver when keeping track of sequence numbers, buffers the frames in memory and sends non acknowledgement for only frame which is missing or damaged. The sender will send/retransmit packet for which NACK (non-acknowledgement) is received.



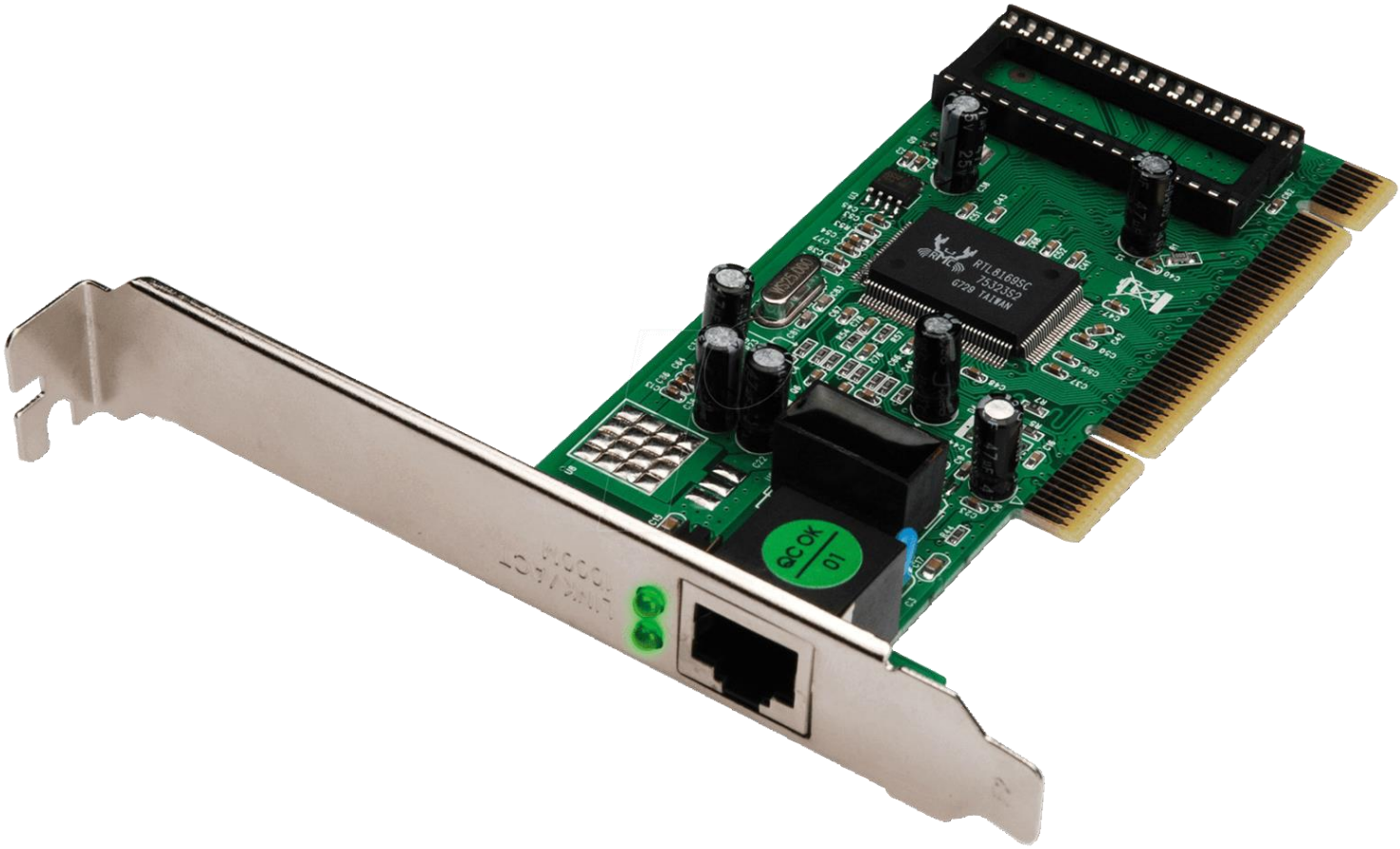
2.5.2.3 Ethernet:

Ethernet is a protocol that uses Data Link layer as services, and physical layer as technologies, it's the family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards and it supports data bandwidth from 10 to 100,000 Mbps.

- **Ethernet adapter:** or Ethernet card, it uses commonly an algorithm called Ethernet Media Access Control (MAC) which is implemented in Hardware on the network adaptor.

Access method of Ethernet: CSMA/CD (1-persitant access control protocol) (Carrier Sense Multiple Access with collision detection).

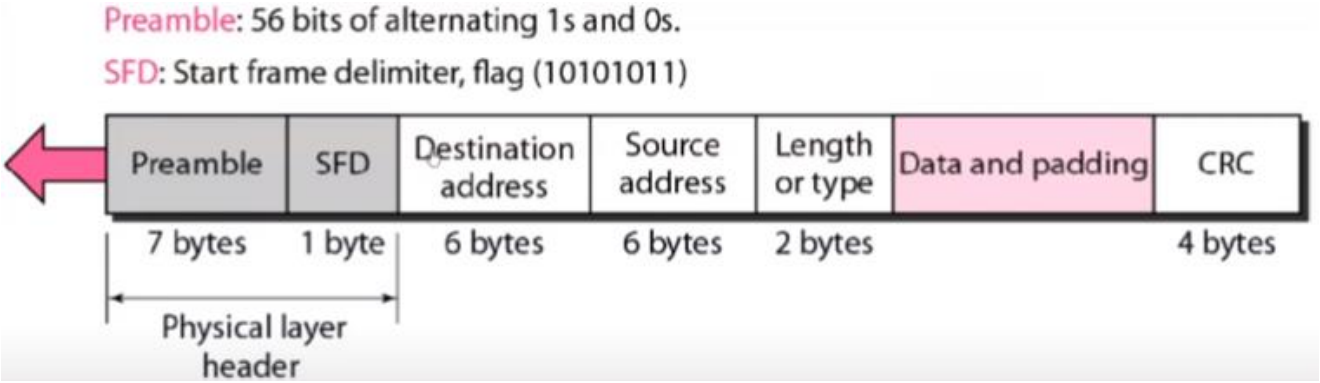
Encoding method: Manchester Encoding Techniques for converting data into signals.



- **Ethernet frame format**

Basic frame format which is required for all MAC implementation is defined in IEEE 802.3 standard. Though several optional formats are being used to extend the protocol's basic capability.

Ethernet frame starts with Preamble and SFD, both works at the physical layer. Ethernet header contains both Source and Destination MAC address, Data and padding are the output frame from the network layer. And the last field is CRC which is used to detect the error.



- **PREAMBLE** – Ethernet frame starts with 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization. Preamble indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
- **Start of frame delimiter (SFD)** – This is a 1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of the frame, which is the destination address. Sometimes SFD is considered the part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.
- **Destination Address** – This is 6-Byte field which contains the MAC address of machine for which data is destined.
- **Source Address** – This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.
- **Length** – Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.
- **Data** – This is the place where actual data is inserted, also known as Payload. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e., 46 bytes, then padding 0's is added to meet the minimum possible length.
- **Cyclic Redundancy Check (CRC)** – CRC is 4 Byte field used to error detection. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field.

Notes:

- ✓ Size of frame of Ethernet IEEE 802.3 varies 64 bytes to 1518 bytes including data length (46 to 1500 bytes).
- ✓ The least significant bit of the first byte defines the type of address, if the bit is 0, the address is Unicast, otherwise, it's multicast. If all the bits are 1's, then it is broadcast.
- **Ethernet Transmitter algorithm: (Ethernet Media Access Control)**

When the adapter has a frame to send and the line is idle, it transmits the frame immediately. The upper bound of 1500 bytes in the message means that the adapter can occupy the line for a fixed length of time. when the adapter has a frame to send and the line is busy, it waits for the line to go idle and then transmits immediately, the ethernet is said to be CSMA/CD 1-persistant protocol because an adaptor with a frame to send transmits with probability 1 whenever a busy line goes idle.

Since there is no centralized control, it is possible for two (or more) adaptors to begin transmitting in the same time, either because both found the line to be idle, or both had been waiting for a busy line to become idle, when this happens, the two (or more) frames are said to be collide on the network. Since Ethernet supports collision detection, each sender is able to determine that a collision is in progress, at the moment an adaptor detects that its frame is colliding with another, it first makes sure to transmit a 32-bits jamming sequence and then stops transmission. Thus, a transmitter will minimally send 96 bits in the case of collision 64-bits (preamble & SFD) + 32-bits (jamming sequence).

- **Exponential Backoff:**

Once an adaptor had detected a collision, and stopped its transmission, it waits a certain amount of time and tries again, each time the adapter fails to transmit, it doubles the amount of time it waits before trying again. This strategy of doubling the delay interval between each retransmission attempt is known as Exponential backoff.

