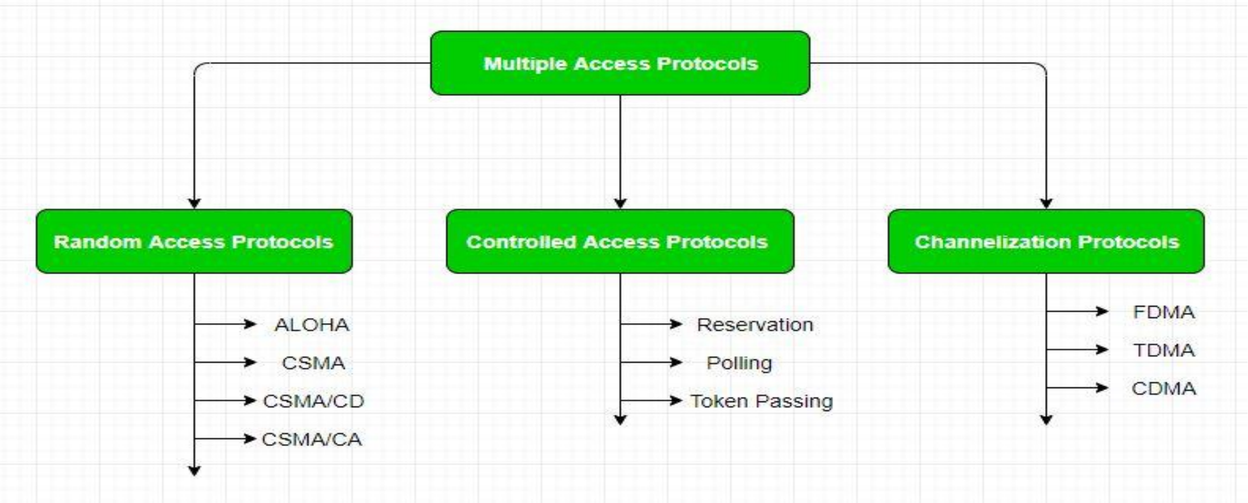
Unit - 3

Multiple Access Protocols



Random Access Protocols

Random access protocols assign uniform priority to all connected nodes. Any node can send data if the transmission channel is idle. No fixed time or fixed sequence is given for data transmission.

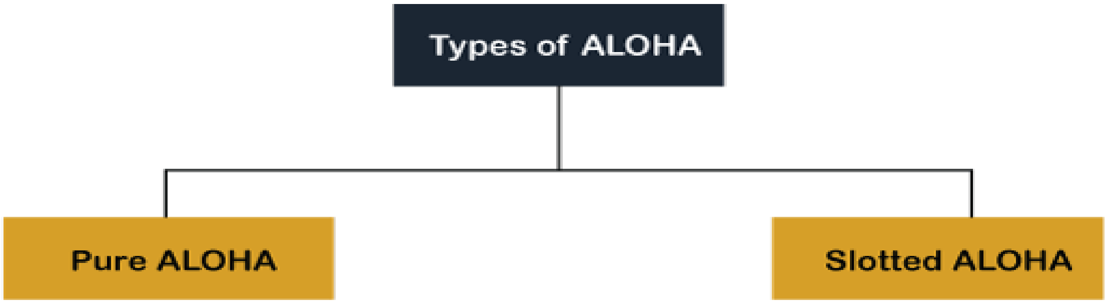
The four random access protocols are−

- ALOHA
- Carrier sense multiple access (CMSA)
- Carrier sense multiple access with collision detection (CMSA/CD)
- Carrier sense multiple access with collision avoidance (CMSA/CA)

Aloha Rules

1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.

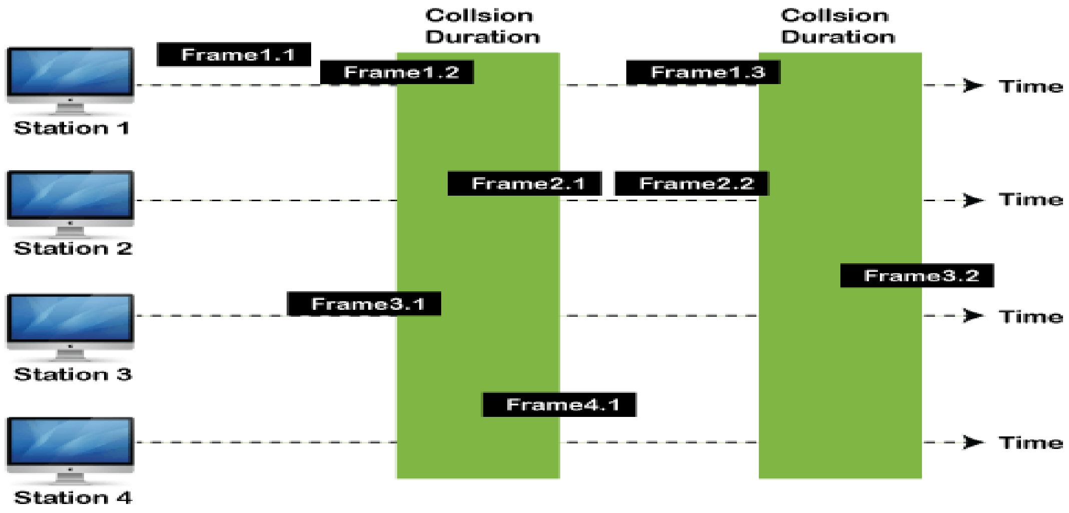
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



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 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.



Frames in Pure ALOHA

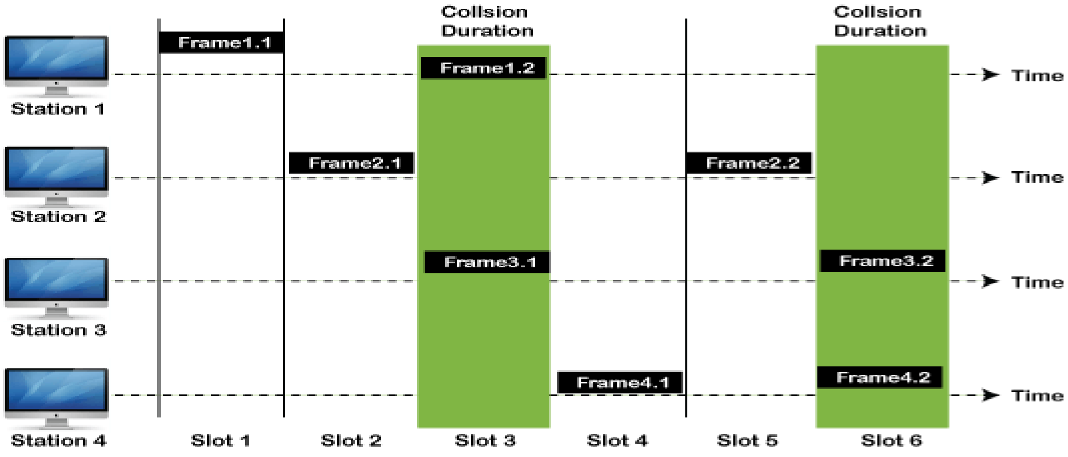
As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

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

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.

