

Laboratóriumi segédlet

LTE hálózati vizsgálatok

Varga Pál és Olaszi Péter

BME-TMIT SmartCom Lab
2017

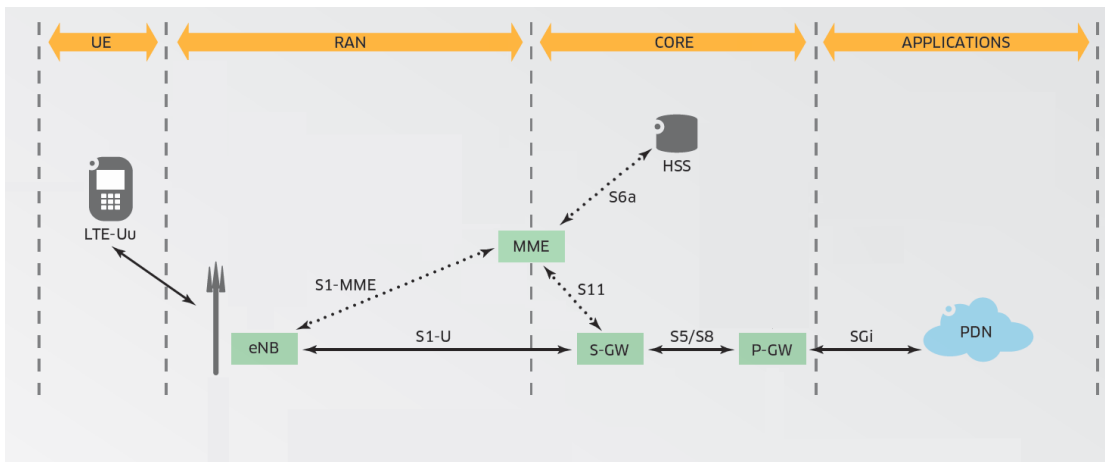
1 Bevezetés

1.1. A mérés célja

A mérés során a hallgatók megismerkednek az LTE mobil távközlő hálózat elemeivel és a berendezések közötti távközlési interfészekkel. A telepített teszhálózaton elsajátítják az üzembe helyezés és konfiguráció lépéseit. A jelzés- és a felhasználói csatorna vizsgálatával megismerkednek a végberendezés és a hálózat közötti távközlési protokollok alapvető procedúráival.

1.2. Az LTE mobil kommunikációs hálózat főbb komponensei

Az LTE mobil kommunikációs hálózat alapvető rendszerlemeit és az azok közötti távközlési interfészeket az 1.1 ábra mutatja be.



1.1. ábra. Az LTE kommunikációs hálózat alapvető rendszerlemei
Forrás: http://mars.merhot.dk/mediawiki/images/1/14/LTE_poster.pdf

A végberendezés (*User Equipment*, UE) az LTE-Uu interfészen keresztül kapcsolódik a rádiós hozzáférési hálózathoz (*Radio Access Network*, RAN). Végberendezésre például a mobiltelefon, mobil internettel rendelkező tablet, vagy laptop LTE USB modemmel. A hozzáférési hálózatot az LTE bázisállomások alkotják (Evolved Node-B, eNode-B/eNB/ENB).

1 Bevezetés

A végberendezés részét képezi az USIM kártya. Technikailag a kézbe fogható plasztiklapnak a benne található áramköri elemmel együtt a neve *Universal Integrated Circuit Card* (UICC). Ezen belül található a *Subscriber Identity Module* (SIM) nevű integrált áramkör, amely hardver formában valósítja meg a kártya azonosítási, titkosítási és adattárolási funkcióit. Az *Universal Subscriber Identity Module* (USIM) abban különbözik a SIM-től, hogy nagyobb tárhely van a telefonkönyv számára, hosszabb titkos kulcsot tud használni, és segítségével a végberendezés is képes a hálózat viszont-autentikációjára, ami a készüléket védetté teszi a hálózat nevében fellépő adathalászzal szemben. Ebben a dokumentumban a továbbiakban az *USIM kártya* kifejezés alatt az UICC plasztiklapot és a rajta elhelyezett USIM áramkört értjük.

Az eNB-k az aggregációs IP hálózaton keresztül kapcsolódnak az LTE maghálózat berendezéseire (*Evolved Packet Core*, EPC/Core). A jelzésréteg (*Control Plane*, CP) forgalma az eNB és a *Mobility Management Entity* (MME) között az S1-MME interfészen keresztül folyik.

A felhasználói réteg (*User Plane*, UP) a felhasználói adatforgalmat továbbítja az eNB és a *Serving Gateway* (S-GW/SGW) között az S1-U interfészen keresztül. A felhasználói adatforgalom a *Packet Data Gateway* (P-GW/PGW) berendezés közreműködésével, az SGI interfészen keresztül jut ki a nyilvános csomagkapcsolt adathálózatra (*Public Data Network*, PDN/Internet), illetve az azokon elérhető szolgáltatásokhoz és alkalmazásokhoz (*Applications*). A maghálózatban általában több SGW gyűjti össze az ENB-k felhasználói forgalmát, és továbbítja az (általában egy) PGW felé az S5/S8 interfészen keresztül.

Az MME az S11 interfészen keresztül vezérli az SGW-k működését. A felhasználói adatbázis és az előfizetői jogosultságok kezelését a *Home Subscriber Server* (HSS) végzi, amely az S6a interfészen keresztül kommunikál az MME-vel.

1.3. A mérőhely eszközei

1.3.1. Eszközök a végberendezés oldalán

- Mini PC, Windows 7 operációs rendszerrel. (Név: *Timelord*)
Ez valósítja meg a mobil végberendezés funkcióját.
- Huawei Vodafone K5150 LTE USB modem.
A végberendezés számára biztosítja az LTE rádiós összeköttetést.
- USIM kártya
Az LTE USB modemben helyezkedik el. Feladata a végberendezés és a hálózat közötti azonosítás és autentikáció.

A végberendezés funkcióját megvalósító *Timelord* mini PC és a hozzá kapcsolódó LTE USB modem az 1.2 ábrán látható.

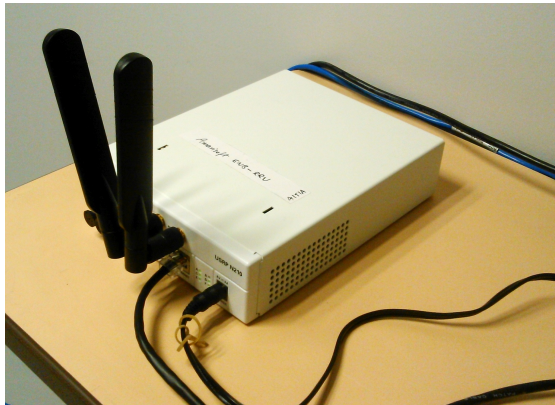


1.2. ábra. A végberendezés funkcióját a *Timelord* mini PC és a hozzá kapcsolódó LTE USB modem megvalósítja meg

1.3.2. Eszközök az LTE maghálózat oldalán

- Gigabyte GB-BXi7-4770R Mini PC (Név: *gig*)
Ezen az eszközön fut az LTE maghálózat (EPC) és a rádiós bázisállomás (ENB) funkcióját megvalósító két szoftvermodul. Operációs rendszer: Linux Fedora 23. LTE szoftver: Amari LTE.
- StarTech.com USB-to-Ethernet 3.0 adapter. MAC address: 00-0A-CD-27-D8-D0
A mini PC számára biztosít egy plusz Ethernet interfészt USB 3.0 porton keresztül. Ez az eszköz szolgál az SGi interfészként.
- Remote Radio Unit (RRU): Ettus-National Instrument USRP N210
Ez a bázisállomás (eNodeB) rádiós egysége.
- 2 db. 700-2600 MHz 4G LTE omnidirectional antenna
Az USRP N210 rádiós fejegység része.

