RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL New Scheme Based On AICTE Flexible Curricula Computer Science & Engineering, VI-Semester CS-602 Computer Network

Topic covered:-

Unit-III

MAC Sub layer: MAC Addressing, Binary Exponential Back-off (BEB) Algorithm, Distributed Random Access Schemes/Contention Schemes: for Data Services (ALOHA and Slotted ALOHA), for Local-Area Networks (CSMA, CSMA/CD, CSMA/CA), Collision Free Protocols: Basic Bit Map, BRAP, Binary Count Down, MLMA Limited Contention Protocols: Adaptive Tree Walk, Performance Measuring Metrics. IEEE Standards 802 series & their variant.

MAC Sub layer:

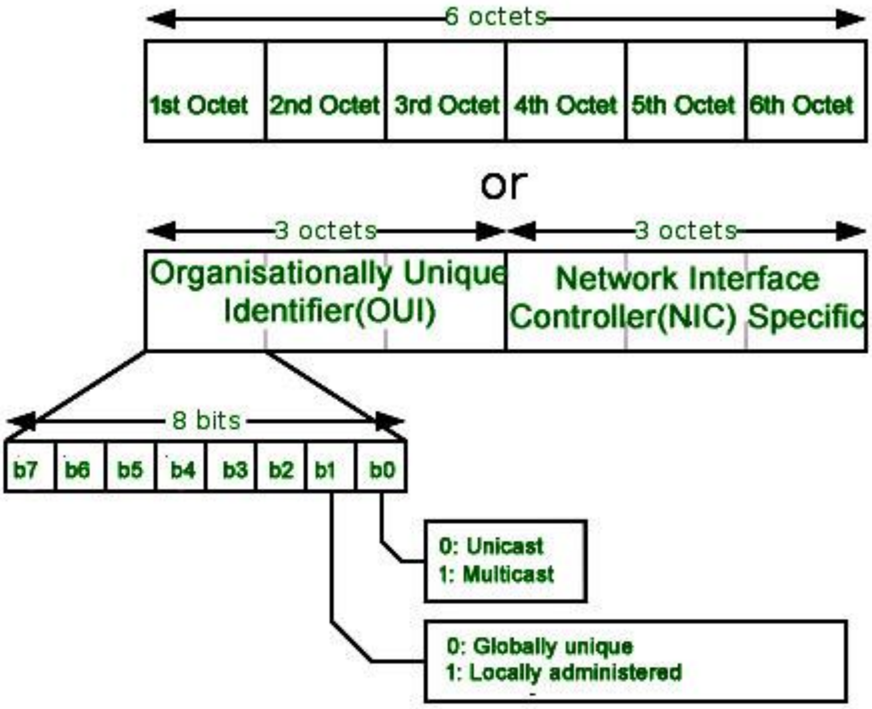
In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data Link Layer. In this article, we will discuss about addressing in DLL, which is MAC Address.

Media Access Control (MAC) Address –

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.



Format of MAC Address –

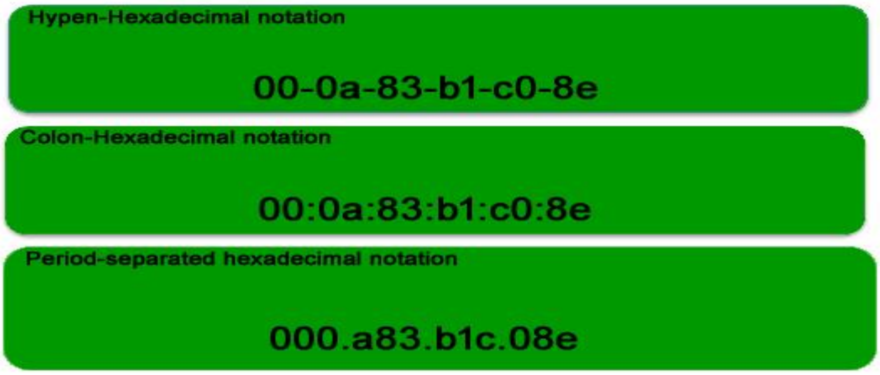
MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (**Organizational Unique**

Identifier). IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.
Here are some OUI of well known manufacturers :

```
CC:46:D6 - Cisco

3C:5A:B4 - Google, Inc.

3C:D9:2B - Hewlett Packard

00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD
```

The rightmost six digits represents **Network Interface Controller**, which is assigned by manufacturer.

As discussed above, MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats –



Hypen-Hexadecimal notation

00-0a-83-b1-c0-8e

Colon-Hexadecimal notation

00:0a:83:b1:c0:8e

Period-separated hexadecimal notation

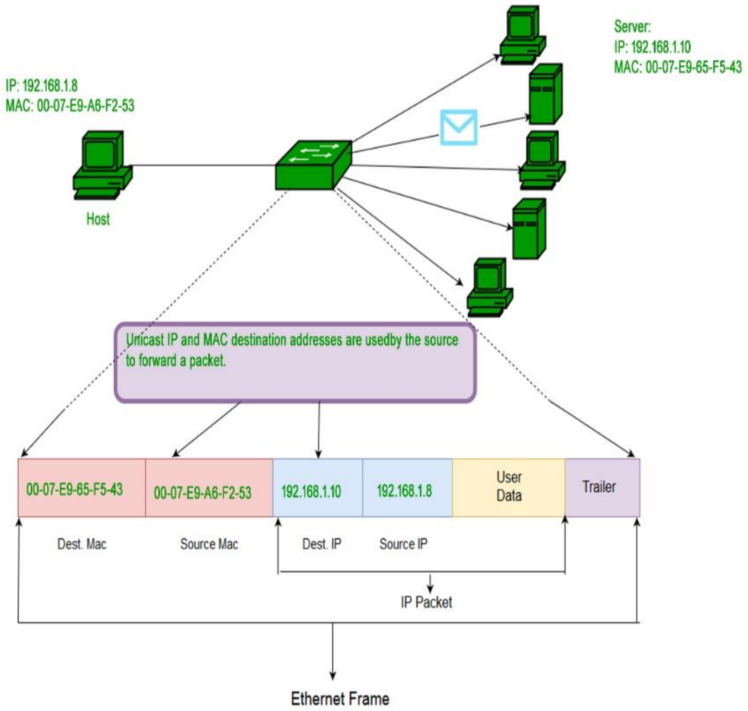
000.a83.b1c.08e

Note: Colon-Hexadecimal notation is used by *Linux OS* and Period-separated Hexadecimal notation is used by *Cisco Systems*.