3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

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

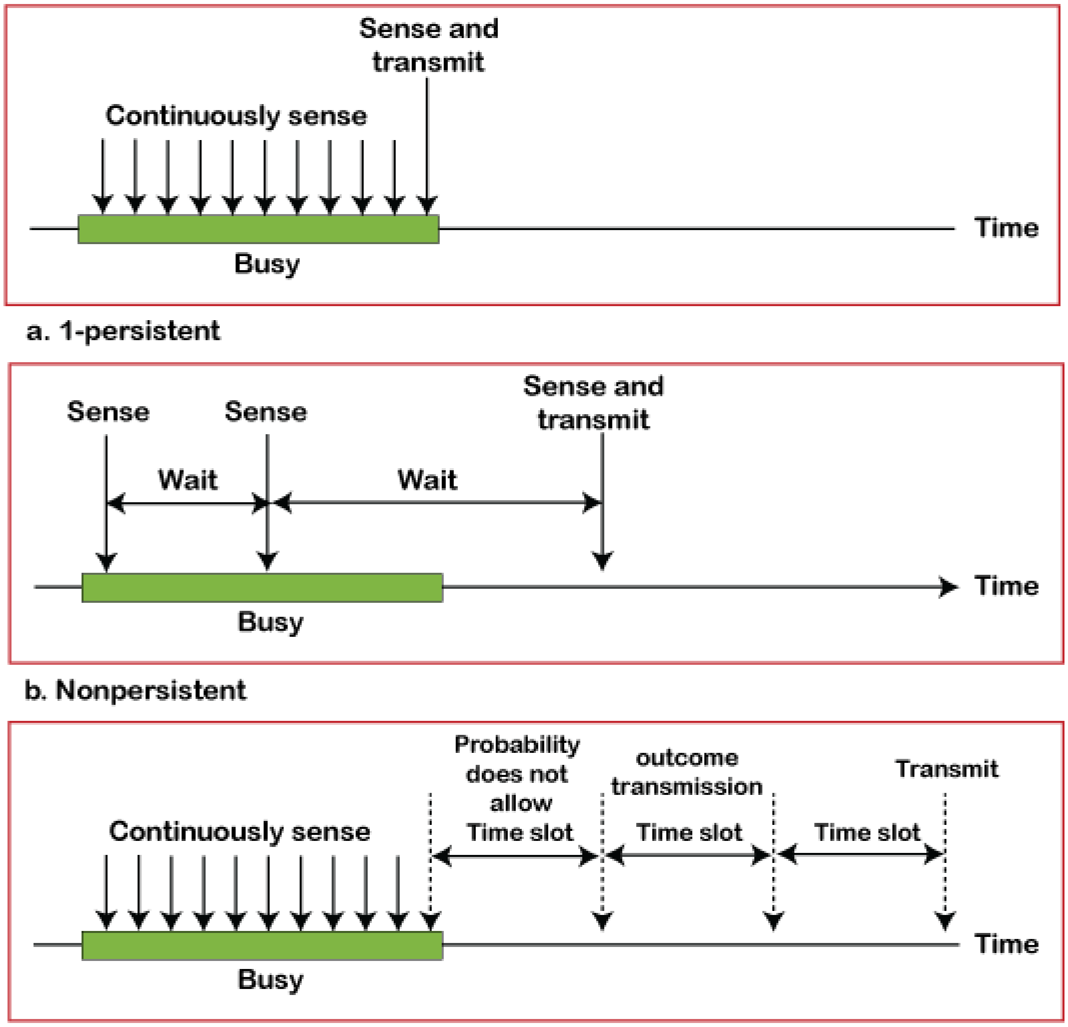
CSMA Access Modes

1-Persistent: 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.

Non-Persistent: 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.

P-Persistent: 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.

O- Persistent: 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

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.

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:

Inter frame 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 **Inter frame** 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.

B. Controlled Access Protocol

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

C. Channelization Protocols

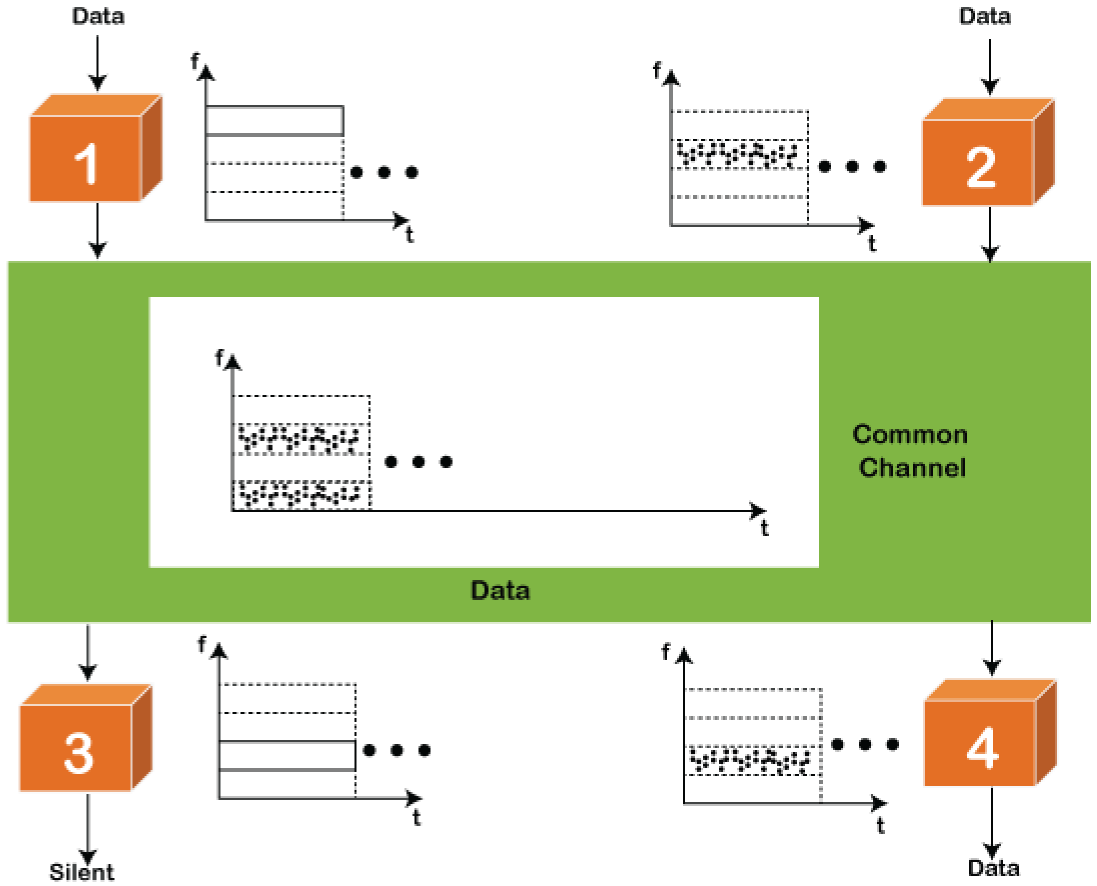
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)

FDMA

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



TDMA

Time Division Multiple Access (TDMA) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same frequency bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

CDMA

The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

Differences between Pure and Slotted Aloha

Pure Aloha	**Slotted Aloha**
In this Aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for Pure Aloha = 2 x Tt	Vulnerable time for Slotted Aloha = Tt
In Pure Aloha, Probability of successful transmission of the data packet = G x e-2Greduce	In Slotted Aloha, Probability of successful transmission of the data packet = G x e-G
In Pure Aloha, Maximum efficiency = 18.4%	In Slotted Aloha, Maximum efficiency = 36.8%
Pure Aloha doesn’t reduces the number of collisions to half.	Slotted Aloha reduces the number of collisions to half and doubles the efficiency of Pure Aloha.

Collision-Free Protocols

Almost collisions can be avoided in CSMA/CD.they can still occur during the contention period.the collision during contention period adversely affects the system performance, this happens when the cable is long and length of packet are short. This problem becomes serious as fiber optics network come into use. Here we shall discuss some protocols that resolve the collision during the contention period.

- Bit-map Protocol
- Binary Countdown
- Limited Contention Protocols
- The Adaptive Tree Walk Protocol

Pure and slotted Aloha, CSMA and CSMA/CD are Contention based Protocols:

- Try-if collide-Retry
  - No guarantee of performance
    - What happen if the network load is high?

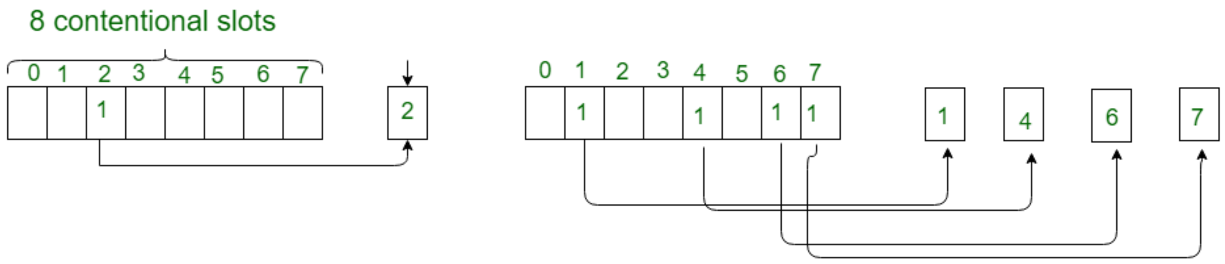
Collision Free Protocols:

- Pay constant overhead to achieve performance guarantee
- Good when network load is high

1. Bit-map Protocol:

Bit map protocol is collision free Protocol in In bitmap protocol method, each contention period consists of exactly N slots. if any station has to send frame, then it transmits a 1 bit in the respective slot. For example if station 2 has a frame to send, it transmits a 1 bit during the second slot.

In general Station 1 Announce the fact that it has a frame questions by inserting a 1 bit into slot 1. In this way, each station has complete knowledge of which station wishes to transmit. There will never be any collisions because everyone agrees on who goes next. Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called Reservation Protocols.



