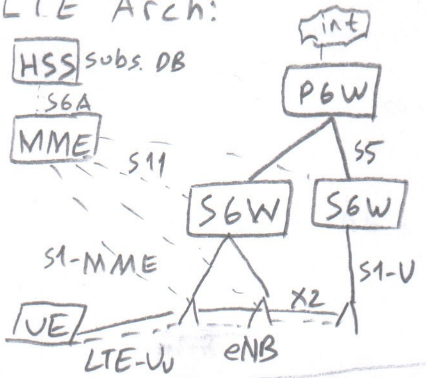
LTE Arch:



Tugrul Yatagan 504161551

NAS: UE-MME

AS: UE-eNB, (Radio Res. Cont.)

HSS: auth, loc. man

MME: control plane, intermediate auth NAS security idle mobility hand.

PGW: user plane UE IP⑥ allocation

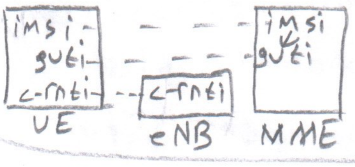
SGW: user plane inter eNB mobility

eNB: connection mobility mgmt RB control

$IMSI \to \underbrace{\overset{3}{MCC} + \overset{2-3}{MNC}}_{PLMN-ID} + \overset{9-10}{MSIN}$

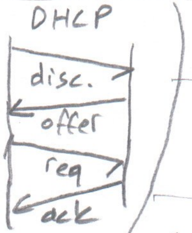
GUTI → globally uniq. temp.

C-RNTI → cell-rad. net. temp.



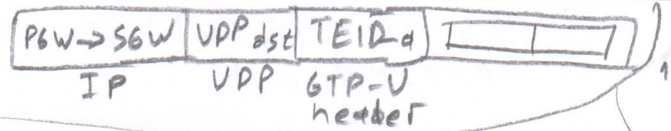
GTP-C tunnel (SGW-PGW)

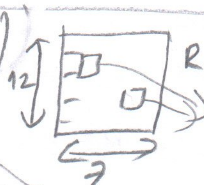
attach goal → obtain ip, authen. author.



OFDM → 1 subframe = 1ms, 10 subframe → radio frame

GTP





Resource Block

Reference Signal

Sending node → Correspondent Node

Moving node → MN, UE

Mobility provide "seamless"

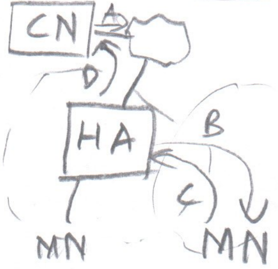
Identifier → does not change as MN moves

Locator → current point of attachment, topol. correct addr

IP layer solution: 1) routing-update 2) Tunneling/Mapping (GTP, MIP)

Transport layer solution: mpTCP (connection over multip. interface).

1) IP unchanged, routing table update ↑ 2) routing isnt impacted

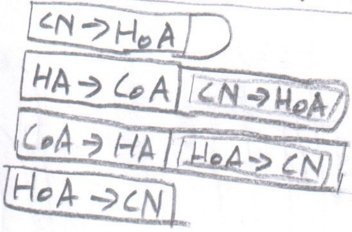


A) CN-HA

B) HA-MN

C) MN-HA

D) HA-CN



IP isnt designed with mobility

Identifier-Locator seperation protocols, rendezvous

handovers are prepared. source nNB decides. S1 and X2 handov

service contunity.

S1 → MME degisir SGW belki

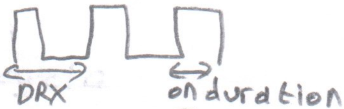
X2 → MME sabit SGW degisebilir

1) Connected mode → tx/rx on / can handover

2) idle mode → rx period. on. / can TA update / paging broadcast channel

1 → network (mme) knows cell / 2 → network (mme) knows TA

UE and MME keep track of state.



