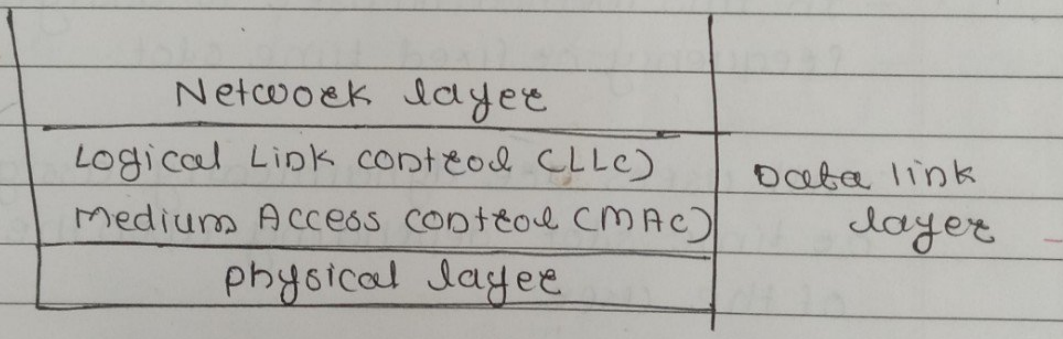
(3) Medium Access Control Sublayer

Introduction

* In broadcast n/w, several stations share a single comm.^{n} channel.
* The major issue in these n/w is which station should transmit data at a given time.
- This process of deciding the turn of different stations is known as channel allocation.
- To co-ordinate the access to the channel, multiple access protocols are required
- All these protocols being to the MAC sublayer
- Data link layer is divided into two sublayers
  i) Logical Link control (LLC)
  ii) Medium Access control (MAC)



- LLC is responsible for error control & flow control
- MAC is responsible for multiple access resolutions.

Channel Allocation Problem

* In broadcast n/w, single channel is shared by several stations.
- This channel can be allocated to only one transmitting user at a time.

i) Static channel allocation
ii) Dynamic channel allocation

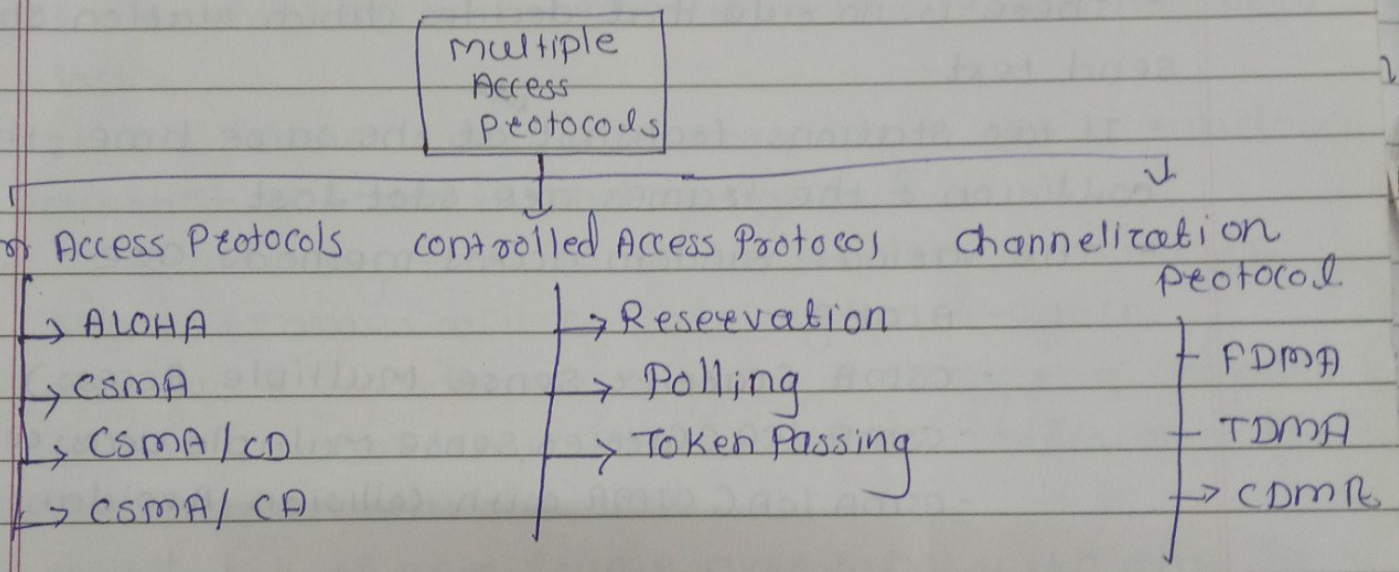
i) Static channel allocations
- In this method, single channel is divided among various users either on the basis of frequency or on the basis of time.
- It either uses FDM (Frequency Division Multiplexing) or TDM (Time Division Multiplexing).
- In FDM, fixed frequency is assigned to each user whereas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

ii) 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.

Date : / /

Multiple Access Protocols

- Many protocols have been defined to handle the access to shared link.
- These protocols are organized in 3 different groups.
  i) Random Access Protocols
  ii) Controlled Access Protocols
  iii) Channelization Protocols.