A Bit-map Protocol.

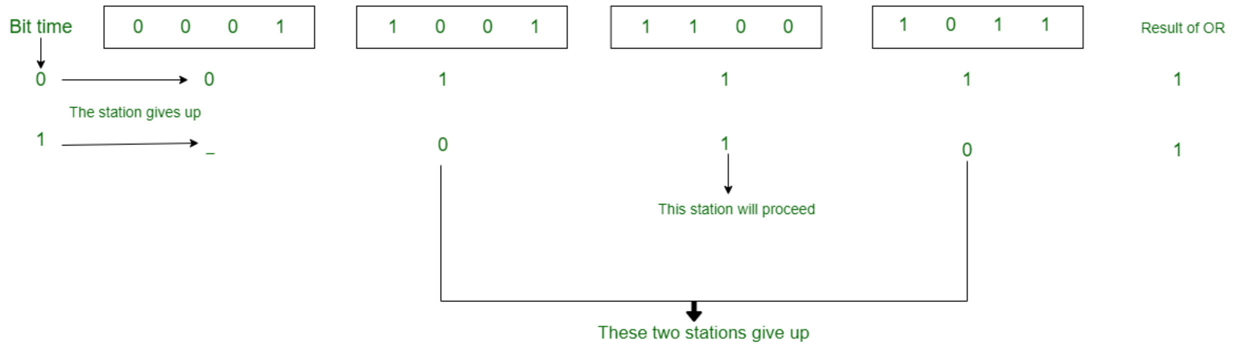
For analyzing the performance of this protocol, We will measure time in units of the contention bits slot, with a data frame consisting of d time units. Under low load conditions, the bitmap will simply be repeated over and over, for lack of data frames.All the stations have something to send all the time at high load, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame. Generally, high numbered stations have to wait for half a scan before starting to transmit low numbered stations have to wait for half a scan(N/2 bit slots) before starting to transmit, low numbered stations have to wait on an average 1.5 N slots.

2. Binary Countdown:

Binary countdown protocol is used to overcome the overhead 1 bit per binary station. In binary countdown, binary station addresses are used. A station wanting to use the channel broadcast its address as binary bit string starting with the high order bit. All addresses are assumed of the same length. Here, we will see the example to illustrate the working of the binary countdown.

In this method, different station addresses are ORed together who decide the priority of transmitting. If these stations 0001, 1001, 1100, 1011 all are trying to seize the channel for transmission. All the station at first broadcast their most significant address bit that is 0, 1, 1, 1 respectively. The most significant bits are ORed together. Station 0001 see the 1MSB in another station addresses and knows that a higher numbered station is competing for the channel, so it gives up for the current round.

Other three stations 1001, 1100, 1011 continue. The next bit is 1 at station 1100, swiss station 1011 and 1001 give up. Then station 110 starts transmitting a frame, after which another bidding cycle starts.



Binary countdown

Limited Contention Protocols:

Limited Contention Protocols are the media access control (MAC) protocols that combines the advantages of collision based protocols and collision free protocols. They behave like slotted ALOHA under light loads and bitmap protocols under heavy loads.

- Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.
- Collision free protocols (bitmap, binary Countdown) are good when load is high.
- How about combining their advantages
  1. Behave like the ALOHA scheme under light load
  2. Behave like the bitmap scheme under heavy load.

Example – An example of limited contention protocol is Adaptive Tree Walk Protocol.

Adaptive Tree Walk Protocol:

partition the group of station and limit the contention for each slot.

Under light load, everyone can try for each slot like aloha

Under heavy load, only a group can try for each slot

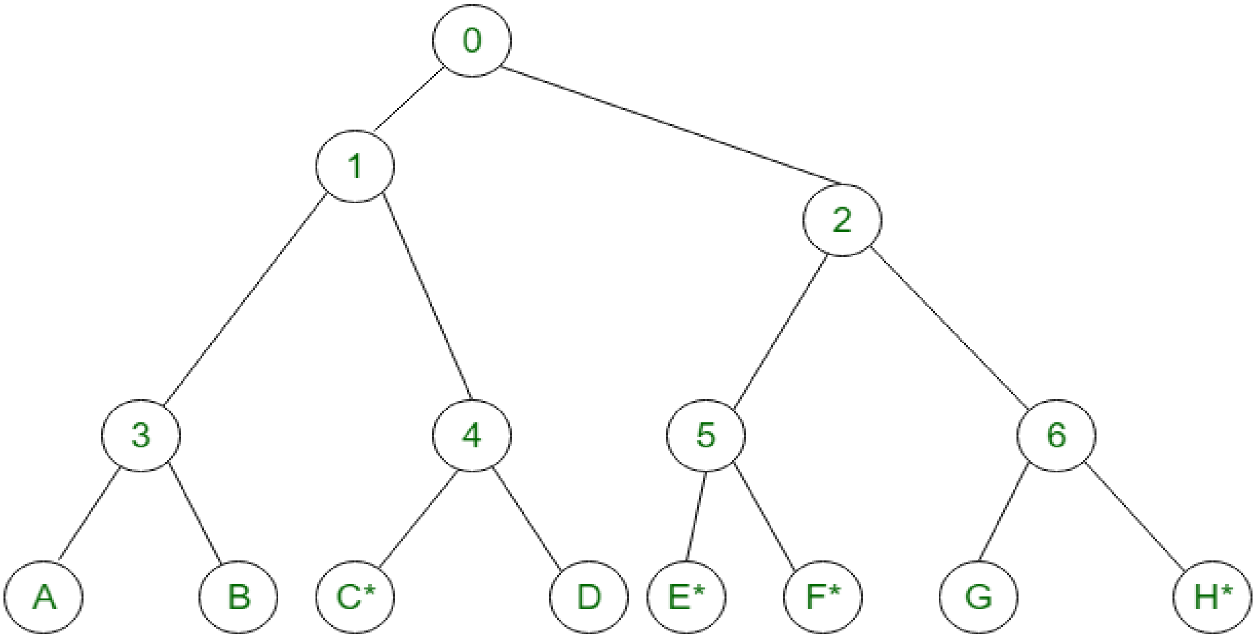
How do we do it:

treat every stations as the leaf of a binary tree

first slot (after successful transmission), all stations can try to get the slot(under the root node).

if no conflict, fine

in case of conflict, only nodes under a subtree get to try for the next one. (depth first search)



- Slot-0: C*, E*, F*, H* (all nodes under node 0 can try which are going to send), conflict
- Slot-1: C* (all nodes under node 1can try}, C sends
- Slot-2: E*, F*, H*(all nodes under node 2 can try}, conflict
- Slot-3: E*, F* (all nodes under node 5 can try to send), conflict
- Slot-4: E* (all nodes under E can try), E sends
- Slot-5: F* (all nodes under F can try), F sends
- Slot-6: H* (all nodes under node 6 can try to send), H sends.

Wavelength Division Multiple Access Protocols

Wavelength division multiplexing (WDM) is a technique of multiplexing multiple optical carrier signals through a single optical fiber channel by varying the wavelengths of laser lights. WDM allows communication in both the directions in the fiber cable.

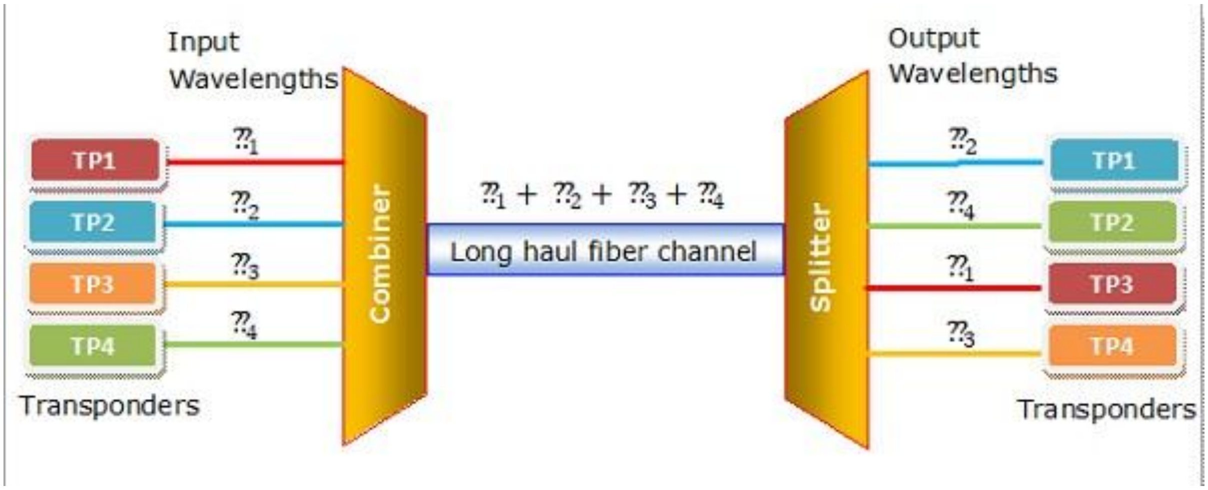
Concept and Process

In WDM, the optical signals from different sources or (transponders) are combined by a multiplexer, which is essentially an optical combiner. They are combined so that their wavelengths are different.

