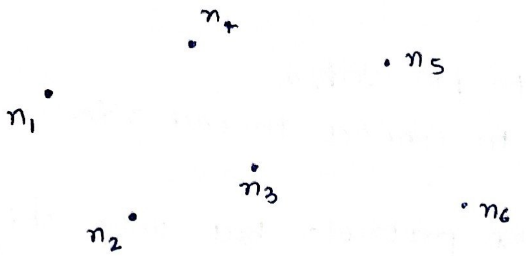
17th March (ppt also).

Ad-hoc network

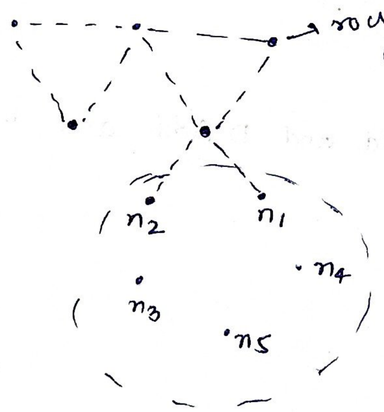
① MANET (Mobile Ad hoc network)



→ nodes and router both present
→ mobile nodes - constant speed
- stop for some time (pause time)
- move in random direction

→ any node can work as host or a router

Mesh

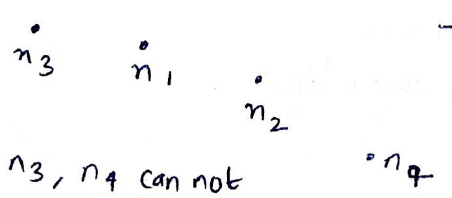


→ routers are connected to each other

MANET

Mesh routers → • stationary nodes mostly
• connected to nearby routers wirelessly
• with each router a Ad-hoc network may be connected.

• 3G, 4G, 5G not involved in Adhoc
• To DS and from DS are 0 then its Ad-hoc

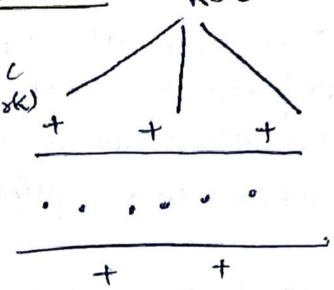


n_3, n_4 can not send directly

→ • so since n_4 is in range of n_3, n_3 can send it to n_4 and then to n_2 and n_2 can forward it to n_4.

host (receiving or sending but not forwarding)
router (receiving and forwarding)

VANET
↓
(Ad hoc network)



RSU - Road side unit
- Direction along road
- Speed - high

(variation of MANET)

• 2 way of communication:
① V2V (vehicle to vehicle)
② V2X (vehicle to roadside)

(possible one or two are connected to internet)

- nodes almost stationary (less motion)
- Act as router of nodes
- find some value and pass to other
- Battery power

Adhock Networks →

Atod 9

even if the subnets are same, we have to forward (Routing) / broadcast)

→ There are different form of Ad-hoc network (4 types)

- General Application of Ad hoc network
  - Some kind of 'Disaster'
  - Infrastructure not working
  - Situations where its difficult to put Infra
  - where two equipments wants to connect to each other.

Routing Protocols (There are around 40-50 protocols but only 4 have RFC)

→ DSR (Dynamic source Routing)
→ AODV (Adhoc on demand Distance Vector Routing)
} for both we will be considering MANET
→ OLSR
→ TBRPS (Topology broadcast based on reverse path forwarding)

Two standard

:- ① IEEE
② Internet engineering task force

We will be seeing DSR and AODV

* AODV

- Table driven (packet going out, packet contains S.Add and D.Add and during forwarding it reaches from - - - - - -)

- Source routing

* DSR
(Contains the whole path, address of immediate nodes) inside packet

→ proactive Routing (overhead reduces, delay increases) (No root)
→ Reactive Routing (
* In wired, change of topology were very rare, but in Adhoc network, the root and topology changes frequently.
- If topology changes frequently overhead increases.
"Jab pyaas lagi to kua khodna shuru kia"

Reactive routing → When packet received, reaction starts
- AODV and DSR are both reactive routing

(node changes so does route changes)
(If route is not used in that time interval hence overhead is useless.
hence why overhead reduces in Reactive.

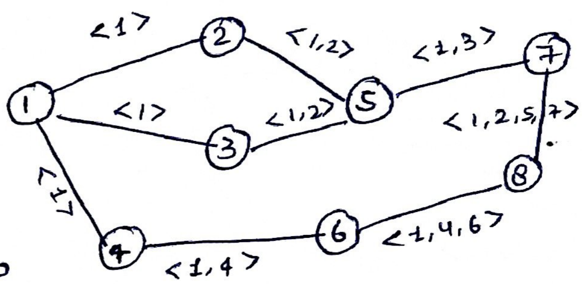
Ques- How does overhead reduce in Reactive?

Ans- In reactive routing nodes location frequently changes, and since the route is given beforehand. when sending packet if the route is not used in time interval the node location changes hence, its useless, the overhead is useless. Hence why overhead reduces but delay increases in Reactive Routing

i)- Route discovery
ii)- Route maintainance

DSR

1)- Route Discovery :- A node only try to find a route if it has same packet to send to destination and currently no known route to destination.



→ if a node has a packet P to send to destination
let 1 to 8.

i)- node(1) search its route cache. If route is present, send packet P to 8 through route.

ii)- if no route in route cache of 1.
Broadcast a Route request with unique id & DA
<1, 8, 42>
id

iii)- A node which receive route request do following
- check if node already received same route request
Request - if so discard it
- if DA is own address of node then R. Request reached to target, send route reply
- if node has route to destination send Route Reply.

iv)- Otherwise node append its own address to list of traversed nodes in packet + rebroadcast Route request.

<R. Reply>
<8, 7, 5, 3, 1>
(unicast back)

Route error msg

id
<1, 8, 3, 4 2>
<1, 8, 3, 4, 42>. append its own address in list
id

AODV : Ad hoc on Demand Distance Vector Routing

19 march

DSN - Destination sequence number

↓

To tell if a route is fresh or old. And if the DSN is low then the route is invalid and it high then valid (in case of 2 DSN)

→ contain only one route in route cache

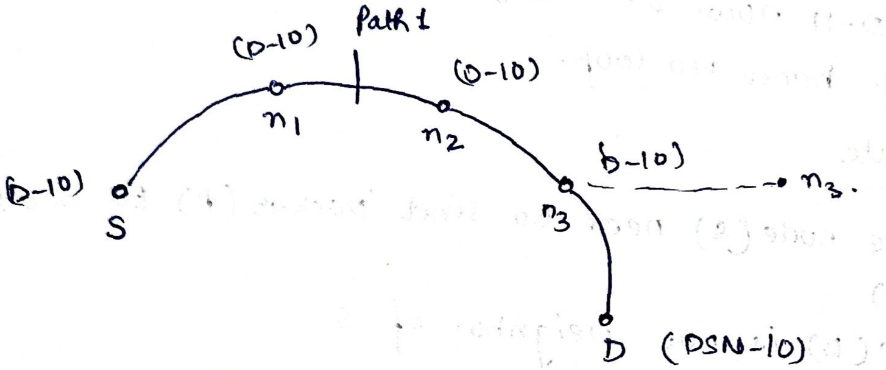
i) checks if the packet has already been seen or not upon receiving.