Az LTE hálózat elemei a 1.3 ábrán láthatók. A rádiós egység (1.3a ábra) I/Q interfésze az Ethernet porton közvetlenül kapcsolódik a Gigabyte mini PC (1.3b ábra) beépített Ethernet portjára. A mini PC futtatja az EPC és ENB BBU szoftvermodulokat. Az SGi interfészt az USB-Ethernet átalakító (1.3c ábra) biztosítja – az LTE hálózat ezen keresztül eléri el a nyilvános csomagkapcsolt adathálózatot.



(a) A rádiós egység Ethernet porton keresztül kapcsolódik a *gig* mini PC-hez



(b) A *gig* mini PC futtatja az EPC és ENB BBU szoftvermodulokat



(c) Az SGi interfész USB-Ethernet porton biztosít kapcsolatot az Internettel

1.3. ábra. Az LTE hálózatot megvalósító rendszerelemek

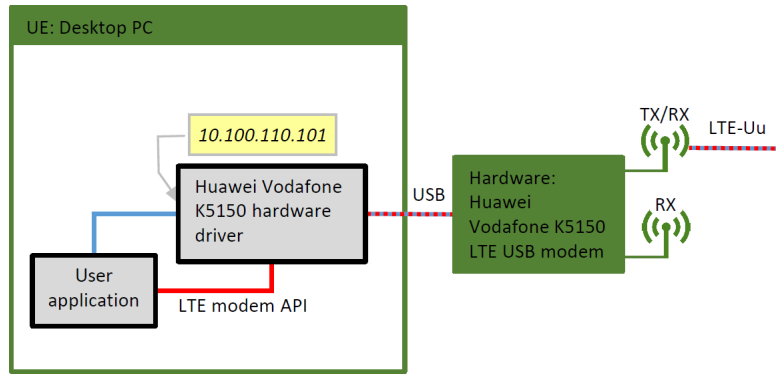
1.4. A mérési elrendezés

A mérési elrendezést a 1.4 és 1.5 ábrák mutatják be. A zöld keretek a hardverelemeket jelölik; baloldalt a 1.4 ábrán a felhasználói végberendezést alkotó *Timelord* mini PC-t, amelyhez az LTE USB modem csatlakozik. A UE az *LTE-Uu* rádiós interfészen keresztül kapcsolódik az USRP N210 rádiós fejegységhez (RRU), amely Ethernet interfészen kapcsolódik a Gigabyte mini PC-hez, amely egyben valósítja meg az ENB alapsávi egységének (*Baseband Unit*, BBU) és az LTE maghálózat (*Evolved Packet Core*, EPC) funkcióját (1.5 ábra).

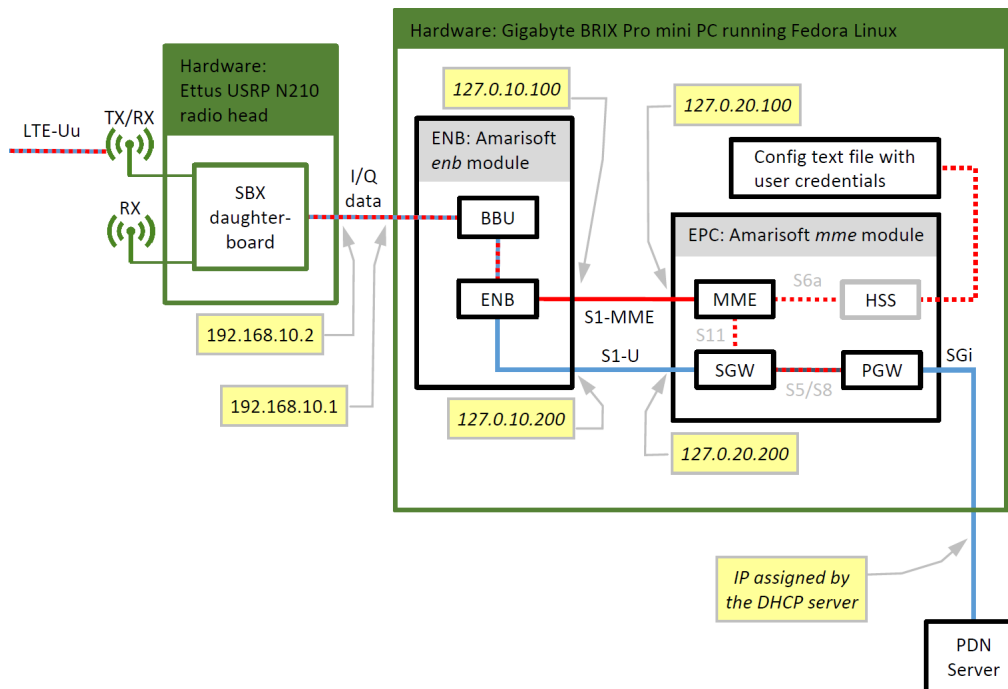
A fekete keretek a szoftvermodulokat jelölik. A végberendezés oldalán az LTE modem meghajtószoftverét és a felhasználói alkalmazást jelöltük. Az LTE hálózat oldalán az Amarisoft *enb* szoftvermodul az ENB + BBU funkcióit, az Amarisoft *mme* modul pedig az EPC (MME + SGW + PGW + HSS) funkcióit valósítja meg.

A modulok között a piros vonalak a jelzésréteg, a kék vonalak a felhasználói réteg interfészeit jelölik. A piros-kék szaggatott vonalak a kombinált csatornákat jelölik. Az ábrán fekete címke jelöli a megfigyelhető (monitorozható) interfészeket (USB, LTE-Uu, I/Q data, S1-MME, S1-U, SGi). Szürkével jelöltük a nem monitorozható, csak szoftvermodul belsejében megvalósított interfészeket (S11, S5/S8, S6a).

Sárga címkék jelölik a megfigyelhető interfészek IP címeit. A végberendezés számára



1.4. ábra. A mérési elrendezés a végberendezés oldalán



1.5. ábra. A mérési elrendezés az LTE maghálózat oldalán

ebben a mérési elrendezésben a *Smartjac 1* USIM kártyához a hálózat a *10.100.110.101* címet osztja ki. A hálózat oldalán az ENB BBU és RRU közötti I/Q interfész rendre a *192.168.10.1*, illetve *192.168.10.2* címeket kapja. A maghálózati funkciót megvalósító *gig* mini PC-n belül 4 külön IP címet vettünk fel a *loopback* interfészen az ENB és MME közötti S1-MME interfész (*127.0.10.100*, *127.0.20.100*), illetve az ENB és az SGW közötti S1-U interfész (*127.0.10.200*, *127.0.20.200*) vizsgálatára. Az SGi interfész PGW oldali IP címét a tanszéki hálózat DHCP szervere osztja ki.

2 Mérési feladatok

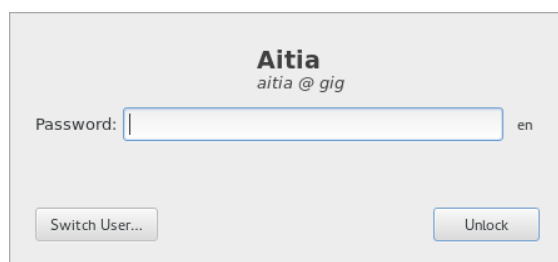
- A rendszer hardverelemeinek azonosítása.
- Az LTE hálózat szoftverelemeinek azonosítása.
- Az előfizetői adatbázis konfigurációjának vizsgálata. A maghálózat indítása.
- Az ENB konfigurációjának vizsgálata. Az ENB szoftvermodul elindítása. Az S1 interfész felépülésének ellenőrzése.
- Az LTE USB modem csatlakoztatása a *Timelord* PC-hez. Az *Attach* procedúra lépéseinek ellenőrzése a Hálózati oldalon futtatott *Wireshark*-kal. A felhasználó-azonosítás, autentikáció, kulcsválasztás, és alapértelmezett vivő kiosztási lépéseinek végigkövetése.
- A végberendezés oldalán az LTE USB modem kliensszoftver konfigurációjának vizsgálata. Kapcsolat típusa, preferált hálózat neve.
- Forgalmazás. A felhasználói adatforgalom vizsgálata az S1-U interfészen (GTP-U tunneling) és az SGi interfészen.