Lucky | Page No.:
Date : 4 / /

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 stations to transmit data. They can transmit in random order.
- There is no rule that decides which station should send text.
- If two stations transmit data at the same time, there is collision & 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 (CSMA with collision Avoidance)

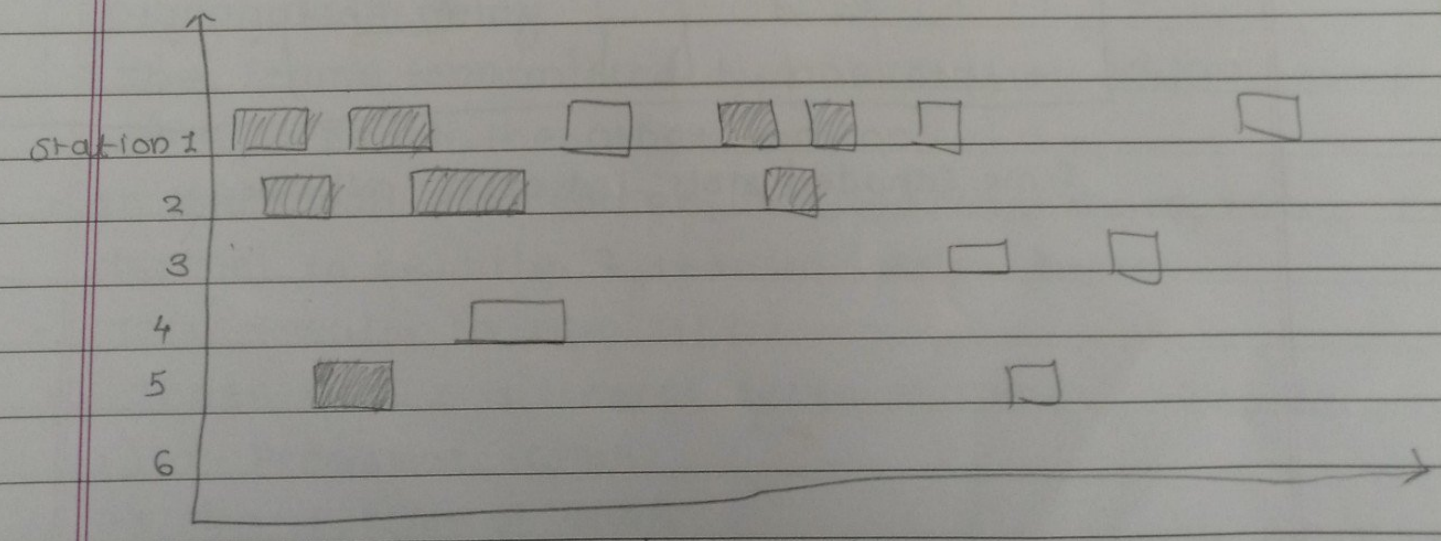
ALOHA (Additive Links On-Live Hawaii Area)

i) ALOHA was developed at University of Hawaii in early 1970s by Norman Abramson
ii) It was used for ground based radio broadcasting
iii) In this method, stations share a common channel
iv) when two stations transmit simultaneously, collision occurs & frames are lost

v) There are two different versions of ALOHA
   a) Pure ALOHA
   b) Slotted ALOHA

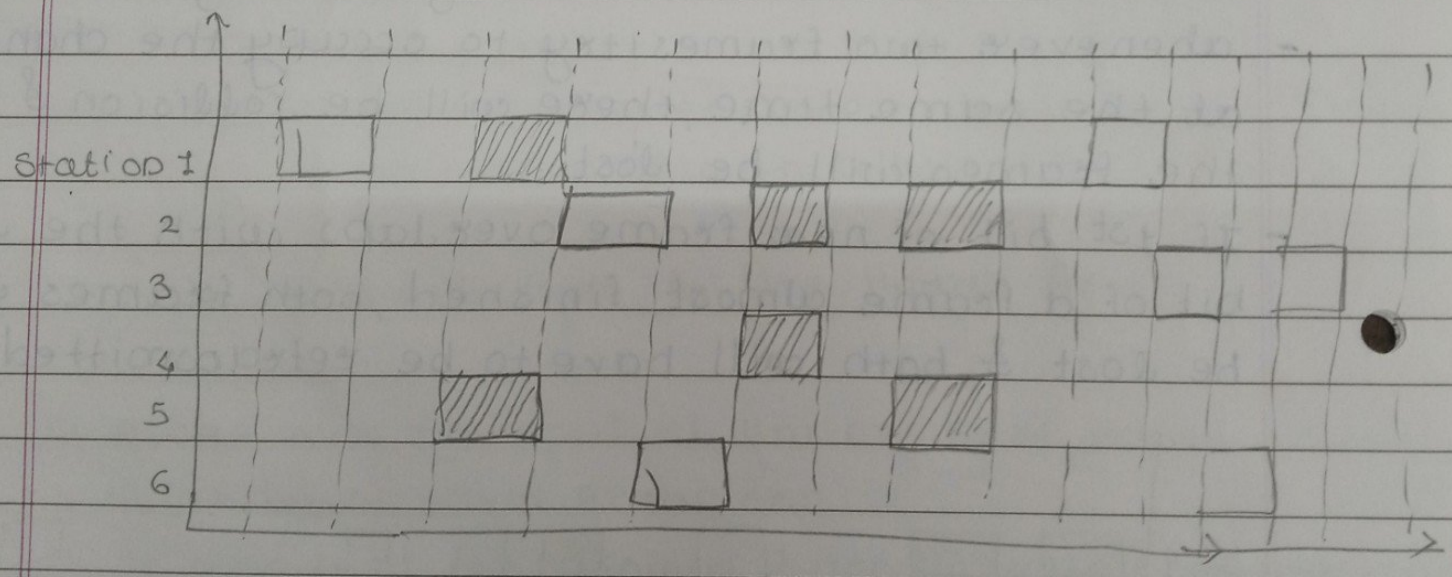
a) Pure ALOHA

- In pure ALOHA, stations transmit frames whenever they have data to send.
- When two stations transmit simultaneously, there is collision & 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, stations waits for a random amount of time & send it again.
- This waiting time must be random, otherwise same frames will collide again & again.
- Whenever two frames try to occupy the channel at the same time, there will be collision & both the frames will be lost.
- If 1st bit of new frame overlaps with the last bit of a frame almost finished, both frames will be lost & both will have to be retransmitted.



