Slovenská Technická Univerzita v Bratislave
Fakulta Informatiky a Informačných Technológií
Ilkovičova 2, 842 16 Bratislava 4

Integrácia VoIP do LTE technológie [LTE2VoIP]

Dokumentácia k dielu

Autori:

Bc. Martin Dulovič
Bc. Martin Dubovský
Bc. Andrej Kapusta
Bc. Matúš Kislan
Bc. Tomáš Krkoš
Bc. Pavol Macho
Bc. Juraj Matuš

Vedúci tímu: doc. Ing. Ivan Kotuliak, PhD.
Akademický rok: 2015/2016
Miesto: Bratislava
Dátum: 19. mája 2016

Obsah

1 Úvod **3**

2 Slovník **5**

3 Globálne ciele pre zimný semester **8**

4 Celkový pohľad na systém **9**

4.1 Architektúra 9

4.1.1 LTE architektúra 9

4.1.2 E-UTRAN (LTE access) 9

4.1.3 EPC (LTE core) 10

5 Moduly systému **14**

5.1 Kabinet APM30H ver.D 14

5.1.1 Použité komponenty 15

5.1.2 Príprava na inštaláciu 16

5.1.3 Samotná inštalácia 17

5.1.4 Záver 19

5.2 IMS 19

5.2.1 IMS 19

5.2.2 Inštalácia IMS 20

5.2.3 Konfigurácia 21

5.2.4 Vytvorenie úvodného obsahu SQL databázy 21

5.2.5 Inštalácia a konfigurácia RTPProxy 22

5.2.6 Spustenie IMS 22

5.2.7 Informácie o serveri 23

5.3 HSS 23

6 SIM karty **25**

7 Testovanie systému **26**

7.1 IMS - IP Multimedia Subsystem 26

7.1.1 Autentifikácia 27

7.1.2 Hovor 28
7.2 EPC - Evolved Packet Core 28
7.2.1 Prihlásenie do systému 28

Zoznam použitej literatúry **29**

Príloha A: Technická dokumentácia

Príloha B: Príručka k vyrobeniu koncoviek na RF káble

Príloha C: Technická dokumentácia

1. Úvod

FIIT STU disponuje technológiou LTE, čo je technológia umužňujúca prístup do internetovej siete. Technológia ale sama o sebe neumožňuje hovory. Mobilné telefóny s podporou technológie VoLTE (napr. iPhone 6, Nokia Lumia, niektoré novšie zariadenia Android) umožňujú využitie siete LTE aj na telefonické hovory. Technológia VoLTE na prenos a prepojenie využíva architektúru IMS.

Cieľom projektu je vytvoriť prepojenie LTE a VoIP technológií pre prezentačné a výskumné účely. LTE je najmodernejšia komerčne používaná mobilná sieť. VoIP použité v projekte bude v súlade so štandardmi založené na SIP protokole, pričom použitie IMS architektúry môže byť výhodnou. Výsledkom projektu má byť pripravená a nakonfigurovaná sieť, ktorá podporuje telefónne hovory z moderných zariadení.

Výsledkom projektu budú vzorové scenáre predvedenia funkčnosti LTE siete vrátane funkčného telefónneho hovoru. Dôležitým výsledkom bude automatizované štartovanie celého systému, kvalitná dokumentácia na oživenie systému v prípade poruchy aj niekým mimo tímu.

Projekt je zameraný najmä na integráciu a dokumentáciu celého procesu, nutnosť vývoja nových modulov je minimálna.

Tento dokument stanoví ciele projektu na zimný semester 3. V kapitole 4 bude systém popísaný bližšie, a to vrátane priblíženia zvolenej architektúry systému 4.1.

V kapitole 5 bude systém rozdelený do jednotlivých modulov. Každý modul bude opísaný z vyššieho pohľadu, z pohľadu funkcionality, a tiež bude zdokumentovaná práca a jednotlivé príbehy týkajúce sa modulu.

Testovacie scenáre na vyššie overenie funkcionality celého produktu budú popísané v kapitole 7.

V prílohách bude obsiahnutý manuál pre použitie A a technická dokumentácia B.

2. Slovník

3GPP

3rd Generation Partnership Project - štandardizačná organizácia založená na spolupráci významných telefonických spoločností.