2.1. A rendszer hardverelemeinek azonosítása

Azonosítsa a 1.2 és 1.3 ábrák segítségével a mérési elrendezés hardver elemeit.

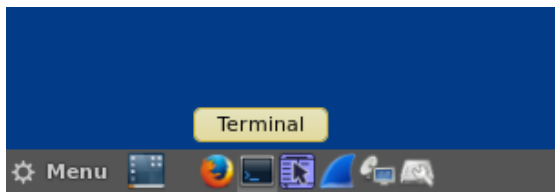
2.2. Az EPC maghálózat szoftverelemeinek azonosítása

Jelentkezzen be az LTE hálózat szoftvermoduljait futtató *gig* Gigabyte mini PC-re (2.1 ábra). Login: *aitia* jelszó: *wp6demo*.



2.1. ábra. Bejelentkezés a *gig* mini PC-re

Indítson egy terminált (2.2 ábra) az EPC modul futtatásához.



2.2. ábra. Terminál indítása

Váltson át `root` felhasználóra a `su` parancs kiadásával. Jelszó: `wp6demo`. Vizsgálja meg az EPC modul konfigurációs beállításait a `/root/mme/config/mme.cfg` fájlban.

A konfigurációs fájlban található hivatkozás a Home Subscriber Server (HSS) `combo_wp6_demo_ue.db` felhasználói adatbázisára. A mérés során az *AITIA Smartjac 1* USIM kártyát használjuk (2.1 lista). A számunkra releváns értékek az International Mobile Subscriber Identifier, IMSI (001010000000001), az integritás-ellenőrzéshez és titkosításhoz használt K kulcs (00112233445566778899AABBCCDDEEFF), a hozzáférési pont neve (*Access Point Name: test123*), illetve a végberendezés számára kiosztott (esetünkben fix) IP cím (10.100.110.101).

A végberendezés oldalán a fenti adatok közül az IMSI és a K kulcs értékét az USIM kártya tartalmazza. A hozzáférési pont nevét az LTE modem konfigurációs dialógusablakában kell megadni. Az IP címet a hálózat osztja ki – esetünkben a felhasználói adatbázisban az IMSI értékhez rögzített érték alapján. Megjegyezzük, hogy lehetséges az UE IP címek automatikus kiosztása is az MME konfigurációs fájljában megadott címtartomány alapján.

Az USIM kártyára a gyártáskor kerülnek rá a fenti azonosítók, amelyek utólag nem módosíthatók. Ezeket az azonosítókat a mobilszolgáltatóknak is be kell tölteniük a HSS adatbázisába.

2.1. Listing. USIM kártya paraméterek

```
{
  // AITIA Smartjac 1
  sim_algo: "milenage",
  imsi: "001010000000001",
  op: "ab0104babe8ed026f9cb54b56d04da26",
  amf: 0x9001,
  sqn: "000000000000",
  K: "00112233445566778899AABBCCDDEEFF",
  pdn_list:
  [{
    access_point_name: "test123",
    ipv4_addr: "10.100.110.101",
    default: true,
  }],
},
```

Az EPC hálózat indítása a `runmme` script-tel történik (2.3 ábra).

2.3 A Wireshark indítása a maghálózat monitorozására



```
aitia@gig:/home/aitia
File Edit View Search Terminal Help
[aitia@gig ~]$ su
Password:
[root@gig aitia]# ./runmme
LTE MME version 2015-10-28, Copyright (C) 2012-2015 Amarisoft
This software is licensed to Aitia.
(mme) █
```

2.3. ábra. Az EPC indítása

Amikor fut az EPC, az (mme) promptnál kiadott `ue` paranccsal kérhetjük le a csatlakozott végberendezések listáját. Az összes parancs listázásához: `help`.

Ha probléma adódik az EPC indításakor, akkor a lépéseket külön kell elvégezni (2.2). Az `enp0s20u2u1` az USB-Ethernet adapter neve, amelyet az `ip addr` parancs kiadásával kapunk meg.

2.2. Listing. Az EPC indítása lépésenként

```
$ su
# cd /root/mme
# ./lte_init.sh enp0s20u2u1
# ./ltemme config/mme.cfg
```

2.3. A Wireshark indítása a maghálózat monitorozására

Az ENB és a maghálózat közötti S1 interfész vizsgálatához a *Wireshark* programot használjuk. A *gig* gépen a táncán található ikon segítségével először indítsa el a *Wireshark*-ot. Az interfészek listájából válassza ki a *localhost*-ot jelölő *lo* interfészt. Ez lefedi az összes `127.*.*.*` IP címet.

A vizsgálatok megkönnyítésére az interfész forgalmát többféleképpen is szűrhetjük. Az ENB–MME közötti *S1-MME* jelzésinterfész két végpontja a (ENB: `127.0.10.100`, MME: `127.0.20.100`) például a `ip_addr=127.0.10.100 display filter` beállítással szűrhető. Alternatív megoldás a `sctp` szűrő felvétele, amely csak az SCTP protokoll által szállított jelzésforgalmat jeleníti meg.

A felhasználói adatforgalom az ENB és SGW közötti *S1-U* interfészen halad. Ennek végpontjai az `127.0.10.200` (ENB) és a `127.0.20.200` (SGW) IP címek. Ennek forgalma vagy a `ip_addr=127.0.10.200 display filter` beállítással, vagy pedig a `gtp` szűrővel monitorozható – ez utóbbi azért működik, mert a felhasználói adatforgalmat a *GPRS Tunneling Protocol (GTP-U)* szállítja.

2.4. Az ENB konfigurációja

Indítson egy második terminált. Az ENB szoftvermodult futtatásához szintén `root` jogosultságra van szükség: `su`, jelszó: `wp6demo`.