ii) if a request that has already been procesed is received. it drops the request.

iii). To tell a route is new/fresh route DSN is used, DSN is assigned by the destination.

iv) the one having the greater DSN is valid.

v) - Route request carries the DSN



neighbors

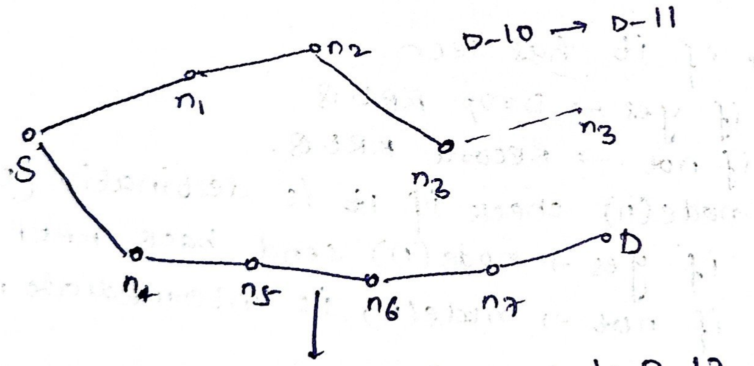
↳ HELLO Pattern)

sends a msg upon receiving a reply it knows these are my neighbours.

n3 → moved-out of range of n2.

n2 → find route or link n3 broken

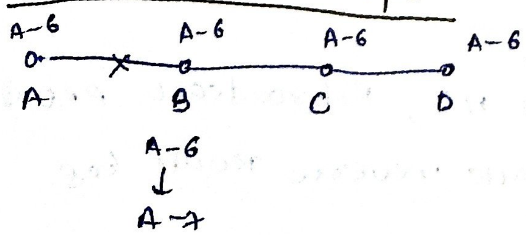
n2 - RERR : Route error. return back to S.



Path-2 the DSN is D-12

only in case of case of Route error the DSN changes, otherwise only destination ~~DA~~ is the one that assign a DSN.

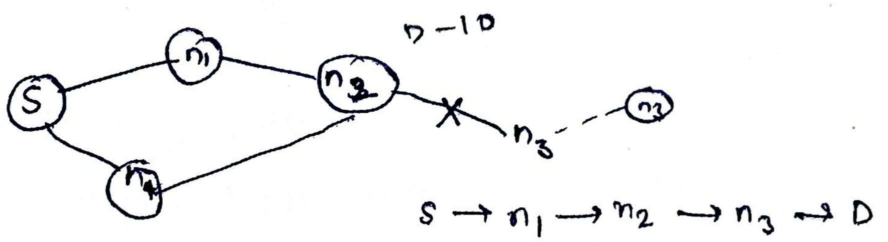
How it avoid loops



B notice route is broken and changes the DSN A-6 to A-7

now: if C → send A-6 - for node A

B → will ~~redirec~~ reject it Because A7 > A6.



S → n1 → n2 → n3 → D

(n2 → RERR to S.

if msg is lost S will assume the route is working but n_2 knows that path is broken so it will send a new path to D so sends a request which is received by n_4 and n_4 sends ~~it~~ to S.

$n_2 \rightarrow$ RERR to S
↳ lost

$n_2 \rightarrow$ search new path for D
RREQ

$S \rightarrow$ get RREQ from n_4

$S \rightarrow$ RREP -

Loop
$n_2 \rightarrow n_1 \rightarrow S \rightarrow n_4 \rightarrow n_2$
$n_2 \rightarrow n_4 \rightarrow S \rightarrow n_1 \rightarrow n_2$

DSN at n_2 = D-10

n_2 - link b/w n_3 broken so.

D-11

$n_2 \rightarrow$ RREQ
↓
D-11

n_2 sends RREQ D-11..

S has D-11 now. It won't tell that it has a new loop hence No loop.

Steps to discover a route

Route Discovery

- if source node (S) need to send packet (P) to another node (D)
- Destination node (D) is not neighbor of S
- Source (S) check if it has route to D

if yes → send packet (P) to D

if not → source (S) broadcast RREQ → < S-add, S-seqno, D-add, D-seqno, HC, id >

→ RREQ reaches to node (n)

- node (n) checks if it has seen RREQ → if yes → Drop RREQ

if not → Record RREQ.

- node (n) check if it is destination (D)

if yes → node (n) send back RREP to S

if not → node (n) is intermediate node

- check if node (n) has route to D

if yes → node (n) send RREP to S & D both

if not → node (n) increases HC, Rebroadcast RREQ. and route reverse Route to S.

RREP

originator - add

Dest - add

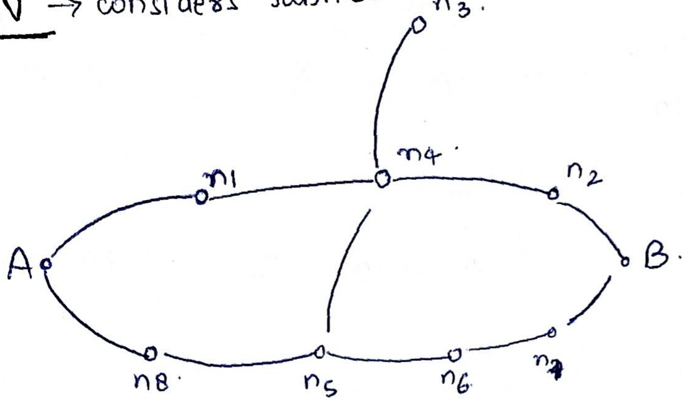
Dest - seq no

HC

id

24/03/2025

AODV → considers subnet also



* A → originator (sending a route request)

P - packet

① A $\xrightarrow{P}$ B

(B is not neighbour of A

② A ⟶ RREQ to B. (UDP packet)

RREQ -

SA	S.seq. no	DA	D.seq no	HC	id
A	A-10	B	B-8	0	42

③ Broadcast by A and this RREQ reaches to neighbour of A

*(at the time of broadcasting packet is encapsulated with ethernet layer, link layer)

IP broadcast → 255.255.255.255

Hardware broadcast → ff:ff:ff:ff

④ RREQ — n_1 & n_8.

n_1 & n_8 → no route to B.

n_1, n_8 → Record route request

first n_1 & n_8 check if RREQ seen or not to avoid duplicates if seen before then drop request

⑤- n_1 → Rebroadcast RREQ.

A	A-10	B	B-8	1	42

⑥- n_1 $\xrightarrow{RREQ}$ n_4

⑦- n_4 → check RREQ → seen or not, Record it

→ no route to B

→ rebroadcast RREQ after increasing HC = HC+1

A	A-10	B	B-8	2	42

⑧ - n_4 → n_3.

