

Juhani Nuorteva

LTE-verkon toiminta paketti- ja käskeytasolla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinööryö

2.5.2014

Alkulause

Insinööri työ tehtiin Metropolia Ammattikorkeakoulun LTE-laboratoriolle. Työ perustui vahvasti sekä teoriaan että käytäntöön Wireshark-tietojen avulla, joista erityiskiitos kuuluu Ferenc Muskatalille. Suuri kiitos kuuluu myös insinööri työ valvojille Ville Jääskeläiselle, joka auttoi työn korjauksessa ja Jukka Honkaniemelle asiantuntevista neuvoista sekä insinööri työ kielellisistä korjauksista vastanneelle Jussi Alhorinteelle.

Helsingissä 2.5.2014

Juhani Nuorteva

Tekijä(t) Otsikko	Juhani Nuorteva LTE-verkon toiminta paketti- ja käskytasolla
Sivumäärä Aika	53 sivua + 1 liitettä 2.5.2014
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Ville Jääskeläinen Tuntiopettaja Jukka Honkaniemi
<p>LTE eli Long Term Evolution on mobiiliverkkotekniikka, joka on tullut jäädäkseen. Se tuo internetiä ja puhelinverkkoja lähemmäs toisiaan pakettipohjaisella liikenteellään ja tässä insinööriyössä tarkastellaankin LTE-verkon toimintaa tarkemmin Metropolia Ammattikorkeakoulun verkon mittakaavassa paketti- ja käskytasolla.</p> <p>Insinööriyössä tutkitaan aluksi Metropolia Ammattikorkeakoulun mittakaavassa olevaa LTE-verkon loogista rakennetta ja siihen kuuluvia verkkoelementtejä keskeisine tehtävineen. Tästä siirrytään tarkastelemaan käskyjä kuljettavia protokollapinoja ja niiden rakennetta sekä tehtävää eri verkkoelementtien välillä. Neljännessä kappaleessa työ laajentuu LTE-verkon toiminnan tarkasteluun käskytasolla, jossa käydään muun muassa päätelaitteen yhteyden salaus, rekisteröinti ja autentikointi sekä verkosta irtautumisen teoriaa kokonaisuudessaan. Työssä verrataan myös wiresharkista saatuja käytännön tuloksia LTE-verkon toiminnasta luvussa 5, jossa tutkitaan samalla tarkemmin protokollien kuljettamaa tietoa eri verkkoelementtien välillä.</p> <p>Työssä käytettiin paljon kirjoista ja internetistä saatua teoriapohjaa LTE-verkon toiminnasta, mutta wiresharkista saatujen tuloksien avulla työhön saatiin yhdistettyä myös käytäntö. Rajaus tehtiin aiheen laajuuden vuoksi, mutta insinööriyötä voidaan laajentaa tulevaisuudessa esimerkiksi LTE roaming -mittakaavaan tai tutkimalla radiorajapintaa tarkemmin pakettitasolla. Metropolian hiljattain valmistuneen LTE-verkon avulla työhön saatiin myös lisättyä mainintoja fyysisen ja loogisen verkkorakenteen välillä.</p> <p>Käytännön havaintojen kautta insinööriyö toimii apuna sekä perustana operaattorin verkon toiminnan ja kokonaisuuden hahmottamisessa. Lopputyön tarkoituksena on toimia myös ohjeena Metropolian LTE-laboratorioverkon toimintaan tutustuville opettajille ja oppilaille sekä antaa syvällistä käytännön tietoa, miten LTE-verkko toimii ja mitä tehtäviä jokaiselle verkkoelementille kuuluu.</p>	
Avainsanat	LTE, verkkoelementit, protokollat, käskyt, LTE verkon toiminnan teoria, Wireshark-käyttö.

Author(s) Title	Juhani Nuorteva LTE network operation in packet and command level
Number of Pages Date	53 pages + 1 appendices 2 May 2014
Degree	Bachelor of Engineering (B.Eng)
Degree Programme	Information Technology program
Specialisation option	Data Networks
Instructor(s)	Ville Jääskeläinen, Principal lecturer Jukka Honkaniemi, Visiting lecturer
<p>LTE also known as Long Term Evolution is mobile network technology that is here to stay. It brings the internet and mobile network closer together with packet based network traffic. In this thesis the main idea is to examine LTE network operation in packet and command level within the limits of Metropolia University of Applied Sciences LTE network.</p> <p>In this thesis the logical structure of LTE network and the main elements within the limits of Metropolia University of Applied Sciences network, were first examined. On this topic the thesis also focused on LTE protocol stacks, their structures and tasks between different network elements. Chapter four shows LTE network works in command level step by step. Topics such as user equipment registration, connection encryption, authentication procedure and de-registration are looked more closely. The thesis ends in chapter five where these commands are looked more thoroughly in packet level with the help of wireshark program.</p> <p>There is a lot of LTE theory information that was used from books and the internet, but with the help of wireshark captures from real life situations practical information was gathered. This thesis was made within the limits of Metropolia University of Applied Sciences LTE network because there was so much information about the topic in packet and command level. However this thesis can be expanded easily to LTE roaming or studying more the LTE-Uu interface packet level traffic between UE and eNodeB. Thanks to Metropolia's newly finished LTE network there was also a chance to look at some of the differences between physical and logical structure of the network.</p> <p>Through practical observation this thesis acts as a foundation for understanding how real operator's mobile networks work. The goal of this thesis is to be a manual for students and teachers when doing research about Metropolia's new LTE laboratory network. It also provides deeper knowledge of how LTE network works and what tasks different network elements have.</p>	
Keywords	LTE, network elements, protocols, commands, LTE network operation theory, wireshark analyze.

Sisällys

Lyhenteet

1	Johdanto	1
2	LTE-verkon looginen rakenne ja verkkoelementit	1
2.1	Verkkoympäristön rakenne	1
2.2	UE-verkkoelementti	4
2.3	eNodeB-verkkoelementti	4
2.4	Mobility Management Entity -verkkoelementti	5
2.5	Home Subscription Server -verkkoelementti	6
2.6	SAE-GW-verkkoelementti	7
3	LTE-verkon protokollat	8
3.1	Control Plane -yhteyden protokollapinon rakenne	9
3.2	User Plane -yhteyden protokollapinon rakenne	10
4	LTE-verkon toiminnan teoriaa	11
4.1	Päätelaitteen radiokaistan ajoituksen valinta ja RRC-yhteyden avaus	12
4.2	Päätelaitteen LTE-verkkoon liittyminen ja autentikointi	14
4.3	User Plane -tunneliyhteyden avaus	18
4.4	Päätelaitteen yhteyden muodostaminen LTE-verkkoon lepotilasta	21
4.5	Aktiivisen ja lepotilassa olevan päätelaitteen sammutus LTE-verkossa	24
4.6	LTE-verkkopalveluiden mainostus eli paging	26
5	LTE-verkon protokollien kuljettama tieto pakettitasolla	28
5.1	Wireshark-monitorointityökalu	29
5.2	MME:n ja HSS:n välillä	30
5.3	eNodeB ja MME:n välillä	33
5.3.1	Päätelaitteen käynnistäminen ja verkkoon liittyminen	33
5.3.2	Päätelaitteen siirtyminen aktiivtilasta lepotilaan	40
5.3.3	Päätelaitteen irtautuminen verkosta kokonaan	42
5.3.4	Verkon mainostus eli paging	45
5.4	SAE-GW ja MME:n välillä	45
6	Yhteenveto	52
	Lähteet	53

Liitteet

Liite 1. Metropolian LTE verkosta tehty rakennekuva fyysisistä laitteista

Lyhenteet

AMBR	Aggregate Maximum Bit-Rate. Suurin sallittu lataus tai lähetysohjeen tiedonsiirtonopeus.
APN	Access Point Name. Päätepiste GPRS-, 3G- tai 4G-pohjaisen verkon ja ulkoverkon eli internetin välillä.
AUTN	Authentication Token. Autentikointitunnus.
AVP	Attribute-Value Pairs. DIAMETER-protokollassa käytettävän datan esitysmuoto.
CCCH	Common Control Channel. Päätelaitteen yhteyden luonnissa käytettävä looginen kanava.
CGI	Cell Global Identity. Radiotukiaseman globaalitunniste.
CP	Control Plane. Signaalintyhteys.
C-RNTI	Cell Radio Network Temporary Identifier. RRC-yhteyden muodostuksessa käytettävä tunnistetieto.
DCCH	Dedicated Control Channel. Päätelaitteen yhteyden kontrolloinnissa käytettävä looginen kanava.
DRB	Data Radio Bearer. User Plane -signaalintyhteyden kuljettaja.
DRX	Discontinuous Reception. Mobiiliverkoissa käytetty metodi, jolla säästetään päätelaitteen akkua.
EBI	EPS Bearer Identity. EPS-verkon yhteyden identiteetti.
ECGI	EUTRAN Cell Global Identifier. EUTRAN – tukevan radiotukiaseman globaali tunniste.
EEA	EPS Encryption Algorithm. EPS-verkossa käytössä oleva salausalgoritmi.

eNodeB	E-UTRAN Node B. LTE-verkkotekniikkaa tukeva radiotukiasema.
EPC	Evolved Packet Core. LTE-verkon ydinalue, johon kuuluvat MME-, HSS-, S-GW ja P-GW-verkkoelementit.
EPS	Evolved Packet System. LTE-verkon arkkitehtuuri.
E-RAB	EUTRAN Radio Access Bearer. EUTRAN-radiosignaalin kantaja.
ESM	EPS Session Management. EPS-verkoalueen yhteyden hallinta.
E-UTRAN	Evolved Universal Terrestrial Radio Access Network. LTE-tekniikkaa tukevien radiotukiasemien alue.
FQDN	Fully Qualified Domain Name. Tarkennettu verkko-osoite.
F-TEID	Fully Qualified Tunnel Endpoint Identifier. Tarkennettu signalointitunnelin päätepisteen tunniste.
GPRS	General Packet Radio Service. Pakettikytkentäinen tiedonsiirtopalvelu.
GRE	Generic Routing Encapsulation. Ciscon kehittämä tunnelointiprotokolla.
GTP	GPRS Tunnel Protocol. GPRS-tunnelointiprotokolla.
GTP-C	GPRS Tunnel Protocol-Control plane. GPRS-tunnelointiprotokolla Control Plane -yhteyttä varten.
GTP-U	GPRS Tunnel Protocol-User plane. GPRS-tunnelointiprotokolla User Plane -yhteyttä varten.
GUMMEI	Globally Unique Mobility Management Entity Identifier. Tunnistetieto, jolla yksittäinen MME voidaan tunnistaa maailmanlaajuisesti.
GUTI	Globally Unique Temporary Identifier. Tunnistetieto, jolla päätelaite voidaan tunnistaa maailmanlaajuisesti.
HSS	Home Subscription Server. LTE-verkon käyttäjäprofiilien tietokanta.

ID	Identity. Identiteetti/tunniste.
IMSI	International Mobile Subscriber Identity. Puhelimen SIM-kortissa oleva tunnistetieto autentikointia varten.
K-ASME	Key Access Security Management Entity. Avain MME:lle.
K-eNB	Key for eNodeB. Avain eNodeB:lle.
K-NAS-enc	NAS layer encryption key. NAS-kerroksen salausavain.
K-NAS-int	NAS layer integrity protection key. NAS-kerroksen eheyden varmistusavain.
KSI-ASME	Key Selection Identifier Access Security Management Entity. Tämän avulla päätelaite saa valittua oikean K-ASME-avaimen.
LTE	Long Term Evolution. Tunnetaan kaupallisessa mediassa myös nimellä 4G.
MAC	Medium Access Control. Fyysisen kerroksen resurssien jako käyttäjälle.
MCC	Mobile Country Code. Puhelimen hallinoidun operaattorin verkkoaluekoodi.
MIP	Mobile IP. Päätelaitteen IP-osoite.
MME	Mobility Management Entity. Päätelaitteen tunnistamisesta LTE-verkkoon vastaava verkkoelementti.
MMEC	Mobility Management Entity Code. Yksittäisen MME:n tunnistetieto.
MMEGI	Mobility Management Entity Group Identifier. Yksittäisen MME:n ryhmätunnistetieto.
MMEI	Mobility Management Entity Identity. Tunnistetieto, jolla MME voidaan tunnistaa operaattorin sisäisestä verkosta.

MNC	Mobile Network Code. Puhelimen maakoodi.
Mo-data	Mobile originating data. Matkapuhelimesta tuleva data.
Mo-signaling	Mobile originating signaling. Matkapuhelimesta tuleva signaali.
MSISDN	Mobile Station International ISDN Number. Päätelaitteen puhelinnumero.
Mt-access	Mobile terminating access. Puhelimen yhteyden avaus.
M-TMSI	MME-Temporary Mobile Subscriber Identity. Tunnistieto, jolla voidaan tunnistaa, mihin MME-verkkoelementtiin päätelaite on yhteydessä.
NAS	Non-access stratum. Looginen yhteysprotokolla päätelaitteen UE ja eNodeB välisessä yhteydessä.
OFDMA	Orthogonal Frequency Division Multiple Access. Radioyhteydellä käytettävä digitaalinen modulaatio lataussuuntaan.
PCRF	Policy and Charging Resource Function. Laskutuksesta ja verkkokäytön oikeuksien jaosta vastaava verkkoelementti.
PDCP	Packet Data Convergence Protocol. Layer 2 -tason protokolla.
PDN	Packet Data Network. Pakettipohjainen verkko.
P-GW	Packet Data Network Gateway. Verkkoelementti, joka toimii yhteysankkurina EPC-runkoverkon rajalla.
PHR	Power Head Room. Kertoo, kuinka paljon päätelaitteella on vielä tehoa radiosignaalin vahvistamiseen.
PLMN	Public Land Mobile Network. Julkinen matkapuhelinverkko.
RACH	Random Access Channel. Radiosignaalin ajoitukseen käytettävä kanava.
RAND	Random Number. Satunnainen luku.

RA-RNTI	Random Access Radio Network Temporary Identifier. Random Access -vaiheen väliaikainen tunnistetieto.
RAT	Radio Access Technology. Radiotukiaseman ja päätelaitteen välillä käytettävä radiotekniikka.
RES	Authentication Result. Autentikoinnin tulos.
RLC	Radio Link Control. Radiolinkin kontrollointiin käytettävä protokolla.
RRC	Radio Resource Control. Radioresurssien kontrollointi.
S1AP	S1 Application Protocol. S1-sovellusprotokolla.
SAE	System Architecture Evolution. 3GPP:n määrittelemän LTE-ydinverkon standardinimitys.
SAE-GW	System Architecture Evolution Gateway. Verkkoelementeistä S-GW ja P-GW yhdessä käytettävä nimitys.
SC-FDMA	Single Carrier Frequency Division Multiple Access. Radioyhteydellä käytettävä digitaalinen modulaatio lähetyssuuntaan.
S-GW	Serving Gateway. UP-yhteyden tunnelointia kontrolloiva verkkoelementti.
SRB	Signaling Radio Bearer. Control Plane -radiosignaalin kantaja.
S-TMSI	SAE Temporary Mobile Subscriber Identifier. Tunnistetieto, jolla päätelaite voidaan identifioida operaattoriverkkotasolla.
TAC	Tracking Area Code. Seuranta-alue koodi.
TAI	Tracking Area Identity. Seuranta-alue-tunniste.
TEID	Tunnel Endpoint Identifier. Signaalintunnelin päätepisteen tunniste.
UDP	User Datagram Protocol. Yhteyden muodostuksessa ja tiedostojen siirrossa käytettävä protokolla.

UE	User Equipment. Käyttäjän päätelaite.
UL-SCH	Uplink Shared Channel. Jaettu lähetyslinkki kanava.
UP	User Plane. Datatunneliyhteys.
USIM	Universal Subscriber Identity Module. Älykortti matkapuhelimessa, joka sisältää muun muassa käyttäjän IMSI-tunnisteen.
XRES	Expected Authentication Result. Odotettava autentikoinnin tulos.

1 Johdanto

Long Term Evolution (LTE) verkko on tuttu monelle, vaikka termi ei ehkä sanoisi aluksi mitään, koska kaupallinen media mainostaa tätä tekniikkaa tutulla nimellä 4G. Ennen mobiiliverkko ja internet olivat kaksi eri asiaa, mutta LTE-tekniikka tuo näitä kahta asiaa yhteen. Jo nimi Long Term Evolution ilmaisee, että tätä tekniikkaa suunnitellaan pitemmälle aikavälille käytettäväksi kuin aiempia verkkosukupolven tekniikoita.

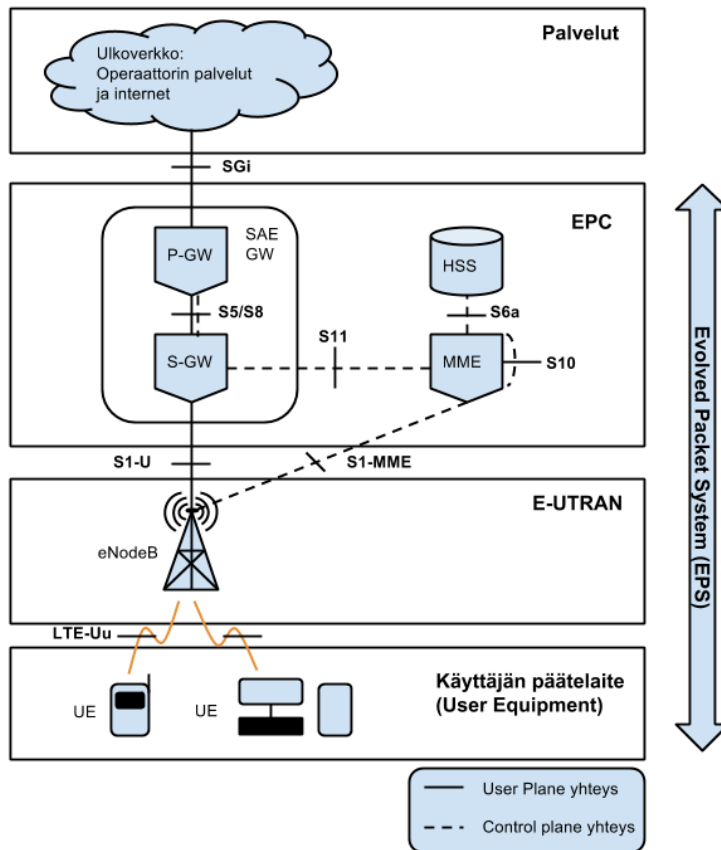
Tässä insinööriyössä pyritään ratkaisemaan teorian ja käytännön kautta, miten LTE-verkko toimii paketti- ja käskytasolla. Työ rajattiin Metropolia Ammattikorkeakoulun LTE-verkon mittakaavaan ja toteutettiin käyttämällä internetistä löytyvää teoriapohjaa sekä käytäntöä Wireshark-ohjelmasta saatujen paketti- ja käskytietojen avulla. Työssä esiintyvät kuvat ovat omia piirroksia lukuun ottamatta kuvia 2, 3, 4, 5, 8 sekä liitettä 1. Luvussa 2 kuvataan LTE-verkon keskeiset elementit ja niiden väliset rajapinnat. Näiden rajapintojen lähempää tarkastelua varten luvussa 3 käydään läpi tiedonkuljetuksesta vastaavat protokollapinot sekä User Plane- ja Control Plane -yhteydet erikseen tiedon kuljetuksessa. Luvussa 4 käydään LTE-verkon toiminnan teoriaa läpi sekä, mitä käskyjä eri laitteiden välillä liikkuu esimerkiksi päätelaitteen liittyessä verkkoon ensimmäistä kertaa. Luvussa 5 syvennytään lopuksi yksittäisten pakettien kuljettamaan tietoon ja rakenteeseen Evolved Packet Core (EPC) -verkkoalueella.

2 LTE-verkon looginen rakenne ja verkkoelementit

Metropolia Ammattikorkeakoululle rakennettiin noin vuosi sitten aito LTE-verkko. Tässä insinööriyössä rajataankin aihealue rakennettuun verkkoalueeseen. Seuraavissa luvuissa käydään läpi verkkoympäristön rakenne tarkemmin sekä eri verkkoelementit ja niiden väliset yhteydet.

2.1 Verkkoympäristön rakenne

Tässä insinööriyössä tarkastellaan kuvassa 1 esitettyä LTE-verkkoa pelkässä Evolved Packet System (EPS) -ympäristössä, koska Metropolian LTE-verkkoon ei kuulu kaikkia operaattoriverkon elementtejä. [1.]



Kuva 1: LTE-verkon looginen rakenne Metropolian mittakaavassa [vrt. 1, s.25].

LTE-verkko rakentuu tässä ympäristössä käyttäjän päätelaitteesta User Equipment (UE), joka on yhteydessä E-UTRA Node B (eNodeB) -radiotukiasemaan. Näiden välistä yhteyttä kutsutaan LTE-Uu:ksi ja radiotukiasemien välistä aluetta kutsutaan nimellä Evolved Universal Terrestrial Radio Access Network (E-UTRAN). [1.]

E-UTRAN-radiotukiasema alueesta siirrytään Evolved Packet Core (EPC) -runkoverkkoalueelle, josta löytyvät loppukäyttäjän autentikoinnista huolehtivat Mobility Management Entity- (MME) ja Home Subscription Server (HSS) -verkkoelementit. Loppukäyttäjän yhteyden reitityksestä internetiin tai operaattorin tarjoamiin palveluihin vastaavat Serving Gateway- (S-GW) ja Packet Data Network Gateway (P-GW) -verkkoelementit. Näistä kahdesta verkkoelementistä yhdessä käytetään nimeä System Architecture Evolution Gateway (SAE-GW). Metropolia Ammattikorkeakoulun LTE-verkossa ei ole Policy and Charging Resource Function (PCRF) -verkkoelementtiä, joka puuttuu siksi kuvasta 1. Tämän verkkoelementti olisi ollut vastuussa muun muassa laskutustietojen luovutuksesta P-GW:lle. Insinööriön liitteestä 1 voi tarkastella Metropolian LTE-verkon todellista verkkorakennetta tällä hetkellä. [1.]

Verkkoelementtien välillä kulkee kahdentyyppistä liikennettä: Control plane (CP) signalointiyhteys ja User Plane (UP) tunnelointiyhteys. Control Plane on näistä käyttäjän ensimmäiseksi muodostama yhteys, jolla hänet autentikoidaan ja rekisteröidään LTE-verkkoon. Vasta tämän jälkeen käyttäjä avaa User Plane -yhteyden, jonka avulla siirretään dataa käyttäjän päätelaitteen ja ulkoverkon välillä sekä käytetään operaattorin tarjoamia palveluja. Välivaiheet käsitellään tarkemmin luvussa 4.

Erilaiset signaaliyhteydet verkkoelementtien välillä:

- LTE-Uu on päätelaitteen UE ja radiotukiaseman eNodeB:n välillä kulkevaa radorajapintayhteys, jossa kulkee muun muassa Radio Resource Control (RRC) kuljetusprotokollayhteys. Non-access stratum (NAS) -yhteys kulkee osittain LTE-Uu- ja S1-MME -rajapinnan kautta päätelaitteen ja MME:n välillä. Näistä kahdesta yhteydestä on mainittu tarkemmin luvussa 3.1.1. [1.]
- S1-MME ohjaa Control Plane signalointiyhteyden protokollapinoa E-UTRANin ja MME:n välillä. Kuljetusprotokollana toimii S1 Application Protocol (S1AP), josta on tarkempi maininta kappaleessa 3.1. [11; 12.]
- S1-U ohjaa päätelaitteelta tulevaa User Plane -tunnelointiyhteyttä eNodeB:n ja S-GW:n välillä tai radiotukiaseman vaihdossa User Plane -tunnelointiyhteyden uudelleenreitityksestä päätelaitteelle. Kuljetusprotokollana toimii GPRS Tunnel Protocol-User plane (GTP-U), josta tarkempi maininta on luvussa 3.1. [11.]
- S5/S8 ohjaa liikennettä S-GW:n ja P-GW:n verkkoelementtien välillä. Periaatteessa S5- ja S8-yhteydet ovat yksi ja sama liittymä mutta erona on, että S5- User Plane -tunnelointiyhteys on verkonsisäinen, kun taas S8 Control Plane -signalointiyhteyttä käytetään muun muassa LTE roaming -verkkovierailussa kahden eri operaattoriverkon välillä. Metropolian verkossa ei ole aiemmin mainittua PCRF-verkkoelementtiä, joten tässäkin yhteydessä kuljetusprotokollana toimii pelkästään GPRS Tunnel Protocol-User plane (GTP-U) ja GPRS Tunnel Protocol-Control plane (GTP-C). [11; 14; 18.]
- S6a ohjaa päätelaitteen autentikointiin liittyvää liikennettä MME- ja HSS - verkkoelementtien välillä. [11.]

- S10-yhteys on kahden MME-verkkoelementin välistä yhteyttä varten. Metropolian LTE-verkossa on vain yksi MME, joten S10-yhteys ei ole käytössä. [11.]
- S11 ohjaa MME:n ja S-GW:n välistä kontrolliyhteyttä. [11.]
- SGi ohjaa User Plane tunneliyhteyttä P-GW:n ja ulkoverkon välillä. [11.]

2.2 UE-verkkoelementti

User Equipment (UE) on loppukäyttäjän päätelaite, jolla muodostetaan yhteys Metropolia Ammattikorkeakoulun LTE-verkkoon. Se voi olla tässä tapauksessa LTE-yhteysvalmiudella varustettu puhelin tai tietokone, jossa on 4G-modeemi (mökkula). LTE-yhteyttä varten käyttäjällä on oltava USIM-kortti, jonka avulla autentikointi UE:n ja MME-verkkoelementin välillä voidaan tehdä. [1.]

