ASST. PROFESSOR/ECE

EC8551 - CN

UNIT - II

MEDIA ACCESS AND INTERNETWORKING

INTRODUCTION:

Data link layer as two Sublayers.

Upper sublayer is responsible for data link control.

lower sublayer is responsible for resolving access to the Shared media.

Data link layer divided into two functionality-oriented Sublayers.

1. Data link Control 2. Multiple-Access resolution

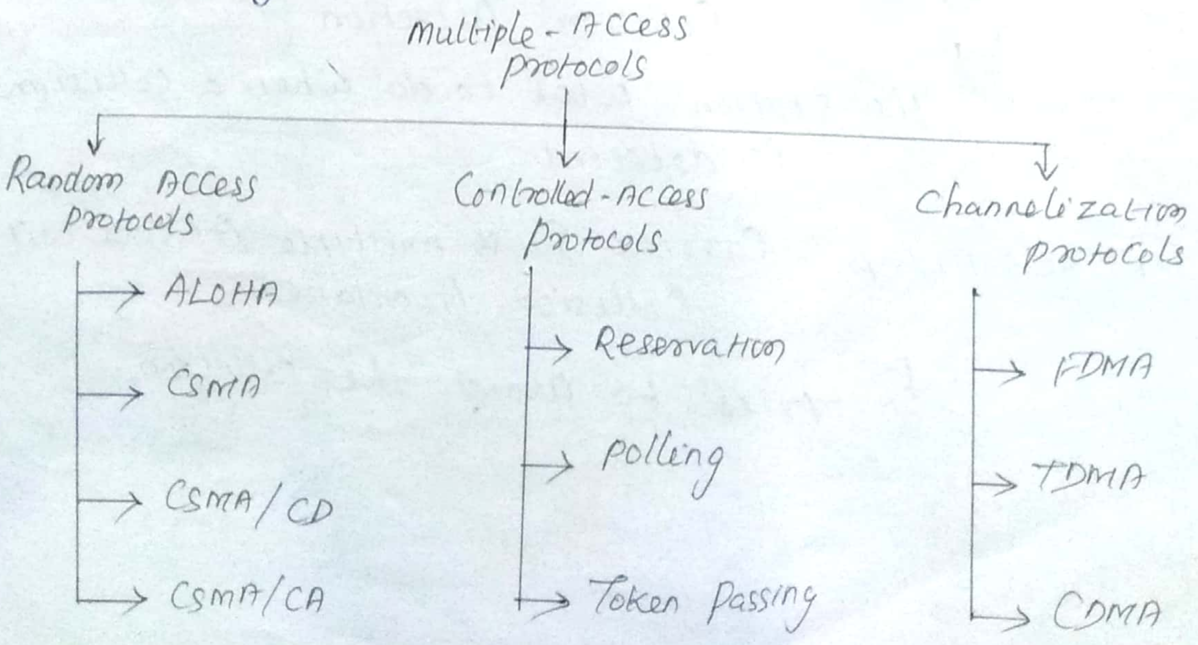
Upper sub layer is resposible for flow and Error Control is called LLC (logical link control)

Lower sublayer is responsible for multiple access resolution is called MAC (Media Access Control)

When nodes (or Stations are connected and use a Common link called a Multipoint (or broadcast link.

Multiple-access protocol to coordinate access to the link.

Taxonomy of Multiple-Access protocols:



RANDOM ACCESS:
(or)
Contention methods, No station is superior to another station and none is assigned the control over another.

No station permits (or) does not permit, another station to send.

At each instance, a station has data to send uses a procedure defined by protocol to make a decision on whether (or) not to send.

Two Features:

1) No scheduled time for a station to transmit. Transmission is random among the stations. It is called Random Access.

2) No rules specify which station should send next. Stations compete with one another to access the medium. is called Contention method.

If more than one station tries to send, there is an Access Conflict is known - Collision.

Random access methods are evolved from a interesting protocol known as ALOHA.

which used a very simple procedure called Multiple Access (MA).

Two methods:

(i) CSMA/CD - Carrier Sense Multiple Access with Collision Detection.

↓ The station what to do when a collision is detected.

(ii) CSMA/CA - Carrier Sense multiple Access with Collision Avoidance.

↓ tries to avoid the collision.

ALOHA

Earliest random access method, developed at university of Hawaii 1970.

Designed for radio (wireless) LAN, used on any shared medium.

The Medium shared between the stations.

when a station sends data, another station may attempt to do at same time.

The data from two stations collide and become garbled.

PURE ALOHA:

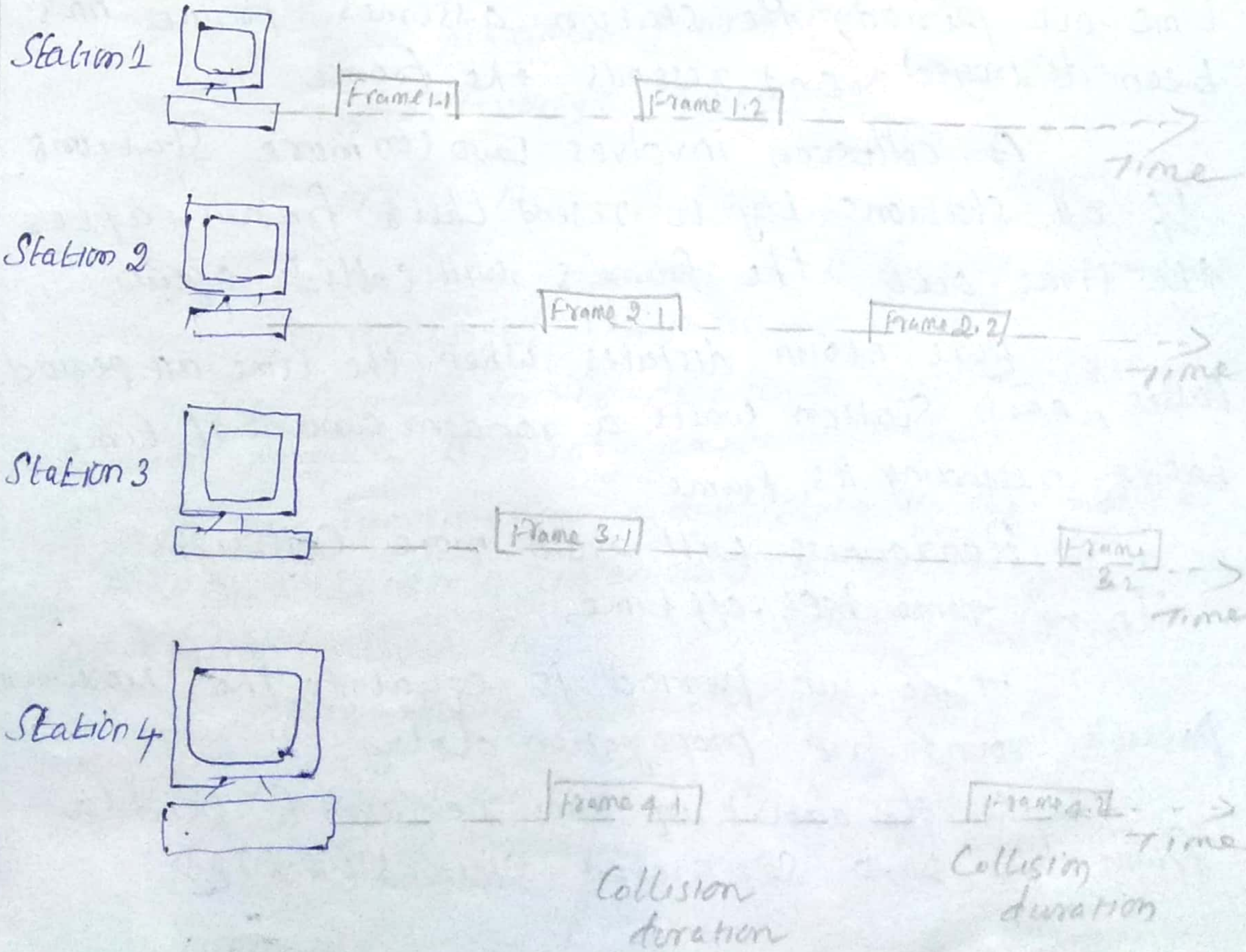
The original ALOHA protocol is called pure ALOHA.

It is simple but elegant protocol.

Each station sends a frame whenever it has a frame to send.

It's only one channel to share, possibility of collision b/w frames from different stations.

Fig: Frames in a pure ALOHA Network



Four Stations (unrealistic Assumption) Contend with one another for access to the Shared Channel.

Each station Sends two frames, total of eight frames on the Shared medium.

Some of frames Collide multiple frames in Contention for the Shared Channel.

Fig. Shows only two frames Survive. frame 1.1 from Station 1 and frame 3.2 from Station 3.

If one bit of a frame Coexists on channel with one bit from another frame, is a collision and both will destroyed.

Need to resend the frames are destroyed during transmission.

Pure ALOHA protocol relies on acknowledgments from the R_x^r. when a station sends a frame, it expects the R_x^r to send an acknowledgment.

If acknowledgment does not arrive after a time-out period, the station assumes frame has been destroyed and resends the frame.

A collision involves two (or) more Stations. If all Stations try to resend their frames after the time-out, the frames will collide again.

Pure-ALOHA dictates when the time-out period Passes, each Station waits a random amount of time before resending its frame.

