CH:3

GSM = Global System for Mobile Comms.

(Digital Cellular)

- GSM - 900 MHz
  - 890 - 915 → uplink
  - 935 - 960 → downlink
- GSM - 1800 MHz
  - 1710 - 1785 → uplink
  - 1805 - 1880 → downlink
- GSM - 1900 MHz (Personal Comms)
  - 1850-1915 → uplink
  - 1930-1990 → downlink

Characteristic :

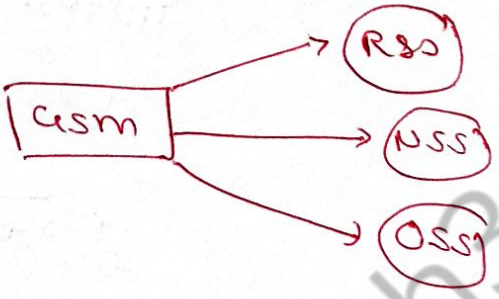
- Communication
- Total mobility
- Worldwide connectivity
- High capacity
- Security fxns
- High transmission quality

GSM
↳ based on [set of standards] formulated in the early (1980's) by Companies [NOKIA, MOTOROLA, etc]

Gsm Architecture

Divided into 3 parts:

1. Radio / Base station Subsystem (RSS & BSS)
2. Network switching subsystem (NSS)
3. Operation support subsystem (OSS)



Additional component

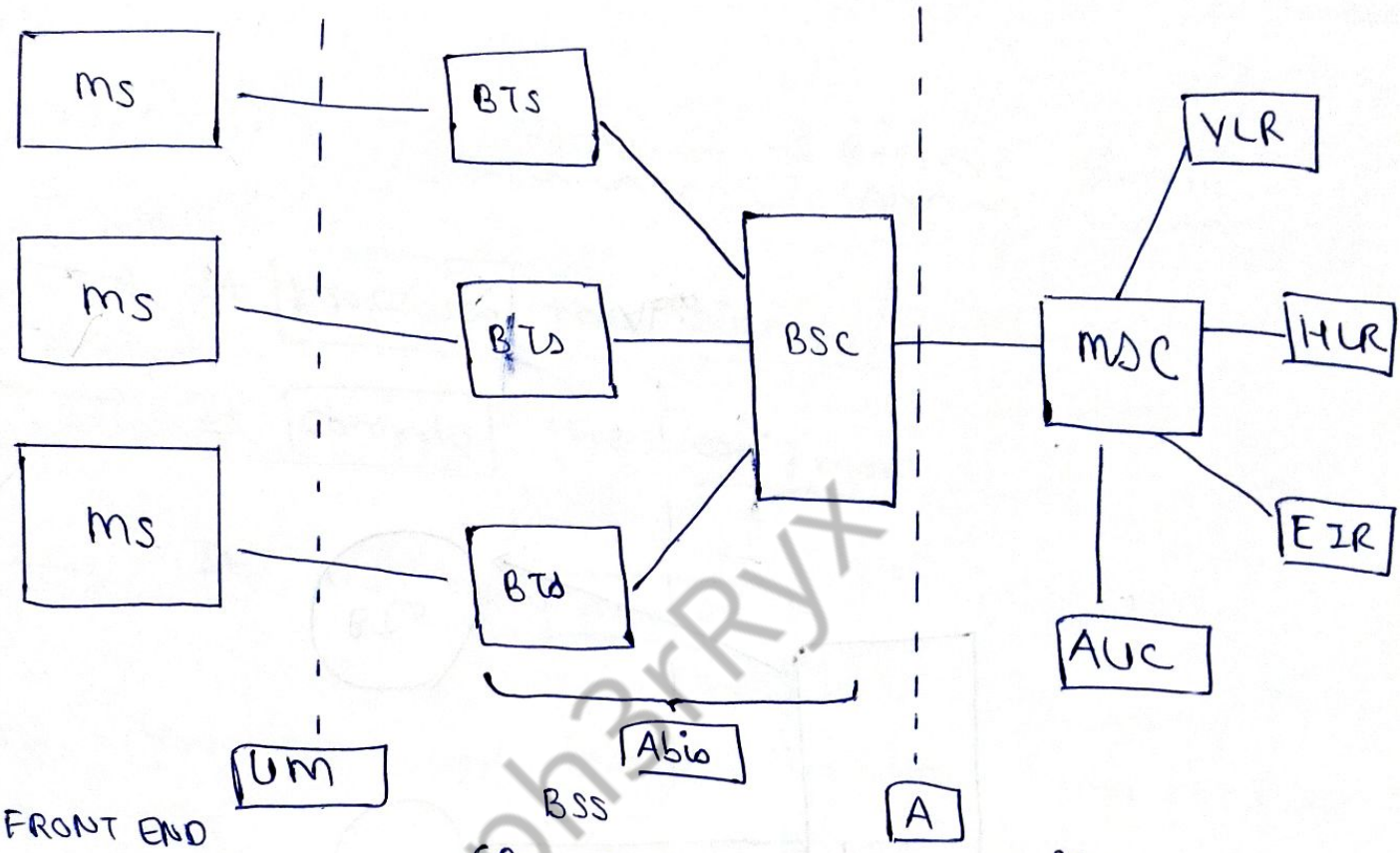
- HLR => Home Location register
- VLR => Vistor Location register
- EIR => Equipment Identity register
- AUC => Authentication center

(HLR, VLR, EIR, AUC) — registers / database.

- SMS SC => SMS serving center
- Gmsc => Gateway MSC
- CBC => ChargeBack center
- TRAU => Transcode & Adaptation Unit.

~~Structure~~

Architecture



MS ⟶ mobile service
BTS ⟶ Base station service
→ Connected via (Um) interface

(Tower) BTS ⟶ Base Transreciever Station
BSC ⟶ Base station Controller
→ Connected via (Abis) interface.

MSC ⟶ mobile station controller
→ Connected via (A) interface.

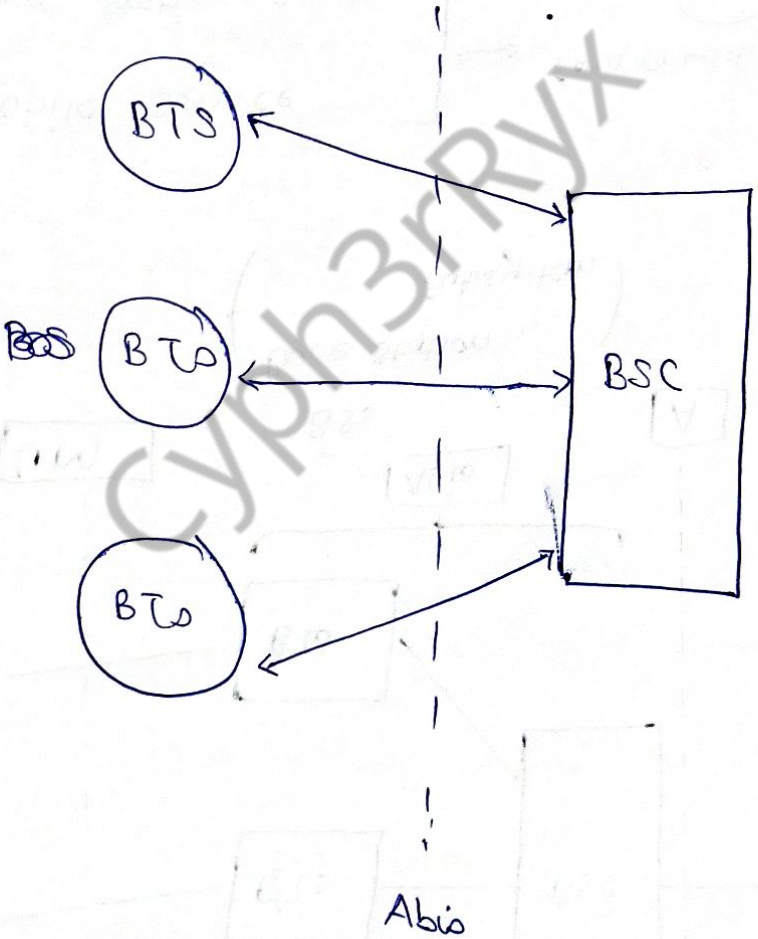
Here, MS — front end → mobile service] children's child

BTS — middle logic → Base Transceiver service] — child

BSC — middle logic → Base station controller] — Parent

MSC — Back end → Mobile station controller.] Grand Parent

BSS :



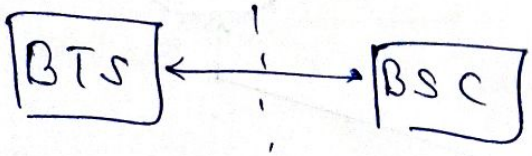
BTS is like a "Tower of mobile"

- TRX → Transmit & Recieve signals.
- It processes the signals.
- It controls the equipment.
- It also has antennas

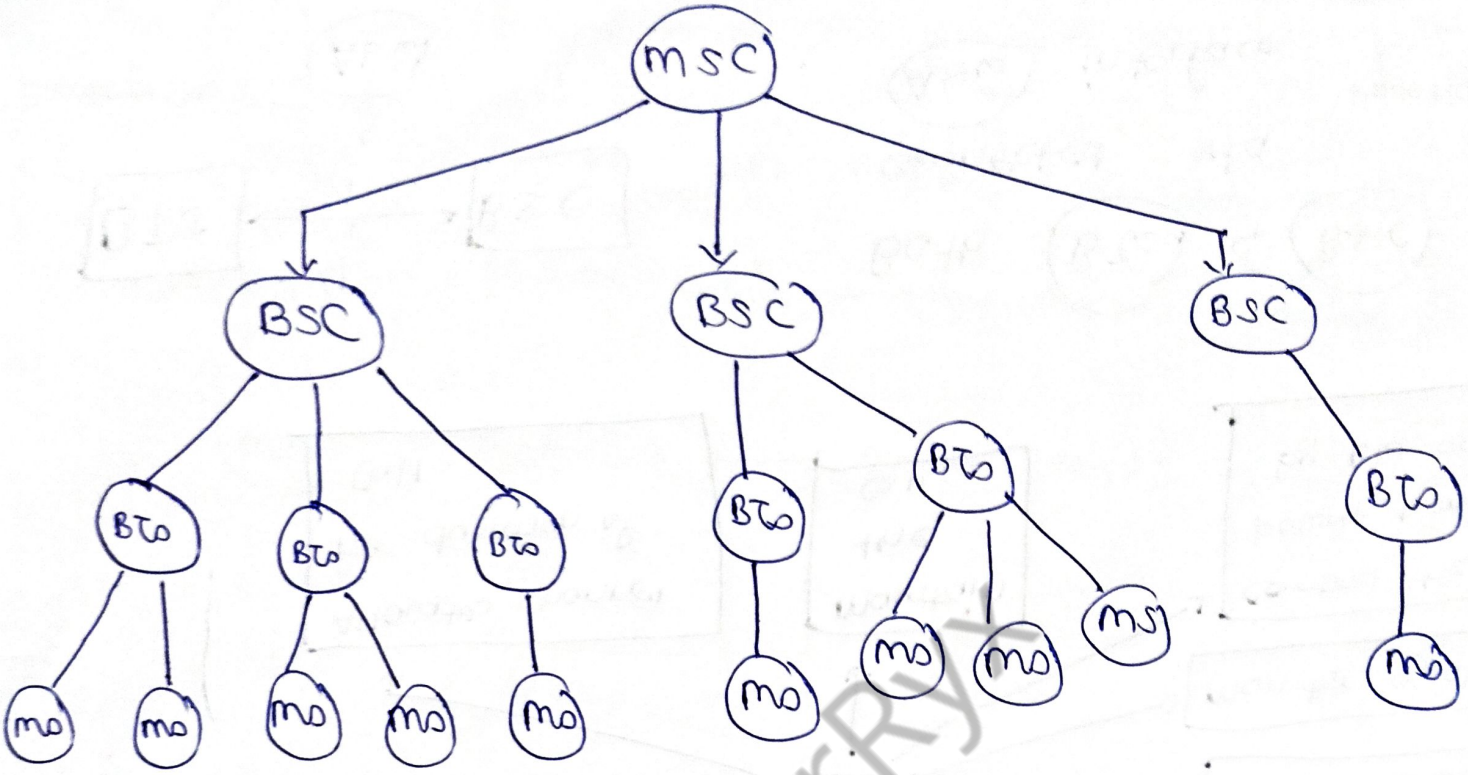
Lets say you call your friend, you need some medium for the call.