UE-päätelaite vastaa yhteyden muodostamisesta, ylläpitämisestä ja katkaisusta eNodeB-radiotukiaseman välillä tarpeen mukaan. Laite voi myös sisältää valmiudet tavallisen VoIP-puhelun avaamiseen esimerkiksi Skype-ohjelman avulla. Käytännössä Metropolialla on tällä hetkellä 4G-modeemilla varustettu testitietokone, johon voidaan avata etäyhteys päätelaitteen UE:n ja eNodeB:n välistä pakettiliikennettä tarkasteltaessa. [1.]

2.3 eNodeB-verkkoelementti

eNodeB on radorajapinnasta vastaava radiotukiasema, joka huolehtii sekä autentikointi liikenteestä (CP) ja käyttäjän palveluyhteydestä (UP). Isommissa operaattorien LTE-verkoissa radiotukiasemia on enemmän kuin yksi ja niiden välistä yhteyttä kutsutaan X2. Kuvassa 2 on esitetty eNodeB:n keskeiset tehtävät eri verkkoelementtien välillä. [1.]

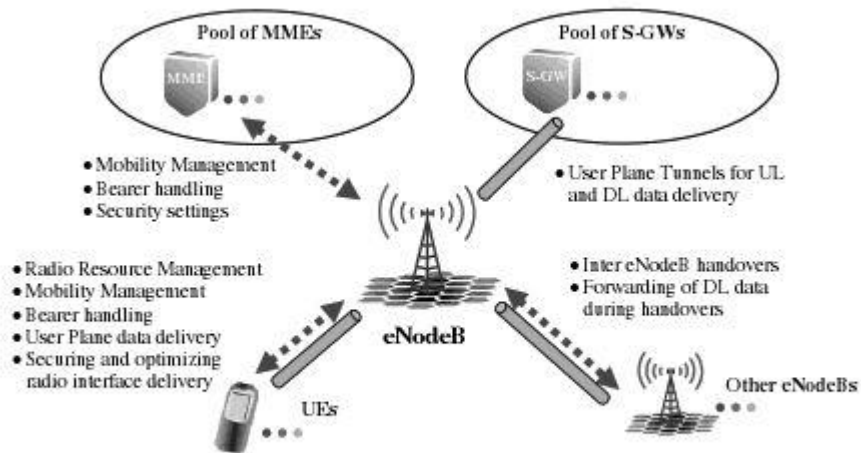


Figure 3.3 cNodeB connections to other logical nodes and main functions

Kuva 2: eNodeB-radiotukiaseman tehtävät eri verkkoelementtien välillä [1, s.28].

Radiotukiasemalla on keskeinen rooli LTE-verkossa. Tätä on havainnollistettu kuvassa 2. Lyhyesti kuvan 2 putki kuvaa UP-tunneliyhteyttä ja katkoviiva CP-signaalintyhteyttä. Päätelaitteen UE välisessä yhteydessä eNodeB:n tehtävänä on huolehtia radioresurssien hallinnasta, puhelimen paikannuksesta ja mobiilipalveluiden tarjoamisesta, handover-vaihdosta toisten eNodeB-radiotukiasemien välillä, UP-datayhteyden käsittelystä sekä radorajapinnan salauksesta että optimoinnista. [1; 6.]

EPC-runkoverkon verkkoelementtien välillä eNodeB:llä on monia tehtäviä. eNodeB ohjaa muun muassa autentikointi liikennettä (CP) UE:n ja MME:n välillä, kun käyttäjä pyytää lupaa rekisteröityä LTE-verkon käyttäjäksi. Tähän kuuluu myös salausavainosien jako, josta kerrotaan tarkemmin luvussa 4.2. Radiotukiasema eNodeB ottaa myös selvää vaihtoehtoisesta MME-verkkoelementistä, mikäli päätelaitetta aiemmin palvellut ei vastaa pyyntöihin enää. Päätelaitteen rekisteröityessä onnistuneesti LTE-verkkoon eNodeB avaa myös UP-tunneliyhteyden S-GW-verkkoelementin välille internetyhteyttä varten. [1.]

2.4 Mobility Management Entity -verkkoelementti

Mobility Management Entity (MME) toimii EPC-runkoverkon kontrollikeskuksena, ja sen kautta kulkee pelkästään CP-yhteys. Kuvassa 3 on esitetty MME-tehtävät eri verkkoelementtien välillä.

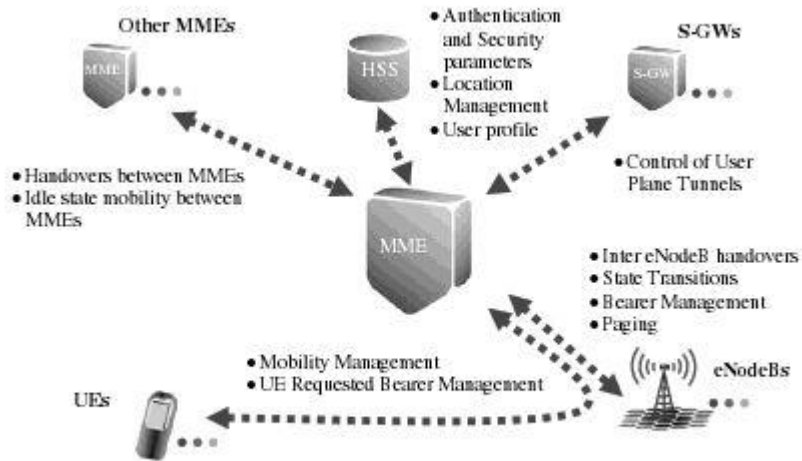


Figure 3.4 MME connections to other logical nodes and main functions

Kuva 3: MME:n tehtävät eri verkkoelementtien välillä [1, s.30].

Yksi MME:n tärkeimmistä tehtävistä on päätelaitteen UE autentikointi ja rekisteröinti LTE-verkkoon, jossa tarvitaan yhteyttä HSS-tietokantaan verkkokäyttäjistä. MME ottaa aluksi selvää rekisteröityvästä käyttäjästä autentikointihaasteella. Tämän jälkeen se vertaa päätelaitteen UE autentikointivastausta HSS:ltä saatujen tietojen kanssa, jonka jälkeen MME kysyy vielä HSS:ltä verkkoalueen käyttöluvan päätelaitteelle UE. Lopulta näiden välivaiheiden jälkeen MME lähettää vahvistuksen, että käyttäjä voi avata data yhteyden UP yhteystunnelin avulla. MME:n tehtävänä on myös kertoa päätelaitteen UE paikannustiedot niiden vaihtuessa. Tämä kuvaa MME:n ja HSS:n välistä yhteyttä kuvassa 3. [1.]

MME:llä on myös yhteys S-GW:hen, joka on User Plane -yhteystunnelin kontrollointia varten. MME huolehtii myös salausavaimien jaosta, jotta yhteys on suojattu ja turvallinen käyttäjälle. Salausavaimien jaosta käydään tarkemmin luvussa 4.2. [1.]

2.5 Home Subscription Server -verkkoelementti

HSS toimii LTE-verkon käyttäjäprofiilien arkistona. Se säilyttää myös tiedot mihin operaattorin tarjoamiin palveluihin päätelaitteella on käyttöoikeus. Tästä esimerkkinä on, ovatko verkkovierailut muiden maiden operaattoriverkossa sallittuja ja onko käyttäjällä puhelinyhteyden lisäksi datayhteys oikeus. Tämän lisäksi HSS:llä pitää olla suora yhteys kaikkiin muihin MME-verkkoelementteihin, joihin loppukäyttäjällä UE on

verkkovierailuoikeus. Se on tärkeää tilanteessa, kun uusi MME ilmoittaa HSS:lle olevansa vastuussa UE-käyttäjän yhteydestä ja autentikoinnista. HSS tietää silloin sulkea yhteyden aiemmin käytettyyn MME-elementtiin. [1.]

2.6 SAE-GW-verkkoelementti

SAE-GW koostuu Metropolialla kahdesta eri verkkoelementistä: S-GW:stä ja P-GW:stä. Todellisuudessa nämä verkkoelementit on virtualisoitu ja yhdistetty Metropolian verkkototeutuksessa yhteen fyysiseen laitteeseen. Ne on silti hyvä nähdä kahtena eri asiana. S-GW eli Serving Gateway on näistä ensimmäinen, jonka tehtävänä on kontrolloida UP-yhteyden tunnelointia. Sillä on myös muita tärkeitä ominaisuuksia isommassa operaattoriverkossa, mutta Metropolian LTE-verkon tämän hetkisen toiminnan kannalta se vastaa UP yhteystunnelin kontrolloinnista. [1.]

UP-yhteys jatkaa tästä eteenpäin P-GW:lle eli Packet Data Network Gatewaylle, joka toimii eräänlaisena yhteysankkurina EPC-runkoverkon rajalla ja on yhteydessä ulkoverkossa sijaitsevaan DHCP-palvelimeen. P-GW:n tehtävänä on jakaa päätelaite UE:lle EPS-verkkoalueen sisäinen IP-osoite sekä yhdistää ulkoverkosta saatu IP-osoite UE päätelaitteelle datatunneliyhteyden avauksen jälkeen (User Plane). Näin päätelaite voidaan tunnistaa myös ulkoverkosta eli internetistä. Tämä toteutetaan aina, kun käyttäjä haluaa avata datayhteyden. [1.]

3 LTE-verkon protokollat

Tarkemmin tarkasteltuna LTE-verkossa EPS-alueella tietoa ja käskyjä kuljetetaan protokollapinojen avulla sekä Control Plane- että User Plane -yhteyksissä. Ne muistuttavat hyvin paljon tuttuja internetissä käytettäviä protokollia, mutta eroja syntyy etenkin kolmannen ja neljännen kerroksen protokollissa. Seuraavana on kuvattu tarkemmin, mitä eri protokollapinot sisältävät kerroksittain tarkasteltaessa:

- Fyysinen kerros (Physical Layer): Tämä kerros sisältää fyysisen radiosignaalin kuljettamat bittitiedot. Radiotukiaseman ja päätelaitteen välillä näitä tekniikoita on kahta erilaista: OFDMA-lataussuuntaa varten ja SC-FDMA-lähetys-suuntaa varten. Latauksella tarkoitetaan käyttäjälle päin tulevaa yhteyttä ja lähetyksellä käyttäjältä pois päin kulkevaa liikennettä. [20.]
- MAC kerros: Medium Access Control -protokolla kuljettaa tiedot sekä lähettäjän että kohteen MAC-osoitteesta. MAC-kerros vastaa siitä, kuinka fyysisen kerroksen resurssit annetaan käyttäjälle. [20.]
- RLC: Radio Link Control -protokolla huolehtii radioyhteyden laadusta ARQ:n (Automatic Retransmission on reQuest) avulla. Tämän lisäksi se segmentoi ja kokoaa tietoa uudestaan tarvittaessa ylemmiltä protokollapinon kerroksilta. [20.]
- PDCP: Layer 2 -tason Packet Data Convergence Protocol (PDCP) -protokollaa käytetään sekä käyttäjän avaamassa User Plane -yhteydessä että Control Plane -yhteydessä RRC-protokollan kanssa. PDCP:tä käytetään kaiken liikenteen siirtämisessä, ja se vastaa muun muassa salauksesta ja siitä, että radorajapinnan paketit tulevat oikeassa järjestyksessä.
- Network layer IP: Kuljettaa päätelaitteen LTE-verkon EPS-alueella olevaa sisäistä IP-osoitetta.
- RRC: Radio Resource Control kuljetusprotokolla kuljettaa tietoa UE ja eNodeB:n signalointiyhteyden välillä. Sen tehtäviin kuuluu muun muassa kuljettaa autentikointitietoja käyttäjän rekisteröityessä LTE-verkkoon. [20.]
- NAS: Non-access stratum -protokolla on päätelaitteen UE ja verkkoelementin MME välistä loogista yhteyttä varten. Tämä protokolla kuljettaa tietoa muun muassa autentikoinnista, turvallisuusasetuksista sekä EPS-verkon läpi tulevan signalointitunnelin tiedot. [20.]
- SCTP: Yhteydellinen protokolla kuten TCP mutta on optimoitu yksittäisten signalointiviestien kuljettamiseen. Käytetään vain Control Plane -yhteydessä.
- S1AP: Tätä protokollaa käytetään Control Planen yhteydessä tiedon kuljetusprotokollana radiotukiasema eNodeB:n ja MME:n välillä.

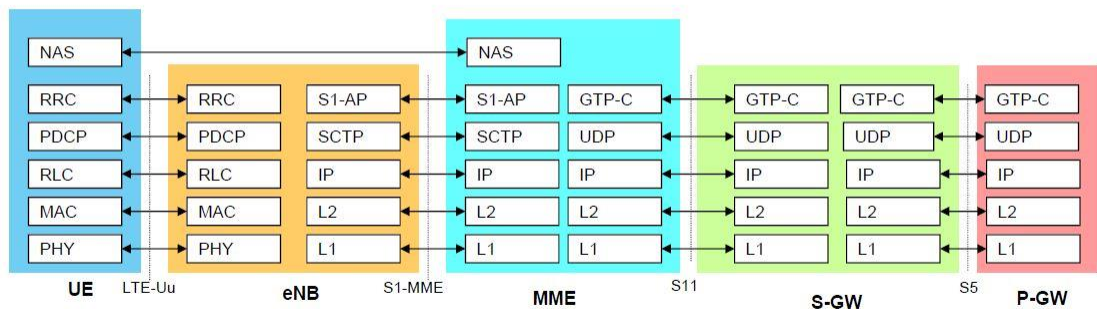
- UDP: User Datagram Protocol sisältää sekä viestin lähettäjän että kohteen porttitiedot. [43.]
- GTP-C/GTP-U: Nämä protokollat kuljettavat tietoa suurimmaksi osaksi MME-, S-GW- ja P-GW-verkkoelementtien välillä mutta GTP-U toimii tämän lisäksi myös radiotukiasema eNodeB:n ja MME:n välissä. Wiresharkilla tarkasteltaessa nämä kaksi protokollaa tunnetaan LTE-verkossa nimellä GTPv2 ja vanhemman mobiiliverkko sukupolven tekniikassa pelkällä nimellä GTP.

Seuraavissa luvuissa katsotaan tarkemmin, millaisia protokollapinoja näistä muodostuu Control Plane- ja User Plane -yhteyksissä. [4; 20.]

3.1 Control Plane -yhteyden protokollapinon rakenne

Control Plane on ensimmäinen yhteys, jonka käyttäjä avaa ennen kuin hän pääsee käyttämään LTE-verkon datapalveluja. Kuvassa 4 on esitetty Control Plane -yhteyden protokollapinojen rakenne eri verkkoelementtien välillä.

Protocol Stacks: Control Plane

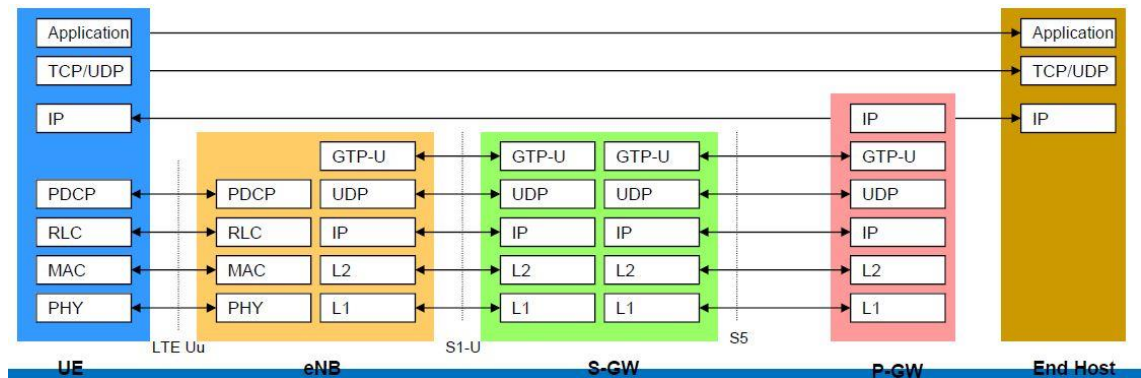


Kuva 4: Control Plane -yhteyden protokollapinot eri verkkoelementtien välillä [18, kalvo 8.].

CP-yhteydessä tärkeänä osana ovat kuljettajaprotokollat RRC/NAS, S1AP/NAS ja GTP-C. RRC kuljettaa tietoa päätelaitteen UE ja radiotukiasema eNodeB:n välillä. Se sisältää myös myöhemmissä vaiheissa NAS-yhteysprotokollan tiedot MME:n välillä. S1AP-kuljetusprotokolla kuljettaa tietoa radiotukiaseman ja MME-verkkoelementin välillä. Tarkemmin tarkasteltuna myöhemmässä luvussa 5 huomataan, että NAS-yhteyden tiedot ovat S1AP-protokollan sisällä. GTP-C-kuljetusprotokolla toimii verkkoelementtien MME, S-GW ja P-GW välillä.

3.2 User Plane -yhteyden protokollapinon rakenne

User Plane -yhteys muistuttaa aiemman kappaleen protokollapinon rakennetta mutta siinä on kuitenkin selviä eroja. Kuvassa 5 on esitetty User Plane -yhteyden protokollapinon rakenne.

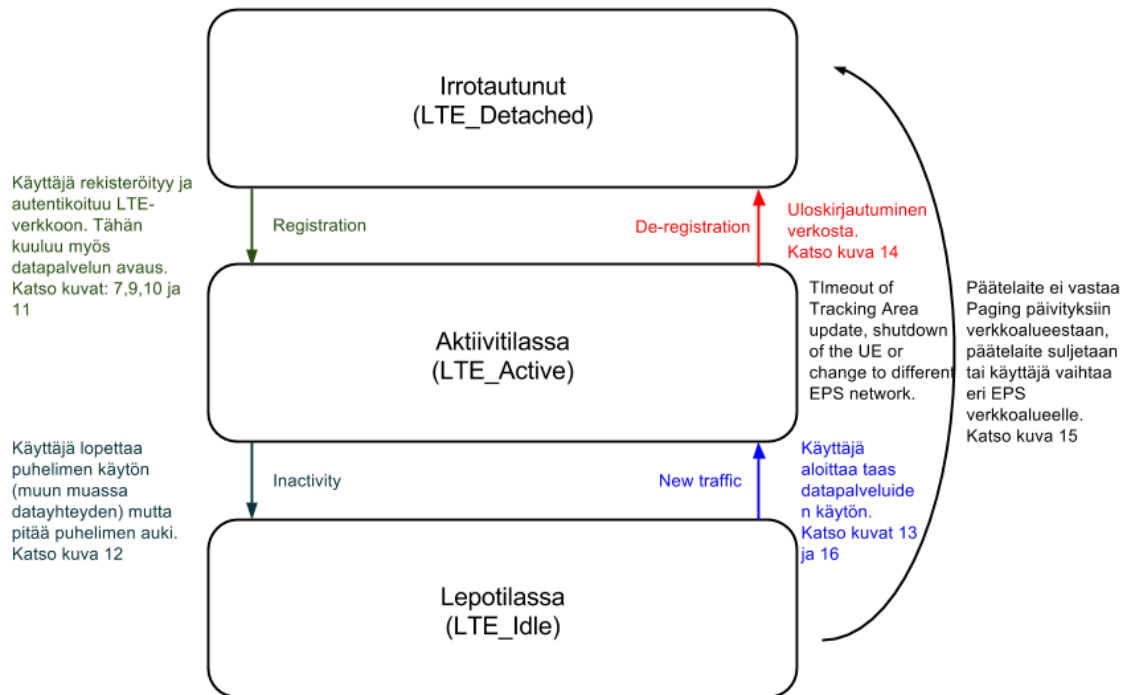


Kuva 5: User Plane -yhteyden protokollapinot eri verkkoelementtien välillä [18, kalvo 9].

Päätelaitteen ja eNodeB:n väliltä tuttua RRC-protokollaa ei ole User Plane -yhteydessä vaan Layer 2 -tason PDCP-protokollan jälkeen pinossa tulee ulkoverkon IP-osoite, TCP/UDP ja sovelluskerros. Tästä eteenpäin GTP-U-protokolla hoitaa käyttäjän datayhteyden tiedon kuljetuksen kaikkien muiden verkkoelementtien välillä ennen kuin paketti ohjataan ulkoverkkoalueen palveluntarjoajalle, mikä on kuvassa nimellä End Host. LTE-verkon User Plane -yhteyden protokollapinot on myös suunniteltu kuljettamaan kahta IP-osoitetta. Kuvassa kolmannella tasolla oleva sisäinen IP-osoite on päätelaitteen EPS-verkkoalueen tunnistamista varten, kun taas ylemmällä tasolla oleva IP-osoite on päätelaitteen ulkoverkosta tunnistamista varten.

4 LTE-verkon toiminnan teoriaa

Kuljetusprotokollien jälkeen tässä luvussa käydään läpi päätelaitteen yhteyden muodostaminen LTE-verkkoon ja mitä tapahtuu käskytasolla. Viitaten lähteeseen [34] on tärkeää huomata, että välivaiheita voi olla enemmänkin oikeassa LTE-verkossa.



Kuva 6: LTE-päätelaitteen eri tilat verkossa. [vrt. 11, s 8.]

Tässä kappaleessa kerrotaan yksityiskohtaisesti, millä tavalla päätelaite rekisteröityy LTE-verkkoon ja mitä tapahtuu sen jälkeen. Kuvassa 6 käyttäjän rekisteröitymistä aktiivtilaan LTE-verkossa kuvataan luvuissa 4.1, 4.2 ja 4.3. Seuraavassa luvussa 4.4 käyn läpi tässä insinööriyössä miten päätelaite joutuu lepotilaan ja miten lepotilasta palataan takaisin aktiivtilaan. Luvussa 4.5 käsitellään puhelimen sammutukseen liittyvät verkkotapahtumat ja viimeisessä kappaleessa 4.6 käyn läpi LTE-verkon mainostuksen eli paging-vaiheen, jossa keskitytään kuvassa mustalla nuolella kuvattuun verkkotilanvaihtoon.

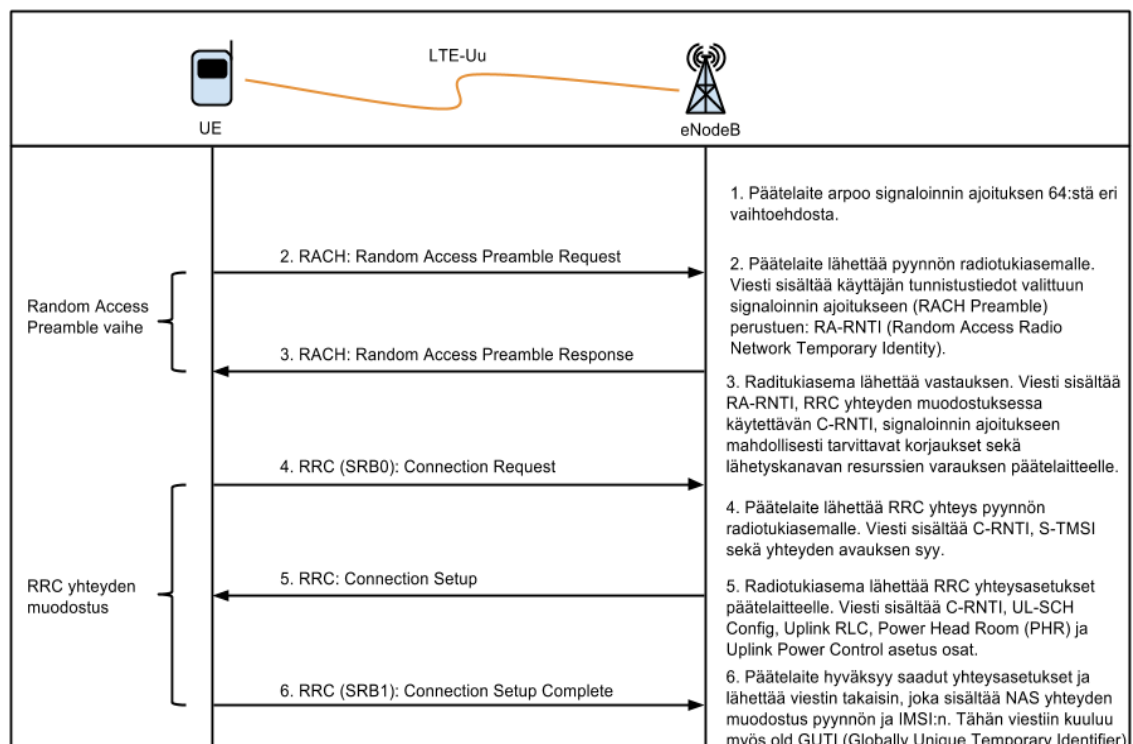
Piirretyissä kaavioissa esiintyy myös Signaling Radio Bearers (SRB) -merkintä. Nämä ovat radiosignaalin kantajia, joita käytetään vain RRC ja NAS -viesteissä Control Plane-yhteydessä. Ne voidaan jakaa kolmeen eri osaan:

- SRB0: Käytetään RRC-radorajapinnan viesteissä Common Control Channel (CCCH) loogisella kanavalla.
- SRB1: Käytetään NAS-viestien lähetykseen Dedicated Control Channel (DCCH) loogisella kanavalla.
- SRB2: Käytetään tärkeissä RRC-viesteissä (high priority) DCCH loogisella kanavalla. [26.]

Tämän lisäksi kuvassa 9 mainitaan Data Radio Bearer (DRB), joka toimii taas User Plane -signaaliyhteyden kuljettajana.

4.1 Päätelaitteen radiokaistan ajoituksen valinta ja RRC-yhteyden avaus

Ennen kuin päätelaite pääsee avaamaan yhteyttä EPC-verkkoalueelle ja rekisteröitymään käyttäjäksi, sen on avattava aluksi yhteys radiotukiaseman eNodeB:n välille. Tähän kuuluu Random Access Preamble ja RRC-yhteyden avaus vaihe, jotka on esitetty kuvassa 7.