BBU

Basebad Unit.

CPRI

Common Public Radio Interface.

E-UTRAN

Evolved UMTS Terrestral Radio Access Network.

eNode-B

E-UTRAN Node-B.

EPC

Evolved Packed Core.

EPU

Emergency Power Unit.

GPS

Global Positioning System.

IMS

IP Multimedia Subsystem [1, 2].

LMT

Local Maintenence Terminal.

LTE

Long Term Evolution.

MME

Mobility Management Entity.

OM

Operation and Maintenence.

PMU

Power Monitoring unit.

PSU

Power Supply Unit.

RRU

Radio Frequency Unit.

S-GW

Serwing Gateway.

SIP

Session Initiation Protocol.

SLPU

Signal Lightning Protection Unit.

UELP

Universal E1/T1 Lightning Protection Unit.

UFLP

Universal FE Lightning Protection Unit.

USB

Universal Serial Bus.

VoIP

Voice over IP.

VoLTE

Voice over LTE [3].

3. Globálne ciele pre zimný semester

Ako už bolo spomenuté v úvode dokumentu, cieľom je vytvorenie funkčnej LTE siete, ktorá umožni prenos dátových paketov po sieti. Keďže architektúra LTE je tvorená z mnohých časti, jednak z hardware časti a core časti, ktorá je zodpovedná za registrovanie nových používateľov a správne smerovanie paketov, podrobnejšie rozpísané v kapitole 4.1 Architektúra. Ako hlavný cieľ sme si zvolili zmontovať dodané hardware komponenty do funkčnej podoby, ktorá umožní prijímanie a vysielanie dát. Spomedzi existujúcich technológii na LTE access vrstvu nám bolo poskytnuté hardware-ové riešenie od Huawei. Pre poskytnutie funkcionality LTE siete je potrebne prepojenie access vrstvy a core vrsty, pričom ako core vrstva nám bolo poskytnuté virtuálne riešenie cisco zariadení od Sanetu. Po skonštruovaní hardware access vrstvy je nutne dané zariadenie prepojiť s nakonfigurovaným core komponentom LTE siete. Pri konfigurovaní core vrstvy je potrebné nakonfigurovať správne smerovanie paketov medzi komponentami, nastaviť komponent na registráciu nových používateľov, komponent na prihlasovanie používateľov.

Do konca zimného semestra plánujeme zostrojiť a prepojiť access vrstvu s nakonfigurovanou core vrstvu LTE siete a otestovať funkčnosť nášho riešenia jednoduchým prihlásením používateľov a . Pre otestovanie funkčnosti a následne k jej plnohodnotnému používanie je potrebné zabezpečiť zariadenia, ktoré budú schopné sa do danej siete prihlásiť a využívať. Vedľajšími úlohami a cieľmi bude nájsť konkrétne SIM karty, ktoré podporujú pripojenie do LTE sieti a zároveň bude schopné im nahrať používateľské údaje. K týmto SIM kartám je potrebné nájsť mobilné zariadenia, ktoré budú schopne s danými SIM kartami kompatibilné a zároveň budú odblokované pre LTE siete. Pre umožnenie prenosu hlasových záznamov, teda pre telefonovanie je potrebné implementovať a nakonfigurovať nad core vrstvou buď SIP protokol, alebo prepojenie core vrstvy s IMS architektúrou, ktorá umožňuje prenos multimediálneho obsahu cez IP vrstvu.