- **Ethernet advantages:**
  - ✓ Ethernet is the most widely used LAN technology.
  - ✓ Ethernet is relatively inexpensive.
  - ✓ In Ethernet, all the nodes have the same privileges. It does not follow client-server architecture.
  - ✓ Maintenance and administration are simple.
  - ✓ The cable used to connect systems in ethernet is robust to noise.
  - ✓ As it is robust to the noise, the quality of the data transfer does not degrade. the data transfer quality.
  - ✓ With latest version such as gigabit ethernet, the transfer speeds in Gbps have become possible.
- **Ethernet disadvantages:**
  - ✓ Under heavy loads, too much of the network's capacity is wasted by collision.
  - ✓ It does not good for real-time application and interactive application.
  - ✓ As the network cannot set priority for the packets, it is not suitable for a client-server architecture.
  - ✓ For interactive applications, dummy data have to be fed to make the frame size 46 Bytes which is mandatory.
  - ✓ After receiving a packet, the receiver doesn't send any acknowledgement.
- **Ethernet categories:**

CATEGORY	SHIELDING	MAX TRANSMISSION SPEED (AT 100 METERS)
Cat 3	Unshielded	10 Mbps
Cat 5	Unshielded	10/100 Mbps
Cat 5e	Unshielded	1000 Mbps / 1 Gbps
Cat 6	Shielded or Unshielded	1000 Mbps / 1 Gbps
Cat 6a	Shielded	10000 Mbps / 10 Gbps
Cat 7	Shielded	10000 Mbps / 10 Gbps
Cat 8	Shielded	Up to 40 Gbps

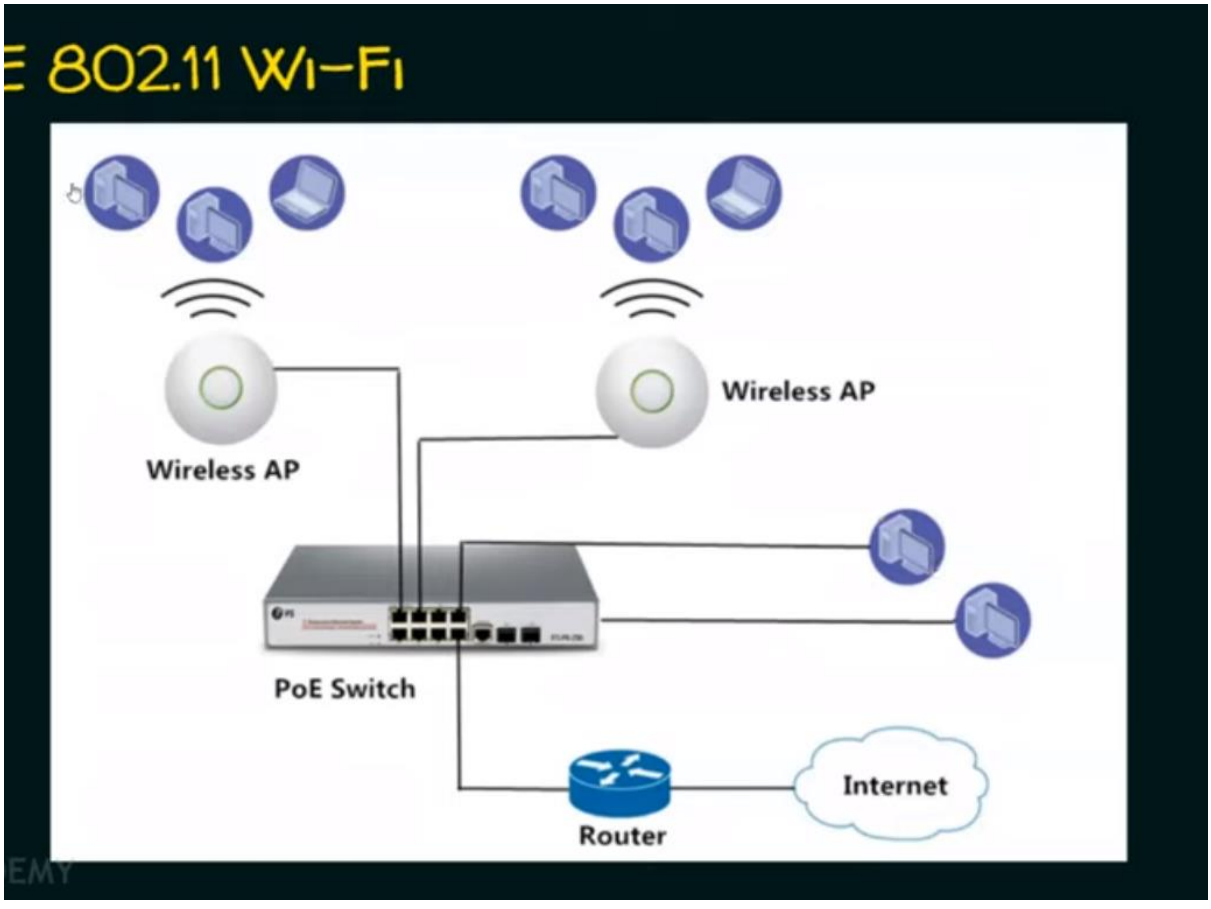
2.5.2.4 IEEE 802.11 Wireless Fidelity (Wi-Fi):

Wi-Fi is a protocol that uses Data Link layer as services, and physical layer as technologies, it's a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby digital devices to exchange data by radio waves. These are the most widely used computer networks in the world, used globally in home and small office networks to link desktop and laptop computers, tablet computers, smartphones, smart TVs, printers, and smart speakers together and to a wireless router to connect them to the Internet, and in wireless access points in public places like coffee shops, hotels, libraries and airports to provide the public Internet access for mobile devices.

802.11 uses widely 5 GHz radio band (High Frequency) which has 23 overlapping channels but there are also other frequencies. Access method of IEEE 802.11 Wi-Fi: CSMA/CA (Carrier Sense Multiple Access with collision avoidance)

- **Wireless Router:**

A wireless router, also called a Wi-Fi router combines the networking functions of a wireless access point and a router. A router connects local networks to other local networks or to the Internet. A wireless access point connects devices to the network wirelessly (by the air using radio frequencies).



Wireless Router = Router + Switch + Wireless APs

- **Wi-Fi Protocols:**

Year	WiFi Versions/Protocols	Old name	New name
1999	First Generation	WiFi 802.11b	WiFI 1
1999	Second Generation	WiFi 802.11a	WiFi 2
2003	Third Generation	WiFI 802.11g	WiFi 3
2009	Four Generation	WiFi 802.11n	WiFi 4
2014	Fifth Generation	WiFi 802.11ac	WiFi 5
2019	Sixth Generation	WiFi 802.11ax	WiFi 6

Protocol	Frequency	Channel Width	Maximum data rate (theoretical)
802.11 ax	2.4 or 5GHz	20, 40, 80, 160MHz	2.4 Gbps
802.11 ac wave2	5 GHz	20, 40, 80, 160MHz	1.73 Gbps
802.11 ac wave1	5 GHz	20, 40, 80MHz	866.7 Mbps
802.11n	2.4 or 5 GHz	20, 40MHz	450 Mbps
802.11g	2.4 GHz	20 MHz	54 Mbps
802.11a	5 GHz	20 MHz	54 Mbps
802.11b	2.4 GHz	20 MHz	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	2 Mbps

- **Modes of Wi-Fi:**
  - **Infrastructure mode:**

In this mode, the access point is a centralized system and there is always a fixed infrastructure. For example, if a device A want to connect with another device B, device A needs always to connect with a fixed AP and then connect to the device B.

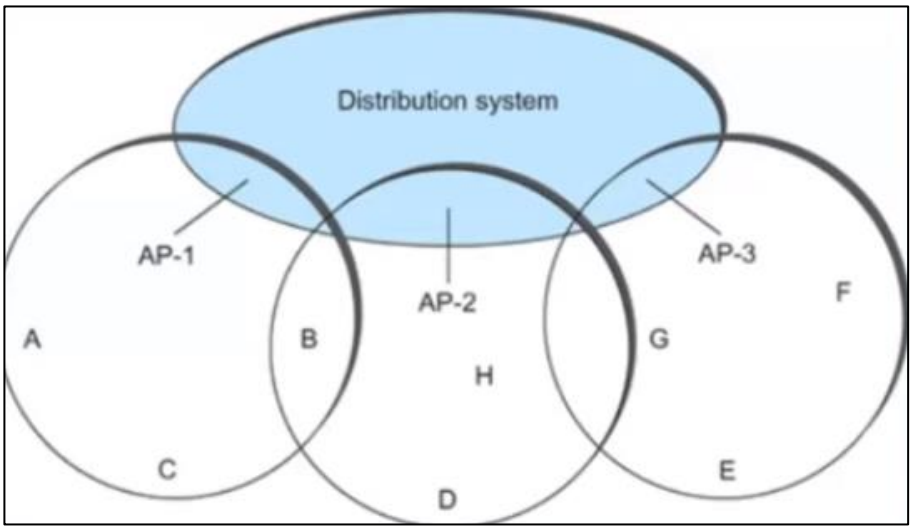
Ad-Hoc or Wi-Fi direct mode:

For Ad-Hoc mode, there are not a fixed infrastructure and we have not a centralized system. For example, if we have a mobile device and it is connected to an AP1 to connect to a device B, it will not always connect with this AP1, it can change connection to another AP that can be available in any moment. Or it can connect directly to the device B.

- **IEEE 802.11 Distribution system:**

802.11 is suitable for an ad-hoc configuration of nodes that may or may not be able to communicate with all other nodes. Nodes are free to move around and the set of directly reachable nodes may change over time.

To deal with this mobility and partial connectivity 802.11 defines additional structures on a set of nodes, instead of all nodes being created equal, some nodes are allowed to move and others are wired network infrastructure, they are called Access Point (AP) and they are connected to each other by a so-called distribution system.



In this example:

We have each node associates itself with one access point.

- Node A communicate with C directly.
- Node A communicate with node E, A first sends a frame to its AP-1 which forwards the frame across the distribution system to AP-3 which finally transmits the frame to E.