b) slotted ALOHA

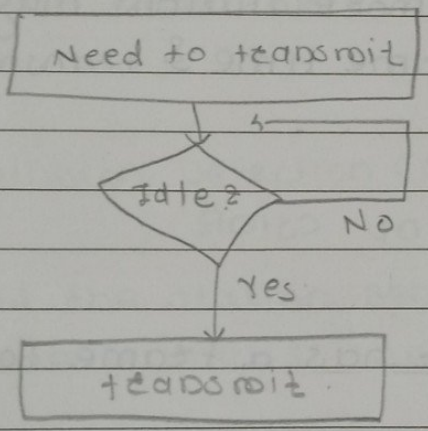
- slotted ALOHA was invented to improve the efficiency of pure ALOHA
- In slotted ALOHA time of the channel is divided into intervals called slots.
- The station can send a frame only at the beginning of the slot & only one frame is sent in each
- If any station is not able to place the frame onto the channel at the begining 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



Time (shaded slots indicates collisions)

Carrier Sense Multiple Access (CSMA)

- CSMA was developed to overcome the problems of ALOHA i.e. to minimize the chances of collision.
- It 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 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 mean time, other station may sense the channel to be idle & transmit it's frames.
- This results in the collission.
- There are 3 different types of CSMA protocols.
  i) 1-persistent CSMA
  ii) Non-persistent CSMA
  iii) P-persistent CSMA

i) 1 Persistent CSMA

- In this method, station that wants to transmit data continuously senses the channel to checks whether the channel is idle or busy.
- If the channel is busy, station sense channel 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 & transmit their frames.

ii)

ii) 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 & 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 & will retransmit at the same time.

iii) P - Persistent CSMA

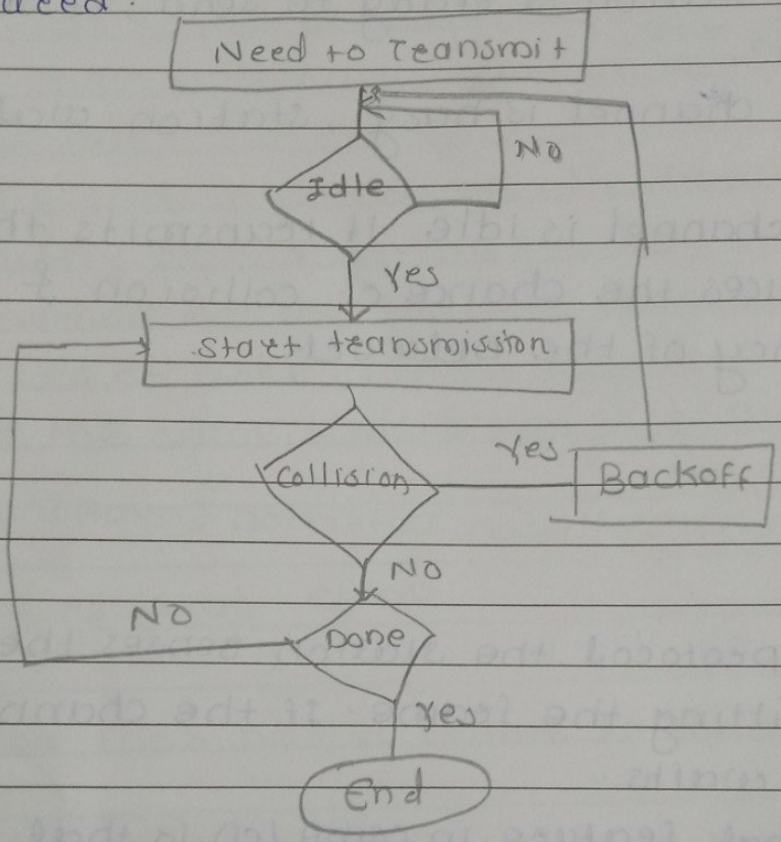
- In this method, the channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- When a station is ready to send, it senses the channel.
- If the channel is busy, station waits until next slot.
- If the channel is idle, it transmits the frame.
- It reduces the chance of collision & 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 is CSMA
- The stations continue to transmit even though they find that collision has occured.
- In CSMA/CD the station that sends the data on the channel, continues to sense the channel even after data transmission.
- If collision is detected, the station aborts its transmission & waits for a random amount of time & sends it's data again.

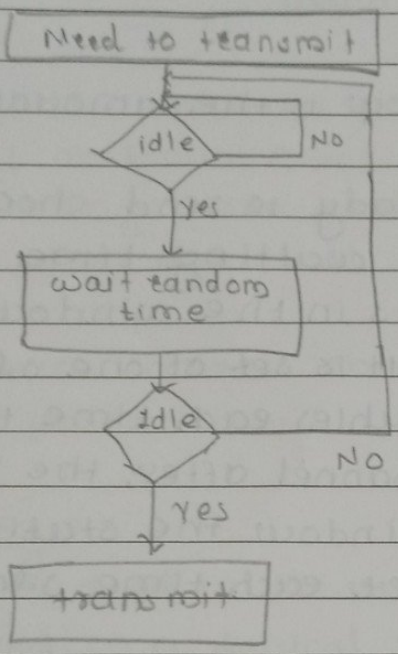
As soon as a collision is detected, the transmitting station release a jam signal.

- Jam signal alerts other stations, stations are not supposed to transmit immediately after the collision has occured.



CSMA with collision Avoidance (CSMA/CA)

- This protocol is used in wireless network because they cannot detect the collision.
- So, the only solution is collision avoidance
- It avoids the collision by using 3 basic tech.
  a) Interframe space
  b) contention window
  c) Acknowledgement



d) 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 it's destination.
- If after this IFS time channel is still idle, the station can send the frame

b) contention window

- contention window is the amount of time divided into two slots.
- station i.e ready to send chooses random no. of slots as it's waiting time.
- The no. of slots in the window changes with time
- It means that it is set of one slot for the 1st time & then doubles each time the station can't detect an idle channel after the IFS time
- In contention window the station needs to sense the channel after each time slot.

c) Acknowledgment

- Despite all the precautions, collisions may occure & destroy the data.
- Positive acknowledgment & the time-out times helps guarantee that the receiver has received the frame.