That medium is set by BSC

- handle handover
- monitor quality
- Allocates channel for duration of call
- maintain the call
- control the power transmitted by BTs or MS



Both BTs & BSC are connected via Abis interface.



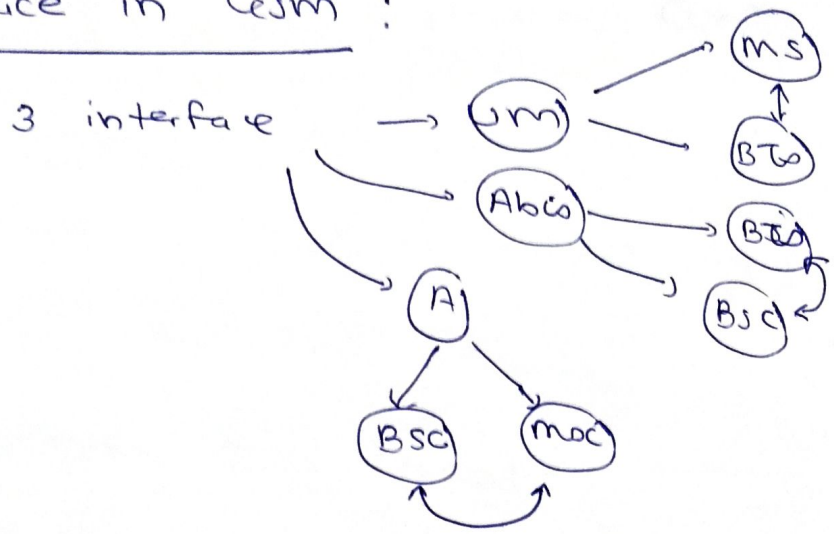
MSC = Root node

BSC's = Children nodes

BTS = Siblings

MS = leaf node.

Interface in GSM :



(1) Um interface :

- betn (MS) & (BTS)
- Uses (TDMA)
- Transmit & recieve info / traffic

(2) ABIS interface :

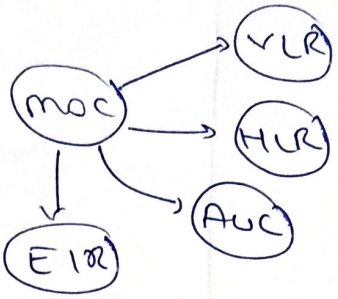
- betn (BTS) & (BSC)
- Transmit Traffic & inform [BSC] & [BTS]
- Uses [Link ACCESS Protocol]

LAP →

(3) A interface :

- between (BSC) & (MSC)
- manages (BSS)
- Call handling
- manages mobility
- Bandwidth max. [2Mbps]

MSC Register



① HLR : Home Location Register

↳ stores permanent data about subscriber (profile, location, status)

↳ stores subscription info of registered user is stored

SIM info goes to HLR

② VLR : Visitor Location Register

↳ Stores temporary data about subscriber

↳ Integrated with MSC

↳ works in co-ordination with HLR

me = Gujarat

me move to Assam

ASSAM HLR = no info of me

so ASSAM HLR contact GUJARAT HLR

Info transmission

then I get service in Assam.

Annexure No :

(3) AuC => Authentication Center.

↳ Protected Database

↳ Stores a copy of secret key

↳ Used for authentication

↳ protection from fraud.

(4) EIR => Equipment Identity Register.

↳ A type of database

⇓

Contains a list of all mobile on network.

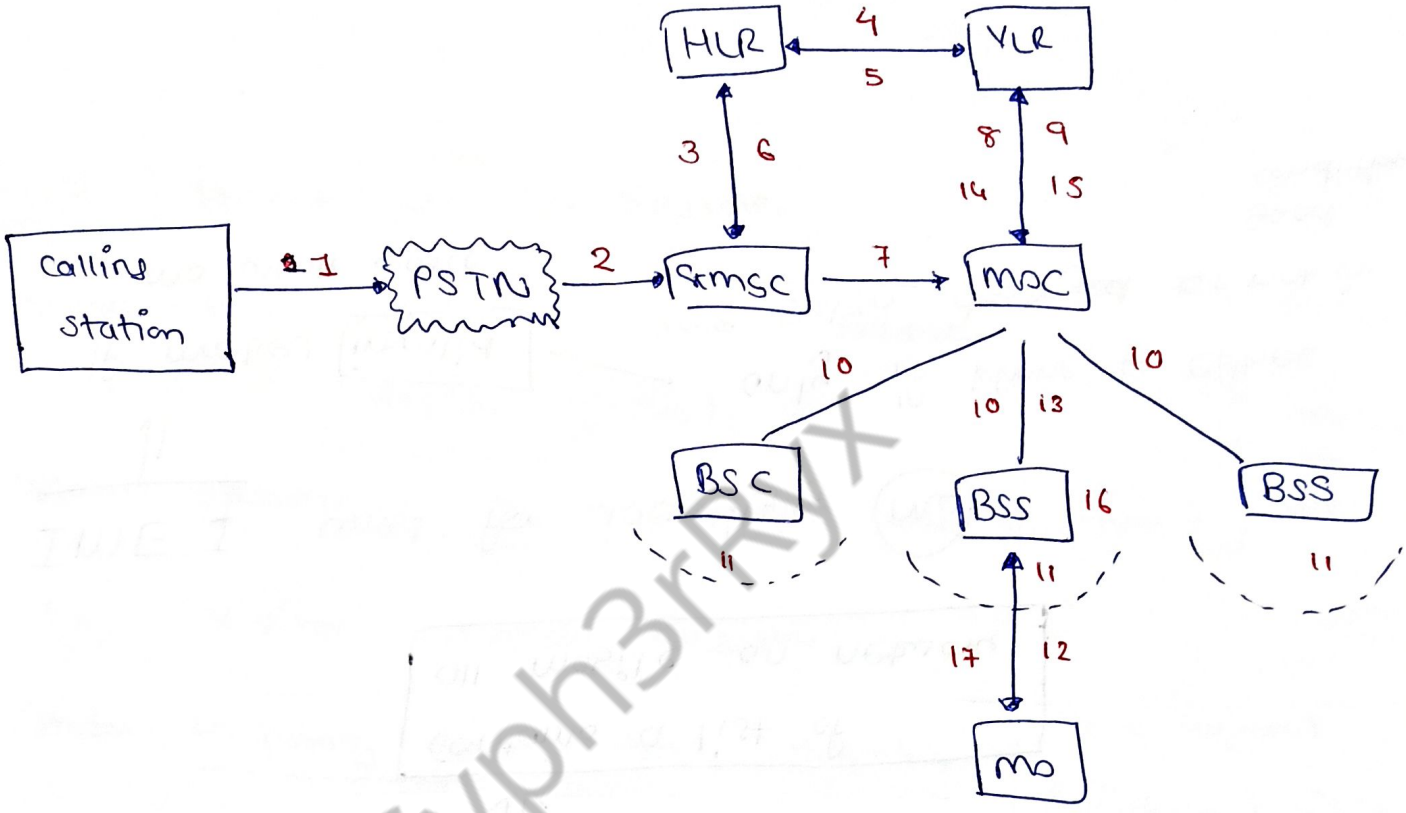
↳ IMEI used for identifying (no)

⇓

if marked invalid → only if phone is either stolen, destroyed or not in good condition.

no work work.

Call routing in GSM : (MTC)



1 ⇒ Calling a GSM subscriber.

2 ⇒ forward a call to GMSC

3 ⇒ signal call setup to HLR

4, 5 ⇒ Request VLR

6 ⇒ forward MSC to GMSC

Annexure No :

7 => forward call to current MSC

8, 9 => get current status of MSC

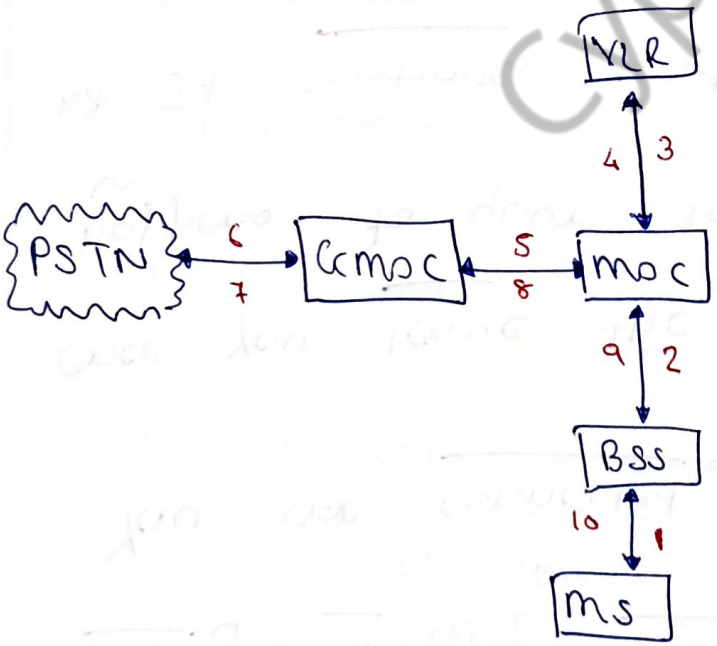
10, 11 => Paging of MS

12, 13 => MS Answer

14, 15 => security checks.

16, 17 => connexn setup.

Call from mobile: (MOC)



1, 2 : Connexn request

3, 4 : security check

5, 8 : resource check (if ckt is free or not)

9, 10 : call setup

Handover:

Suppose you are in a car and you are talking w/ your friend on mobile phone.

You are connected to Base Station - (1)

Once you leave the radius of BS-(1), what happens to your call?

- It continues and find the Base Station - (2) which is nearest to your location and it will directly connect you with that BS and call continues.

Whole above process is called "Handover".

Annexure No :

How it happens ?

MS & BTS provide info for handover

↓

weak link & quality check

Measurement info —send→ every 0.5 second

↳ contain quality of current link & quality of certain channel in neighbouring cell

Once MS moves away from BTS (old) to new BTS (closer)

Handover decision don't depend on actual value of recieved signal

but on average value

BSC collect values of [bit error rate, signal level] from BTS & MS

(i) MS —send→ measurement report ⟶ BTS(old)

(ii) BTS(old) —send→ measurement result ⟶ BSC(old)

IF HO is required then.,

(iii) BSC(old) —send→ MSC

(iv) MSC —request→ For HO ⟶ BSC new

(v) BSC(new) will allocate resources

(vi) BSC(new) —send→ Channel activation —request→ BTS(new)

(vii) BTS(new) —send→ Acknowledgement ⟶ BSC(new)

(viii) BSC(new) —HO Request / Ack→ MSC

(ix) MSC —HO Command→ BSC(old)

(x) BSC(old) —HO Command→ BTS(old)

(xi) BTS(old) —HO Command→ MS(old)

(xii) HO Access from old MS ⟶ new BTS

Link established & HO complete w/ clear commands

Annexure No :

GSM Address & Identifier :

1. Mobile Station International ISDN number :

- MSISDN
  - has country code
  - national dest. code
  - subscriber no.