The combined signal is transmitted via a single optical fiber strand. At the receiving end, a demultiplexer splits the incoming beam into its components and each of the beams is send to the corresponding receivers.

Example

The following diagram conceptually represents multiplexing using WDM. It has 4 optical signals having 4 different wavelengths. Each of the four senders generates data streams of a particular wavelength. The optical combiner multiplexes the signals and transmits them over a single long-haul fiber channel. At the receiving end, the splitter demultiplexes the signal into the original 4 data streams.



Categories of WDM

Based upon the wavelength, WDM can be divided into two categories −

- Course WDM (CWDM) : CWDM generally operates with 8 channels where the spacing between the channels is 20 nm (nanometers) apart. It consumes less energy than DWDM and is less expensive. However, the capacity of the links, as well as the distance supported, is lesser.
- Dense WDM (DWDM) : In DWDM, the number of multiplexed channels much larger than CWDM. It is either 40 at 100GHz spacing or 80 with 50GHz spacing. Due to this, they can transmit the huge quantity of data through a single fiber link. DWDM is generally applied in core networks of telecommunications and cable networks. It is also used in cloud data centers for their IaaS services.

802.11 MAC Sublayer Protocol

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

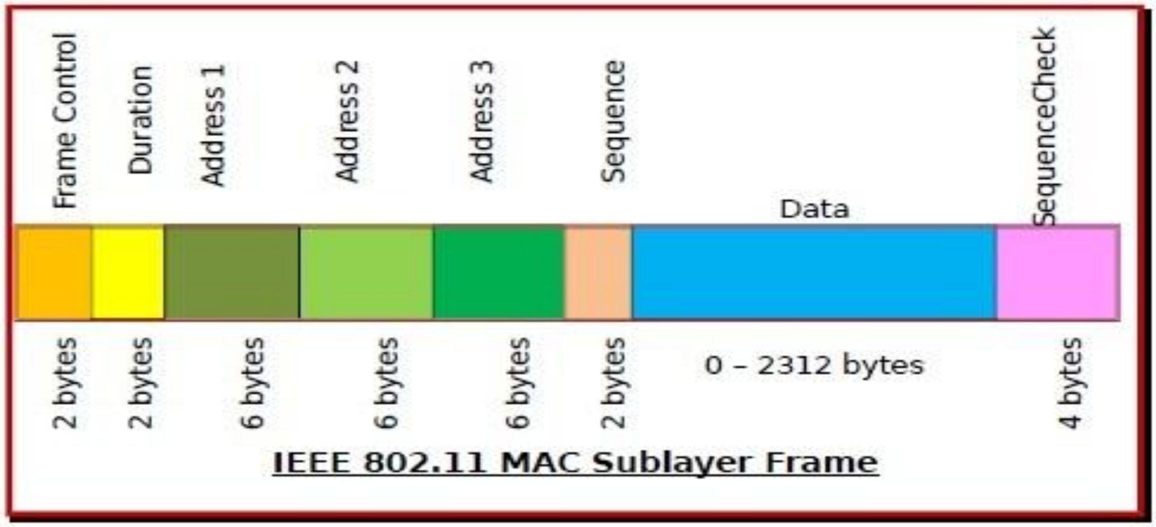
The 802.11 MAC sublayer provides an abstraction of the physical layer to the logical link control sublayer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.

MAC Sublayer frame of IEEE 802.11

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are −

- **Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.

- **Address fields** − There are three 6-byte address fields containing addresses of source, immediate destination and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers.
- **Data** − This is a variable sized field carries the data from the upper layers. The maximum size of data field is 2312 bytes.
- **Check Sequence** − It is a 4-byte field containing error detection information.



Avoidance of Collisions by 802.11 MAC Sublayer

In wireless systems, the method of collision detection does not work. It uses a protocol called carrier sense multiple access with collision avoidance (CSMA/CA).

The method of CSMA/CA is −

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
- After sending the frame, it sets a timer.
- The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.

- Otherwise, it waits for a back-off time period and restarts the algorithm.

Co-ordination Functions in 802.11 MAC Sublayer

IEEE 802.11 MAC Sublayer uses two co-ordination functions for collision avoidance before transmission −

- **Distributed Coordination Function (DCF)** −
    - It is a mandatory function used in CSMA/CA.
    - It is used in distributed contention-based channel access.
    - It is deployed in both Infrastructure BSS (basic service set) as well as Independent BSS.
- **Point Coordination Function (PCF)** −
    - It is an optional function used by 802.11 MAC Sublayer.
    - It is used in centralized contention-free channel access.
    - It is deployed in Infrastructure BSS only.

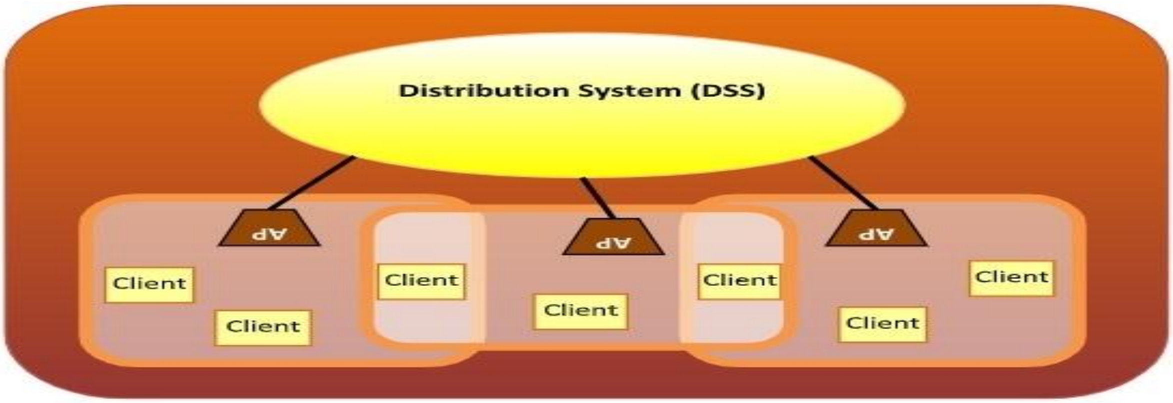
Wireless LAN protocols

Wireless LANs refer to LANs (Local Area Networks) that use high frequency radio waves instead of cables for connecting the devices. It can be conceived as a set of laptops and other wireless devices communicating by radio signals. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

Configuration of Wireless LANs

Each station in a Wireless LAN has a wireless network interface controller. A station can be of two categories −

- **Wireless Access Point (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access points. The APs are wired together using fiber or copper wires, through the distribution system.
- **Client** − Clients are workstations, computers, laptops, printers, smart phones etc. They are around tens of meters within the range of an AP.



Types of WLAN Protocols

IEEE 802.11 or WiFi has a number of variations, the main among which are −

- **802.11a Protocol**− This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).
- **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
- **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.
- **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

Ethernet:

