Computer Network Components / Devices

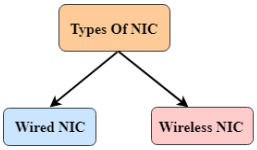
Computer network components are the *major parts* which are needed to *install the software*. Some important network components are **NIC**, **switch**, **cable**, **hub**, **router**, and **modem**. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

Following are the major components required to install a network:

NIC(Network Interface Card)

- NIC stands for network interface card.
- NIC is a hardware component used to connect a computer with another computer onto a network
- It can support a transfer rate of 10,100 to 1000 Mb/s.
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

There are two types of NIC:



1. Wired NIC
2. Wireless NIC

Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

Wireless NIC: The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

Hub

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

- **Active Hub:-** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub:-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub:-** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Switch

Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Types of Switch

1. **Unmanaged switches**: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. **Managed switches**: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. **Smart switches**: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
4. **Layer 2 switches**: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
5. **Layer 3 switches**: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
6. **PoE switches**: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
7. **.**
8.
9. : These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
10. Rack-mounted switches: These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
11. Desktop switches: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
12. Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Router

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Advantages Of Router:

- **Security:** The information which is transmitted to the network will traverse the entire cable, but the only specified device which has been addressed can read the data.
- **Reliability:** If the server has stopped functioning, the network goes down, but no other networks are affected that are served by the router.
- **Performance:** Router enhances the overall performance of the network. Suppose there are 24 workstations in a network generates a same amount of traffic. This increases the traffic load on the network. Router splits the single network into two networks of 12 workstations each, reduces the traffic load by half.
- **Network range**

Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

- Standard PC modem or Dial-up modem
- Cellular Modem
- Cable modem

Cables and Connectors

Cable is a transmission media used for transmitting a signal.

There are three types of cables used in transmission:

- Twisted pair cable
- Coaxial cable
- Fibre-optic cable

Repeater

– A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal

becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device

Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

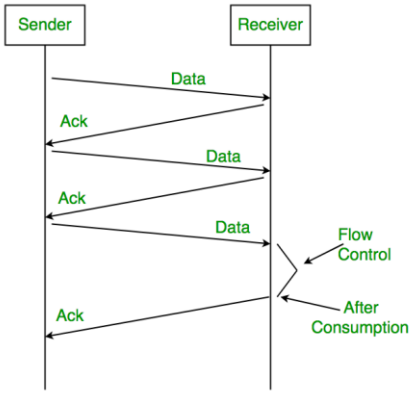
- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Simple Stop and Wait protocol:

Sender:
Rule 1) Send one data packet at a time.
Rule 2) Send the next packet only after receiving acknowledgement for the previous.

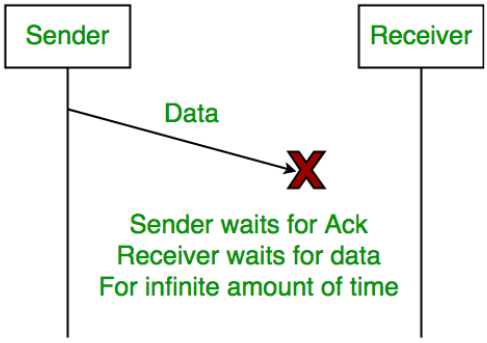
Receiver:

Rule 1) Send acknowledgement after receiving and consuming a data packet.
Rule 2) After consuming packet acknowledgement need to be sent (Flow Control)

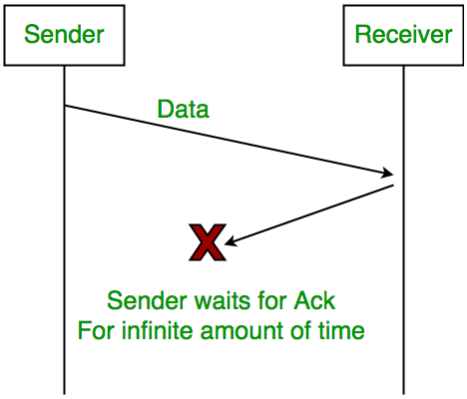


Problems :

1. Lost Data



2. Lost Acknowledgement:



3. Delayed Acknowledgement/Data: After a timeout on the sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop and Wait ARQ

Useful Terms:

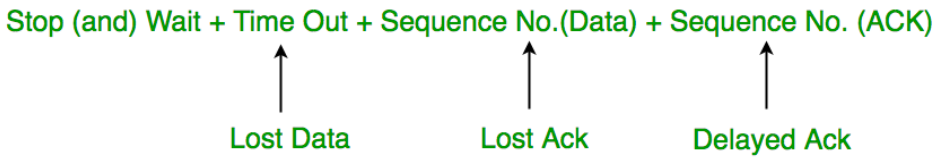
- **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.

  Propagation Delay = (Distance between routers) / (Velocity of propagation)

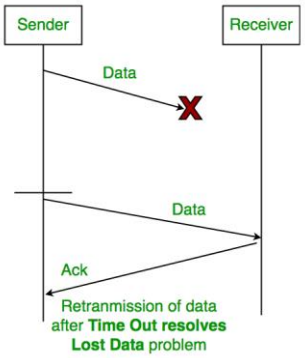
- RoundTripTime (**RTT**) = Amount of time taken by a packet to reach the receiver + Time taken by the Acknowledgement to reach the sender
- TimeOut (**TO**) = 2* RTT
- Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 255 seconds)

Stop and Wait for ARQ (Automatic Repeat Request)

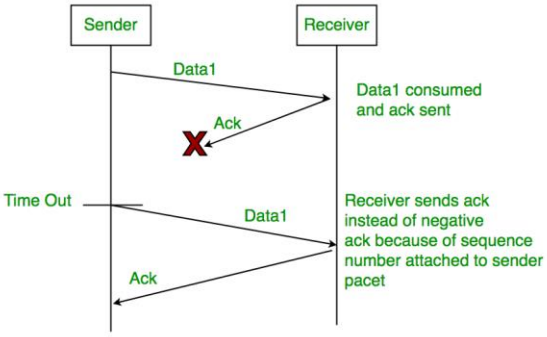
The above 3 problems are resolved by Stop and Wait for ARQ (Automatic Repeat Request) that does both error control and flow control.



1. Time Out:



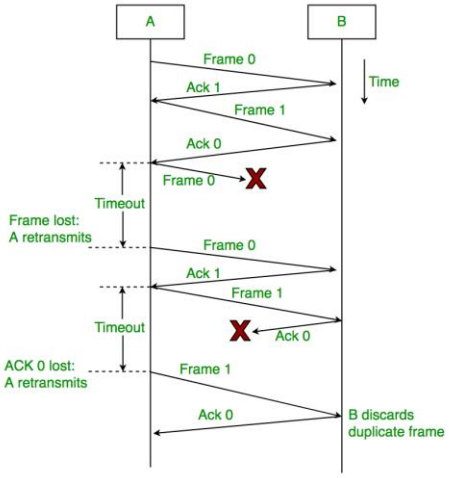
2. Sequence Number (Data)



3. Delayed Acknowledgement:
This is resolved by introducing sequence numbers for acknowledgement also.

Working of Stop and Wait for ARQ:

1) Sender A sends a data frame or packet with sequence number 0.
2) Receiver B, after receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet)
There is only a one-bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.



Characteristics of Stop and Wait ARQ:

- It uses a link between sender and receiver as a half-duplex link
- Throughput = 1 Data packet/frame per RTT
- If the Bandwidth*Delay product is very high, then they stop and wait for protocol if it is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example of "**Closed Loop OR connection-oriented** " protocols
- It is a special category of SWP where its window size is 1
- Irrespective of the number of packets sender is having stop and wait for protocol requires only 2 sequence numbers 0 and 1

Constraints:

Stop and Wait ARQ has very less efficiency , it can be improved by increasing the window size. Also , for better efficiency , Go back N and Selective Repeat Protocols are used.

The Stop and Wait ARQ solves the main three problems but may cause big performance issues as the sender always waits for acknowledgement even if it has the next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country through a high-speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence number. We will be discussing these protocols in the next articles.

So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections but performs badly for distant connections like satellite connections.