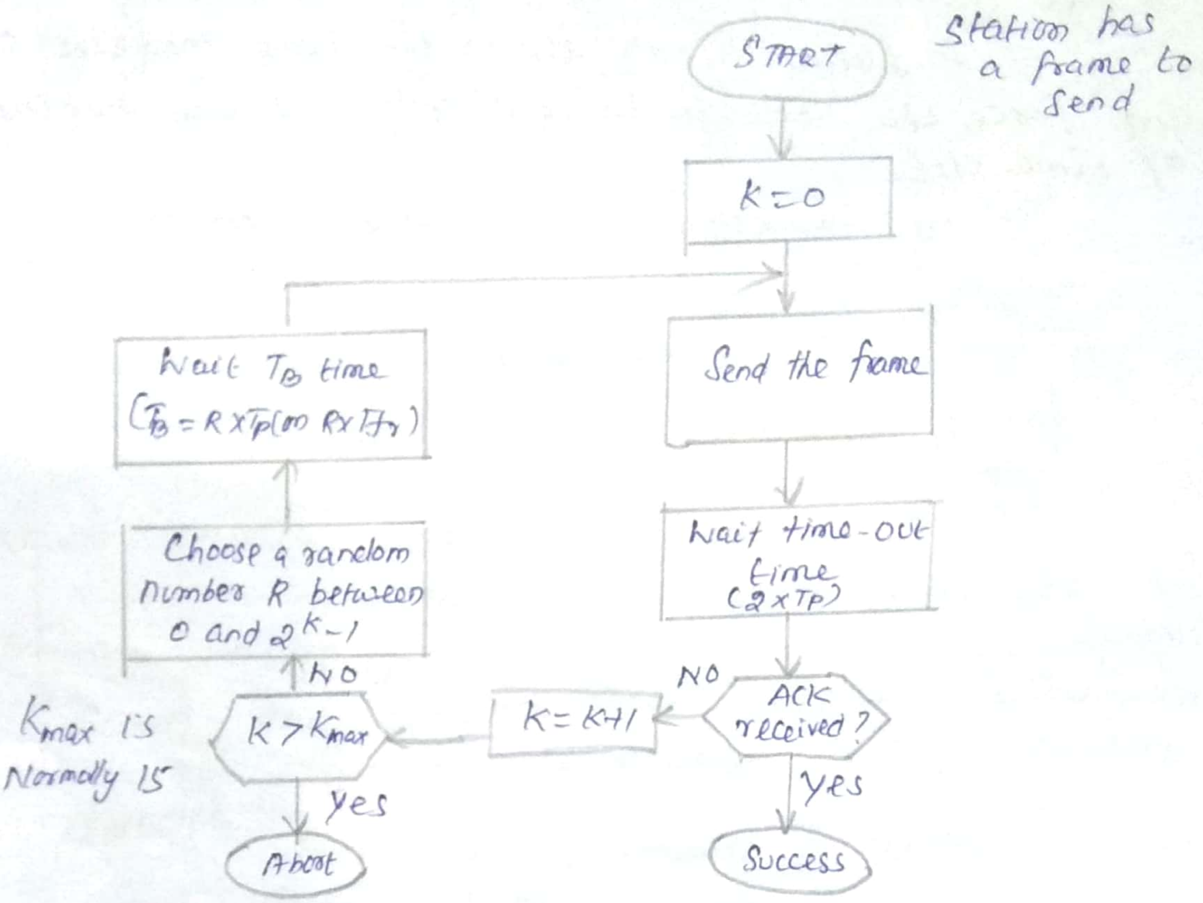
Randomness will avoid more Collisions.

T_B → Time back-off time

Time-out Period is equal to the Maximum possible round-trip propagation delay,

Twice the amount of time required to send a frame b/w two Separated Stations ($2 \times T_P$)

PROCEDURE FOR PURE-ALOHA PROTOCOL:


START
Station has a frame to send
K=0
Send the frame
Wait time-out time (2×Tp)
NO
ACK received?
yes
Success
K=K+1
K>Kmax
yes
Abort
NO
Choose a random number R between 0 and 2^K-1
Wait TB time (TB = R×Tp (or R×Tfr))
Kmax is Normally 15

K → Number of attempts

T_p → Maximum propagation time

T_{fr} → Average transmission time for a frame

T_B → Back-off time.

T_B → Random value depends on 'K' (no of attempted unsuccessful transmissions)

The formula for T_B depends on implementation Common formula is binary exponential back-off

for each transmission, a multiplier in the range 0 to 2^k-1 randomly chosen and multiplied by T_p (Maximum propagation time (or) T_{fr}.

Pure ALOHA Vulnerable time $= 2 \times T_{fr}$

The throughput for pure ALOHA is $S = G \times e^{-2G}$

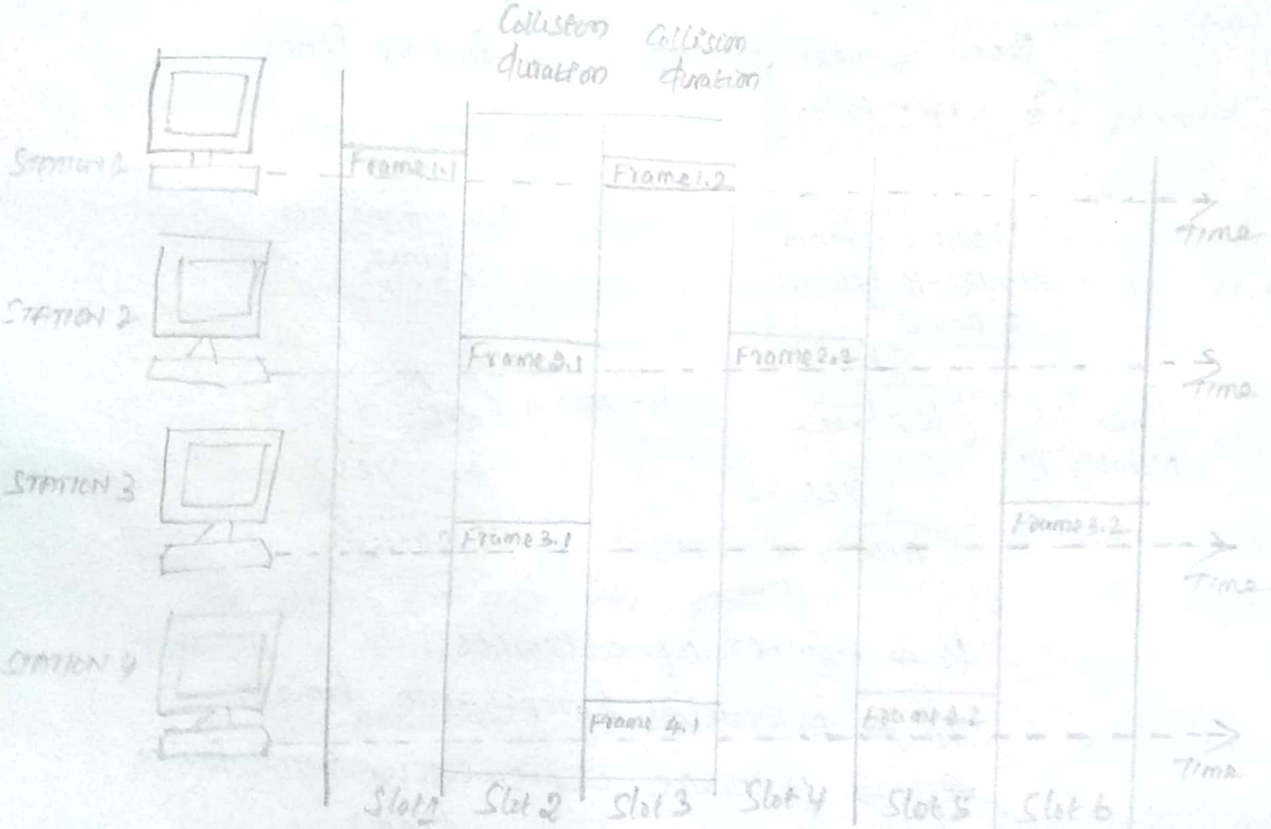
The maximum throughput $S_{max} = 0.184$ when $G = (1/2)$

SLOTTED ALOHA:

Slotted ALOHA was invented to improve the efficiency of pure ALOHA.

In Slotted ALOHA divide the time into slots of T_{fr} s and force the station to send only at the beginning of time slot.

Fig. Frames in a Slotted ALOHA Network



A station is allowed to send only at the beginning of Synchronized time slot, If a Station misses this moment it must wait until the beginning of the next time slot.

The station which started at beginning of this slot already finished sending its frame.

Still the possibility of collision if two stations try to send at beginning of same time slot

The vulnerable time is now reduced to one-half equal to T_{fr}.

THROUGHPUT: $S = G \times e^{-G}$

The maximum throughput $S_{max} = 0.368$ when $G = 1$

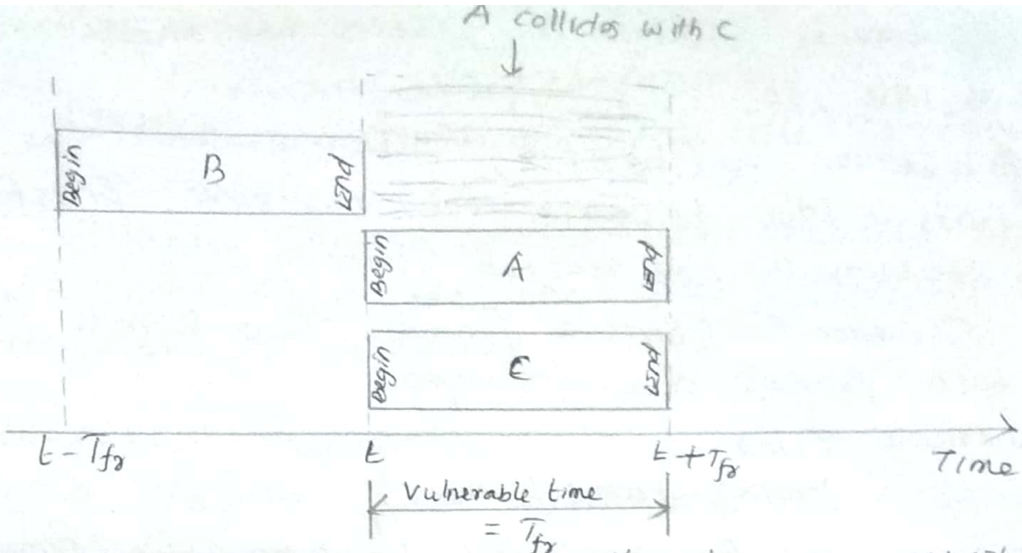


Fig. Vulnerable Time for Slotted ALOHA protocol

CARRIER SENSE MULTIPLE ACCESS [CSMA]

To minimize the collision and increase the performance, CSMA was developed.