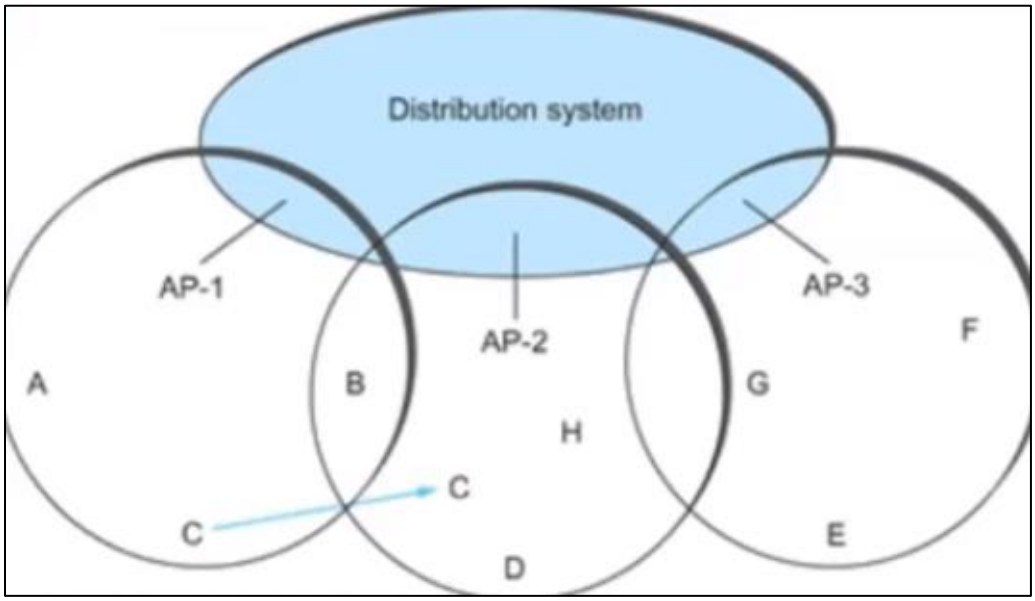
We have each node associates itself with one access point.

- **How the nodes select their AP**

The technique for selecting an AP is called scanning:

- The node sends a Probe frame.
- All APs within reach reply with a Probe Response frame.
- The node selects one of the access points and sends to that AP an association request.
- The AP replies an association response frame.

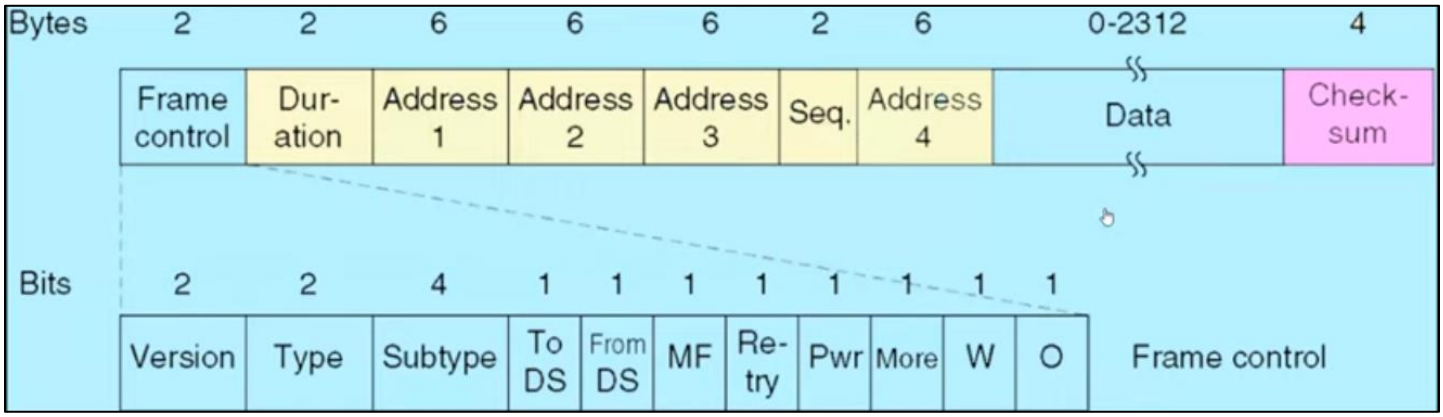
- **When the node becomes unhappy with its current AP:**
  - Because the signal from its current AP has weakened due to the node moving away from it.
  - Whenever a node acquires a new AP, the new AP notifies the old AP of the changes via the distribution system.
- **Type of scanning:**



  - **Active scanning**

    We have the node C moves from the cell serviced by AP-1 to the cell serviced by AP-2, it sends Probe frames and it receives probe responses frame from AP-1 and AP-2, at some point C prefer AP-2 over AP-1, and so it associates itself with that access point. This is called active scanning since the node is actively searching for an access point.
  - **Passive scanning**

    APs sends periodically a beacons frame that advertise the capabilities of the access point, these include the transmission rate supported by the AP, a node select the AP based on its beacon frame. So, the node associate with the better AP that have the better transmission rate.
- **Wi-Fi frame format:**



  - **Frame Control:** it takes 2 bytes starting field composed of 11 subfields. It contains control information of the frame. the subfields are:
    - Protocol version: is a two bits field set to 00, it has been included to allow future versions of IEEE 802.11 to operate simultaneously.

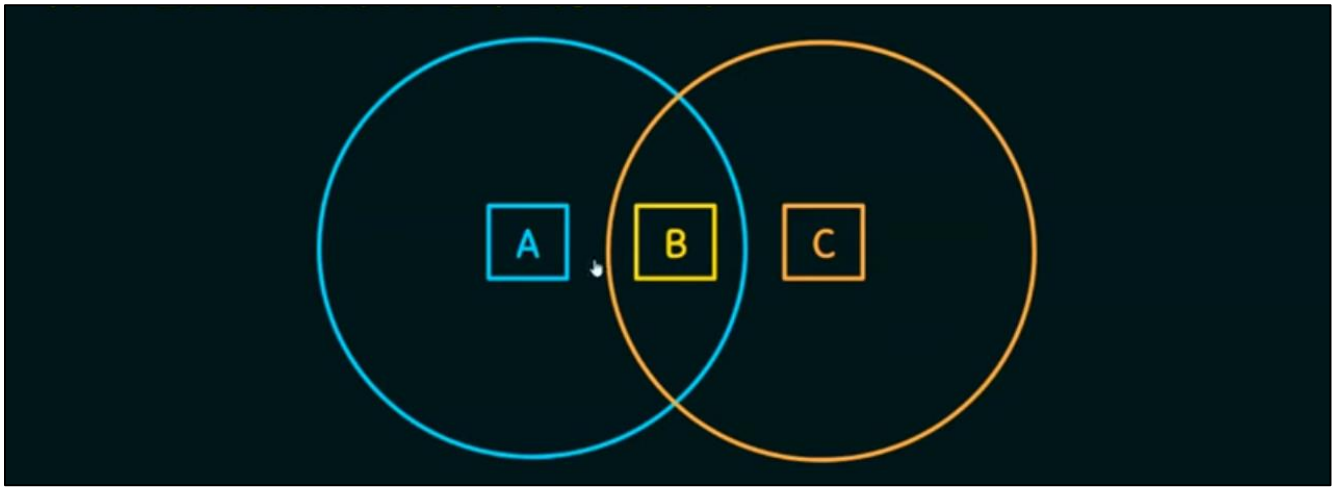
- Type: two bits subfield that specifies whether the frame is a data frame, control frame or a management frame.
- Subtype: it's a four bits subfield states whether the field is a request to send (RTS) or a clear to send (CTS) control frame. For a regular data frame, the value is set to 0000.
- TO DS: A single bit subfield indicating whether the frame is going to the access point (AC), which coordinate the communication in centralized wireless system.
- From DS: a single bit subfield indicating whether the frame is coming from the access point.
- MF: it means more fragments and it's a subfield which when set to 1 indicates that more fragments would follow.
- Retry: A single bit subfield which when set to 1 specifies a retransmission of a previous frame.
- Pwr: Power management is a single bit subfield indicating that the sender is adopting power-save mode.
- More: A single bit subfield showing that sender has further data frames for the receiver.
- W: WEP is a single bit subfield indicating that this is an encrypted frame.
- Order: The last subfield, of one – bit, informs the receiver that to the higher layers the frames should be in an ordered sequence.

- **Duration:** it's a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.
- **Addresses:** these addresses deals with MAC addresses.

To DS	*From* DS	*Address* 1	*Address* 2	*Address* 3	*Address* 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	SendingAP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	SendingAP	Destination	Source

- **Sequence:** It a 2 bytes field that stores the frame numbers. It detects duplicate frames and determines the order of frames for higher layers. Among the 16 bits, the first 4 bits provides identification to the fragment and the rest 12 bits contains the sequence number that increments with each transmission.

