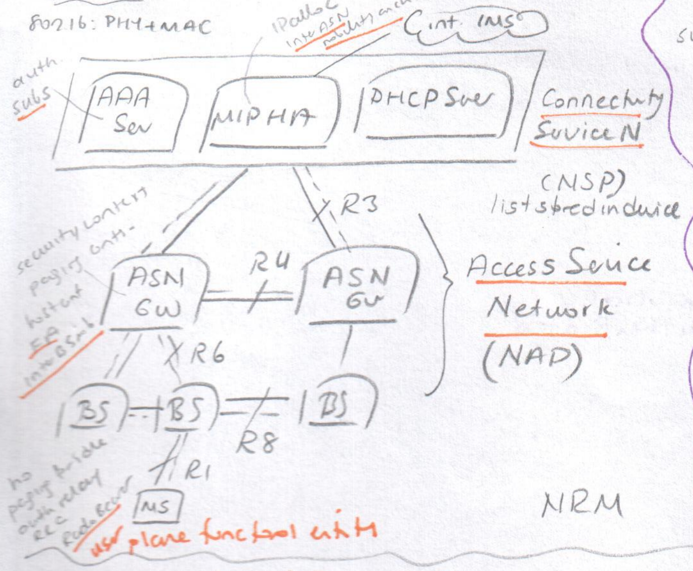
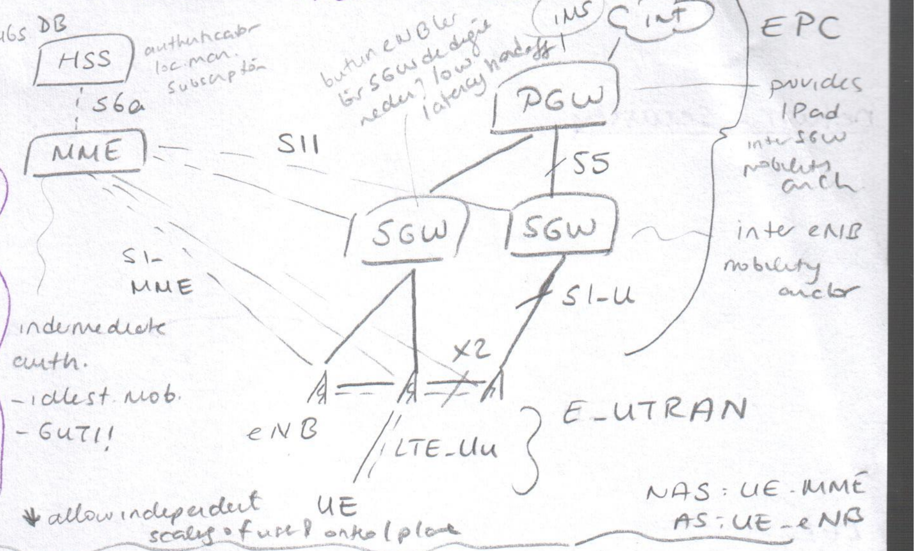
Wi MAX Network Architectue



LTE Network Architecture



IMSI : MCC + MNC + MISN (in SIM)
3 2-3 9-10
mobile country code
PLMN mobile network code
mobile subs identification

MSISDN phone #: CC + NDC + SN (IMSI – MSISDN mapping in HLR)
country code
national dest code (identify operator)
subscriber number:

CRNTI (cell radio n. TI) eNB provides (for RRC con.)
GUTI (globally uniq TI) MME " 56bit + PLMN!

GTP-C tunnel (SGW↔PGW)
tunnel endpoint PMIP for GTPC tunnel.
+IP+UDP port selection.

Goal: obtain IP address UE scans / selects

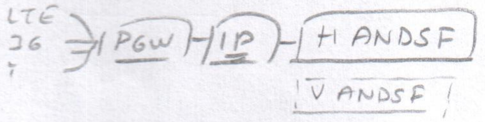
PLMN Selection, **power on aut.** registered → eq → eq home → user cont → op cont → RSSI → RSSI

man last " , eq, yoksa EHPLMN highest p yoksa aynı elite user a.