CSMA, each station first listen to the medium (or) check the state of the medium before sending.

principle "Sense before transmit" (or) "listen before talk"

It can reduce the possiblity of collision but cannot eliminate it. Stations are connected to share channel

The possibility of collision still Exists because propagation delay.

When a station sends a frame, still take time for first bit to reach every stations and every station to sense it.

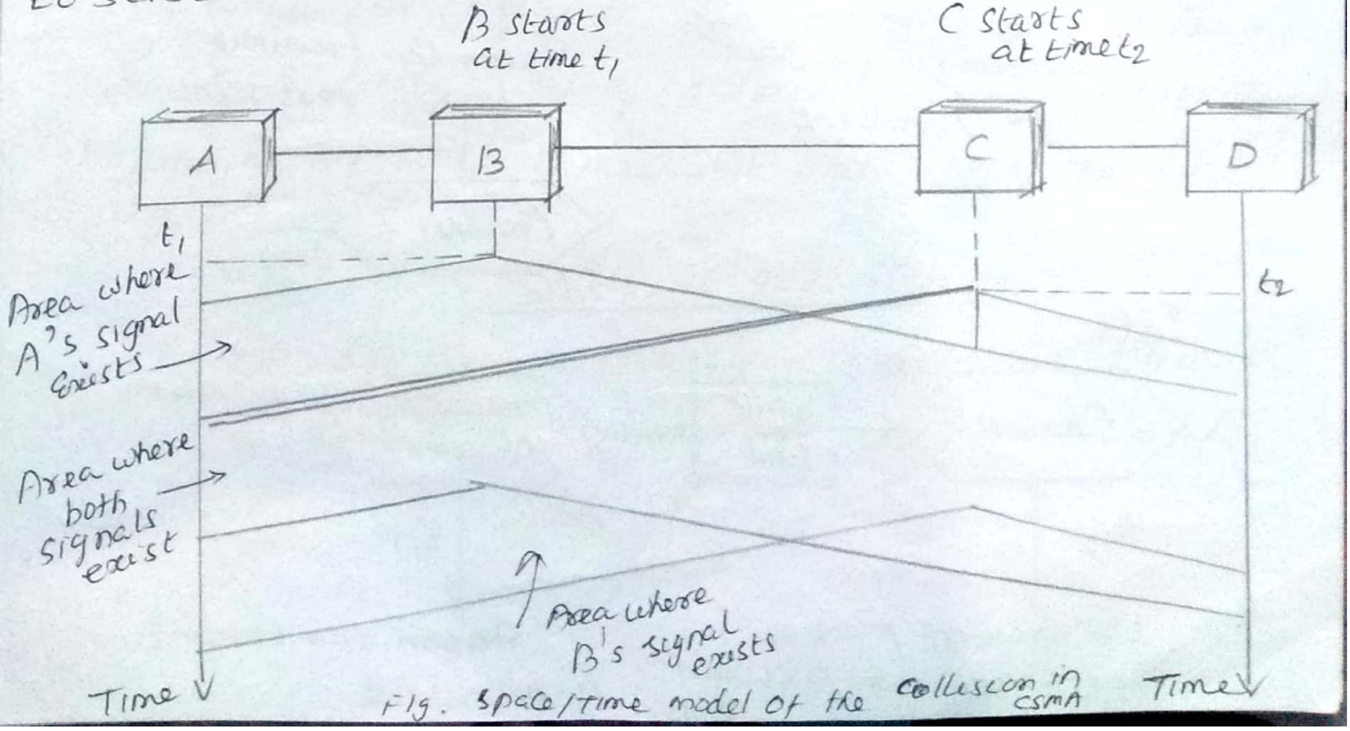

B starts at time t_1
C starts at time t_2
A
B
C
D
t_1
t_2
Area where A's signal exists
Area where both signals exist
Area where B's signal exists
Time
Time

Fig. space/time model of the collision in CSMA

At time t_1, Station B senseses the medium and finds it idle, so sends a frame.

At time t_2 ($t_2 > t_1$), Station C senses the medium and finds it idle, because at this time, first bits from station B not reached Station C.

Station C sends a frame. Two signals Collide and both frames are destroyed.

vulnerable Time:

propagation time T_p

Time needed for a signal to propagate from one end of the medium to other.

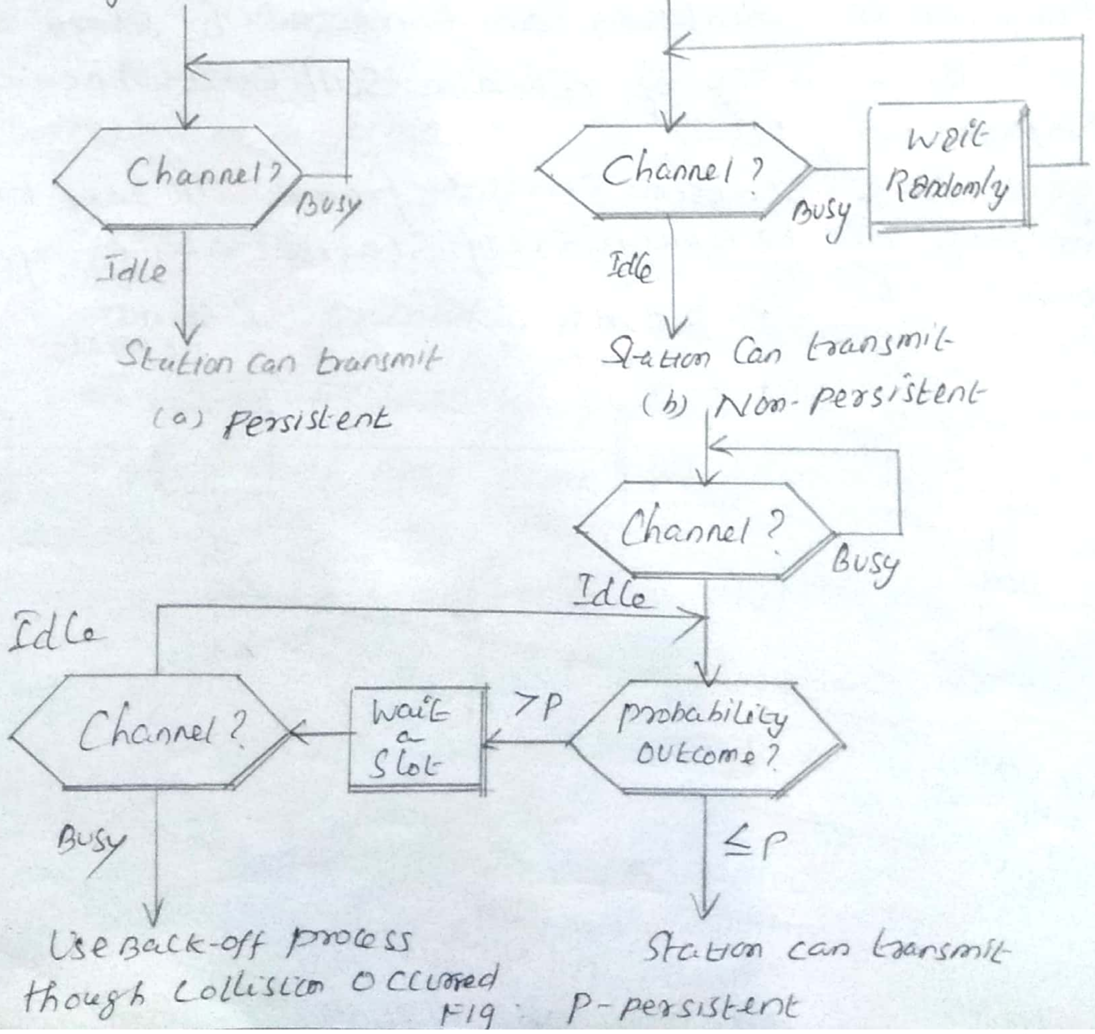
When station sends a frame, & any other Station tries to send a frame during this time, a collision will Result.

Station D at time $t_1 + T_p$.

Behavior of Three persistence Methods.

1. persistent 2. Non-persistent 3. p-persistent

Flow diagram for Three persistence Methods.



(a) Persistent

(b) Non-persistent

Fig: P-persistent

1. persistent method:

Simple and straightforward.
after the station finds the line idle, it sends frame immediately

Highest chance of collision because two (or more stations find the line idle & send frames immediately. eg. Ethernet

2. Non-persistent method:

a station has a frame to send senses the line. If line is idle, it sends immediately
If line is not idle, it waits a Random amount of time and senses the line again.

It reduces the chance of collision because two (or more stations wait same amount of time and retry to send simultaneously.

It reduces the efficiency of N/w

3. p-persistent Method:

Used if channel time slots with a slot duration equal to (or greater than maximum propagation time.

It reduces the collision & improves efficiency

Steps:

1. with probability p, the station sends its frame.
2. with probability q = 1 - p, the station waits for beginning of next time slot and check the line again.

a) If line is idle, it goes step 1

b) If the line is busy, it acts as through collision occurred & uses back off procedure

CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD)

CSMA method does not specify the procedure following a collision.

CSMA/CD augments algorithm to handle collision

a station monitors the medium after it sends a frame to see if transmission was successful.