(2) Controlled Access Protocol

- In this method, the stations consults each other to find which station has a right to send.
- A station can't send unless it has been authorized by other station
- The different controlled access methods are.
  i) Reservation
  ii) Polling
  iii) Token passing

Date : / /

i) Polling

- Polling methods work in those nlw where primary & 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 & secondary device follows the instructions.

ii) Token passing

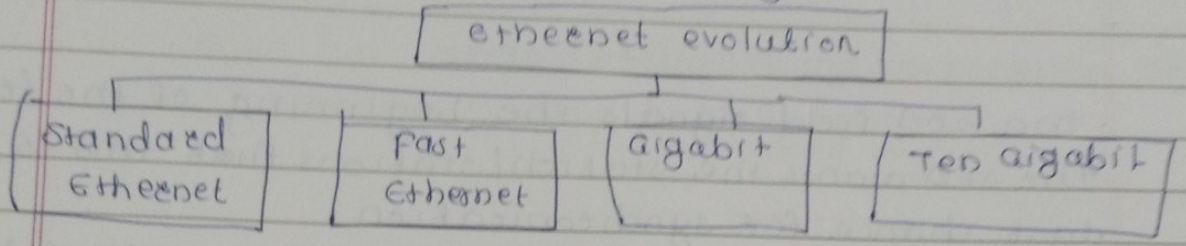
- This method is used in those nlw where the stations are organized in a logical ring.
- In such nlw, a special packet called token is circulated through ring
- stations that processes the token has the right to access the channel.
- whenever any station has some data to send, it waits for the token. It transmits data only after it gets the possession of token.
- After transmitting the data, the station releases the token & 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.

iii) channelization protocol

- channelization is multiple access method in which the available bandwidth of a link is shared in time, frequency or code between different stations.
- There are 3 basic channelization protocols.
  a) Frequency Division Multiple Access (FDMA)
  b) Time ——— " ——— (TDMA)
  c) code ——— " ——— (CDMA)

Ethernet

- The original Ethernet was created in 1976 at Xerox's Palo Alto Research center (PARC)
- Since, then it has gone through 4 generation



* 802.3 MAC frame

MAC sublayer

MAC sublayer frames data received from the upper layer & passes them to the physical layer.

Frame format

- The ethernet contains 7 fields.
- Ethernet does not provide any mechanism for acknowledging received frames, making is what is known as an unreliable medium. Acknowledgment must be implemented at the higher layers.

Preamble - 56 bits of alternating 1s & 0s

SFD - start frame delimiter flag (10101011)

Preamble	SFD	Destination Address	Source Address	Length/ type	Data & Padding	CRC
7 byte	1byte	6bytes	6byte	2byte		4byte

Fig → 802.3 MAC frame

Preamble

The 1st field of the 802.3 frame contains 7 bytes of alternating 0s & 1s that alerts the receiving system to the coming frame & enables it to synchronize its input timing

- The pattern provides only as alerts the receiver tha the next 8 timing pulse.
- The preamble is actually added at the physical layer & is not part of the frame.

Start frame delimiter (SFD)
- The 2nd field signals the beginning of the frame
- The SFD warns the station/stations that this is the last chance for synchronization.
- The last 2 bit is 11 & alerts the receiver that the next field is the destination address.

Destination Address
The DA field is 6 bytes & contains the physical address of the destination station or stations to receive the packet.

Source Address (SA)
- The SA field is also 6 bytes & contains the physical address of the sender of the packet.

Length / type
- This field is defined as a type field or length field.
- The original Ethernet used this field as the type field to define the upper layer protocol using the MAC frame.
- The IEEE standard used it as the length field to define the no. of bytes in the data field.

Data
This field carries data encapsulated from the upper layer protocol. It is minimum of 46 & maximum of 1500 bytes

Lucky | Page No.: | Date: / /

CRC

- The last field contains error detection info.
- 32 bits.

Frame length

- Ethernet has imposed restrictions on both the minimum & maximum length of a frame