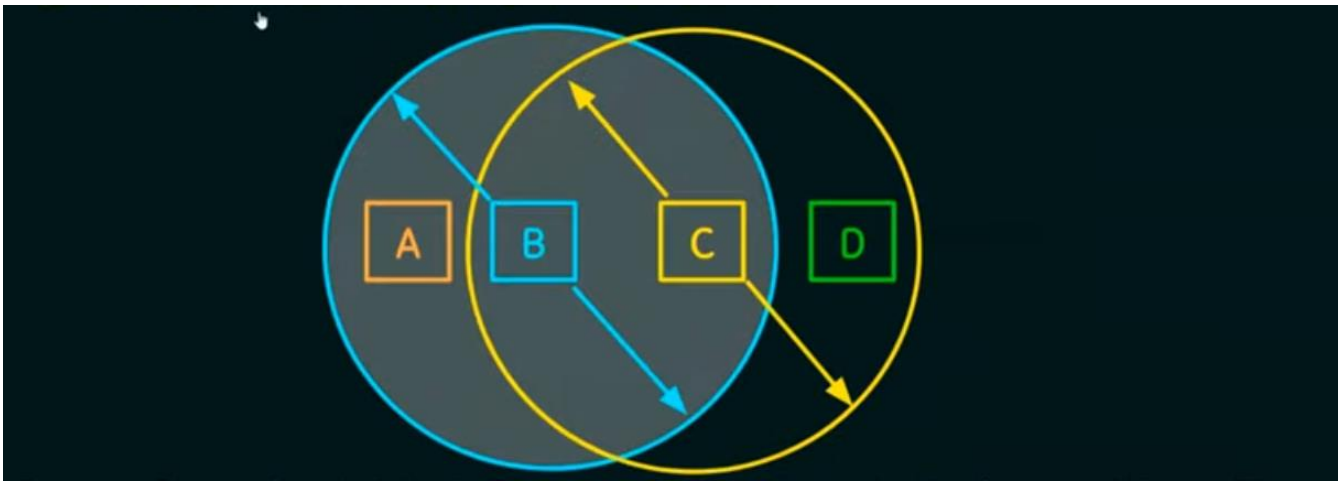
- **Exposed terminal problems:**
  - **Hidden terminal problem:**



A, B, C are three nodes, A and B want to communicate with C, so each one sends it a frame.

- A and C are unaware of each other since their signals do not carry that far.
- Theses two frames collide with each other at B (but unlike an Ethernet, neither A nor C is aware of this collision)
- A and C are said to hidden nodes with respect to each other.

  - **Exposed terminal problem:**



Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.

- It would a mistake for C conclude that it cannot transmit to anyone just because it can hear B's transmission.

- **Solution for these problems**

802.11 addresses these two problems with an algorithm called Multiple Access with Collision Avoidance (MACA).

  - **MACA (Multiple Access with Collision Avoidance)**

- Sender and receiver exchange control frames with each other before the sender actually transmits any data.
- This exchange informs all nearby nodes that a transmission is about to begin.
- Sender transmits a Request include an (RTS) frame to the receiver. The RTS frame includes a field that indicates how long the sender wants to hold the medium. Length of the data frame to be transmitted.

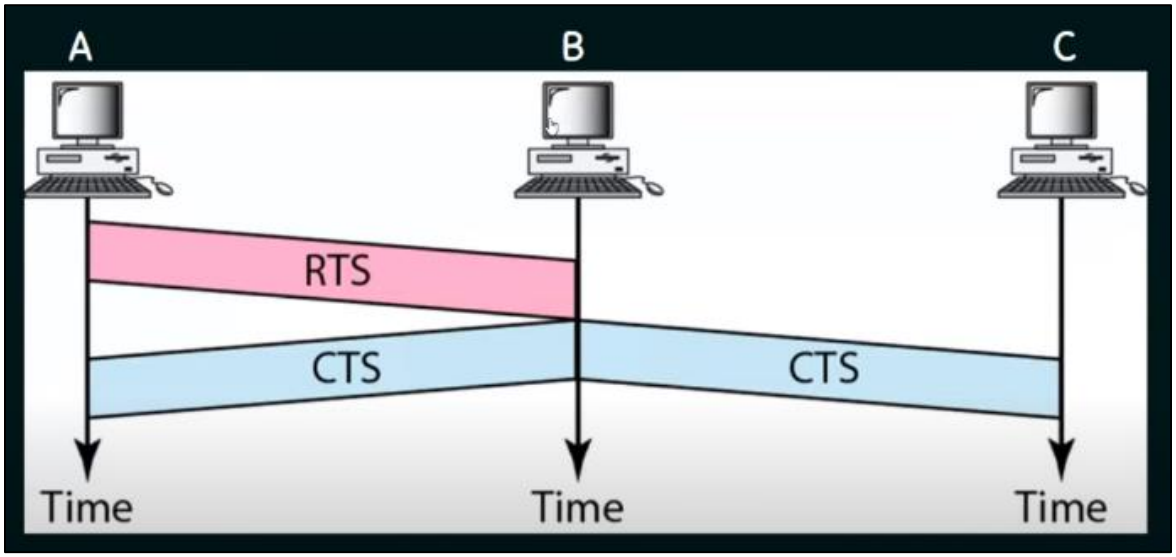
- Receiver replies with a Clear to Send (CTS) frame. This frame echoes this length field back to the sender
- Any node that sees the CTS frame knows that, it's close to the receiver and it cannot transmit for the period of time it takes to send a frame of the specified length.
- Any node that sees the RTS frame but not the CTS frame, it can not interact with the receiver and it's free to transmit.
-

➢ **MACAW (for Wireless LANs)**

The idea of using acknowledgement (ACK) in MACA is Proposed in MACAW. Receiver sends an ACK to the sender after successfully receiving a frame including data. All nodes must wait for this ACK before trying to transmit another packet of frame including data.

If two or more nodes detect an idle link and try to transmit an RTS frame at the same time:

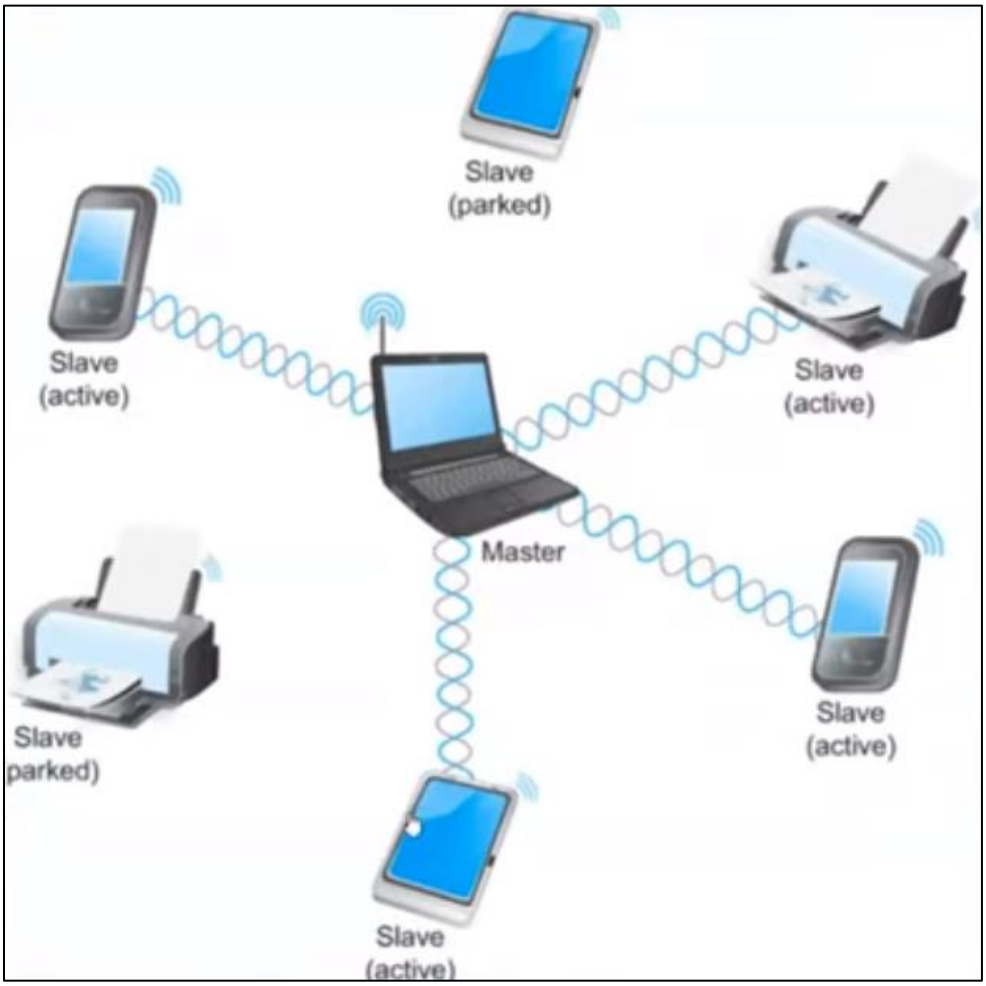
- Their RTS frame will collide with each other.
- 802.11 does not support collision detection.
- So, the senders realize the collision has happened when they do not receive the CTS frame after a period of time.
- In this case, they each wait a random amount of time before trying again.
- The amount of time a given node delays is defined by the same Exponential backoff algorithm used in Ethernet.