→ n_2 → Record RREQ. → rebroadcast after inc HC

→ n_5 → (X) (same RREQ as seen before)

⑨- n_5 → n_4 → (X) (same RREQ)

n_6 (record RREQ and rebroadcast)

A	A-10	B	B-8	3	42

→ n_7 → B

Rebroadcast

A	A-10	B	B-8	4	42

n_5 re broadcast

⑩- n_2 ⟶ B

after inc HC → 4.

make —

* At every node at the time of broadcasting a reverse route is also recorded for route reply.

Reverse route at each node is recorded. (Routing tables at each node)

n_1

dest	nexthop	met	(DSN) seq no	time
A	A	1	A-10	10

n_8

A	A	1	A-10	10

n_5

A	n_8	2	A-10	10

n_4 Keep reverse route

A	n_1	2	A-10	10.

n_6

A	n_5	3	A-10	10.

n_2 reverse route

A	n_4	3	A-10	10

(when n_2 send packet) → B

A	n_2	4	A-10	50

(ii) - B → RREP to A.

↓

< originator Add, dest-Add, dest seq no, HC=0 id >

*(RREP → unicast packet in which if packet is sent it will add or UDP packet is encapsulated with IP layer + link layer in which

S-IP → (B-IP)

D-IP → (A-IP)

Note- All intermediate node make entry at the time of RREQ and RREP so routing table changes at the time of RREP.

(1) at B

		greater sequence no		
A	B	B-12	0	42

B checks its routing table and send packet to n_2

(2) at n_2 → check its routing table (reverse routing path) and send packet to n_4 and also make a forward entry for this also

RREP -

A	B	B-12	1	42

→ n_4

n_2

A	n_4	3	A-10	10
B	B	1	B-12	50

3) Now n_4 → checks its reverse routing path and sends packet to next hop n_1

RREP

A	B	B-12	2	42

at n_4 (Routing table)

A	n_1	2	A-10	10
B	n_2	2	B-12	50

4) Now n_1 → checks its reverse routing path and sends packet to next hop A.

RREP

A	B	B-12	3	42

at n_1 (Routing table)

A	A	1	A-10	10
B	n_4	3	B-12	50

5) Now A receive this packet and make entry for B.

A (Routing table)

B	n_1	4	B-12	50

Case-II → Intermediate node have route to B:

A → B RREQ (A → n_1 → n_4
RREQ RREQ (have route to B

& n_4 has route to B.

at n_4

B	n_2	2	B-10	50

↑

> RREQ (B-8) (here B-10 > B-8 RREQ seq no here it is valid route & and send reply)

Now R4 send reply to A (sends RREP) (* Intermediate node send RREP to both source Add & dest Add)

- R4 ⟶ A

RREP·

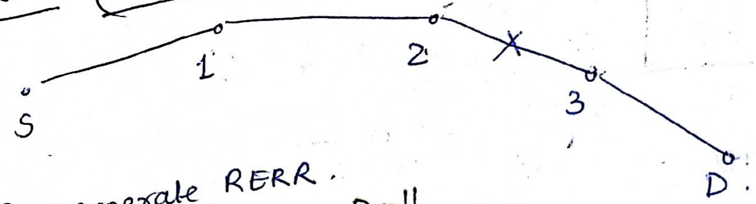
A	B	B-10	HC=2	42

- R4 ⟶ B (Assume A fictitious RREQ from B to A)

RREP (B-9 B-12, anything) → check)

A	A	A-10	HC=2	42

RERR (Route maintenance)



2 → generate RERR.

(DC = 2, 3, ~~3-10~~ 3-11, D, ~~D-10~~ D-11)

↓ Destination unreachable count

↓ (node 2, change DSN of unreachable node and increase by 1)

→ 2 → generate RERR

→ S → 1 → 2 → 3 → D

but when 3 move to different location

now 3 → out of reach of 2

(2 → routing table entry.

dest	next	met		
D	3	2	D-10	50

(as 2 know that 3 is unreachable and now 2 checks its routing table and came to know 3 is next hop of D so, D is also unreachable for 2.)

RERR → (may be broadcast or unicast)

↓

precursor node, or nodes,

↓

A node maintain list of pre cursor nodes that may be forwarding packet on this route.

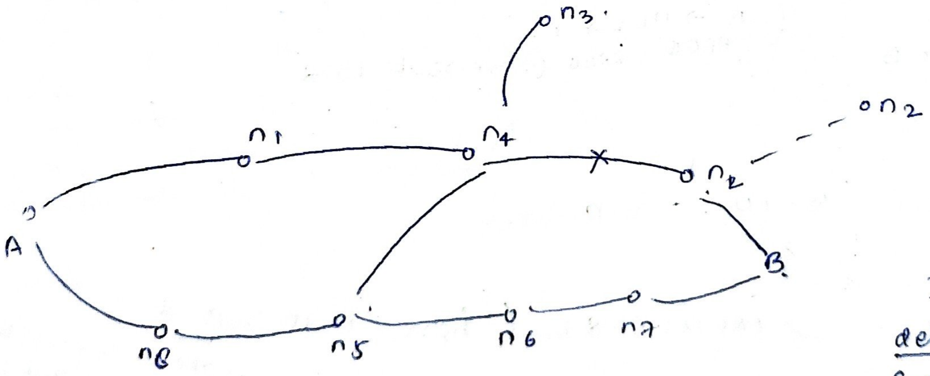
- List of precursor in a routing table entry contains those neighbouring nodes to which RREP forwarded or generated.

→ Now let us suppose in previous diagram if n_2 ~~reach~~ move to another location now generate RERR

✓ for n_4, (n_1, n_3, n_5 → precursor node)

↓

(more than one precursor node so RERR will be broadcasted. so all the node receiving RERR will delete entry to destination from table).



n_4 generate route ~~ge~~ error

→ (DC = 2, 2, ~~2-10~~ 2-11, B, ~~B-8~~ B-9)

↓

n_4 (n_4 broadcast to n_3, n_5, n_1)

delete entries for path B.

now n_3, n_5, n_1

n_5 → n_8, n_6

n_8 → A

→ n_1 → A

Also entry of precursor node is added to routing table.

* (seq-no dekhna hai)

26 March (Aditi sir ke notes)

UDP – Packet loss is not an issue in UDP.