1 → PGW $\overset{S5}{—}$ SGW $\overset{S11}{—}$ MME $\overset{NAS}{—}$ UE ; SGW $\underset{S1-U}{—}$ eNB — UE

2 → PGW $\overset{S5}{—}$ SGW $\overset{S11}{—}$ MME eNB UE

MME → has UE info ; eNB → hasnt UE info

↑#TA = less signal but ↑# eNBs that UE paged in

TAI → MCC + MNC + TAC

$SFN \bmod T = (T/N) \cdot (UE\_ID \bmod N)$ | $i\_s = floor(UE\text{-}ID / N) \bmod N_s$

$T = min(T_c, T_{ue})$ | $N = min(T, N_f \cdot T)$ | $N_s = max(1, N_f)$

Security:

- ID authentication, verify who you are (IMSI)
- Data authentication, data came from the source
- Data integrity protection, nobody alters data
- confidentiality, encryption only src and dst can unders.
- authorization, access resource only you can
- privacy, keeping your id secret
- non-repudiation. undeniable evidence that msg is from sender

man in the midde can listen, delay, delete, modify, replay, create

symmetric key: shared, private key scheme $Enc_k(p)=c$; $Dec_k(c)=p$

asymmetric key: puplic key scheme $Enc_{pk}(p)=c$; $Dec_{sk}(c)=p$

$Enc_{sk}(p)=c$; $Dec_{pk}(c)=p$

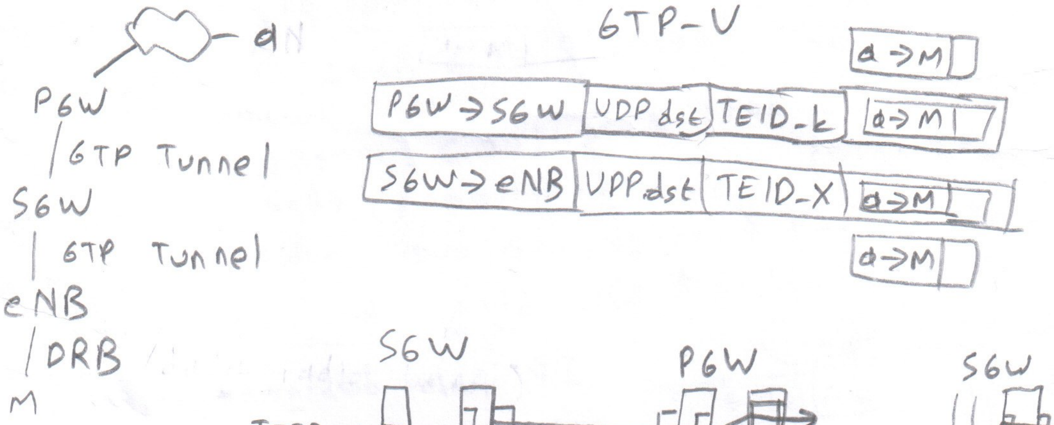
IMSI → send over air only during attach, GUTI is used insteed

IMEI → only sent to MME (in NAS), not eNB

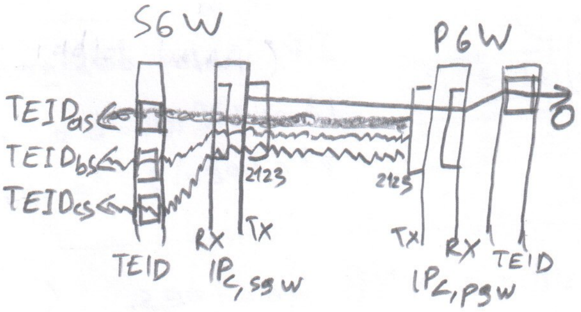
MSISDN → CC + NDC + SN
+90 533 1234567

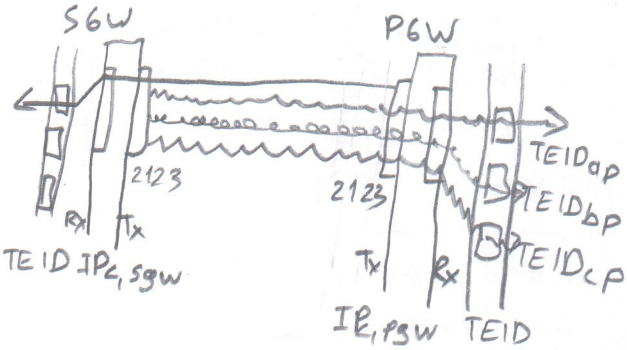
eNB

SRB (signaling) | DRB (data radio UE bearer)



TEID → Tunnel endpoint identifier


SGW
PGW
TEID_as
TEID_bs
TEID_cs
2123
2125
TEID
RX
Tx
IP_c,sgw
Tx
RX
TEID
IP_c,pgw


SGW
PGW
2123
2123
TEID_ap
TEID_bp
TEID_cp
Rx
Tx
TEID
IP_c,sgw
Tx
Rx
IP_c,pgw
TEID