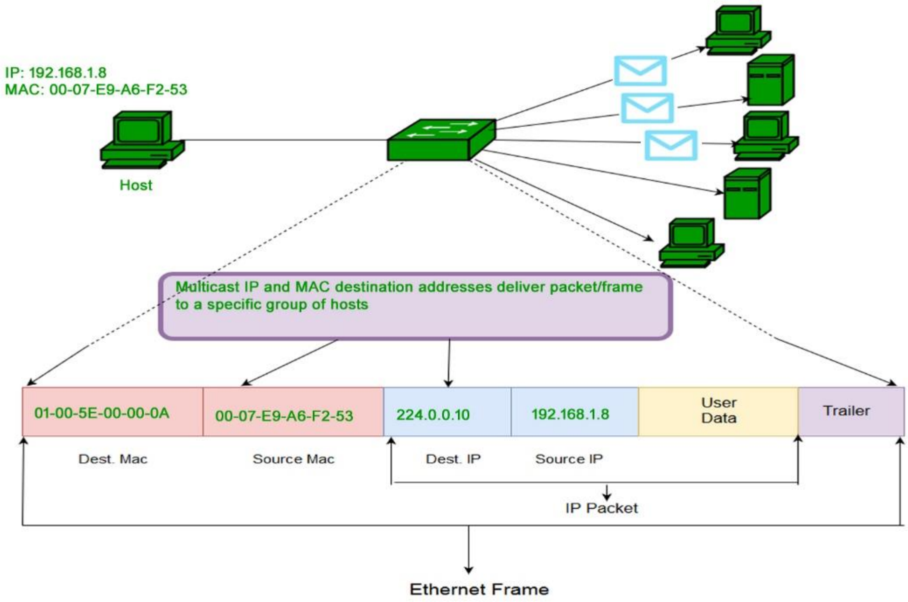
Note – LAN technologies like Token Ring, Ethernet use MAC Address as their Physical address but there are some networks (AppleTalk) which does not use MAC address.

Types of MAC Address –

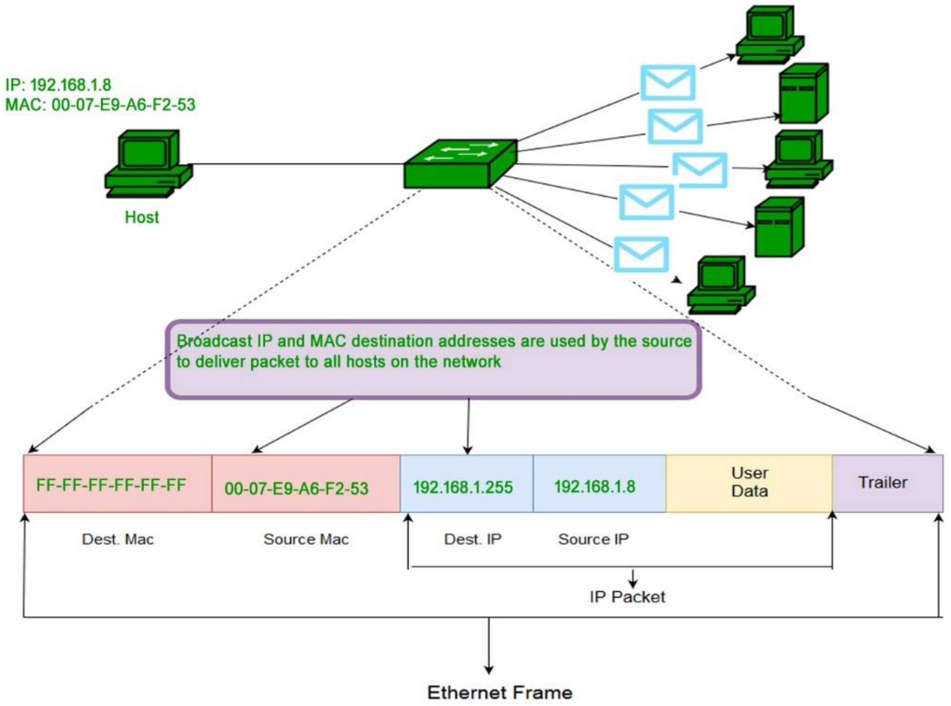
1. **Unicast –** A Unicast addressed frame is only sent out to the interface leading to specific NIC. If the LSB (least significant bit) of first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.



2. **Multicast –** Multicast address allow the source to send a frame to group of devices. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) of first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.



3. **Broadcast –** Similar to Network Layer, Broadcast is also possible on underlying layer(Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred as broadcast address. Frames which are destined with MAC address FF-FF-FF-FF-FF-FF will reach to every computer belong to that LAN segment.



What is MAC Cloning –

Some ISPs use MAC address inorder to assign IP address to gateway device. When device connects to the ISP, DHCP server records the MAC address and then assign IP address. Now the system will be identified through MAC address. When the device gets disconnected, it looses the IP address. If user wants to reconnect, DHCP server checks if the device is connected before. If so, then server tries to assign same IP address (in case lease period not expired). In case user changed the router, user has to inform the ISP about new MAC address because new MAC address is unknown to ISP, so connection cannot be established.
Or the other option is **Cloning**, user can simply clone the registered MAC address with ISP. Now router keeps reporting old MAC address to ISP and there will be no connection issue.

Binary Exponential Backoff:- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free.

When more than one stations send their frames simultaneously, collision occurs. Back-off algorithm is a collision resolution mechanism which is commonly used to schedule retransmissions after collisions in Ethernet. The waiting time that a station waits before attempting retransmission of the frame is called as back off time.

Algorithm of CSMA/CD

Step 1) When a frame is ready, the transmitting station checks whether the channel is idle or busy.

Step 2) If the channel is busy, the station waits until the channel becomes idle.

Step 3) If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.

Step 4) If a collision is detected, the station starts the binary exponential backoff algorithm.

Step 5) The station resets the retransmission counters and completes frame transmission.

Binary Exponential Back off Algorithm in case of Collision:

Step 1) The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.

Step 2) The station increments the retransmission counter, c, that denote the number of collisions.