Station is finished, collision frame is sent again

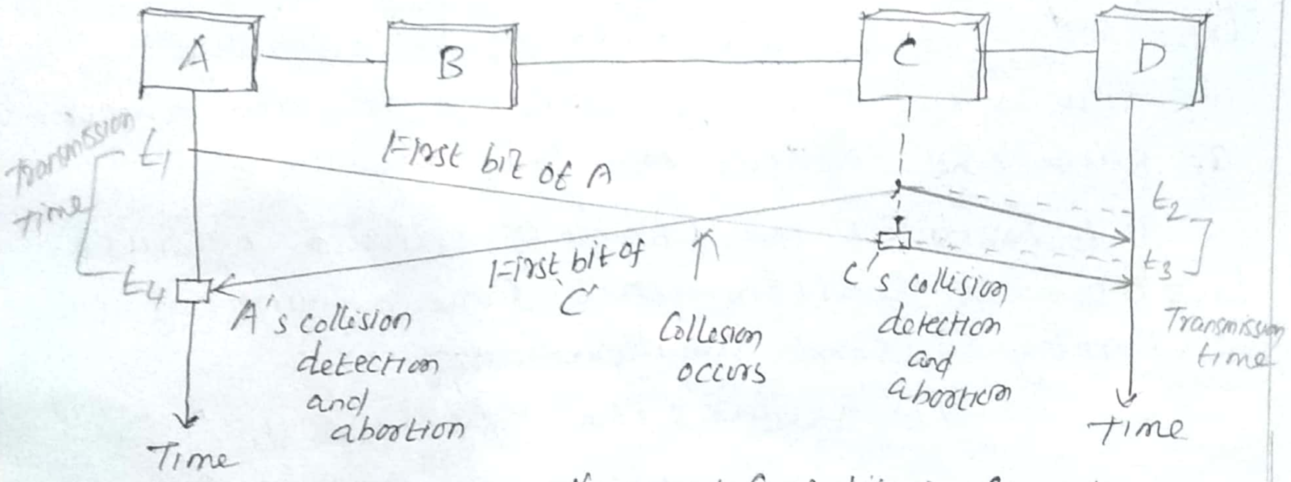


Fig: Collision of first bit in CSMA/CD.

At time t_1, Station A executed its persistence procedure & starts sending the bits of its frame.

At time t_2, Station C not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in frame, which propagate both to left and to right.

Collision occurs sometime after time t_2. Station C detects a collision at time t_3 it receives first bit of A's frame.

Station C immediately (or after a short time aborts transmission.

Station A detects collision at time t_4 it receives the first bit of C's frame. It also immediately aborts transmission

A transmits for duration $t_4 - t_1$

C transmits for duration $t_3 - t_2$

Protocol work, length of any frame divided by bit rate in this protocol must be more than either of these durations.

At time t_4, transmission of A's frame, incomplete, aborted. At time t_3, the transmission of B's frame though incomplete, is aborted.

k → No of attempts

T_p → Maximum propagation Time

T_{fr} → Avg Transmission time for a frame

T_B → Back-off Time

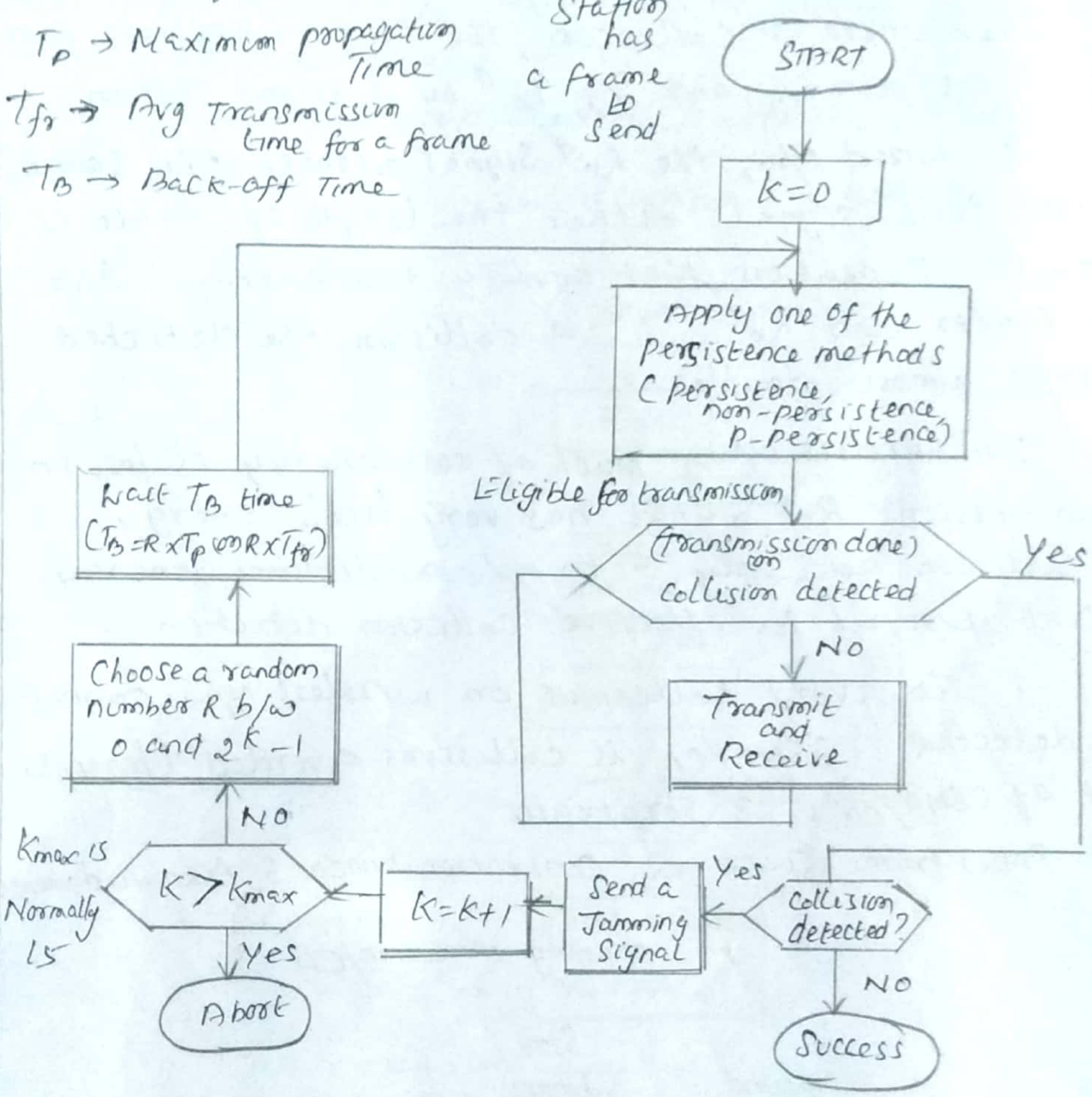

Station has a frame to send
START
k=0
Apply one of the persistence methods (persistence, non-persistence, p-persistence)
Eligible for transmission
(Transmission done) (or) collision detected
Yes
NO
Transmit and Receive
Collision detected?
Yes
NO
Success
Send a Jamming Signal
K=k+1
K > Kmax
Kmax is Normally 15
NO
Yes
Abort
Choose a random number R b/w 0 and $2^k - 1$
Wait T_B time ($T_B = R \times T_p$ (or) $R \times T_{fr}$)

Fig. Flow diagram for CSMA/CD

Throughput.

CSMA/CD is greater than pure (or) slotted ALoha. Maximum throughput occurs at a different value of G and based on persistence method and value of p in the p-persistent approach.

1. persistent max throughput around 50% when G=1.

Non-persistent " " 90% G b/w 3 and 8.

CSMA/CA - [CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE]

A station needs to be able to receive while Tx^g to detect a Collision.

when there is no Collision, the Station receives one S/g, its own Signal.

when there is collision, the station receives two S/g's, its own S/g and S/g Tx^d by a second Station

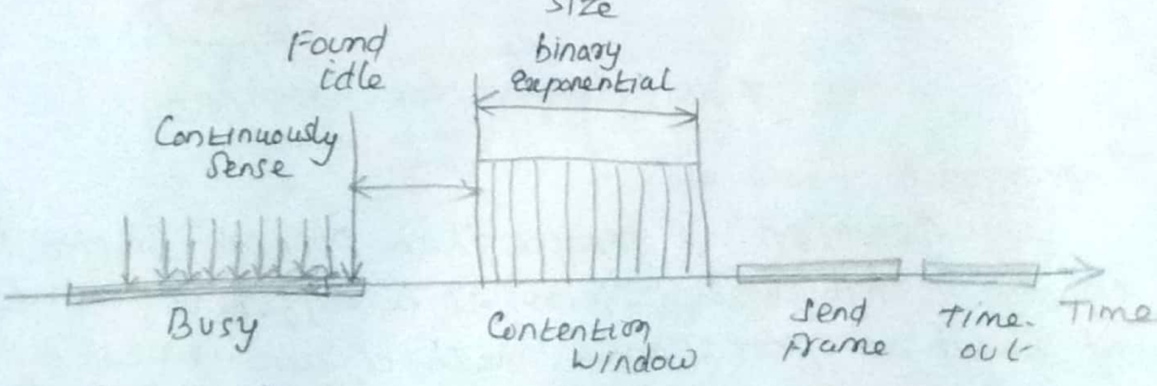
In wired N/w, the Rx^d Signal almost the same energy sent signal either the length of Cable is Short con Repeaters that amplify the energy b/w the sender and Rx^r. ∴ a collision, the detected energy almost doubles.

In wireless N/w, Much of sent energy is lost in Transmission. Rx^d signal has very little energy. a collision add only 5 to 10% additional energy. Not useful for effective collision detection.

To avoid collisions on wireless N/w cannot be detected. CSMA/CA is collisions avoided through use of CSMA/CA's 3 Strategies.