Kuva 7: Random Access Channel vaihe ja RRC yhteyden muodostaminen. [vrt. 16; 18; 22.]

LTE-verkossa on paljon päätelaitekäyttäjiä, joten ensimmäisessä vaiheessa UE:n pitää arvioida signaalin muodostuksen ajoitus. Signaalin ajoituskohtia on yhteensä 64, joista UE:n on arvottava yksi. Toisessa vaiheessa kuvassa päätelaite lähettää Random Access Preamble -pyynnön radiotukiasemalle perustuen valittuun signaalin ajoitukseen. Tässä vaiheessa jos jollain muulla päätelaitteella on samaan aikaan ajoitettu signaali päätelaitteen Random Access Preamble -pyynnön lähetyksessä, nämä haastepyynnöt törmäävät toisiinsa ja päätelaitteen on valittava toinen signaalin ajoituskohta ja lähetettävä haaste uudelleen. Signaloinnin ajoitus perustuu radiotukiasemissa käytettyyn Zadoff-Chu-sekvenssiin. [17; 19; 21; 22; 23.]

Kolmannessa vaiheessa radiotukiasema lähettää vastauksen Random Access Preamble -kyselyyn. Vastaus sisältää päätelaitteen oman Random Access Radio Network Temporary (RA-RNTI) -tunnistetiedon, RRC-yhteyden muodostuksessa käytettävän C-RNTI (Cell Radio Network Temporary Identifier) -tunnisteen, signaloinnin ajoitukseen mahdollisesti tarvittavat korjaukset johtuen päätelaitteen ja radiotukiaseman välisestä etäisyydestä (round trip delay) sekä vaihtoehtoisesti (Uplink Grant Resources) lähetyiskanavan resurssien varauksen päätelaitteelle Uplink Shared Channel (UL-SCH) lähetyisyhteyttä varten. [17; 19; 21; 22; 23; 24.]

Random Access Preamble -vaiheen jälkeen päätelaite siirtyy RRC-yhteyden avaamiseen radiotukiaseman välille. Tässä neljännessä vaiheessa päätelaite lähettää RRC-yhteyspyynnön käyttäen aiemmin saatua väliaikaista tunnistetietoa C-RNTI - radiotukiaseman kanssa. Tämän lisäksi viesti sisältää päätelaitteen SAE Temporary Mobile Subscriber Identity (S-TMSI) -tunnistetiedot runkoverkolle ja yhteyden muodostamisen syyn. Yhteyden muodostamisessa prioriteettivaihtoehdot ovat: 1. Häätöpuhelu (Emergency call) 2. Korkean prioriteetin liikenne (High priority access) esimerkiksi tavalliset puhelut 3. Käyttäjän tunnistautuminen ja rekisteröityminen verkkoon (Mt-access) 4. Control Plane signaaliyhteys runkoverkkoon (Mo-signalling) esimerkiksi päätelaitteen paikantamista varten 5. User Plane -datatunnelyhteys operaattorin tarjoamiin internetpalveluihin (Mo-data). Radiotukiasema tunnistaa RRC-pyyntö (SRB0) ja siirtyy viidenteen vaiheeseen. Radiotukiasema lähettää RRC-yhteyden asetukset päätelaitteelle. Viesti sisältää myös muun muassa asetus osat UL-

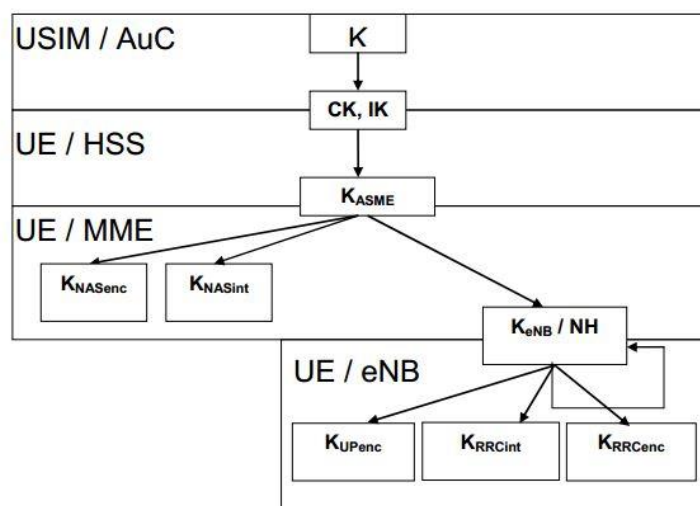
SCH Config, Uplink RLC, Power Head Room (PHR) ja Uplink Power Control. [17; 19; 21; 22; 23; 24; 25.]

Viimeisessä vaiheessa päätelaite vastaanottaa RRC-yhteysasetukset radiotukiasemalta ja lähettää vastauksen, joka sisältää pyynnön avata NAS-yhteyden ja old Globally Unique Temporary Identifier (old GUTI) -tunnistetiedon, jonka avulla radiotukiasema valitsee seuraavassa autentikointivaiheessa uuden MME:n sekä päätelaitteen IMSI tiedot. Tämän radiosignaalinviestin kantajana toimii SRB1, ja viesti sisältää vaihtoehtoisesti tämän lisäksi old Globally Unique Mobility Management Entity Identifierin (old GUMMEI), jonka avulla uusi MME pystyy päättelemään aiemmin käytössä olleen MME:n ja kysyä siltä HSS:n sijaan salausavaintiedot. Tässä tapauksessa viesti ei kuitenkaan sisällä vielä tietoa päätelaitetta aiemmin palvelleesta MME:stä (old GUMMEI), koska käyttäjä rekisteröityy LTE-verkkoon ensimmäistä kertaa. LTE roamingissa jos päätelaite siirtyisi toiselle verkkoalueelle old GUMMEI olisi mukana viestissä. [17; 19; 22.]

4.2 Päätelaitteen LTE-verkkoon liittyminen ja autentikointi

Tästä eteenpäin alkaa päätelaitteen autentikointi ja muun muassa salausvaihe, joten sitä ennen on aluksi katsottava, miten salausavainhierarkia toimii LTE-verkossa. Tämä on esitetty kuvassa 8.

- **ASME = Access Security Management Entity, located at the MME**

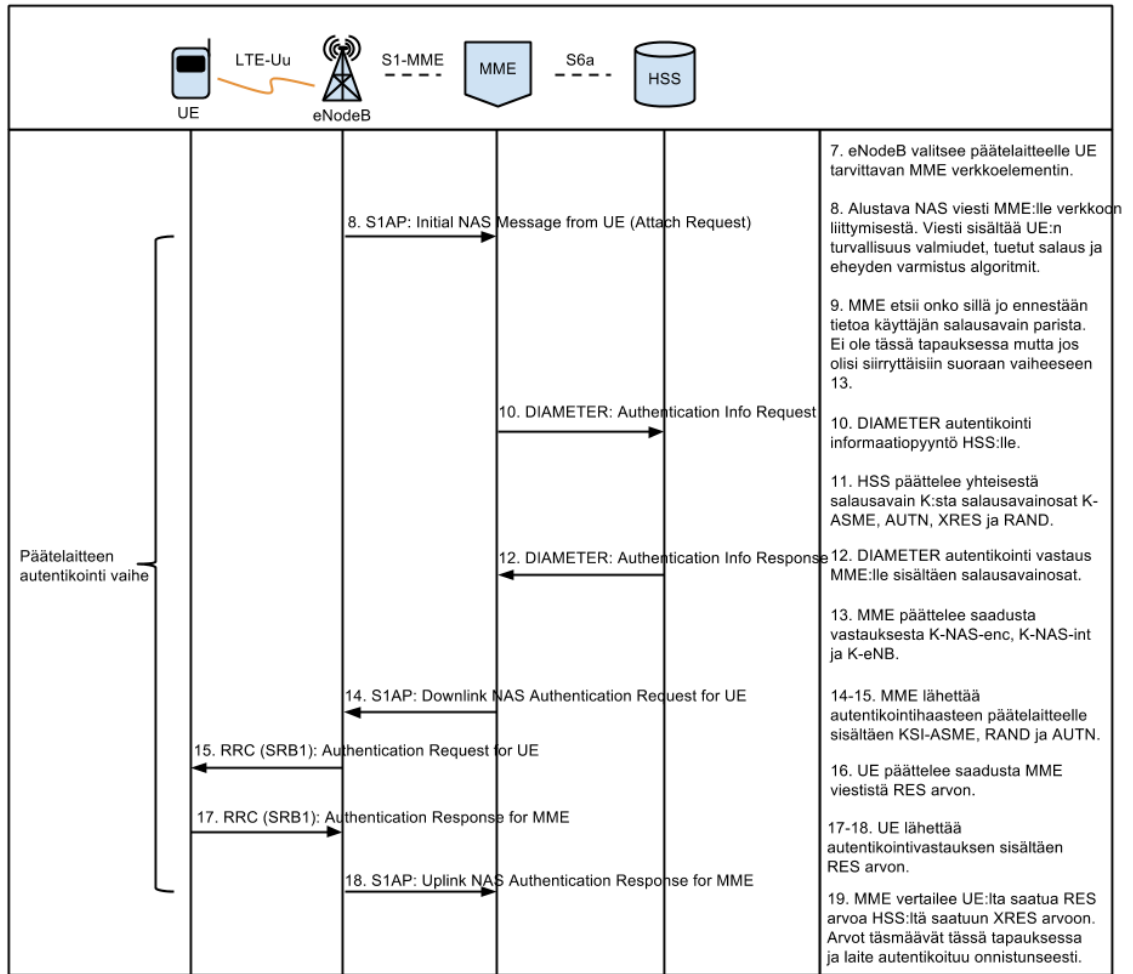


Kuva 8: LTE-salausavain K:n hierarkia Irfan Alin kalvosarjasta. [17.]

Käyttäjän tullessa operaattoriasiakkaaksi LTE-yhteysvalmiudella hän saa salausavaimella K ohjelmoidun USIM-kortin päätelaitettaan varten. K viittaa tässä tapauksessa englanninkieliseen sanaan Key. Tästä hetkestä lähtien USIM-kortilla varustetulla päätelaitteella sekä HSS-verkkoelementillä on silloin olemassa yhteinen salausavain K, jota käytetään myöhemmin asiakkaan autentikoinnissa LTE-verkkoon. [9.]

Tarkasteltaessa HSS:lle ja UE:lle valittua salausavain K:ta se koostuu tarkemmin kahdesta avainosasta, jotka ovat Cyphering Key (CK) ja Integrity Key (IK). Suomeksi kyseessä on salausavain K ja eheyden varmistusavain K. Eheyden varmistuksella suojellaan käyttäjää man in the middle -hyökkäyksiltä, jossa kolmannen osapuolen kautta kulkenut paketti olisi tutkittu ennen saapumista päämääräänsä. Eheyden varmistuksessa tämä huomataan, koska paketin rakenne on silloin muuttunut. HSS muuntaa salausavaimen K muotoon K-ASME Mobile Management Entityä varten verkkokäyttäjän autentikoinnissa. MME jakaa K-ASME-salausavainosan kolmeen eri osaan, joita ovat K-NASenc, K-NASint ja K-eNB. Näistä kaksi ensimmäistä osaa on NAS-yhteyden salauksen ja eheyden varmistamiseen tarvittavia avaimia, ja K-eNB toimitetaan radiotukiasemalle eNodeB:lle nimensä mukaisesti. Radiotukiasema jakaa saadun K-eNB-salausavainosan vielä kolmeen salausavainosaan K-UPenc, K-RRCint ja K-RRCenc. Ensimmäistä salausavainosaa käytetään User Plane -yhteyden salauksen varmistukseen ja kahta jälkimmäistä salausavain osaa käytetään RRC-radiolinkin salaukseen ja eheyden varmistamiseen päätelaitteen UE ja radiotukiasema eNodeB:n välillä. [16; 17.]

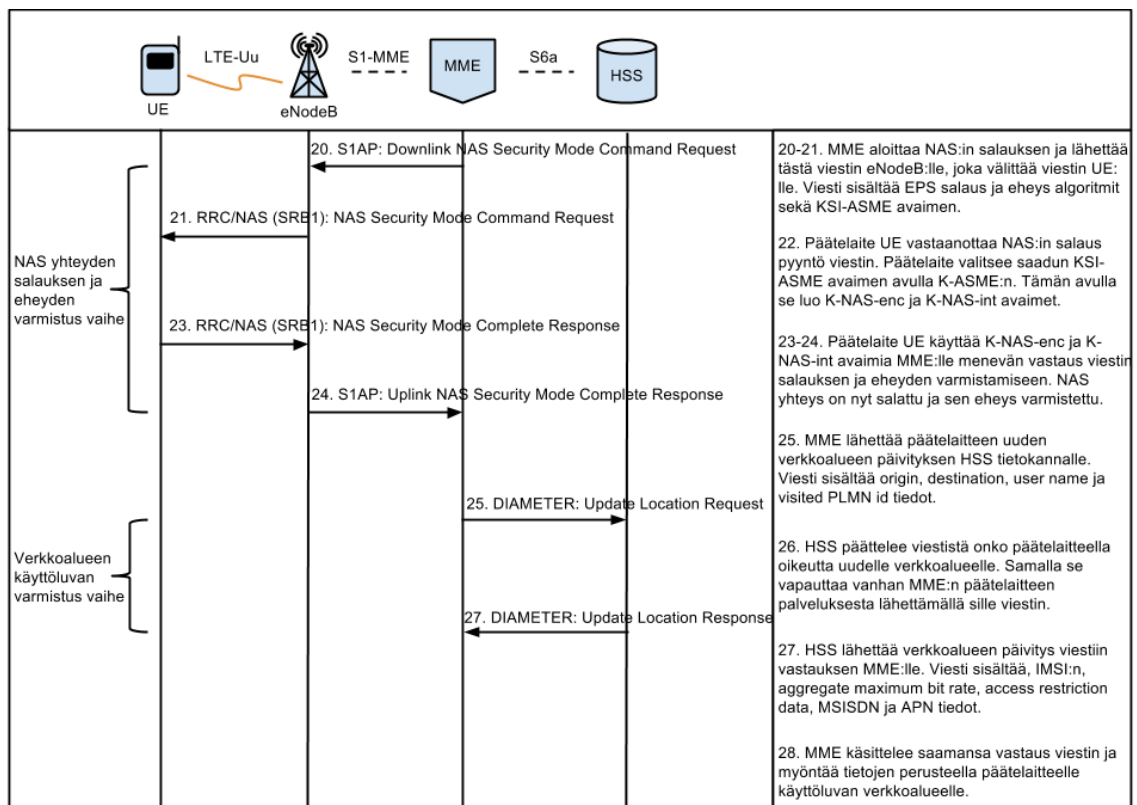
Tämän hierarkia esittelyn tarkoituksena on toimia apuna, kun seuraavaksi tässä insinööriyössä käydään läpi muun muassa päätelaitteen autentikointi ja NAS sekä AS yhteyksien salauksen ja eheyden varmistus salausavain K hierarkia ideaa käyttäen. Autentikointi vaihe on esitetty kuvassa 9.



Kuva 9: Päälaitteen autentikointivaihe runkoverkon kanssa [vrt. 9; 17; 19].

USIM-kortilla varustettu päätelaite UE on jo aiemmin avannut RRC-yhteyden radiotukiaseman välillä luvussa 4.1. Tästä hetkestä lähtien radiotukiasema lähettää alustavan NAS-viestipyynnön MME-verkkoelementille. MME tarkistaa tämän jälkeen, onko sillä jo ennestään käyttäjistä salausavainparitunnistetta K. Tässä tapauksessa käyttäjä on ensimmäistä kertaa verkossa, joten MME:llä ei ole välimuistissa salausavain pari tunnistetta, joten se lähettää autentikointi kyselyn DIAMETER protokollan avulla HSS-tietokannalle. Tämän jälkeen HSS etsii käyttäjälle tarkoitetun salausavain parin K tietokannastaan. Löydettyään salausavainparin HSS laskee K-ASME-, AUTN eli Authentication token-, XRES eli Expected Authentication Result- ja RAND eli Random Number -arvot salausavaimesta. Tämän jälkeen se lähettää päättelemänsä tiedot MME:lle. Tästä tiedosta MME generoi K-NAS-enc-, K-NAS-int- ja K-eNB-salausavainosat. [9; 10.]

Vasta tämän jälkeen MME lähettää vaiheessa 14 salaamattoman autentikointipyynnön päätelaitteelle, joka sisältää RAND-, AUTN- ja KSI-ASME-arvot. Päätelaite selvittää heti tämän jälkeen salausavain K parinsa USIM-kortilta. Tämän avulla ja MME:ltä saaduista AUTN ja RAND -arvoista se laskee autentikointituloksen eli RES-arvon. Tämän jälkeen päätelaite lähettää RES-arvon takaisin MME:lle. MME vertaa päätelaitteelta saatua RES-arvoa HSS:ltä saatuun XRES-arvoon. Tässä tapauksessa nämä arvot täsmäävät eli autentikointi onnistuu. Tästä edetään seuraavaksi NAS-yhteyden salauksen ja eheyden varmistusvaiheeseen sekä verkkoalueen käyttöluvan varmistukseen, joka havainnollistettu kuvassa 10. [9.]



Kuva 10: NAS-salauksen ja eheyden varmistus sekä verkkoalueen käyttöluvan varmistus [vrt. 9; 17; 19].

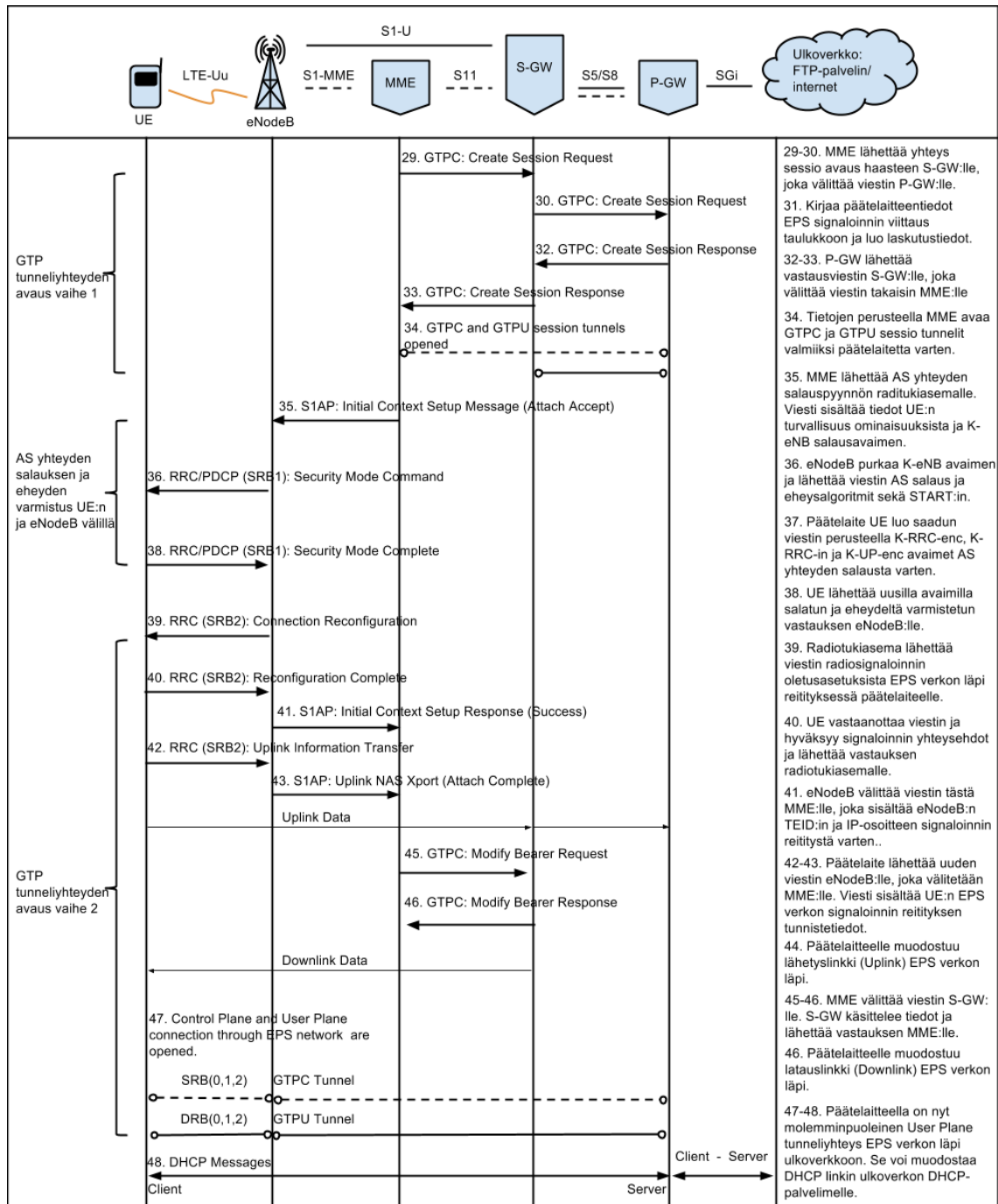
Ensimmäisenä käydään läpi NAS:in salauksen ja eheyden varmistusvaihe. MME lähettää päätelaitteelle NAS-turvallisuushaasteen. Haaste sisältää EPS-salauksen ja eheydenvarmistus algoritmit sekä KSI-ASME-avaimen. KSI-ASME-avaimen avulla päätelaite saa valittua oikean K-ASME-avaimen. Päätelaitteen käyttää NAS-turvallisuushaasteen salauksen päättelyyn valittua K-ASME-avainta sekä EPS-salausalgoritmia ja luo näistä K-NAS-enc-salausavaimen. Salausalgoritmin päättelyn

jälkeen päätelaite selvittää K-ASME:n sekä EPS-eheysalgoritmit avulla K-NAS-inteheysavaimen. Päätelyn tehtyään päätelaite lähettää nämä avaimet vastauksena NAS salauksen ja eheyden varmistusviestiin vaiheessa 23 eNodeB välittää viestin seuraavassa vaiheessa MME:lle ja näin NAS-yhteys on sekä salattu että eheydeltä varmistettu. [9.]

Tästä siirrytään seuraavaksi verkkoalueen käyttöluvan varmistusvaiheeseen. Tämä vaihe jää pois Metropolian LTE-verkossa, koska siinä ei ole vierasverkkoaluetta. Operaattoreilla tämä vaihe on ja sen takia tämä käsitellään tässä insinööriyössä läpi. MME lähettää aluksi käyttäjän verkkoalueen paikan päivityksen HSS:lle. Viesti sisältää tiedon päätelaitteen alkuperästä (origin), määränpäästä (destination), käyttäjänimen (user name/IMSI) sekä Visited PLMN ID:n. HSS katsoo saadusta viestistä, onko käyttäjällä aiemmin palvelut MME:tä ja vapauttaa tarvittaessa vanhan MME:n päätelaitteen palveluksesta lähettämällä sille viestin, joka sisältää käyttäjän IMSI tunniste. Vanha MME hyväksyy uudet ehdot ja lähettää kiittauksen HSS:lle. Tämän jälkeen HSS lähettää vastausviestin MME:lle vaiheessa 27, joka sisältää verkko käyttäjän tilaustiedot (subscription data). Tarkemmin viesti sisältää tiedon onko käyttäjällä oikeus verkkoalueelle, IMSI tunniste, käyttäjän datayhteyden rajoitusmääritykset, määritykset maksimikaistasta latauksessa ja lähetyksessä, käyttäjän puhelinnumero tunniste (MSISDN) sekä Access Point Name (APN) tiedot. MME vastaanottaa viestin ja hyväksyy päätelaitteen LTE-verkon käytön saadun vastauksen perusteella. Tästä eteenpäin käyttäjälle lähetetään luomaan User Plane -tunneliyhteyttä, joka käydään seuraavassa kappaleessa. [17; 19; 27.]

4.3 User Plane -tunneliyhteyden avaus

Käyttäjän onnistuneen autentikoinnin, NAS-yhteyden salauksen ja eheyden varmistuksen ja verkkoalueen käyttöluvan varmistuksen jälkeen päätelaitteelle luodaan User Plane -datatunneliyhteys ulkoverkkoon. Kuvassa 11 tämä vaihe käydään läpi kokonaisuudessaan. GTPC ja GTPU ovat sama asia kuin aiemmissa luvuissa mainitut GTP-C ja GTP-U.



Kuva 11: User Plane -tunneliyhteyden avaus kaikkine vaiheineen [vrt. 9; 18; 19; 27].

Vaiheet (29-30): User Plane -tunneliyhteyden avaus alkaa ensimmäisellä osalla, jossa MME:n lähettää GTPC-kuljetusprotokollan avulla haasteviestin S-GW:lle, jossa pyydetään lupaa avata GTP-yhteyssessio päätelaitetta varten. Tässä viestissä on muun muassa käyttäjän International Mobile Subscriber Identity- (IMSI) ja Radio Access Technology (RAT) -tiedot, päätelaitteelle avattavan tunneliyhteyden

tunnistetieto eli Tunnel Endpoint Identifier TEID, Packet Data Network type (IPV4 tai IPV6) eli pakettipohjaisen yhteyden IP-tyyppi, puhelinnumero eli MSISDN ja Packet Data Network ja P-GW:n IP-osoitteet. Teoriassa viesti sisältäisi myös päätelaitteen sisäverkon IP-osoitteen tässä vaiheessa ja viesti välitettäisiin erilliselle P-GW-verkkoelementille. Käytännössä Wireshark-testiympäristössä nämä kaksi laitetta oli kuitenkin virtualisoitu yhdeksi ja samaksi laitteeksi, joten tämä välivaihe jäi pois luvun 5 tarkastelussa. Teoriassa viesti P-GW:lle sisältäisi IMSI-, MSISDN-, APN- ja S-GW IP-osoitetiedot. [19; 27.]