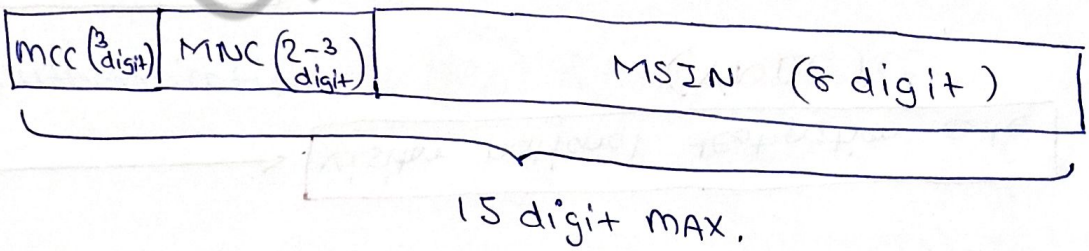
GSM user main part PHONE NO.

2. International Mobile Subscriber Identity

- IMSI
  - mobile country code
  - mobile network code
  - MSIN

Used for internal unique identification of a subscriber.

Sim card



3. Temporary Mobile Subscriber Identity

- TMSI
  - selected by current VLR
  - valid temporarily with VLR area
  - VLR change TMSI periodically

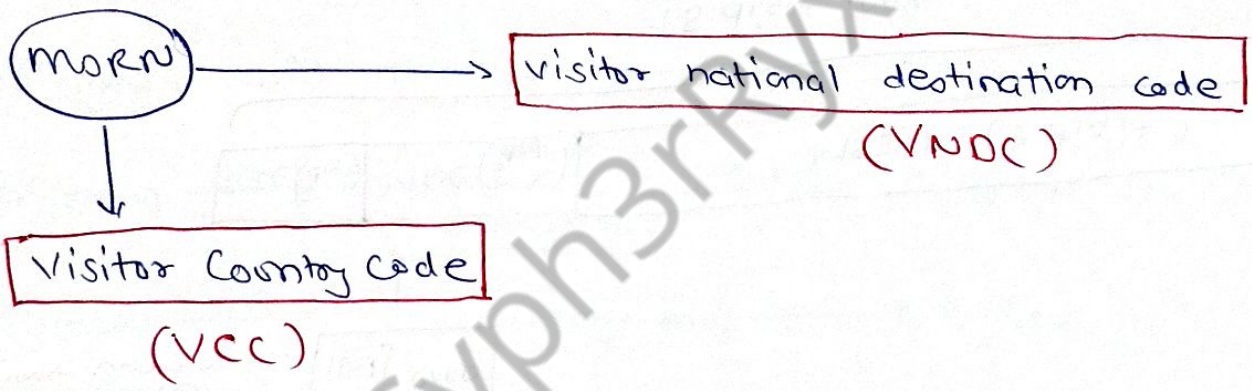
To hide IMSI, GSM uses (4) byte TMSI

4. Mobile Station Roaming Number (MSRN):

VLR generates MSRN on request from MSC

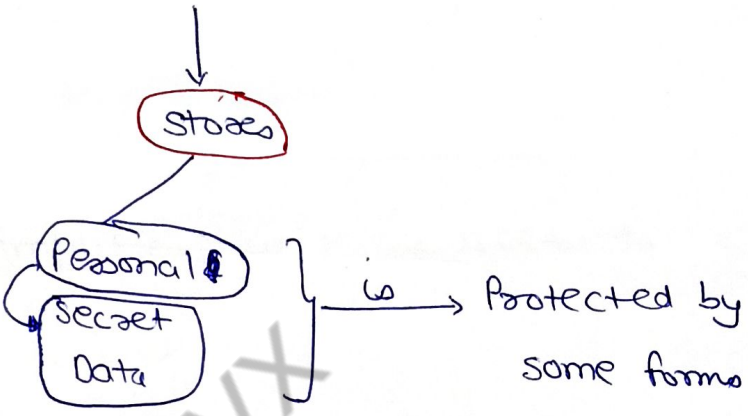
Address stored in HLR

Temporary address hides [identity & location] of a subscriber.



Gsm security :

↳ offer security using confidential information stored in AuC and SIM



Forms of security :

① Confidentiality :

↳ All user data = encrypted

↳ After authentication BTS & MSC APPLY encryption To Voice, data

② Authentication :

↳ Before a subscriber uses any service he/she must be authenticated

Based on SIm which stores

Ki = individual key

IMSI = user identifi.

Algorithm

③ Anonymity :

↳ All data must be encrypted before transmission

Algorithm

A3 ⟶ Authentication

A5 ⟶ Encryption

A8 ⟶ Generate Cipher keys

Annexure No :

GPRS → General Packet Radio Service

- New version of GSM
- GPRS deals with both data & voice

It greatly improves & simplifies wireless access to packet data networks.

GPRS → applies → Packet radio Principals → TO → TRANSFER

TRANSFER → USER DATA PACKETS → between → External Network & MS

Benefits :

1. New Data Service
2. High speed Data
3. Constant Connectivity
4. Ckt switching & Packet switching can be used parallely.

Packet Mode Transfer :

Exhibits Traffic Patterns as,

(i) frequent transmission of small volumes

(ii) Provides the selection of QoS parameter for service requesters

(iii) Also allow for [broadcast, multicast & unicast]

(iv) Network provider should be charging money on volume and not on connection time like in GSM.

GPRS QoS :

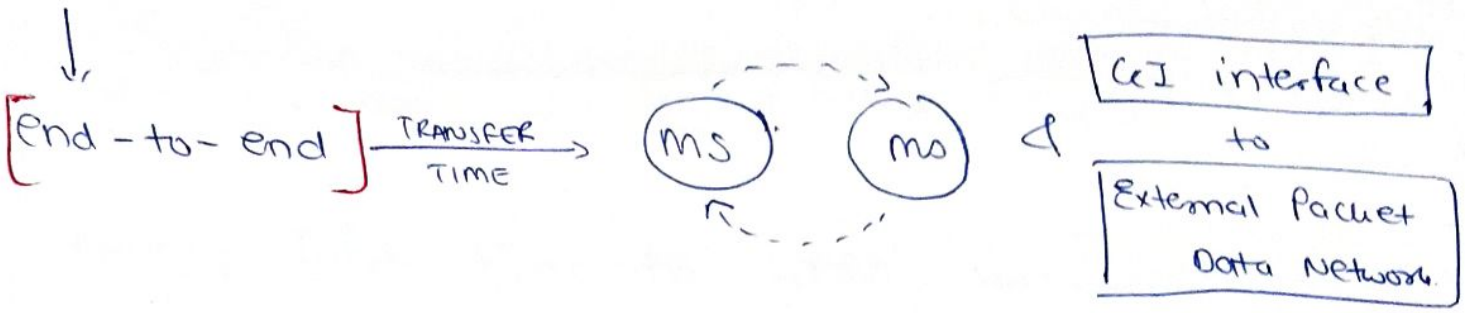
Parameter : Reliability

Classes defined → guarantees → max. value for

- Probability of loss
- Duplication
- missequencing
- Corruption of packets

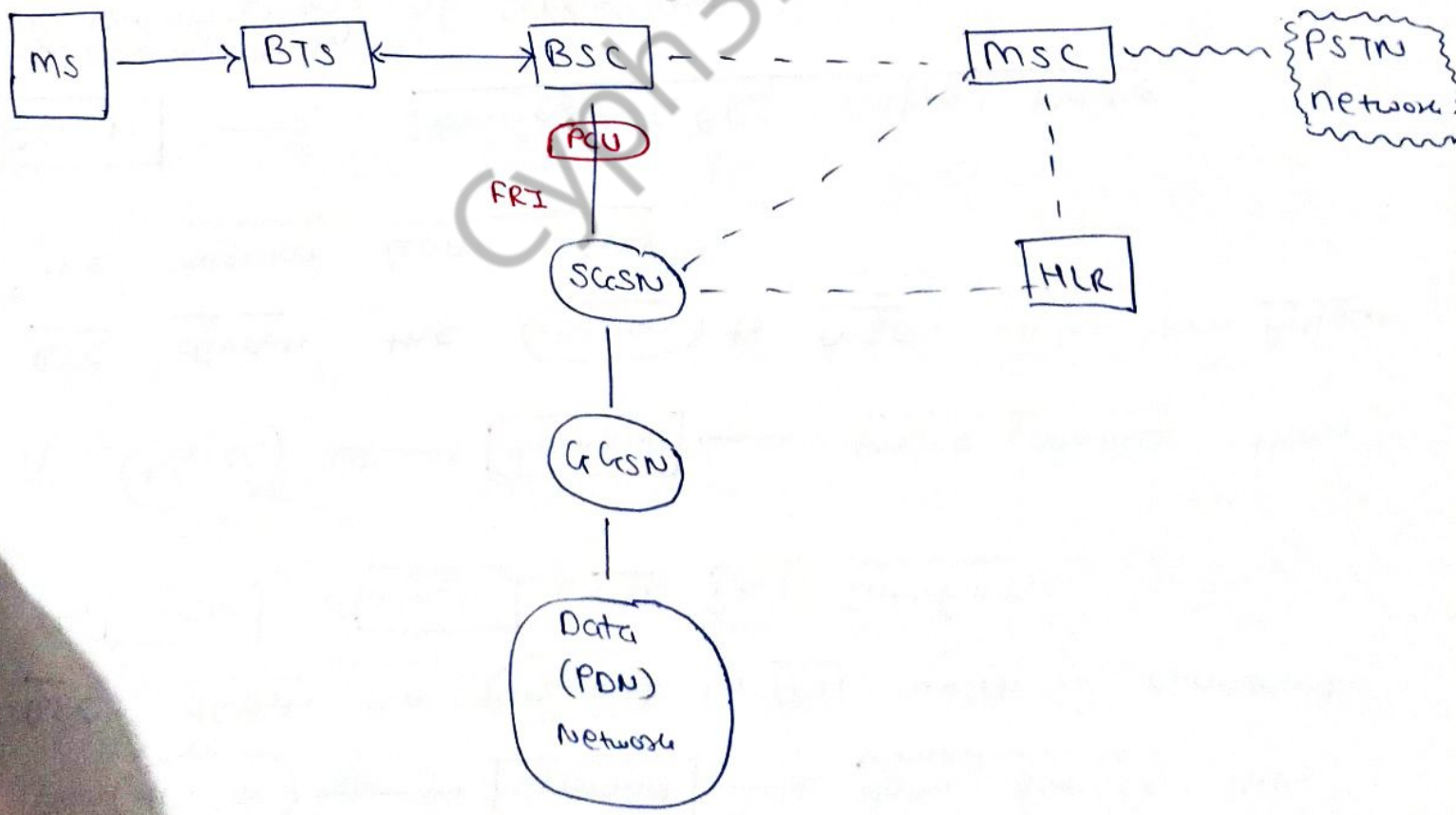
Annexure No :

Delay



Throughput :

GPRS Architecture :



Enrollment No :

Page No :

PCU → Packet Control Unit

↳ if device → demand → data services then BSC diverts the request to PCU which is connected to SGSN & GGSN via FRI interface.

↳ if device → demand → voice services then BSC diverts the request to MSC which then follow the regular com flow.

SGSN → Serving GPRS Support Node

↳ Authentication of GPRS user

↳ Data Compression

↳ Registration of mobile in network

↳ keep track of individuals Location.