Step 3) The station selects a random number of slot times in the range 0 and $2^c - 1$. For example, after the first collision (i.e. c = 1), the station will wait for either 0 or 1 slot times. After the second collision (i.e. c = 2), the station will wait anything between 0 to 3 slot times. After the third collision (i.e. c = 3), the station will wait anything between 0 to 7 slot times, and so forth.

Step 4) If the station selects a number k in the range 0 and 2c – 1, then

Back_off_time = k × Time slot,

where a time slot is equal to round trip time (RTT).

Step 5) And the end of the backoff time, the station attempts retransmission by continuing with the CSMA/CD algorithm.

Step 6) If the maximum number of retransmission attempts is reached, then the station aborts transmission.

Channel Allocation Problem

In broadcast networks, single channel is shared by several stations.
This channel can be allocated to only one transmitting user at a time.
There are two different methods of channel allocations:
Static Channel Allocation
Dynamic Channel Allocation

Static Channel Allocations

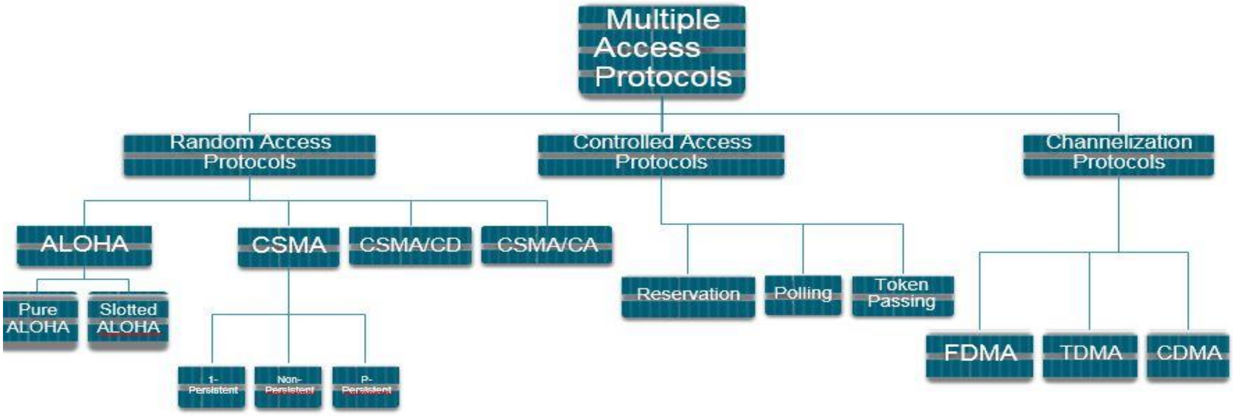
- In this method, a single channel is divided among various users either on the basis of frequency or on the basis of time.
- It either uses FDM (Frequency Division Multiplexing) or TDM (Time Division Multiplexing).
- In FDM, fixed frequency is assigned to each user, whereas, in TDM, fixed time slot is assigned to each user.

Dynamic Channel Allocation

In this method, no user is assigned fixed frequency or fixed time slot.All users are dynamically assigned frequency or time slot, depending upon the requirements of the user.

Multiple Access Protocols

Many protocols have been defined to handle the access to shared link.
These protocols are organized in three different groups.:
Random Access Protocols
Controlled Access Protocols
Channelization Protocols



1. Random Access Protocols

It is also called Contention Method. In this method, there is no control station. Any station can send the data.The station can make a decision on whether or not to send data. This decision depends on the state of the channel, i.e. channel is busy or idle. There is no scheduled time for a stations to transmit. They can transmit in random order.

Random Access Protocols

There is no rule that decides which station should send next.If two stations transmit at the same time, there is collision and the frames are lost.The various random access methods are:

ALOHA
CSMA (Carrier Sense Multiple Access)
CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

ALOHA

ALOHA was developed at University of Hawaii in early 1970s by Norman Abramson. It was used for ground based radio broadcasting. In this method, stations share a common channel. When two stations transmit simultaneously, collision occurs and frames are lost. There are two different versions of ALOHA:

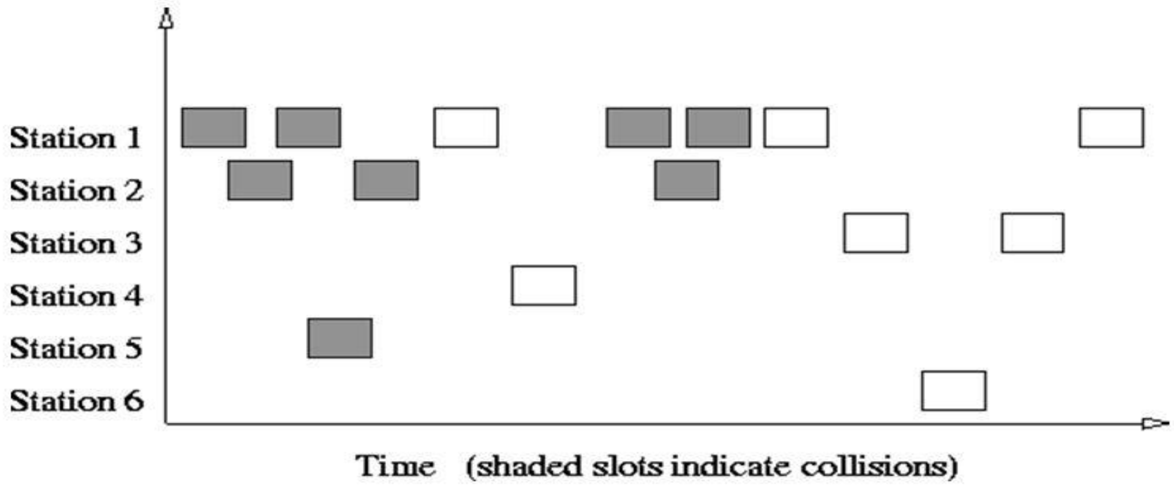
Pure ALOHA
Slotted ALOHA

Pure ALOHA

In pure ALOHA, stations transmit frames whenever they have data to send. When two stations transmit simultaneously, there is collision and frames are lost. In pure ALOHA, whenever any station transmits a frame, it expects an acknowledgement from the receiver.