TCP → Packet loss wireless link
- bit error on wireless medium
- mobility

TCP deal with

Packet loss :- Detect via – time out, no Ack.
- goes to slow start
  Assume congestion
- unable to find loss is –
  - due to congestion
  - due to bit error on wireless medium
  - due to mobility

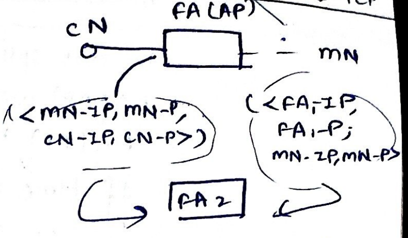
Result – performance degrade

Cannot change – TCP – because of large Installation base

(TCP 'today' + Resource management)

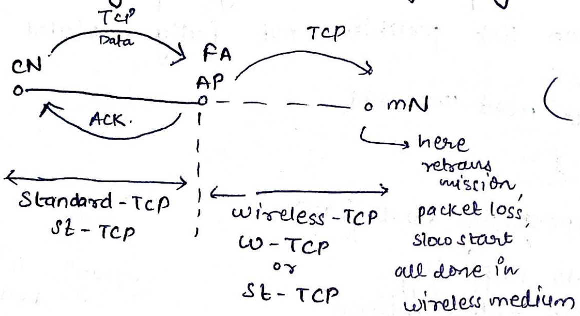
" Read ppt + sir Notes for Theory of TCP.

Socket Transfer in I-TCP



as it is transfer to FA_2 when MN moves to FA_2

I-TCP (Indirect TCP) //



(TCP connection is established b/w CN & MN which is virtual and we split connection at AP.

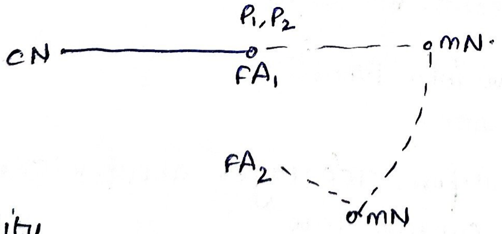
→ There is a violation of end-to-end connectivity because acknowledgement is sent by AP not MN (where packet actually need to sent) and due to which for entire duration AP have to buffer all packets on the behalf of MN.

- split connection at FA(AP)
- FA(AP) act as proxy

$$\left.\begin{array}{l} CN \xrightarrow{P} FA\,(AP) \\ FA\,(AP) \xrightarrow{P} MN \end{array}\right\} \text{(split into two connections)}$$

→ FA(AP) buffer packet, send Ack to CN, now forward buffered packet to MN & Receive Ack from MN.

//.



* chances of AP crashing can led to permanent loss of data.

Mobility

- MN moves from FA_1 to FA_2
- FA_1 received packet P_1, P_2 & Ack send to CN
- Now FA_1 unable to send packet to MN
- when MN register with FA_2
- FA_2 can inform FA_1 for location update of MN
- FA_1 transmit P_1, P_2 to FA_2

- Socket transfer from FA_1 to FA_2 to maintain TCP connection.

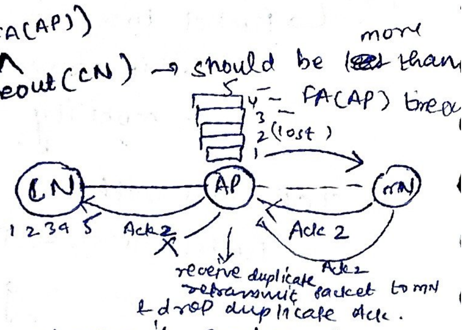
Snoop-TCP → • Do not split the connection (TCP connection b/w CN + MN.
• AP monitor the packet transfer and Ack.

(end to end semantic are retained

CN — FA(AP) — MN (error prone area.)

→ timeout (FA(AP))

→ timeout (CN) → should be more than FA(AP) timeout



- do not split
- FA(AP) watch packet & Ack
- FA(AP) buffer packets & set time out
- If time out at FA(AP) for a packet retransmit the packet to MN
- if FA(AP) receive duplicate Ack then it retransmit packet to MN & filter (drop) out duplicate Ack.

MN to CN – FA(AP) snoop packet stream & detect gap in seq. No. send N-Ack to MN + MN retransmit missing packet.

Adv → E-T-E connection
- NO handover of state on change of FA } disadvantage of indirect TCP.

Disadv – wireless link problem not fully isolated from wired link
- N-Ack need on MN.

M-TCP → (imp) • uses supervising host (SH)

• SH – No buffering
- No retransmission
- monitor all packets.
- if disconnection detected (through MAC Layer → when SH do not receive Ack for some time from MN)
- send WS = 0 to CN
- CN do not transfer any thing
- when connection detected.
old or new SH reopen window by sending WS = old value.

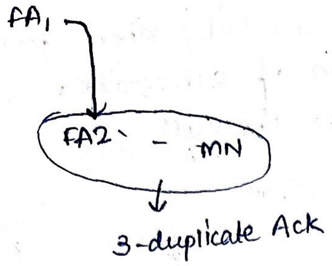
here AP does not send acknowledgement to CN until/unless it get acknowledgement from MN.

Zero window Advertisement sent to CN from AP

Transmission / time out freezing:
- mobile host drive into tunnel
- cross Layer
- MAC layer inform TCP layer about interruption
- TCP freeze current state
- timer + congestion window
- when MAC layer detect connection again it inform TCP
- TCP resume connection from same point.

* hold or last acknowledgement at AP is use to send ZW Ack to FN if there is chances of disconnection

- Fast retransmit / Fast recovery



- Selective Repeat

T-TCP - Transaction Oriented TCP.
  - connection setup & break
    7 packets → 2 to 3 packets.

2/04/2025 (4G, 5G → Editions)

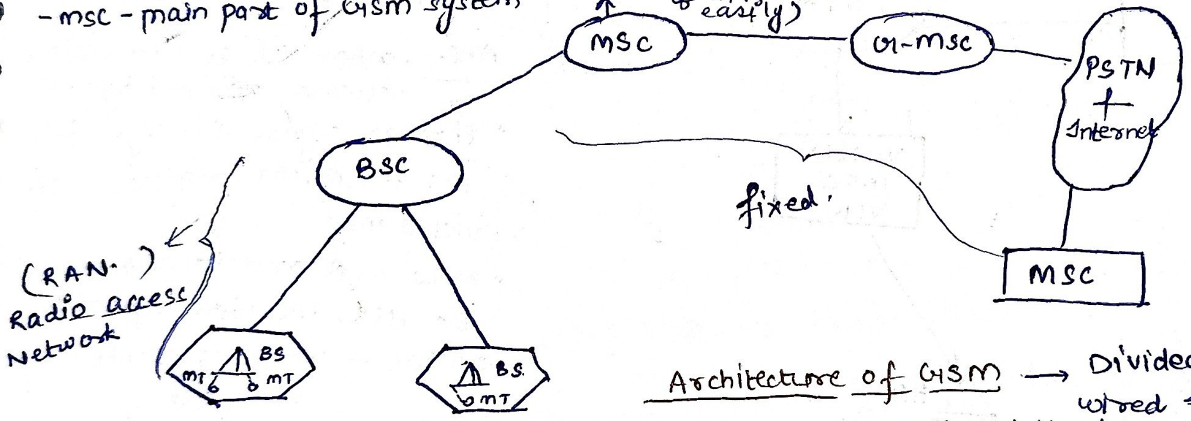
MT → mobile Terminal or mobile station

PSTN - Public switch Telephone Network (circuit switch)

GSM 2G, 3G → Global System for mobile communication

- certain no of Base station are connected to BSC.
- msc - main part of GSM system

(should know the exact locations & MT so that can route call easily)



Architecture of GSM → Divided into two parts wired & wireless.