2.5.2.4 Bluetooth:

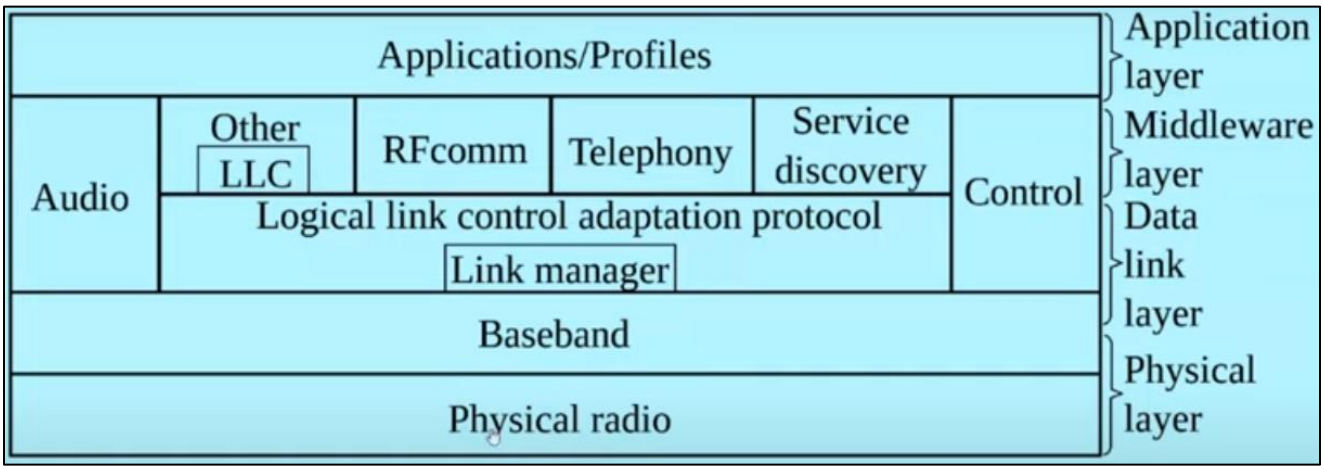
Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waved in the ISM radio bands, from 2.4 to 2.485 GHz, and building personal area networks (PANs). Bluetooth have an entire suite of protocols, which it calls profiles, for a range of applications (for example a profile gives a mobile computer access to a wired LAN).

The basic Bluetooth network configuration is called a piconet. It consists of a master and up to seven slave devices, all the communication are between the slaves and master, slaves cannot communicate directly with each other.



- **Bluetooth devices:**

- **Bluetooth pros:**
  - Low cost.
  - Easy to use.
  - It can penetrate through walls.
  - It creates an Ad-Hoc connection immediately without any wires.
  - It used for voice and data transfer.
- **Bluetooth cons:**
  - Less secure.
  - Slow data transfer.
  - Small range (10 meters).
- **Bluetooth protocols stack:**



- **Physical radio layer (RF):** it performs modulation/demodulation of the data into RF (radio signals). It defines the physical characteristics of Bluetooth transceiver (transmitter and receptor). It defines two types of physical link: connection-less (defined by any path) and connection-oriented (take predefined path).
- **Baseband Link layer:** it performs the connection establishment within a piconet.
- **Link manager protocols layer:** it performs the management of the already established links. It also includes authentication and encryption processes.
- **Logical Link Control and Adaptation protocol layer:** it is also known as the heart of the Bluetooth protocol stack. It allows the communication between upper and lower layers of the Bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs the segmentation (make packets from big size of data) and multiplexing.
- **RFcomm layer:** It is short for Radio Frontend Component It provides serial interfaces with WAP and OBEX.
- **TCS:** It is short for Telephony Control Protocol. It provides telephony service.
- **SDP layer:** It is short for Service Discovery protocol. It allows to discover the services available on another Bluetooth enabled device.
- **Application layer:** It enables the user to interact with the application.

2.5.3 Network Layer

2.5.3.1 IPv4 address:

An IPv4 address is a 32-bits address that uniquely and universally defines the connection of a device (for example a computer or a router) to the internet. An IPv4 address is 32 bits long. Two devices on the internet can never have the same address at the same time. The address space of IPv4 is 2^(32) or 4.294.967.296.

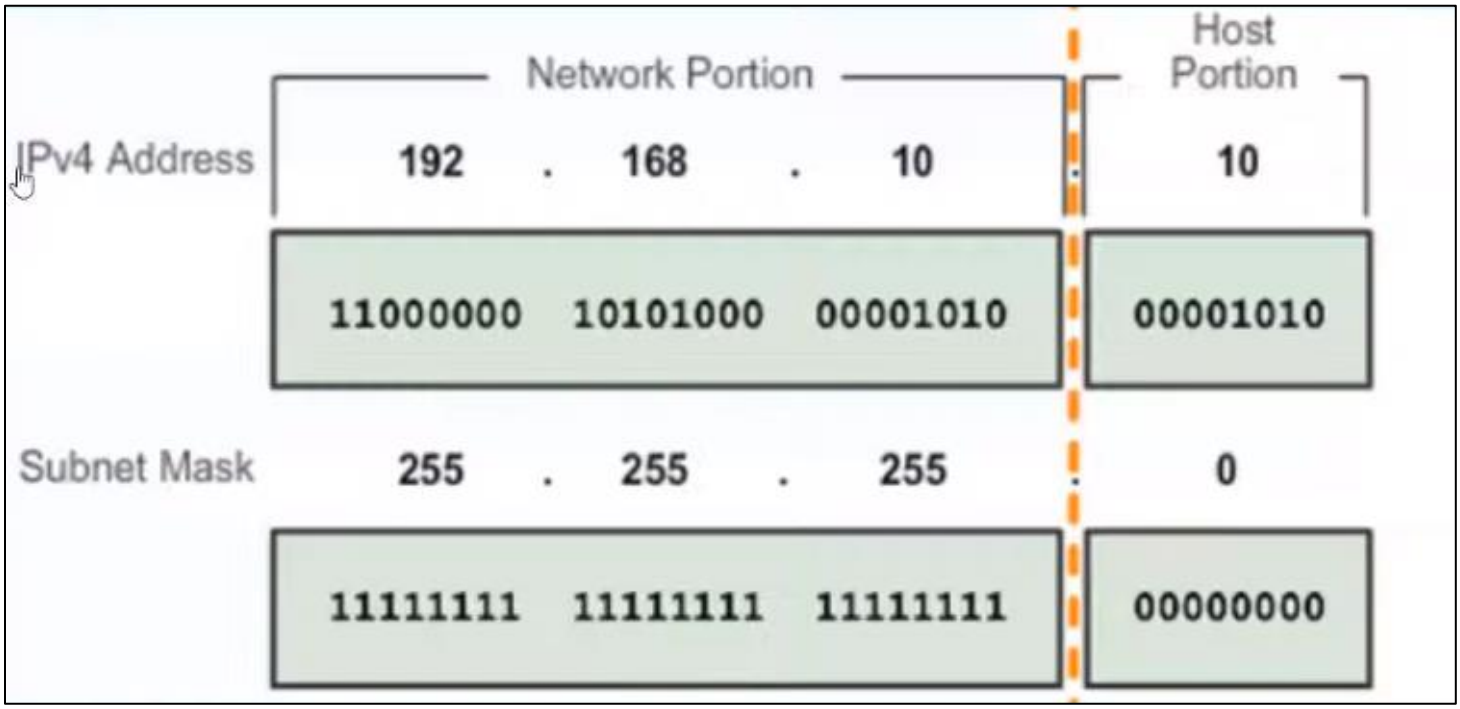
There are two notations to show an IPv4 address: binary notation (for example: 01010101 01010101 01010101 01010101) and dotted decimal notation (for example: 117.149.29.5) and we have only from 0.0.0.0 to 255.255.255.255 .

- **IPv4 classes:**

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

- **Subnet mask:**

Subnet mask is a separate 32-bit pattern used to define the network and host portions of an address, it doesn't actually contain the network or host portion of an IPv4 address, it just says where to look for these portions in a given IPv4 address.



Valid Subnet masks

Valid subnet masks are masks with continuous ones from the right to the left started by

10000000 00000000 00000000 00000000

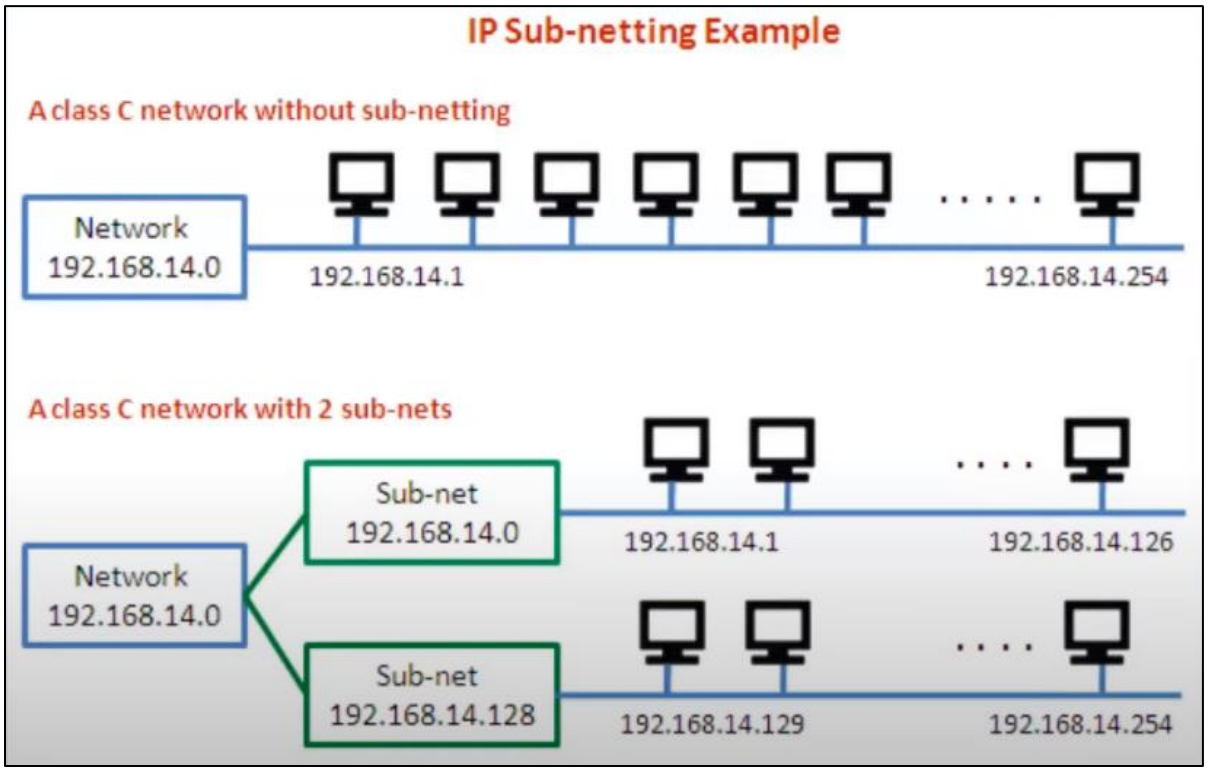
to

11111111 11111111 11111111 11111111

/n	Mask	/n	Mask	/n	Mask	/n	Mask
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