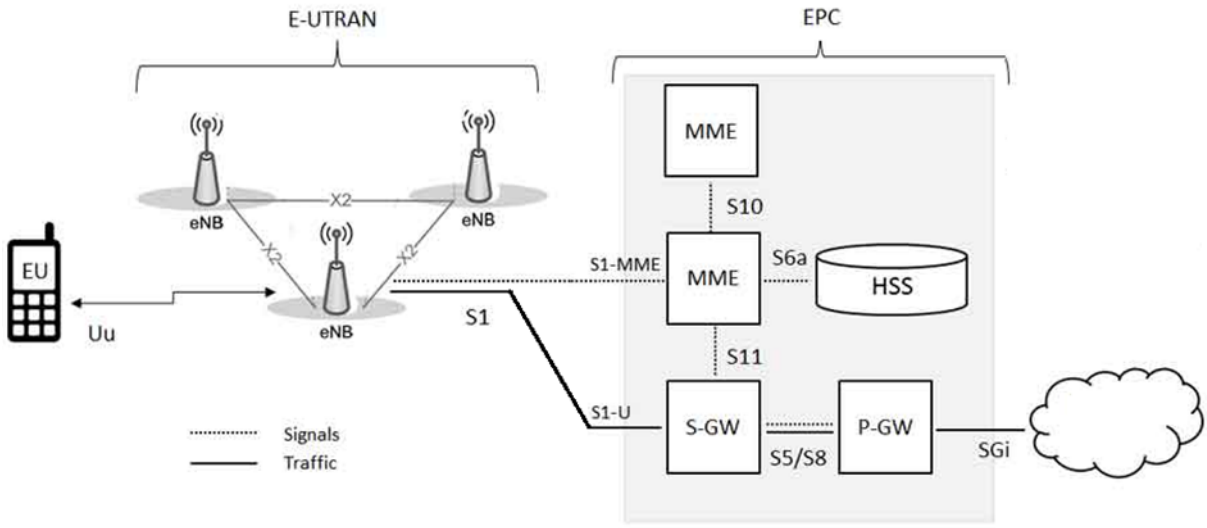
4. Celkový pohľad na systém

4.1 Architektúra

Sekcia obsahuje rozdelenie a popis jednotlivých častí LTE architektúry, ako aj zariadení či iných architektúr, ktoré využívajú danú LTE architektúru.

4.1.1 LTE architektúra

Ako môžeme vidieť na obrázku 4.1.1, architektúru je možné rozdeliť na dve časti. LTE Access (E-utran) a LTE core (EPC). Na obrázku sa ešte nachádza UE (user equipment). Jedná sa o mobilné zariadenie s prislúchajúcou USIM kartou. Oblak na obrázku znázorňuje pripojenie na inú architektúru, sieť. Môže sa jednať napríklad o IMS či Internet.



Obr. 4.1: Architektúra LTE

4.1.2 E-UTRAN (LTE access)

Rádiová prístupová sieť E-UTRAN poskytuje užívateľom prístup ku službám, ktoré poskytuje paketová sieť EPC, čiže zaisťuje spojenie medzi UE (User Equipment) a EPC.

Obsahuje len základňové stanice eNB, ktoré tak tvoria celú pevnú časť systému a plnia funkcie ako základňovej stanice, tak aj riadiacej jednotky rádiovej siete. Každá eNB zaisťuje rádiové pokrytie danej oblasti E-UTRAN rádiovým signálom a prideľuje jednotlivé rádiové kanály podľa stanovených priorít a požadovanej kvality služieb QoS. Vykonáva meranie signálu a spoločne s hodnotami od UE rozhoduje o handovere. Jednotlivé eNB sú medzi sebou prepojené rozhraním X2, ktoré sa využíva pri handovere a s EPC sú spojené cez rozhranie S1. Každá eNB môže obsluhovať niekoľko UE, pričom jedno UE môže byť obsluhované súčasne len jednou eNB. UE je vždy prepojené s jedným MME (Mobility Management Entity) a S-GW (Serving Gateway), a eNB musí preto toto spojenie sledovať. Po pripojení UE do siete cez nové eNB, zaistí toto eNB smerovanie k MME, s ktorým bolo UE naposledy spojené. V prípade, že nie je MME k dispozícii alebo chýbajú smerovacie informácie, vyberie eNB nové MME. Dôležitou funkciou je aj mobility manažment, čiže sledovanie pohybu účastníka v sieti.

4.1.3 EPC (LTE core)

Na obrázku 4.1.3 môžeme vidieť zloženie časti EPC (Evolved Packet Core). Skladá sa z nasledovných komponentov:

- MME (Mobility Management Entity)
- S-GW (Serving Gateway)
- P-GW (Packet Data Network Gateway)
- HSS (Home Subscriber Server)

MME

MME je kľúčový pre spojenie s časťou LTE Access. Manažuje stav spojenia, autentifikáciu, prepojiteľnosť medzi 3GPP, 2G a 3G a ponúka mnoho ďalšej funkcionality. MME funkcia je podporovaná dokumentom Cisco ASR 5000.MME je zodpovedné za výber S-GW, P-GW. Pri autentifikácii je zodpovedné za interakciu s HSS, kde sa nachádzajú jednotlivé profily používateľov.