Traditional Ethernet, Switched Ethernet, Fast Ethernet, Gigabit Ethernet

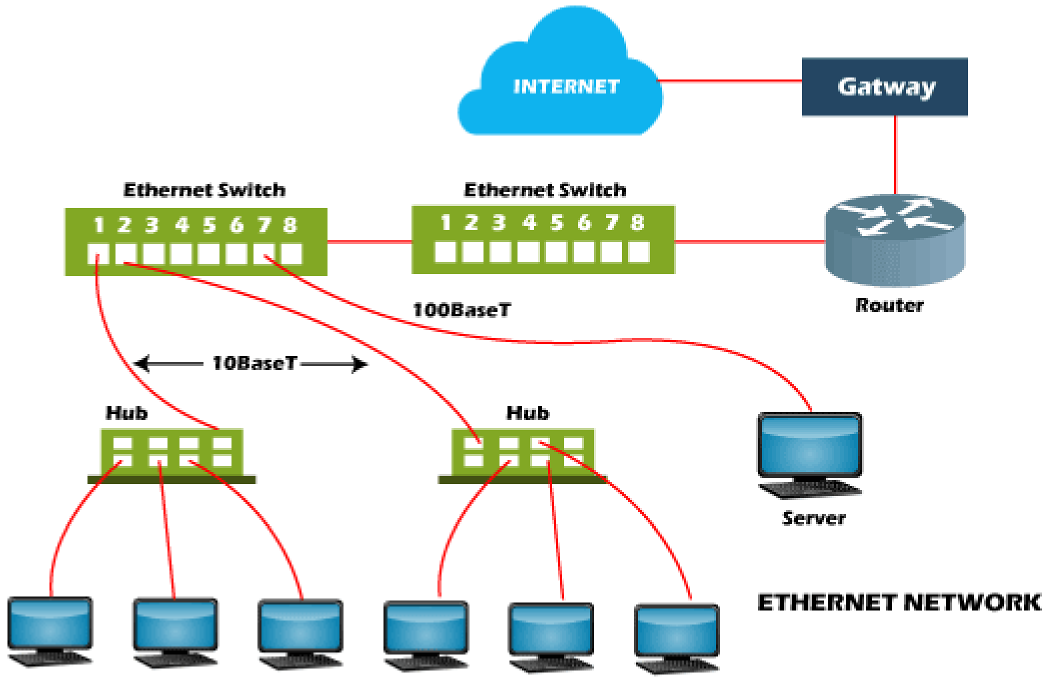
What is Ethernet?

Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by LAN and WAN within buildings, homes, and even small neighborhoods.

It offers a simple user interface that helps to connect various devices easily, such as switches, routers, and computers. A local area network (LAN) can be created with the help of a single router and a few Ethernet cables, which enable communication between all linked devices. This is because an Ethernet port is included in your laptop in which one end of a cable is plugged in and connect the other to a router. Ethernet ports are slightly wider, and they look similar to telephone jacks.

With lower-speed Ethernet cables and devices, most of the Ethernet devices are backward compatible. However, the speed of the connection will be as fast as the lowest common denominator. For instance, the computer will only have the potential to forward and receive data at 10 Mbps if you attach a computer with a 10BASE-T NIC to a 100BASE-T network. Also, the maximum data transfer rate will be 100 Mbps if you have a Gigabit Ethernet router and use it to connect the device.

The wireless networks replaced Ethernet in many areas; however, Ethernet is still more common for wired networking. Wi-Fi reduces the need for cabling as it allows the users to connect smartphones or laptops to a network without the required cable. While comparing with Gigabit Ethernet, the faster maximum data transfer rates are provided by the 802.11ac Wi-Fi standard. Still, as compared to a wireless network, wired connections are more secure and are less prone to interference. This is the main reason to still use Ethernet by many businesses and organizations.



Different Types of Ethernet Networks

An Ethernet device with CAT5/CAT6 copper cables is connected to a fiber optic cable through fiber optic media converters. The distance covered by the network is significantly increased by this extension for fiber optic cable. There are some kinds of Ethernet networks, which are discussed below:

- **Fast Ethernet:** This type of Ethernet is usually supported by a twisted pair or CAT5 cable, which has the potential to transfer or receive data at around100 Mbps. They function at 100Base and 10/100Base Ethernet on the fiber side of the link if any device such as a camera, laptop, or other is connected to a network. The fiber optic cable and twisted pair cable are used by fast Ethernet to create communication. The 100BASE-TX, 100BASE-FX, and 100BASE-T4 are the three categories of Fast Ethernet.
- **Gigabit Ethernet:** This type of Ethernet network is an upgrade from Fast Ethernet, which uses fiber optic cable and twisted pair cable to create communication. It can transfer data at a rate of 1000 Mbps or 1Gbps. In modern times, gigabit Ethernet is more common. This network type also uses CAT5e or other advanced cables, which can transfer data at a rate of 10 Gbps.

The primary intention of developing the gigabit Ethernet was to full fill the user's requirements, such as faster transfer of data, faster communication network, and more.

- **10-Gigabit Ethernet:** This type of network can transmit data at a rate of 10 Gigabit/second, considered a more advanced and high-speed network. It makes use of CAT6a or CAT7 twisted-pair cables and fiber optic cables as well. This network can be expended up to nearly 10,000 meters with the help of using a fiber optic cable.

- **Switch Ethernet:** This type of network involves adding switches or hubs, which helps to improve network throughput as each workstation in this network can have its own dedicated 10 Mbps connection instead of sharing the medium. Instead of using a crossover cable, a regular network cable is used when a switch is used in a network. For the latest Ethernet, it supports 1000Mbps to 10 Gbps and 10Mbps to 100Mbps for fast Ethernet.

Advantages of Ethernet

- It is not much costly to form an Ethernet network. As compared to other systems of connecting computers, it is relatively inexpensive.
- Ethernet network provides high security for data as it uses firewalls in terms of data security.

- Also, the Gigabit network allows the users to transmit data at a speed of 1-100Gbps.
- In this network, the quality of the data transfer does maintain.
- In this network, administration and maintenance are easier.
- The latest version of gigabit ethernet and wireless ethernet have the potential to transmit data at the speed of 1-100Gbps.

Disadvantages of Ethernet

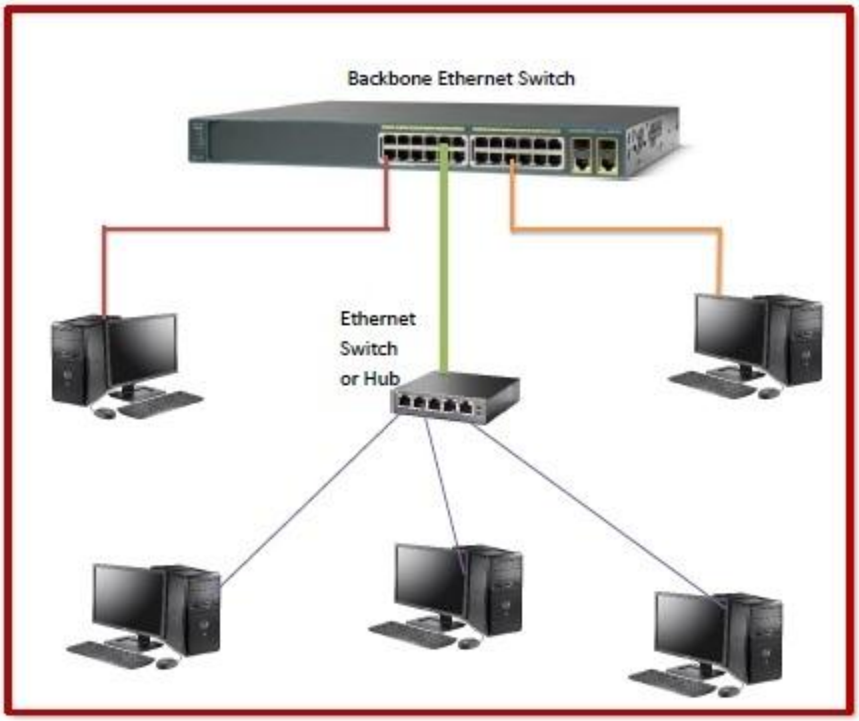
- It needs deterministic service; therefore, it is not considered the best for real-time applications.
- The wired Ethernet network restricts you in terms of distances, and it is best for using in short distances.
- If you create a wired ethernet network that needs cables, hubs, switches, routers, they increase the cost of installation.
- Data needs quick transfer in an interactive application, as well as data is very small.
- In ethernet network, any acknowledge is not sent by receiver after accepting a packet.
- If you are planning to set up a wireless Ethernet network, it can be difficult if you have no experience in the network field.
- Comparing with the wired Ethernet network, wireless network is not more secure.
- The full-duplex data communication mode is not supported by the 100Base-T4 version.
- Additionally, finding a problem is very difficult in an Ethernet network (if has), as it is not easy to determine which node or cable is causing the problem.

Switched Ethernet

Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s as IEEE 802.3 standard. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

In switched Ethernet, the hub connecting the stations of the classic Ethernet is replaced by a switch. The switch connects the high-speed backplane bus to all the stations in the LAN. The switch-box contains a number of ports, typically within the range of 4 – 48. A station can be connected in the network by simply plugging a connector to any of the ports. Connections from a backbone Ethernet switch can go to computers, peripherals or other Ethernet switches and Ethernet hubs.