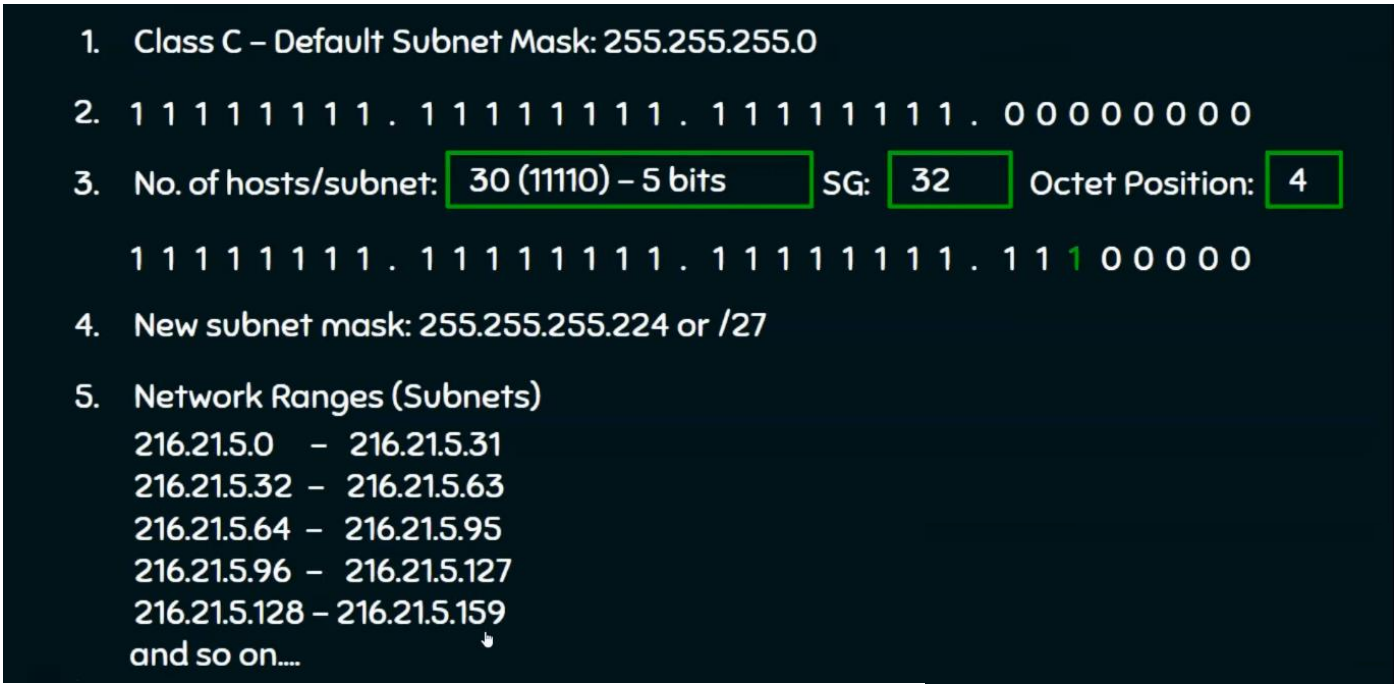
Subnetting

A subnetwork or subnet is a logical subdivision of an IP network, The practice of dividing a network into two or more networks is called subnetting. Computers that are belong to subnet are addressed with an identical most-significant bit-group in their IP addresses.



- Subnetting is defined by 5 steps:
  A. Identify the class of the IP address and note the default subnet mask.
  B. Convert the default subnet mask into binary.
  C. Note the number of hosts required per subnet and find the subnet generator (SG) and octet position.
  D. Generate the new subnet mask.
  E. Use the SG and generate the network ranges (subnets) in the appropriate octet position.

  example: subnet the IP address 216.21.5.0 into 30 hosts in each subnet.



Fixed Length subnet masking (FLSM)

FLSM creates subnets of the same size and an equal number of host identifiers for each network.

Variable Length subnet masking (VLSM)

VLSM creates subnets with varying sizes with a variable number of hosts for each network.

Private IP addresses

Early network design, when global end-to-end connectivity was envisioned for communication with all internet hosts, intended that IP addresses be globally unique. However, it was found that this was not always necessary as private networks developed and public address space needed to be conserved.

Computers not connected to the internet, such as factory machines that communicate only with each other via TCP/IP, need not have globally unique IP addresses, Today, such private networks are widely used and typically connect to the internet with network address translation (NAT), when needed.

Hosts that do not require access to the internet can use private addresses:

- 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

The aforementioned are the three non-overlapping ranges of IPv4 addresses for private networks are reserved.

Special use IPv4 addresses

- Network and broadcast addresses: within each network the first and last addresses cannot be assigned to hosts.
- Loopback addresses: 127.0.0.0 to 127.255.255.255 are reserved.
- Link-Local addresses: 169.254.0.0 to 169.254.255.255 addresses can be automatically assigned to the local host.
- Test-NET addresses: 192.0.2.0 to 192.0.2.255 set aside for teaching and learning purposes, used in documentation and network examples.
- Experimental addresses: 240.0.0.0 to 255.255.255.254 are listed as reserved.

Drawbacks of classful addressing:

Lack of Internal Address Flexibility: Big organizations are assigned large, "monolithic" blocks of addresses that don't match well the structure of their underlying internal networks.

Inefficient Use of Address Space: The existence of only three block sizes (classes A, B and C) leads to waste of limited IP address space.

Proliferation Of Router Table Entries: As the Internet grows, more and more entries are required for routers to handle the routing of IP datagrams, which causes performance problems for routers. Attempting to reduce inefficient address space allocation leads to even more router table entries.

3. Network Performance:

We can determine the network's performance and how good is it. By measuring the following performance Values:

- **Bandwidth:**
  - **Informal:** it's the maximum amount of data that can be transmitted per second.
  - **Formal:** it's the bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.
- **Throughput:**
  - **Informal:** it's the actual amount of data that passes through the medium.
  - **Formal:** it's a measure of how fast we can actually send data through a network.

The difference between bandwidth and throughput is that bandwidth is the capacity of transmission and throughput is the real transmission speed. (throughput < bandwidth)

- **Latency (delay):**
  Latency is the time 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. Latency is made of four components: 1. Transmission delay 2. Propagation delay 3. Queueing delay 4. Processing delay
  Latency = Transmission delay + Propagation delay + Queueing delay + Processing delay
  Transmission delay: is the time it takes to place the complete data packet on the transmission medium.

$$Transmission\ Time = \frac{Message\ size}{Bandwidth}$$

Propagation delay: time it takes for a bit to go from device A to device B.

$$Propagation\ Time = \frac{Distance}{Propagation\ speed}$$

Queuing delay: the third component in latency is the queuing time, the time needed for each intermediate or end device to hold the message before it can be processed. The queuing time is not a fixed factor, it changes with the load imposed on the network. When there is heavy traffic on the network the queuing time increases.

Preprocessing delay: is how much time the node takes to process the message.

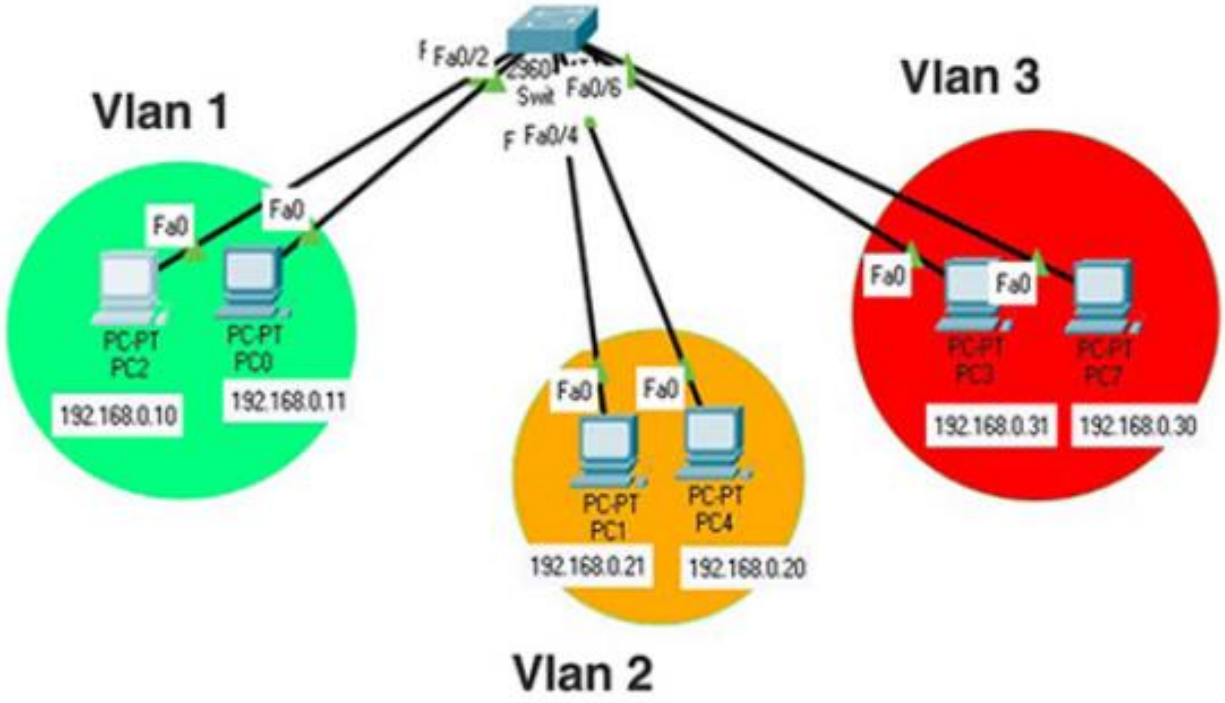
Round trip time: it is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgement of that signal to be received. With Tp is the propagation time.

$$RTT = 2 \times T_p$$

4. VLAN (Virtual LAN)

A VLAN is a logical partition of Layer 2 network. Multiple partitions can be created, allowing for multiple VLANs to co-exist. Each VLAN is a broadcast domain, usually with its own IP network. VLAN are mutually isolated and packets can only pass between them via a router. The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch. The host grouped within a VLAN are unaware of the VLAN's existence.