Advantages of Stop and Wait ARQ :

- **Simple Implementation:** Stop and Wait ARQ is a simple protocol that is easy to implement in both hardware and software. It does not require complex algorithms or hardware components, making it an inexpensive and efficient option.
- **Error Detection:** Stop and Wait ARQ detects errors in the transmitted data by using checksums or cyclic redundancy checks (CRC). If an error is detected, the receiver sends a negative acknowledgment (NAK) to the sender, indicating that the data needs to be retransmitted.
- **Reliable:** Stop and Wait ARQ ensures that the data is transmitted reliably and in order. The receiver cannot move on to the next data packet until it receives the current one. This ensures that the data is received in the correct order and eliminates the possibility of data corruption.
- **Flow Control:** Stop and Wait ARQ can be used for flow control, where the receiver can control the rate at which the sender transmits data. This is useful in situations where the receiver has limited buffer space or processing power.
- **Backward Compatibility:** Stop and Wait ARQ is compatible with many existing systems and protocols, making it a popular choice for communication over unreliable channels.

Disadvantages of Stop and Wait ARQ :

- **Low Efficiency:** Stop and Wait ARQ has low efficiency as it requires the sender to wait for an acknowledgment from the receiver before sending the next data packet. This results in a low data transmission rate, especially for large data sets.
- **High Latency:** Stop and Wait ARQ introduces additional latency in the transmission of data, as the sender must wait for an acknowledgment before sending the next packet. This can be a problem for real-time applications such as video streaming or online gaming.
- **Limited Bandwidth Utilization:** Stop and Wait ARQ does not utilize the available bandwidth efficiently, as the sender can transmit only one data packet at a time. This

results in underutilization of the channel, which can be a problem in situations where the available bandwidth is limited.

- **Limited Error Recovery:** Stop and Wait ARQ has limited error recovery capabilities. If a data packet is lost or corrupted, the sender must retransmit the entire packet, which can be time-consuming and can result in further delays.
- **Vulnerable to Channel Noise:** Stop and Wait ARQ is vulnerable to channel noise, which can cause errors in the transmitted data. This can result in frequent retransmissions and can impact the overall efficiency of the protocol.

Sliding Window Protocol

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

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

Types of Sliding Window Protocol

Sliding window protocol has two types:

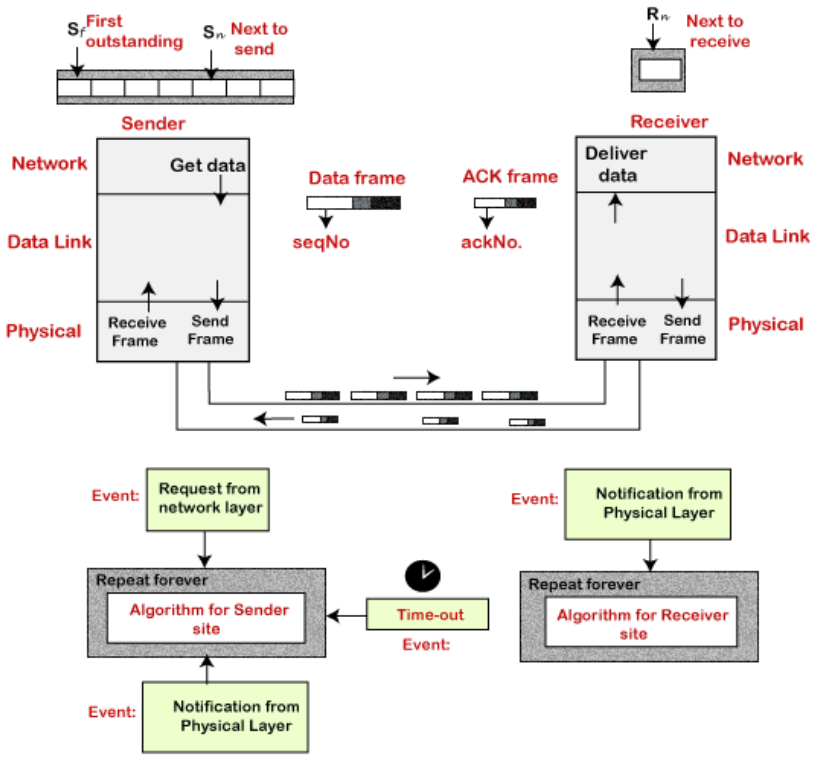
1. Go-Back-N ARQ
2. Selective Repeat ARQ

Go-Back-N ARQ

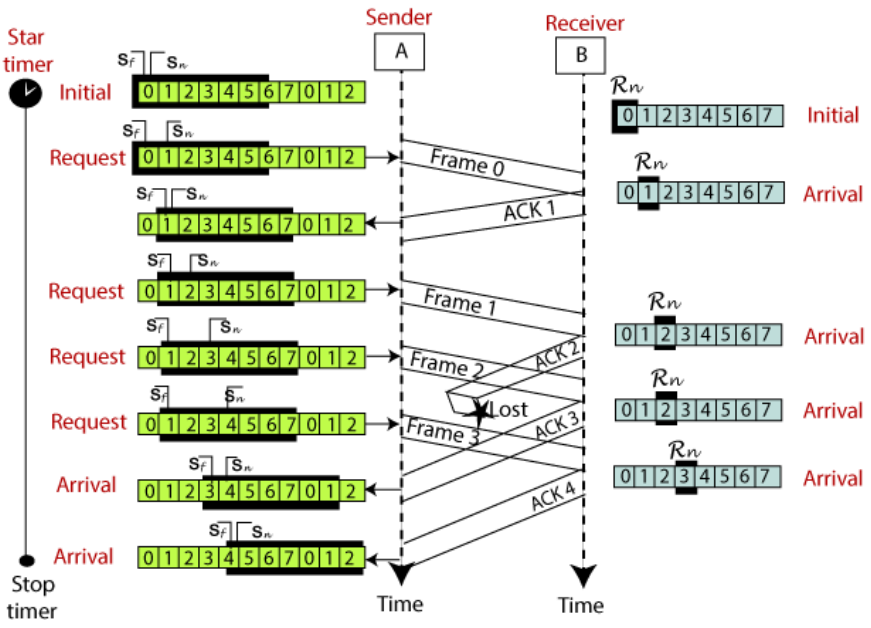
Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

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

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



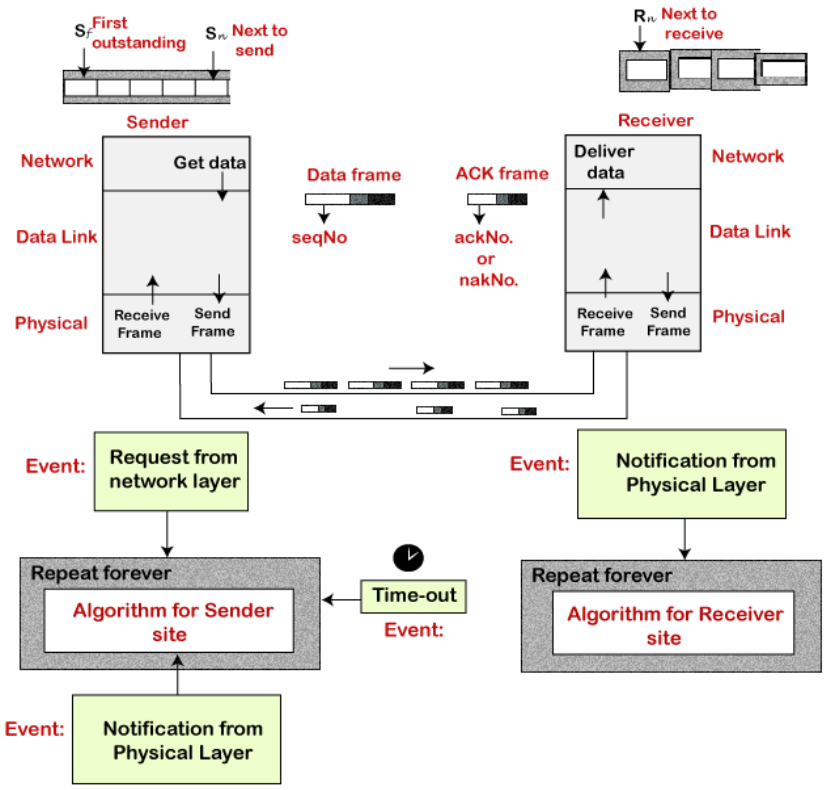
The example of Go-Back-N ARQ is shown below in the figure.