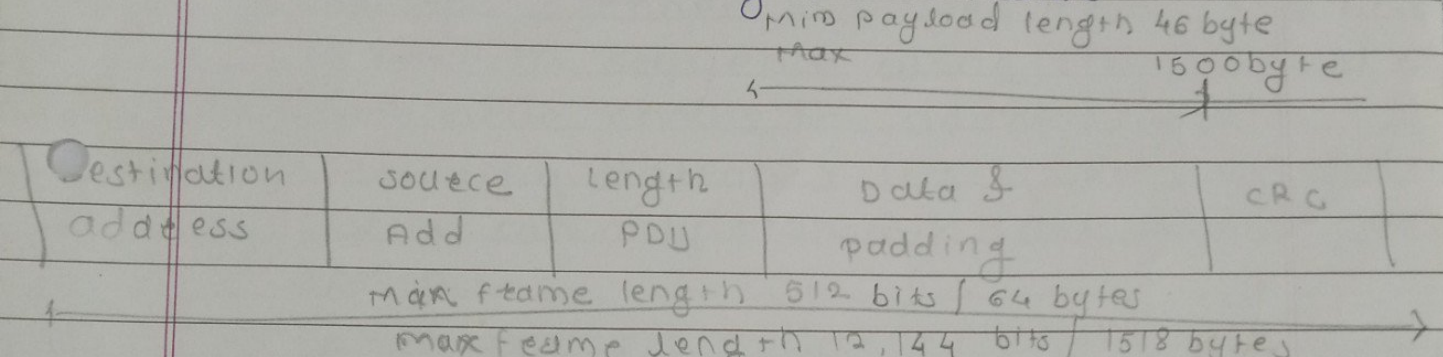
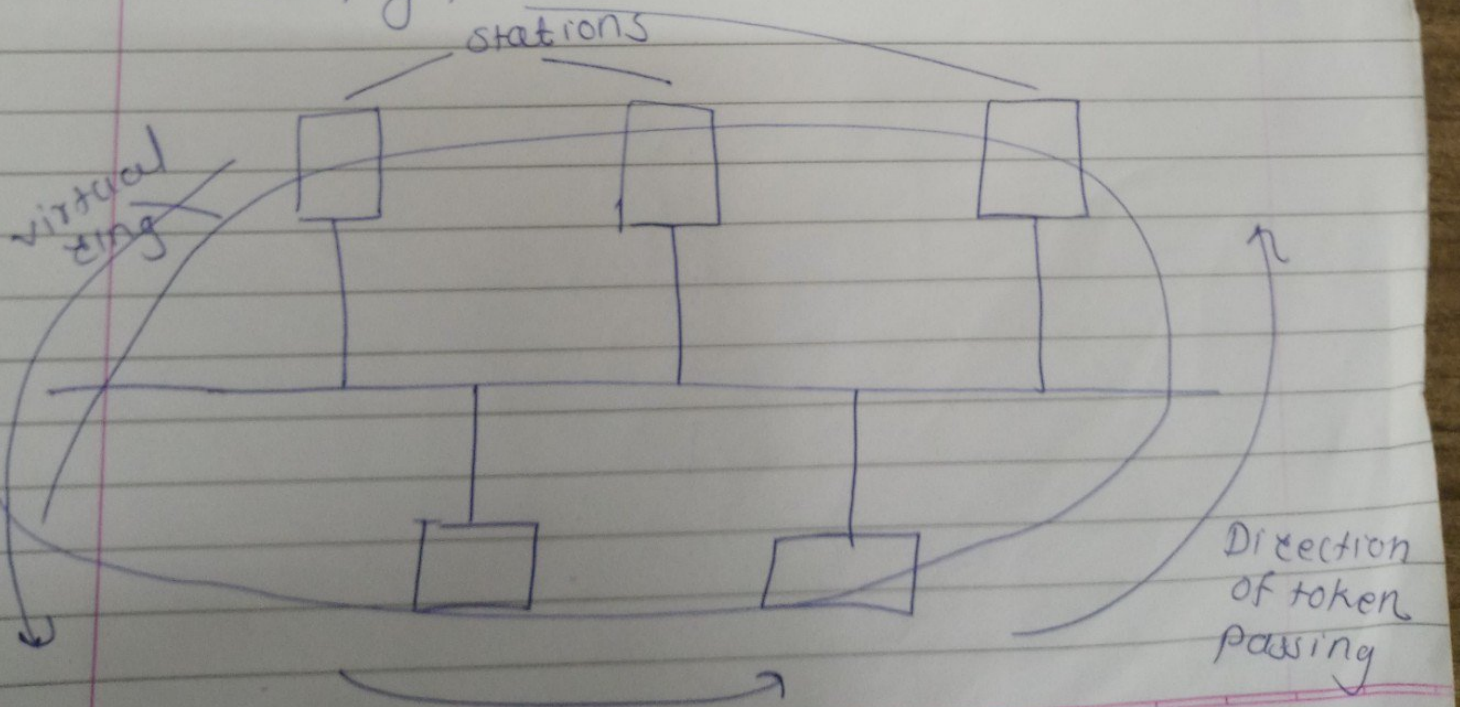


Fig - Min & max length

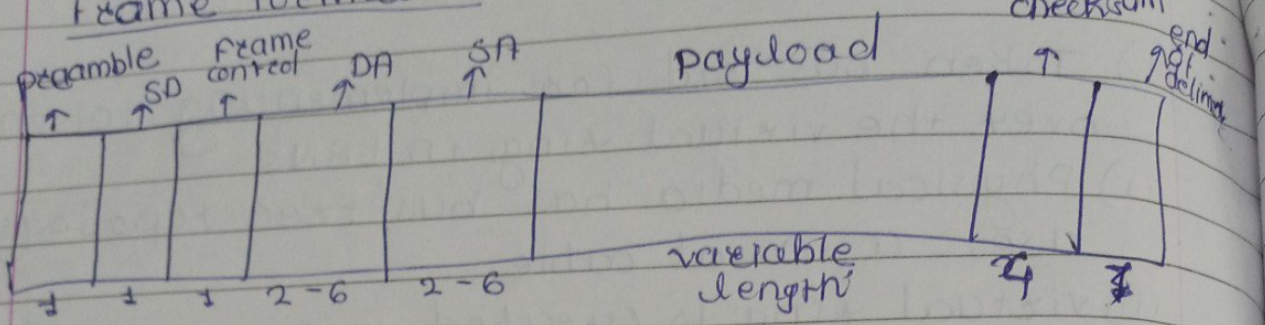
- The minimum length restriction is required for the correct operation of CSMA/CD
- An Ethernet frame needs to have minimum length of 512 bits or 64 bytes.
- Part of this length is the header & trailer.
- If we count 18 bytes of header & trailer address & bytes of length or type & 4 bytes of CRC then the minimum length of data from the upper layer is 64 - 18 = 46 bytes.
- If the upper layer packet is less than 46 bytes, padding is added to make up the difference
- The standard defines the max. length of frame 1518 bytes
- If we subtract the 18 bytes of header & trailer the max length of payload is 1500 bytes.