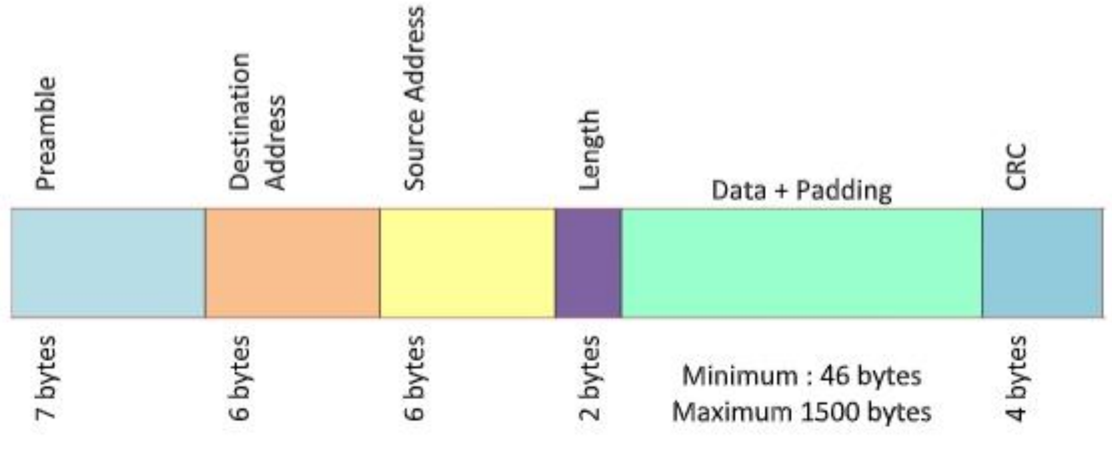
The following diagram shows configuration of a switched Ethernet −



Frame Format of Switched Ethernet

The frame format of switched Ethernet is same as that of classic Ethernet. The fields are −

- **Preamble:** An 8 bytes starting field that provides alert and timing pulse for transmission.
- **Destination Address:** A 6 byte field containing physical address of destination stations.
- **Source Address**: A 6 byte field containing the physical address of the sending station.
- **Length**: A 2 bytes field that stores the number of bytes in the data field.
- **Data:** A variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding:** Extra bits added to the data to bring its length to the minimum size of 46 bytes.
- **CRC:** A 4 byte field that contains the error detection information.



Switched Ethernet Frame Format

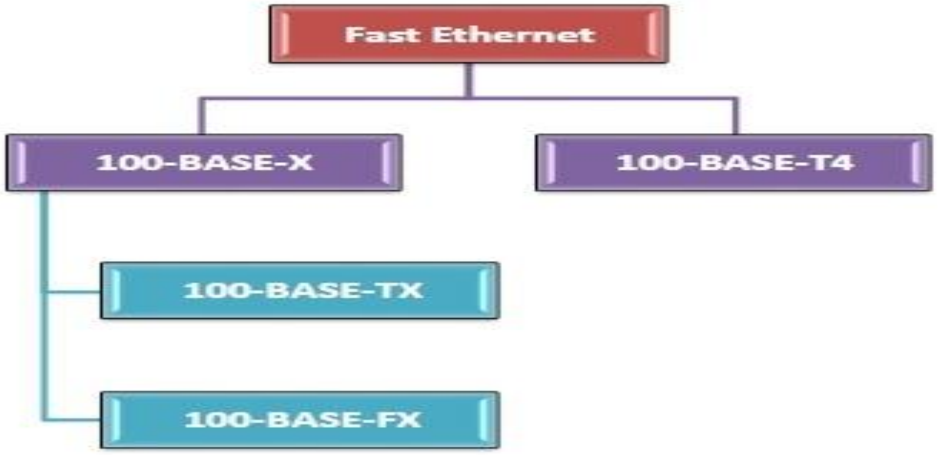
Fast Ethernet (802.3u)

In computer networks, Fast Ethernet is a variation of Ethernet standards that carry data traffic at 100 Mbps (Mega bits per second) in local area networks (LAN). It was launched as the IEEE 802.3u standard in 1995, and stayed the fastest network till the introduction of Gigabit Ethernet.

Fast Ethernet is popularly named as 100-BASE-X. Here, 100 is the maximum throughput, i.e. 100 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used, which is TX or FX.

Varieties of Fast Ethernet

The common varieties of fast Ethernet are 100-Base-TX, 100-BASE-FX and 100-Base-T4.



- **100-Base-T4**

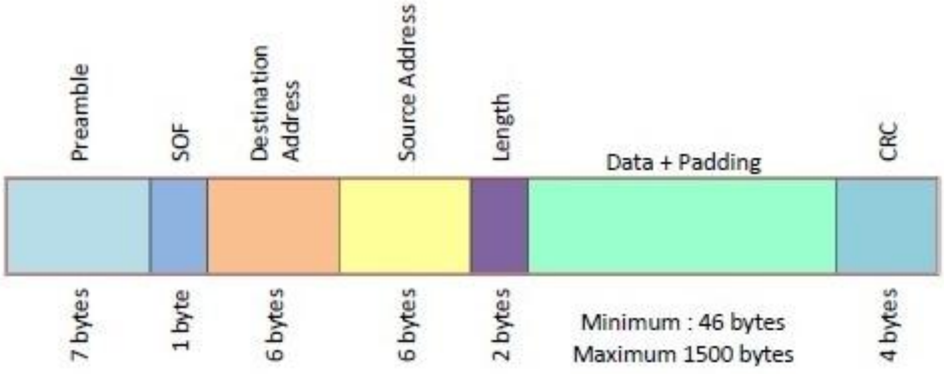
    - This has four pairs of UTP of Category 3, two of which are bi-directional and the other two are unidirectional.
    - In each direction, three pairs can be used simultaneously for data transmission.
    - Each twisted pair is capable of transmitting a maximum of 25Mbaud data. Thus the three pairs can handle a maximum of 75Mbaud data.
    - It uses the encoding scheme 8B/6T (eight binary/six ternary).
- **100-Base-TX**
    - This has either two pairs of unshielded twisted pairs (UTP) category 5 wires or two shielded twisted pairs (STP) type 1 wires. One pair transmits frames from hub to the device and the other from device to hub.
    - Maximum distance between hub and station is 100m.
    - It has a data rate of 125 Mbps.
    - It uses MLT-3 encoding scheme along with 4B/5B block coding.
- **100-BASE-FX**
    - This has two pairs of optical fibers. One pair transmits frames from hub to the device and the other from device to hub.
    - Maximum distance between hub and station is 2000m.
    - It has a data rate of 125 Mbps.
    - It uses NRZ-I encoding scheme along with 4B/5B block coding.

Frame Format of IEEE 802.3

The frame format of IEEE 802.3u is same as IEEE 802.3. The fields in the frame are:

- **Preamble** – It is a 7 bytes starting field that provides alert and timing pulse for transmission.
- **Start of Frame Delimiter (SOF)** – It is a 1 byte field that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address** – It is a 6 byte field containing physical address of destination stations.
- **Source Address** – It is a 6 byte field containing the physical address of the sending station.
- **Length** – It a 2 bytes field that stores the number of bytes in the data field.

- **Data** – This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding** – This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC** – CRC stands for cyclic redundancy check. It contains the error detection information.



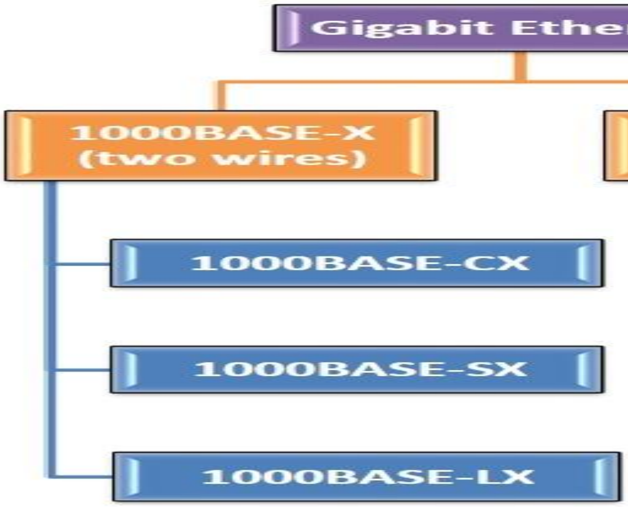
IEEE 802.3 Frame Format

Gigabit Ethernet

In computer networks, Gigabit Ethernet (GbE) is the family of Ethernet technologies that achieve theoretical data rates of 1 gigabit per second (1 Gbps). It was introduced in 1999 and was defined by the IEEE 802.3ab standard.

Varieties of Gigabit Ethernet

The popular varieties of fast Ethernet are 1000Base-SX, 1000Base-LX, 1000BASE-T and 1000Base-CX.