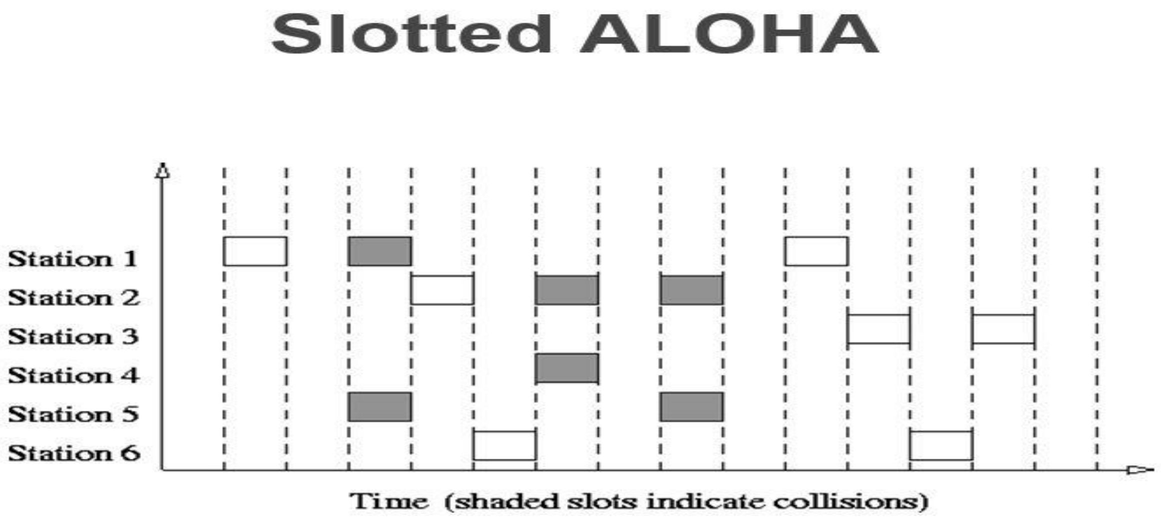
If acknowledgement is not received within specified time, the station assumes that the frame has been lost. If the frame is lost, station waits for a random amount of time and sends it again.This waiting time must be random, otherwise, same frames will collide again and again. Whenever two frames try to occupy the channel at the same time, there will be collision and both the frames will be lost.

If first bit of a new frame overlaps with the last bit of a frame almost finished, both frames will be lost and both will have to be retransmitted.



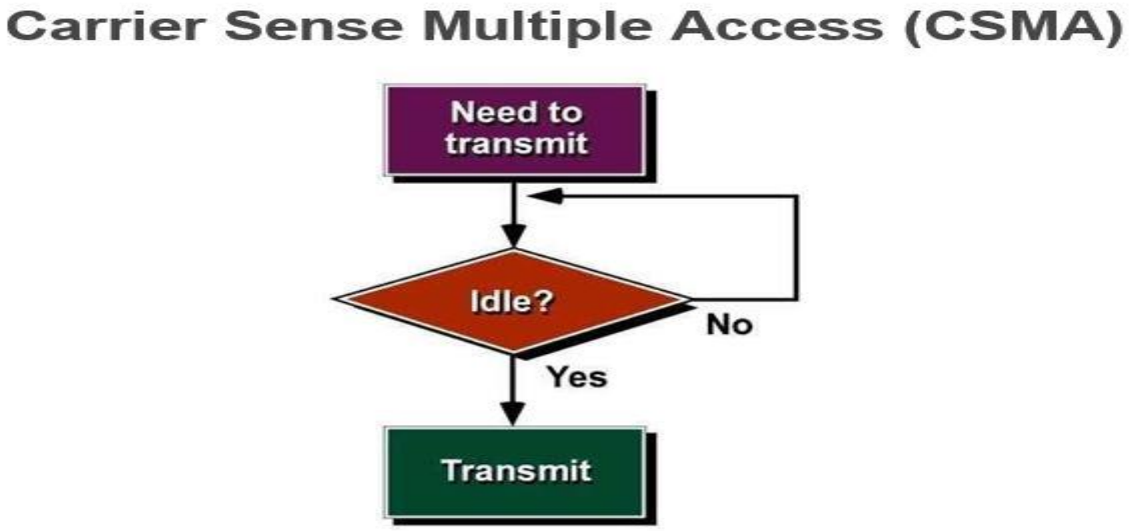
Slotted ALOHA

Slotted ALOHA was invented to improve the efficiency of pure ALOHAIn slotted ALOHA, time of the channel is divided into intervals called slots.The station can send a frame only at the beginning of the slot and only one frame is sent in each slot.If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the next time slot.There is still a possibility of collision if two stations try to send at the beginning of the same time slot.



Carrier Sense Multiple Access (CSMA)

CSMA was developed to overcome the problems of ALOHA i.e. tominimize the chances of collision.CSMA is based on the principle of “carrier sense”.The station sense the carrier or channel before transmitting a frame. It means the station checks whether the channel is idle or busy.The chances of collision reduces to a great extent if a station checks the channel before trying to use it. The chances of collision still exists because of propagation delay. The frame transmitted by one station takes some time to reach the other station. In the meantime, other station may sense the channel to be idle and transmit its frames. This results in the collision.



There are three different types of CSMA protocols:

1-Persistent CSMA
Non-Persistent CSMA
P-Persistent CSMA

1-Persistent CSMA

In this method, station that wants to transmit data, continuously senses the channel to check whether he channel is idle or busy. If the channel is busy, station waits until it becomes idle. When the station detects an idle channel, it immediately transmits the frame.

This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.

Non-Persistent CSMA

A station that has a frame to send, senses the channel.If the channel is idle, it sends immediately. If the channel is busy, it waits a random amount of time and then senses the channel again. It reduces the chance of collision because the stations wait for a random amount of time .It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.