UE can change PLMN within same country MCC of new = MCC of reg.

cell sel.
active: net.
idle: UE)
eNB decides

non_3GPP LTE 3G ? ⇒ PGW – IP – H ANDSF over IP access network discovery selection function.
V ANDSF



wimax . NAP discovery, NSP access discovery, NSP en. & sel., ASN attach. based on NSP (use NAI to determine next AAA)

∝ SIM contains RATs/freqs at least for H/EH PLMN
∝ wimax; device has NSP lists.

3GPP - PLMN ids in bcast info
wiMAX - NAP in DLMAP in 6

OFDM in DL power ampl. ineff. & receiver complexity avoidance UL → SCFDM

Radio Frame 10ms, Subframe 1ms, Slot = 0.5ms in f domain RB = 12 subcarriers × 7 symbols = 1slot
180 KHz

$SFN_T = \frac{T}{N}(UEid \bmod N)$ – min (T, # of paging frames per frame × T)
min (true Tc) Nf
32, 64, 128, 256

$is = \left\lfloor \frac{UEid}{N} \right\rfloor \bmod Ns$ max (1, Nf)

tracking area code

NS	is 0	1	2	3
1	9	–	–	–
2	4	9	–	–
4	0	4	5	9

} PO

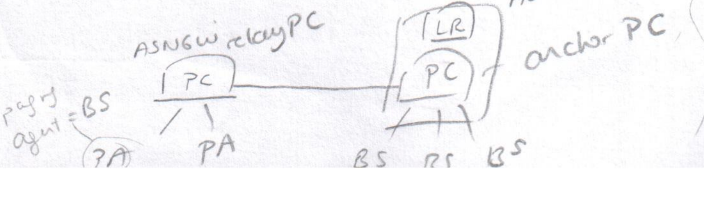
active mode: granularity of cell
idle mode LA/TA
LTE non-overlap
each cell in eNB can belong + 1 TA. UE can admit to multiple
content transfer

TAI: PLMN + 16bit TAC, MME Service Area, route to get to old MME: use GUTI
(PLMN, cell-id, TAI is bcasted)

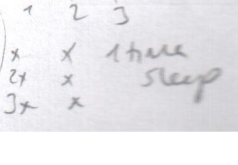
WiMax paging ↑ update ↓

WiMAX overlapping TAs, UE can belong to only one PG (paging group) (LTE, multiple TAs) paging ↑ update ↓

paging controller
ASNGW can request another ASNGW to also page UE! R4
(not in LTE, 1 MME!)



LTE
wimax sleep ≡ DRX
short
long



Dynamic TA → Thresh → time
→ Movement
→ Profile → Distance

Paging → simult
→ sequential (page last kown loc than othe)
→ profile

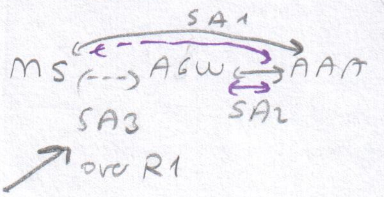
MME Group MME-Group code (group) UE tells eNB which MME has its context, when UE does TAU MME provides new GUTI

network security - authentication (device, data origin), authorization, integrity prot, replay protection, privacy, non-rep.

symm same key both ends, asym public-private key pair (only known by entity)

hash → message integrity
→ auth. (MD5, SHA-1)
HMAC-SHA-1) hash based mes auth code

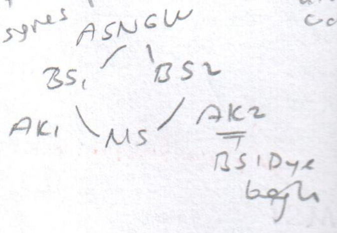
3 party security model



mutually authenticated

dynamically established

public key'ini bana gönderdeken impersonation attack olabilir! bu yüzden x509 CA signs public key



KEK delivering other keys security

C-MAC Key used for protecting control mes.