IEEE 802.4 Standards

i) Token bus is std for implementing token ring over the virtual ring in LANs
ii) Physical media has bus/tree topology & uses co-axial cable
iii) virtual ring is created with the nodes/stations & token is passed from one node to next in sequence along this virtual ring
iv) each node knows the address of it's preceding station & it's succeeding station
v) station can only transmit data when it has token
vi) token bus is similar to token ring
vii) Token is small message that circulates among stations of computer network providing permission to the stations for transmission if station has data to transmit when it receives a token it sends data & then passes token to the next station; otherwise it simply passes the token to next station



Frame format of Token Bus



i) Preamble → 1 byte for synchronization

ii) start delimeter → 1 byte that marks beginning of the frame

iii) Frame control → 1 byte that specifies whether this is data frame / control frame

iv) DA → 2-6 byte that specifies address of destn.

v) SA → 2-6 byte — " — " — source

vi) Payload → variable length field that carries data from nlw layer

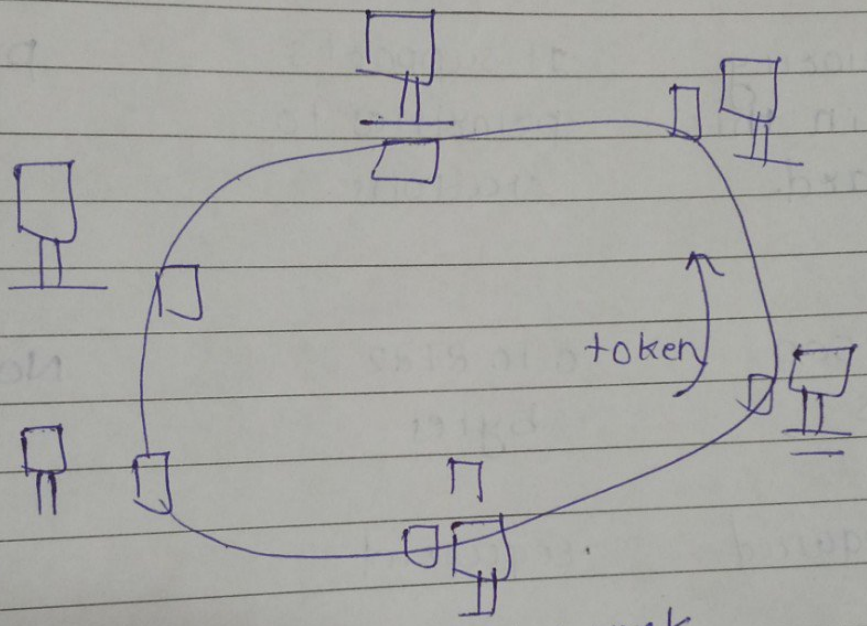
vii) checksum - 4 bytes frame check sequence for error detection

viii) End delimeter → 1 byte that marks end of frame.

i) In token ring, special bit pattern knowns as token, circulates around the ring when all the stations are idle.

ii) whenever station wants to transmit frame, it inverts single bit of 3 byte token which instantaneously changes it into normal data packet.

iii) Token rotates in the ring, it is guaranteed that every node gets the token



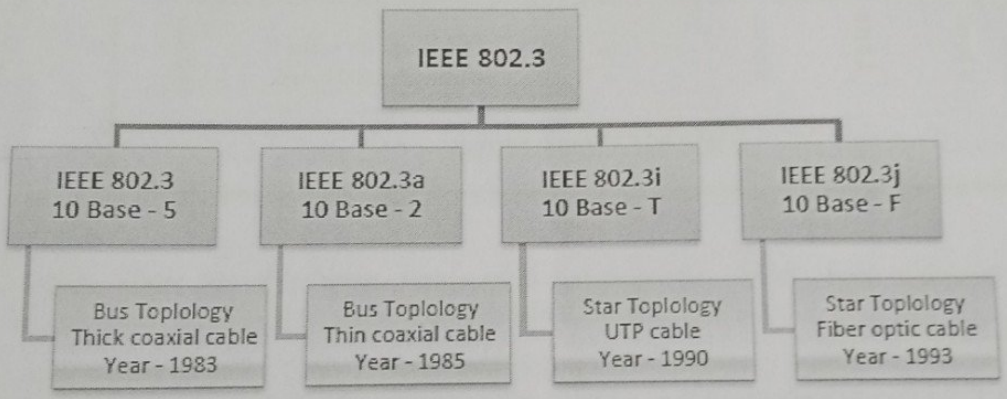
Ring Network

	802.3	IEEE 802.4	IEEE 802.5
1)	Topology used in IEEE 802.3 is Bus Topology	Bus/tree topology	Ring Topology
2 Size of frame	1572 bytes	8202 bytes	variable size
3. Priority	No priority given in this standard.	It supports priorities to stations	priorities are possible
4 Size of Data field	0 to 1500 bytes	0 to 8182 bytes	No limit
modems	Not required	required	required
protocol	is very simple	extremely complex	moderately complex
	Applicable an Real time appln & interactive appln	Real time traffic	Both

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.

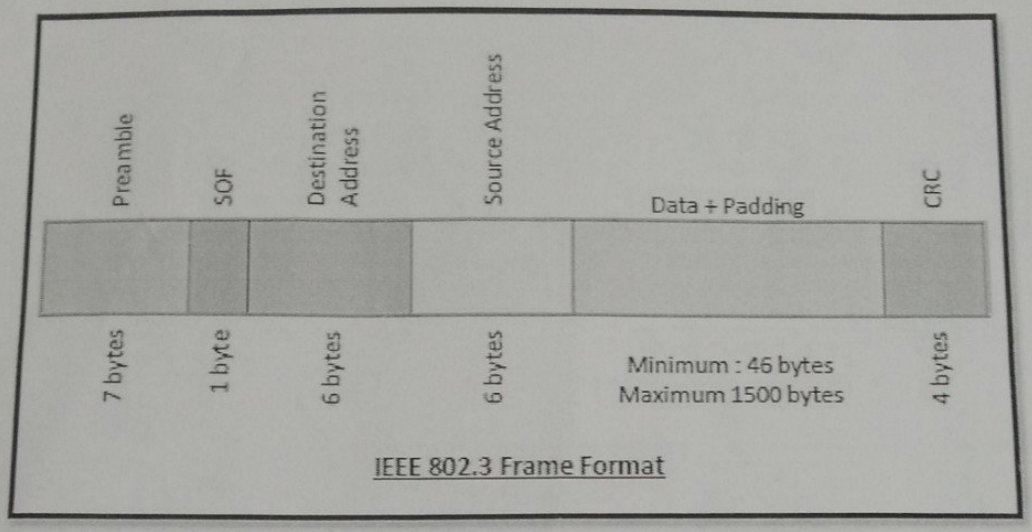


Frame Format of IEEE 802.3

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.