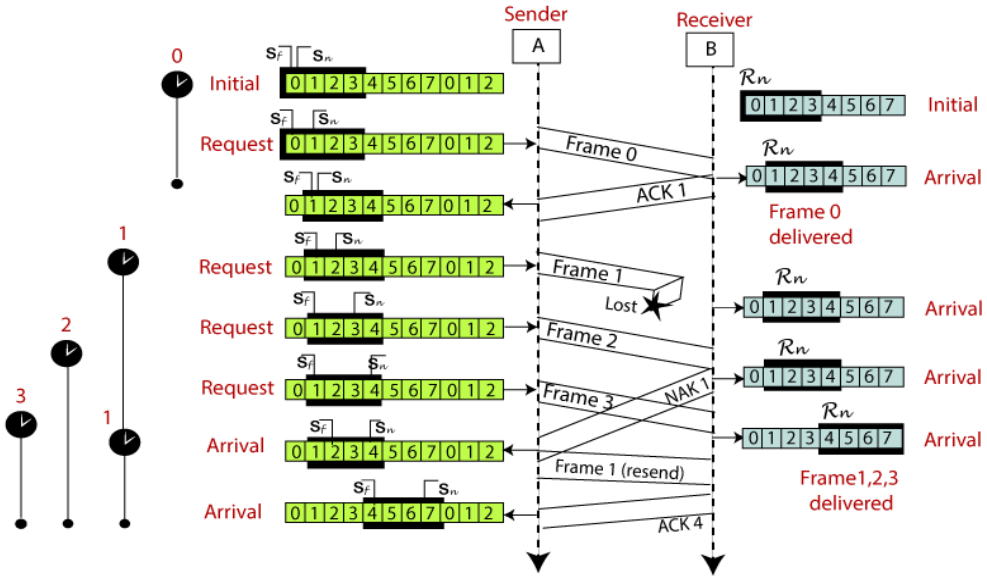
Selective Repeat ARQ

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

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



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



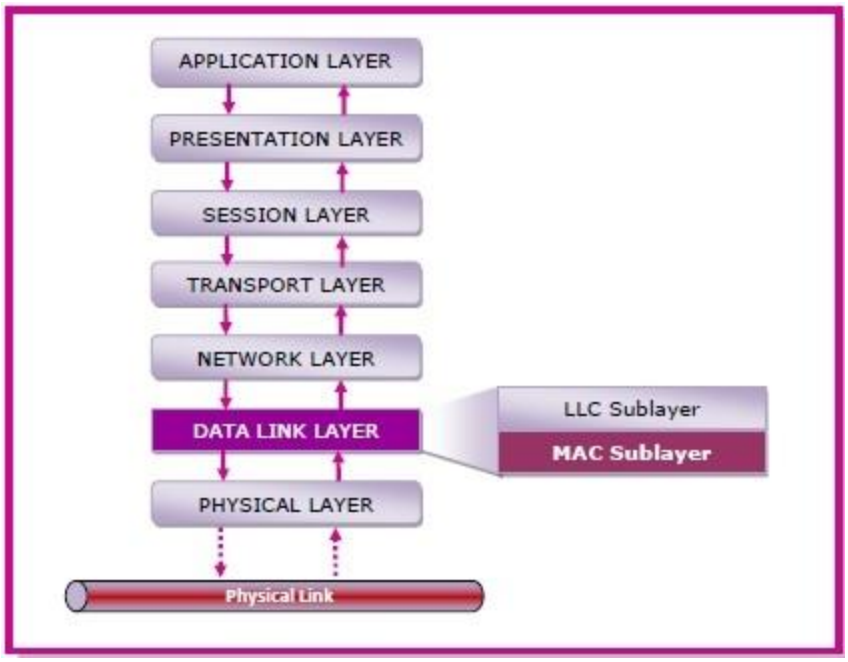
Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is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

MAC Layer

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sublayers –

- The logical link control (LLC) sublayer
- The medium access control (MAC) sublayer

The following diagram depicts the position of the MAC layer –



Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC Addresses

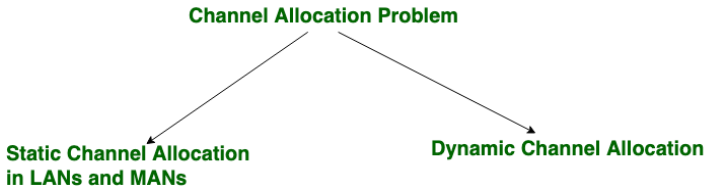
MAC address or media access control address is a unique identifier allotted to a **network interface controller (NIC)** of a device. It is used as a network address for data transmission within a network segment like **Ethernet**, **Wi-Fi**, and **Bluetooth**.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two

hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

Channel Allocation Problem in Computer Network

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



These are explained as following below.

1. Static Channel Allocation in LANs and MANs:

It is the classical or traditional approach of allocating a single channel among multiple competing users using Frequency Division Multiplexing (FDM). if there are N users, the frequency channel is divided into N equal sized portions (bandwidth), each user being assigned one portion. since each user has a private frequency band, there is no interference between users.
However, it is not suitable in case of a large number of users with variable bandwidth requirements.
It is not efficient to divide into fixed number of chunks.

T = 1/(U*C-L)

T(FDM) = N*T(1/U(C/N)-L/N)

Where,

T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time

2. Dynamic Channel Allocation:
In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.
This allocation scheme optimises bandwidth usage and results is faster transmissions.
Dynamic channel allocation is further divided into:

1. **Centralised Allocation**
2. **Distributed Allocation**

Possible assumptions include:

Station Model:
Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.

Single Channel Assumption:
In this allocation all stations are equivalent and can send and receive on that channel.

Collision Assumption:
If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must re transmitted. Collisions are only possible error.

Time can be divided into Slotted or Continuous.

Stations can sense a channel is busy before they try it.
Protocol Assumption:

- N independent stations.
- A station is blocked until its generated frame is transmitted.

- probability of a frame being generated in a period of length Dt is IDt where I is the arrival rate of frames.
- Only a single Channel available.
- Time can be either: Continuous or slotted.
- **Carrier Sense:** A station can sense if a channel is already busy before transmission.
- **No Carrier Sense:** Time out used to sense loss data.

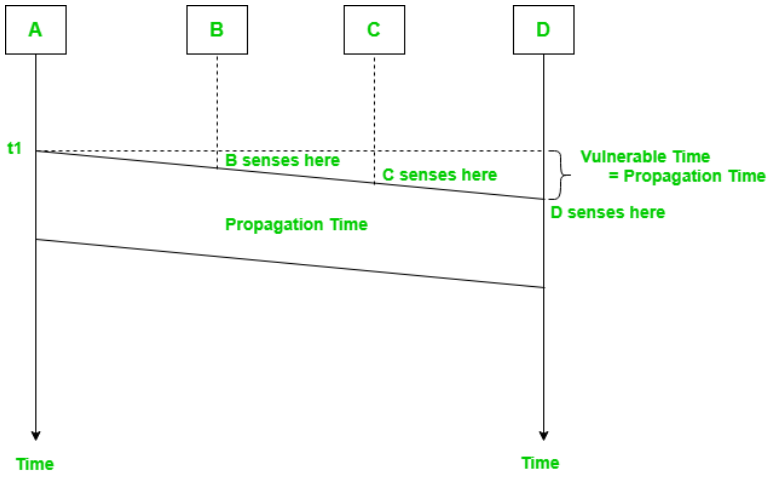
Carrier Sense Multiple Access (CSMA)

- This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

Prerequisite - Multiple Access Protocols

Vulnerable Time:

Vulnerable time = Propagation time (Tp)



The persistence methods can be applied to help the station take action when the channel is busy/idle.

Types of CSMA Access Modes:

There are 4 types of access modes available in CSMA. It is also referred as 4 different types of CSMA protocols which decide the time to start sending data across shared media.