S-GW

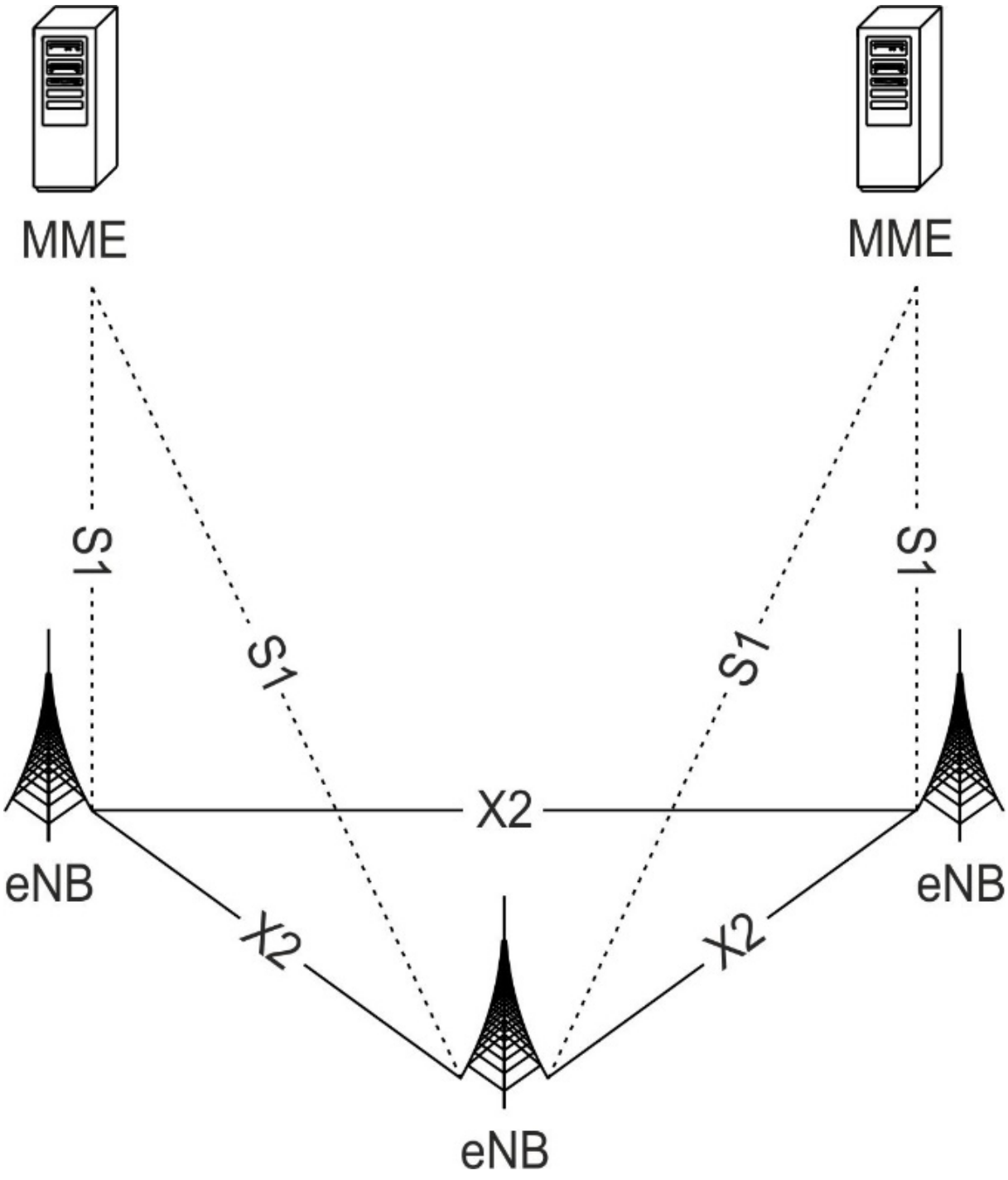
S-GW je zodpovedná za zachovanie spojenia počas odovzdávania hovoru v rámci toho istého eNB, medzi rôznymi eNB, ako aj medzi rôznymi 3GPP systémami. Funkčnosťou sa S-GW podobá 3G SGSN, avšak neobsahuje funkcie ovládajúce mobilitu a správu používateľských relácií. Jej dôležitou funkcionalitou je okrem iného aj smerovanie paketov medzi P-GW a E-UTRAN.