IEEE 802.3 Frame Format

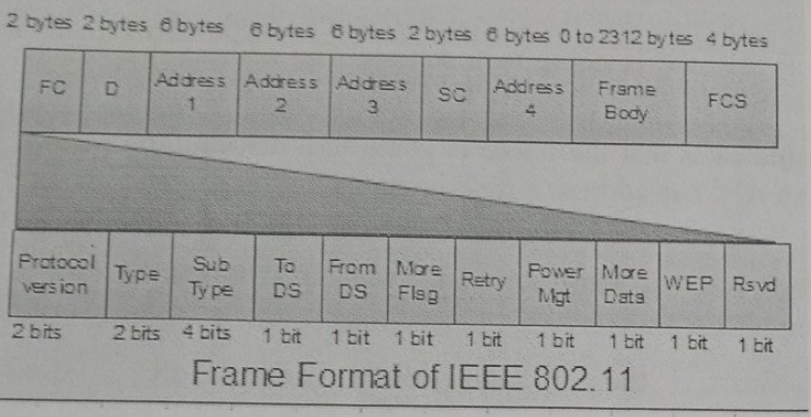
Token Bus (IEEE 802.4)

Token Bus (IEEE 802.4) is a standard for implementing token ring over the 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 the 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 –

Subtype	It defines the subtype of esch type,for control frame subtype fields are 1011 RTS,1100-CTS,1101-ACK
TO DS	Indicates Frame is going to distributed system
From DS	Indicates Frame is coming from distributed system
More Flag	if the value is 1,means more fragments
Retry	if the value is 1,means retrans mitted frame
Power Mgt	if the value is 1,means station is in power management mode
More Data	if the value is 1,means station has more data to send
Wep	Wep stands for wired equivalent privacy; if set to 1 means encryption is implimented
Rsvd	Reserved



Frame Format of IEEE 802.11

2. **D**. It stands for duration and is of 2 bytes. This field defines the duration for which the frame and its acknowledgement will occupy the channel. It is also used to set the value of NA V for other stations.

3. **Addresses**. There are 4 address fields of 6 bytes length. These four addresses represent source, destination, source base station and destination base station.

4. **Sequence Control (SC).** This 2 byte field defines the sequence number of frame to be used in flow control.

5. **Frame body**. This field can be between 0 and 2312 bytes. It contains the information.

6. FCS. This field is 4 bytes long and contains 'cRC-32 error detection sequence.

IEEE 802.11 Frame types

There are three different types of frames:

1. Management frame

2. Control frame

3. Data frame

1. **Management frame**. These are used for initial communication between stations and access points.

2. **Control frame**. These are used for accessing the channel and acknowledging frames. The control frames are RTS and CTS.

3. **Data frame**. These are used for carrying data and control information.

802.11 Addressing

- There are four different addressing cases depending upon the value of *To DS And from* DS subfields of FC field.
- Each flag can be 0 or 1, resulting in 4 different situations.

1. If *To* DS = 0 and *From* DS = 0, it indicates that frame is not going to distribution system and is not coming from a distribution system. The frame is going from one station in a BSS to another.

2. If *To* DS = 0 and *From* DS = 1, it indicates that the frame is coming from a distribution system. The frame is coming from an AP and is going to a station. The address 3 contains original sender of the frame (in another BSS).

3. If *To* DS = 1 and *From* DS = 0, it indicates that the frame is going to a distribution system. The frame is going from a station to an AP. The address 3 field contains the final destination of the frame.

4. If *To* DS = 1 and *From* DS = 1,it indicates that frame is going from one AP to another AP in a wireless distributed system.

The table below specifies the addresses of all four cases.

TO DS	From DS	Address 1	Address 2	Address3	Addres 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Protocols for Wireless LAN

S.No.	IEEE 802.3	IEEE 802.4	IEEE 802.5
1.	Topology used in IEEE 802.3 is Bus Topology.	Topology used in IEEE 802.4 is Bus or Tree Topology.	Topology used in IEEE 802.5 is Ring Topology.
2.	Size of the frame format in IEEE 802.3 standard is 1572 bytes.	Size of the frame format in IEEE 802.4 standard is 8202 bytes.	Frame format in IEEE 802.5 standard is of the variable size.

- **Destination Address:** 2-6 bytes that specifies address of destination station.
- **Source Address:** 2-6 bytes that specifies address of source station.
- **Payload:** A variable length field that carries the data from the network layer.
- **Checksum:** 4 bytes frame check sequence for error detection.
- **End Delimiter:** 1 byte that marks the end of the frame.

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.