1. **1-Persistent:** It senses the shared channel first and delivers the data right away if the channel is idle. If not, it must wait and ***continuously*** track for the channel to become idle and then broadcast the frame without condition as soon as it does. It is an aggressive transmission algorithm.
2. **Non-Persistent:** It first assesses the channel before transmitting data; if the channel is idle, the node transmits data right away. If not, the station must wait for an arbitrary amount of time (***not continuously***), and when it discovers the channel is empty, it sends the frames.
3. **P-Persistent:** It consists of the 1-Persistent and Non-Persistent modes combined. Each node observes the channel in the 1Persistent mode, and if the channel is idle, it sends a frame with a P probability. If the data is not transferred, the frame restarts with the following time slot after waiting for a (q = 1-p probability) random period.
4. **O-Persistent:** A supervisory node gives each node a transmission order. Nodes wait for their time slot according to their allocated transmission sequence when the transmission medium is idle.

Advantages of CSMA:

1. **Increased efficiency:** CSMA ensures that only one device communicates on the network at a time, reducing collisions and improving network efficiency.
2. **Simplicity:** CSMA is a simple protocol that is easy to implement and does not require complex hardware or software.
3. **Flexibility:** CSMA is a flexible protocol that can be used in a wide range of network environments, including wired and wireless networks.
4. **Low cost:** CSMA does not require expensive hardware or software, making it a cost-effective solution for network communication.

Disadvantages of CSMA:

1. **Limited scalability:** CSMA is not a scalable protocol and can become inefficient as the number of devices on the network increases.
2. **Delay:** In busy networks, the requirement to sense the medium and wait for an available channel can result in delays and increased latency.
3. **Limited reliability:** CSMA can be affected by interference, noise, and other factors, resulting in unreliable communication.
4. **Vulnerability to attacks:** CSMA can be vulnerable to certain types of attacks, such as jamming and denial-of-service attacks, which can disrupt network communication.

Collision Detection in CSMA/CD

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media access control method that was widely used in Early Ethernet technology/LANs when there used to be shared Bus Topology and each node (Computers) were connected By Coaxial Cables. Now a Days Ethernet is Full Duplex and Topology is either Star (connected via Switch or Router) or Point to Point (Direct Connection). Hence CSMA/CD is not used but they are still supported though.

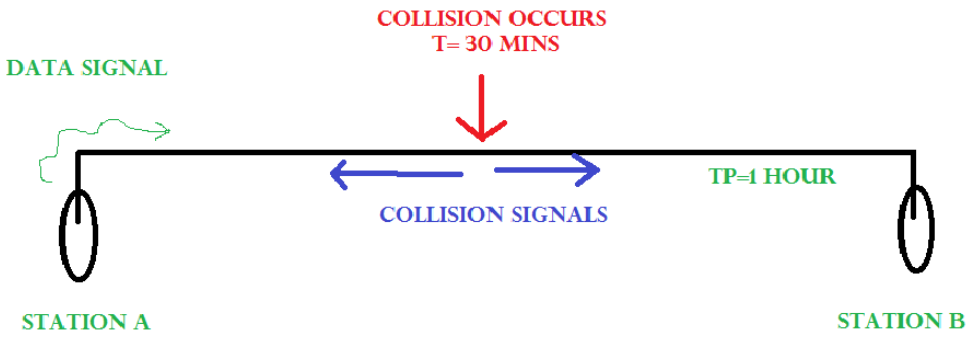
Consider a scenario where there are 'n' stations on a link and all are waiting to transfer data through that channel. In this case, all 'n' stations would want to access the link/channel to transfer their own data. The problem arises when more than one station transmits the data at the moment. In this case, there will be collisions in the data from different stations.

CSMA/CD is one such technique where different stations that follow this protocol agree on some terms and collision detection measures for effective transmission. This protocol decides which station will transmit when so that data reaches the destination without corruption.

How CSMA/CD works?

- **Step 1:** Check if the sender is ready for transmitting data packets.
- **Step 2:** Check if the transmission link is idle.
  Sender has to keep on checking if the transmission link/medium is idle. For this, it continuously senses transmissions from other nodes. Sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise, it refrains from sending data.
- **Step 3:** Transmit the data & check for collisions.
  Sender transmits its data on the link. CSMA/CD does not use an 'acknowledgment' system. It checks for successful and unsuccessful transmissions through collision signals. During transmission, if a collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time intervals before it resends the frame. After some random time, it again attempts to transfer the data and repeats the above process.
- **Step 4:** If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

How does a station know if its data collide?



Consider the above situation. Two stations, A & B.
Propagation Time: Tp = 1 hr (Signal takes 1 hr to go from A to B)

At time t=0, A transmits its data.

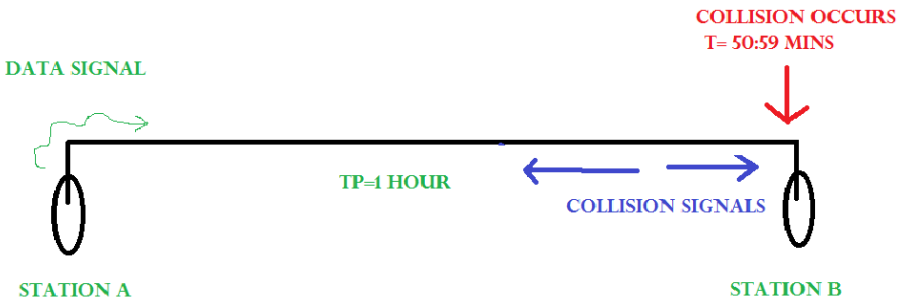
t= 30 mins : Collision occurs.

After the collision occurs, a collision signal is generated and sent to both A & B to inform the stations about the collision. Since the collision happened midway, the collision signal also takes 30 minutes to reach A & B.

Therefore, t=1 hr: A & B receive collision signals.

This collision signal is received by all the stations on that link. Then,

How to ensure that it is our station's data that collided?
For this, Transmission time (Tt) > Propagation Time (Tp) [Rough bound]
This is because we want that before we transmit the last bit of our data from our station, we should at least be sure that some of the bits have already reached their destination. This ensures that the link is not busy and collisions will not occur.
But, above is a loose bound. We have not taken the time taken by the collision signal to travel back to us. For this consider the worst-case scenario.
Consider the above system again.



At time t=0, A transmits its data.

t= 59:59 mins : Collision occurs

This collision occurs just before the data reaches B. Now the collision signal takes 59:59 minutes again to reach A. Hence, A receives the collision information approximately after 2 hours, that is, after 2 * Tp.

Hence, to ensure tighter bound, to detect the collision completely,

Tt > >= 2 * Tp

This is the maximum collision time that a system can take to detect if the collision was of its own data.

What should be the minimum length of the packet to be transmitted?

Transmission Time = Tt = Length of the packet/ Bandwidth of the link

[Number of bits transmitted by sender per second]

Substituting above, we get,

Length of the packet/ Bandwidth of the link>= 2 * Tp

Length of the packet >= 2 * Tp * Bandwidth of the link

Padding helps in cases where we do not have such long packets. We can pad extra characters to the end of our data to satisfy the above condition.

Collision detection in CSMA/CD involves the following features:

- **Carrier sense:** Before transmitting data, a device listens to the network to check if the transmission medium is free. If the medium is busy, the device waits until it becomes free before transmitting data.
- **Multiple Access:** In a CSMA/CD network, multiple devices share the same transmission medium. Each device has equal access to the medium, and any device can transmit data when the medium is free.
- **Collision detection:** If two or more devices transmit data simultaneously, a collision occurs. When a device detects a collision, it immediately stops transmitting and sends a jam signal to inform all other devices on the network of the collision. The devices then wait for a random time before attempting to transmit again, to reduce the chances of another collision.
- **Backoff algorithm:** In CSMA/CD, a backoff algorithm is used to determine when a device can retransmit data after a collision. The algorithm uses a random delay before a device retransmits data, to reduce the likelihood of another collision occurring.

- **Minimum frame size:** CSMA/CD requires a minimum frame size to ensure that all devices have enough time to detect a collision before the transmission ends. If a frame is too short, a device may not detect a collision and continue transmitting, leading to data corruption on the network.