P-GW

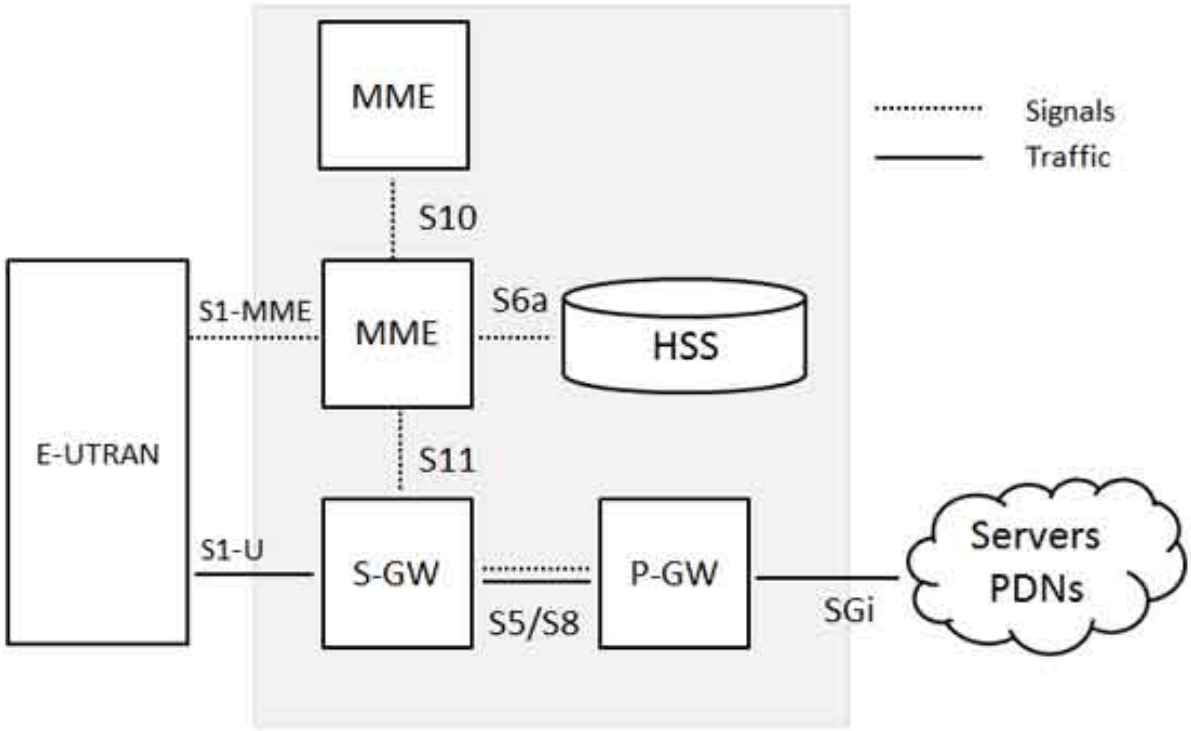
P-GW je základným smerovačom , ktorý poskytuje smerovanie von z architektúry. Jedná sa teda o prepojenie LTE a niektorými prístupovými systémami 3GPP a všetkými prístupovými systémami nepatriacimi do skupiny 3GPP.

HSS

HSS je hlavnou databázou obsahujúcou všetky informácie týkajúce sa používateľských profilov, ktoré slúžia na podporu zostavovania a ovládania jednotlivých používateľských relácií. Ak totiž systém podporuje viacero funkcionalít, nemusí mať každý používateľ prístup ku všetkým, preto je nutné mať databázu obsahujúcu všetky informácie.



Obr. 4.2: Architektúra E-UTRAN



Obr. 4.3: Vyznačená plocha zachytávajúca EPC

5. Moduly systému

5.1 Kabinet APM30H ver.D

Hlavným hardvérovým komponentom projektu je kabinet APM30H ver.D. Skladanie kabinetu a jeho komponentov je popísané v tejto sekcii.