P-Persistent CSMA

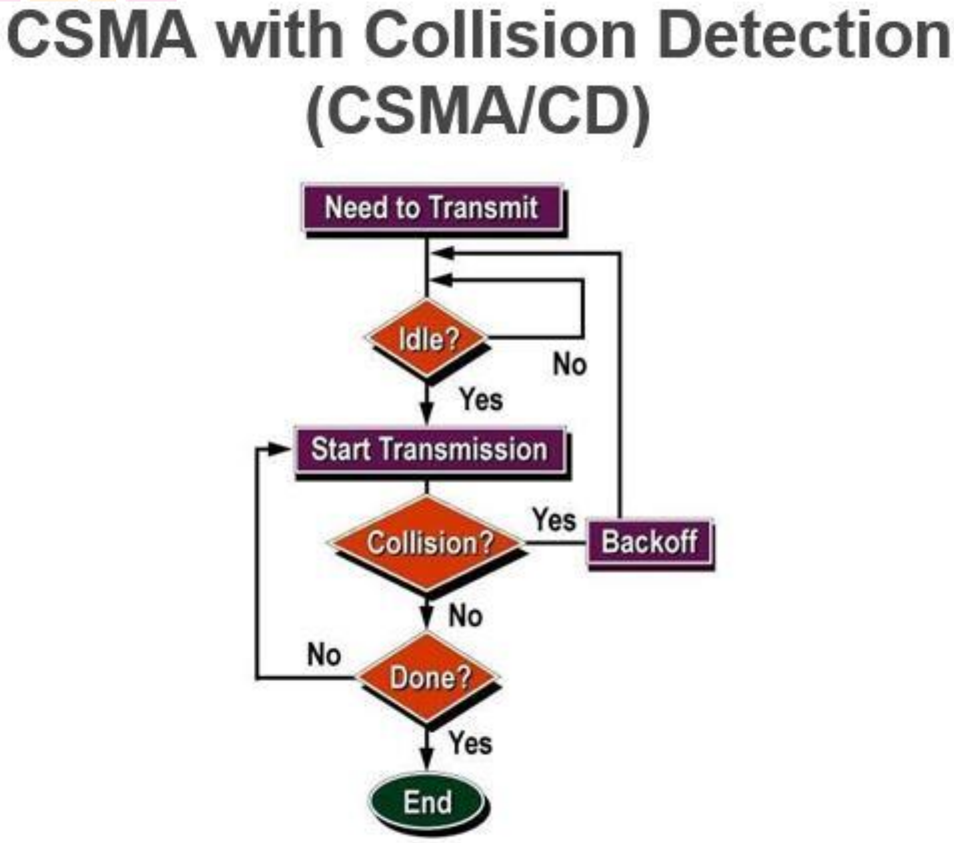
In this method, the channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time. When a station is ready to send, it senses the channel. If the channel is busy, station waits until next slot. If the channel is idle, it transmits the frame. It reduces the chance of collision and improves the efficiency of the network.

CSMA with Collision Detection (CSMA/CD)

In this protocol, the station senses the channel before transmitting the frame. If the channel is busy, the station waits. Additional feature in CSMA/CD is that the stations can detect collisions. The stations abort their transmission as soon as they detect collision. This feature is not present in CSMA. The stations continue to transmit even though they find that collision has occurred.

CSMA with Collision Detection (CSMA/CD)

In CSMA/CD, the station that sends its data on the channel, continues to sense the channel even after data transmission. If collision is detected, the station aborts its transmission and waits for a random amount of time & sends its data again.As soon as a collision is detected, the transmitting station release a jam signal. Jam signal alerts other stations. Stations are not supposed to transmit immediately after the collision has occurred.

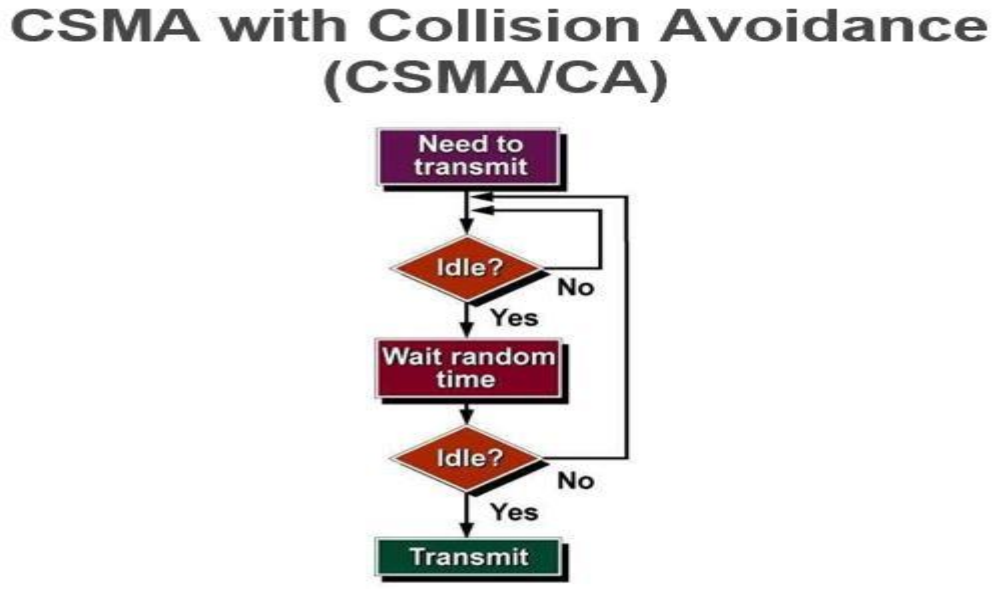


CSMA with Collision Avoidance (CSMA/CA)

This protocol is used in wireless networks because they cannot detect the collision.

So, the only solution is collision avoidance.It avoids the collision by using three basic techniques:

Interframe Space
Contention Window
Acknowledgements



Interframe Space

Whenever the channel is found idle, the station does not transmit immediately.

It waits for a period of time called Interframe Space (IFS).When channel is sensed idle, it may be possible that some distant station may have already **started transmitting.**

Therefore, the purpose of IFS time is to allow this transmitted signal to reach its destination.

If after this IFS time, channel is still idle, the station can send the frames.

Contention Window

Contention window is the amount of time divided into slots.Station that is ready to send chooses a random number of slots as its waiting time.The number of slots in the window changes with time.It means that it is set of one slot for the first time, and then doubles each time the station cannot detect an idle channel after the IFS time.In contention window, the station needs to sense the channel after each time slot.

Acknowledgment

Despite all the precautions, collisions may occur and destroy the data.Positive acknowledgement and the time-out timer helps guarantee that the receiver has received the frame.

Controlled Access Protocol

In this method, the stations consult each other to find which station has a right to send.A station cannot send unless it has been authorized by other station. The different controlled access methods are:

Reservation
Polling
Token Passing

Reservation

In this method, a station needs to make a reservation before sending data.
The time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.If there are N stations, then there are exactly N reservation slots in the reservation frame. Each slot belongs to a station.When a station needs to send a frame, it makes a reservation in its own slot.The stations that have made reservations can send their frames after the reservation frame.