•

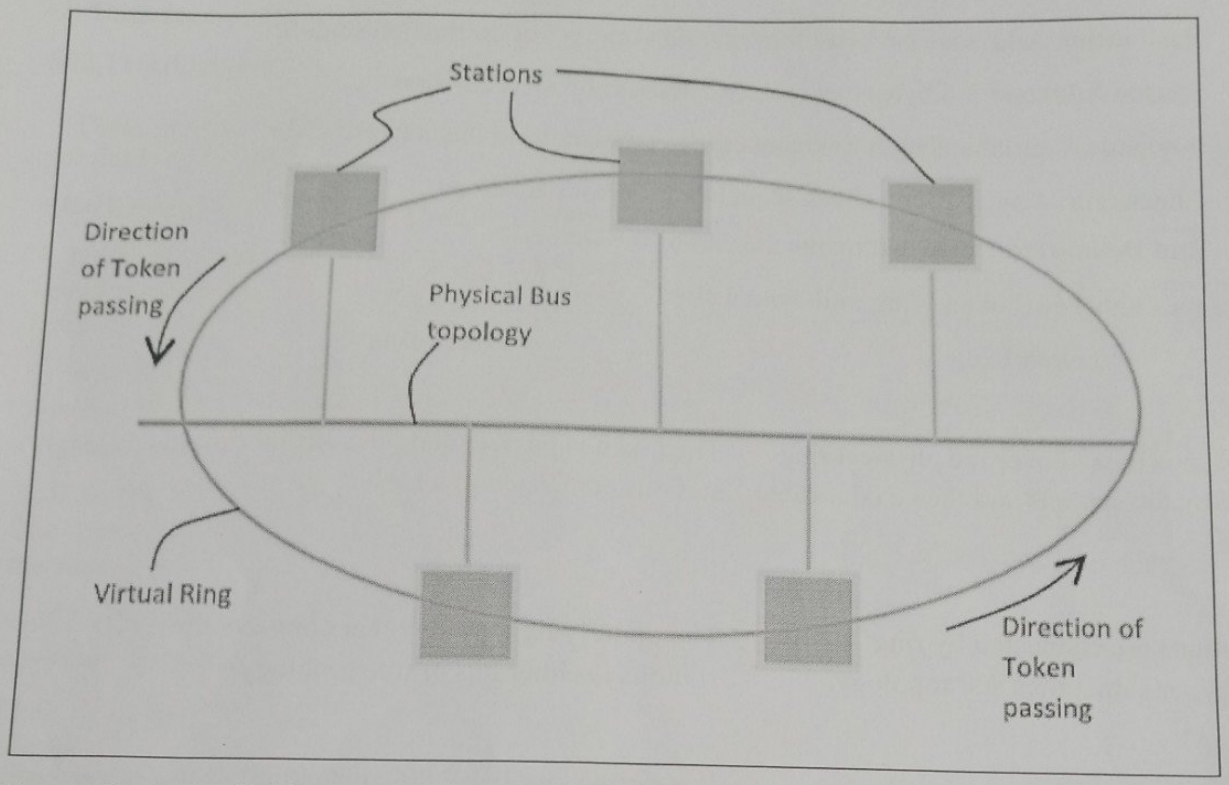
Frame Format of 802.11

The MAC layer frame consists of nine fields.

1. Frame Control (FC). This is 2 byte field and defines the type of frame and some control information. This field contains several different subfields.

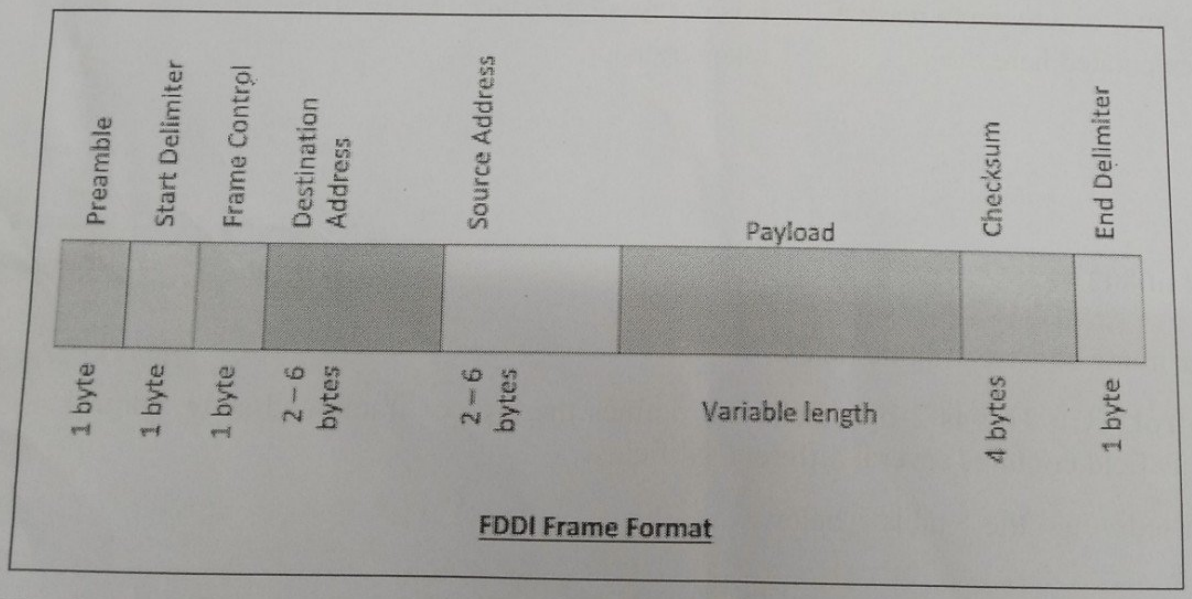
These are listed in the table below:

Field	Explanation
Version	The Current Version is 0.
Type	Specifies the type of information in the frame body 00-Management,01-control,and 10-Data.



Frame Format of Token Bus

The frame format is given by the following diagram –



The fields of a token bus frame are –

- **Preamble:** 1 byte for synchronization.
- **Start Delimiter:** 1 byte that marks the beginning of the frame.
- **Frame Control:** 1 byte that specifies whether this is a data frame or control frame.

S.No.	IEEE 802.3	IEEE 802.4	IEEE 802.5
3.	There is no priority given in this standard.	It supports priorities to stations.	In IEEE 802.5 priorities are possible
4.	Size of the data field is 0 to 1500 bytes.	Size of the data field is 0 to 8182 bytes.	No limit is of the size of the data field.
5.	Minimum frame required is 64 bytes.	It can handle short minimum frames.	It supports both short and large frames.
6.	Efficiency decreases when speed increases and throughput is affected by the collision.	Throughput & efficiency at very high loads are outstanding.	Throughput & efficiency at very high loads are outstanding.
7.	Modems are not required.	Modems are required in this standard.	Like IEEE 802.4, modems are also required in it.
8.	Protocol is very simple.	Protocol is extremely complex.	Protocol is moderately complex.
9.	It is not applicable on Real time applications, interactive Applications and Client-Server applications.	It is applicable to Real time traffic.	It can be applied for Real time applications and interactive applications because there is no limitation on the size of data.