1000BASE-CX

- Defined by IEEE 802.3z standard
- The initial standard for Gigabit Ethernet
- Uses shielded twisted pair cables with DE-9 or 8P8C connector
- Maximum segment length is 25 metres
- Uses NRZ line encoding and 8B/6B block encoding

1000BASE-SX

- Defined by IEEE 802.3z standard
- Uses a pair of fibre optic cables of a shorter wavelength having 770 – 860 nm diameter
- The maximum segment length varies from 220 – 550 metres depending upon the fiber properties.
- Uses NRZ line encoding and 8B/10B block encoding

1000BASE-LX

- Defined by IEEE 802.3z standard
- Uses a pair of fibre optic cables of a longer wavelength having 1270 – 1355 nm diameter
- Maximum segment length is 500 metres
- Can cover distances up to 5 km
- Uses NRZ line encoding and 8B/10B block encoding

1000BASE-T

- Defined by IEEE 802.3ab standard

- Uses a pair four lanes of twisted-pair cables (Cat-5, Cat-5e, Cat-6, Cat-7)
- Maximum segment length is 100 metres
- Uses trellis code modulation technique

Data Link Layer Switching

Network switching is the process of forwarding data frames or packets from one port to another leading to data transmission from source to destination. Data link layer is the second layer of the Open System Interconnections (OSI) model whose function is to divide the stream of bits from physical layer into data frames and transmit the frames according to switching requirements. Switching in data link layer is done by network devices called **bridges**.

Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Why is Switching Concept required?

Switching concept is developed because of the following reasons:

- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

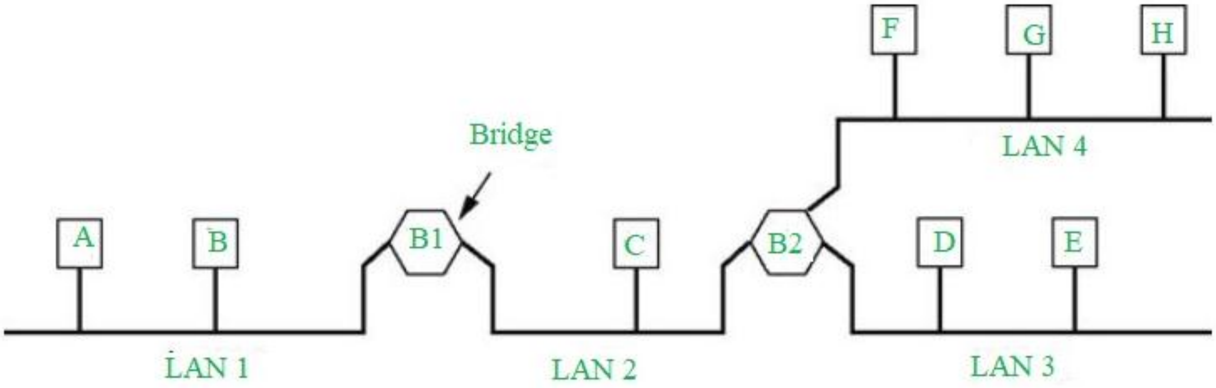
- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Bridges (local Internetworking device)

Local Internetworking is one which is within the same organization i.e. same building or same campus, then for the networking, we may not require the full power of the router. We can do it with a data link layer device called a bridge.

Bridges:

Bridges are a data link layer device and can connect to different networks as well as connect different networks of different types. Bridges from 802.x to 802.y where x & y may both be Ethernet or one can be Ethernet and other may be a token ring, etc. It locally connects small LANs, whereas if LANs are big then bridges can no longer handle them. Bridge follows a protocol in IEEE format execute 802.1 which is a spanning tree of bridges.



In the above figure, there are four LANs that are connected by two bridges. Bridge 1 has two ports, one connecting to LAN 1 other connecting to LAN 2, Bridge 2 has three connecting to LAN 2, LAN 3, and LAN 4. So, A can communicate with H through two bridges.

- **Bridges (Link Layer Device) –**
  It stores and forwards Ethernet frames, i.e., it has to do with the MAC address rather than the IP address, they handle the hardware addresses. I also examine the frame header and selectively forward frames based on MAC destination address, such as in the given figure if Bridge 2 receives a packet then it will selectively decide whether to send it to LAN 3 or LAN 4.
  When a frame is to be forwarded in a segment it uses CSMA/CD to access the segment. These are transparent, i.e., hosts are unaware of the presence of bridges, it appears to them as a single whole network. Bridges need not be configured they are plug-and-play and self-learning devices, i.e. a bridge has a learning table, they learn which hosts can be reached through which interfaces. At the physical level, the bridge boosts the signal strength like a

repeater or completely regenerates the signal.

- **Ethernet Bridges –**

  A bridge stores the hardware addresses observed from frames received by each interface and uses this information to learn which frames need to be forwarded by the bridge.

What if the host is moved to another segment or a new host is connected to a segment?
If a new host is connected then the learning process of bridges is going to be a continuous process. Suppose if we move from LAN 1 to LAN 2 some machine, i.e. MAC address moves from LAN 1 to LAN 2, which means table entries should leave after some time so that the data remains fresh and relevant.

Spanning Tree Bridges & their Protocol

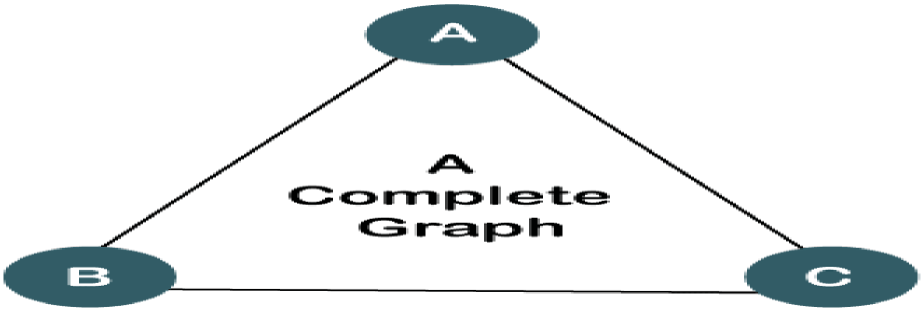
The spanning tree protocol is also known as STP. It is a protocol that monitors the overall performance of the network. The main task of the spanning tree protocol is to remove the redundant link. This protocol uses the Spanning tree algorithm (STA), which is used to detect the redundant link. The STA maintains the topology database that is used to find the redundant links. If the redundant link is found, then the link gets disabled. Once the redundant links are removed, then only those links will remain active which are chosen by the STA. If a new link is added or some existing link is removed, then the STA will be re-executed to adjust the changes.

Before understanding the spanning tree protocol, we first looked at the complete graph and spanning tree.

A complete graph is a graph in which a line connects each pair of vertices. In other words, we can say that all the points are connected by a maximum number of lines. In computer networking, the complete graph can also be said as a fully meshed network.

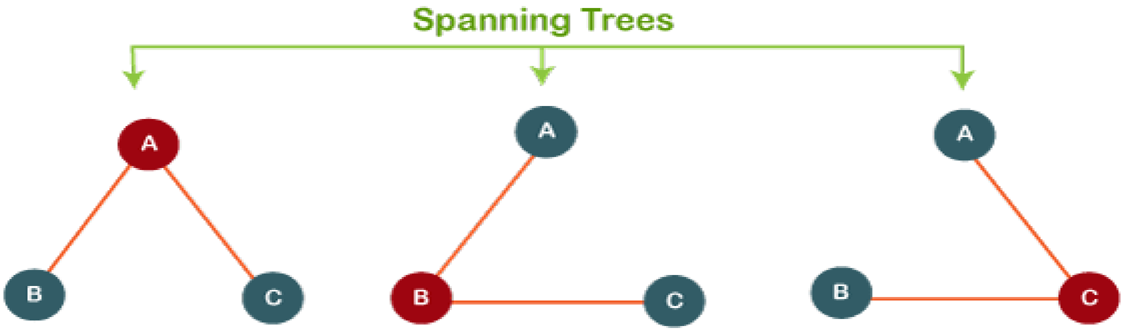
Let's understand the complete graph through an example.

Suppose there are three points, i.e., A, B, and C. Three lines connect these three points. A line connects every two-point, and we get a complete graph.



The complete graph is formed when a maximum number of lines connect all the points, whereas the spanning tree is formed when a minimum number of lines connects all the points.

From the above complete graph, we can get three spanning trees.



1. A is directly connected to B and C, while B and C are indirectly connected through A. In this spanning tree, A is a central point and all the points are connected without any formation of loops.
2. B is directly connected to A and C, while A and C are connected through B. B is a bridge between A and C, or we can say that B is a central point. In this case, also, all the points are connected without any formation of loops.