Vaiheet (31-34): P-GW vastaanottaa viestin ja kirjaa tiedot EPS-signaloinnin viittaustaulukkoon ja luo samalla tunnistetiedot päätelaitteen laskutusta varten (Charging Id). Tämän jälkeen P-GW lähettää vastauksen S-GW:lle, jossa kerrotaan P-GW:n User Plane -tunneliyhteyden osoite, P-GW:n TEID-tiedot User Plane- ja Control Plane -yhteyksiä varten sekä päätelaitteen EPS Bearer ID (EBI) signalointitunnelin ja QoS (Quality of Service) -tiedot. P-GW lähettää heti tämän jälkeen tiedot latauslinkin tiedot S-GW:lle. Lopulta S-GW lähettää MME:lle viestin yhteysession avauksesta ja samalla pyynnön päätelaitteen signaloinnin oletusasetuksista. Tässä vaiheessa MME:n ja P-GW välille on luotu sessiot GTPC- ja GTPU-tunneliyhteyksistä (vaihe 34). [19; 27.]

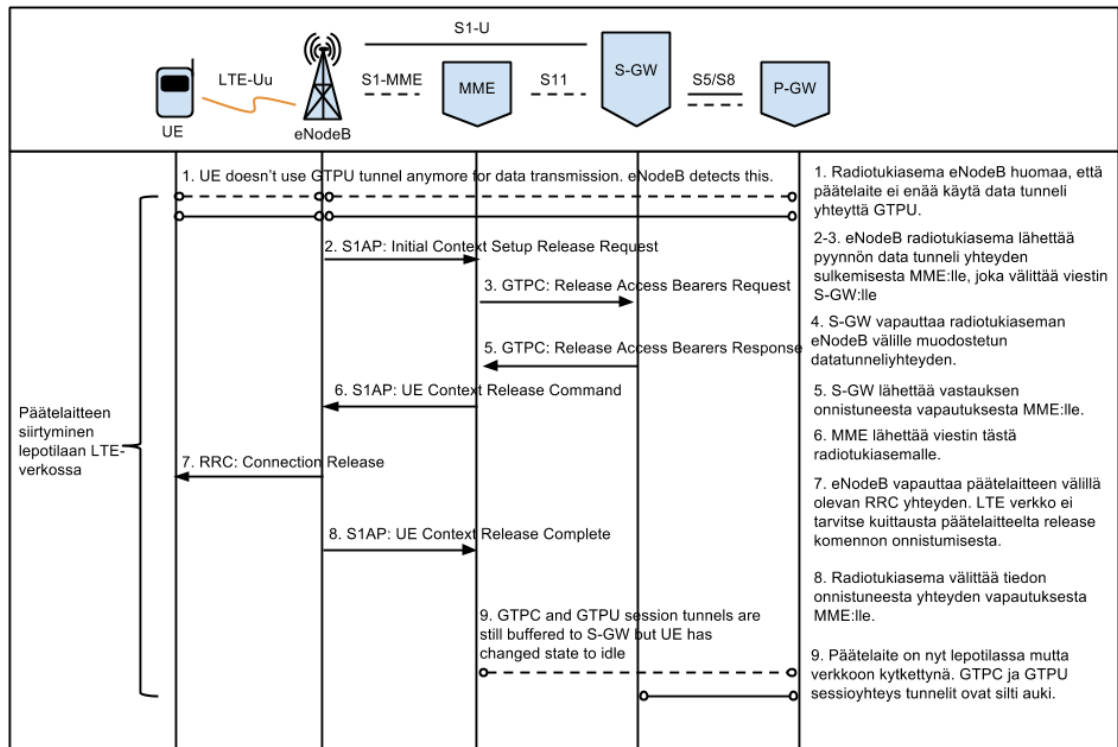
Vaiheet (35-38): Tästä alkaa AS-yhteyden salauksen ja eheyden varmistus. AS-yhteyksikäsitteeseen kuuluu RRC- (Control Plane -yhteysprotokolla) ja PDCP (User Plane -yhteysprotokolla) -yhteydet päätelaitteen ja radiotukiasema eNodeB:n välillä. MME lähettää pyynnön eNodeB:lle, joka sisältää tiedot päätelaitteen UE-turvallisuus ominaisuuksista (Security Capabilities) sekä K-eNB-salausavainosan radiotukiasemaa varten. Radiotukiasema eNodeB vastaanottaa viestin ja lähettää yhteyden turvaamiskäskyn päätelaitteelle UE. Viesti sisältää AS-yhteyden salaus- ja eheysalgoritmit sekä START-salaus- ja eheysparametrit. Päätelaite vastaanottaa viestin tiedot ja lähtee luomaan K-RRC-enc- ja K-RRC-int-avainosia RRC-yhteyden salauksen ja eheyden varmistusta sekä K-UP-enc-avainosaa PDCP (User Plane) -yhteyden salausta varten. Päätelaite luo K-RRC-enc- ja K-UP-enc-avaimet saadusta AS-salausalgoritmista ja paljon aiemmin tulleesta K-ASME-avainosasta. Tämä jälkeen päätelaite luo K-RRC-int-avaimen käyttämällä saatuja AS-eheysalgoritmia sekä K-ASME-avainosaa. Lopulta päätelaite UE lähettää salauksella ja eheydellä varmistetun vastauksen radiotukiasemalle takaisin. [9; 19.]

(Vaiheet 39-44): Tästä siirrytään GTP-tunneliyhteyden avauksen toiseen vaiheeseen. Radiotukiasema eNodeB lähettää viestin radiosignaloinnin oletusasetuksista päätelaitteelle UE. Viesti sisältää EPS-verkon radiosignaloinnin identiteetin tunnistetiedot tunneliyhteyden avausta ulkoverkkoon varten (EPS Radio Bearer Identity), APN-tiedot ja HSS:n myöntämä Packet Data Network verkon IP-osoite. Päätelaite UE vastaanottaa viestin, hyväksyy tulleet ehdot ja asetukset ja lähettää vastausviestin radiotukiasema eNodeB:lle. Radiotukiasema lähettää tämän jälkeen viestin MME:lle, joka sisältää eNodeB:n TEID-tunnelointiyhteyden tunnistetiedot ja IP-osoitetiedon, jota käytetään oikean S1-U-yhteyden valitsemiseen latauslinkin (Downlink data) tietoja varten. Tämän jälkeen päätelaite UE lähettää uuden viestin radiotukiasema eNodeB:lle, jossa kerrotaan laitteen EPS-verkon signaloinnin identiteetin tunnistetiedot (EPS Bearer Identity), NAS-sekvenssiarvot (NAS sequence number) ja NAS-MAC-tiedot. Radiotukiasema eNodeB välittää nämä tiedot MME:lle. Tässä vaiheessa päätelaitteelle UE muodostuu koko runkoverkon läpi menevä datan lähetyslinkki (Uplink Data) P-GW:lle asti. [19; 27.]

(Vaiheet 45-48): Tästä eteenpäin MME välittää S-GW:lle pyynnön, joka sisältää päätelaitteen EPS-verkon signaloinnin identiteetin tunnistetiedot (EPS Bearer Identity) sekä eNodeB:n IP-osoitteen ja TEID-tiedot. S-GW vastaanottaa viestin ja käsittelee pyynnön. Se lähettää vastauksen MME:lle, joka sisältää päätelaitteen EPS-verkon signaloinnin identiteetin tunnistetiedot (EPS Bearer Identity). Tämän jälkeen päätelaite UE saa datan latauslinkin (Downlink data) runkoverkon läpi P-GW:lle asti. Päätelaite on saanut avattua User Plane -datatunneliyhteyden sekä lähetys- että lataussuunnassa runkoverkon läpi. Tämä tarkoittaa myös DHCP-yhteyttä ulkoverkkoon. [19; 27.]

4.4 Päätelaitteen yhteyden muodostaminen LTE-verkkoon lepotilasta

Käyttäjä on nyt rekisteröitynyt LTE-verkkoon ja muodostanut itselleen User Plane -data tunneliyhteyden ulkoverkkoon ja käyttää yhteyttä aktiivisesti jonkin aikaa, kunnes päättää lopettaa internetselailun. Hän jättää päätelaitteensa kuitenkin päälle, ja se pysyy kytkettynä verkkoon. Radiotukiasema havaitsee silloin jossain vaiheessa, että käyttäjällä on User Plane -datatunneliyhteys auki edelleen, mutta sen läpi ei kulje enää yhtään liikennettä ulkoverkkoon. [20; 32.]

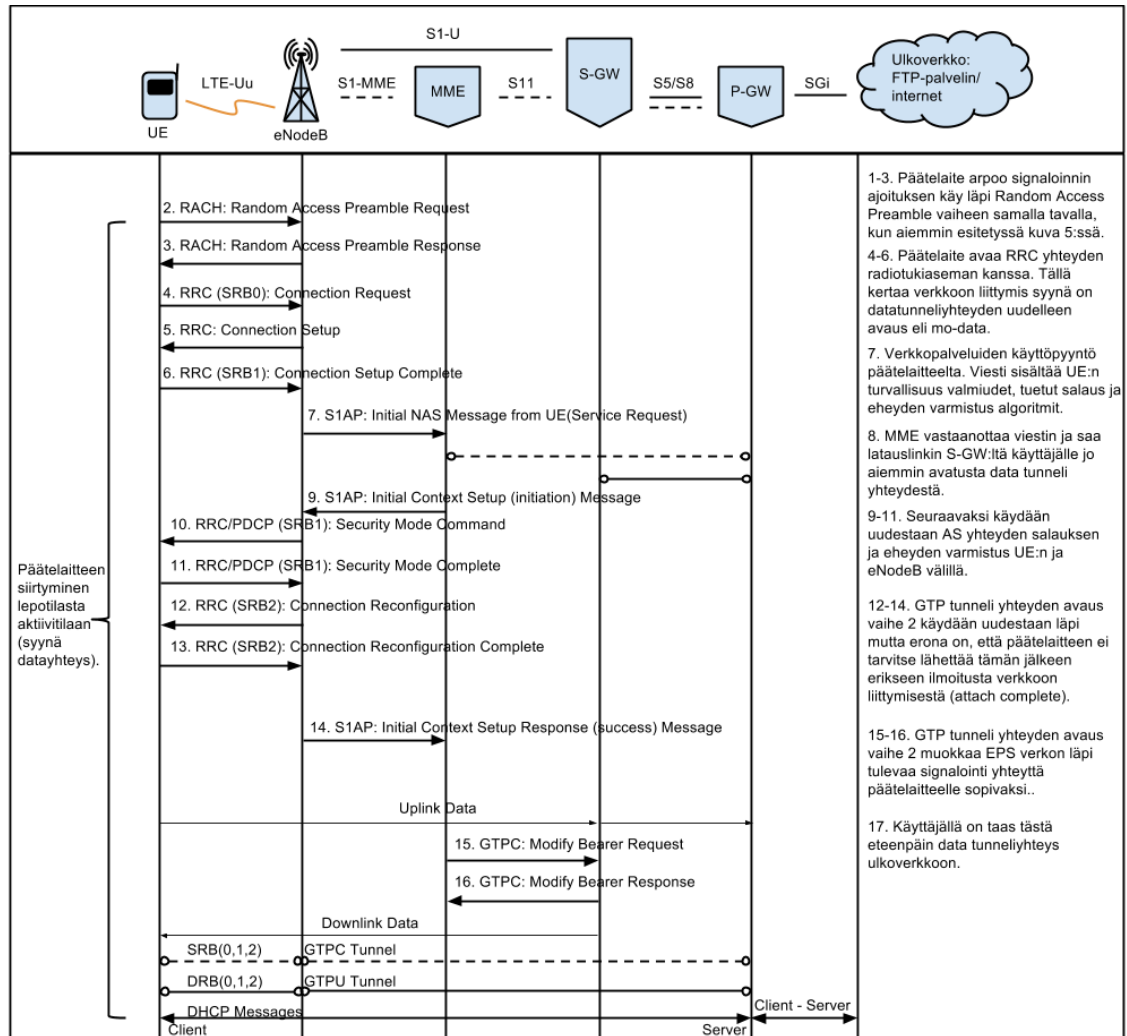


Kuva 12: LTE-verkkoon kytkeytyneen päätelaitteen siirtyminen lepotilaan [vrt. 19; 20; 32.].

Tästä alkaa päätelaitteen radorajapinnan varaaman kaistan vapautus (RRC connection release procedure), joka on havainnollistettu kuvassa 12. Radiotukiasema eNodeB välittää pyynnön radiokaistan vapautuksesta MME:lle, joka välittää tiedon S-GW:lle. Viesti sisältää tiedon, että päätelaite on mennyt lepotilaan (Idle state) radiotukiasema eNodeB alueelta. S-GW vapauttaa radiotukiasema eNodeB:n datatunneliyhteyden reitityksessä. Tämä tarkoittaa päätelaitteelta EPS-verkon läpi kulkevan User Plane -datatunneliyhteyden sulkemista toistaiseksi. Tässä tapauksessa S-GW:lle laitteelle jää kuitenkin käyttäjälle varattu GTP-yhteystunneli auki. Lopulta S-GW vastaa MME:lle onnistuneesta User Plane -datatunneliyhteyden sulkemisesta väliaikaisesti. MME lähettää tästä tiedon radiotukiasema eNodeB:lle, joka vapauttaa UE:n välillä olevan RRC-yhteyden. Radiotukiasema eNodeB lähettää vastauksen MME:lle onnistuneesta päätelaitteen lepotilaan siirtymisestä ja UE:n yhteyden vapautuksesta. [19; 20; 32.]

Käyttäjän ollessa nyt lepotilassa LTE-verkossa hän päättää aloittaa taas internetselailun. Tässä yhteys luodaan samalla periaatteella, kuin aiemmissa

kappaleissa 4.1-4.3, mutta tällä kertaa käyttäjän ei tarvitse erikseen autentikoitua LTE-verkkoon uudestaan, salata ja varmistaa NAS-yhteyden eheys, kysyä lupaa verkkoalueella vierailusta sekä luoda yhteystunnelisessio uudestaan S-GW:n ja P-GW:n välille muun muassa laskutustietoja varten. Kuvassa 13 esitetään tämä vaihe tarkemmin. [32; 34.]



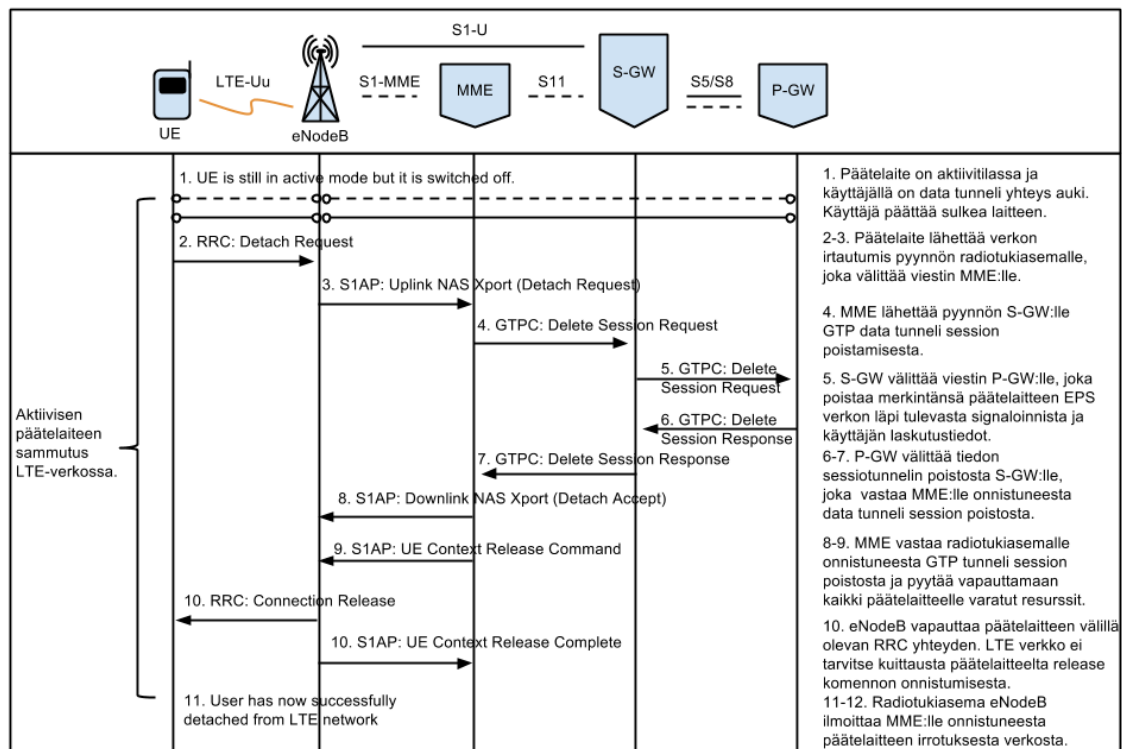
Kuva 13: Päätelaitteen siirtyminen lepotilasta (LTE_Idle) takaisin aktiivitilaan (LTE_Active) [vrt. 18; 19; 32].

Kuvassa 13 verkkokäyttäjä siirtyy lepotilasta takaisin aktiivitilaan, jotta hän voi taas käyttää LTE-verkon tarjoamaa datapalvelua. Päätelaite käy samalla tavalla aluksi kuvan 7 mukaan Random Access Preamble- ja RRC-yhteyden avauksen uudestaan. Tällä kertaa erona on, että käyttäjän verkon liittymissyynä on mo-data eli datatunneliyhteyden luominen internet selailua varten. Päätelaitteen UE ja

radiotukiasema eNodeB välille muodostetun yhteyden jälkeen välitetään viesti MME:lle, jossa pyydetään avata käyttäjälle jo aikaisemmin avattu GTP User Plane -datatunneliyhteys. S-GW välittää avatusta yhteystunnelista latauslinkin MME:lle. Tästä eteenpäin käydään AS-yhteyden salauksen ja eheyden varmistusvaihe sekä GTP-tunneliyhteyden avauksen toinen osa samalla tavalla kuin kuvassa 11. Ainoana erona on, että päätelaitteen ei tarvitse lähettää viestiä onnistuneesta verkkoon liittymisestä (Uplink NAS Xport: attach complete). Tämän jälkeen käyttäjällä on taas mahdollisuus lukea sähköposti tai käyttää ulkoverkosta saatavia datapalveluita. [19; 27.]

4.5 Aktiivisen ja lepotilassa olevan päätelaitteen sammutus LTE-verkossa

Aktiivisen päätelaitteen sammutuksessa kaikki alkaa siitä, kun päätelaite lähettää samalla pyynnön irtautua LTE-verkosta. Tämä on esitetty kuvassa 14.

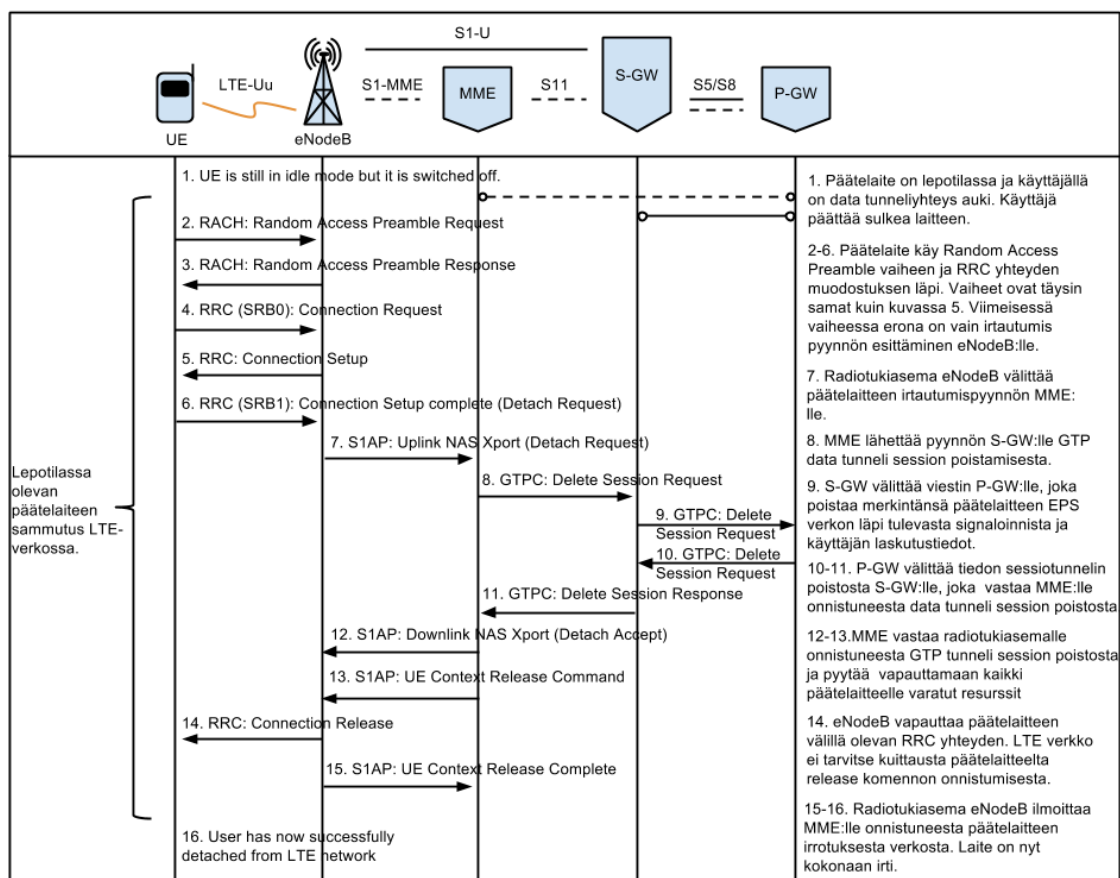


Kuva 14: Aktiivisen päätelaitteen sammutus LTE verkossa [vrt. 35, s. 188.].

Radiotukiasema vastaanottaa viestin ja lähettää tästä tiedon MME:lle. Tästä pyyntö jatkaa S-GW:lle, jolta pyydetään poistamaan käyttäjälle varattu GTP-yhteystunneli. Ennen kuin S-GW lähettää vastauksen MME:lle se poistaa oman merkintänsä

päätelaitteelta EPS-verkon läpi tulevan signalointitunnelista ja käyttäjän laskutustiedot. MME saa lopulta viestin S-GW:ltä onnistuneesta GTP-tunnelisession poistosta ja pyytää tämän jälkeen eNodeB-radiotukiasemalta vastausta päätelaitteen UE-verkon vapautus tilasta. Radiotukiasema vapauttaa päätelaitteen RRC-yhteyden, hävittää kaikki päätelaitteelle varatut resurssien varaus tiedot ja lopulta lähettää viestin takaisin MME:lle onnistuneesta päätelaitteen verkko irtautumisesta. [35.]

Lepotilassa olevan päätelaitteen sammutuksessa käydään läpi samalla tavalla kuvan 14 vaiheet, mutta puhelin joutuu tätä ennen avaamaan Random Access Preamble- ja RRC-yhteyden. Kuvassa 15 tämä vaihe on esitetty tarkemmin. [35.]



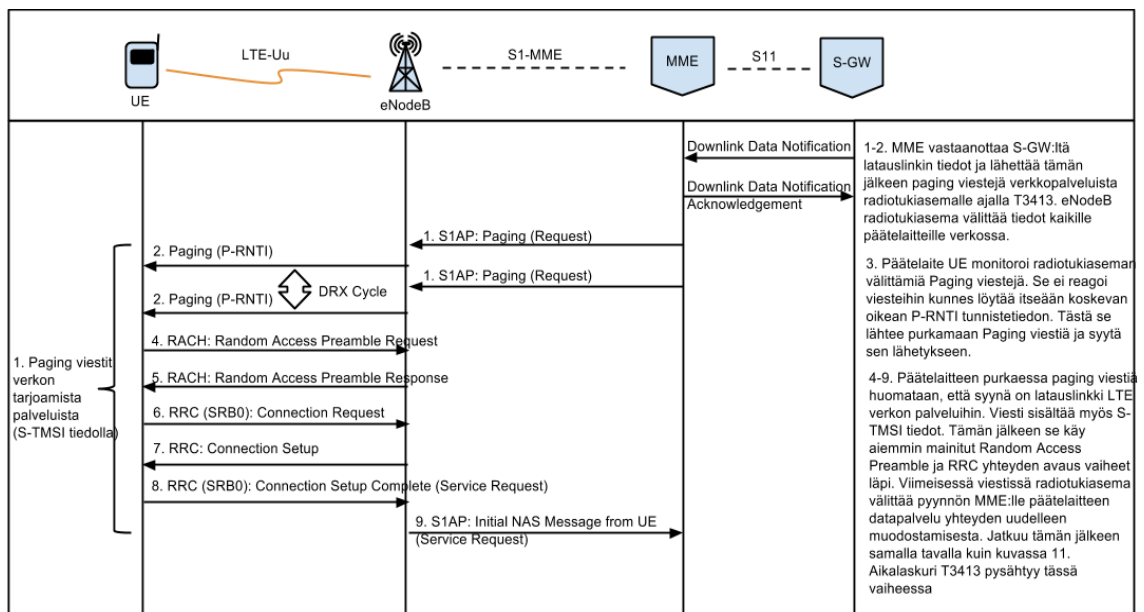
Kuva 15: Lepotilassa olevan päätelaitteen sammutus LTE-verkossa [vrt. 35, s. 188].

Kummassakin näistä sammutus tapauksista MME säilyttää välimuistissa päätelaitteen IMSI, GUTI ja salausavainosat tulevaa yhteydenottoa varten. Se kuinka pitkään nämä tiedot pysyvät MME:n välimuistissa, vaihtelee operaattorikohtaisesti mutta tällä tavalla sen ei tarvitse ottaa yhteyttä HSS:ään uudestaan puhelimen autentikoinnissa.