1. Inter frame Space 2. Contention window 3. Acknowledgments

Fig. Timing in CSMA/CA



1. IFS (Interframe Space):

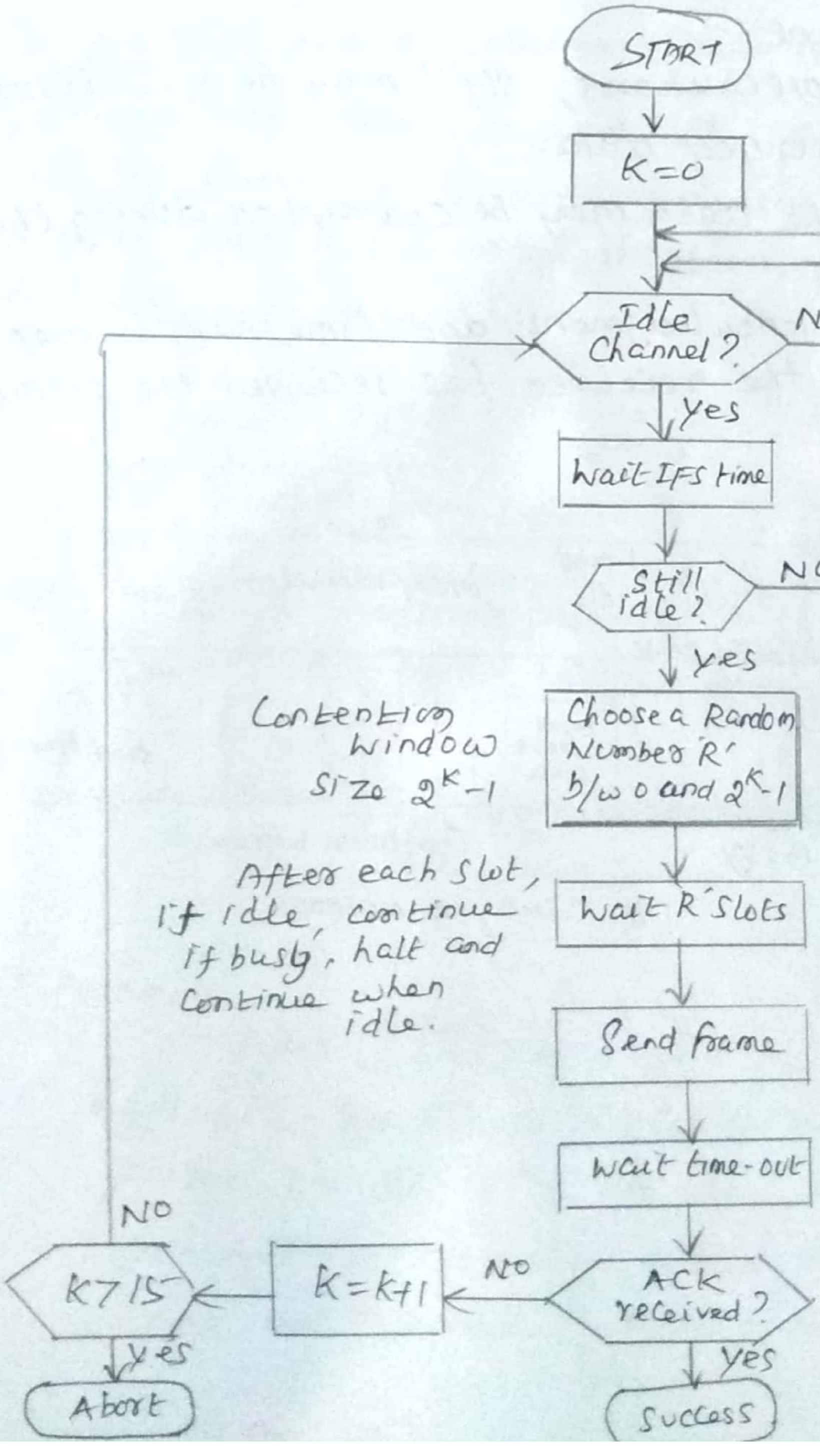
Collisions are avoided by deferring transmission even if channel is found idle. when idle channel is found the station does not send immediately. It waits for a period of time called Interframe Space (or) IFS.

IFS time allow the front of Txd S/g by distant station to reach this station.

After IFS time channel is still idle the station can send, It still needs to wait a time equal to contention time (described text)

IFS variable can used to prioritize stations (or) Frame type.

Fig. Flow diagram for CSMA/CA


START
K=0
Idle Channel?
NO
yes
Wait IFS time
Still idle?
NO
yes
Choose a Random Number R' b/w 0 and 2^K-1
Contention window size 2^K-1
Wait R' slots
After each slot, if idle, continue if busy, halt and continue when idle.
Send frame
Wait time-out
ACK received?
NO
K=K+1
K>15
NO
yes
Abort
yes
Success

2. Contention window:

An amount of time divided into slots. A station is ready to send chooses a random number of slots as wait time.

No of slots in the window changes according to binary exponential back-off strategy.

"In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window, it stops the timer and restarts it when the channel becomes idle."

3. Acknowledgment:

with all precautions, still may be a collision resulting in destroyed data.

In addition, the data may be corrupted during the transmission

positive acknowledgment and time-out timer help guarantee the receiver has received the frame.

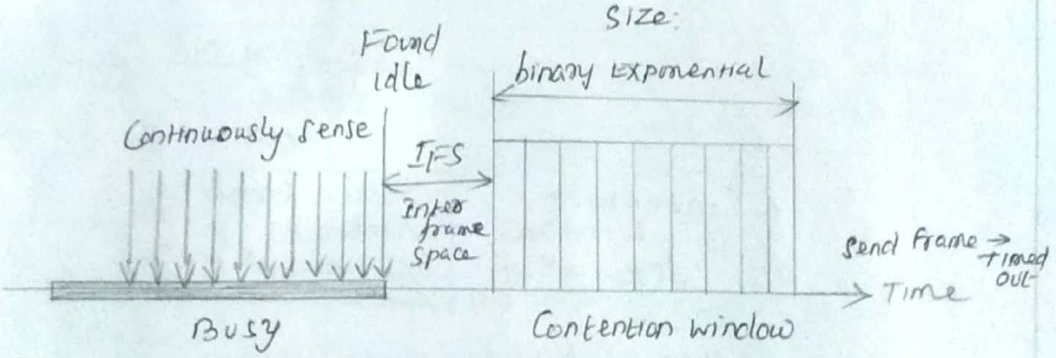


Fig: CSMA/CA METHODS

STANDARD ETHERNET : IEEE 802.3

The original Ethernet technology with the data rate of 10Mbps as Standard Ethernet

Fast Ethernet (100 Mbps)

Gigabit Ethernet (1 Gbps)

Ten-Gigabit Ethernet (100 Gbps)

Characteristics:

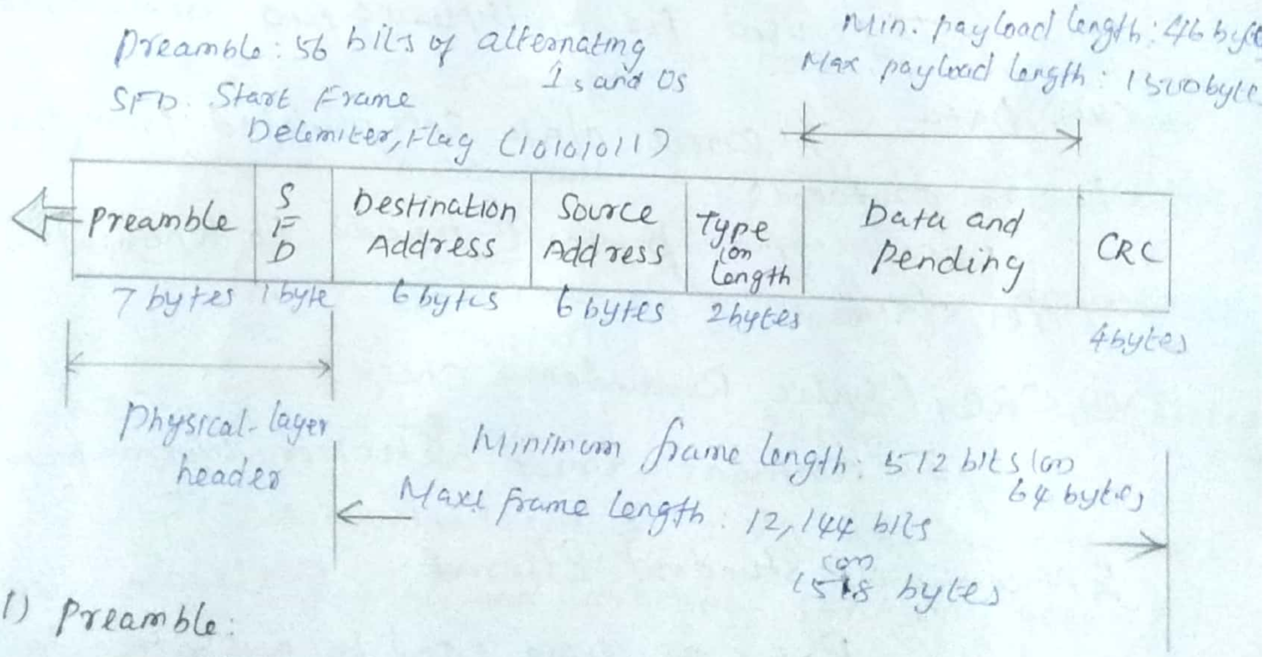
1. Connectionless
2. Unreliable service

1. Each frame sent is independent of previous (or) next frame.
2. No Connection Establishment (or) Connection termination phases.

(2) Unreliable like IP and UDP (User Datagram protocol)

If frame is corrupted during transmission and receiver finds out about Correction.

Ethernet frame:


Preamble: 56 bits of alternating 1s and 0s
SFD: Start Frame Delimiter, Flag (10101011)
Min. payload length: 46 byte
Max payload length: 1500 byte
Preamble
S F D
Destination Address
Source Address
Type (or) Length
Data and Pending
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits (or) 64 bytes
Maxi frame length: 12,144 bits (or) 1518 bytes

(1) Preamble:

7 bytes (56 bits) of 0's and 1's.

Enable to synchronize clock its out of Synchronization pattern provides only an alert and timing pulse. Preamble is actually added at the physical layer and not (formally) part of the frame.

ii) Start Frame delimiter (SFD)
S/g's of field is beginning of the frame.
It warns the Station (or Stations is the last chance for synchronization.

(iii) Destination Address (DA)
6 bytes (48 bits) and contains the link layer address of destination station (or stations to receive the packet.