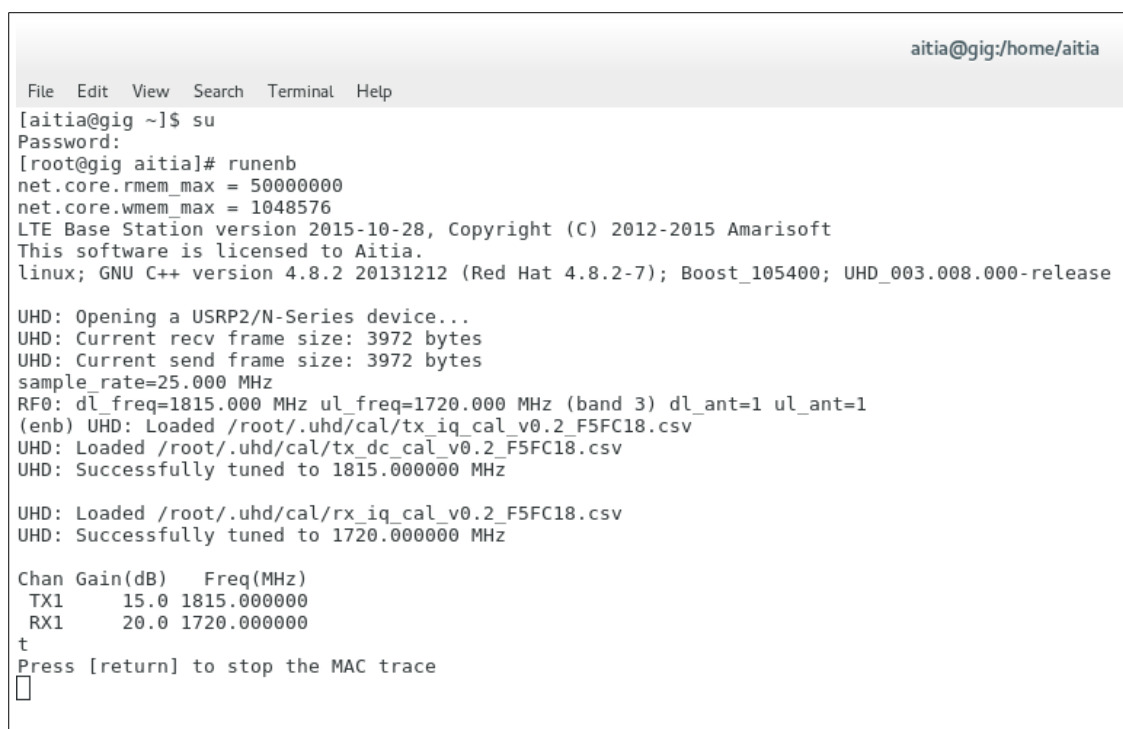
2 Mérés feladatok

Vizsgálja meg az ENB konfigurációs fájlját: `/root/enb/config/enb.cfg`. Itt állíthatók egyebek mellett az *S1-MME* interfész ENB és MME oldali IP címei, az *S1-U* interfész lokális címe, illetve a *cell_list* blokkon belül a cella paraméterei. Ezek közül számunkra fontos az *EUTRA Absolute Radio-Frequency Channel Number* (EARFCN) *downlink* értéket rögzítő *dl_earfcn* kulcs, aminek értéke a jelenlegi beállításban 1300. Ez a 3-as LTE sávban a DL csatornán az 1815.0 MHz-es középfrekvenciának felel meg. Az LTE frekvenciasávokról összefoglalót, illetve középfrekvencia-EARFCN kalkulátort a http://niviuk.free.fr/lte_band.php címen talál.

2.5. Az ENB indítása

Az ENB szoftvermodul indítása előtt győződjön meg róla, hogy az *USRP N210* rádiós egység működik. A készülék dobozán nincsen bekapcsoló gomb; a tápegység csatlakoztatásakor azonnal elindul.

Indítsa el az ENB szoftvermodult a `runenb` script futtatásával (2.4).



```
aitia@gig:/home/aitia
File Edit View Search Terminal Help
[aitia@gig ~]$ su
Password:
[root@gig aitia]# runenb
net.core.rmem_max = 50000000
net.core.wmem_max = 1048576
LTE Base Station version 2015-10-28, Copyright (C) 2012-2015 Amarisoft
This software is licensed to Aitia.
linux; GNU C++ version 4.8.2 20131212 (Red Hat 4.8.2-7); Boost_105400; UHD_003.008.000-release

UHD: Opening a USRP2/N-Series device...
UHD: Current recv frame size: 3972 bytes
UHD: Current send frame size: 3972 bytes
sample_rate=25.000 MHz
RF0: dl_freq=1815.000 MHz ul_freq=1720.000 MHz (band 3) dl_ant=1 ul_ant=1
(enb) UHD: Loaded /root/.uhd/cal/tx_iq_cal_v0.2_F5FC18.csv
UHD: Loaded /root/.uhd/cal/tx_dc_cal_v0.2_F5FC18.csv
UHD: Successfully tuned to 1815.000000 MHz


UHD: Loaded /root/.uhd/cal/rx_iq_cal_v0.2_F5FC18.csv
UHD: Successfully tuned to 1720.000000 MHz

Chan Gain(dB)  Freq(MHz)
TX1      15.0 1815.000000
RX1      20.0 1720.000000
t
Press [return] to stop the MAC trace
□
```

2.4. ábra. Az ENB indítása

Az ENB modul indulásakor megjeleníti a *downlink* és *uplink* frekvenciákat: RF0: `dl_freq=1815.000 MHz ul_freq=1720.000 MHz`.

Ha az ENB modul indítása sikertelen, és *core dump*-pal elszáll, annak oka lehet például, hogy az ENB-RRU és az ENB-BBU közötti I/Q interfész (a mini PC beépített Ethernet portján) nincs megfelelően konfigurálva. Ebben az esetben a *Taskbar* jobb szélén

található  ikonra kattintva a hálózati adapterek listájában győződjön meg róla, hogy az *S1* interfészen az *RRU* beállítás van aktiválva, és hogy a `ping 192.168.10.2` parancsra válaszol az USRP N210.

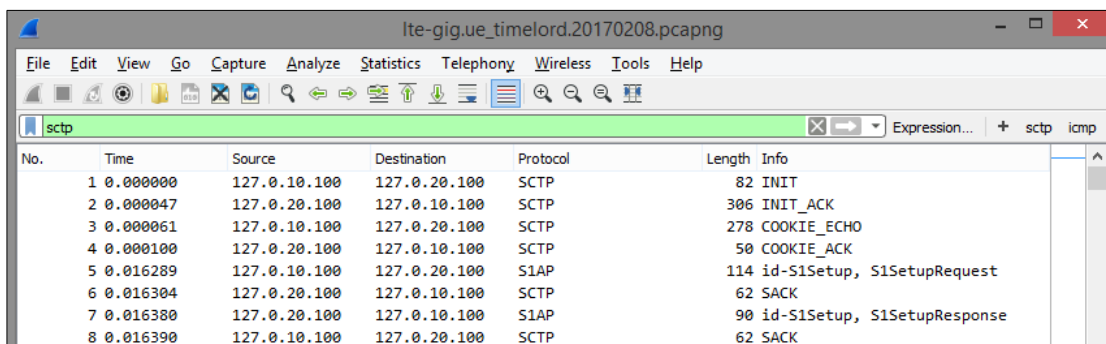
Az ENB modul kézi indítása az alábbi parancsokkal történik (2.3).

2.3. Listing. Az ENB indítása lépésenként

```
$ su
# cd /root/enb
# ./lte_init.sh
# ./lteenb config/enb.cfg
```

Az ENB modul indítása után adja ki a `t` (*trace*) parancsot. Ezzel nyomon követheti az *LTE-Uu* rádiós interfész aktuális állapotát.

Az ENB az indítás után a konfigurációs fájlban megadott IP címen automatikusan kapcsolódik az MME-hez. *Wireshark*-ban követhető az SCTP kapcsolat felépülése (`INIT` → `INIT_ACK` → `COOKIE_ECHO` → `COOKIE_ACK`), illetve az *S1AP* protokoll *S1Setup* procedúrája: `S1SetupRequest` → `S1SetupResponse` (2.5 ábra).



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.10.100	127.0.20.100	SCTP	82	INIT
2	0.000047	127.0.20.100	127.0.10.100	SCTP	306	INIT_ACK
3	0.000061	127.0.10.100	127.0.20.100	SCTP	278	COOKIE_ECHO
4	0.000100	127.0.20.100	127.0.10.100	SCTP	50	COOKIE_ACK
5	0.016289	127.0.10.100	127.0.20.100	S1AP	114	id-S1Setup, S1SetupRequest
6	0.016304	127.0.20.100	127.0.10.100	SCTP	62	SACK
7	0.016380	127.0.20.100	127.0.10.100	S1AP	90	id-S1Setup, S1SetupResponse
8	0.016390	127.0.10.100	127.0.20.100	SCTP	62	SACK

2.5. ábra. Az SCTP kapcsolatfelépítés és az *S1Setup* procedúra az *S1-MME* interfészen

2.6. A végberendezés kapcsolódása a hálózathoz

A végberendezés kapcsolódásának monitorozása maghálózat oldalán történik. Ezért először a *gig* mini PC-n indítsa el a *Wireshark*-ot, és válassza ki a *lo* interfészt a *localhost* forgalom rögzítéséhez. A *display filter* beállítása most is `sctp` legyen.