TEK traffic keys randomly generated in BS & delivered. Sent to MS with KEK

multicast bcast

AGW
BS1 BS2
MS
~~AK~~ AK1 - CMAC PN
MS: pm → ak1 ↔ cmac - pn1
CMAC-KEY-*
CMAC-PN-* for replay attacks!

cache (CMAC-PREKEY, CMAC-KEY COUNT, CMAC-KEY-, CMAC-PN-*, BS flushes)

R1 security message integrity: AES-CMAC control packets uses CMAC-KEY--

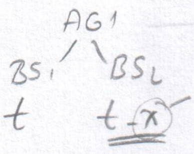
encryption AES CCM using TEK) Data packets are encrypted

Device + Subsriber Authentication with EAP TTLS

authentication, authorization, session key generation & dist = t olsun.

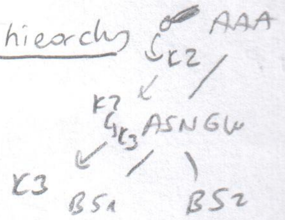
AG1 2 3 4
t t t t
→

opt: hierarchical



authentication authorization kesdeh

key hierarchy



→ sadece K3u tekrar yarat!

preauthentication (authorization has lifetime!)

context transfer: transfer security context (MSK, --)

roaming
kt. Gm! alper 0 clear wea

E2End, ex IPsec, HTTPS wimax, LTE MAC security

Last-mile Secure (L2): ex wiFi at home, AP de laptop arası secure DSL'e gecince no secure

DHCP, ARP, DNS spoofing, traffic analysis - - ⇒ L2

privacy against intermediaries require → E2E exit VPN (midway not E2E)

S1: service req
S2 arch model high level sp
S3 protocol specs - -

app layer HTTPS, authentication + username/pwd

privacy hide from neighbors - L2
" " intermediaries E2E
) use pseudo ID during access authentication "I'm Alper"
pseudo MAC (802.16m will support)

MS ↔ Vodafone AAA secure

LTE SEC

network access security radio link for encryp + int for RRC & NAS, encry for data (not integrity)

gerçek Mac'i intermediaryler bilmez.

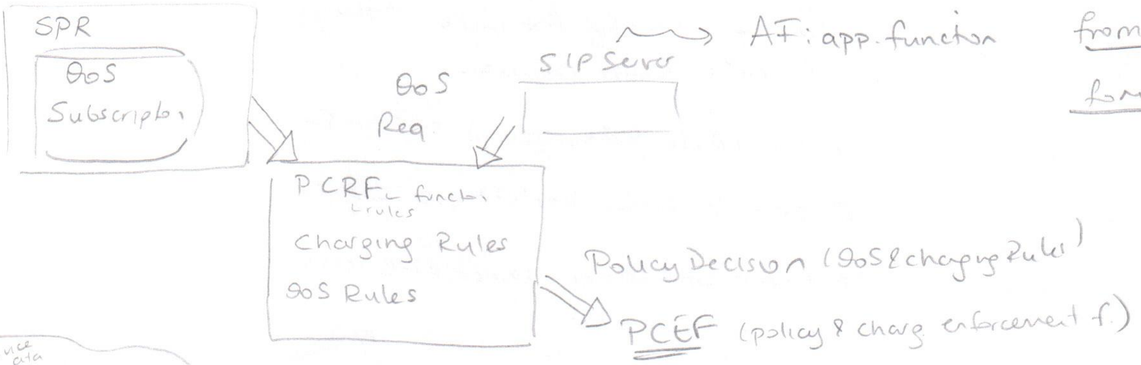
network domain between PLMNs. IS AKN, tunnel mode EAP, user domain user sim USIM, user terminal authentication (if SIM locked pw)

LTE Kasme ≡ session key in WiMAX

QoS user satisfaction, because we donot have enough resources, where: chokepoints

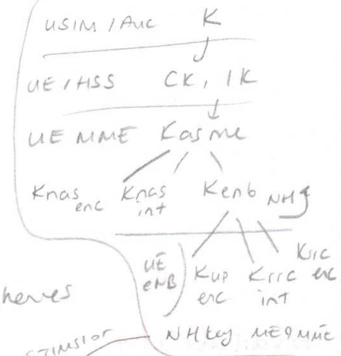
highest cong: eNB ↔ UE
medium: access network (enB ↔ CN) backhaul, least con: local office.