C is directly connected to both A and B, while A and B are connected through C. Therefore, C is a bridge between A and B, and C is a central point. In this case, all the points are connected without any formation of loops.

Till now, we have observed two basic features of spanning-tree:

- It does not contain any loop.

- It is minimally connected.

What is a spanning tree protocol?

The spanning tree protocol is a layer 2 protocol that tends to solve the problems when the computers use the shared telecommunications paths on a local area network. When they share the common path, if all the computers send the data simultaneously, it affects the overall network performance and brings all the network traffic near a halt.

The spanning tree protocol (STP) overcomes this situation by using the concept of bridge looping. Bridge looping is used when there are multiple connections between the two endpoints, and messages are sent continuously, which leads to the flooding of the network. To remove the looping, STP divides the LAN network into two or more segments with the help of a device known as bridges. The bridge is used to connect the two segments so when the message is sent, the message is passed through the bridge to reach the intended destination. The bridge determines whether the message is for the same segment or a different segment, and it works accordingly. This network segmentation greatly reduces the chances of a network coming to a halt.

How spanning tree protocol works?

The following are the steps that spanning tree protocol uses:

- This protocol selects one switch as a root bridge where the root bridge is a central point as when the message is sent; then it always passes through the bridge.
- It selects the shortest path from a switch to the root bridge.
- It blocks the links that cause the looping on a network, and all the blocked links are maintained as backups. It can also activate the blocked links whenever the active link fails. Therefore, we can say that it also provides fault tolerance on a network.

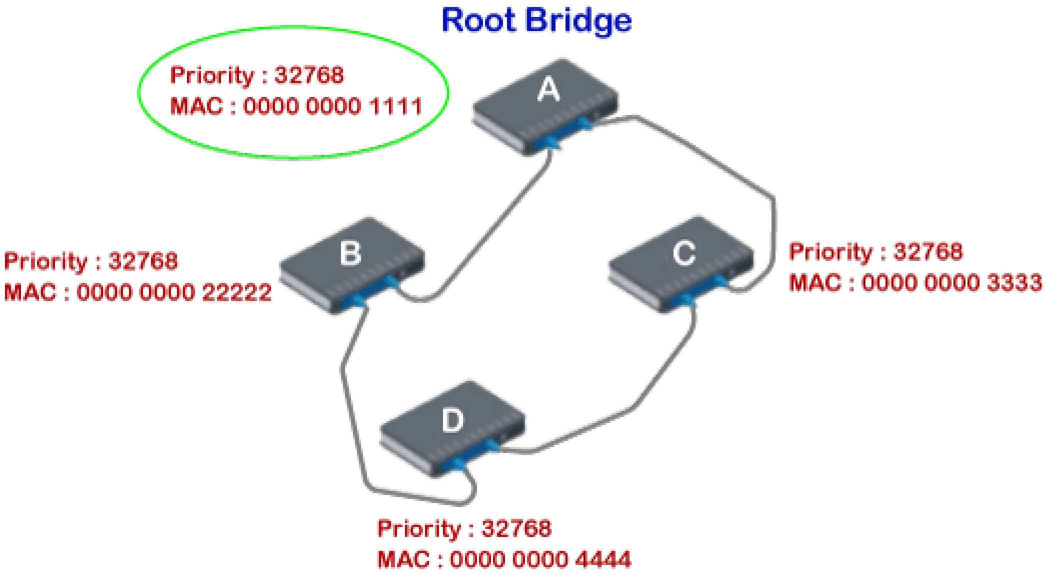
Ports in STP

There are five ports used in STP:

- **Root port:** The root port is a port that has the lowest cost path to the root bridge.
- **Designated port:** The designated port is a port that forwards the traffic away from the root bridge.
- **Blocking port:** The blocking port is a port that receives the frames, but it neither forwards nor sends the frames. It simply drops the received frames.
- **Backup port:** The backup port is a port that provides the backup path in a spanning

  tree if a designated port fails. This port gets active immediately when the designated port fails.
- **Alternate port:** The alternate port is a port that provides the alternate path to the root bridge if the root bridge fails.

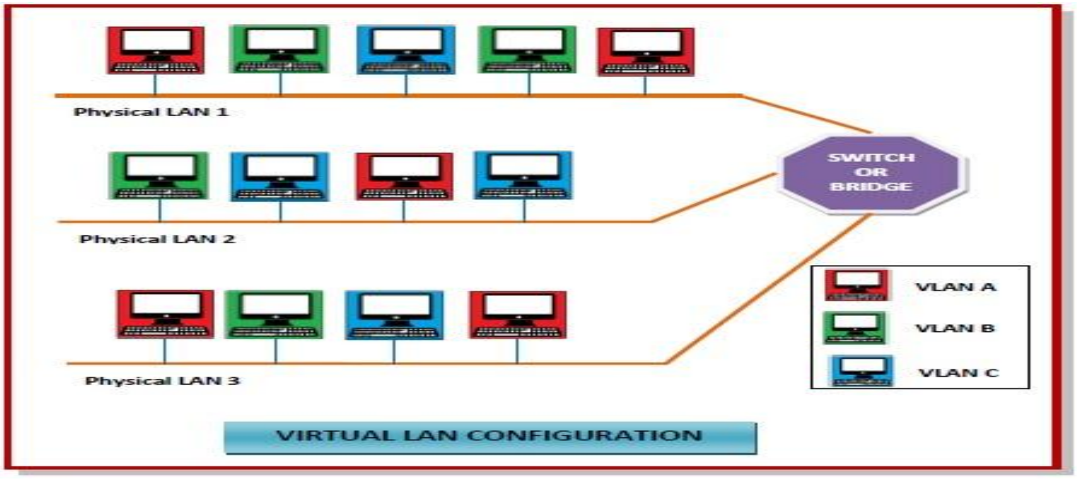
Let's understand through an example.



Suppose there are four switches A, B, C, and D on a local area network. There are redundant links that exist among these interconnected devices. In the above figure, there are two paths that exist, i.e., DBA and DCA. Link redundancy is good for network availability, but it creates layer 2 loops. The question arises "how network blocks the unwanted links to avoid the loops without destroying the link redundancy?". The answer to this question is STP. First, STP chooses one switch as a root bridge. In the above case, A switch is chosen as a root bridge. Next, other switches select the path to the root bridge, having the least path cost. Now we look at the switch B. For switch B, there are two paths that exist to reach switch A (root bridge), i.e., BDCA and BA. The path BDCA costs 7 while the path BA costs 2. Therefore, path BA is chosen to reach the root bridge. The port at switch B is selected as a root port, and the other end is a designated port. Now we look at the switch C. From switch C, there are two paths that exist, i.e., CDBA and CA. The least-cost path is CA, as it costs 1. Thus, it is selected as a root port, and the other end is selected as a designated port. Now we look at the switch D. For switch D, there are two paths that exist to reach switch A, i.e., DBA and DCA. The path DBA costs 4 while the DCA costs 5. Therefore, path DBA is chosen as it has the least cost path. The port on D is selected as a root port, and on the other end, switch B is selected as a designated port. In this example, we have observed that the root bridge can contain many designated ports, but it does not contain a root port.

What is Virtual LAN?

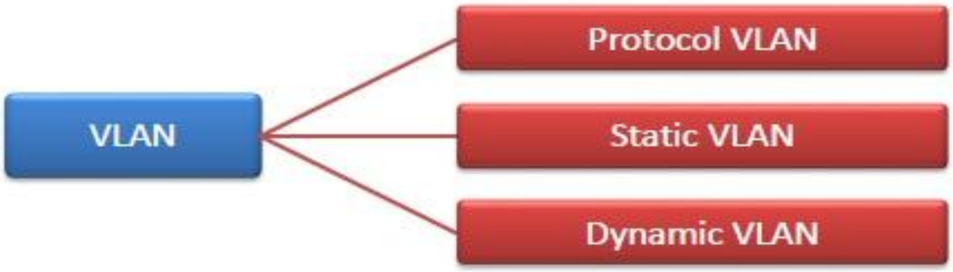
Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network. Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.



Features of VLANs

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

Types of VLANs



- Protocol VLAN − Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.
- Port-based VLAN − This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- Dynamic VLAN − Here, the network administrator simply defines network membership according to device characteristics.

Advantages –

- **Performance –**

  The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.
- **Formation of virtual groups –**

  As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.
- **Security –**

  In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
- **Flexibility –**

  VLAN provide flexibility to add, remove the number of host we want.
- **Cost reduction –**

  VLANs can be used to create broadcast domains which eliminate the need for expensive routers.

  By using Vlan, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.