A mobil végberendezés funkcióját a *Timelord* mini PC valósítja meg. Csatlakoztassa az LTE USB modemet a mini PC egyik USB portjára. Várakozzon, amíg az UE oldalon a Windows felismeri az USB eszközt. A modem úgy van beállítva, hogy automatikusan felcsatlakozzon az általa már ismert mobilhálózatra. Ez a művelet akár fél percig is eltarthat.

A folyamat a hálózat oldalán követhető nyomon. Az *enb* modul terminálablakában (ahol az ENB indítása után a `t` parancsral elindítottuk a *trace* kiírást) rövidesen megjelenik a PRACH jel. A *Physical Random Access Channel* szolgál arra, hogy a végberendezés bejelentkezzen a cellára, és az ENB ezen keresztül osztja ki a dedikált *uplink* és

2 Mérési feladatok

downlink rádiófrekvenciákat, amelyeken keresztül az UE a későbbiekben forgalmaz (2.6 ábra). A kapcsolódást követően a *trace* parancs táblázatos formában jeleníti meg a rádiós csatorna *downlink* és *uplink* paramétereit. A számunkra releváns értékek az **UE_ID**, a **cqi** (*Channel Quality Indicator*, 0[rossz]...15[nagyon jó]), **retx** (blokk újraküldések száma), **brate** (átlagos bitráta), **snr** (*uplink* jel-zaj viszony), és a **phr** (*power headroom*, teljesítmény-tartalék az UE oldalán a kívánt *uplink* jelszint tartásához – negatív értéknél már nem tudja tartani a szükséges jelszintet az UE).

```

aitia@gig:~/enb
File Edit View Search Terminal Help

(enb) [root@gig enb]#
[root@gig enb]# ./lte_init.sh
net.core.rmem_max = 50000000
net.core.wmem_max = 1048576
[root@gig enb]# ./lteenb config/enb.cfg
LTE Base Station version 2015-10-28, Copyright (C) 2012-2015 Amarisoft
This software is licensed to Aitia.
linux; GNU C++ version 4.8.2 20131212 (Red Hat 4.8.2-7); Boost_105400; UHD_003.008.000-release

UHD: Opening a USRP2/N-Series device...
UHD: Current recv frame size: 3972 bytes
UHD: Current send frame size: 3972 bytes
sample_rate=25.000 MHz
RF0: dl_freq=1815.000 MHz ul_freq=1720.000 MHz (band 3) dl_ant=1 ul_ant=1
(enb) UHD: Loaded /root/.uhd/cal/tx_iq_cal_v0.2_F5FC18.csv
UHD: Loaded /root/.uhd/cal/tx_dc_cal_v0.2_F5FC18.csv
UHD: Successfully tuned to 1815.000000 MHz

UHD: Loaded /root/.uhd/cal/rx_iq_cal_v0.2_F5FC18.csv
UHD: Successfully tuned to 1720.000000 MHz

Chan Gain(dB)   Freq(MHz)
TX1      15.0 1815.000000
RX1      20.0 1720.000000
t
Press [return] to stop the MAC trace
s1
S1 connection state:
- server=127.0.20.100:36412 state=setup_done PLMN=00101
(enb) t
Press [return] to stop the MAC trace
PRACH: cell=01 seq=33 ta=6 snr=27.6 dB
-----DL-----UL-----
UE_ID CL RNTI cqi ri mcs retx txok brate snr puc1 mcs retx rxok brate turbo phr
  1 01 003d 13 1 8.8 0 6 764 8.0 3.3 13.5 0 5 1.17k 1/1.4/2 40
  1 01 003d 13 1 24.0 2 10 2.87k 10.8 11.2 10.8 0 8 2.67k 1/1.0/1 40
  1 01 003d 13 1 24.0 0 2 520 11.0 13.1 14.0 0 2 744 1/1.0/1 40
  1 01 003d 13 1 24.0 0 8 4.25k 12.2 11.7 13.8 0 9 2.34k 1/1.0/1 40
  1 01 003d 13 1 24.0 4 16 10.0k 13.5 11.2 14.3 0 15 5.46k 1/1.1/2 40
  1 01 003d 12 1 21.0 3 8 4.32k 11.2 10.1 15.9 0 11 3.16k 1/1.0/1 40
  1 01 003d 11 1 22.0 1 15 13.6k 10.9 12.0 15.4 0 26 13.2k 1/1.1/2 40
  1 01 003d 13 1 - 0 0 0 9.9 - - 0 0 0 - 40
  1 01 003d 13 1 24.0 2 4 3.48k 8.8 9.8 13.5 0 6 2.28k 1/1.2/2 40
  1 01 003d 13 1 24.0 5 20 16.3k 9.0 11.7 15.0 0 23 7.21k 1/1.0/2 40
-----DL-----UL-----
UE_ID CL RNTI cqi ri mcs retx txok brate snr puc1 mcs retx rxok brate turbo phr
  1 01 003d 13 1 23.0 0 4 1.97k 9.5 12.3 15.0 0 5 1.35k 1/1.4/2 40
  1 01 003d 13 1 23.2 3 12 10.9k 10.7 11.1 15.1 0 16 6.60k 1/1.0/1 40
  1 01 003d 13 1 - 0 0 0 10.9 - - 0 0 0 - 40
  1 01 003d 12 1 - 0 0 0 11.3 - - 0 0 0 - 40

```

2.6. ábra. A végberendezés kapcsolódása az ENB-hez

Az UE és a hálózat közötti kommunikáció a rádiós hozzáférési réteg felett, a *Non-Access Startum* (NAS) rétegben történik. Ennek lépései a *Wireshark* log-ban követhetők (2.7 ábra). Az *Attach* procedúra során a készülék regisztrálja magát a hálózatban: tudatja, hogy melyik cellában tartózkodik, azonosítja és hitelesíti magát (és a hálózatot), illetve megegyeznek a hálózattal az integritás-ellenőrzéshez és titkosításhoz használt kulcsokban. Az LTE esetében az *Attach* kéréssel egyidejűleg a UE PDN kapcsolatot is kér a hálózattól; ennek során osztja ki a hálózat az UE IP címét.

A megfigyelhető lépések a következők: az UE által küldött *Attach + PDN Connectivity* kérésre a hálózat először az *Identity* eljárással azonosítja a végberendezést, majd az *Authentication* eljárással a felek kölcsönösen hitelesítik egymást. Ezt követően a *Security Mode* eljárással megegyeznek a használt titkos kulcsokban. Az *ESM Information* üzenetekben a hálózat további *Session Management* információt kér és kap a végberendezéstől. Az IP cím kiosztása az *Attach Accept*-et követően az *Activate default EPS bearer context request* üzenetben történik. Az eljárást az UE által küldött *Attach complete*, *Activate default EPS bearer context accept* üzenet zárja.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.10.100	127.0.20.100	SIAP/NAS-EPS	210	id-initialUEMessage, Attach request, PDN connectivity request
2	0.000105	127.0.20.100	127.0.10.100	SIAP/NAS-EPS	106	SACK id-downlinkNASTransport, Identity request
3	0.056039	127.0.10.100	127.0.20.100	SIAP/NAS-EPS	142	SACK id-uplinkNASTransport, Identity response
4	0.056136	127.0.20.100	127.0.10.100	SIAP/NAS-EPS	138	SACK id-downlinkNASTransport, Authentication request
5	0.136009	127.0.10.100	127.0.20.100	SIAP/NAS-EPS	142	SACK id-uplinkNASTransport, Authentication response
6	0.136081	127.0.20.100	127.0.10.100	SIAP/NAS-EPS	122	SACK id-downlinkNASTransport, Security mode command
7	0.176003	127.0.10.100	127.0.20.100	SIAP/NAS-EPS	146	SACK id-uplinkNASTransport, Security mode complete
8	0.176099	127.0.20.100	127.0.10.100	SIAP/NAS-EPS	114	SACK id-downlinkNASTransport, ESM information request
9	0.216014	127.0.10.100	127.0.20.100	SIAP/NAS-EPS	142	SACK id-uplinkNASTransport, ESM information response
10	0.216131	127.0.20.100	127.0.10.100	SIAP/NAS-EPS	266	SACK id-InitialContextSetup, InitialContextSetupRequest, Attach accept, Activate default EPS bearer-
14	0.376011	127.0.10.100	127.0.20.100	SIAP/NAS-EPS	122	id-uplinkNASTransport, Attach complete, Activate default EPS bearer context accept