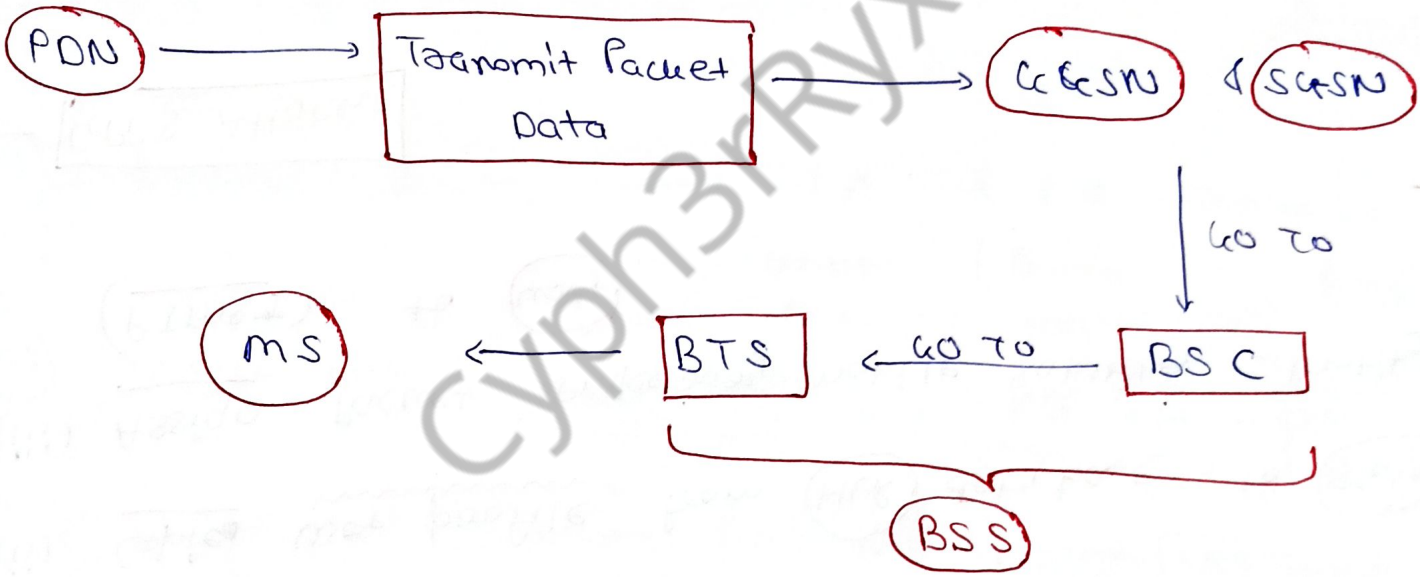
↳ keep track of billing information.

GGSN → Gateway GPRS Support Node

↳ mediator between PDN and SGSN

- routing information for GPRS users
- perform address conversion
- Data Tunneling via Encapsulation

Working :



GPRS Operations

1. Attachment & Detachment
2. Mobility management
3. Routing
4. Communication with IP network.

(1) GPRS Attachment & Detachment operations:

Before a (MS) uses (GPRS) service,

MS must register with (SGSN) of GPRS network.

Network,

(i) Check Authorization of user

(ii) Copies user profile from (HLR) data base to (SGSN)

(iii) Assign Packet Temporary mobile Subscriber Identity (PTMSI) to (user)

GPRS Attach

GPRS Detach also works in similar way & it is used for disconnecting from network.

(2) Mobility Management :

↳ main task → To → keep track → user location

↳ MS send location update to SGSN

so that network can be aware of current location of MS

↳ (3) States exist & diff. strategies applied

LOCATION UPDATE

MS crosses border → LA (Location Access) & RA (Routing Area) should be done.

MS moves within same LA but diff. RA → RA Update

" " " same LA & RA → Cell update

Packet sent to MS = Paging required

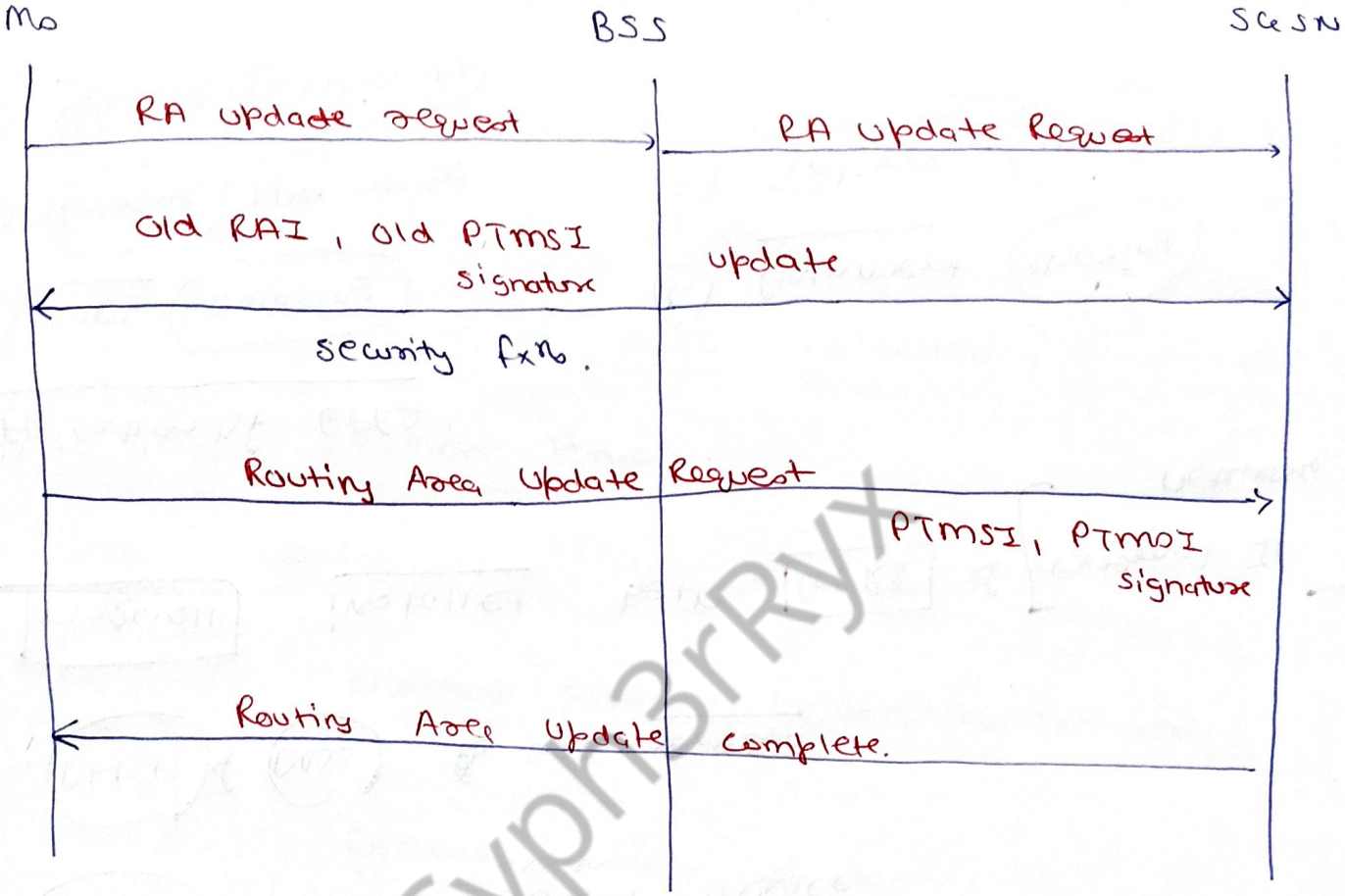
↳ to find accurate location.

- Uplink wasted for paging response
- Downlink requires paging for delay

RA Update :

- MS moves to new RA → sends → Routing Area Update Request (RAU)
  - Routing Area Update Request (RAU) → including → Routing Area Identity (RAI)
    - Routing Area Identity (RAI) → To → Old RA
- Request recieved at BSS
  - it adds Cell identifier (CI) to new cell
- Based on RAI & CI data → SGSN give new RAI
- Also SGSN assigns a new PTMSI to user.

3. Routing



Inter SGSN Routing :

MS moved to an RA ⟶ Diff. SGSN

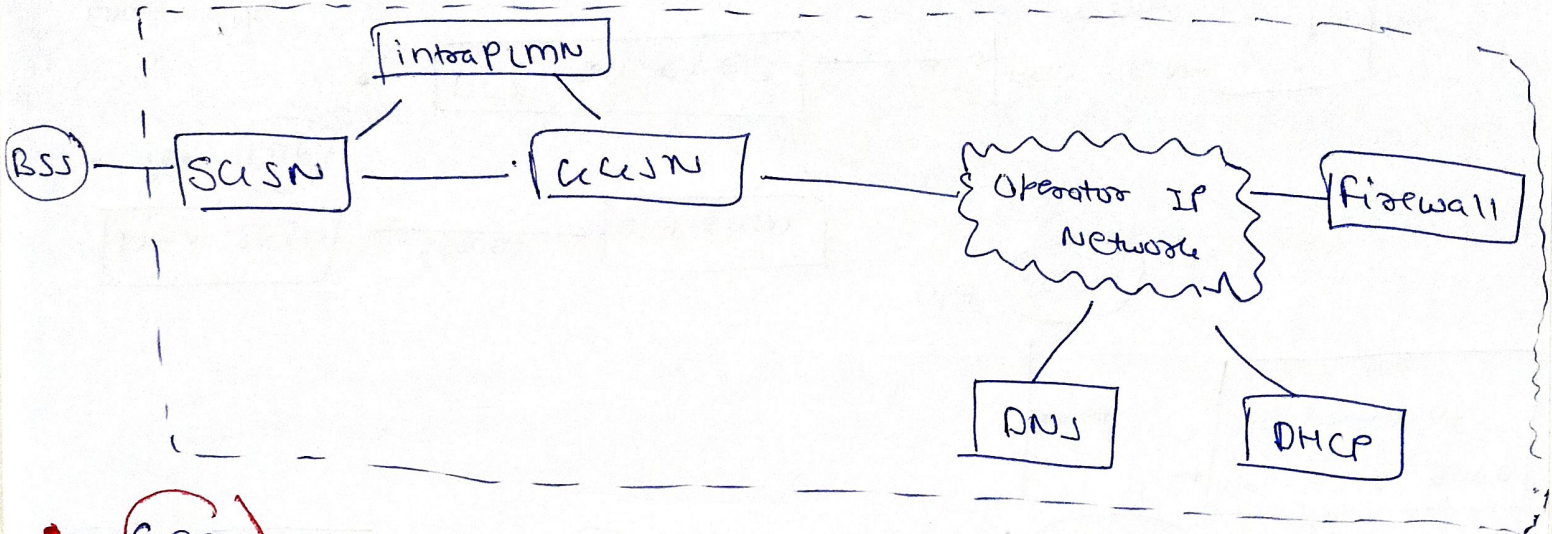
- contacts → old SGSN
- new SGSN have no profile of MS

New SGSN ⟶ Request ⟶ old SGSN

↳ for PDP

- PDP recieved ⟶ new SGSN inform GGSN & network

(4) Communication with IP networks



- GPRS inter connected w/ internet network.
- GGSN is a router device
- DHCP & DNS are servers.
- Firewall installed betn GPRS & [external IP network.]

Application of GPRS:

(1) Web browsing
(2) Remote LAN access
(3) Vehicle positioning
(4) Document sharing
(5) Internet email

Billing & charging in GPRS

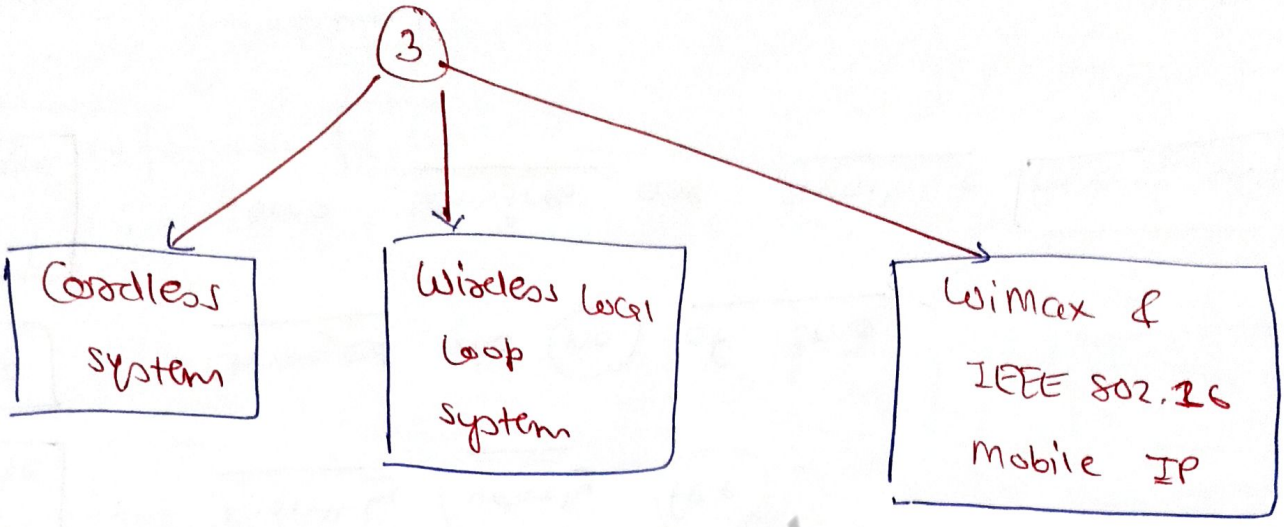
GGSN & SGSN collect billing info in CDR

CDR → Charging Data Records.