(iv) SA (Source Address)
It contains the link layer address of the Sender of the packet.

(v) Type (or length: It defines the upper layer protocol whose packet is encapsulated in the frame.
Protocol can be IP, ARP (Address Resolution protocol)
OSPF (Open Shortest path First)
It is used for Multiplexing and demultiplexing

(vi) Data:
It carries data encapsulated from the upper-layer protocols.
upper layer protocol needs to know the length of its data.

(vii) CRC: (Cyclic Redundancy check)
It contains Error detection information.

Efficiency of Standard Ethernet:
Ratio of time used by a station to send data to the time medium is occupied by this Station.

Efficiency = $1/(1+6.4\times a)$

a → Parameter is the no of frames on the medium.
a = propagation delay / transmission delay.

Ex: Soln: Standard Ethernet with transmission rate 10 Mbps (1×10^7)

Length of the medium = 2500 m

Size of the frame = 512 bits

Propagation Speed of the S/g in cable is normally = 2×10^8 m/s

Propagation delay = $2500/(2\times10^8)$

= 12.5 μs

Transmission delay = $512/(10^7)$

= 51.2 μs

$a = 12.5/51.2$

$a = 0.24$

Efficiency = $1/(1 + 6.4 + 0.24)$

= 39%.

Implementation: (Data Rate 10 Mbps)

Implementation	Medium	Medium Length	Encoding
10 Base 5	Thick Co-axial	500 m	Manchester (Base band)
10 Base 2	Thin co-axial	185 m	Manchester
10 Base-T	2-UTP (unshielded twisted pair)	100 m	Manchester
10 Base-F	2-Fiber	2000 m	Manchester

It uses Baseband S/g, The bits are changed to a digital signal and directly sent on the line.

10Base5: 1st implementation is called 10 Base5 (or Thick Ethernet (or Thicknet.

Use a bus topology with External Transceiver Connected via a thick coaxial cable.

If a length of more than 500 m is upto five segments, each a maximum of 500 meters, using Repeaters

10 Base 2:

2nd implementation is called 10Base 2, thin Ethernet (or) Cheapernet.

Uses a Bus topology. Cable is much Thinner and more flexible.

It's a part of N/w interface Card (NIC) is installed inside the station.

10-Base -T -

3rd implementation is called 10 Base-T (or) Twisted-Pair Ethernet.

It uses a physical star topology.

Stations are Connected to a hub via two pairs of twisted cable.

To minimize the effect of attenuation in twisted Cable.

10-Base-F : Fiber Ethernet.

It uses a Star topology to connect Stations to hub Stations are Connected to hub two fiber-optic cables.

FAST ETHERNET (100 MBPS)

1990's LAN technologies with transmission rate higher than 10 Mbps.

The new generation wast called Fast Ethernet.

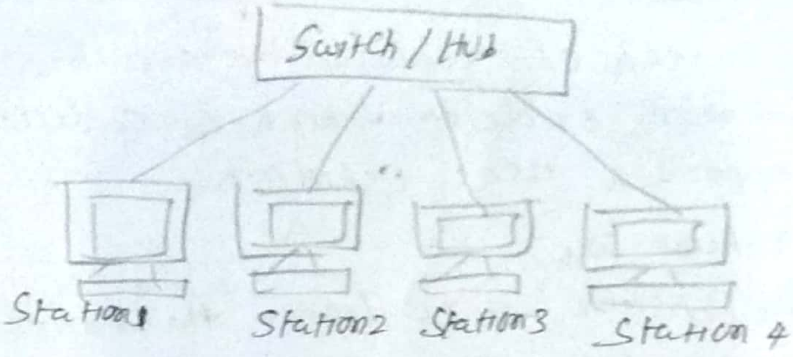
Features:

1. upgrade the data rate to 100 Mbps
2. Make it Compatible with Standared Ethernet
3. Keep the Same 48-bit address
4. Keep the same frame format.

Fast Ethernet is called "autonegotiation".

It was designed for,

* To allow incompatible devices to connet to one another.
* To allow one device to multiple capabilities
* To allow a station a check a hub's capabilities



point-to-point Communication

Fig : Fast Ethernet topology.

Implementation	Medium	Medium length	wires	Encoding
100Base-TX	UTP (or) STP	100m	2	4B5B+MLT-3
100Base-FX	Fiber	185m	2	4B5B+NRZ-I
100Base-T4	UTP	100m	4	Two 8B/6T.

GIGABIT ETHERNET:

higher data rate 1000 Mbps.

IEEE Standards called Standard 802.3z.

The design follows,

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard (or) Fast Ethernet
3 use the same 48-bit address
4. Use the Same frame format
5. Keep the same minimum and maximum frame lengths.
6. to support auttonegotiation as defined in Fast Ethernet.

Full-duplex Mode: a Central Switch connected to all Computers (or) other Switches.

For each input port, each switch has buffers are Stored in data until they are Tx^d.

CSMA/CD is not used.

Full-duplex mode of Gigabit Ethernet, no collision. Maximum length of cable is determined by Signal attenuating in cable.

Half-duplex-Mode.

a switch can replaced by a hub. act as a common cable in which a collision occur. The approach uses CSMA/CD.

CSMA/CD scheme are,

1. Carrier Extension. → It defines the minimum length of frame as 512 bytes (4096) bits.

2. Frame Bursting: Each frame carries redundant data. to improve efficiency, frame bursting was proposed.

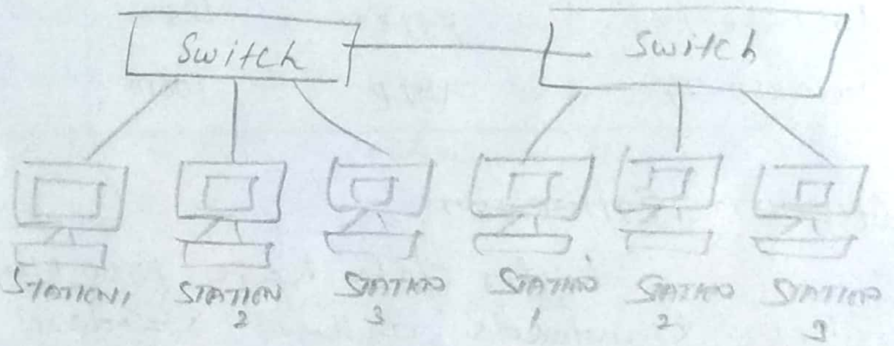


Fig: Two stars based on point-to-point.

WIRELESS LAN [IEEE 802.11]

IEEE has defined specifications for wireless LAN, called IEEE 802.11.

Covers the physical and data-link layers.

Sometimes called wireless Ethernet"

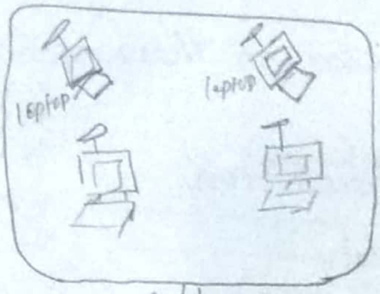
Some contries, USA, The public uses the term WiFi (wireless fidelity).

ARCHITECTURE:

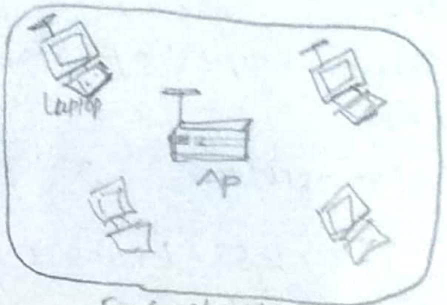
The Standard defines two kind of services

1. BSS (Basic Service Set)
2. ESS (Extended Service Set)

1. BSS: A basic service set is made of stationary (or) mobile wireless stations and central base station is known as Access point (AP).



Adhoc BSS



Infrastructure BSS

A BSS is made of stationary (or Mobile wireless stations and optional Central Base Station, known as Access point (AP)

BSS without an AP is a Stand-alone Network and Cannot send data to other BSSs. called Adhoc architecture

Stations a N/w without need of an AP, locate one another and agree to part of a BSS.

A BSS with AP referred to infrastructure BSS

ESS. [Extended Service Set].

Made up of two (or More BSSs with APs BSSs are Connected through a distribution System Which is a wired (or a wireless N/w

distribution S/m Connects the APs in the BSSs.

IEEE 802.11 does not restrict the distribution System.

Any IEEE LAN such as Ethernet.

Mobile stations are Normal Stations inside a BSS

Stationary Stations are AP Stations are part of a wired LAN

When BSS, are Connected, the Stations within reach of one another can Communicate without use of AP.

Communication b/w Station in a BSS & outside BSS occurs via A.P.

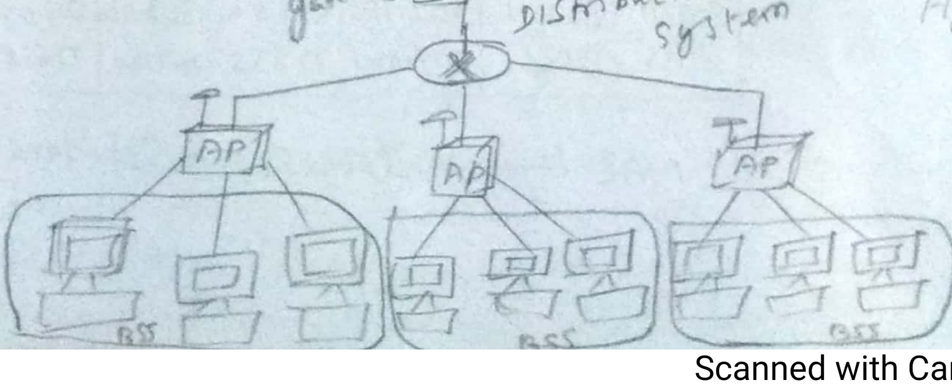


Fig. Extended Service set

STATION TYPE.

Three types of Stations based on their mobility in wireless LAN.