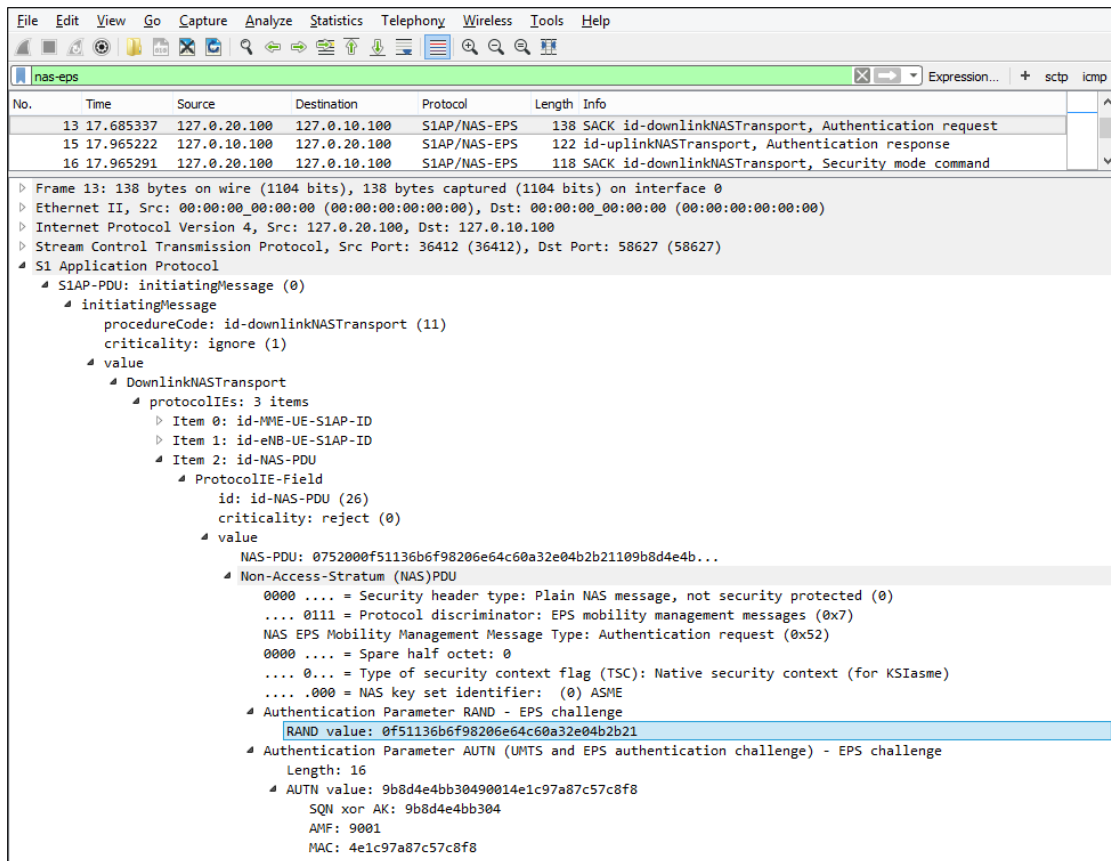
2.7. ábra. Az *Attach* procedúra lépései az UE és a hálózat között

Vizsgáljuk meg az autentikáció lépéseit. Az autentikációt a hálózat kezdeményezi. Ennek során a hálózat generál egy véletlen számot (RAND), és azt az előfizető USIM kártyájához tartozó K kulcs felhasználásával titkosítja. Ezt követően a RAND értékét és a titkosított véletlen bitsorozat egy részét (az AUTN mezőben) elküldi a végberendezésben az *Authentication request* üzenet részeként (2.8 ábra).

A végberendezés a kapott RAND számot szintén titkosítja az USIM kártyán található K kulcs felhasználásával. Ezt követően ellenőrzi, hogy az AUTN paraméterben kapott érték megegyezik-e az általa kapott titkosított bitsorozat megfelelő részével. Ha az AUTN értéke különbözik, akkor az UE megszakítja az *Attach* procedúrát. Ha a két érték megegyezik, akkor az UE meggyőződött róla, hogy a hálózat valóban ismeri azt a K kulcsot, amely az USIM kártyán is szerepel. Ekkor az *Authentication response* üzenet RES mezőjében visszaküldi a titkosított bitsorozat egy másik szakaszát (2.9 ábra). A hálózat a kapott RES értéket összeveti az általa titkosított érték megfelelő szakaszával. Ha az érték különbözik, akkor a hálózat megszakítja az *Attach* eljárást. Ha megegyezik, akkor a hálózat folytatja az *Authentication and key agreement* (AKA) műveletet a *Security Mode* procedúrával.

A fenti üzenetváltásban szereplő AUTN érték teszi lehetővé, hogy a végberendezés is hitelesíthesse a hálózatot. Ahogy korábban említettük, egyebek mellett a kölcsönös

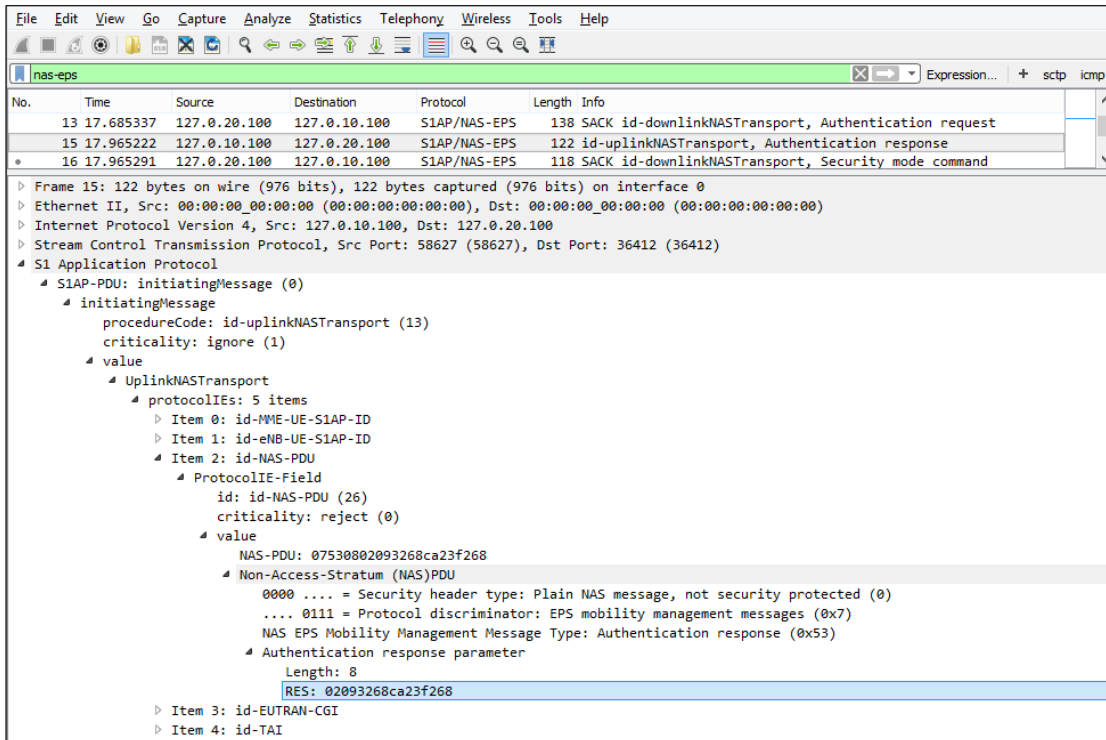
2 Mérés feladatok



2.8. ábra. Az Authentication Request üzenet tartalmazza a RAND és AUTN értékeket

hitelesítés képessége különbözteti meg az USIM kártyát a SIM kártyától.