FACTORS:

1. Volume : Amount of data uploaded / downloaded.
2. Duration : session length
3. Time : which time data was used
4. Final Destination : charged according to location network
5. Location : Current position of MS
6. QoS : Charged according to service quality
7. Flat rate : monthly / yearly fee
8. SMS : Charged via no. of SMS
9. Free of charge : Some services are available free of cost

Wireless operation & Standards:



Cordless System:

(1) Residential : A single (BS) provide in house voice & Data support

(2) Office : small office => single (BS)
large office => multiple (BS)

(3) Telepoint : A (BS) for public place
eg. Airport, Railway, etc.

- Frequency limited
- Inexpensive Handset
- low power design

Wireless Local Loop (WLL):

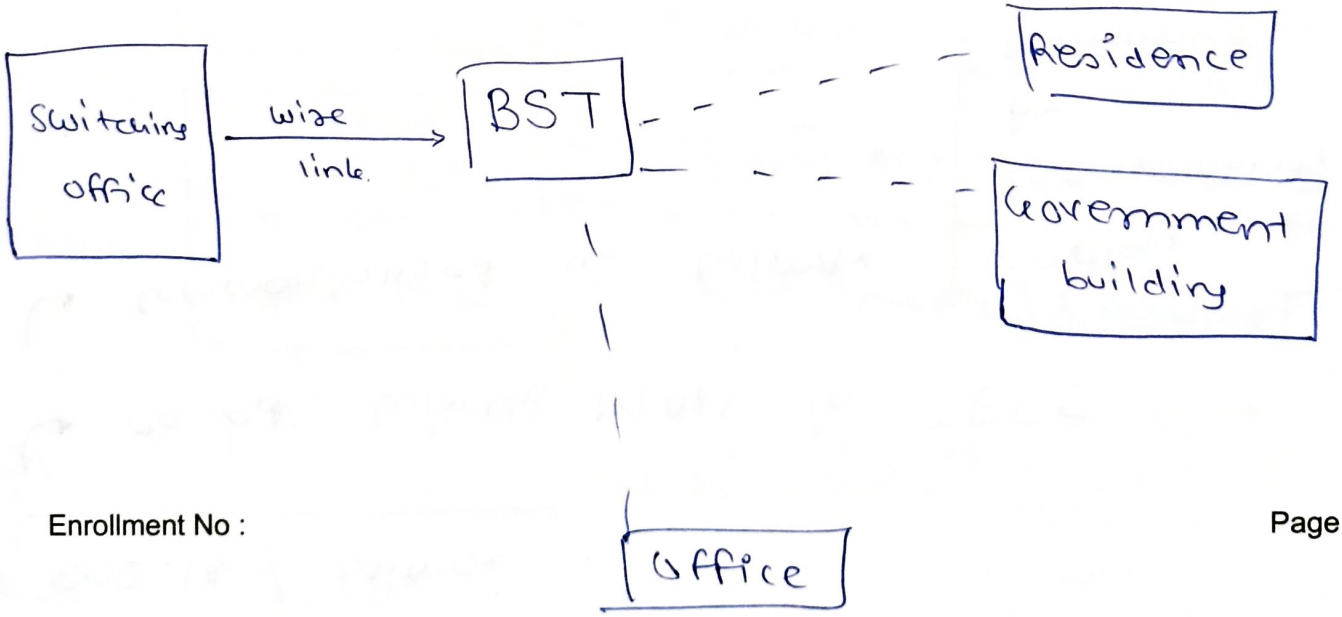
Use of wireless communication link as [last mile / first mile] (link) to deliver [POTS (Plain Old Telephone service)]

or to deliver [Internet Access] to customers.

wired tech need reliable, high speed access by [residential, buisness & government]

Es. ISDN, Cable modems

Wireless local loop : • replace existing telephone service
• give high speed 2-way [voice & data]



802.16 / Wimax

↳ called Wireless MAN in IEEE

↳ commercialized as WiMAX [Wireless Interoperability for Microwave Access]

↳ Develops "system profiles" which define [mandatory & optional] features of standard.

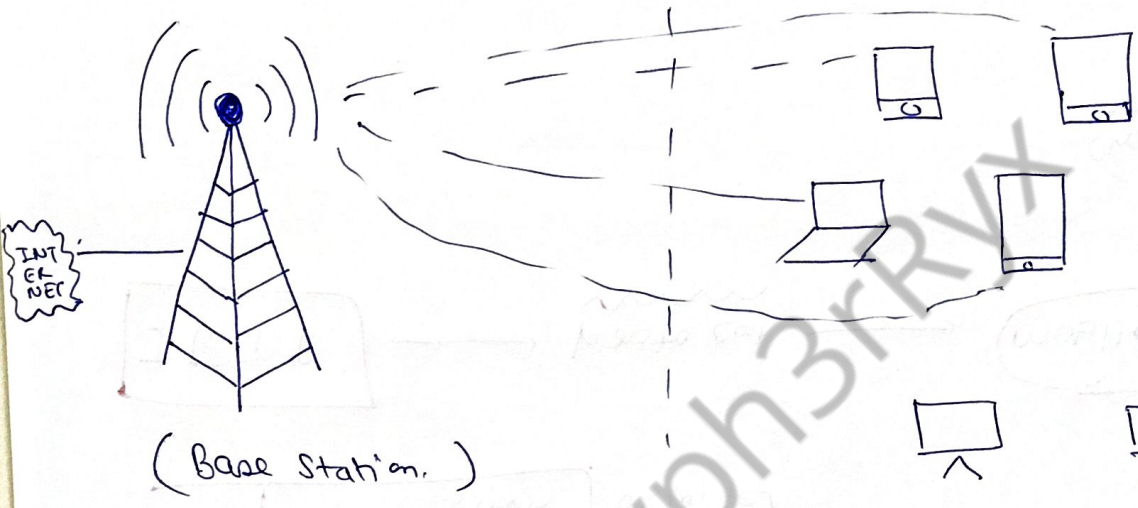
Annexure No :

802.16 Standards Development

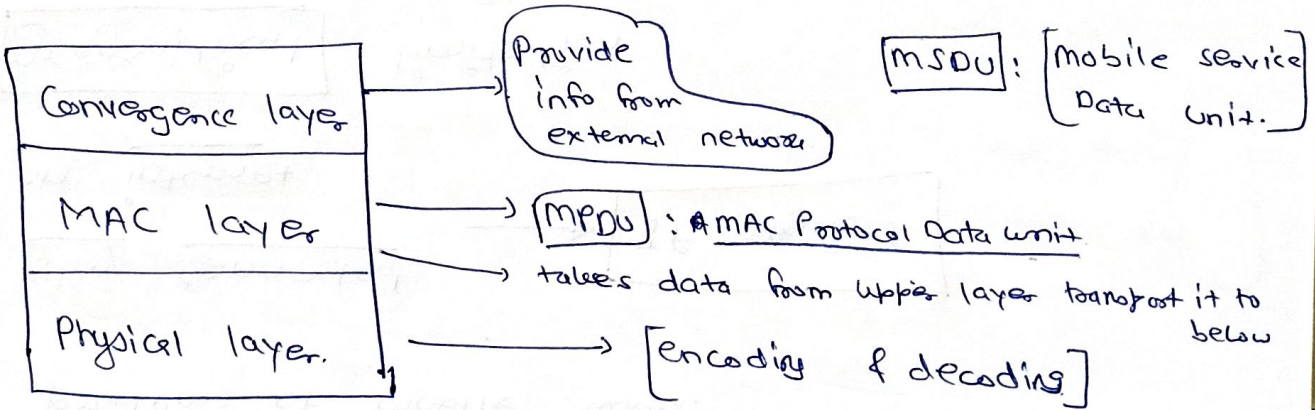
- Data rate : 70mbps
- Provide high speed over WAN
- Point to Point
- multiple Physical layer & MAC option

Services

- IP
- Bridged LAN
- Voice transport
- Data transport



Layers :



Enrollment No :

Page No :

Mobile IP :

↳ Developed as a means for transparency dealings with problems of mobile users.

To stay connected on internet → IP required

- No geographical limitation
- Support security
- No modification required

IETF → protocol → mobile device

↓

Change position in network

↓

without changing IP

Requirements:

① Compatability:

- Support same 2 layer protocal as IP
- no change in current system & router required.
- MS can communicate w/ fixed system.

② Security:

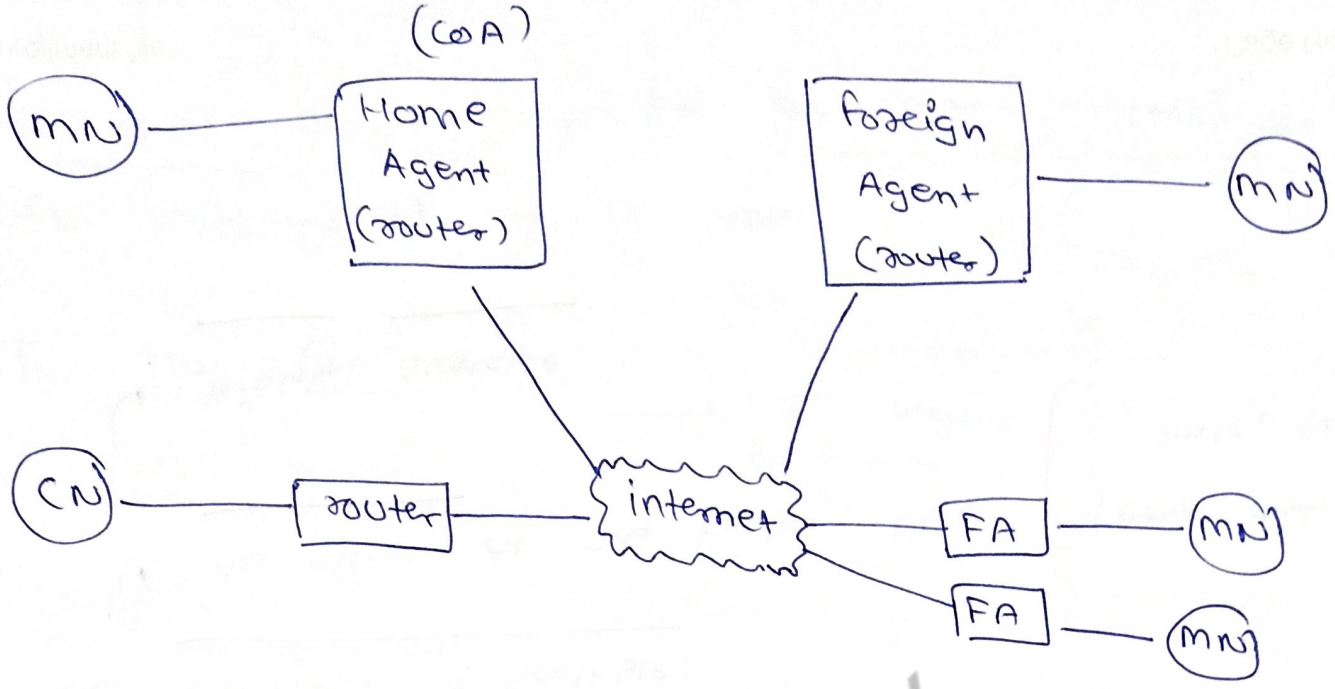
- Authentication of all registration message is necessary.