Polling

Polling method works in those networks where primary and secondary stations exist.
All data exchanges are made through primary device even when the final destination is a **secondary device.**
Primary device controls the link and secondary device follow the instructions.

Token Passing

Token passing method is used in those networks where the stations are organized in a logical ring. In such networks, a special packet called token is circulated through the ring. Station that possesses the token has the right to access the channel. Whenever any station has some data to send, it waits for the token. It transmits data only after it gets the possession of token. After transmitting the data, the station releases the token and passes it to the next station in the ring. If any station that receives the token has no data to send, it simply passes the token to the next station in the ring.

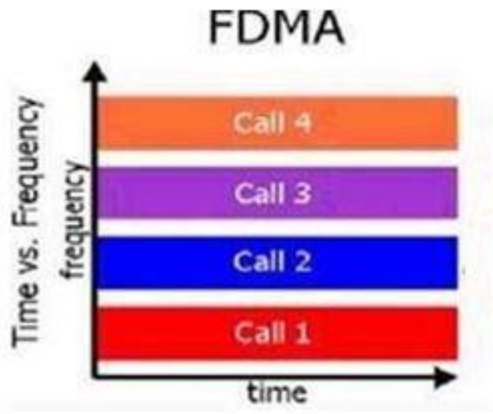
Channelization Protocol

Channelization is a multiple access method in which the available bandwidth of a link is shared in time, frequency or code between different stations.There are three basic channelization protocols:

Frequency Division Multiple Access (FDMA)
Time Division Multiple Access (TDMA)
Code Division Multiple Access (CDMA)

FDMA

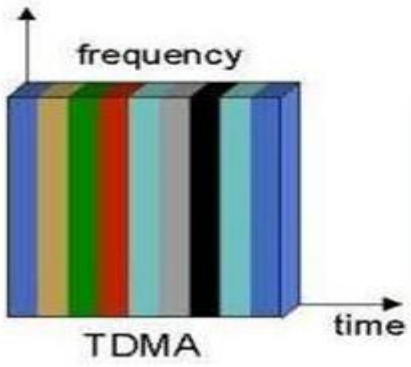
In FDMA, the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. This band is reserved for that station for all the time. The frequency bands of different stations are separated by small bands of unused frequency. These unused bands are called guard bands that prevent station interferences. FDMA is different from FDM (Frequency Division Multiplexing).FDM is a physical layer technique, whereas, FDMA is an access method in the data link layer.



c

TDMA

In TDMA, the bandwidth of channel is divided among various stations on the basis of time. Each station is allocated a time slot during which it can send its data. Each station must know the beginning of its time slot. TDMA requires synchronization between different stations. Synchronization is achieved by using some synchronization bits at the beginning of each slot. TDMA is also different from TDM. TDM is a physical layer technique, whereas, TDMA is an access method in data link layer.



CDMA

Unlike TDMA, in CDMA all stations can transmit data simultaneously. Multiple simultaneous transmissions are separated using coding theory. In CDMA, each user is given a unique code sequence.

Collision-Free Protocols in Computer Network:

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. Popular Collision Free Protocols are as follows:-

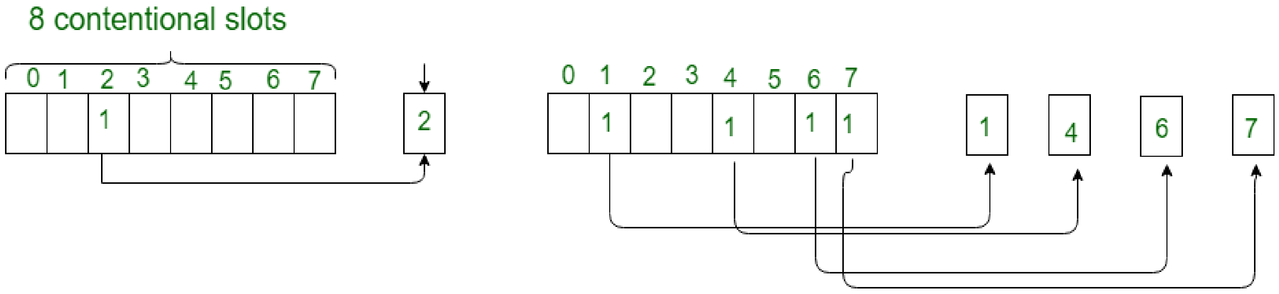
Bit-map Protocol
Binary Countdown
Limited Contention Protocols
The Adaptive Tree Walk Protocol

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.

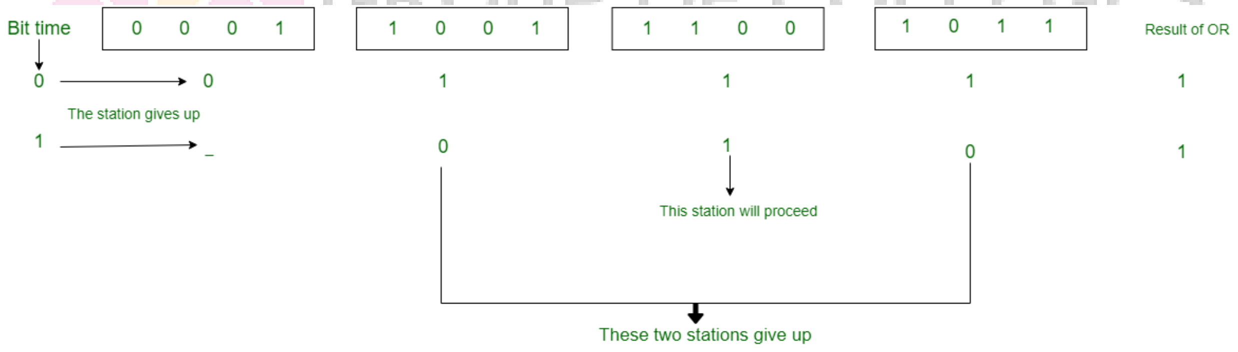
Generally, high numbered stations have to wait for half a scan before starting to transmit low numbered stations have to wait for half a scan(N/2 bit slots) before starting to transmit, low numbered stations have to wait on an average 1.5 N slots.

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.