PCC provides IP flow (SDF) based QoS (flow 5 tuple sad + dad + sport + dport + protol)

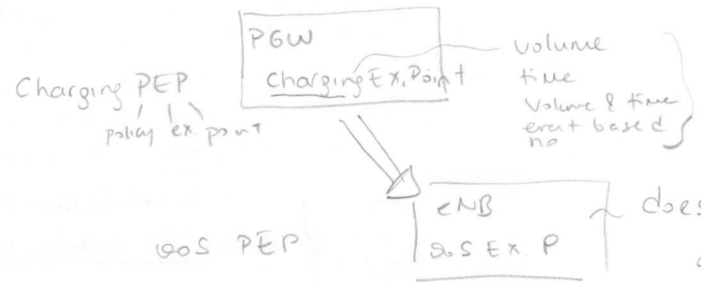


AF: app. function

from AF: network initiated
from user: user "



SDF level data flow QoS Params
QCI, ARP, MBR, GBR
use 9..15
Beare Level
QCI, ARP, GBR, AMBR
video/voice



volume
time
Volume & time
event based
no
charging schemes

does QoS rule enforcement
admisson control + scheduling

STIMSI or GUTI — IMSI subscriber
IMEI hardware
only sent to MME in NAS after setup securely

dedicated bearer/s
default bearer

1 or more flows mapped into EPS Bearer on S5 & S1 → GTP-U, on air → Radio
for dunlink mapping is done in PGW / for uplink mapping is done on UE!
SGW & eNB are only aware of EPS Bearers not individual flows !

right now, all service is BE

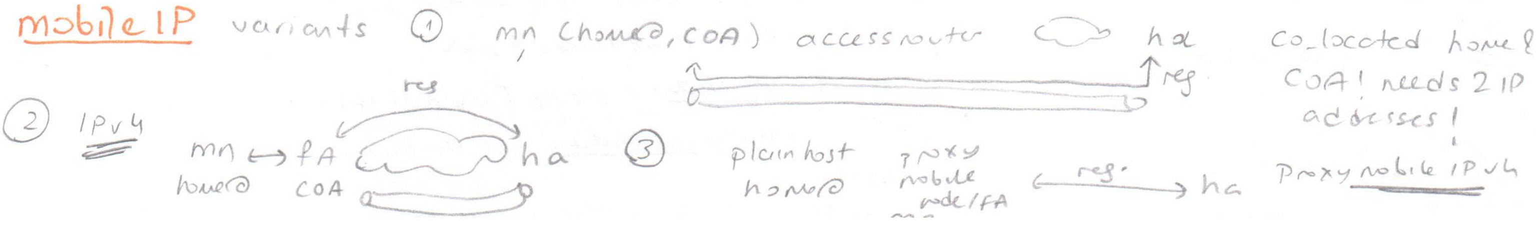
mobility L2 handover - micro (ASN), L3 handover macro (CSN)
transparent to CSN R3
R4 & R6
inter ASN intra ASN

candidate BSs tested & final set is conveyed to MS
HO action MOB-MSHO-IND reqa controlled uncont ENG-REQ
ms informs target BS for HO to executed

HO phases - ms decides HO target, HO preperation MOB_MS/BSHO_REQ

R4 (inter ASN) authenticator & DP in same ASN, R6 (intra ASN) auth stays DP stays
data path uzadı ⇒ CSN'e haber ver / rely on anchoring
R3 HO → authenticator stays in ASNGW1, DP moves to new & data path is new). signalling latency
(PM key is known only by ASN1)
solution: perform reauthentication new ms → pmk
flowlarda CMAC_key_Count update et! uncontrolled HO da context req + path + key count or do.

mobile IP variants



Co_located home & COA! needs 2 IP addresses!