1. No-transition 2. BSS-transition

3 ESS-transition Mobility

1. A Station either Stationary (not moving)(or) Moving only inside a BSS.

2. A station BSS transition Mobility can move from one BSS to another, but movement is Confined inside one ESS.

3. It can move from one ESS to another.

IEEE 802.11 does not guarantee that Communication is continuous during the move.

MAC Sub layer:

IEEE 802.11 defines two MAC Sublayer.

1. DCF [Distributed Coordination Function]

2. PCF [point Coordination Function]

MAC Sublayer relationship b/w two, LLC sublayer & Physical layer.

DCF: DCF uses CSMA/CA as access method.

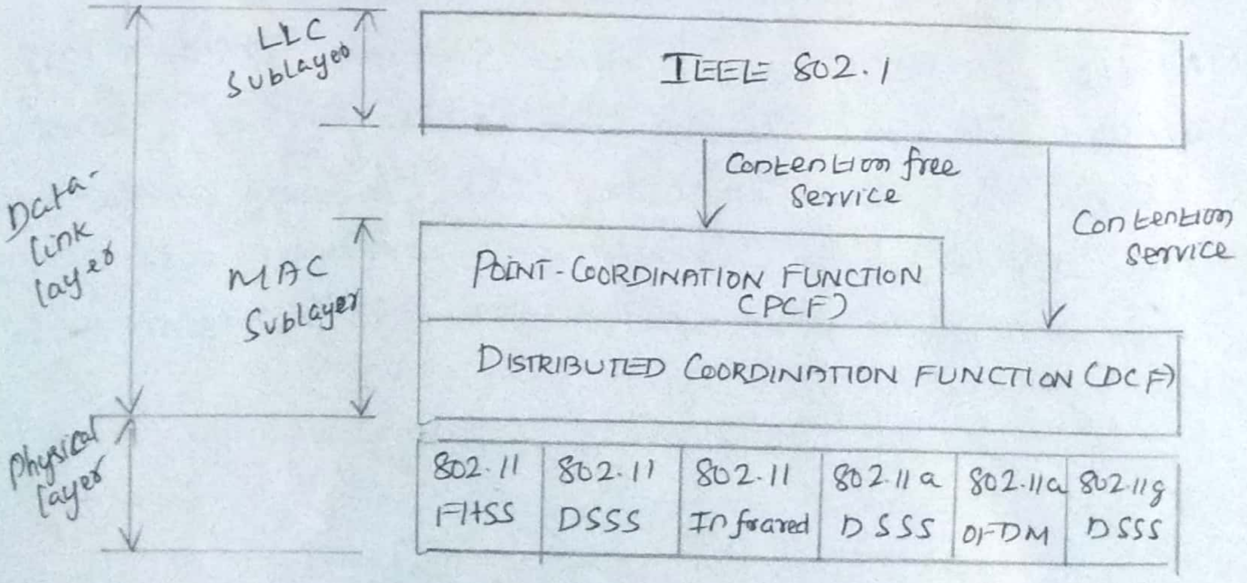


Fig: MAC layer in IEEE 802.11 Standard.

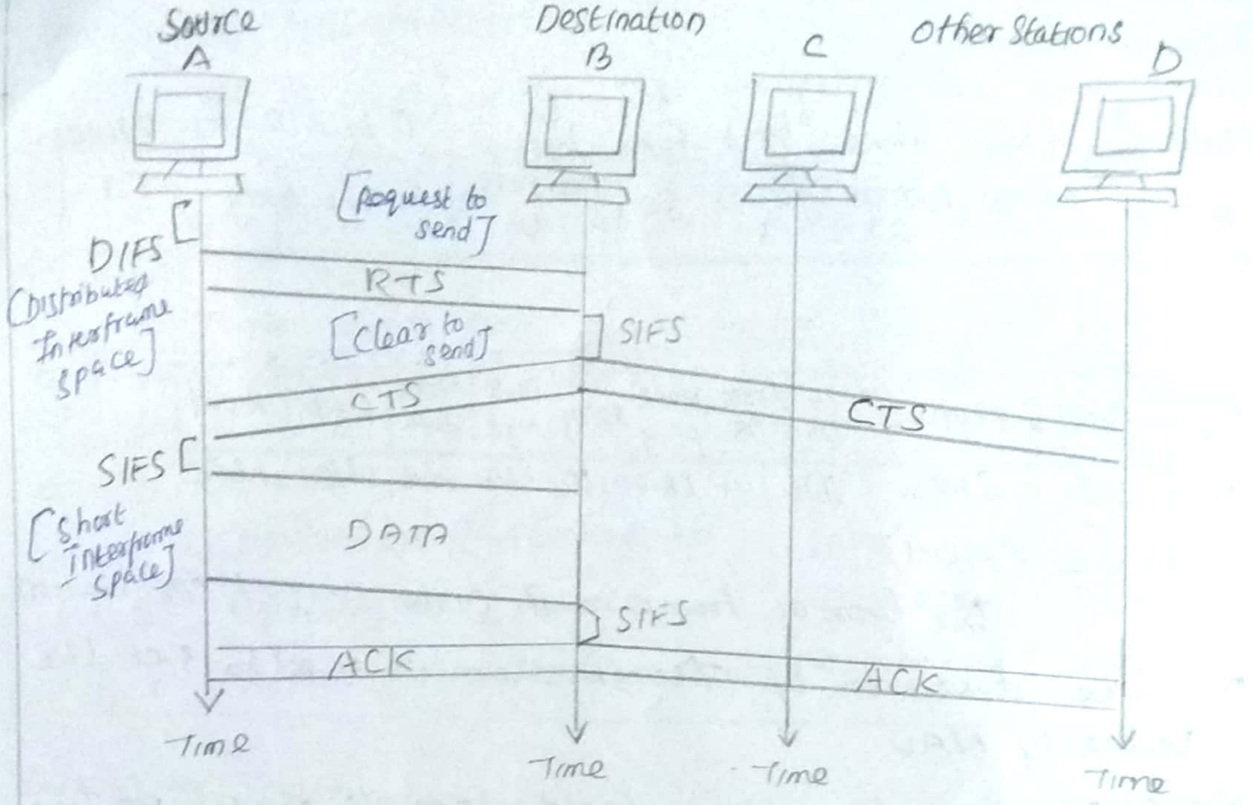


Fig. CSMA/CA and NAV [NETWORK ALLOCATION VECTOR]

NETWORK ALLOCATION VECTOR (NAV):

When a Station Sends an RTS frame, the duration of time it needs to occupy the channel. The stations are affected by transmission Create a timer called a NAV.

Collision DURING HANDSHAKING.

What happens if there is a Collision during the time when RTS (or) CTS control frames in transition often called Handshaking period.

Two (or) More Stations try to send RTS frames at same time. These Control frames may collide.

PCF [point Coordination Function]

It is an optimal acces method Can implemented in an infrastructure Network (not in ad hoc Network)

It's implemented on top of the DCF and used mostly for time-Sensitive transmission

A repetition interval designed to cover both Contention-free PCF and Contention-based DCF traffic.

Repeatition interval, repeated Continuosly, Starts with a special Control frame called beacon frame.

FRAME FORMAT :

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	Frame body	FCS

Protocol version	Type	Subtype	To DS	From DS	More flag	Retry	Pwr mgt	More data	WEP	Rsvd
2bits	2bits	4 bits	1bit	1bit	1bit	1bit	1bit	1 bit	1 bit	1 bit

FC (Frame Control) :
The type of frame and some control information

D. The duration of Transmission is used to set the value of NAV.

Addresses : each address field depends on the value of To DS and From DS subfields.

Sequence Control (SC). First 4 bits define the fragment number, last 12 bits define the Sequence Number.

Frame body: It contains information based on the type and subtype defined in FC field.

FCS : It contains a CRC-32 error detection sequence. [Frame check sequence]

Frame types : 1. Management frames
IEEE 802.11 2. Control Frames
3. data frames

Management frames : Used for initial communication between stations and access point (AP).

Control frames :
used for Accessing the channel and acknowledging frames.

Data Frames :
used for carrying data and Control informations.

ADDRESSING MECHANISM:

It is defined by the value of the two flags in FC Field, To DS and From DS.

Each flag Can be either 0 (or) 1, resulting in four different Situations.

Table: Addresses

To DS	From DS	Address 1	Address 2	Address 3	Address 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

WIRELESS PROTOCOLS:

Wireless LAN, instead use either radio (or) infrared technology to connect a node (or) group of nodes into main body of N/w.

LANs require special MAC Sublayer protocol.

CSMA protocol cannot be used with wireless LANs.

The protocol designed for wireless LANs is MACA.

MACA:

MACA protocol is based on IEEE 802.11 wireless standards.

The sender to stimulate the receiver into outputting a Short frame.

Transmitter sends RTS (Request to Send) signal to the receiver and receiver replies it with CTS (Clear to send), signal transmitter will transmit the data frames to Rx.

MACAW:

The MACAW protocol is the improvement of MACA.

ACK frame is introduced after each data frame.

Mechanism for stations to exchange information about congestion introduced. To improve the S/m Performance.

REQUIREMENTS OF WIRELESS LAN:

1. Number of Nodes
2. Throughput
3. connection to backbone LAN
4. Service Area
5. Battery power consumption
6. Transmission Robustness and Security
7. Hand off / roaming

APPLICATION OF WLAN:

1. LAN Extension

2. Cross building interconnect

3. Nomadic access

4. Ad hoc Networking.

BLUETOOTH:

It is a wireless LAN technology designed to connect devices of different functions such as Telephones, notebooks, Computers (desktop and Laptop), Camera, printers.

A BT LAN is an ad hoc Network, which Means that network is formed spontaneously, the devices, sometimes called gadgets, find each other and make a n/w called a PICONET.

A BT LAN can be connected to the internet if one of the gadgets capability.

BT Applications, Peripheral devices such a wireless mouse can keyboard can Communicate with the Computer through this technology.

BT was originally Started by Ericssion company
It's named Harald Blaatand, King of Denmark (940-981)
Blaatand translates to Bluetooth in English.