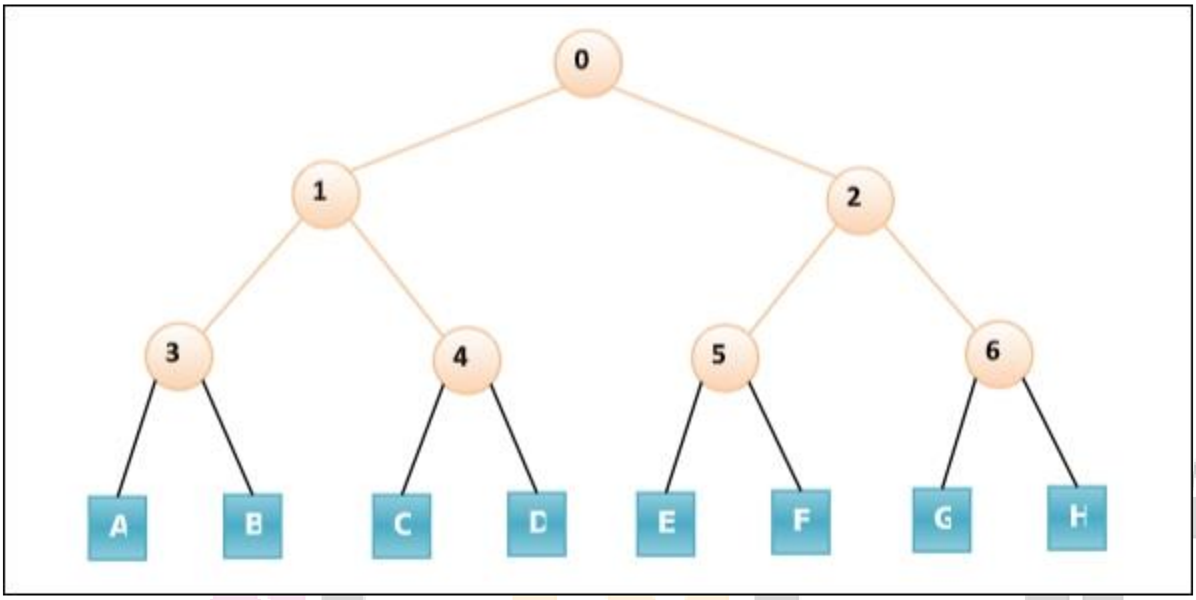
Binary countdown

Limited Contention Protocols:

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

Adaptive Tree Walk Protocol

In adaptive tree walk protocol, the stations or nodes are arranged in the form of a binary tree as follows -



Initially all nodes (A, B ……. G, H) are permitted to compete for the channel. If a node is successful in acquiring the channel, it transmits its frame. In case of collision, the nodes are divided into two groups (A, B, C, D in one group and E, F, G, H in another group). Nodes belonging to only one of them is permitted for competing. This process continues until successful transmission occurs.

MLMA Limited Contention Protocols: Adaptive Tree Walk Under conditions of light load, contention is preferable due to its low delay. As the load increases, contention becomes increasingly less attractive, because the overload associated with channel arbitration becomes greater. Just the reverse is true for contention - free protocols. At low load, they have high delay, but as the load increases , the channel efficiency improves rather than getting worse as it does for contention protocols.

It is obvious that the probablity of some station aquiring the channel could only be increased by decreasing the amount of competition. The limited contention protocols do exactly that. They first divide the stations up into (not necessarily disjoint) groups. Only the members of group 0 are permitted to compete for slot 0. The competition for aquiring the slot within a group is contention based. If one of the members of that group succeeds, it aquires the channel and transmits a frame. If there is collision or no node of a particular group wants to send then the members of the next group compete for the next slot. The probablity of a particular node is set to a particular value (optimum).

IEEE Standards 802 series & their variant

Various IEEE 802 standards are as

IEEE 802.1 High Level Interface
IEEE 802.2 Logical Link Control(LLC)
IEEE 802.3 Ethernet
IEEE 802.4 Token Bus
IEEE 802.5 Token Ring
IEEE 802.6 Metropolitan Area Networks
IEEE 802.7 Broadband LANs
IEEE 802.8 Fiber Optic LANS
IEEE 802.9 Integrated Data and Voice Network
IEEE 802.10 Security
IEEE 802.11 Wireless Network

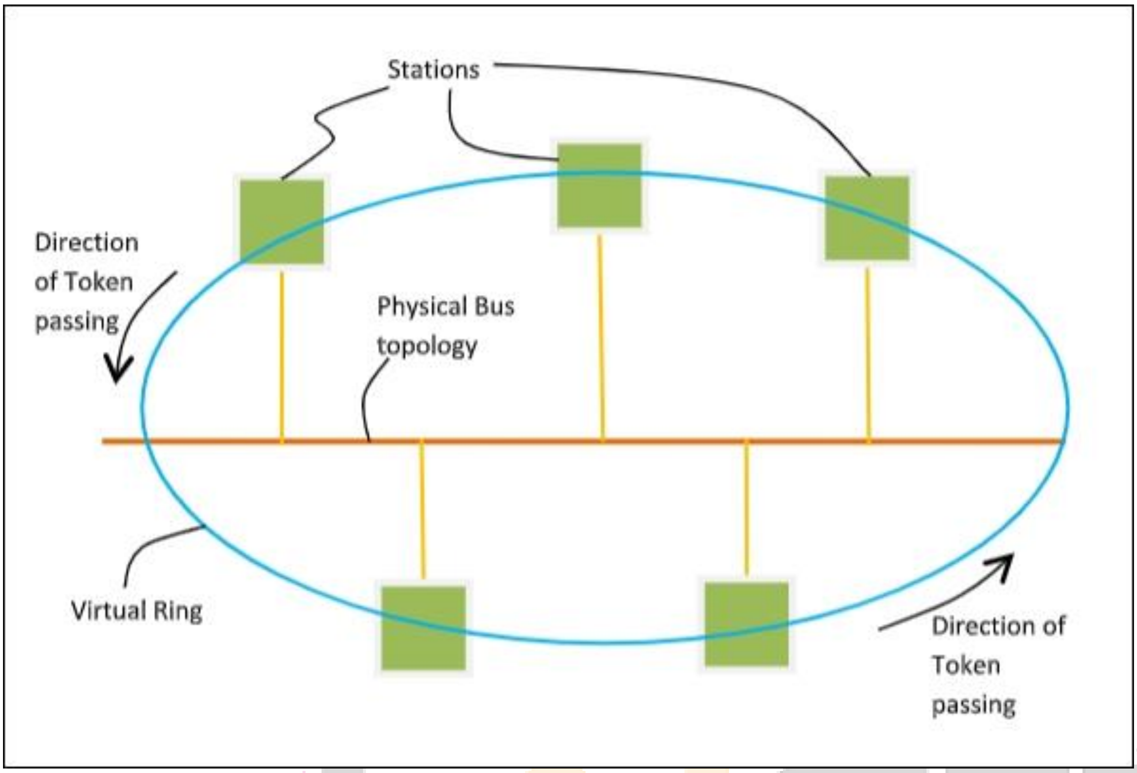
Ethernet – Ethernet is a 10Mbps LAN that uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol to control access network. When an endstation (network device) transmits data, every endstation on the LAN receives it. Each endstation checks the data packet to see whether the destination address matches its own address. If the addresses match, the endstation accepts and processes the packet. If they do not match, it disregards the packet. If two endstations transmit data simultaneously, a collision occurs and the result is a composite, garbled message. All endstations on the network, including the transmitting endstations, detect the collision and ignore the message. Each endstation that wants to transmit waits a random amount of time and then attempts to transmit again. This method is usually used for traditional Ethernet LAN.
Fast Ethernet – This is an extension of 10Mbps Ethernet standard and supports speed upto 100Mbps. The access method used is CSMA/CD .For physical connections Star wiring topology is used. Fast Ethernet is becoming very popular as an upgradation from 10Mbps Ethernet LAN to Fast Ethernet LAN is quite easy.