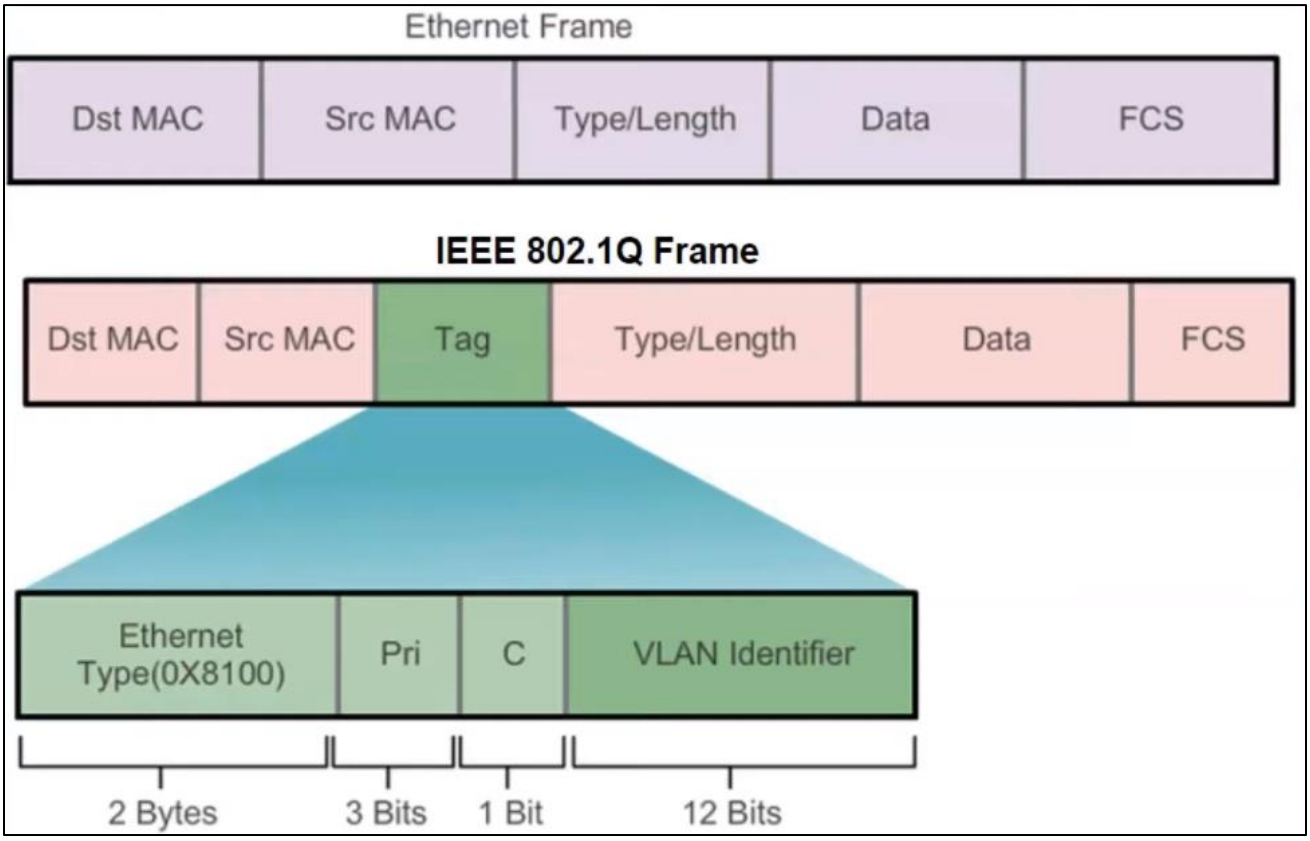
Types of VLANs Data VLAN, Default VLAN, Native VLAN, Management VLAN, Voice VLAN.



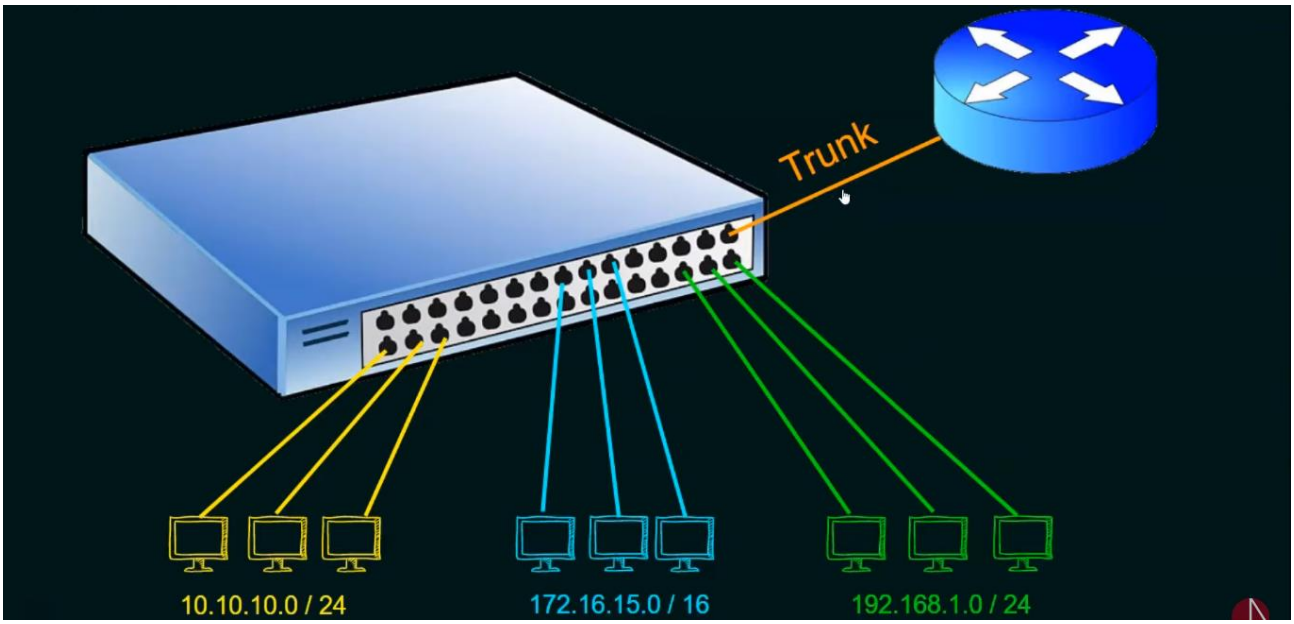
4.1 Benefits of VLAN

- ✓ Security.
- ✓ Cost reduction.
- ✓ Better performance.
- ✓ Shrink broadcast domains.
- ✓ Improved IT staff efficiency.
- ✓ Simpler project and application management.

4.2 VLAN frame tagging

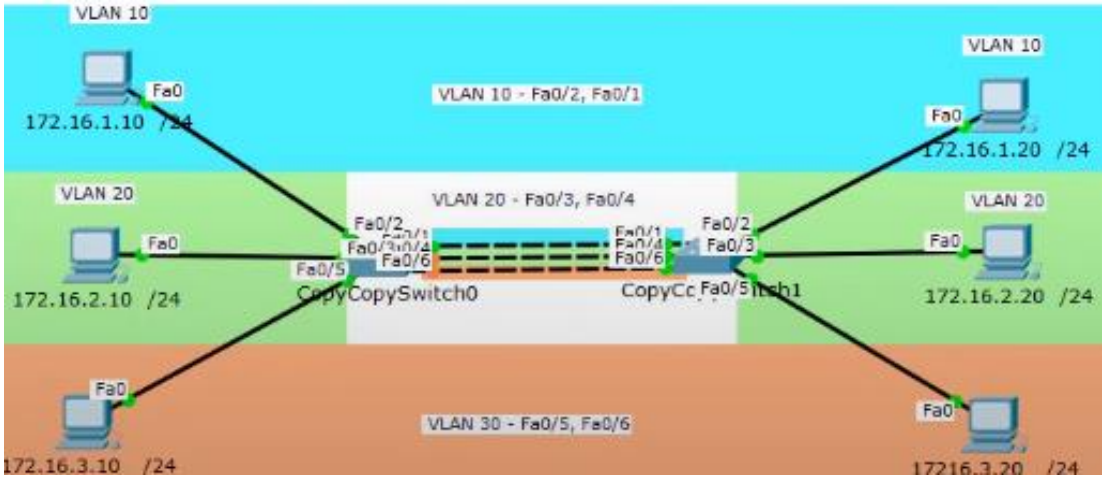


Frame tagging is the process of adding a VLAN identification header to the frame. It is used to properly transmit multiple VLAN frames through a trunk link (for example Ethernet). Switches tag frames to identify the VLAN to that they belong. Different tagging protocols exist; IEEE 802.1Q is a very popular example.