Advantages of CSMA/CD:

- **Simple and widely used:** CSMA/CD is a widely used protocol for Ethernet networks, and its simplicity makes it easy to implement and use.
  Fairness: In a CSMA/CD network, all devices have equal access to the transmission medium, which ensures fairness in data transmission.
  Efficiency: CSMA/CD allows for efficient use of the transmission medium by preventing unnecessary collisions and reducing network congestion.

Disadvantages of CSMA/CD:

- **Limited scalability:** CSMA/CD has limitations in terms of scalability, and it may not be suitable for large networks with a high number of devices.
  Vulnerability to collisions: While CSMA/CD can detect collisions, it cannot prevent them from occurring. Collisions can lead to data corruption, retransmission delays, and reduced network performance.
  Inefficient use of bandwidth: CSMA/CD uses a random backoff algorithm that can result in inefficient use of network bandwidth if a device continually experiences collisions.
  Susceptibility to security attacks: CSMA/CD does not provide any security features, and the protocol is vulnerable to security attacks such as packet sniffing and spoofing.

Efficiency of CSMA/CD

Carrier sense multiple access with collision detection (CSMA/CD) – The CSMA method does not tell us what to do in case there is a collision. Carrier sense multiple access with collision detection (CSMA/CD) adds to the CSMA algorithm to deal with the collision. In CSMA/CD, the size of a frame must be large enough so that collision can be detected by the sender while sending the frame. So, the frame transmission delay must be at least *two times* the maximum propagation delay. Assume some station transmitted data packet and successfully get to the destination but it is just the *Best Case*, so we have to take the *Worst Case* scenario in which there will be contention slots. Contention slots are those slots that are not able to transmit their

journey due to the collision. Suppose station A transmitted data but collide and the worst-case time wasted is **2Tp** and then some station B found out a way to transmit the data so it took (As shown in Figure)

Tp (propagation delay) + Tt(transmission time)

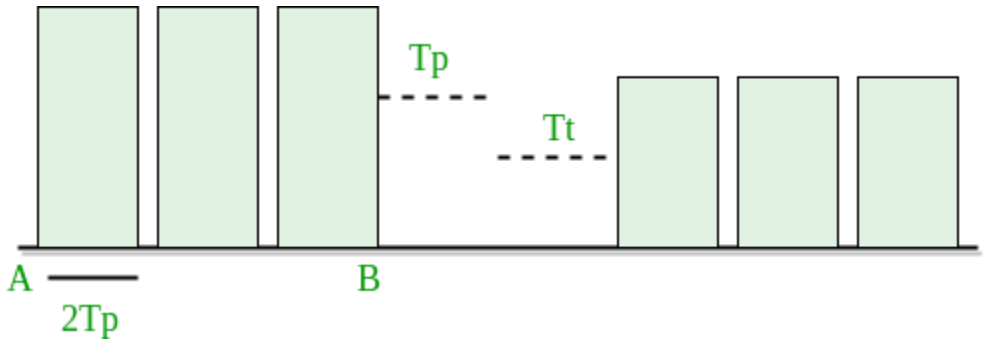
Now we don't know how many contention slots, so we consider the worst-case to be of **n** contention slots.

Efficiency = Tt / (C*2*Tp + Tt + Tp)

Tt - transmission time

Tp - propagation time

C - number of collision



Efficiency = 1/(e*2a + 1 + a)

a = Tp/Tt

e = 2.72

Now

Efficiency = 1/(1 + 6.44a)

Further Analysis of Efficiency :

Efficiency = 1/ (1 + 6.44a)

= 1/ {1 + 6.44(Tp/Tt)}

= 1/ {1 + 6.44((distance/speed)/(packet length/Bandwidth))}

= 1/ {1+ 6.44 ((distance * bandwidth)/ (speed*packet length))}

From this derivation, we can conclude many relations :

- If distance increases, the efficiency of CSMA decreases.
- CSMA is not suitable for long-distance networks like WAN but works optimally for LAN.
- If the length of the packet is bigger, the efficiency of CSMA also increases; but the maximum limit for length is 1500 Bytes.
- Transmission Time >= 2*Propagation Time

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision. In the case of wireless networks, most of the energy is used for transmission, and the energy of the received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.
These are three types of strategies:

1. **InterFrame Space (IFS):** When a station finds the channel busy it senses the channel again, when the station finds a channel to be idle it waits for a period of time called **IFS time**. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
2. **Contention Window:** It is the amount of time divided into slots. A station that is ready to send frames chooses a random number of slots as **wait time**.
3. **Acknowledgments:** The positive acknowledgments and time-out timer can help guarantee a successful transmission of the frame.

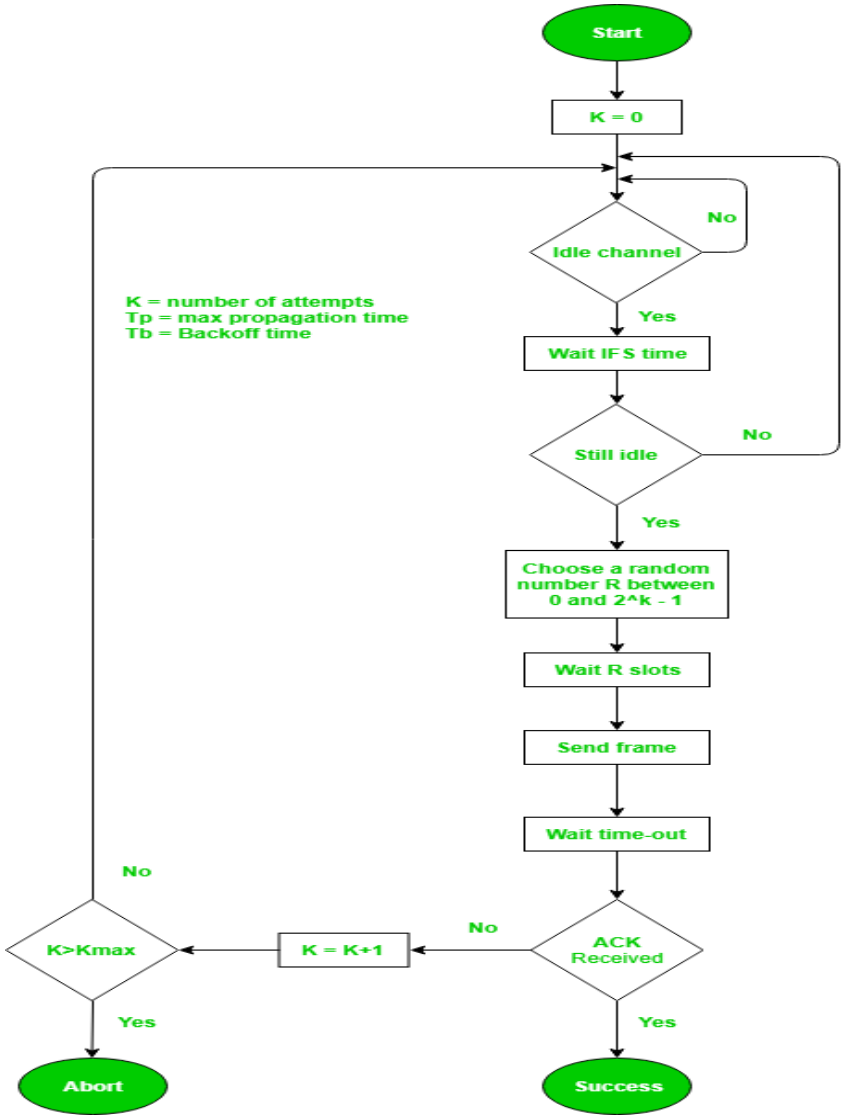
Characteristics of CSMA/CA :

1. **Carrier Sense**: The device listens to the channel before transmitting, to ensure that it is not currently in use by another device.