BTS
BS — Base Station
BSC → Base Station Controller
MSC - Mobile service switching Centre
G-MSC - Gateway MSC - we will refer it as home MSC.
(related to concept of Home network)

(SIM card identify by this number)
SIM, ISMI → identification
Home PLMN → Home public land Mobile Network
Visited PLMN → Visited Network.

MSC → (Keep locations)
- Contain several BSC
- ~~Connecting~~ control all connections upto MT
- Data base Integration < HLR, VLR } Databases present at msc
- Call forwarding
- location management
  - registration of MT with msc (this info use in call forwarding)
  - forwarding reg information to home network.

→ SIM card attached with ISMI number and registered with locality called as home network

HLR → database at home msc (Gmsc)

- Home Location Register
- Permanent Phone number of subscriber + subscriber profile.
- Information about current location of subscriber
- address of visited network to route the call

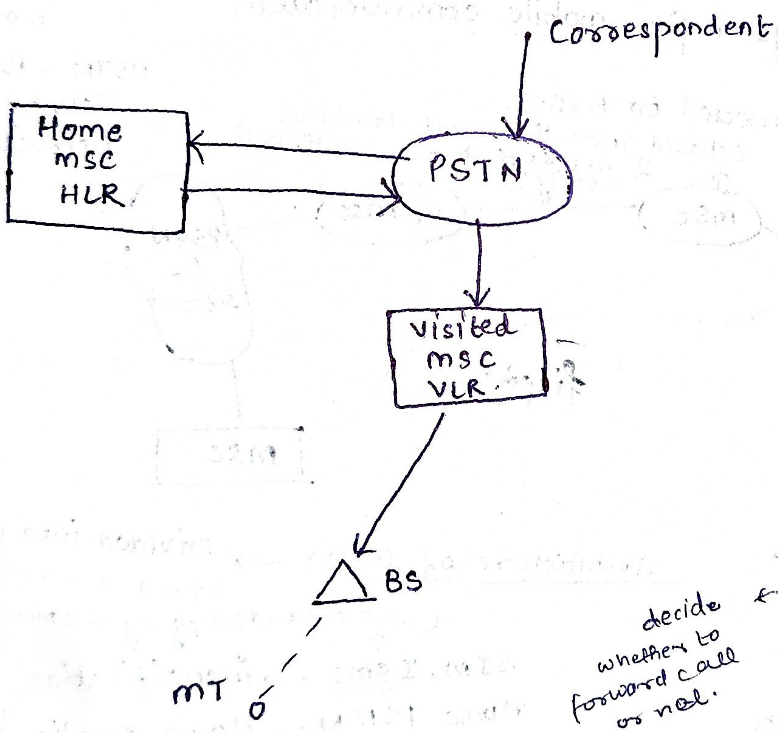
(msc contain VLR)

VLR → Visitor location Register
- database at visited msc

(BS–MT) info inside VLR
- contain entry for each mobile user currently in the network served by VLR (present with particular msc)

(Dynamic database)
- VLR entry come & go as mobile user come & go
- VLR is usually co-located with visited msc.

* Call forwarding (in 2G network, 3G network)



decide whether to forward call or not.

How HLR get Roaming number? or VLR addr.

Ans– • when MT goes to visited network covered by VLR
- through signal exchange b/w MT & VLR. MT register with visited msc.
- Now VLR send location update to HLR, location update contain – roaming number or VLR add
- VLR get info at subscriber from HLR.

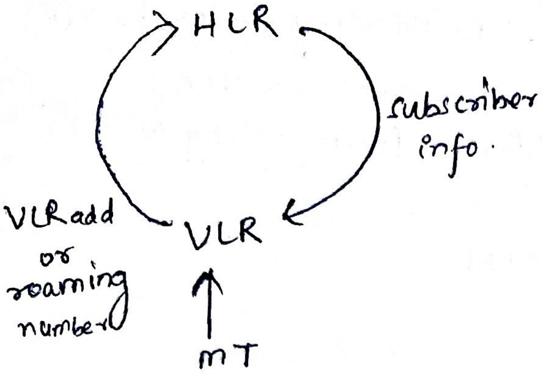
1- Correspondent dial MT permanent number, Through permanent number call goes to Home msc (G-msc) via PSTN.

2- Home msc (G-msc) receive call - equiring to HLR to find location of MT.

3- HLR return - address of VLR — if G-msc get address of VLR - it obtain roaming number from VLR
or
roaming numbers (not visible to user)

to Home msc (G-msc)

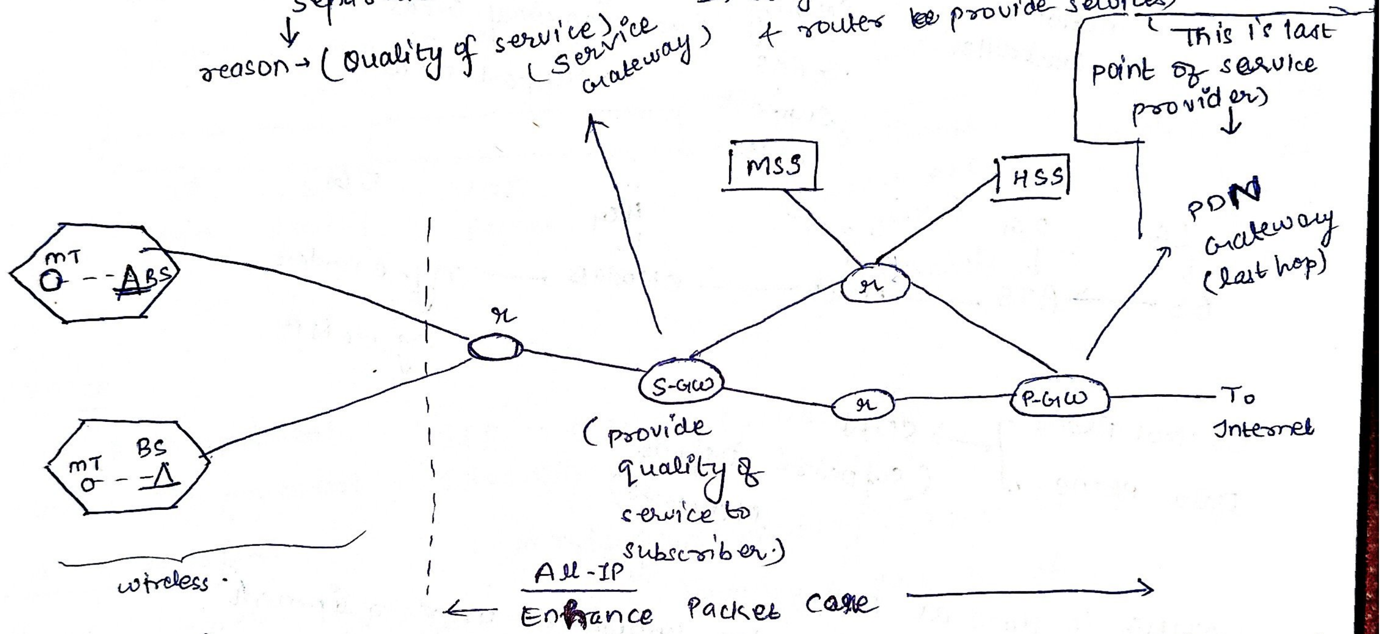
4- Home msc (G-msc) set up second leg of call to visited msc. Visited msc transfer call to BS serving MT.