Kabinet poskytuje vhodné prostredie pre elektornické zariadenia. Jeho najväčšími výhodami sú vynikajúce chladenie, komplexná správa kabeláže, jednoduchá inštalácia, vysoká kompatibilita, vynikajúca bezpečnosť a spoľahlivosť. Kabinet je široko používaný v rôznych datacentrách a „off the house“ miestach, napríklad pri použití s LTE komponentami na streche.

5.1.1 Použité komponenty

EPU05A

Kabinet APM30H ver.D prichádza už spredinštalovaným EPU05A, ktorý obsahuje 6 slotov, z toho 1 slot je rezervovaný pre PMU a 5 je voľných pre PSU. PMU a 2 PSU sú osadené dodávateľom. Súčasťou EPU05A sú aj elektrické vývody (maximálne 30A a 48V) pre zapojenie zariadení ktoré sa inštalujú do kabinetu (napr. BBU, Heater, a pod.) ale aj zariadení, ktoré sa inštalujú mimo kabinet (napr. RRU). EPU05A obsahuje aj prepäťovú ochranu a poistkovú skrinku. Veľkosť EPU05A je 5U.

SLPU

SLPU je malé zariadenie o veľkosti 1U, ktoré poskytuje ochranu pre "trunk" signály. Je konfugurované s UELP alebo UFLP. Dané zariadenie bolo takisto dodané už nainštalované dodávateľom.

BBU 3900

BBU zariadenie je jedno z najdôležitejších zariadení v Access vrstve (E-UTRAN). Dané zariadenie sa stará o komunikáciu medzi eNode-B a MME/S-GW, poskytuje CPRI porty pre komunikáciu s RRU, riadi eNode-B cez OM a signalizačné správy, poskytuje OM kanál pre LMT, poskytuje „clock port" pre časovú synchronizáciu a obsahuje USB port pre uvedenie do prevádzky. Zariadenie BBU 3900 má veľkosť 2U.

GPS satelitná anténa

GPS satelitná anténa je ďalšie zariadenie, ktoré sa inštaluje mimo kabinet. GPS satelitná anténa slúži na časovú synchronizáciu zariadení inštalovaných v kabinete.

AC Heater

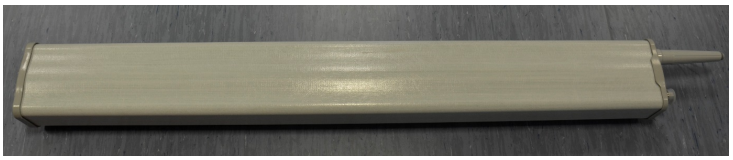
AC Heater zabezpečuje aby zariadenia inštalované v kaninete pracovali vrámci akceptovateľných teplôt. AC Heater začne pracovať (ohrievať kabinet) keď teplota v kabinete klesne pod 1 stupeň celzia, a prestáva pracovať keď teplota v kabinete prekročí 15 stupňov celzia. Je to voliteľné zariadenie, ktoré má menovitý vykurovací výkon 330W a zaberá 1U.

RRU 3938

Zariadenie RRU 3938 sa takisto inštaluje mimo kabinetu. RRU sa nachádza medzi zariadeniami BBU a LTE anténou, toto zariadenie si vyžaduje samostatné napájanie z kabinetu (zariadenie EPU).

LTE anténa

LTE anténa je posledné zaridenie, ktoré sa nachádza mimo kabinetu. Exsitujú 2 typy LTE antény a to antený na vnútorné použitie a antény na vonkajšie použitie. Obe typy antén majú extrémne veľký výkon a preto si vyžadujú dotatočné tienenie.