Käytännössä tämä tarkoittaa kuvassa 7 esiintyvien olevien välivaiheiden 10-12 ohittamista seuraavan kerran, kun käyttäjä laittaa päätelaitteensa päälle LTE-verkossa. [35.]

4.6 LTE-verkkopalveluiden mainostus eli paging

Päätelaitteen ollessa lepotilassa (idle state) LTE-verkko kommunikoi tasaisin väliajoin silti siihen kytkettyjen päätelaitteiden kanssa lähettämällä paging-viestejä. Tämä on LTE-verkon tapa mainostaa omia palvelujaan ja samalla pitää kirjaa, mitkä päätelaitteet ovat edelleen yhteydessä siihen. Päätelaite voi saada näitä viestejä, vaikka sillä olisi jokin välivaihe kesken, mutta silloin se ei huomioi niitä ollenkaan. Radiotukiasemat toimivat LTE-verkolle päätepisteinä paging-viestien lähetykseen. Tässä luvussa käyn tarkasti läpi paging-viestit verkkopalveluiden mainostuksesta ja miten päätelaite niihin reagoi. [31; 33; 37.]



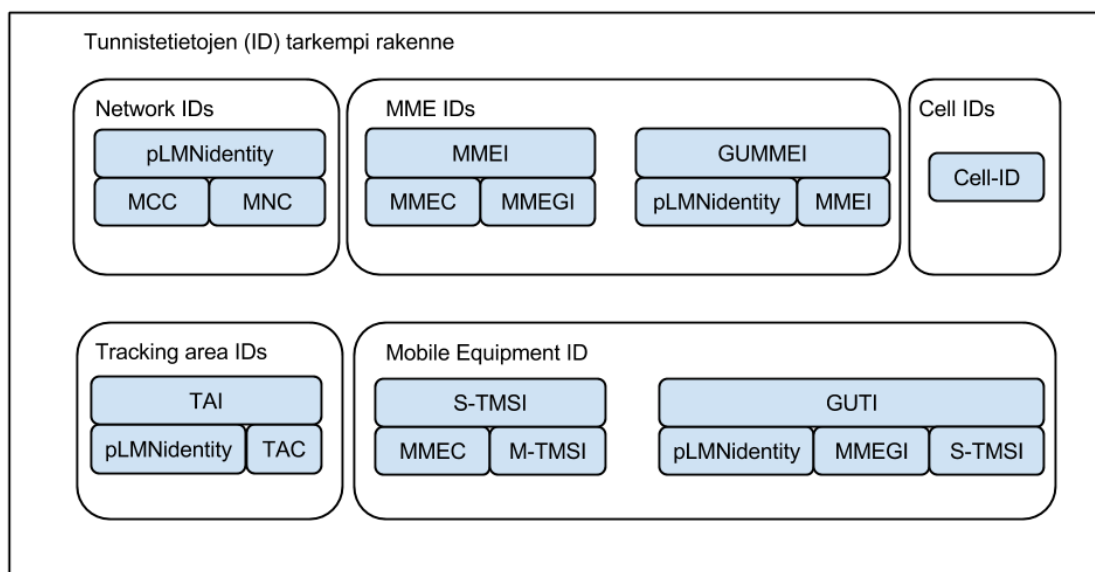
Kuva 16: Paging-verkkopalvelu viesti lepotilassa olevalle laitteelle [vrt. 31.].

Kuvassa 16 on esimerkki siitä, miten päätelaite reagoi verkon palveluita mainostaviin paging-viesteihin lepotilassa. Tämä ei kuitenkaan ole ainut syy, miksi paging-viestejä lähetetään LTE-verkossa. Syynä voi olla myös, että päätelaitteen S-TMSI-tunnistetietoa ei voida käyttää verkon ongelmatilanteessa jolloin lähetetään paging viesti päätelaitteen IMSI-tiedoilla. Tämän jälkeen UE:n on irrottauduttava verkosta

(kuvan 15 idealla) ja kytkeydyttävä uudestaan samalla tavalla, kuin aiemmissa kuvissa 7, 9, 10 ja 11. Tämä on kuitenkin erittäin harvinaista, mutta on hyvä tietää, että kuvassa 16 esiintyvä paging-mainostustyyppi ei ole ainoa lajiaan toimivassa operaattoriverkossa. [31; 33; 37.]

5 LTE-verkon protokollien kuljettama tieto pakettitasolla

Luvussa neljä käytiin läpi käskytasolla insinööriyössä rajatun LTE-verkkoalueen komennot eri verkkoelementtien välillä. Tässä luvussa käsitellään, mitä kaikkea nämä viestit sisältävät tarkemmin. Tämän takia insinööriyön LTE-verkkokäsitystä pitää laajentaa, jotta jokaisella mainitulla tiedolla on merkitys. Tarkastelemme aiemmin esitettyjä tietoja hierarkiassa vielä tarkemmin, joten seuraavaksi käydään LTE-verkon pakettien tunnistetiedot tarkemmin läpi.



Kuva 17: Identity (ID) -tietojen tarkempi rakenne [vrt. 4.].

Kuvassa 17 olevat eri tunnistetiedot tarkoittavat seuraavaa:

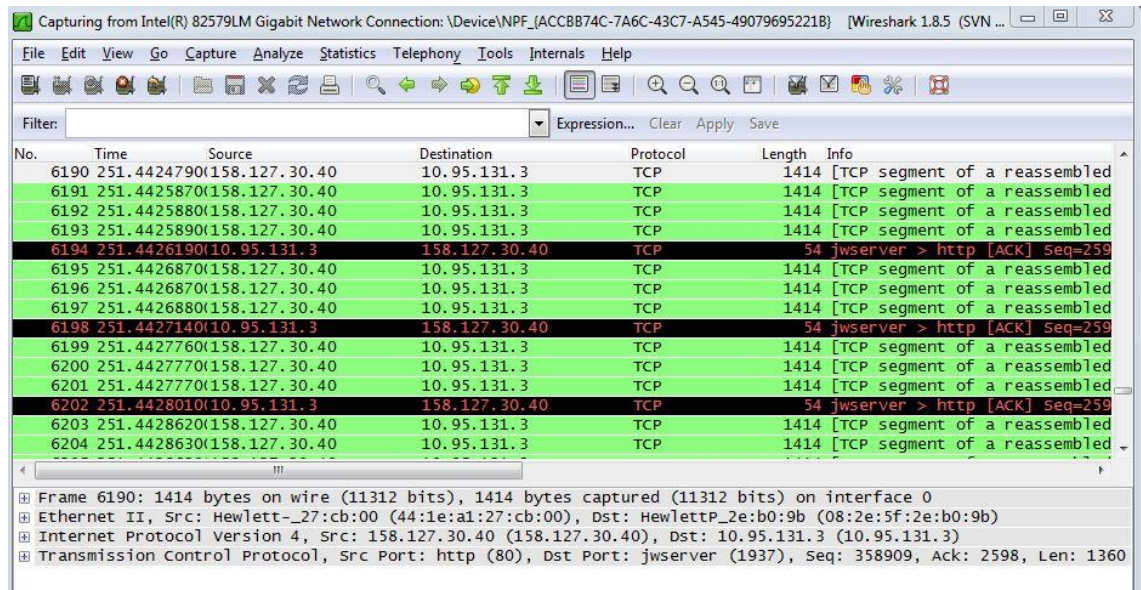
- Network IDs: Operaattorin LTE-verkon tunnistetietona käytetään pLMNidentity (sama kuin aiemmin mainittu PLMN identity), joka koostuu kominumeroisesta puhelimen maakoodista MCC ja puhelimen operaattoriverkkoaluekoodista MNC, joka voi olla kaksi tai kolminumeroinen. Näin voidaan tunnistaa, mistä maasta ja mille operaattorille asiakas kuuluu. [4.]
- MME IDs: Aiemmin mainittu Mobile Management Entity -verkkoelementti tarvitsee myös tunnistetietoja LTE-verkossa. Operaattoriverkossa Mobile Management Entityt on jaettu todellisuudessa eri MME Pool Area alueille, johon voi kuulua yksi tai useampi Mobile Management Entity. Tunnistetietoja MME:llä on kolme erilaista: MMEC, joka on yksittäisen MME:n tunnistetieto ja MMEGI,

joka kertoo, mihin MME Pool area -ryhmäalueelle kyseinen verkkoelementti kuuluu. Nämä tiedot yhdistäessä saadaan MMEI-tunnistetieto, jolla yksittäinen MME voidaan tunnistaa operaattorin sisäisestä verkosta. Tämä ei kuitenkaan riitä, koska on olemassa muitakin operaattoreita eri maissa, joten yhdistetään pLMNidentity- ja MMEI-tiedot. Tästä saadaan GUMMEI-tunnistetieto, jolla yksittäinen MME voidaan tunnistaa mistä päin maailmaa tahansa. [4.]

- Cell IDs: Toimii yksittäisen radiotukiaseman tunnistetietona. Tämän kentän numeerinen arvo voi vaihdella välillä 0-503. [4.]
- Tracking Area IDs: Tämä tunnistetieto sisältää TAC-tiedon käyttäjän vierailomalta radiotukiasemien verkkoalueelta. Yhdelle Tracking Arealle voi kuulua enemmän kuin yksi radiotukiasema, joten sitä varten on aiemmin mainittu Cell-ID-tunnistetieto, jolla myös yksittäinen radiotukiasema voidaan tunnistaa. Pelkällä TAC-tiedolla voidaan radiotukiasemien verkkoalue tunnistaa operaattoritasolla mutta tähän lisättäessä pLMNidentity, alue voidaan tunnistaa mistä päin maailmaa tahansa. [4.]
- Mobile Equipment ID: Päätelaitte pitää pystyä tunnistamaan MME Pool Area -alueelta tarkasti. Sitä varten on tunnistetieto M-TMSI, jolla voidaan tunnistaa mihin MME-verkkoelementtiin päätelaite on yhteydessä. Tähän lisätään aiemmin mainittu MMEC ja saadaan S-TMSI-tunnistetieto, jolla päätelaite voidaan tunnistaa operaattoritasolla. Lopuksi muodostetaan pLMNidentity-, MMEGI- ja S-TMSI -tiedot yhteen ja saadaan GUTI-tunnistetieto, jolla päätelaite voidaan tunnistaa maailmanlaajuisesti. [4.]

5.1 Wireshark-monitorointityökalu

Wireshark on vapaaseen lähdekoodiin perustuva protokollien analysointityökalu. Vuonna 1998 lähteneestä projektista sitä käytetään niin opetuskäytössä kuin operaattoreilla verkon tutkimiseen. [42.]



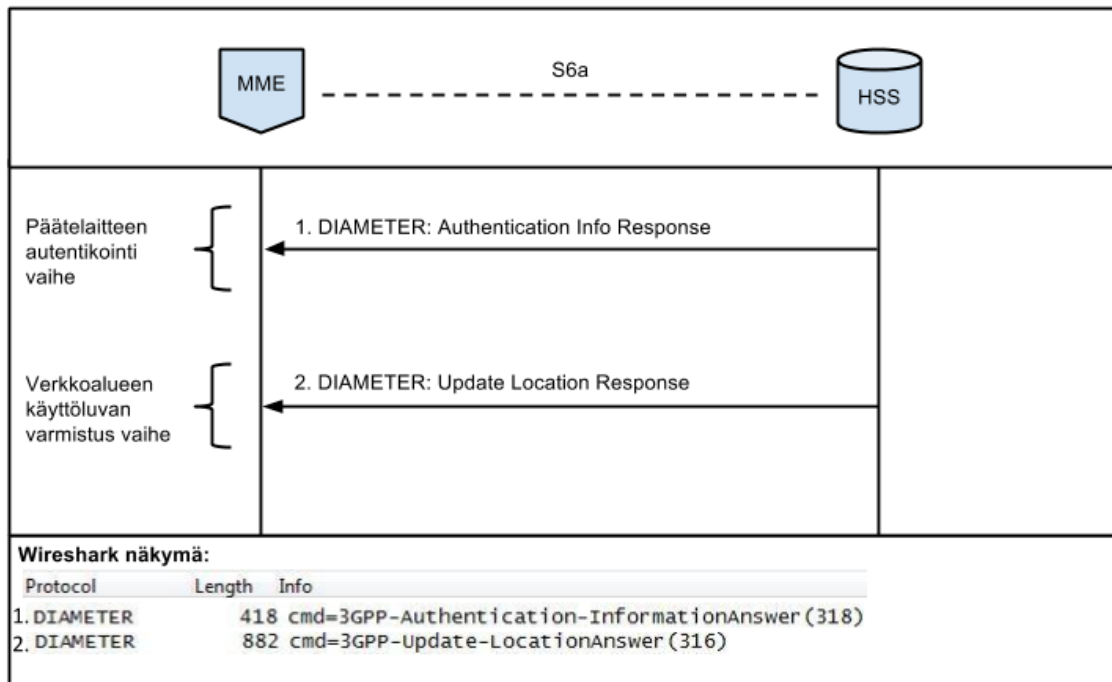
Kuva 18: Wireshark-ohjelma.

LTE-verkon pakettien analysoinnissa operaattoreilla on oma muokattu versio tästä mutta tavallinenkin versio pystyy tunnistamaan LTE-verkkoelementtien välistä liikennettä sellaisenaan, joka on esitetty kuvassa 18. Radiorajapinnan analysoinnissa päätelaitteen UE- ja eNodeB-radiotukiaseman välillä sen sijaan materiaalia oli hankala saada, joten se on jätetty pois tästä työstä. [42.]

Filter-työkäluä kannattaa hyödyntää etsiessä paketteja eri LTE-verkkoelementtien välillä. Näin verkon toiminnasta saa paljon paremman kuvan vaikka se rajaa tarkastelun kahden verkkoelementin välille. Se auttaa myös LTE-verkon vian etsinnässä.

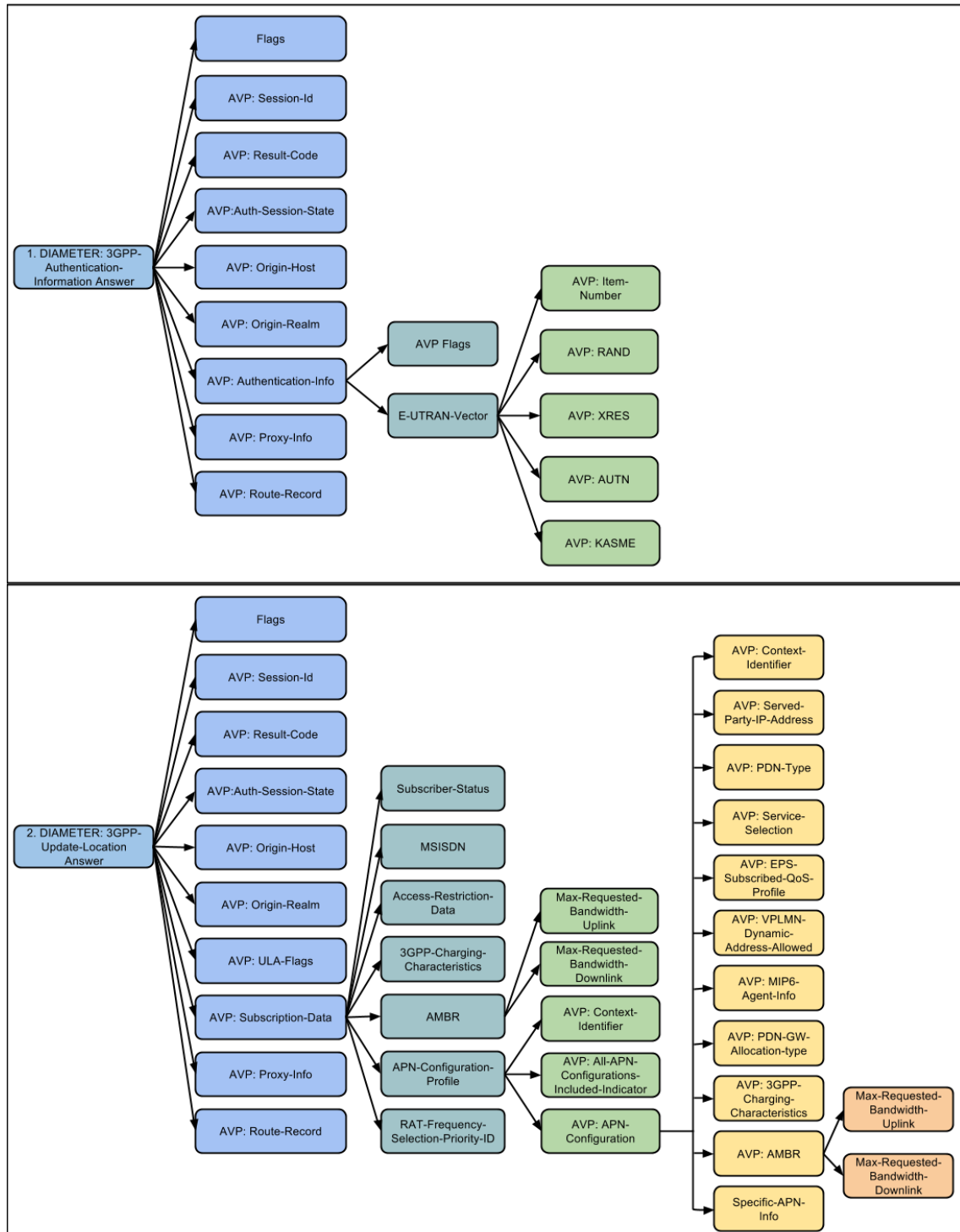
5.2 MME:n ja HSS:n välillä

Wireshark testiympäristössä MME- ja HSS-verkkoelementit oli virtualisoitu yhdeksi ja samaksi laitteeksi, joten sen takia esitän tässä insinööriyössä vain HSS:ltä saadut vastausviestit. Kuvassa 19 havainnollistetaan tarkemmin, mistä viesteistä on kyse.



Kuva 19: Päätelaitteen autentikointi ja verkkoalueen käyttöluvan varmistus vaihe. Kuvan tekemiseen käytetty mallina aiemmin esitettyjä kuvia 7 ja 8.

Aiemmissa Luvuissa on jo mainittu mitä viestit tekevät mutta katsotaan niiden sisältöä tarkemmin. Kuvassa 20 on esitetty näiden kahden viestin tarkempi sisältö hierarkisesti.



Kuva 20: Viestit MME:n ja HSS verkkoelementtien välillä. Ylempi paketti päätelaitteen autentikointivaiheen vastaus ja alempi päätelaitteen verkkoalueen käyttöluvan varmistus. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Ensimmäisessä viestissä voidaan huomata, että HSS on päätellyt aiemmin mainitusta salausavain K:sta salausarvot RAND, XRES, AUTN ja K-ASME. Viestin muista osista mainintana Result-code, joka ilmoittaa onnistuneesta päätelaitteen autentikointitietojen noudosta.

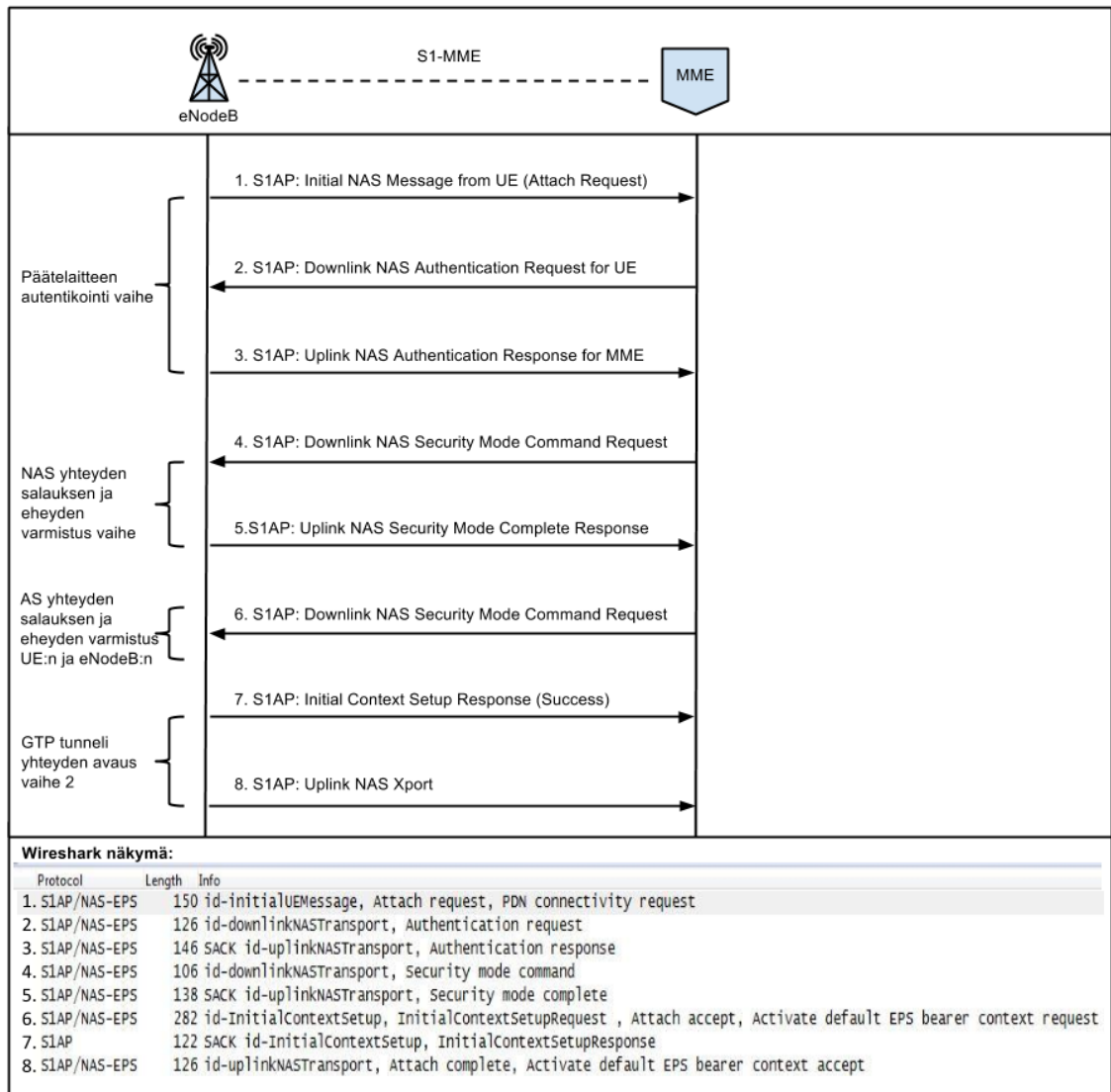
Alempi viesti 2 kuvassa 20 esittää verkkoalueen käyttöluvan varmistusvaiheen vastausviestiä HSS:ltä, joka sisältää huomattavasti enemmän tietoa. Näistä oleelliset tässä insinööriyössä käsiteltävät tiedot löytyvät hierarkiatason kaksi tietoa-alueesta AVP: Subscription Data. Täältä löytyvät päätelaitteen subscriber-status eli tilaajatiedot, joka tässä tapauksessa ilmoittaa hyväksytystä luvasta vierailta autentikoidulla LTE verkkoalueella. MSISDN-tietokenttä sisältää käyttäjän puhelinnumeron ja Access-Restriction-Data palvelun käyttörajoitukset. Tilaa-ajiedoista löytyvät myös laskutukseen liittyvät tiedot 3GPP-Charging-Characteristics tietoa-alueesta sekä Aggregate Maximum Bit Rate (AMBR) -tiedot suurimmasta sallitusta lataus- ja lähetysslinkkikaistasta. Kuvan hierarkian kolmannelta tason tietoa-alueesta APN-Configuration löytyy tarkemmat tiedot päätelaitetta palvelevaa P-GW-verkkoelementtiä varten. [41.]

5.3 eNodeB ja MME:n välillä

Radiotukiaseman eNodeB:n ja MME:n välisten pakettien tarkempaa tarkastelua varten tämä luku on selkeyden vuoksi jaettu neljään alakappaleeseen riippuen päätelaitteen tilasta LTE-verkossa. Aluksi käydään läpi, mitä paketteja näiden kahden verkkoelementin välillä kulkee, kun päätelaite rekisteröityy ja autentikoituu verkkoon (5.3.1). Tämän jälkeen luvussa 5.3.2 käydään läpi aktiivilasta lepotilaan liittyvä pakettiliikenne ja 5.3.3 puolestaan, kun päätelaite irtautuu verkosta kokonaan. Viimeisessä alakappaleessa käsitellään paging-viestien sisältö tarkemmin.