Proxy mobile IPv4

plain host home@ — mobile access GW CoA ⟷ Bindng updat — Local mobility agent) PMIPv6

WimaX NWG supports CMIPv4 / v6, PMIPv4 / v6

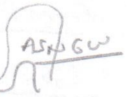
Auth + PMIPclient always co-located + FA in ASN1, DP in ASN2

reauthenticate ucuz olsun Auth + PMIP in ASN1, FA + DP in ASN3

Roaming ms connect internet via VCSN or HCSN acc to HNSP policy

VCSN proposes HA@ home@, HCSN approves or processes its own ad, it is deliverd to MS.

Localized routing



neden ASN verilmez – accounting, firewall, policy, lawful int.
ASN den. BS IP trafik handle edemez.

mpls tunnel 1) roaming de calismaz, 2) mobile IP ile heterogeneous networking yapabiliyoruz

on Demand anchoring IP1 → IP2 → .. devamli degisme, bir trafik basladiysa degis.

LTE → idle – cell sel. resel
→ active – ho → prepared & network controlled. source eNB selects target
X2 handover with no SGW reloc
" " " " "
S1 " " MME & " "
S1 " " " & no " "

S SGW — T SGW olmalı
SeNB — teNB

Availability mtbf / (mtbf + mttr)
one of KPI

99.999 0.001 5.25 min 6 sec.
99.9999 0.0001 31.5 sec 6.6 sec.

network failures → %17
system soft → %27
hardware → %23
human → %18

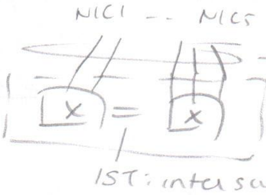
switch/route failure – multiple switch + routing
power supply – UPS, gen
cable – multiple cable
DNS/DHCP – " serv
human – automate! log
disaster – geolocation backup
client – NIC – multiple NIC
soft. hard. – high available platform

L2 1) Redundant network attach
assign virtual IP to NIC1 If it fails bind virtual IP to NIC2 → Gratuitous ARP ile.
sunl linuxlarda virtual IP bağlanır.

2) multi link trunking or link ag
802.3ad: link aggregation ethernet switch & host (client serv) should suppor.

if one of the links fail, others share traffic!) problem: switch capacity! what if it fails.

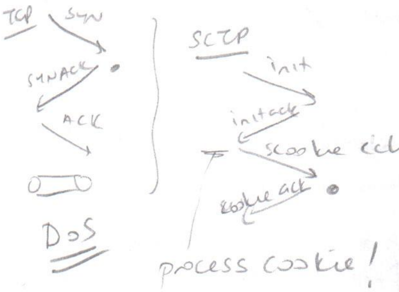
3) Split multi link trunking SMLT



L3 IP Layer Routing
If link fails its cost is ∞
RIP, OSPF var.

Good System Admin
Reliable Backup
Disk & Volume Man (RAID)
Network
Local environment (data)
Client man
Services & App
failovers
replication disaster rec.

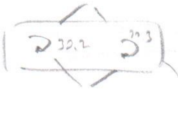
L4 SCTP stream control transfer protocol SCTP sits on IP & makes 2 IP addresses appear to application. new socket needed. SCTP de multiple streams, same connection



process cookie! burden on client.

physical box availability design

– router availability VRRP (virtual router redundancy protcol)
multiple routers have virtual router ids VRID
virtual IP addresses & mac
– serve av: serve farm dist on LAN & WAN
– high availability platform for end hosts.



master/slave, which is master, heartbeat
30.1 virtual router's virtual IP adders.