5.1.2 Príprava na inštaláciu

Na inštaláciu daných zariadení sme potrebovali nasledovné náradia:

- Plochý šrubovák (M4 / M6)
- Krížový šrubovák (M4 / M6)
- Francúzsky kľúč (15 mm / 16 mm)

- Nastaviteľný francúzsky kľúč
- Lámací nožík
- Nožnice na káble
- Kladivo
- Izolačná páska
- Meter

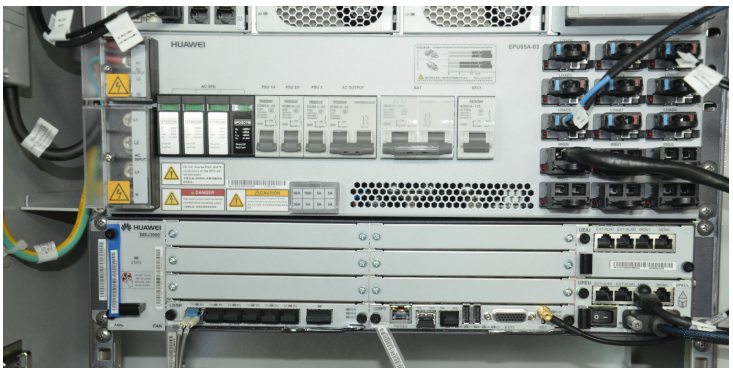
5.1.3 Samotná inštalácia

Kabinet

V prvom kroku sme vybalili kabinet APM30H ver.D a namontovali sme k nemu dodávaný podstavec pomocou pribalených šrubiek a náradia. Následne sme kabinet umiestnili na vhodné miesto, tj. k stene pri elektrickej zástrčke a zástrčke pre ethernet káble s koncovkou RJ-45.

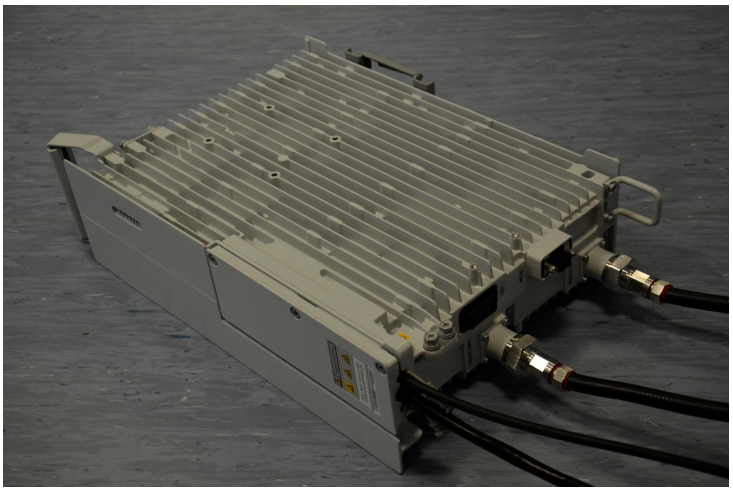
BBU 3900

V druhom kroku sme vybalili zariadenie BBU 3900 a zasunuli ho do najvyššieho voľného slotu v kabinete APM30H ver.D. Kabinet APM30H ver.D má voľné miesto pre zariadenia dokopy vo veľkosti 7U. Po vložení zariadenia sme ho zaistili v kabinete prišrubovaní pomocou šrubiek, ktoré boli v balení a náradia. Následne sme si museli vytvoriť koncovku zo strany pre EPU05A z dodávaného napájacie kábla. Nami vytvorený kábel sme zapojili do portu pre napájanie v BBU a do zariadenia EPU05A, konkrétne do portu "LOAD 6", ktorý slúži na napájanie BBU zariadení. Následne sme zapojili ethernetový kábel s koncovkou RJ-45 do portu "Mon 1" v zariadení BBU 3900, druhý koniec tohto kábla už bol v zariadení EPU05A v časti PMU v porte "COM_IN".