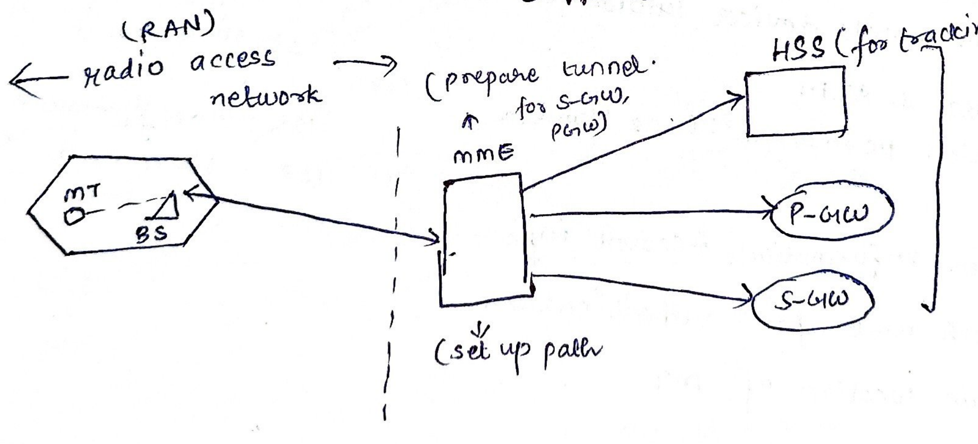


7/04/2025.

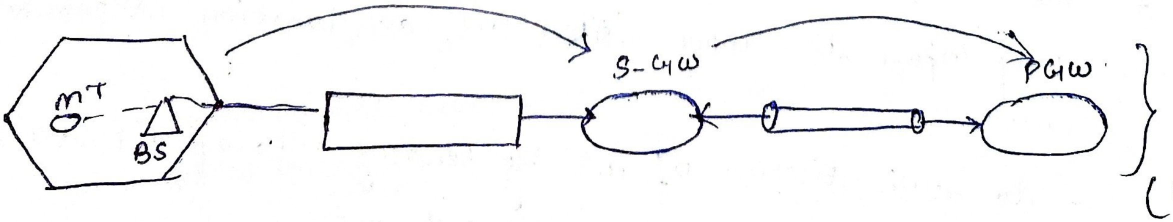
4G - LTE (Data Transmission and call forwarding (voice call) done on separate tunnels) ?

↓ reason → (Quality of service) (Service Gateway) → It goes to internet keeping requirement + router provide services)





Control Plane → (how Routing to be done ↓ how RT to be prepared ↓ All different Routing Algorithm is part of control plane)



User Data Plane (Packet Transmission

(Part of Data Plane) → Packet forwarding logic, Routing Table)

GPRS → Generalised Packet Radio Service

HSS → Home Subscriber server / service → (Functionality similar to HLR)

MME → mobility management Entity (it is related to VLR)
(Similar functionality as VLR)

2G

MT → BS → BSC → MSC → GMSC → PSTN

3G

MT → BS → RNC → MSC → GMCC → PSTN } for call delivery.

RNC → SGSN → GGSN → Internet } for Data Network

(wireless Portion) — MT → BS

RNC → Radio network Controller

SGSN → Serving GPRS support node.

GGSN → Gateway GPRS Support node

1G	2G	3G	4G	5G
BS	BTS	NodeB	eNodeB	ng-enodeB / ng-eNB

BS → BTS — NodeB — eNodeB — ng-enodeB / ng-eNB

Control Plane
Data Plane } → SDN (Software Define Network)

* NATING is done at P-GW
* In 4G, 5G MT or mobile devices known as user equipment.

HSS - store IMSI + SIM information, permanent Phone Number
- like HLR
- subscriber Information, Account info.
- use with MME for authentication
- contain location of MT

at some point
HSS - store dynamic entries also
HLR - store static entries

MME - - Like VLR
- Keep information about visited MT, cell location in carrier's network
- do authentication of MT by sending info of MT to HSS + obtaining info from HSS about MT
- Path, tunnel setup - BS to S-GW + S-GW to P-GW

P-GW → (PDN-Gateway)

- last LTE element that a datagram originating from MT encounter before entering to Larger Internet

(Provide Private IP address to MT)

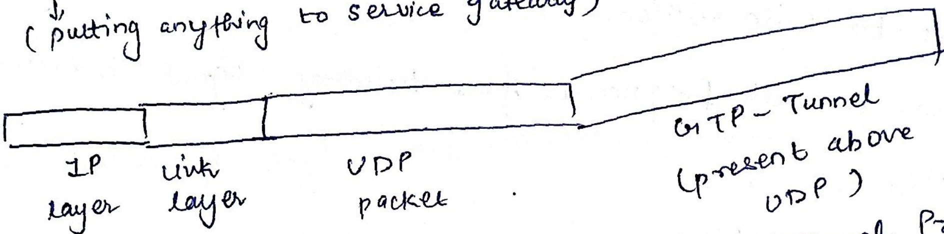
- Provide NAT IP to MT & perform NAT functions.
- Provide NAT IP to MT is hidden behind P-GW of cellular carrier.
- mobility of MT is hidden behind P-GW of cellular carrier.

S-GW

- control QoS
- manage local mobility when MT move among different Base stations
- Tunnel from BS to S-GW change as MT moves
- MME control this change of tunnel b/w S-GW & BS.

(putting anything to service gateway)

packet →



GTP-U → for user plane

GTP-C → for control plane.