Token Bus

Token Bus (IEEE 802.4) is a standard for implementing token ring over virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of token bus is similar to Token Ring.

Token Passing Mechanism in Token Bus

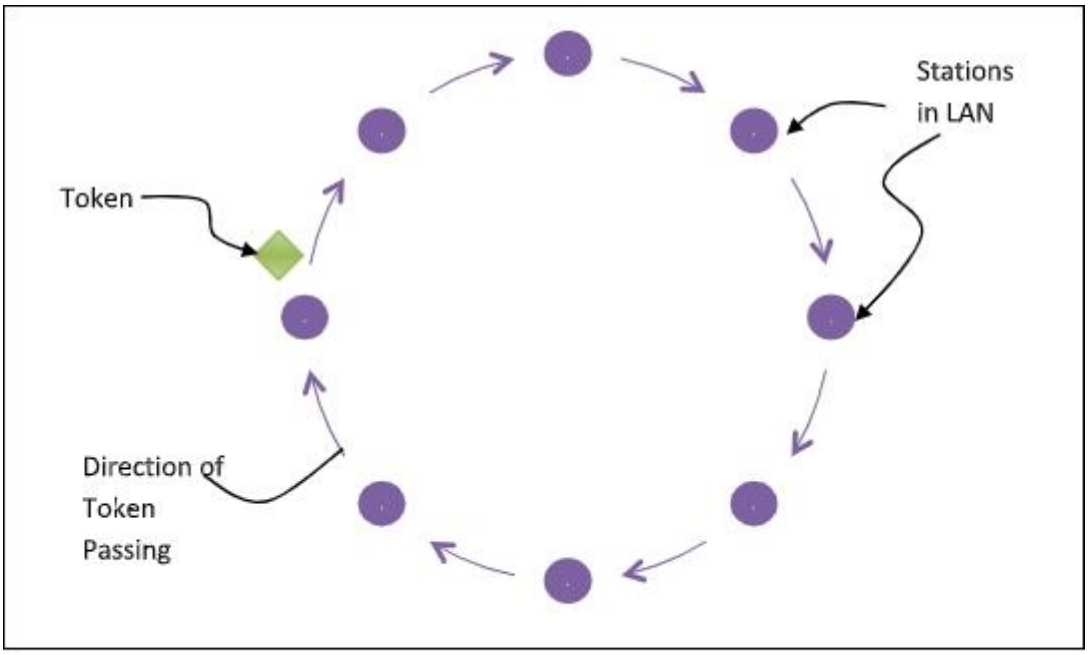
A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station. This is depicted in the following diagram −



Token Ring – Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition. This is a 4-Mbps or 16-Mbps token-passing method, operating in a ring topology. Devices on a Token Ring network get access to the media through token passing. Token and data pass to each station on the ring. The devices pass the token around the ring until one of the computer who wants to transmit data , takes the token and replaces it with a frame. Each device passes the frame to the next device, until the frame reaches its destination. As the frame passes to the intended recipient, the recipient sets certain bits in the frame to indicate that it received the frame. The original sender of the frame strips the frame data off the ring and issues a new token.

Token Passing Mechanism in Token Ring

If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing. In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed. This is shown in the following diagram −



Differences between Token Ring and Token Bus

Token Ring	Token Bus
The token is passed over the physical ring formed by the stations and the coaxial cable network.	The token is passed along the virtual ring of stations connected to a LAN.
The stations are connected by ring topology, or sometimes star topology.	The underlying topology that connects the stations is either bus or tree topology.
It is defined by IEEE 802.5 standard.	It is defined by IEEE 802.4 standard.
The maximum time for a token to reach a station can be calculated here.	It is not feasible to calculate the time for token transfer.

The 802.11 standard is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family −

- **802.11** − This pertains to wireless LANs and provides 1 - or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- **802.11a** − This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency

division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.

- **802.11b** – The 802.11 high rate WiFi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- **802.11g** – This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

Here is the technical comparison between the three major WiFi standards.

Feature	**WiFi (802.11b)**	**WiFi (802.11a/g)**
PrimaryApplication	Wireless LAN	Wireless LAN
Frequency Band	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	25 MHz	20 MHz
Half/Full Duplex	Half	Half
Radio Technology	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth	<=0.44 bps/Hz	≤=2.7 bps/Hz
Efficiency		
Modulation	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	None	Convolutional Code
Encryption	Optional- RC4m (AES in 802.11i)	Optional- RC4(AES in 802.11i)
Mobility	In development	In development
Mesh	Vendor Proprietary	Vendor Proprietary
Access Protocol	CSMA/CA	CSMA/CA

References –

1. https://www.tutorialspoint.com/csma-cd-with-the-binary-exponential-backoff
2. https://www.tutorialspoint.com/token-bus-and-token-ring
3. http://www.cruiserselite.co.in/downloads/btech/materials/second%20sem/3/CN/UNIT-5.pdf
4. https://www.vskills.in/certification/tutorial/basic-network-support/lan-types-ethernet-token-ring-fddi/