③ Transparency:

- only MS keep, IP address & share them
- continuity in communication is maintained.

④ Efficient & Scalable:

- no effect at any factor like [speed, data, rate, etc.]
- highly scalable.



MN = Mobile Node

HA = House Agent

FA = Foreign Agent

CN = Correspondant Node.

(i) MN : End Use device using mobile IP [can change their point of connxn without changing IP]

(ii) CN : Other node for communication.

(iii) HA : House Agent → home router

(iv) FA : Foreign Agent → foreign router.

(v) CoA : Care of Address

- Defines current location of IP.
- Position changes → Packets to CoA & not to MN

Working :

Registration | Discovery | Tunnelling

(I) Agent Discovery :

↳ Used when mobile Node (isn't) in Home network.

thus we need to find foreign agent.

2 methods.

① Agent Advertisement

↳ (FA) & (HA) advertise their presence via periodic messages

↳ message has info, address.

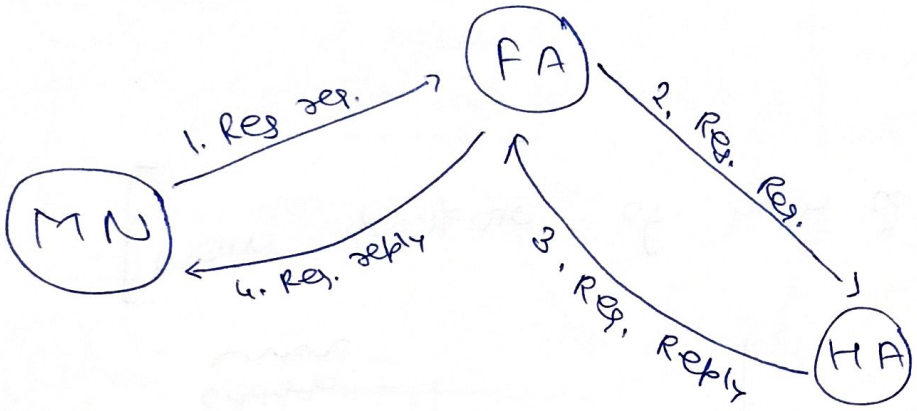
② Agent Solicitation :

↳ Used when (MN) don't get any (CoA)

↳ no flooding of message [1 mess. / second]

[main purpose of both is to find FA.]

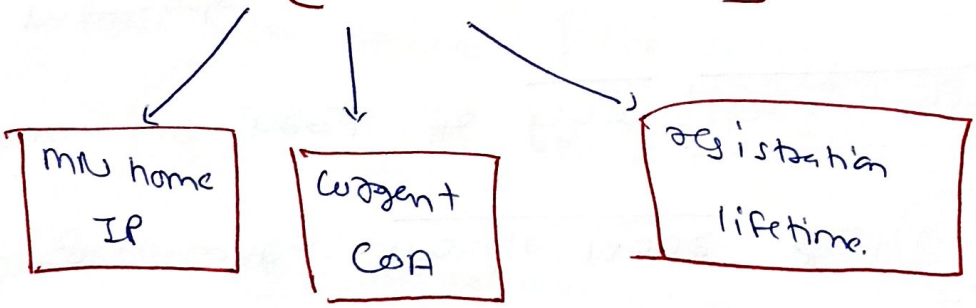
(II) Registration:



↳ MN register w/ HA when CoA is known.

↳ Informs HA about MN current location

- MN send request to FA
- HA setup [mobile binding]



(III) Tunneling & Encapsulation :

↳ Virtual pipe is established for data packets

betn [HA (start)] & [FA (end)]

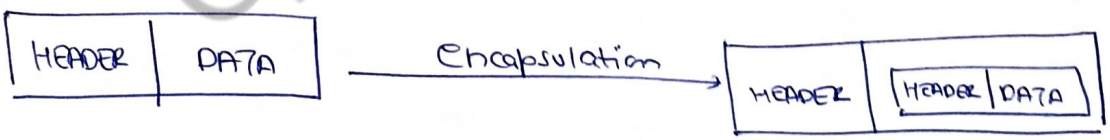
Sending Packet via [Tunnel] &

Acheived via [Encapsulation]

⇓

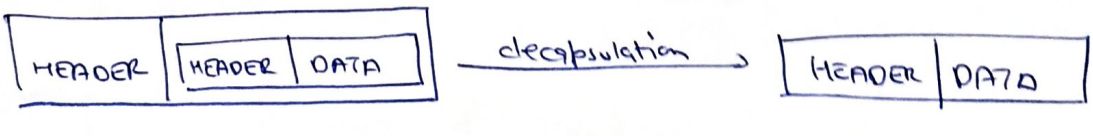
(Wrapping) current [packet data] + [header] into another packet.

Original PACKET :



(Encapsulation)

Decapsulation



CH:4 Wireless LAN → WIFI

Wireless LAN

- wireless transmission
- issues addressed like [high price, licensing, low data rate, etc.]

Requirements :

1. **Area** : 100 – 300 m
2. **No. of nodes** : hundred of node across multiple cell
3. **Power consumption** : low for battery life
4. **Connxn to LAN** : using control module
5. **Security** : Robust & Protected

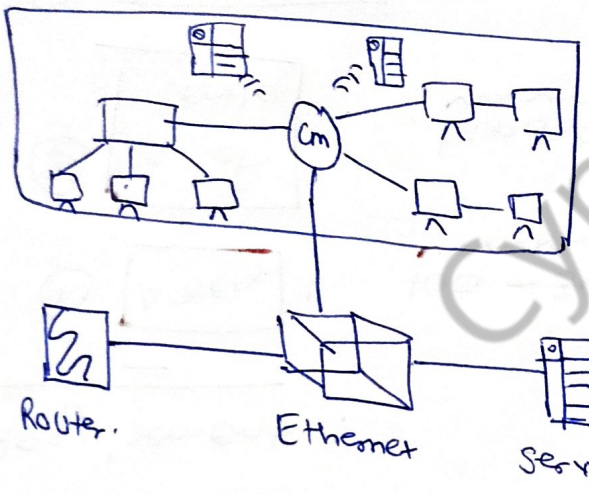
Advantage

- reduce cost
- flexible
- no wires
- more robust

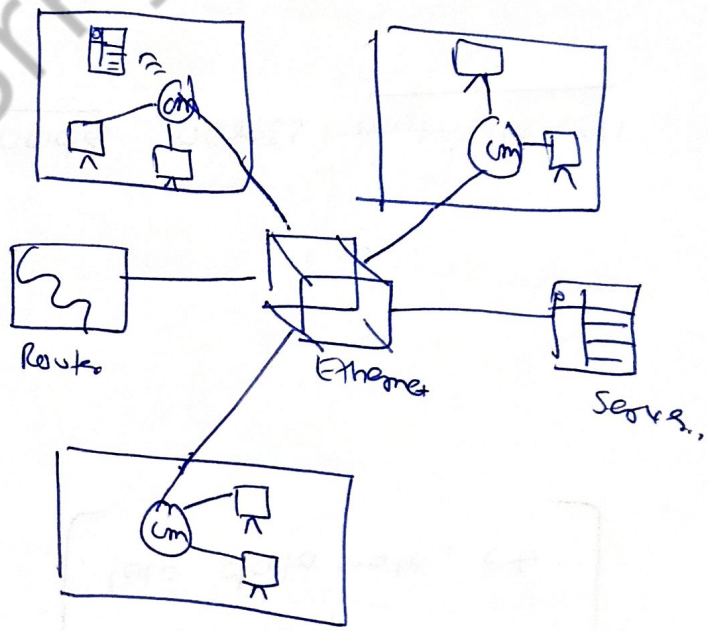
Disadvantage

- less secure
- low bandwidth (10-12 mbps)
- high error

Single cell LAN



Multi cell LAN



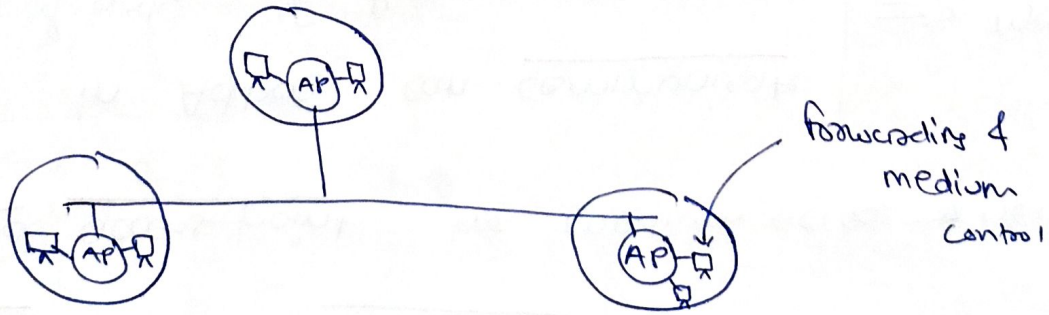
Infrastructure based Network

↳ Provide Access to other network w/ [forwarding fxn, medium access control]

- Comms with only wireless nodes & Access points
- Collison occurs if medium access control is not Coordinated

  but if Access Point control MAC = no collison.
- not used in disaster

Eg. cell phone network
satellite phone network.



Ad hoc network

↳ no need of infrastructure to work.

↳ no access point or medium access necessary

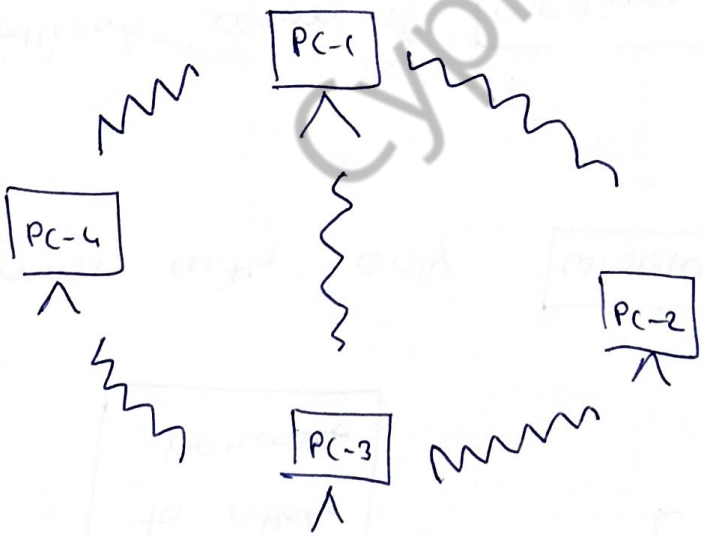
[Nodes in Adhoc can communicate only & only if they are physically reachable] ⇒ most important.

i.e in each other radio range

- Complexity = higher

[each node has medium access mechanism]

eg. needed for unexpected meetings.



AdHoc network

in short: temporary network for comms in wireless form.

IEE 802

↳ It Provides 2 type of Service.

(i) BSS (Basic Service Set)

↳ Station & AP are within same radio coverage.