→ GPRS Tunnel Protocol

For voice

4G use RTP protocol

5G use SCTP protocol

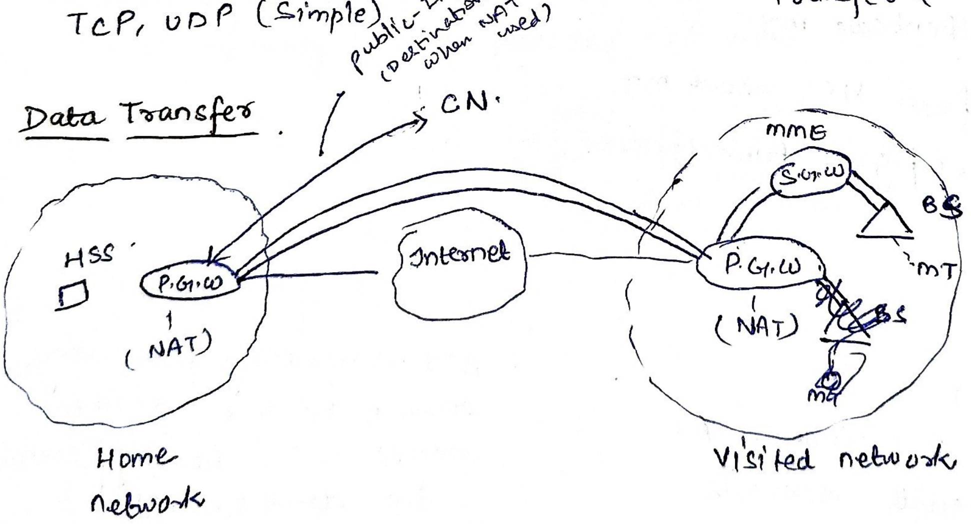
SIP is also use by 4G, 5G. (session initiation Protocol)

For data transfer

TCP, UDP (Simple)

* Triangular routing is used for Data Transfer & call transfer.

Data Transfer

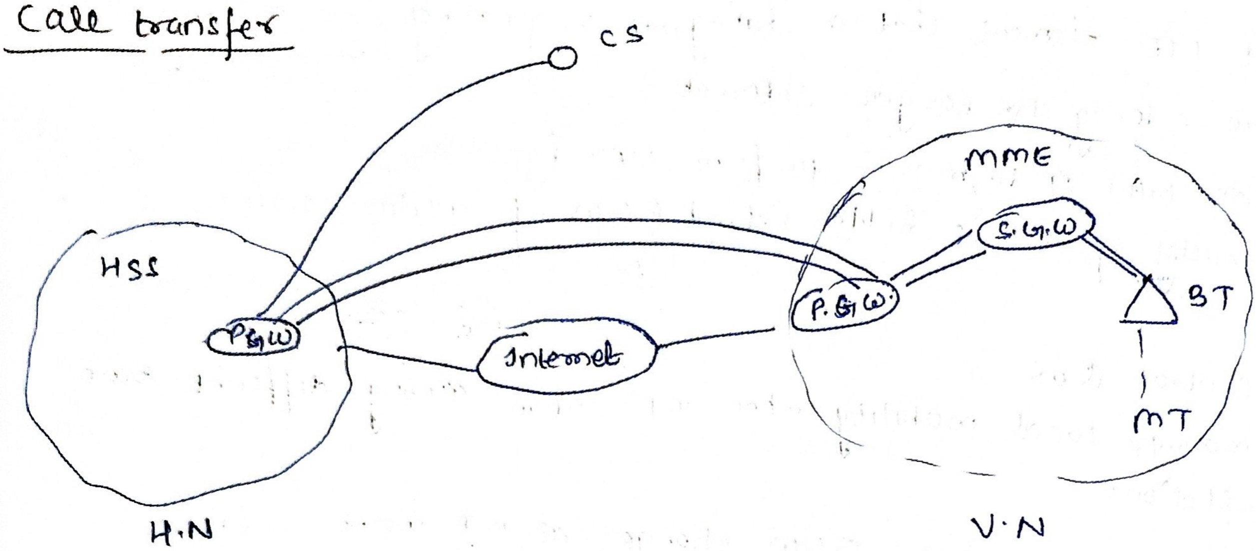


MT → IP, Permanent Phone no

PDN will be able to know for whom this packet is - Public-IP)

(Seperate tunnel created to give ~~traffic~~ priority to voice traffic) within network.

Call transfer



Major steps

MT moves to base station.

- ms – listen to all frequencies for primary signal transmitted by base station.
- It select base station
- it provide IMSI, home network, subscriber info to BS

Associate with MME

- BS control MME
- MME get authentication + subscriber info from HSS
- MME authenticate MT
- MME inform HSS about MT
- MME configure tunnels.

09/04/2025

Hand-off

2G, 3G

(connection ongoing)

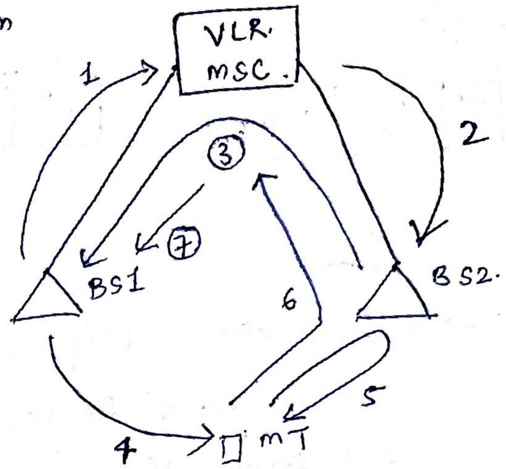
- during call when MT change BS
- when signal strength deteroits
  or
  when cell overloaded

BS1 → currently providing service to MT so BS1 decide either handoff should be done or not.

- MT associated with BS1, find signal strength of BS1 + signal strength of BS2
- if is sent to BS1 - 2 times in one second
- handoff indicated by BS1

Things done during handoff:

i)- BS1 message to visited MSC - Handoff to BS2 of MT



ii)- visited MSC setup path to BS2 & inform BS2 for handoff of MT.
(all main act done by BS2)

iii)- BS2 allocate channel to MT and inform visited MSC & BS1 about path setup & information needed by MT to attach with BS2

iv)- MT is informed by BS1 to perform handoff to BS2

v)- MT & BS2 exchange message to activate new channel.

vi)- MT send handoff complete message to BS2 which is forwarded to visited MSC. Now visited MSC start re-route call to MT via BS2.

vii)- Resources along path to BS1 released (channel or anything should be released by BS1)

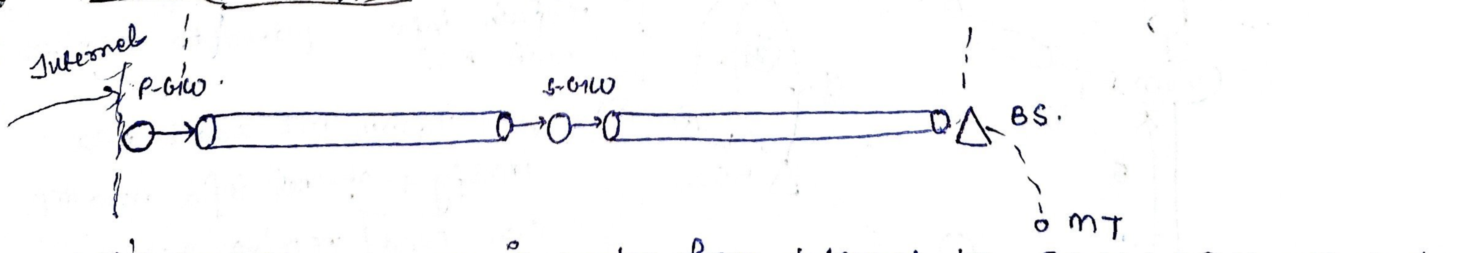
→ In only one Base station (within same BS) & MT handoff can happen if BS change channel.