2. **Multiple Access**: Multiple devices share the same channel and can transmit simultaneously.
3. **Collision Avoidance**: If two or more devices attempt to transmit at the same time, a collision occurs. CSMA/CA uses random backoff time intervals to avoid collisions.
4. **Acknowledgment (ACK)**: After successful transmission, the receiving device sends an ACK to confirm receipt.
5. **Fairness**: The protocol ensures that all devices have equal access to the channel and no single device monopolizes it.
6. **Binary Exponential Backoff**: If a collision occurs, the device waits for a random period of time before attempting to retransmit. The backoff time increases exponentially with each retransmission attempt.
7. **Interframe Spacing**: The protocol requires a minimum amount of time between transmissions to allow the channel to be clear and reduce the likelihood of collisions.
8. **RTS/CTS Handshake**: In some implementations, a Request-To-Send (RTS) and Clear-To-Send (CTS) handshake is used to reserve the channel before transmission. This reduces the chance of collisions and increases efficiency.
9. **Wireless Network Quality**: The performance of CSMA/CA is greatly influenced by the quality of the wireless network, such as the strength of the signal, interference, and network congestion.
10. **Adaptive Behavior**: CSMA/CA can dynamically adjust its behavior in response to changes in network conditions, ensuring the efficient use of the channel and avoiding congestion.

Overall, CSMA/CA balances the need for efficient use of the shared channel with the need to avoid collisions, leading to reliable and fair communication in a wireless network.

Process: The entire process of collision avoidance can be explained as follows:



Collision-Free Protocols in Computer Network

- Almost all collisions can be avoided in **CSMA/CD** but they can still occur during the contention period. The collision during the 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 came 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?

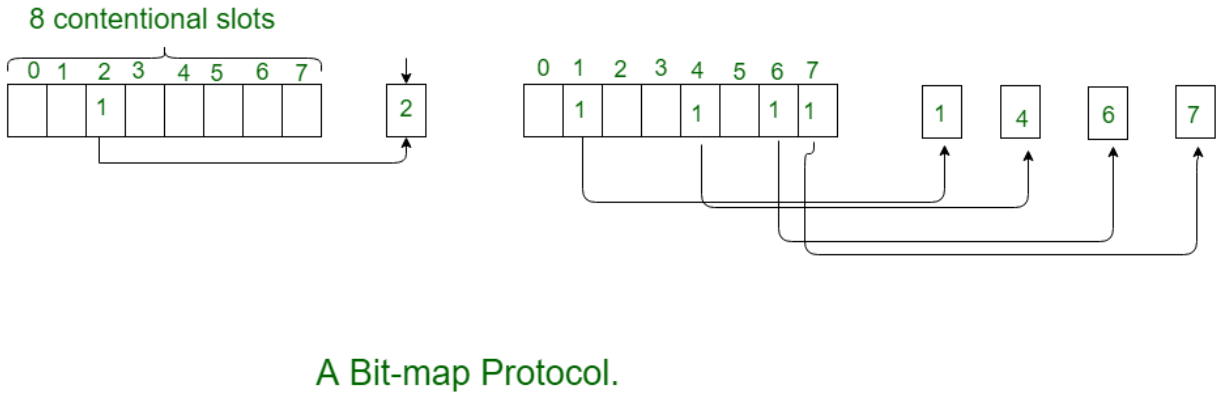
Collision Free Protocols:

- 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 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 corresponding slot. For example, if station 2 has a frame to send, it transmits a 1 bit to the 2nd 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.



Bit Map Protocol fig (1.1)

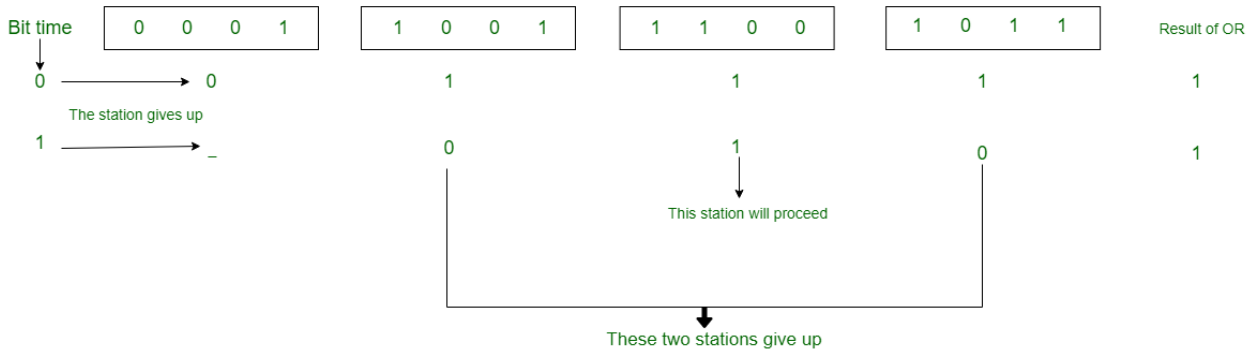
For analyzing the performance of this protocol, We will measure time in units of the contention bits slot, with a data frame consisting of d time units. Under low load conditions, the bitmap will simply be repeated over and over, for lack of data frames. All the stations have something to send all the 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 read 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 read together. Station 0001 see the 1 MSB in another station address 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 station at which next bit is 1 is at station 1100, so station 1011 and 1001 give up because there 2nd bit is 0. Then station 1100 starts transmitting a frame, after which another bidding cycle starts.



Binary countdown

Binary Countdown fig (1.2)

3. Limited Contention Protocols:

- 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 :

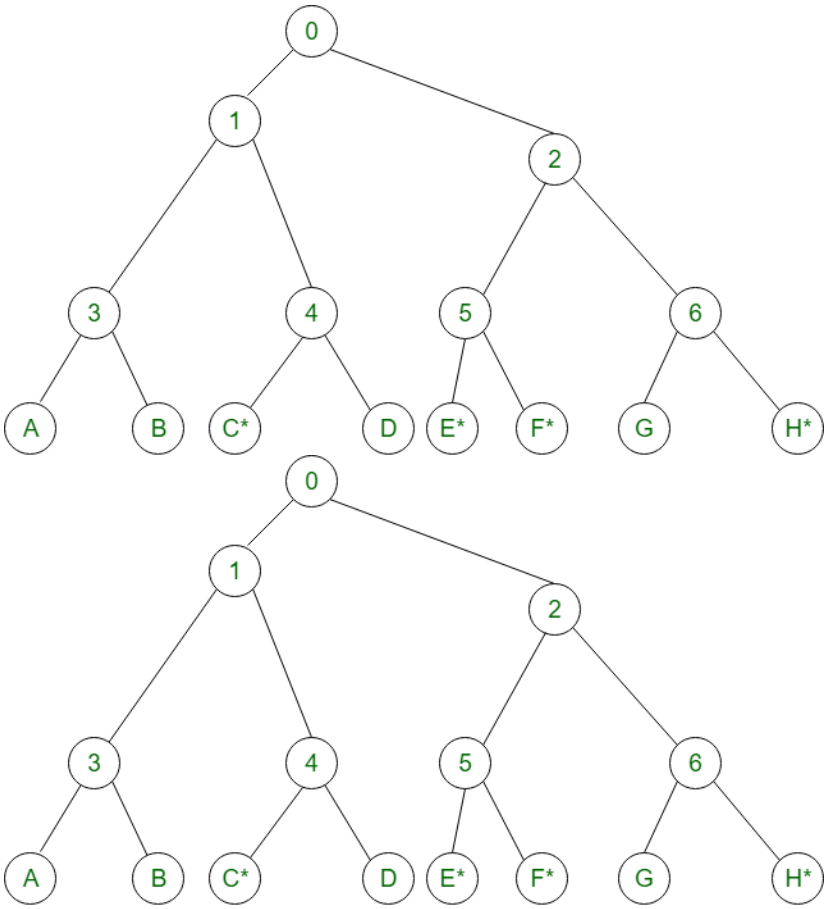
1. Behave like the ALOHA scheme under light load
2. Behave like the bitmap scheme under heavy load.

4. 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 :

1. treat every stations as the leaf of a binary tree
2. first slot (after successful transmission), all stations can try to get the slot(under the root node).
3. If no conflict, fine.
4. Else, in case of conflict, only nodes under a subtree get to try for the next one. (depth first search)



Adaptive Tree Walk Protocol fig (1.3)

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 1 can 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.