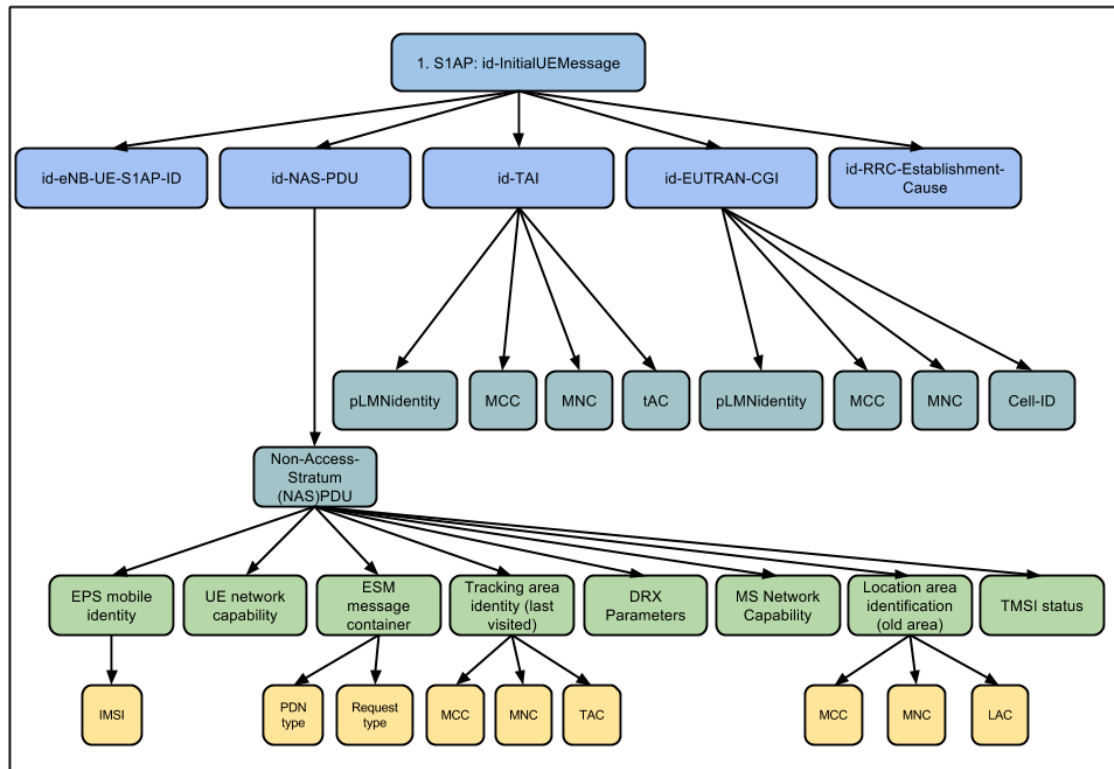
5.3.1 Päätelaitteen käynnistäminen ja verkkoon liittyminen

Aloitetaan käymällä läpi insinööriyössä aiemmin esitetyt välivaiheet kuvista 9, 10 ja 11, mutta tällä kertaa pelkän radiotukiasema eNodeB ja MME:n välillä ja otetaan mukaan Wireshark-näkymä. Kuvassa 21 on havainnollistettu päätelaitteen käynnistäminen ja verkkoon liittyminen eNodeB- ja MME-verkkoelementtien välillä.



Kuva 21: Päätelaitteen käynnistäminen ja verkkoon liittyminen. Tässä kuvassa on esitetty luvuissa 4.1, 4.2 ja 4.3 käydyt välivaiheet yhdessä pelkän eNodeB:n ja MME:n välillä ja todelliset tiedot wiresharkissa.

Tässä luvussa käydään jokainen näistä yllä olevan kuvan viesteistä tarkemmin läpi. Ensimmäisen viestin sisältö on esitetty hierarkisesti alla olevassa kuvassa 22. Tästä S1AP-kuljetusprotokollasta löytyy seuraavaa tietoa:

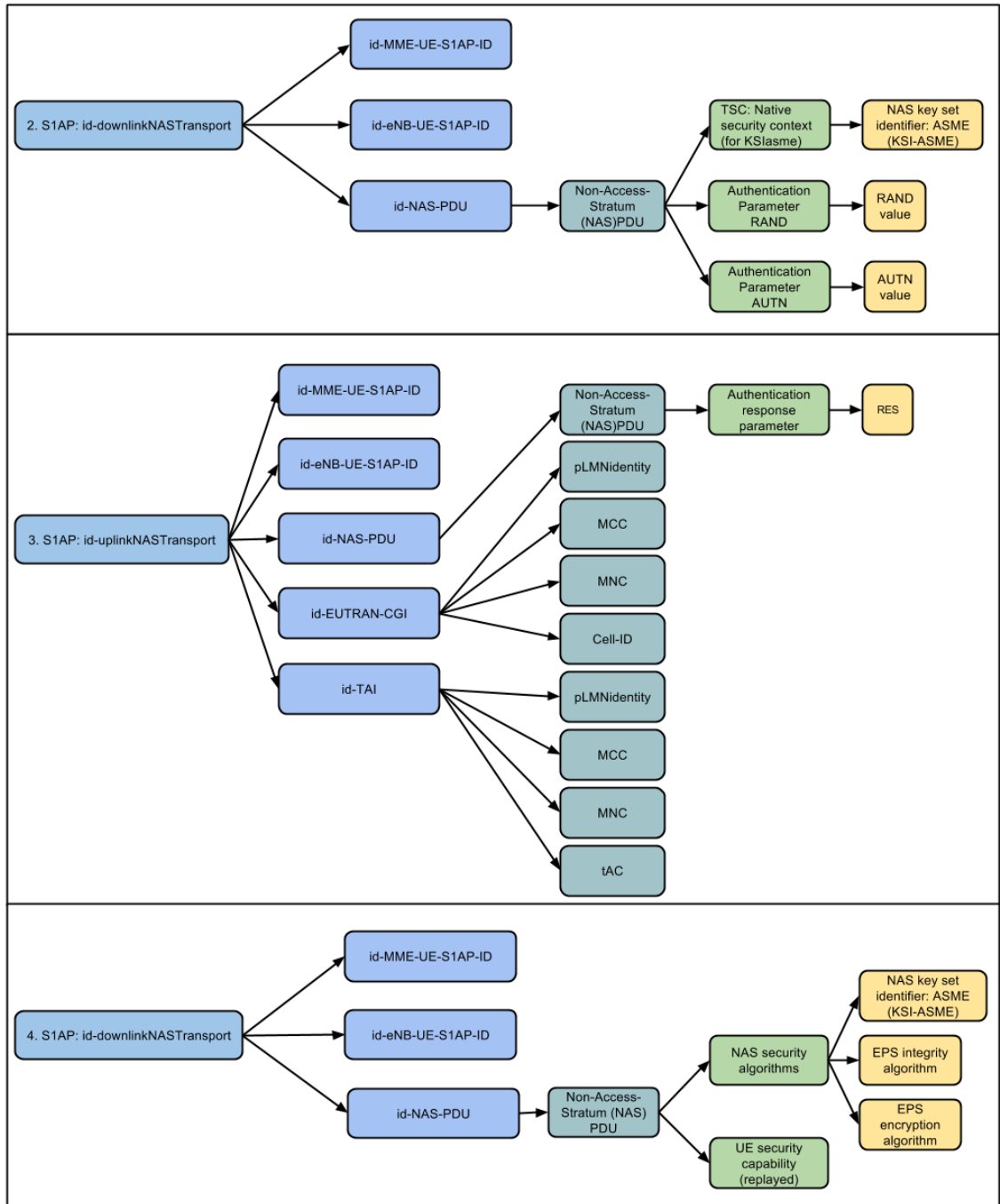


Kuva 22: Ensimmäisen autentikointivaiheen viestin rakenne. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Hierarkiassa tasoittain katsottuna toisella tasolla on id-eNB-UE-S1AP-ID, joka on päätelaitteen ja radiotukiaseman tunnistetieto MME:n välisen S1AP-kuljettajaprotokollan yhteyden tunnistamista varten. Tämän jälkeen hierarkian toisella tasolla on päätelaitteen ja MME:n välistä loogista yhteysprotokollaa varten oleva id-NAS-PDU-tunnistetieto. Tässä tärkeät tunnistetiedot ovat EPS mobile identity, koska se sisältää käyttäjän uniikin IMSI-tiedon, jonka avulla päätelaite autentikoidaan LTE-verkkoon. Tämän lisäksi viestin ESM message container sisältää tiedot PDN type eli onko kyseessä IPv4 vai IPv6 yhteys ja Request type, joka kertoo yhteyspyynnön tiedot. Tässä tapauksessa se on initial attach, koska käyttäjä autentikoituu verkkoon ensimmäistä kertaa. Id-NAS-PDU sisältää muitakin tietoja mutta tracking area identity- ja location area identification -kohdat eivät tässä vaiheessa vielä sisällä mitään aiemmin vierailtujen verkkoalueiden tietoja, koska käyttäjä avaa yhteyttä verkkoon ensimmäistä kertaa.

Kolmas tietoalue toisella hierarkia tasolla sisältää tässä vaiheessa id-TAI-tiedon päätelaitteen radiotukiasemien muodostaman alueen tunnistetiedon. Neljäs tietoalue

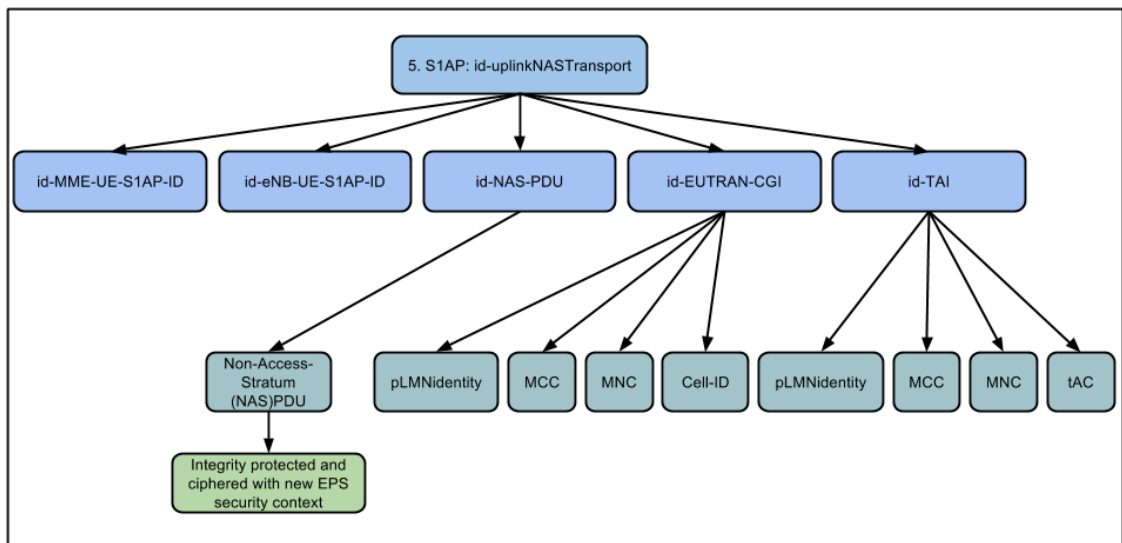
id-EUTRAN-CGI kertoo tässä vaiheessa tarkasti, miltä radiotukiasemalta käyttäjä haluaa liittyä LTE-verkkoon. Lopuksi viimeisenä id-RRC-Establishment-Cause, jossa kerrotaan, minkä takia käyttäjä haluaa avata yhteyden. Tässä tapauksessa syynä on mo-Signalling (3) eli käyttäjä tunnistautuu verkkoon ensimmäistä kertaa. [1.]



Kuva 23: Autentikointivaiheen viestien kaksi ja kolme rakenne sekä NAS-yhteyden salauksen ja eheydenvaihe viestin rakenne (neljäs). Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

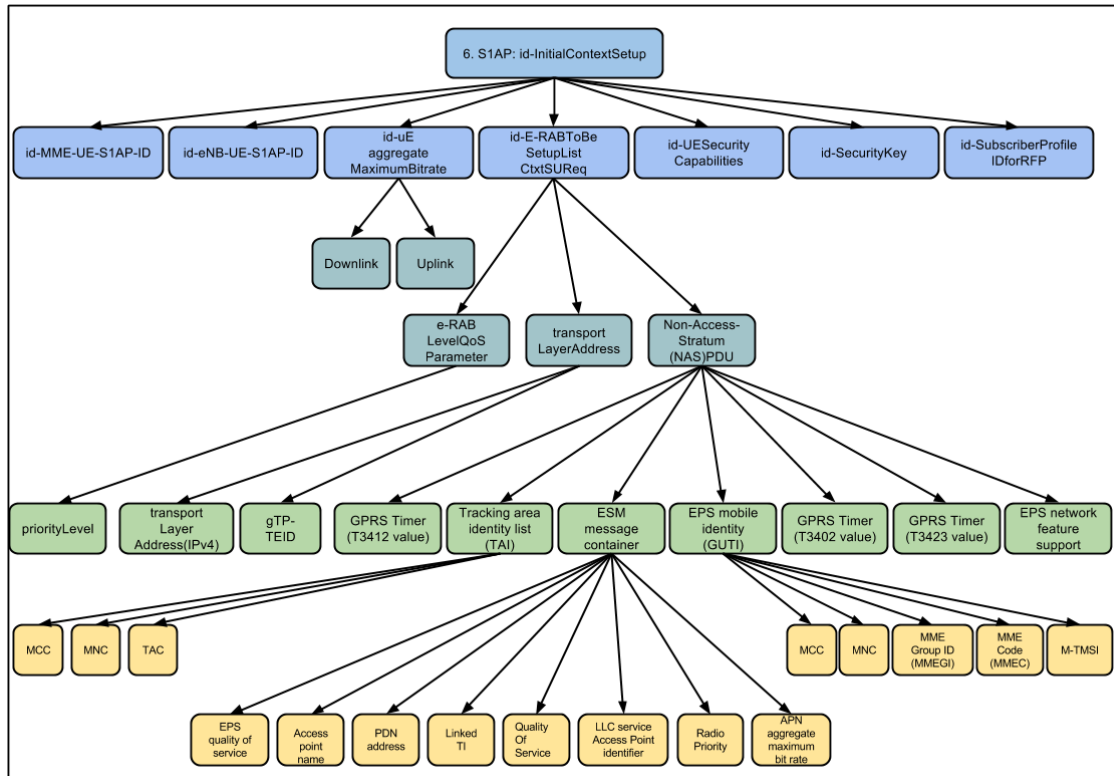
Seuraavaksi tarkastellaan viestien kaksi, kolme ja neljä sisältöä tarkemmin, jotka on esitetty kuvassa 23. Toisessa vaiheessa MME lähettää päätelaitteelle jo aiemmin mainitun autentikointihaasteen. Haaste sisältää RAND, AUTN ja KSI-ASME kuten wiresharkiin perustuvassa kuvassa on esitetty. Päätelaite lähettää vastauksen haasteeseen, joka reitittyy eNodeB:n kautta takaisin MME:lle. Tämä kuvassa oleva kolmas viesti sisältää tässä tapauksessa autentikointihaasteen halutun RES-arvon.

Neljännessä vaiheessa päätelaitteelle lähetetään jo aiemmin mainittu NAS yhteyden salauksen ja eheyden varmistus viesti. Tarkemmin tarkasteltuna kuvassa oleva EPS salausalgoritmi voisi olla tässä tapauksessa EEA0 ja EPS-eheysalgoritmi esimerkiksi 128-EA2-tyyppinen. KSI-ASME-tiedon lisäksi viesti sisältää myös päätelaitteen UE turvallisuus valmiudet. Seuraavaksi tarkastellaan viidettä viestiä, jonka sisältö on esitetty kuvassa 24.



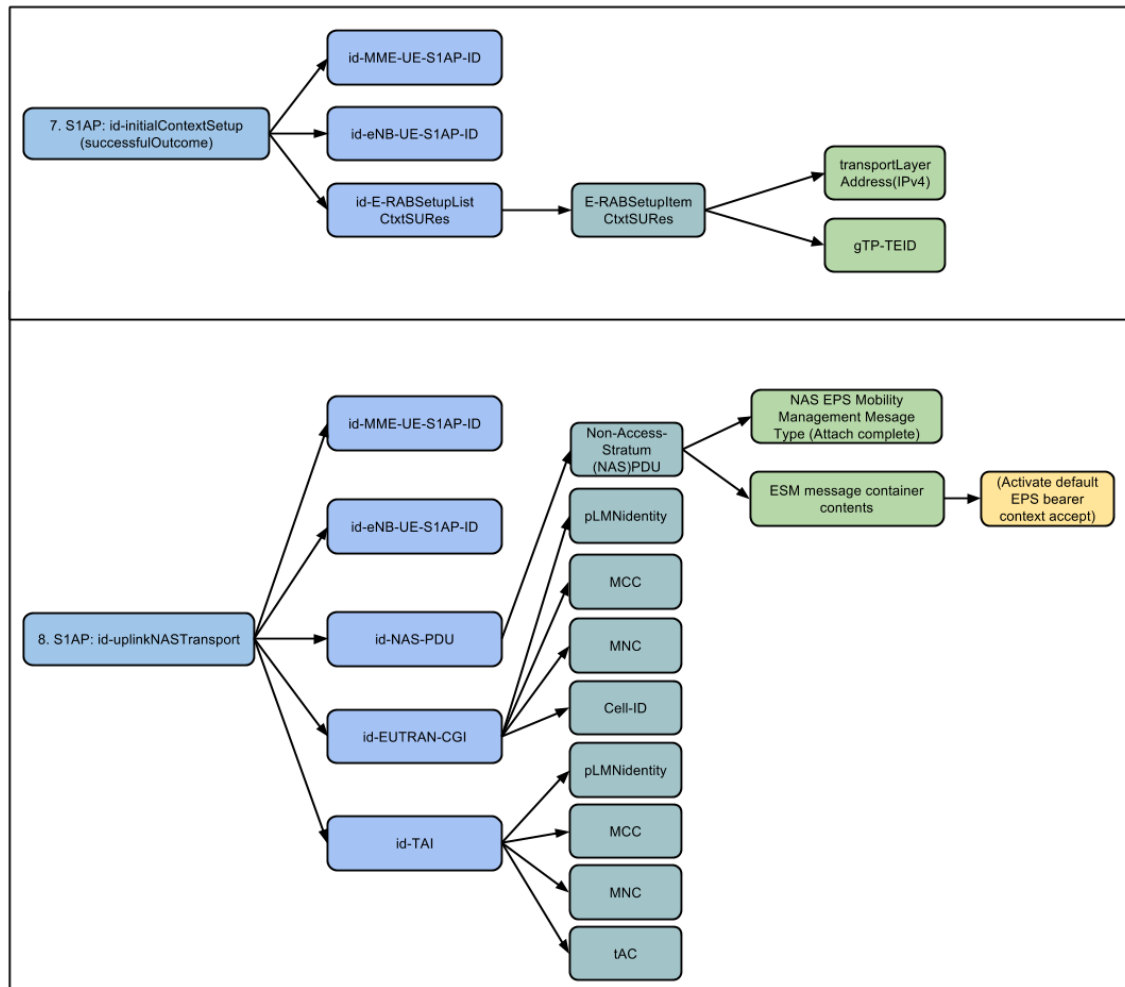
Kuva 24: Viides viesti NAS-yhteyden salauksen ja eheyden varmistusvaiheessa. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Viides viesti on vain vastaus tässä tapauksessa päätelaitteelta MME:lle onnistuneesta NAS-yhteyden salauksesta. Tämä tieto löytyy Wireshark-ohjelmalla ip-NAS-PDU-tietokentän alta.



Kuva 25: Kuudes viesti AS-yhteyden salauksen ja eheyden varmistuksessa. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Tästä eteenpäin siirrytään tarkastelemaan kuudetta viestiä, jonka tietorakenne hierarkisesti on esitetty kuvassa 25. AS-yhteyden salauksen ja eheyden varmistus vaiheessa viesti sisältää tärkeimpinä tietoina päätelaitteen turvallisuus valmiudet (id-UESecurityCapabilities) ja salausavaimen radiotukiasemalle (id-SecurityKey). GPRS Timer -arvot T3402, T3412 ja T3423 ovat normaaleja tähän vaiheeseen ja kuuluvat puhelimen rekisteröinti vaiheeseen. Tarkemmat selostukset eri GPRS Timer -arvoista löytyvät lähteestä 40. Tämän lisäksi gTP-TEID-osa kuvassa sisältää tiedot päätelaitteelta EPS-verkon läpi tulevasta signalointitunnelista, jota käytetään User Plane -yhteyden muodostuksessa. TransportLayerAddress-kohdassa on tässä tapauksessa päätelaitteen kuljetusprotokollan S1AP IP-osoite ja paketti sisältää myös Layer 3 -tasolla LTE-runkoverkon sisäisen IP-osoitteen, joka on saatu P-GW:ltä. Kuudennen viestin jälkeen siirrytään GTP-tunneliyhteyden avauksen toiseen vaiheeseen, jonka viestit on esitetty kuvassa 26. [40.]



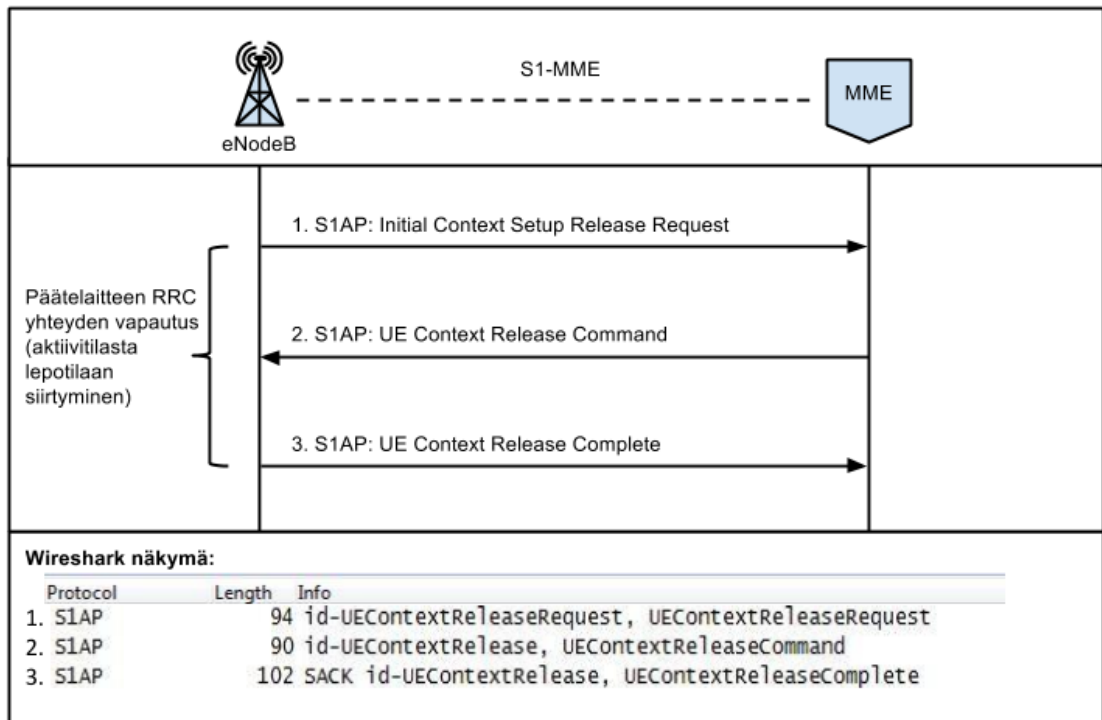
Kuva 26: Seitsemäs ja kahdeksas viesti GTP-tunneliyhteyden muodostuksessa (osa2). Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Radiotukiasema lähettää tässä vaiheessa vain varmistusviestin, että AS-yhteyden salaus onnistui. Viesti sisältää tämän lisäksi käyttäjän ulkoisen yhteyskohteen IP-osoitteen sekä gTP-TEI -tiedot päätelaitteelta EPS-verkon läpi tulevasta signalointitunnelista, jotka on esitetty kuvassa 26.

Viimeisenä viestissä kahdeksan radiotukiasema ilmoittaa MME:lle Non-Access-Stratum (NAS)PDU -tietoa alueen avulla, että päätelaite on kytkeytynyt verkkoon onnistuneesti (Attach complete) ja (Activate default EPS bearer context accept) pyynnön. Tähän päättyy radiotukiaseman ja MME:n välillä käyty vuoropuhelu käyttäjän rekisteröityessä verkkoon onnistuneesti.

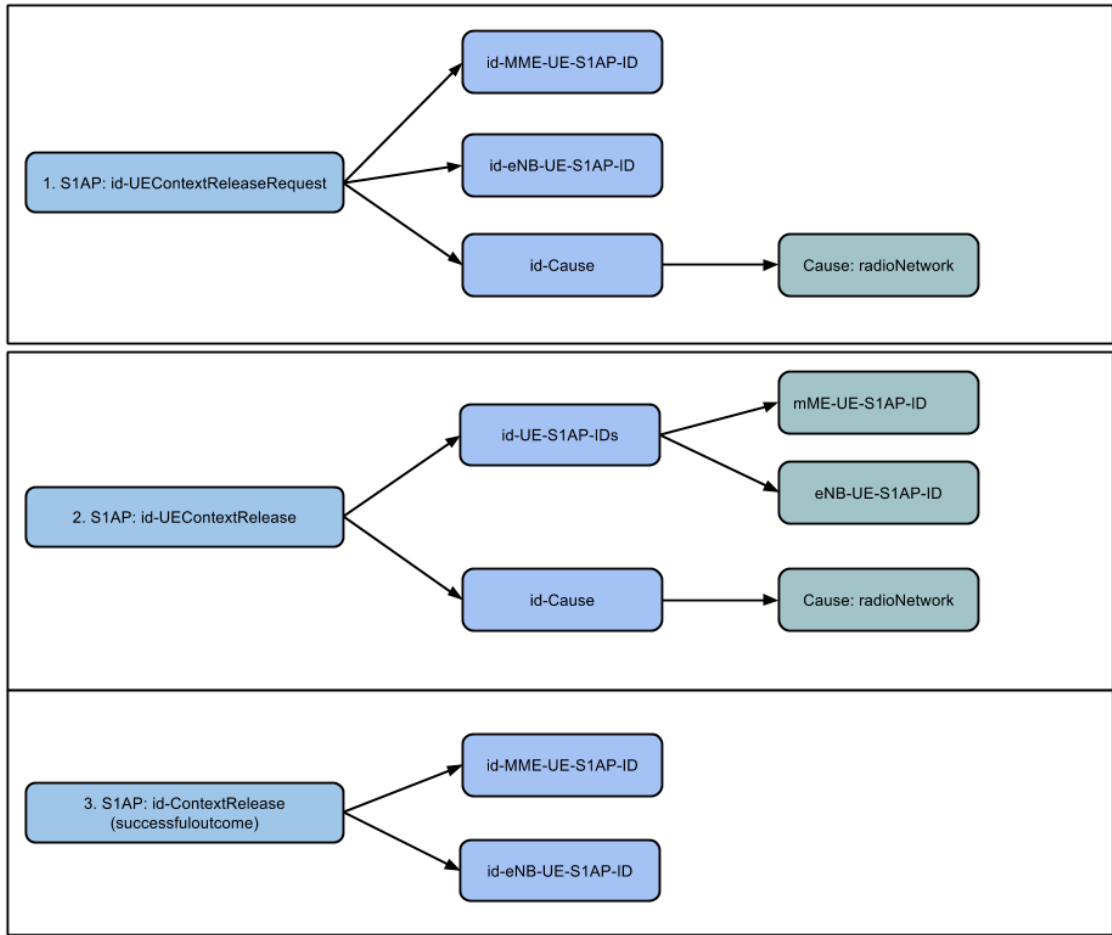
5.3.2 Päätelaitteen siirtyminen aktiivitulasta lepotilaan

Seuraavaksi käydään aiemmin mainittu välivaihe päätelaitteen siirtymisestä lepotilaan eli RRC-yhteyden vapautus. Tässä syynä voi olla monia kuten radioyhteyden katkeaminen äkillisesti mennessä tunneliin, päätelaitteen vaihto eri radiotukiasemalle eli handover tai aktiivitulassa olevan puhelimen siirtyminen lepotilaan.