→ whatever is required for MT to attach to BS2 inform by BS2.

→ when signal strength decreases beyond minimum value (min-SS) then call delivery is not possible ∴ so either — call termination. ✓ (talk to VLR and all registration done) → (location management)
— handoff.

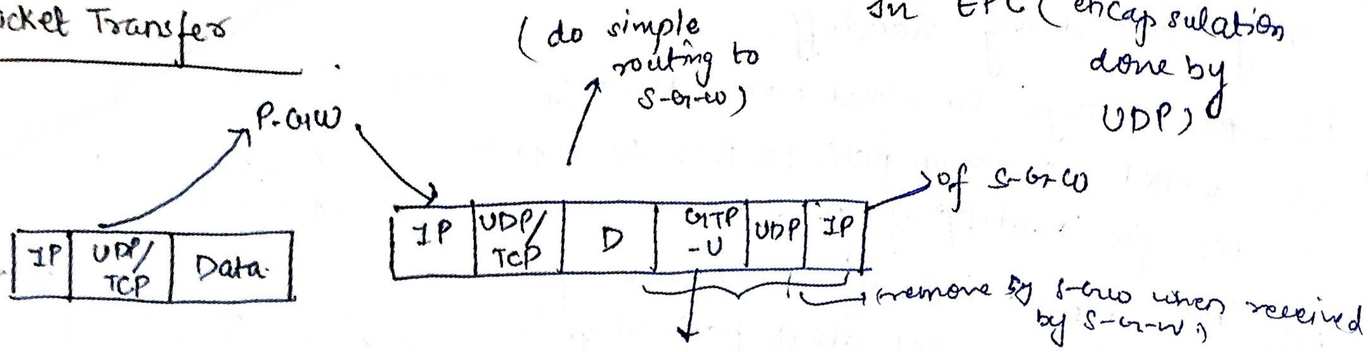
→ $\boxed{\text{handoff value (SS)} > \text{min-SS}}$

4G (Handoff)



• Let's suppose a packet is coming from internet to P-GW (PDN network)

Packet Transfer



TEID → tunnel end identity.

→ S-G-W check this encapsulated packet & check tunnel end identity remove extra headers & Add its own GTP-U, UDP & IP (MT) and sends this new packet to base station

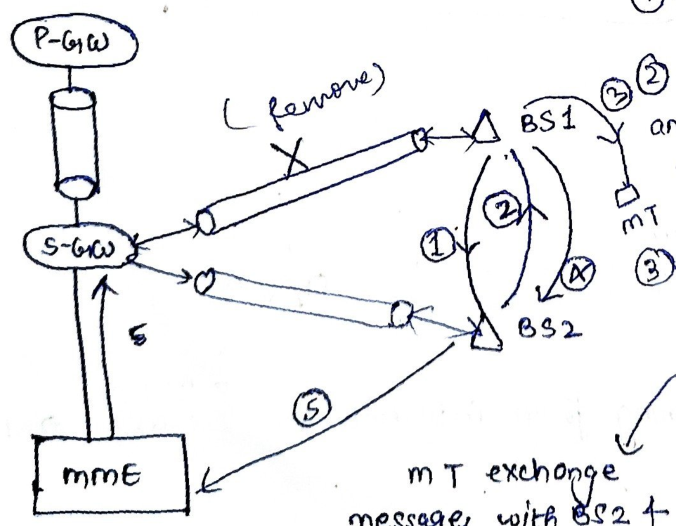
→ Now from Base station we do radio interface to transfer packet to MTP.

→ from internet it receive IP → public-IP of P-GW
but when transferring from PDN Gateway to S-G-W it changes IP (from public IP to private IP of MT)
PDN Gateway do NATing)

→ when voice msg or packet is not going to internet then IP will be private IP.

→ (in calling packet (Data → permanent phone no.) & in PDN Gateway use SIP protocol to find its IP address)

4G (hand off)



① → BS1 select BS2 and send handover Req to BS2

② → BS2 allocate channel for MT and BS2 send handover Req-Ack - contain info required to associate with BS1

③ - BS1 inform MT about BS2 identify & channel info now MT can send/receive datagram to/from BS2.

MT exchange messages with BS2 & inform BS1 handoff complete.

④ BS1 stop forwarding datagram to MT & redirect them to BS2.

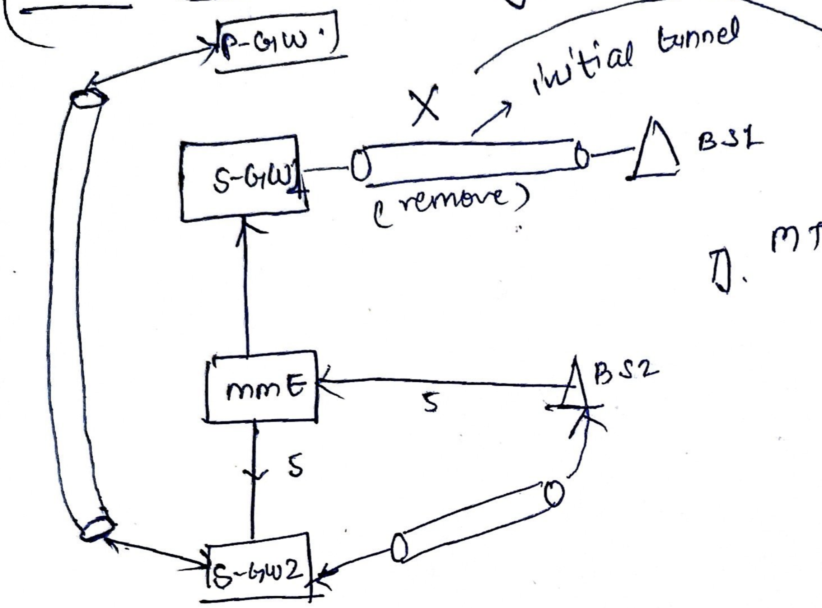
⑤ BS2 forward these datagram to MT

5)- BS2 inform to MME.
MME signals to S-GW for creation of new-tunnel between S-GW & BS2 for MT.

6)- BS2 inform BS1 to release resource associated with MT.

7)- BS2 & MT exchange datagram through new tunnel.

(Case - when S-GW change) (upto 5 step remain same)



before removing this tunnel another tunnel is created b/w P-GW and S-GW2 then after this S-GW1→BS1 ~~Gat~~ tunnel can be remove

In 4G, 5G call is transffered in packet Form while in 2G, 3G call is transffered through circuits. when MT moves from BS1 to BS2 then packet ~~chan~~ coming for MT It can be buffered at BS1 due to packet switching which can not be done on circuit switching (2G, 3G). This is only advantage of 4G, 5G over 2G, 3G.