FDDI

Fiber Distributed Data Interface or FDDI in computer network is a technology primarily used as an internet backbone in Metropolitan Area Networks (MAN) or Campus Area Networks (CAN). It can transmit 100 megabits of data per second and uses a token ring protocol. You can learn about this article's history, uses, and design in this article.

What is Fiber Distributed Data Interface?

Fiber Distributed Data Interface is a network technology that works on the OSI model's physical and data link layer. It derives its transmission protocol from IEEE 802.4 and follows the ANSI standard X3T9. It transmitted data faster than existing ethernet technology, which was 10 Mbps ethernet. FDDI used Optical Fibers to transfer data much quicker than ethernet cables in the 1980s. FDDI had a dual-ring system, with each ring transmitting data in opposite directions; one FDDI ring was backup. When the primary network ring failed, the data transmission channel changed to the second one. This feature made it highly fault-tolerant and reliable.

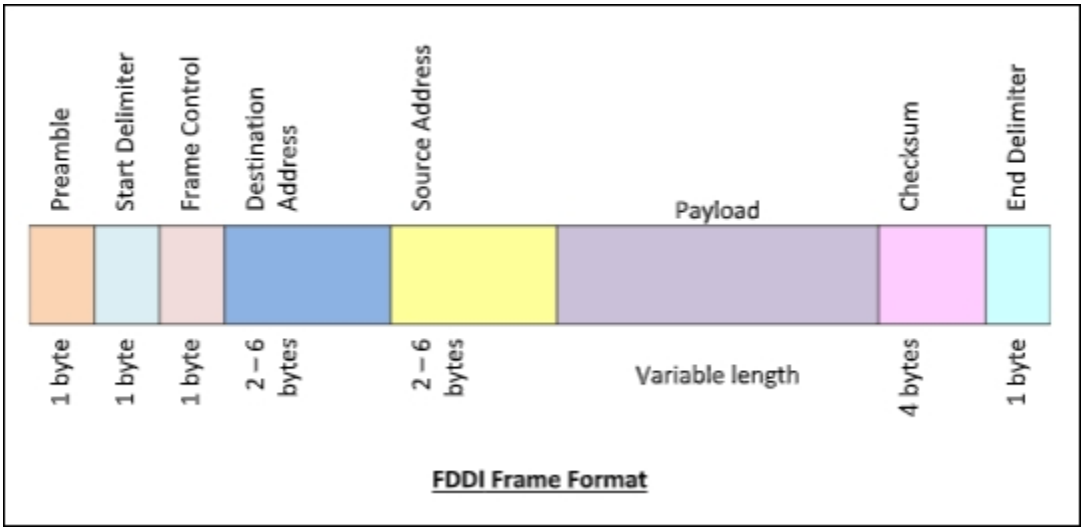
Moreover, the 100 Mbps speed was revolutionary at its launch. FDDI's transmission protocol was also better than the IEEE 802.4, enabling faster data transfer. The Fiber Distributed Data Interface is suitable for LANs, MANs, and CANs but not ideal for a WAN due to some limitations, like low coverage and the requirement of repeaters at frequent intervals.

Fiber Distributed Data Interface: How does it work?

Fiber Distributed Data Interface works using a **token ring protocol** similar to IEEE 802.4. However, instead of using priority for transmission, FDDI uses timed

tokens. That means if any host wants to send a message, it captures the transmitted token. The host can then transmit data for a fixed time. After the allowed time, the captured token passes to the next host. Every host can access the transmitted data and check the destination MAC address. And the network host accepts the data if the destination address matches its own.
Hosts transmit and receive data as frames. Each frame includes the following components:

1. Preamble for synchronization: 1 byte
2. Start Delimiter to indicate the start of the frame: 1 byte
3. Frame Control to specify if it is a control frame or data frame: 1 byte
4. Destination MAC Address: 2-6 bytes
5. Source MAC Address: 2-6 bytes
6. Payload containing the data for transmission: size varies
7. Checksum for verifying the data integrity: 4 bytes
8. End Delimiter: 1 byte



Fiber Distributed Data Interface: History and Use

Campus Area Networks (CANs) and Metropolitan Area Networks (MANs) started using FDDI in the late 1980s. Its speed and capability of connecting up to 1000 hosts were perfect for CANs or MANs; ethernet transmitted only at 10 Mbps

compared to 100 Mbps of FDDI. Besides CAN and MAN, you can also use FDDI to interconnect servers in a room.

With the launch of GigaBit ethernet in 1986, Fiber Distributed Data Interface lost popularity. Gigabit internet provides speeds up to 1Gbps and has a lower installation cost; fiber deployment cost for FDDI are high.

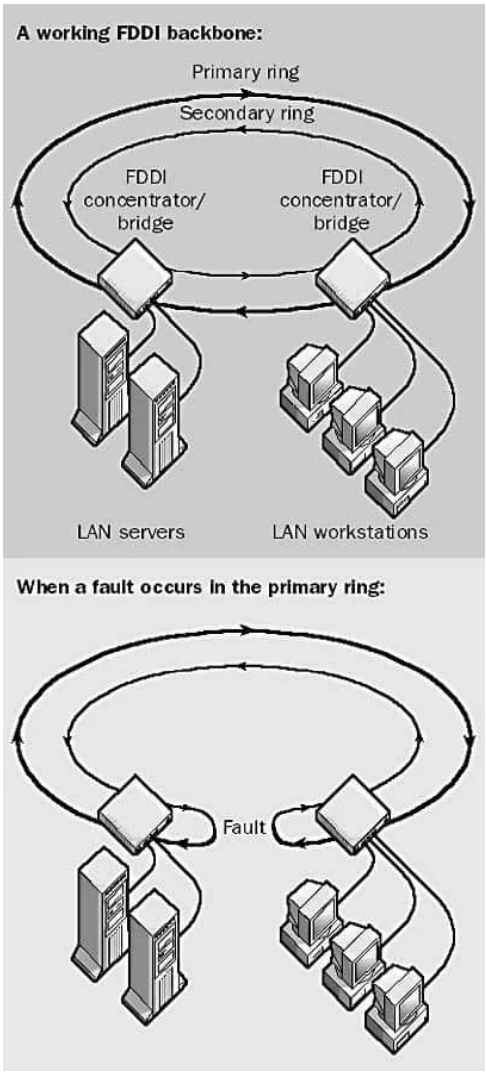
Fiber Distributed Data Interface: Topology and Design

Fiber Distributed Data Interface has two token-passing rings, each transmitting data in opposite directions. One FDDI ring is primary, and the other is secondary, usually reserved in case the primary ring fails. That means FDDI networks have inherent fault tolerance. And that is why you can use them as network backbone in a MAN or CAN. When the primary ring fails, the secondary FDDI ring automatically configures itself to carry data. After that, you can locate, isolate, and repair faults using the beaconing technique.

The fiber network topology is usually a ring; however, you can also use a star topology. The FDDI network rings can have a circumference of 100 km and need a repeater every 2kms. In addition, 500 stations can connect to an FDDI network.

Stations can connect to FDDI in two ways:

1. **Singe-attached**: Stations will only connect to a primary or a secondary ring. They are not ideal for network backbones because they lack fault tolerance. But you can use them to connect servers to a network backbone.
2. **Dual-Attached**: These stations connect to both the rings of an FDDI fiber network and are excellent for network backbones because of the fault tolerance.



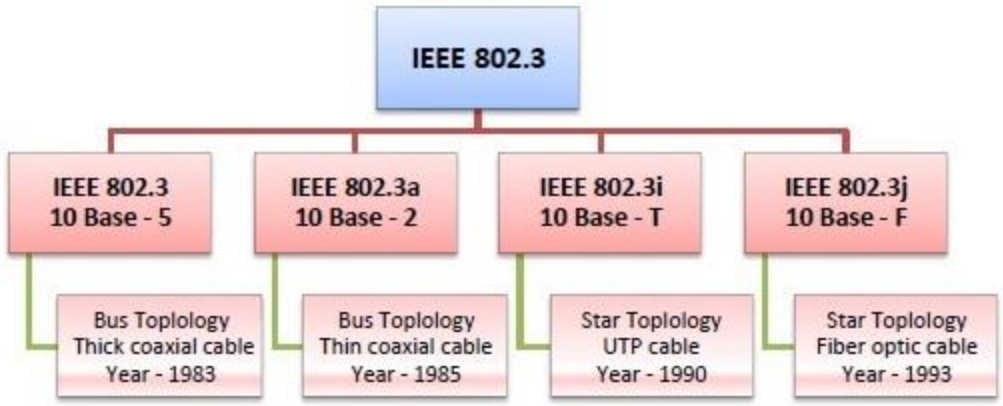
IEEE 802.3

IEEE 802.3 is a set of standards and protocols that define **Ethernet-based networks**. Ethernet technologies are primarily used in **LANs**, though they can also be used in **MANs** and even **WANs**. IEEE 802.3 defines the **physical layer** and the **medium access control (MAC) sub-layer** of the **data link layer** for wired Ethernet networks.