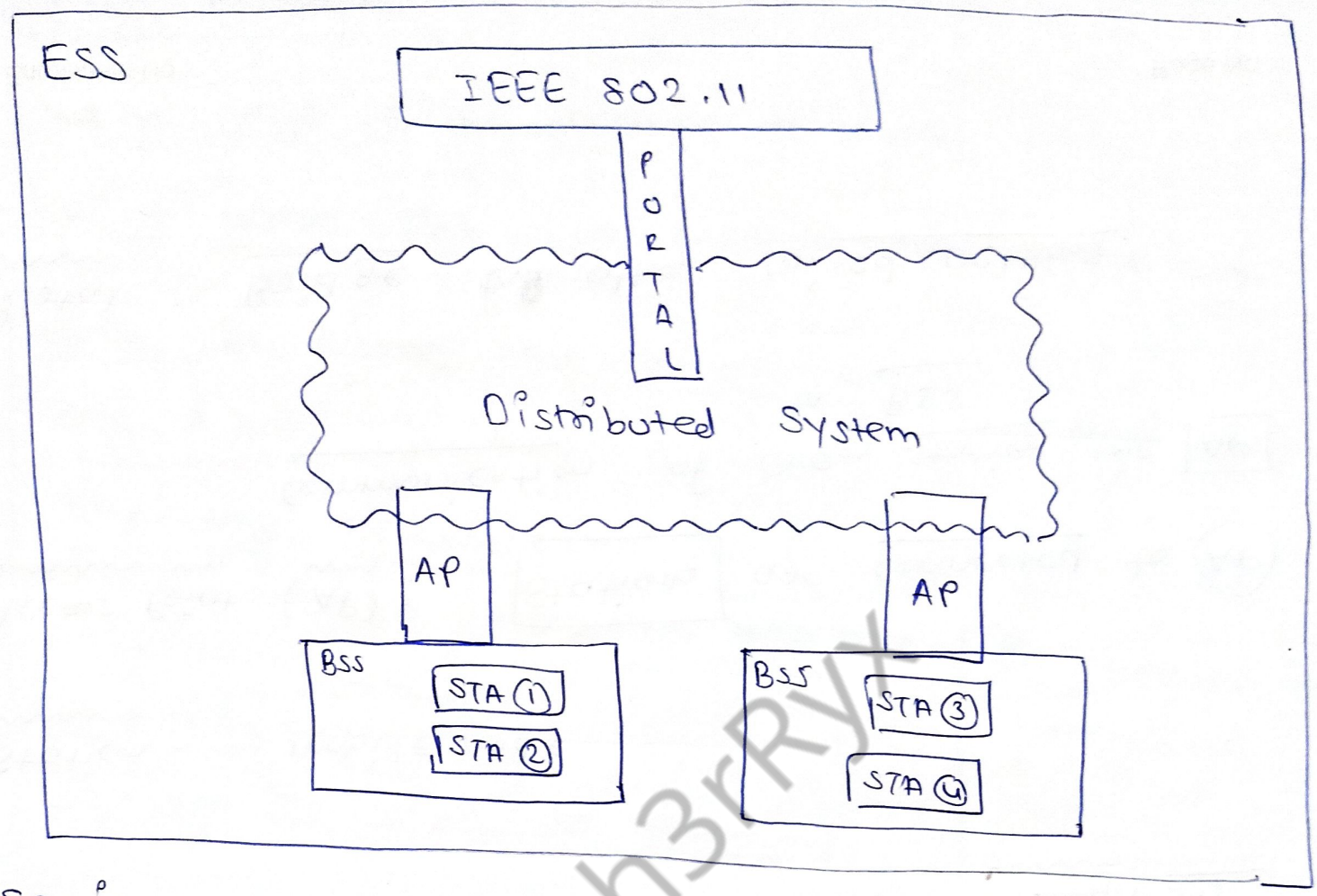
(ii) ESS (Extended Service Set)

↳ Collection of BSS is ESS & we need connect through AP.

Station : mobile node

Access Point (AP) : Stations are connected to (AP). Communication of every station via AP to BSS

Portal : Bridge to other wired network.



· Services :

Defines 9 services by 802.11

↳ equivalent to wired connxn.

AA DDD Im PR

Annexure No :

Service	Provider	Used to support
Association	Distributed System	MSDU Delivery
Authentication	STATION	LAN Access & security
De authentication	STATION	LAN Access & security
Disassociation	Distributed System	MSDU Delivery
Distribution	"	"
Integration	"	"
MSDU Delivery	STATION	MSDU Delivery
Privacy	STATION	LAN Access & security
Reassociation	Distributed System	MSDU Delivery.

Message Distribution

Distribution Service :
- Used by station
- exchange MAC frames.
- if station is in same BSS (DS) goes to single AP of that BSS (refer diagram)

Integration Service : Data Transfer betn [802.11 & 802.x]

Association : establish initial association betn STATION & AP

Disassociation : By STATION or AP

Reassociation : Transfer Association (to) another AP

Medium Access Control : (MAC)

Reliable Data Delievery , Access Control , Security

↓↓

MAC layer data exchang w/ noise & interference

∴ not reliable

↳ Thus it include frames exchange protocol.

↓↓

STATION recieve ACK

if not recieve retransmit.

- 4 frame exchange :

(1) Source issue a RTS frame to destination.
(request to send)

(2) Destination responds with CTS frame
(Clear to send)

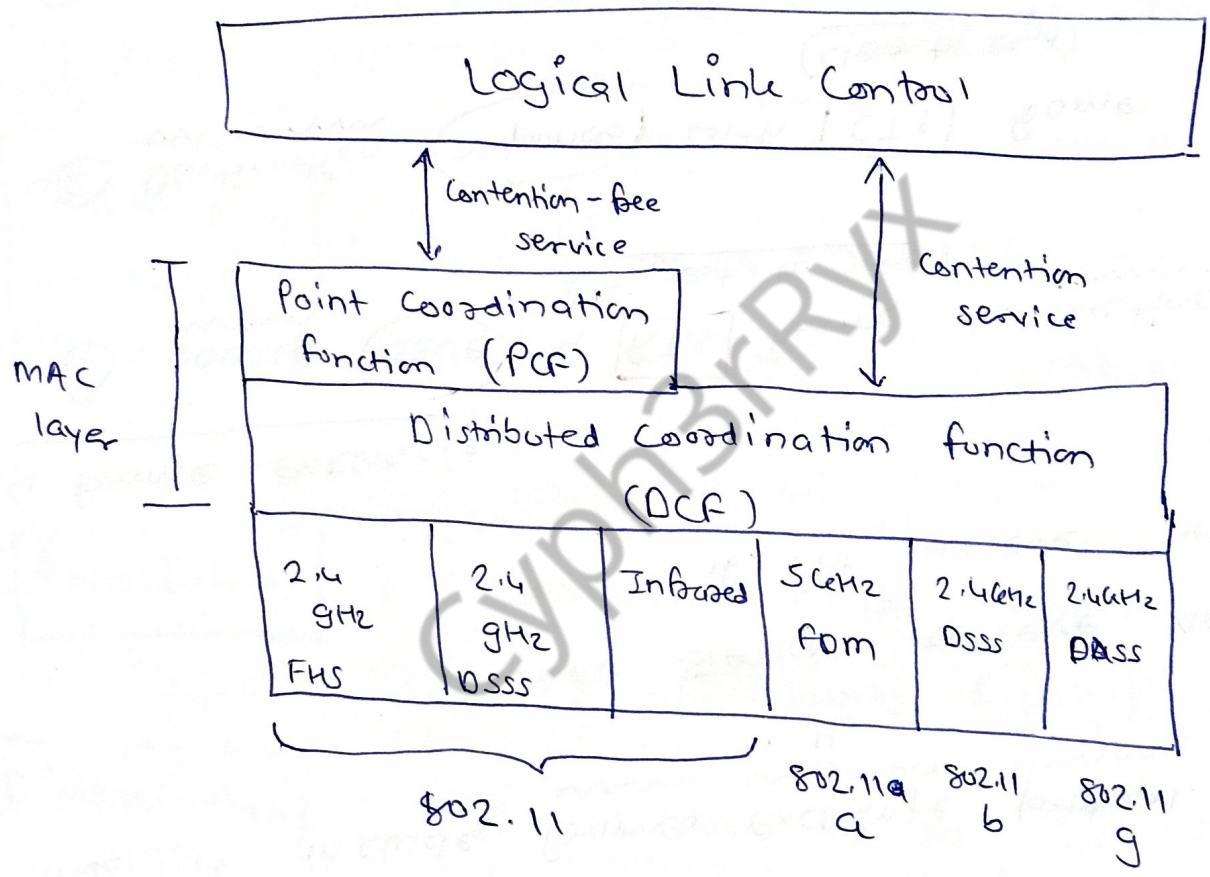
(3) After recieving CTS , source transmit data

(4) Destination reply with ACK

for no collison

RTS alert source
CTS alert destination
] — that data is being transmitted.

MAC Architecture:



* DCF (Distributed Coordination fxn)

if STATION has frame to send
it checks if medium is IDLE to send
if (yes) then it gives permit to it
but if (no) then it waits for transmission to complete.

No collison occurs

* PCF (Point Coordination fxn)

Alternative of DCF

- It (AP) act as coordinator & manages access of device.

Divide time into (2) types

(1) CFP (Contention free period)

(AP) polls each device to determine its transmission needs & grant (permit) to transmit data.

(2) CP (Contention Period)

(Devices) contend for access to the wireless medium using (CSMA/CA) protocol

PCF has Control frames

RTS , CTS , ACK remains same.

PS => Power saving mode ⟶ frame sent to Access point any buffer frame

RTS => Request to send [Ask permission]

CTS => Clear to send [Permission granted]

ACK => successful transmission

CFP => Announce the end of transmission

CF-End + CF-ACK => ACknowledge the end & release the connxn.

DATA frames :

4 ⟶ upper level

DATA ⟶ simple data frame

DATA + CF-ACK ⟶ **Data** & acknowledgement of **Contention free period**

DATA + CF-Poll ⟶ Point coordinator uses it to **deliver data** & request **Send**

DATA + CF-ACK + CF-Poll ⟶ Combine above (all)

Other (4) frames don't carry user data. ⇒ **NULL fxn.**

802.11 a

1. 5 GHz = frequency
2. max. Data = 54 mbps
3. orthogonal frequency Division multiplexing (OFDM)
4. Shorter range
5. few device connxn
6. High Data rate
7. Less interference
8. Not backward compatible

802.11 b

1. 2.4 GHz = frequency
2. max. Data = 11 mbps
3. Direct sequence spread Spectrum (DSSS)
5. Longer range
6. More device connxn
6. Low data rate
7. High interference
8. Is backward compatible

Authentication

↳ establish station identity

- Wireless LAN require one more [stage of authentication].

schemes = handshaking
public key encryption.

De Authentication

↳ involve existing authentication once credential expires.

- Prevent unauthorized access to transmission.
- Better Privacy & High security.