The protocol defines the structure of the tagging header added to the frame. switches add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk port.

When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.



VLAN frame tagging provides one Ethernet link between VLANs. But without a Router it can communicate only on the same VLAN. So, if you need to communicate with all the VLANs, you need to connect a router with one of these two switches. (Check the VLAN Cisco project)

5.Spanning Tree Protocol (STP):

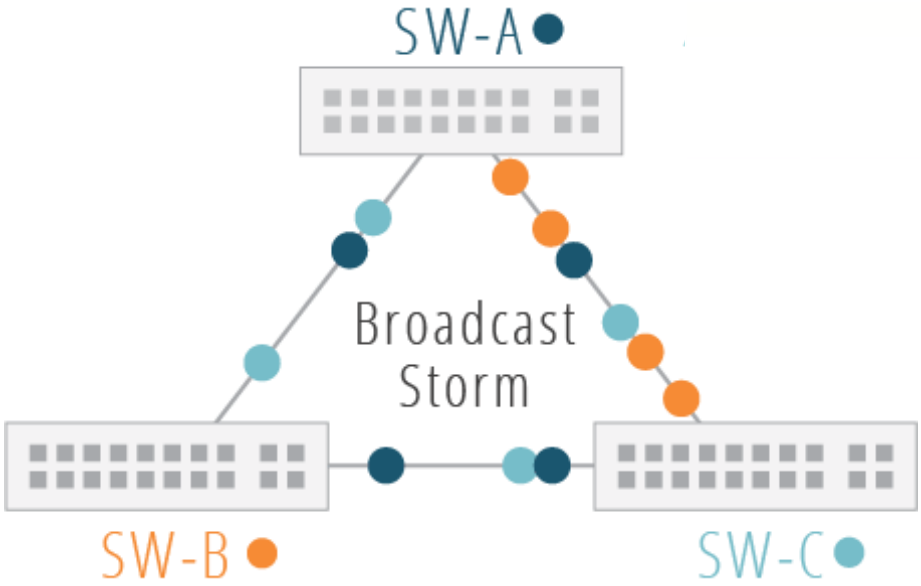
Spanning tree protocol (STP) (IEEE 802.1D) is predominantly used to prevent layer 2 loops and broadcast storms and is also used for network redundancy.

5.1 Redundancy:

Network redundancy is a communications pathway that has additional links to connect all nodes in case one link goes down. And this improves reliability and availability so it's advisable.

5.2 broadcast storm:

Most commonly the cause is a switching loop in the Ethernet network topology (i.e. two or more paths exist between switches). As broadcasts and multicasts are forwarded by switches out of every port, the switch or switches will repeatedly rebroadcast broadcast messages and flood the network. When a frame is sent into a looped topology, it can loop forever. And the network will be down at some point of time.



5.3 Spanning tree protocol

Switches within the same network need to be enabled for STP before they run the spanning tree algorithm so they can accurately determine which switch should be elected the "root bridge." This designated root bridge will be responsible for sending configuration bridge protocol data units (BPDUs) along with other information to its directly connected switches that, in turn, forward the BPDUs to their neighboring switches. Each switch has a bridge ID priority value (BID), which is a combination of a priority value (default 32768) and the switch's own MAC address. The switch with the lowest BID will become the root bridge.

There are five STP switchport states; these are:

- Disabled - The result of an administrative command that will disable the port.
- Blocking - When a device is connected, the port will first enter the blocking state.
- Listening -The switch will listen for and send BPDUs.
- Learning - The switch will receive a superior BPDU, will stop sending its own BPDUs, and will relay the superior BPDUs.
- Forwarding - The port is forwarding traffic.

STP Port Roles:

- **Root:** Ports on non-root switches with the best cost path to root bridge. These ports forward data to the root bridge.
- **Designated:** Ports on root and designated switches. All ports on the root bridge will be designated.
- **Blocked:** All other ports to bridges or switches are in a blocked state. Access ports going to workstations or PCs are not affected.

STP Election Process:

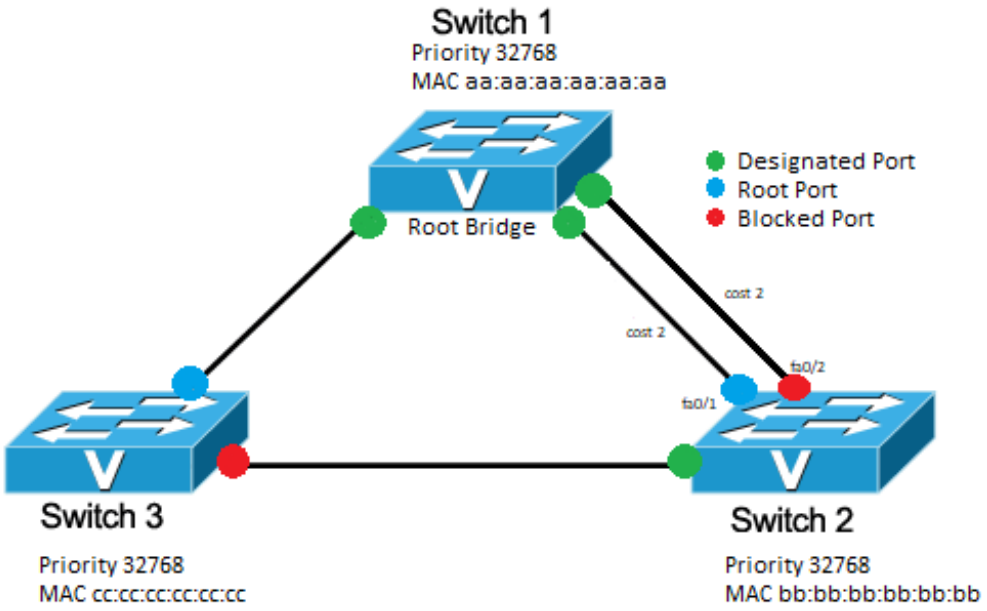
When switches are first turned on, they will send configuration BPDUs containing their BIDs, with each switch initially believing themselves to be the root bridge. However, when a switch receives a BPDU with a superior (lower value) BID, that switch will stop originating configuration BPDUs and will instead relay these superior BPDUs to its neighboring switches.

Once a root bridge has finally been announced, a second election process begins to determine the "root port" selection process (the port on a switch that will forward frames to the root bridge). This process will follow the steps below until a root port is elected:

- A switch port receives superior BPDUs from another switch and identifies that switch as the root bridge.
- The port with the lowest root path is selected as the root port, if possible.
- If the path cost is the same, the switch will select the port with the lowest sender BID as the selected root port.
- If the sender BID is the same (usually the same switch), the port with the lowest physical port number on the sending switch will be selected as the root bridge (as the final tie-breaker).

We have the port cost (path cost) is related with the Link Bandwidth speed.

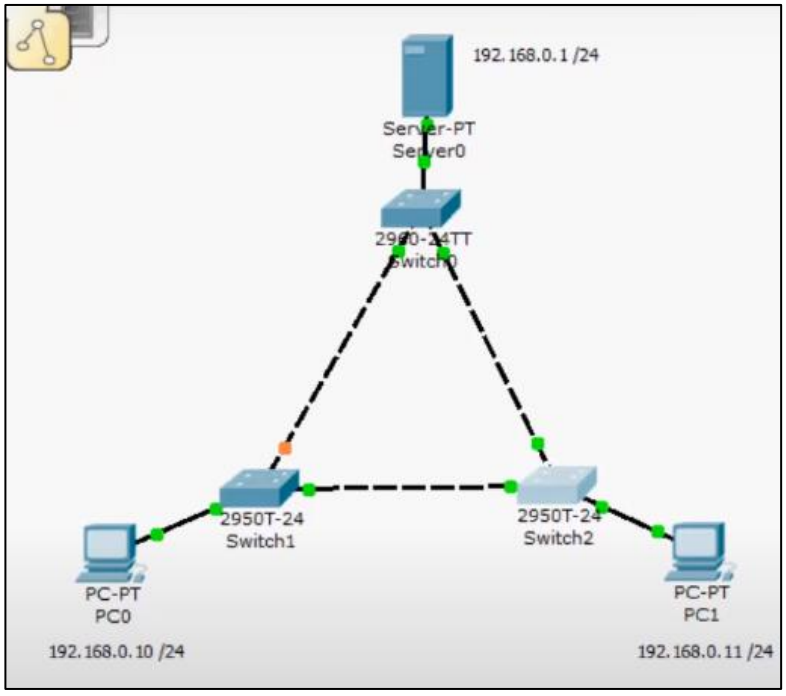
Link Speed(Bandwidth)	Port Cost
10 mbps	100
100 bmps	19
1 gbps	4
10 gbps	2



Note: - sometimes we need to select the root bridge to manually to ensure a short path for transmission. For example:

In this case we have Switch2 with the lowest BPDU, it's the elected root bridge. If PC0 wants to communicate with the server, it will take the longest path (by Switch1, Switch2, Switch0), and it's not the recommended path.

In this case, we have to make Switch0 as a root bridge manually by changing the Bridge ID of the Switch0 and for having lowest BPDU.



- there are other modern and rapid STP protocols such as Rapid STP. They provide a rapid reconnection of the network if one link goes down.