2.7 Az LTE USB modem kliensszoftver konfigurációja



2.9. ábra. Az Authentication Response-ban küldi el az UE a RES értéket

A hálózat az *Attach accept*, *Activate default EPS bearer context request* üzenetben küldi el a végberendezésnek a PDN hozzáféréshez használt IP címet (2.10 ábra).

2.7. Az LTE USB modem kliensszoftver konfigurációja

A végberendezés oldalán vizsgálja meg az LTE USB modem kliensszoftver konfigurációját.

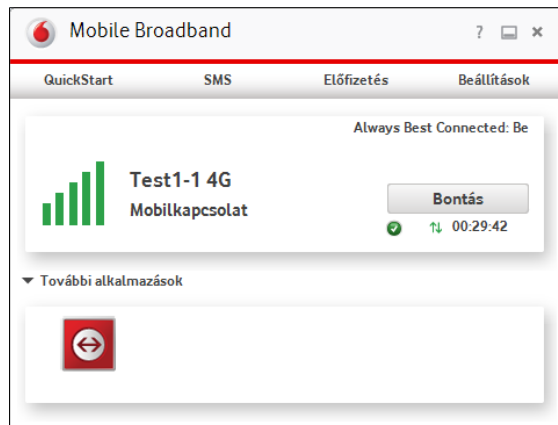
A kliensszoftvert a modem automatikusan telepíti. A *Mobile Broadband* GUI a Windows Start menüből indítható (2.11 ábra).

2 Mérési feladatok

The image shows a Wireshark packet capture analysis. The packet list pane displays several packets, with packet 18 highlighted. The packet details pane shows the structure of the S1 Application Protocol, including the S1AP-PDU: initiatingMessage (0) with procedureCode: id-InitialContextSetup (9) and criticality: reject (0). The value field contains an InitialContextSetupRequest with protocolIEs: 6 items. Item 3 is ProtocolIE-Field: id-E-RABToBeSetupListCtxtSUReq (24) with criticality: reject (0). The value field contains an E-RABToBeSetupListCtxtSUReq: 1 item, which is an E-RABToBeSetupItemCtxtSUReq (52) with criticality: reject (0). The value field contains an E-RABToBeSetupItemCtxtSUReq with e-RAB-ID: 5, e-RABlevelQoSParameters, transportLayerAddress: 7f0014c8 [bit length 32, 0111 1111 0000 0000 0001 0100 1100 1000 decimal value 21307], gTP-TEID: 37a2491b, nAS-PDU: 2712c43f6501074202e006000f110000100245201c10109..., Non-Access-Stratum (NAS)PDU, ESM message container contents, and PDN address: PDN IPv4: 10.100.110.101.

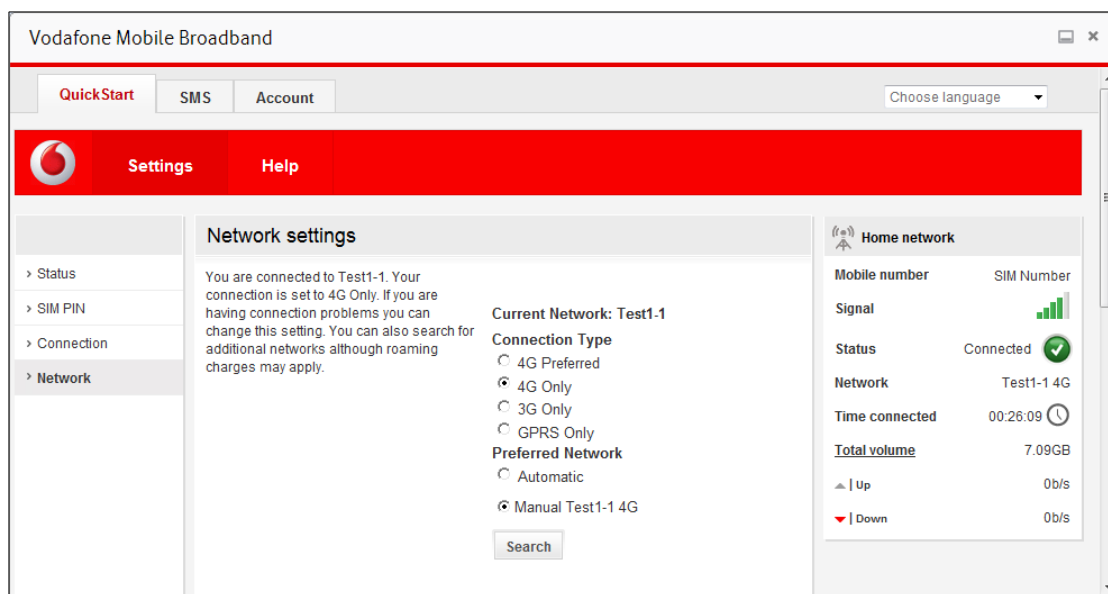
2.10. ábra. Az Activate default EPS bearer context request üzenet tartalmazza a végberendezés IP címét

2.7 Az LTE USB modem kliensszoftver konfigurációja



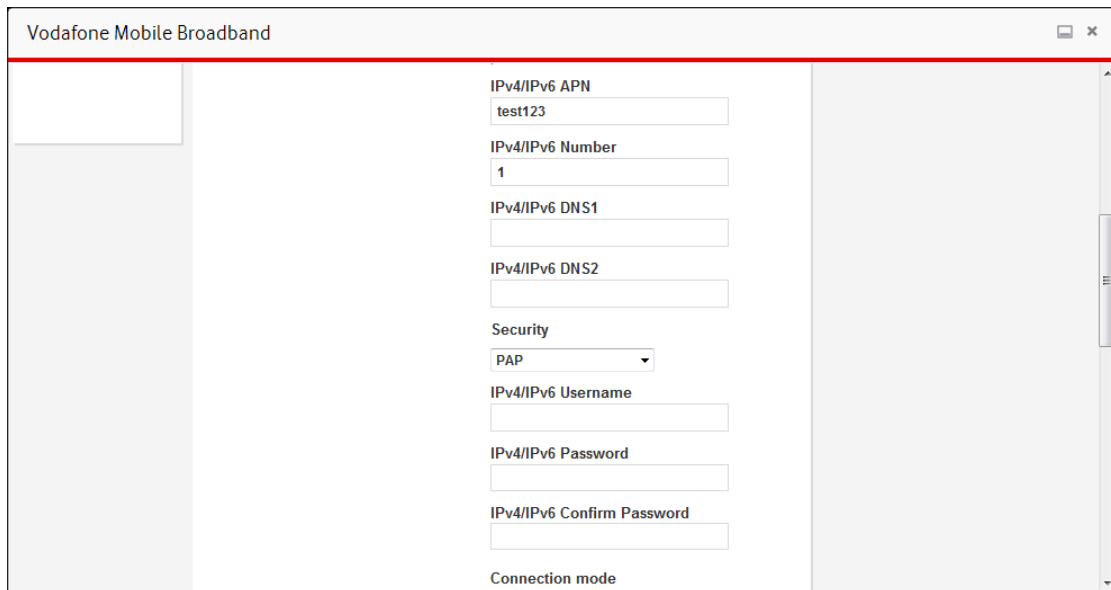
2.11. ábra. Az LTE modem grafikus felhasználói interfésze

A *QuickStart* → *Settings* → *Network* menüben (2.12 ábra) választható a mobilhálózati kapcsolat típusa. Ennek az értéke jelenleg *4G Only*, ami gyorsabb kapcsolódást tesz lehetővé. A preferált hálózatot kézzel választottuk ki: ez a vizsgált *Test1-1* mobilhálózat.