CH: 5 Bluetooth (IEEE 802.15)

Short range wireless comms technology

Simple, secure & everywhere

- Advantage
  - less power consumption
  - Cheap
  - less complicated

V1 → 1999

V1.1 → 2002

V1.2 → 2003 [1 Mbps]

V2 → 2004 [3 Mbps]

V3 (High speed) → 24 Mbps [2009]

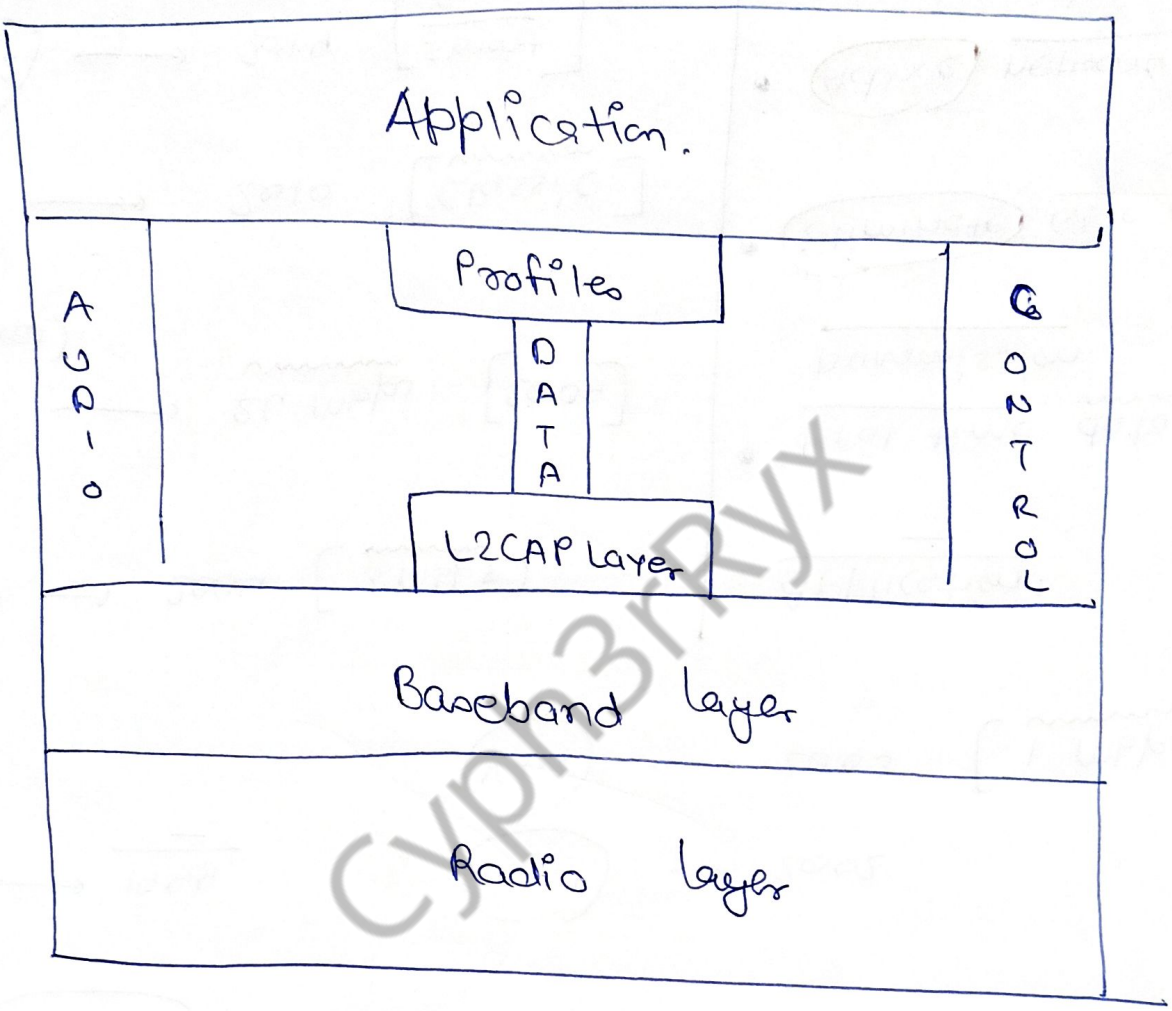
V4 → 2010 [Classic]

V4.2 → 2014 [Smart, fast, IoT]

Application:

- Real time data & voice transmission
- Eliminate Cable work
- Adhoc networking

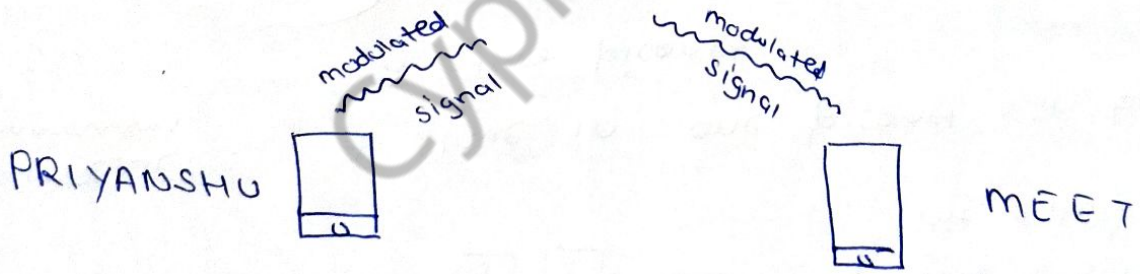
Bluetooth layers:



(1) Physical Radio (RF) layer: (Connxⁿ less layer)

- Performs modulation & demodulation of data into RF signal (Radio frequency signal)
- Data to radio signal.
- Bluetooth (act) as Transreciever.

eg. Priyanshu wants to send song to Meet via Bluetooth



Here Priyanshu's mobile converted the song into signal = modulation

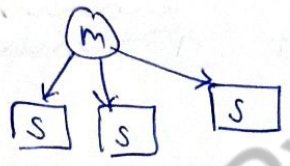
Meet's mobile Capture that signal & convert it into song = demodulation

(2) Baseband link layer:

It establish the connxn in the piconet

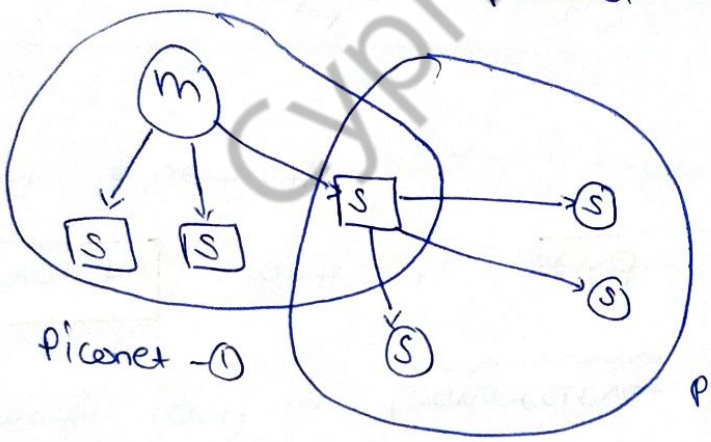
2 type of Bluetooth network:

(i) PICONET: One master - diff. slaves (8 connxn max)



one way only
(master can only send the data)

(ii) SCATTERNET: A slave in one piconet can be master in other piconet



Piconet - ①

Piconet - ②.

NOTE:
- Slaves can not communicate w/ each other

(3) LINK MANAGER:

↳ Performs management of already established links.

↳ Translates commands into operations & manage them.

What else it do?

(i) Attach Slaves to Piconet
(ii) Detach Slaves to Piconet
(iii) Configure branches
(iv) Controlling test mode
(v) Power consumption control
(vi) Establish ACL (Data) & SCO (voice) link

A Link manager is the one that communi-cate with other Link manager of diff. Bluetooth device

via

Link Manager Protocol (LMP)

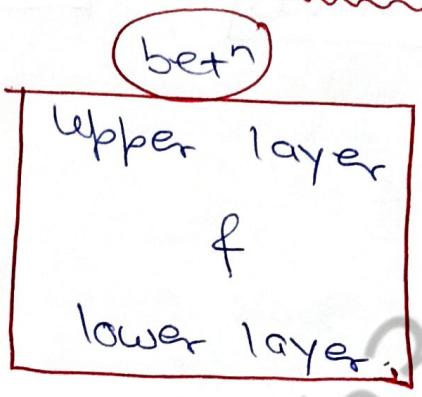
messages as LMP PDU (Protocol Data Unit)

Enable link manager → To → maintain the connxn

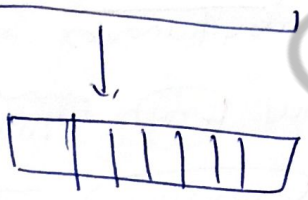
(4) Logical Link Control Adaptation Protocol :

↳ (Heart) of Bluetooth layers (Protocol stack)

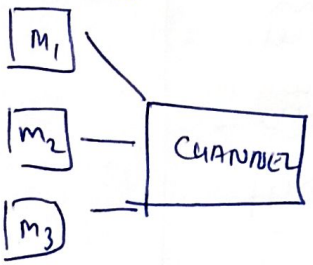
↳ Allows proper communication



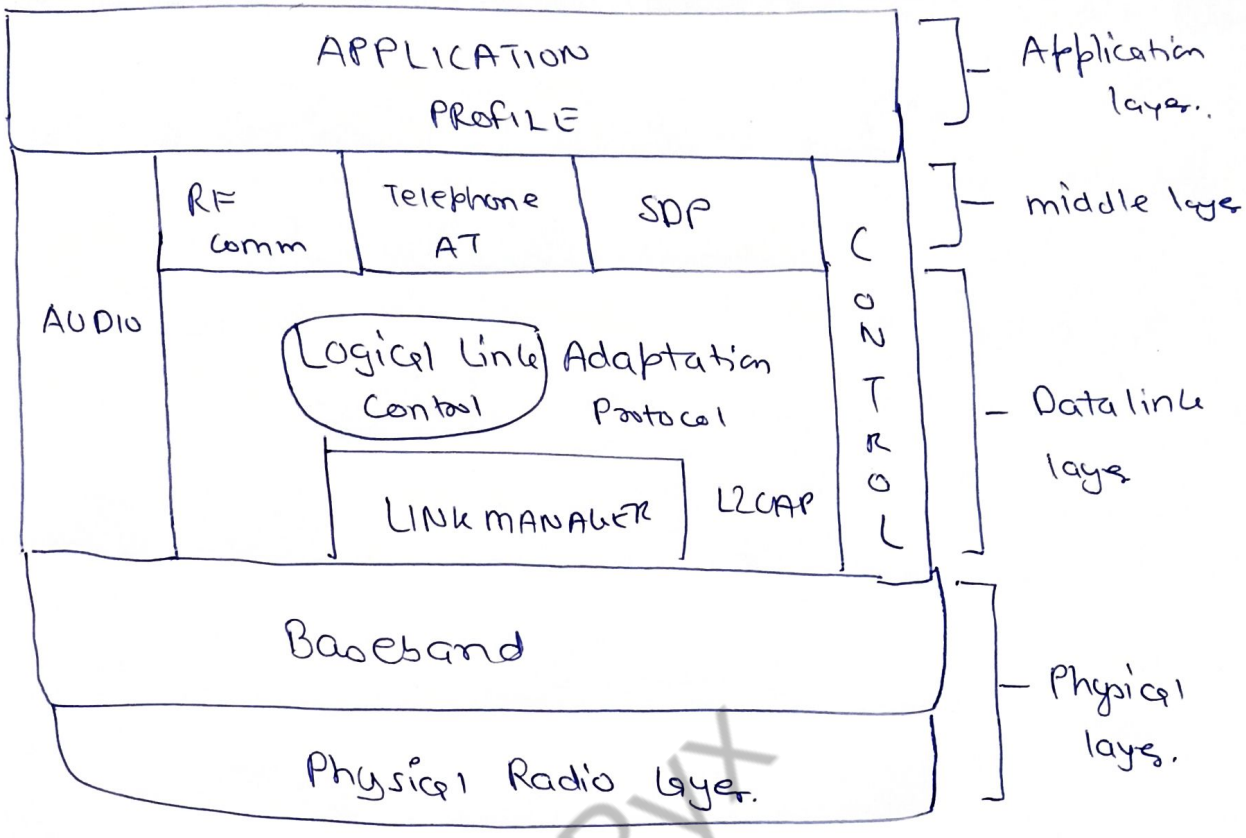
↳ segmentation & multiplexing is done here.



Huge data into small packets



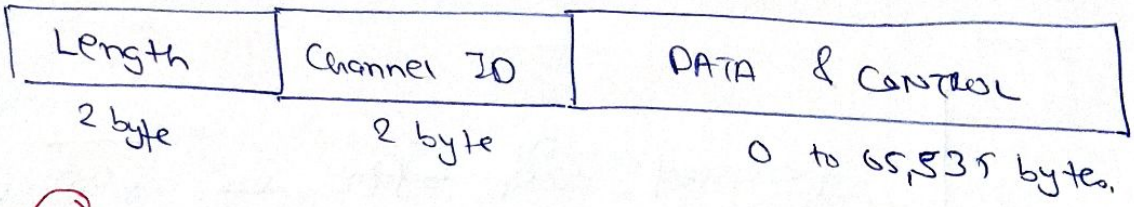
multiple message in single channel.



fxns of L2CAP:

1. multiplexing higher layer protocol
2. segmentation & reassembly
3. Group management
4. QoS for upper layer protocol

L2CAP Data format :



↳ (16) bit length field defines the size of data in bytes coming from upper layer.

↳ Channel ID => unique identifier for virtual channel