Kuva 27: Päätelaitteen siirtyminen lepotilaan LTE-verkossa. Kuvan tekemiseen käytetty mallina kappaleen 4.4 kuvaa 12.

Kuvassa 27 näytetään miltä todellisuudessa aiemmin käyty päätelaitteen siirtyminen lepotilaan vaihe näyttää Wiresharkilla.



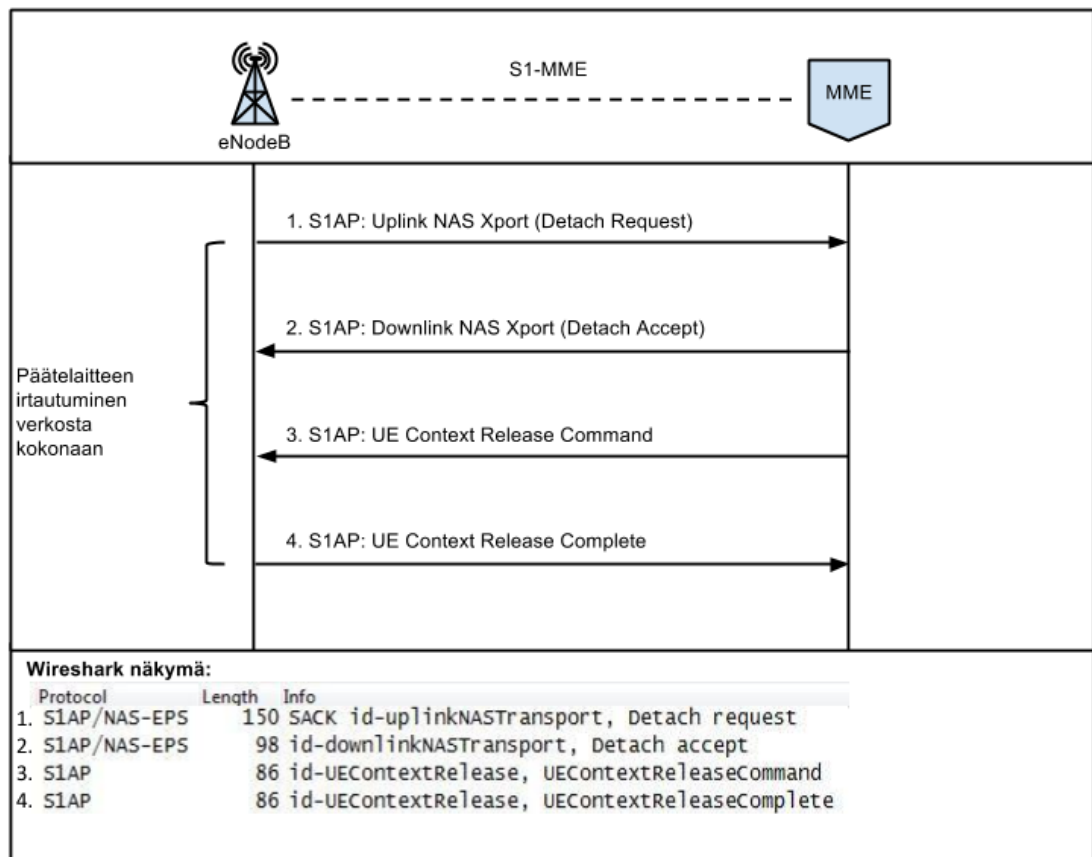
Kuva 28: Viestit 1-3 päätelaitteen siirtymisessä lepotilaan eli RRC-yhteyden vapautus. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Tarkemmin tarkasteltuna käskyjen sisältö näytetään yllä olevassa kuvassa 28. Siinä on esitetty pakettien rakenne RRC-yhteyden vapautuksessa. Ensimmäisessä viestissä olennainen tieto on `id-MME-UE-S1AP-ID`, jolla tunnistetaan päätelaitteen S1AP-yhteys muiden verkkokäyttäjien päätelaitteista ja `id-eNB-S1AP-ID`, jolla tunnistetaan oikean radiotukiaseman ja MME:n välinen S1AP-yhteys. Viimeisenä on `id-Cause`-tietokenttä, joka sisältää syyn, miksi käyttäjän RRC-yhteys vapautetaan.

Seuraavassa viestissä kaksi MME lähettää pyynnön radiotukiasemalle eNodeB päätelaitteen RRC-yhteyden vapautuksesta ja viimeisessä kolmannessa viestissä ilmoitetaan onnistuneesta operaatiosta.

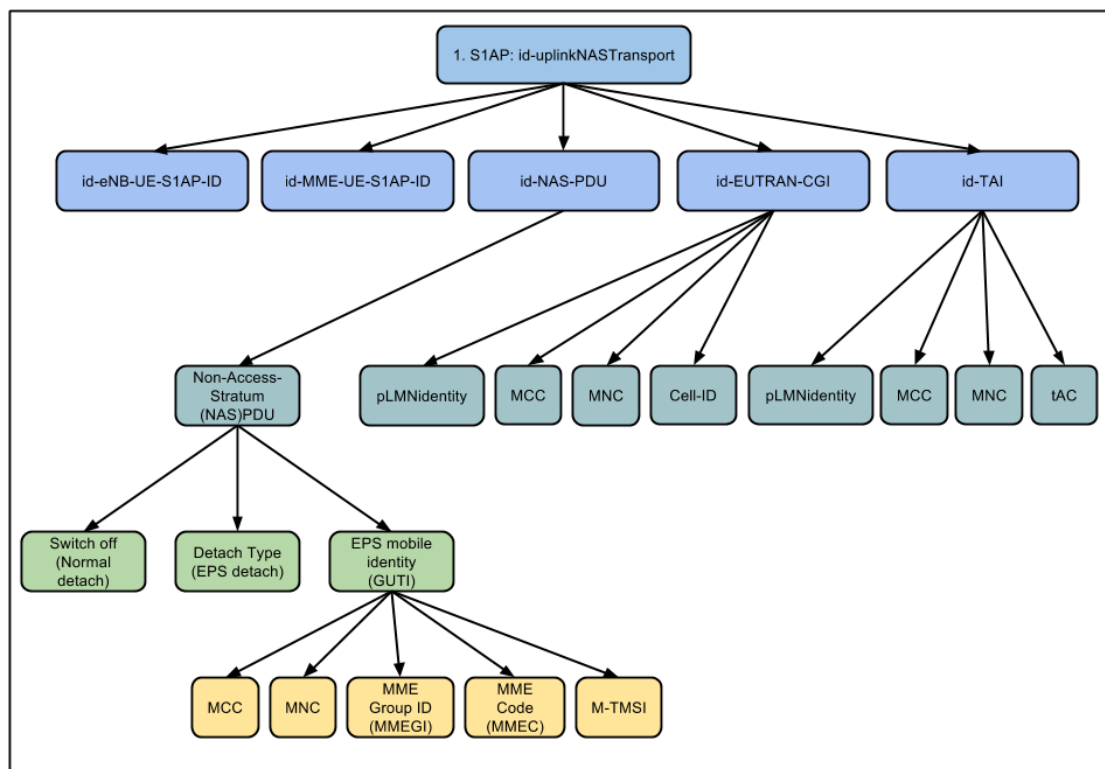
5.3.3 Päätelaitteen irtautuminen verkosta kokonaan

Seuraavaksi tässä luvussa tarkastellaan, miten päätelaite irrottautuu LTE-verkosta kokonaan. Syitä voi olla monia muitakin mutta tässä tapauksessa tarkastelemme normaalia tilannetta missä päätelaite suljetaan. Englanniksi tätä operaatiota kutsutaan nimellä Detach.



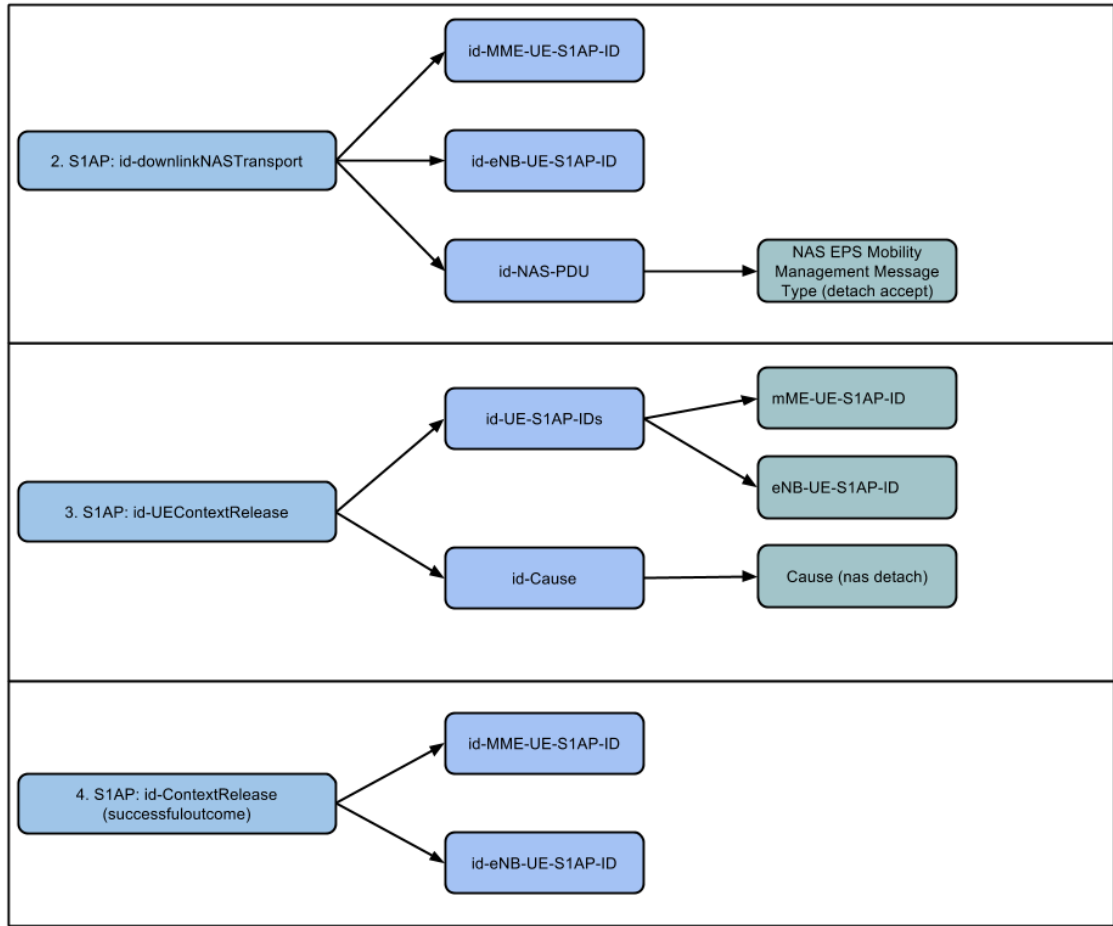
Kuva 29: Päätelaitteen siirtyminen irtautuminen LTE-verkosta. Kuvan tekemiseen käytetty mallina kappaleen 4.5 kuvia 14 ja 15.

Kuvassa 29 on esitetty aiemmin käyty päätelaitteen irtautuminen verkosta kokonaan mutta tällä kertaa wireshark-näkymän kanssa. Tarkastellessa yksittäisiä viestejä ja niiden sisältöä tarkemmin siirrytään kuvaan 30, jossa on esitetty ensimmäisen viestin sisältö tarkemmin.



Kuva 30: Ensimmäinen viesti päätelaitteen irtautumisessa LTE verkosta. Kuvan hierarkiarakenne perustuu Wiresharkista saattuihin tietoihin.

Radiotukiasema aloittaa päätelaitteen irtautumisoperaation välittämällä pyynnön MME:lle. Tässä tapauksessa tärkeät tiedot löytyvät tässä kuvassa id-NAS-PDU, id-EUTRAN-CGI ja id-TAI kohdista. Ensimmäisestä mainitusta id-NAS-PDU sisältää tiedot millainen irtautumisoperaatio on kyseessä (normal detach) ja mitä tästä seuraa (EPS detach eli päätelaitteelta EPS-verkon läpi tulevan signaalintunnelin sulkemista kokonaan). Tästä tietojoukosta löytyy myös päätelaitteen GUTI. id-EUTRAN-CGI tietokenttä kertoo käyttäjää palvelevan radiotukiaseman eNodeB:n tarkat tiedot ja id-TAI-radiotukiasemien muodostaman alueen tiedot (Tracking area identity).

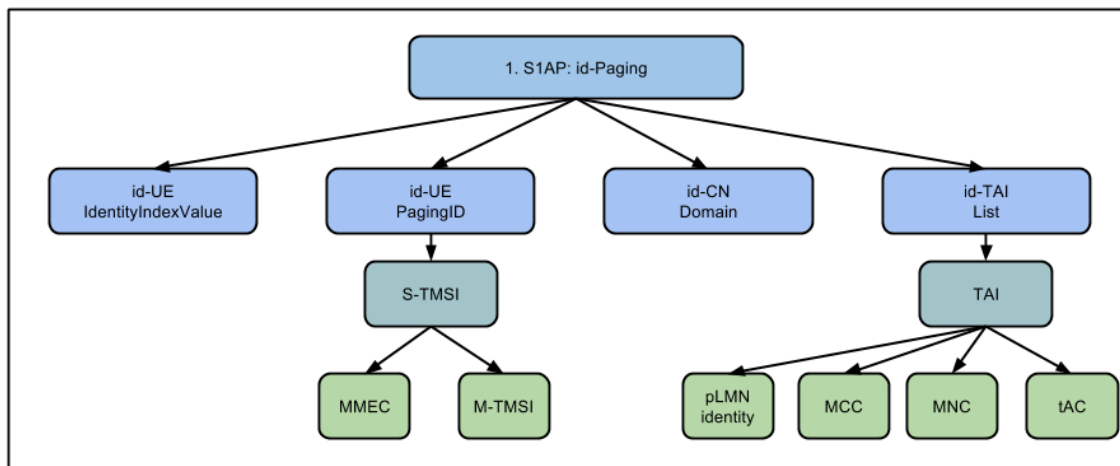


Kuva 31: Viestit 2-4 päätelaitteen irtautumisessa LTE-verkosta. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Seuraavat viestit muistuttavat rakenteeltaan aiemmassa luvussa käytyä päätelaitteen RRC-yhteyden vapautusvaihetta ja ne on kuvattu kuvassa 31. Näistä toisessa viestissä erona kuitenkin on id-NAS-PDU tietokentän sisältämä tieto onnistuneesta päätelaitteen GTP-yhteystunnelin poistosta (detach accept). MME lähettää heti tämän jälkeen viestin kolme, jossa kerrotaan käyttäjän RRC-yhteyden irtautumisen syy. Tässä tapauksessa se on päätelaitteen UE- ja MME-verkkoelementin välinen NAS-yhteyden katkeaminen (nas detach). Viimeisessä viestissä radiotukiasema eNodeB lähettää vielä vastauksen MME:lle onnistuneesta päätelaitteen irtautumisesta.

5.3.4 Verkon mainostus eli paging

LTE-verkon toiminnan teorialuvussa 4 mainittiin lyhyesti paging-viesteistä LTE-verkossa. Esimerkkikuvassa 16 radiotukiasema eNodeB ja MME:n välillä viestin rakenne on seuraava:

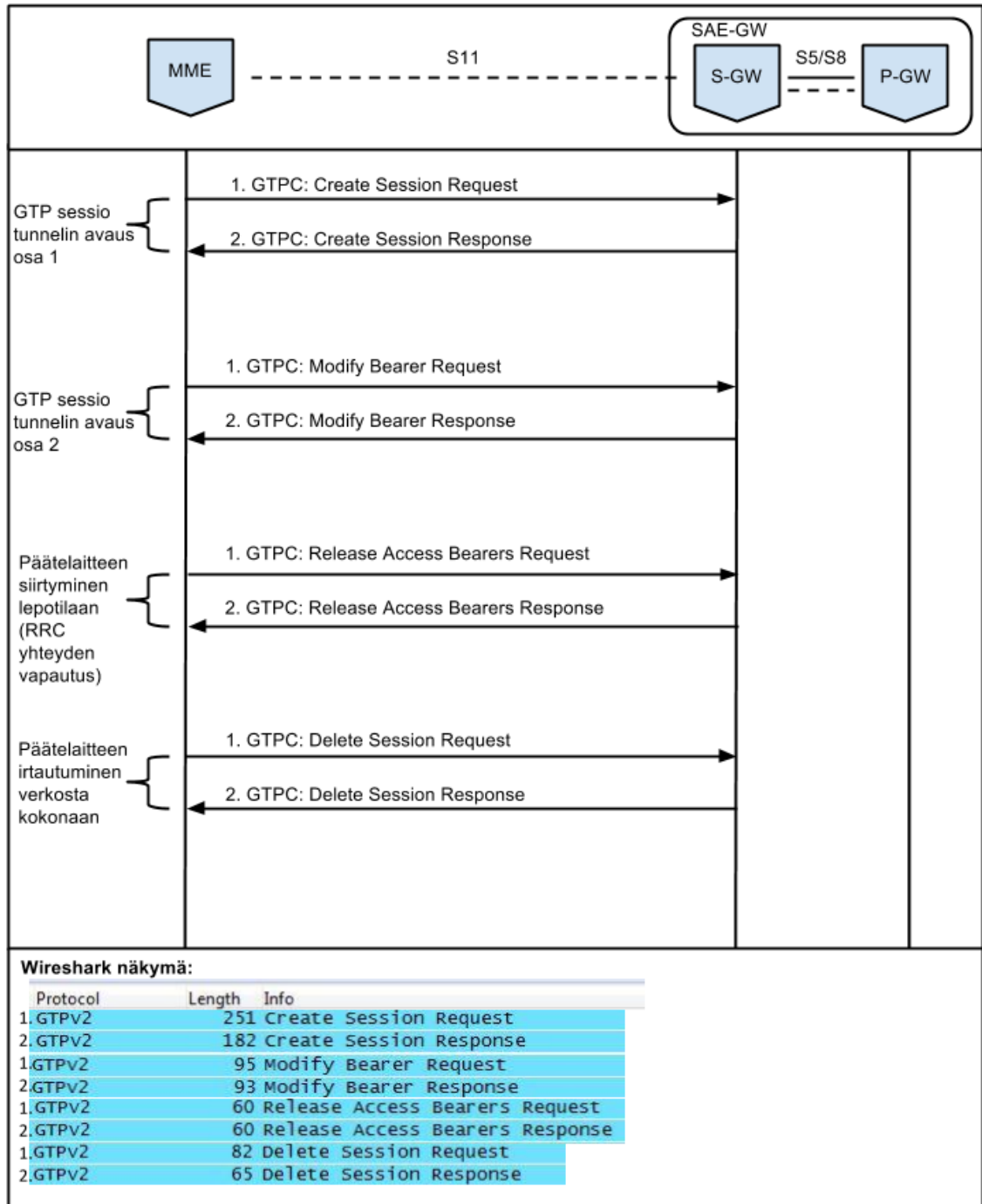


Kuva 32: Viesti 1 päätelaitteen Paging verkkomainostuksessa. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Paging-viesti sisältää tässä tapauksessa aiemmin mainitun päätelaitteen tunnistetiedon S-TMSI. Erikoistilanteessa, kun tätä päätelaitteen tunnistetietoa ei voi käyttää LTE-verkossa tunnistus tehdään IMSI-tiedoilla poikkeuksellisesti. Tämä on mahdollista mutta harvinaista. Paging-mainostusviesti sisältää myös päätelaitteen Tracking Area -tiedot.

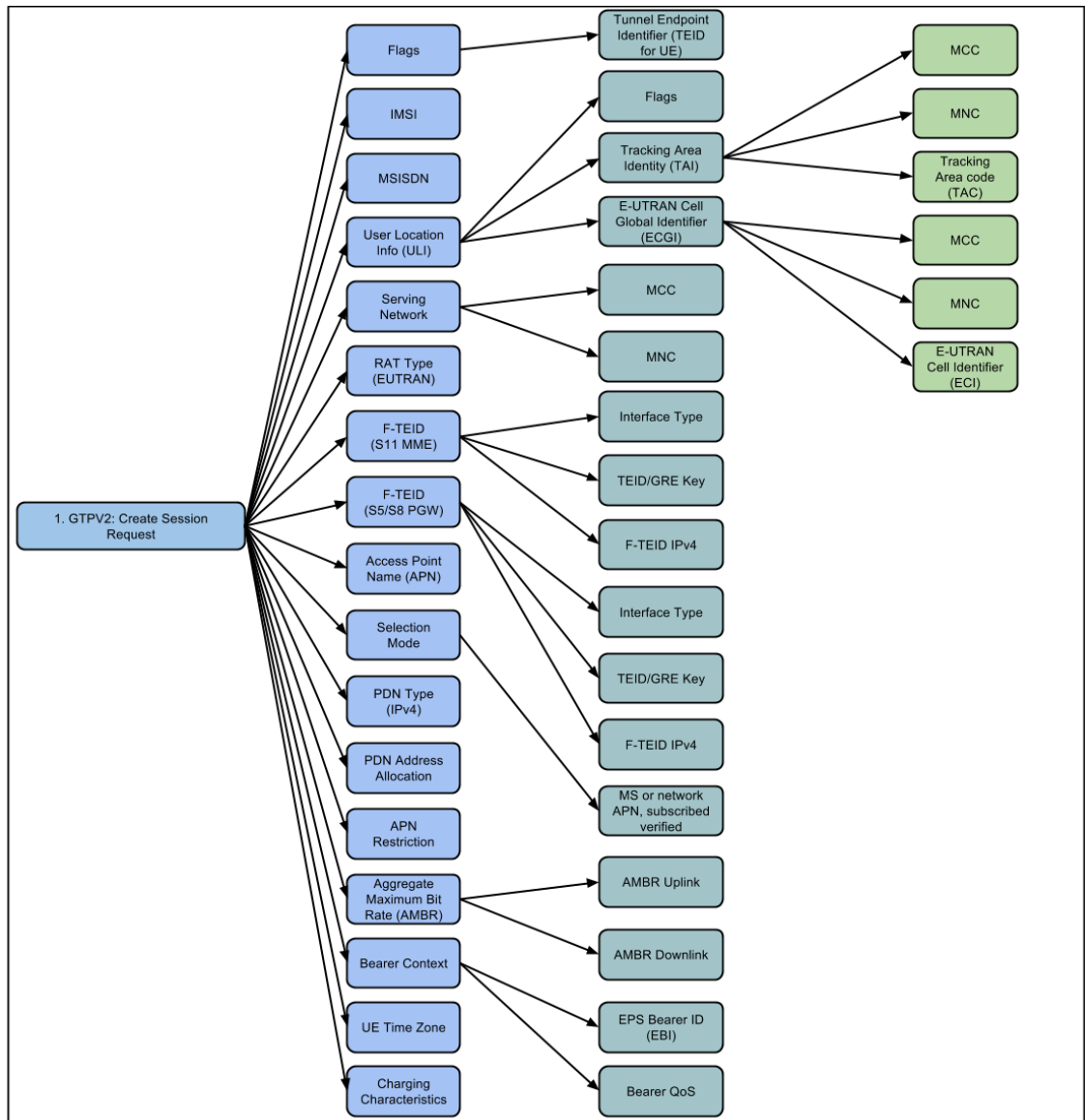
5.4 SAE-GW ja MME:n välillä

Tässä kappaleessa käsitellään paketteja MME:n ja SAE-GW:n välissä. Käsitellen verkkoelementtejä S-GW ja P-GW nimellä SAE-GW, koska todellisuudessa ne olivat virtualisoitu yhteen fyysiseen laitteeseen. Kuvassa 33 on esitetty kaikki aiemmin käydyt mahdolliset välivaiheet näiden verkkoelementtien välillä wireshark-näkymällä.



Kuva 33: MME:n ja SAE-GW:n välillä kulkeva liikenne. Kuvan tekemiseen käytetty aiempia kuvamalleja 9, 10 ja 12.