BT protocol defined by IEEE 802.15 Standard defines a wireless personal - Area N/w (PAN) operable in an area the size of a room (or) hall.

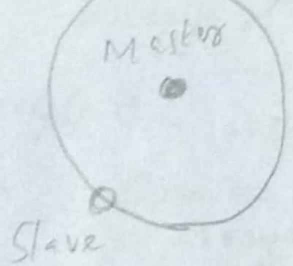
ARCHITECTURE:

Bluetooth defines two types of N/w's
1. Piconet 2. Scatternet

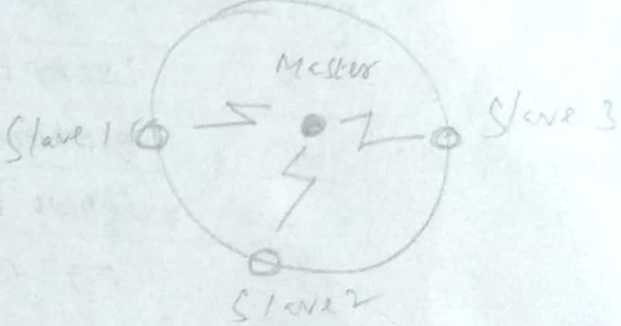
Piconets:

A BT network is called a piconet (or small net. upto 8 stations, one of which is called the primary, the rest are called secondaries.

Piconet can only one primary station. Communication b/w the primary and secondary stations can be one-to-one (or) one-to-many.



(a) Single -Slave piconet



b) Multi-Slave piconet

SCATTERNET:

Piconets can be combined to form is called a scatternet. A secondary station in one piconet can be the primary in another piconet.

Station can receive messages from the primary in first piconet (as secondary) and acting as primary, delivers to secondaries in the 2nd piconet.

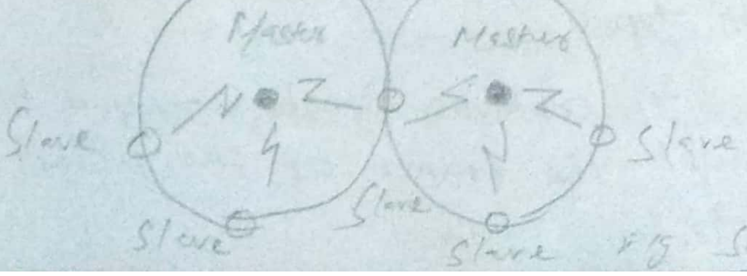


fig Scatternet

BT range ≃ 10 meters Upto 100 meters.

BT globally unlicensed ISM radio band of 2.4GHZ

ISM (Industrial, Scientific and medical) 2.4 - 2.484GHZ

From any authority. BT, Supports both voice and data, it supports both circuit switching and packet switching.

A BT device has a built-in short range radio Tx?. Current data rate is 1Mbps with a 2.4 GHZ.

Interface b/w IEEE 802.11b wireless LANs and Bluetooth LANs

BLUETOOTH LAYER:

L2CAP [logical link Control and Adaptation protocol : (on L2CAP [LL]. → LLC Sublayer in LANs

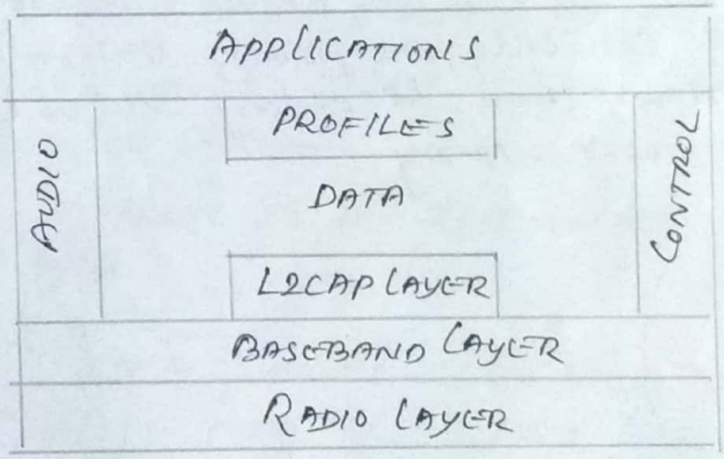


Fig: Bluetooth layers.

2bytes	2 bytes	0 to 65,535 bytes
Length	Channel ID	Data and Control

Fig: L2CAP data packet format

L2CAP → used for data Exchange on ACL Link (Asynchronous Connectionless Link)

SCO channels do not use L2CAP. (Synchronous Connection oriented)

FRAME FORMAT TYPES:

Access code: It contains synchronization bits and to distinguish the frame of one piconet from of another.

Header : Each pattern has following subfields.

Address : Used for broadcast communication from the primary to all secondaries.

Type : Type of data coming from the upper layer.

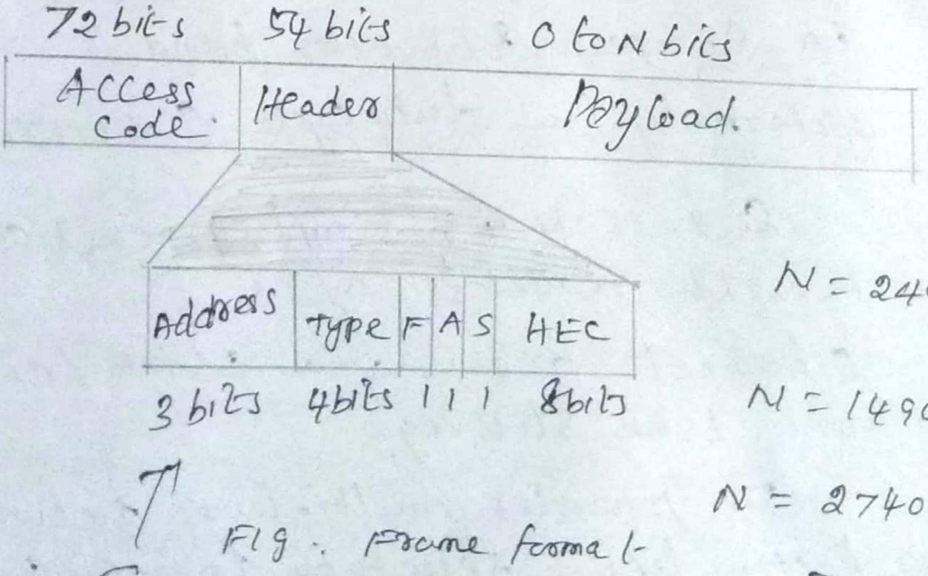
F : Flow control, set 1 device is unable to receive more frames (buffer is full)

A : Acknowledgment.
BT uses stop and wait ARQ. 1 bit is sufficient for acknowledgment.

S : It holds a sequence number.

HEC : 8-bit [header error correction] subfield is a checksum to detect errors in each 18-bit header section.
There is no Retransmission in this sublayer.

payload : It contains data or control information coming from the upper layers.



N = 240 for 1 slot frame

N = 1490 for 3-slot frame

N = 2740 for 5-slot frame.

Fig. Frame format

(18 bit part is repeated 3 times)

ZIGBEE [IEEE 802.15.4]

This standard does not standardize the higher communication protocol layers, including N/w and application layer.

To assure interoperability b/w devices operating the IEEE 802.15.4 standard.

Mission of organization, to define reliable, Cost effective, low-power, wirelessly networked Monitoring and control products based on open global Standard. by Zigbee Alliance.

CHARACTERISTICS:

1. Data rates of 250kbps; 20 kbps and 40kbps
2. Star or peer to peer operation.
3. To support for low latency devices
4. CSMA/CA channel access
5. Dynamic device addressing
6. low power Consumption.
7. 16 channels in 2.4 GHz ISM band, 10 channels in the 915 MHz, ISM band and one channel in European 868 MHz band.
8. Externely low duty cycle (< 0.1%)

802.15.4 is simple packet data protocol for lightweight wireless N/w's.

Channel access via CSMA/CA and optional time slotting.

It provides multi-level security. Long Battery life, selectable latency for controllers, sensors, remote Monitoring and portable Electronics. For Maximum Battery life

Two different device types:

1. FFD (Full Function Device),
2. RFD (Reduced Function Device)
   — only operate in a device mode

Three modes. Device, coordinator PAN Coordinator

IEEE 802.15.4 Physical layer:

Functions of physical layer.

1. Activation and deactivation of Radio Transceiver.
2. Energy detection within current channel
3. Clear channel assessment for received packets
4. channel frequency selection
5. Data transmission and Reception.

Network Layer functions

1. path determination: Route by packets from source to destination. Routing algorithms used
2. switching: Move packets from routers input to appropriate router o/p.
3. Call setup: some N/w architectures require router call setup along path before data flows.

CIRCUIT SWITCHING:

1. There is physical connection b/w Tx? and Rx?
2. All the packet uses same path.
3. Needs an end to end path before the data transmission.
4. Reverses the entire B.W in advance.
5. Charge is based on distance and time but not on traffic
6. wastable of B.W is possible
7. Congestion occurs for minute
8. Cannot support store and forward retransmission
9. Recording of packet can never happen with Circuit switching

PACKET SWITCHING:

1. No physical path is established b/w Tx and Rx.
2. packet travels independently
3. No needs of end-to end path before data transmission
4. Does not Reverse the Bandwidth in advance.
5. Charge is based on both number of bytes and Connect time.
6. No waste of B.w.
7. Congestion occurs Per Minute (packet)
8. It support store and forward transmission
9. Recording of packet is possible.

IPV4 ADDRESSES.

Ip corresponds to the N/w layer in OSI Reference mode and provides a Connectionless Best effort delivery service to the transport layer.

Internet protocol (IP) address a fixed length of 32 bits.

IPv4 addresses are unique. Two devices on internet can never have same address at the same time.

Two level of Hierarchy.

1. Network ID : Identifies the N/w the host is connected to,
2. Host ID : Identifies the Network Connection to the Host rather than the actual host.