2.12. ábra. Az LTE modem hálózati beállításai

A *QuickStart* → *Settings* → *Connection* menüben határozhatók meg a kapcsolat egyéb paraméterei. A számunkra releváns *IPv4/IPv6 APN* beállítás az ablak lefelé görgetésekor jelenik meg (2.13 ábra). Az itt kell megadni ugyanazt a *test123 Access Point Name*-et, amelyet a 2.2 szakaszban látható módon az *EPC* konfigurációs fájljában meghatároztunk.



2.13. ábra. Az APN megadása LTE modem kapcsolati beállításai között

2.8. A végberendezés forgalmazási sebességének mérése

Mérje meg, hogy a végberendezés mekkora sávszélességgel tud forgalmazni *downlink* és *uplink* irányban.

Először a modem *QuickStart* → *Settings* → *Status* menüjében győződjön meg róla, hogy a modem *Connected* állapotban van. Ezt követően a *Timelord* gépen indítson el egy webböngészőt, és például a <http://speedof.me/> oldalon található alkalmazással mérje meg mindkét irányban a sávszélességet. A 2.14 ábrán látható eredményre lehet számítani.

2.9. A végberendezés adatforgalmának vizsgálata

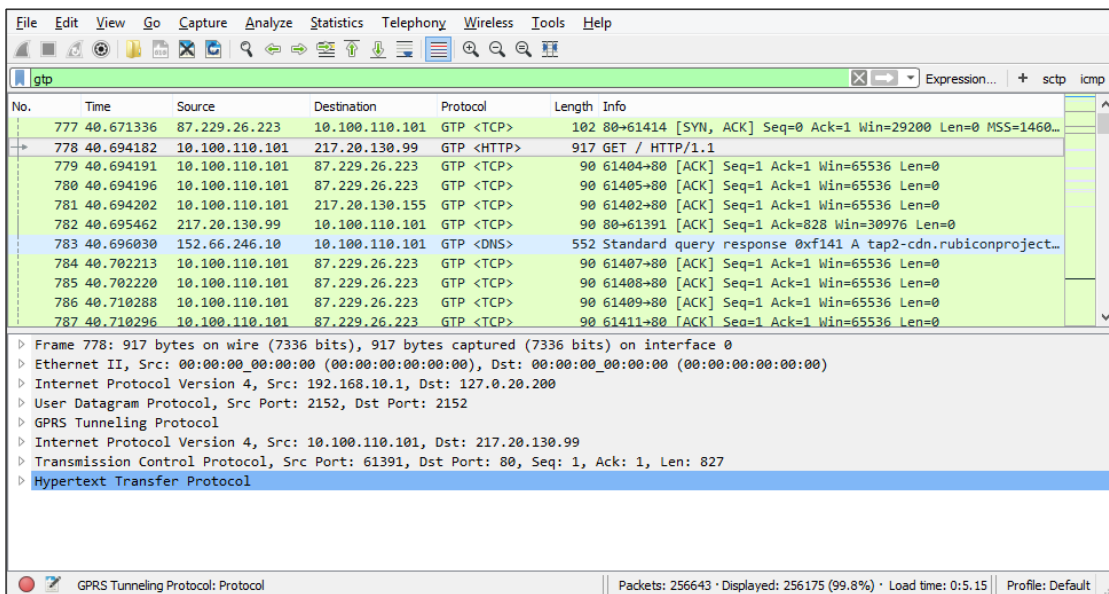
Vizsgálja meg a végberendezés által forgalmazott adatokat a hálózatban. Ehhez indítsa el a *Wireshark*-ot a *gig* mini PC-n. A vizsgált interfész ismét a `lo localhost`. A *Display filter* ezúttal `gtp` legyen – a felhasználó adatforgalom az ENB és az SGW közötti S1-U interfészen az `127.0.10.200` és `127.0.20.200` IP címek között halad, amelyet a GTP-U protokoll csomagol be. (A felhasználó IP csomagjait nem értelmezi a mobilhálózat, azokat csupán szállított adatként továbbítja az `IP | UDP | GTP-U | <user traffic> protocol stack`-en.)

A 2.15 ábra a `10.100.110.101` IP című végberendezés és több másik kiszolgáló közötti forgalmat figyelhetjük meg. Az ábrán egy HTTP kérés, egy DNS válasz, és több TCP csomag látható.

2.10 A mérés elvégzése saját okostelefonnal



2.14. ábra. Az végberendezés DL és UL sávszélességének mérése



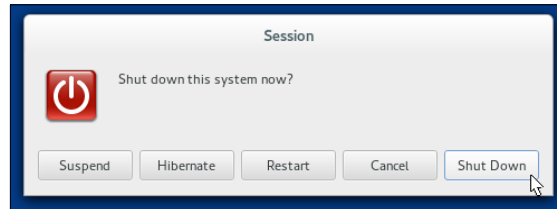
2.15. ábra. A felhasználói adatforgalom vizsgálata az S1-U interfészen

2.10. A mérés elvégzése saját okostelefonnal

Ha rendelkezik saját 4G képes okostelefonnal, akkor végezze el a fenti mérést a saját készülékével is. Micro USIM, illetve nano USIM kártyát a mérésvezető tud a rendelkezésére bocsátani.

2.11. Az LTE hálózat leállítása

A mérés végeztével állítsa le az LTE hálózatot. Ehhez az `(enb)` prompt-nál adja ki a `quit` parancsot. A terminál ablakban az `exit` paranccsal lépjen ki a `root shell`-ből, majd egy újabb `exit` paranccsal zárja be a terminál ablakot. Ugyanígy járjon el az `(mme)`, terminállal is. Zárjon be minden további alkalmazást, majd a *Taskbar* bal alsó sarkában a menüből válassza ki a leállításhoz tartozó ikont. A számítógépet a *Shutdown* gombbal állítsa le (2.16 ábra).



2.16. ábra. Az LTE hálózatot futtató gépet a Shutdown gombbal állítsa le

A végberendezésként használt *Timelord* gépen a Windows-t a szokásos módon állítsa le.

3 Ellenőrző kérdések

- Melyek a vizsgált LTE maghálózat főbb komponensei? Röviden jellemezze a hálózatban betöltött szerepüket.
- Mi a ENB szerepe az LTE rádiós hozzáférési hálózatban?
- Mi a mobil hálózatban használt SIM/USIM kártyák szerepe?
- Mi a főbb különbség a SIM és USIM kártyák között?
- Hol tárolódik a végberendezés és a mobilhálózat közötti jelzés- és adatforgalom integritás-ellenőrzéséhez és titkosításához szükséges K titkos kulcs?
- Milyen üzeneteken keresztül zajlik a végberendezés autentikációja? Mely üzenetben mi a releváns autentikációs paraméter?
- Mi az IMSI, IMEISV és MSISDN rövidítések feloldása? Mire valók ezek az azonosítók?
- Mi a GTP-U protokoll szerepe?
- Rajzolja fel a mérési elrendezés blokkvázlatát.