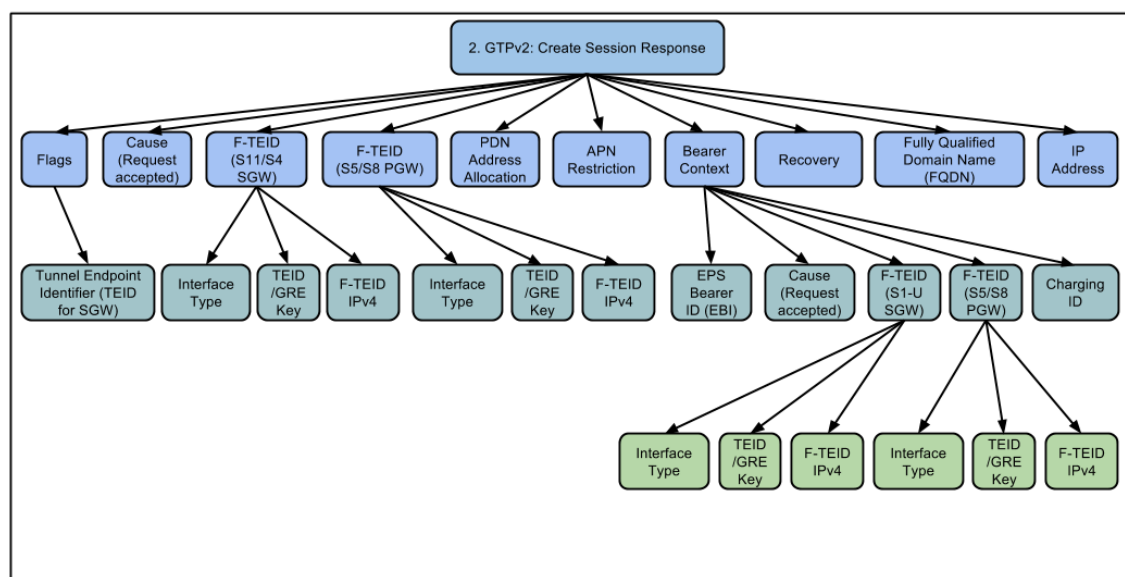
Tässä tapauksessa aiemmin mainitut GTP-C- ja GTP-U-protokollayhteydet ovat todellisessa tilanteessa muotoa GTPV2. Suuren kuvakoon takia ensimmäisen paketin rakenne kuvan hierarkia on käännetty sivuttain, jotta se mahtuisi tähän insinööriyöhön.



Kuva 34: GTP-tunneliyhteyden avauksen (osa 1) ensimmäinen viesti. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Kuvassa 34 GTP-tunneliyhteyden avauksen ensimmäinen viesti sisältää Flags tietoalueen alta päätelaitteelle varatun TEID-tunnistetiedon, joka ei tässä vaiheessa vielä sisällä mitään. Tämän lisäksi kuvassa hierarkiassa toisella tasolta löytyy IMSI- ja MSISDN (puhelinnumero) -tiedot. Käyttäjän paikantamista varten tietoalueesta User Location Info löytyy Tracking Area Identity tiedot eli radiotukiasemien muodostaman alueen tarkkuudella missä päätelaite on sekä ECGI-tieto, joka kertoo käyttäjän vieraileman E-UTRAN-verkkoalueen yksittäisen alueen radiotukiaseman tarkkuudella. Serving Network -tietoalue kertoo tässä tapauksessa käyttäjä palvelevasta

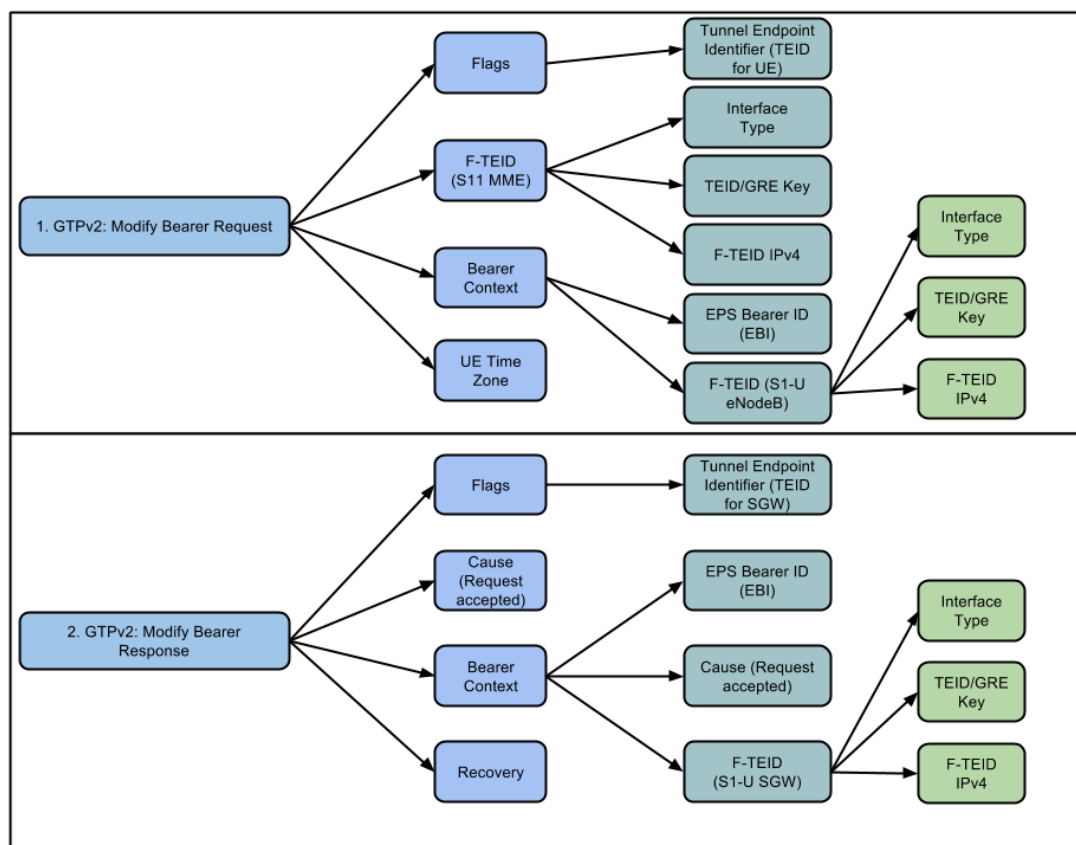
operaattorista ja maa-alueesta. RAT Type kertoo, millä radiotukiasemien muodostamalla alueella päätelaite ja tässä tapauksessa kyse on LTE-verkon E-UTRAN-alueesta. Paketti sisältää myös tiedot MME:n F-TEID ja P-GW:n F-TEID-tunnistetiedot, jota tarvitaan EPS-verkon läpi avattavaa Control Plane -signalointitunneliyhteyttä varten. Access Point Name kertoo tässä tapauksessa S-GW:n verkkonimen. Paketissa oleva Selection Mode tietoalueesta voidaan päätellä minkä tyyppinen päätelaite on ja onko sen verkonkäyttölupa varmistettu aiemmin. PDN Type -tietoalue kertoo verkkotyyppin, mikä voisi tässä tapauksessa olla IPv4. APN restriction kertoo, onko päätelaitteella mitään rajoituksia liittyen verkkoelementtiin P-GW. Aggregate Maximum Bit Rate (AMBR) kertoo lataus- ja lähetylinkin suurimman sallitun bittinopeuden. EPS-signalointitunnelin varten paketista löytyy myös EPS Bearer ID -tunnistetiedot sekä signalointitunnelin ja päätelaitteelle taatun palvelun laadun, mikä löytyy Bearer QoS -tietoalueesta. Kaikkien näiden tietojen lisäksi ensimmäinen paketti sisältää tässä tapauksessa päätelaitteen vierailijan aika-alueen tiedot (UE Time Zone) sekä laskutustiedot (Charging Characteristics).



Kuva 35: GTP-yhteystunnelin avauksen (osa 1) toinen viesti. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

GTP-yhteystunnelin avauksen ensimmäisen viestin jälkeen S-GW lähettää vastauksen takaisin MME:lle, joka on esitetty kuvassa 35. Viesti sisältää Flags-tietokentän alta S-GW:n TEID -tiedot. Lisäksi hierarkian toisella tasolla kuvassa Cause tietokentässä kerrotaan onnistuneesta GTP-tunnelisession kyselyn vastauksesta. Tämä lisäksi viesti

sisältää S-GW- ja P-GW-verkkoelementtien F-TEID-tunnistetiedot EPS-signaalointitunnelin Control Plane -yhteyttä varten. Vastaus sisältää myös jo aiemmassa GTP-tunnelisession avauksessa tutun PDN Address Allocation eli IP-osoitteiden jakamistiedot. APN Restriction kertoo tässä tapauksessa S-GW:n rajoitetiedot. Bearer Context -tietoalueesta löytyy taas tuttu EPS Bearer ID -signaloinnintunnistetieto sekä jo aiemmin mainittu tietokenttä Cause. Eronen aiempaan viestiin Bearer Context -tietoalue sisältää S-GW:n ja P-GW:n F-TEID-tunnistetiedot kohta avattavaa EPS-verkon läpi kulkevaa User Plane -tunneliyhteyttä varten. Viimeisenä operaattorilla pitää olla myös tunnistetieto asiakkaan päätelaitteen laskutusta varten (Charging ID). Kaiken tämän lisäksi viesti sisältää ulkoverkon Fully Qualified Domain Name (FQDN) -nimitiedon sekä päätelaitteen ulkoverkon IP-osoitteen.

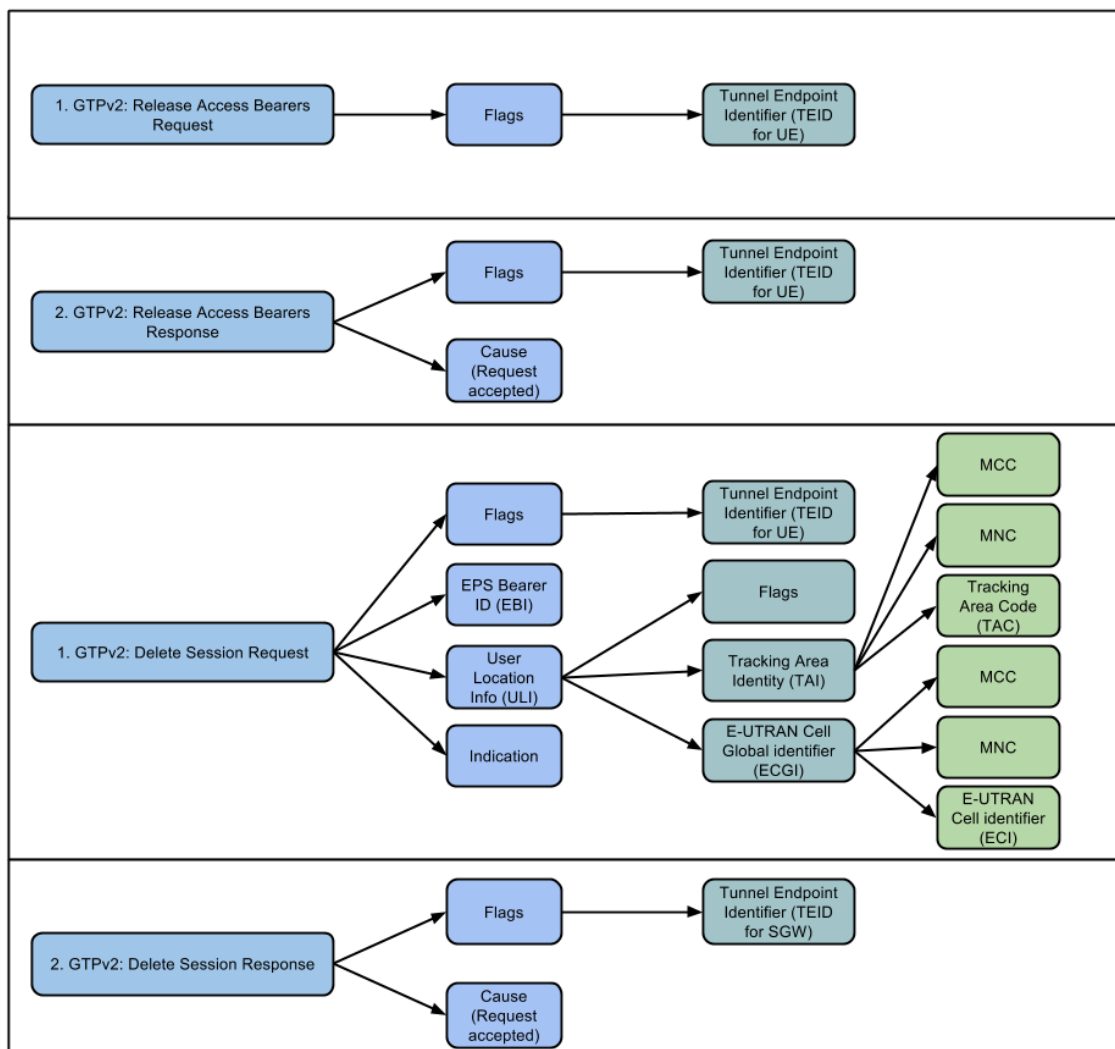


Kuva 36: GTP-yhteystunneli avauksen (osa 2) viestit 1 ja 2. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

GTP-yhteystunnelin avauksen toisessa vaiheessa, joka on esitetty yllä olevassa kuvassa 36 päätelaite lähettää omat EPS-verkon läpi kulkevat tunnistetiedot, jotka löytyvät kuvasta Bearer Context tietoalueen alta nimellä EPS Bearer ID. Tämän lisäksi

sieltä löytyy myös eNodeB:n TEID-tunnistetiedot nimellä F-TEID (S1-U eNodeB) User Plane -datatunneli yhteyden avausta varten. Ensimmäinen viesti sisältää myös päätelaitteen vierailuman aika-alueen tiedot (UE Time Zone) sekä TEID-tiedot MME:lle tulevasta Control Plane yhteydestä (F-TEID S11 MME). Lisäksi viestissä on Flags-tietokentän alla päätelaitteen TEID-tiedot.

S-GW vastaa tähän viestiin MME:lle, jossa kerrotaan Flags-tietokentän alla S-GW:n TEID-tiedot sekä aiemman viestin onnistuneesta vastaanottamisesta (Cause). Viesti sisältää muuten samalla tavalla päätelaitteen EPS-verkon signaloinnin identiteetin tunnistetiedot (EPS Bearer ID) ja tämän lisäksi sieltä löytyy myös S-GW TEID-tiedot nimellä F-TEID (S1-U SGW) User Plane -datatunneli yhteyden avausta varten.



Kuva 37: Päätelaitteen siirtyminen lepotilaan ja verkosta irtautuminen. Kuvan hierarkiarakenne perustuu Wiresharkista saatuihin tietoihin.

Tämän jälkeen siirrytään päätelaitteen lepotilaan ja verkosta irtautumiseen liittyviin vaiheisiin, jotka on kuvattu kuvassa 37. Päätelaitteen siirtyessä lepotilaan tästä lähtee tieto S-GW:lle, jotta päätelaitteelta EPS-verkon läpi kulkeva User Plane - datatunnelyhteys voidaan vapauttaa väliaikaisesti. Kuvassa ensimmäisessä viestissä MME välittää viestin S-GW:lle, joka sisältää päätelaitteen TEID-tiedot User Plane datatunnelyhteyden vapautusta varten Flags tietoaalueen alla. S-GW vastaa tähän toisella viestillä, joka sisältää kuittauksen päätelaitteen TEID-tiedoista sekä syyn viestin lähetykseen. Tässä tapauksessa datatunnelyhteyden vapautus onnistui.

Kuvassa 37 on esitetty tämän jälkeen myös, mitä tapahtuu, kun päätelaite irtautuu verkosta kokonaan. Ensimmäisessä viestissä kerrotaan päätelaitteen TEID-tiedot Flags tietoaalueen alla ja EPS-signaloinnin tunnistustiedot (EPS Bearer ID). Käyttäjän paikkatiedoista (User Location Info) löytyy Tracking Area ID -tietoaalue, joka ilmoittaa päätelaitteen sijainnin radiotukiasemien muodostaman alueen tarkkuudella. Samasta paikasta löytyy myös tarkemmat sijaintitiedot yksittäisen radiotukiaseman tarkkuudella tietoaalueesta E-UTRAN Cell Global Identifier. Viimeisessä eli toisessa viestissä kerrotaan S-GW:n TEID-tiedot ja ilmoitetaan onnistuneesta datayhteystunnelin sulkemisesta.

6 Yhteenveto

Tämän insinööriyön tarkoituksena oli tarkastella LTE-verkon toimintaa paketti ja käskytasolla Metropolia Ammattikorkeakoulun rakentaman verkon mittakaavassa. Alkuperäinen idea oli verrata toiminnan teoriaa wiresharkilla saatuihin tuloksiin, mutta lopulta työssä yhdistettiin teoria ja käytäntö toisiinsa.

Työssä käsiteltiin LTE-verkkoa pala palalta tarkemmin. Toisessa luvussa käytiin LTE-verkon loogisen topologian rakenne läpi verkkoelementteineen ja keskeisine tehtävineen. Tästä siirryttiin tarkastelemaan tietoa ja käskyjä kuljettavien protokollapinojen rakennetta eri verkkoelementtien välillä. Työn neljännessä luvussa käytiin läpi erilaiset välivaiheet päätelaitteen kytkeytyessä ja irrottautuessa LTE-verkosta. Viimeinen luku tarkasteli näiden yksittäisten käskyjen sisältöä tarkemmin wiresharkista saatujen tietojen avulla. Tuloksena syntyi opas LTE-verkon toiminnasta paketti ja käskytasolla, jota voidaan hyödyntää oppimateriaalina.

Kaikkea ei ehditty tutkimaan tässä insinööriyössä, koska aihe oli laaja paketti ja käskytasolla tarkasteltuna. Radiorajapinnan tarkastelu päätelaitteen ja eNodeB-verkkoelementin välillä luvussa 5 wiresharkin avulla jäi tekemättä. Niinpä työtä voitaisiin kehittää vielä eteenpäin ja laajentaa jopa LTE roaming -mittakaavaan. Työn tarkoituksena on toimia teoria ja käytännön pohjana LTE-verkon toiminnan tarkastelussa paketti- ja käskytasolla.

Lähteet

- 1 Harri Holma ja Antti Toskala. 2010. LTE for UMTS: Evolution to LTE-Advanced (2nd Edition). Iso-Britannia: John Willey & Sons, Ltd.
- 2 Välimäki, Ville. 2012. LTE-verkko opetuskäyttöön. Metropolia Ammattikorkeakoulu Helsingin yksikkö, tietotekniikka ja tietoliikennetekniikka, insinööriyö.
- 3 LTE-SAE architecture and performance. Verkkodokumentti. http://www.ericsson.com/ericsson/corpinfo/publications/review/2007_03/file/5_LTE_SAE.pdf. Luettu 11.2.2014.
- 4 LTE Quick Guide. Opetusverkkomateriaali. http://www.tutorialspoint.com/lte/lte_quick_guide.htm. Luettu: 28.3.2014.
- 5 LTE Protocols & Specifications. Verkkodokumentti. [Iteworld.org/lte-protocols-specifications](http://www.iteworld.org/lte-protocols-specifications). Luettu 28.4.2014.
- 6 Mobility management. Verkkodokumentti. http://en.wikipedia.org/wiki/Mobility_management. Luettu 28.4.2014.
- 7 Sauter Martin. 2011. From GSM to LTE : An Introduction to Mobile Networks and Mobile Broadband. Iso-Britannia: John Wiley & Sons, Ltd.
- 8 Agilent Technologies Staff Rumney, Moray. 2013. LTE and the Evolution to 4G Wireless: Design and Measurement Challenges (2nd Edition).
- 9 LTE Security for new user. Verkkodokumentti. <http://www.eventhelix.com/lte/security/lte-security-session-setup.pdf>. Luettu 4.3.2014.
- 10 Diameter (protocol). Verkkodokumentti. [http://en.wikipedia.org/wiki/Diameter_\(protocol\)](http://en.wikipedia.org/wiki/Diameter_(protocol)). Luettu 26.2.2014.
- 11 Long Term Evolution (LTE): A Technical Overview. Verkkodokumentti. http://www.motorolasolutions.com/web/Business/Solutions/Industry%20Solutions/Service%20Providers/Wireless%20Operators/LTE/_Document/Static%20Files/6834_MotDoc_New.pdf. Luettu 6.3.2014.
- 12 S1 Signalling Transport. Verkkodokumentti. <http://www.iteworld.org/specification/s1-signalling-transport>. Luettu 27.2.2014.

- 13 Introduction to Long-Term Evolution (LTE). Kalvosarja.
http://wmnet.cs.nthu.edu.tw/Course/PCS2013/slides/10_Intro_to_LTE_simplified_new.pdf. Luettu 27.2.2014.
- 14 S5/S8 Interface. Verkkoartikkeli. <http://lteguide.blogspot.fi/2011/11/s5s8-interface.html>. Luettu 27.2.2014.
- 15 The LTE Network Architecture. Verkkodokumentti.
http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE_Alcatel_White_Paper.pdf. Luettu 27.2.2014.
- 16 LTE Security Key Hierarchy. Kalvosarja.
<http://www.eventhelix.com/lte/security/lte-security-presentation.pdf>. Luettu 28.2.2014.
- 17 Irfan Ali. LTE Security Overview. Kalvosarja.
<http://www.slideshare.net/aliirfan04/lte-security-overview>. Luettu 28.2.2014.
- 18 Irfan Ali. LTE & EPC Architecture / LTE Attach Procedure. Kalvosarja.
<http://www.slideshare.net/aliirfan04/lte-architecture-and-lte-attach>. Luettu 28.2.2014.
- 19 LTE Attach and Default Bearer Setup Flow. Verkkodokumentti.
<http://www.eventhelix.com/lte/attach/lte-attach.pdf>. Luettu 10.3.2014.
- 20 Penttinen Jyrki. 2012. LTE/SAE Deployment Handbook. Iso-Britannia: John Wiley & Sons, Ltd.
- 21 Random Access Procedure in LTE. Verkkoartikkeli. <http://4g-lte-world.blogspot.fi/2013/04/random-access-procedure-rach-in-lte.html>. Luettu 3.3.2014.
- 22 LTE RRC Connection Setup Messaging. Kalvosarja.
<http://www.eventhelix.com/lte/attach/LTE-RRC-Connection-Setup-Messaging.pdf>. Luettu 28.4.2014.
- 23 LTE Initial Setup. Verkkoartikkeli. <http://wired-n-wireless.blogspot.fi/2009/09/lte-initial-setup.html>. Luettu 3.3.2014.
- 24 LTE Quick Reference: IDs in LTE. Verkkoartikkeli.
http://www.sharetechnote.com/html/Handbook_LTE_IDs_in_LTE.html. Luettu 28.4.2014.
- 25 MO Signalling vs MO Data. Kysymys internetissä.
http://lteuniversity.com/ask_the_expert/f/59/t/3844.aspx. Luettu 3.3.2014.

- 26 RRC protocol. Verkkoartikkeli.
http://www.artizanetworks.com/lte_tut_rrc_pro.html. Luettu 3.3.2014.
- 27 LTE Attach and Default Bearer Setup Messaging. Kalvosarja.
<http://www.eventhelix.com/lte/attach/LTE-Attach-Messaging.pdf>. Luettu 6.3.2014.
- 28 Public data network. Verkkoartikkeli.
http://en.wikipedia.org/wiki/Public_data_network. Luettu 6.3.2014.
- 29 Access Point Name. Verkkoartikkeli.
http://en.wikipedia.org/wiki/Access_Point_Name. Luettu 6.3.2014.
- 30 Maruti Gupta, Ali T. Koc, Rath Vannithamby. Intel Labs, Intel Corporation. Chapter 20 Power Management for 4G Mobile Broadband Wireless Access Networks. Kalvosarja.
http://booksite.elsevier.com/9780124158443/downloads/Chapter_21_PowerEff_Slides.ppt. Luettu 10.3.2014.
- 31 Arijit Satpathy. Test lead for Nokia Siemens Network, India. Paging in LTE. Blogiartikkeli. <http://lteinwireless.blogspot.fi/2012/12/paging-in-lte.html>. Luettu 10.3.2014.
- 32 Artiza Networks. C-plane Protocol Procedure. Verkkodokumentti.
http://www.artizanetworks.com/lte_tut_cpl_pro.html. Luettu 10.3.2014.
- 33 Paging. Verkkoartikkeli. http://www.sharetechnote.com/html/Paging_LTE.html. Luettu 10.3.2014.
- 34 Basic Call Processing – Typical Packet Call. Verkkodokumentti.
http://www.sharetechnote.com/html/BasicCallFlow_LTE.html. Luettu 11.3.2014.
- 35 Christopher Cox. 2012. An Introduction to LTE: LTE, LTE-Advanced, SAE and 4G Mobile Communications (2nd edition). Iso-Britannia: John Wiley & Sons, Ltd.
- 36 Knowing GUTI – Globally Unique Temporary ID. Verkkoblogi. <http://lte-epc.blogspot.fi/2009/11/knowning-guti-globally-unique-temporary.html>. Luettu 12.3.2014.
- 37 Surya Patar. 3GPP LTE training: RRC Paging. Kalvosarja.
<http://www.slideshare.net/spmunda/paging-in-lte>. Luettu 12.3.2014.
- 38 Kumar Swamy Pasupuleti. IOT Test Engineer Ericsson's Mobile Broadband Modules. RRC Connection Release.
<http://howteststuffworks.blogspot.fi/2011/11/rrc-connection-release.html>.

- 39 Long Term Evolution – Evolved Packet Core S1 Interface Conformance Test Plan. Verkkodokumentti. <http://www.msforum.org/techinfo/testplans/msf-p0044.031.pdf>.
- 40 Timer (EPS Mobile Management – UE Side). Verkkodokumentti. http://www.sharetechnote.com/html/Handbook_LTE_Timer_EPS_UE.html. Luettu: 21.3.2014.
- 41 LTE APN. Verkkootikkeli. <http://www.rcrwireless.com/lte/apn-lte.html> Luettu 27.3.2014.
- 42 About Wireshark. Verkkootikkeli. <http://www.wireshark.org/about.html>. Luettu 28.3.2014.
- 43 UDP – User Datagram Protocol. <http://ipv6.com/articles/general/User-Datagram-Protocol.htm>. Luettu 28.3.2014.

Liite 1: Metropolian LTE-verkosta tehty rakennekuva fyysisistä laitteista