IEEE 802.3 Popular Versions

There are a number of versions of IEEE 802.3 protocol. The most popular ones are.

- **IEEE 802.3**: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.
- **IEEE 802.3a**: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- **IEEE 802.3i**: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.
- **IEEE 802.3i**: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.

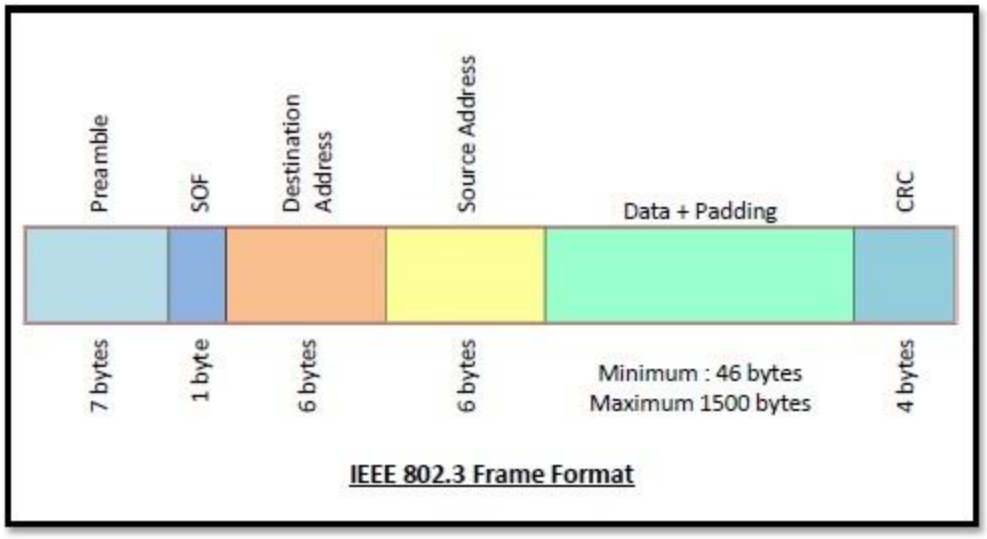


Frame Format of IEEE 802.3

The main fields of a frame of classic Ethernet are -

- **Preamble**: It is a 7 bytes starting field that provides alert and timing pulse for transmission.
- **Start of Frame Delimiter**: 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 7 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.



What are IEEE 802.11 networks?

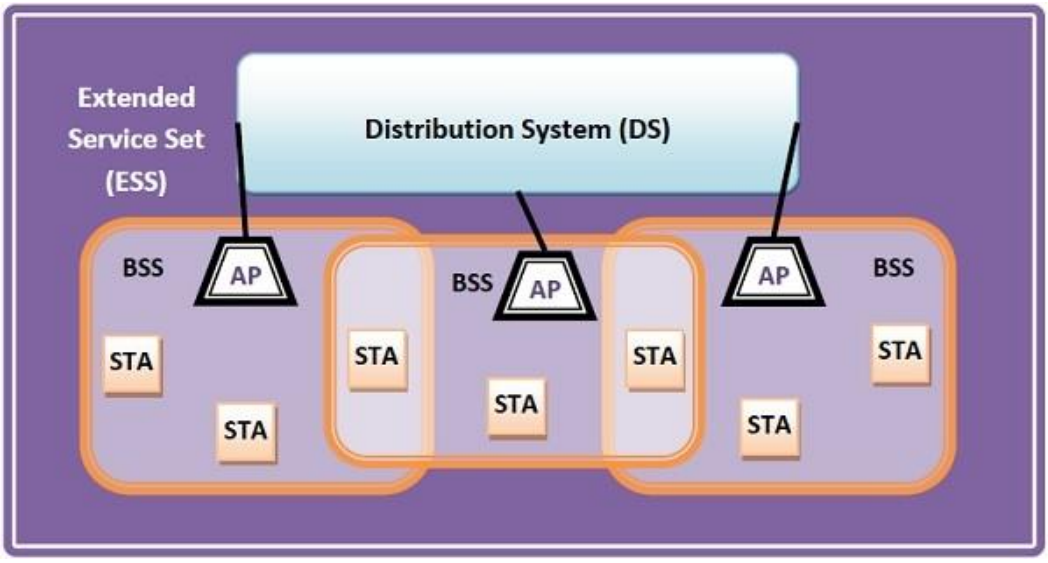
IEEE 802.11 standard, popularly known as **WiFi**, lays down the architecture and specifications of **wireless LANs (WLANs)**. WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in **LAN**. Users connected by WLANs can move around within the area of network coverage.

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows –

- **Stations (STA)** – Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types–
  - Wireless Access Point (WAP) – WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
  - Client. Clients are workstations, computers, laptops, printers, smartphones, etc.
- Each station has a wireless network interface controller.

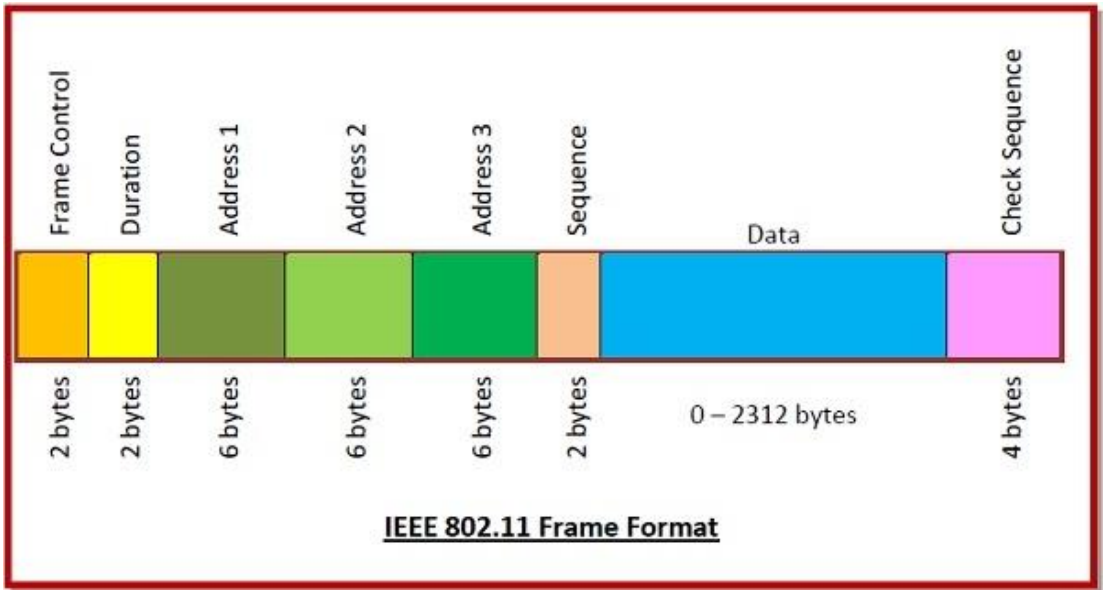
- **Basic Service Set (BSS)** – A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories depending upon the mode of operation–
    - Infrastructure BSS – Here, the devices communicate with other devices through access points.
    - Independent BSS – Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.
- **Extended Service Set (ESS)** – It is a set of all connected BSS.
- **Distribution System (DS)** – It connects access points in ESS.



Frame Format 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 acknowledgment 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 that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence** – It is a 4-byte field containing error detection information.



IEEE 802.11 Frame Format