RRU 3938

V treťom kroku sme vybalili zariadenie RRU 3938. Následne sme si z dodávaného napájacieho kábla namerali a odstrihli nami potrebnú dĺžku pre zapojenie RRU s EPU. Odstrihnutý kábel sme spracovali a vytvoreli vhodné koncovky pre zapojenie zariadení. Po vytvorení koncoviek kábla, sme kábel potiahli cez spodné otvor kabinetu do podstavca a z neho von. Jeden koniec kábla sa zapojil do zariadenia EPU05A v porte s názvom „RRU0“ a druhý koniec kábla sme zapojili do zariadenia RRU 3398 do portu NEG/RTN, ku ktorému sa dostaneme odšrubovaním 3 šrubiek z krytu. Následne sme zapojili optický kábel medzi zariadeniami BBU 3900 a RRU 3938. Tento optický kábel bol už pripravený výrobcom s vytvorenými koncovkami a fixnou dĺžkou 30 metrov. Jeden koniec optického kábla sme zapojili do zariadenia RRU 3938, konkrétne do portu s názvom „CPRI0“. Pre zapojenie druhej strany optického kábla do zariadenia BBU 3900 sme najprv museli daný koniec kábla zapojiť do zariadenia s názvom „Huawei 1.25G-1310nm-10km-SM-ESFP“ a následne dané zariadenia zapojiť do portu s názvom „CPRI0“ v zariadení BBU 3900. Následne sme pripojili do portu s názvom „GPS“ kábel, ktorý mal na druhom konci zariadenie s názvom „Antenna Arrester“, ktoré sa nachádza mezi BBU 3900 a samotnou GPS satelitnou anténou. Pre dané zariadenie bolo treba vytvoriť namerať, zastrihnúť R/F kábel a taktiež jeho koncovky.



LTE Anténa

V štvrtom kroku sme zapojili anténu pre bezdrôtovú komunikáciu koncových zariadení v sieti LTE. LTE anténa sa pripája pomocou 2 R/F káblov so zariadením RRU 3938. Káble trebalo namerať, zastrihnúť a následne pre nich vytvoriť koncovky. Jeden koniec R/F káblov sa zapojil do portu s názvom “ANT_TX/RXA” a “ANT_TX/RXA” a druhý koniec káblov sa zapojil do LTE antény do portov s rovnakým názvom.

AC Heater

Zariadenie AC Heater sme zatiaľ nezapájali, kedže kabinet sa nachádza v zateplenej miestnosti, kde teplota neklesá pod 1 stupeň celzia, kedy AC heater začína s ohrevom.

5.1.4 Záver

Všetky vyššie spomenuté zariadenia tvoria v E-UTRAN (access vrstve) samostatnú jednotku s názvom eNode-B. eNode-B je medzikus, ktorý prepája koncové zariadenia a EPC (core vrstvu).

5.2 IMS

Dôležitým modulom systému je IMS. Rozhodli sme sa pre použitie otvorenej implementácie OpenIMS, ktorú sme nasadili na server v školskej infraštruktúre poskytnutý práve na tieto účely. Postup inštalácie je popísaný v nasledujúcich sekciách. Ako návod slúžili nasledovné zdroje: [4, 5, 6, 7].

5.2.1 IMS

IMS je architektúra, ktorej úlohou je podpora nových IP multimediálnych systémov. Skladá sa s viacerých odlišných elementov spomenutých nižšie.

P-CSCF

P-CSCF (Proxy Call Session Control Function) je inicializačný bod celej architektúry. Jeho úlohou je inicializovať signalizačné spojenia pre IMS dostupné VoLTE zariadenia a používateľov. P-CSCF sa správa ako SIP proxy, ktorá posúva SIP správy medzi používateľmi a IMS jadrom, taktiež zabezpečuje aby daná komunikácia bola bezpečná.

I-CSCF

I-CSCF (Interrogating Call Session Control Function) je kontaktný bod v architektúre pre všetky spojenia smerujúce k používateľom. Jeho úlohou v IMs architektúre je integrovanie s HSS, ktoré umožňuje registrovanie používateľov danej siete. Taktiež ukladá do HSS, cez ktorý S-CSCF komponent ma byť daná komunikácia smerovaná.

S-CSCF

S-CSCF (Serving Call Session Control Function) poskytuje funkcionalitu pre vytváranie spojení, pre ich elimináciu, smerovacie funkcionality pre kontrolu spojení. S-CSCF funguje

ako SIP registar komponent pre VoLTE používateľov, ktoré mu HSS a I-CSCF komponenty pridelia. Pomocou CX diamater protokolu si žiada informácie o používateľoch uložených v HSS. Následne na základe týchto informácii smeruje a vytvára spojenia.

5.2.2 Inštalácia IMS

```
1 apt-get install subversion
```

Výpis 5.1: Inštalácia subversion - nástroj pre verziovanie

```
1 mkdir /opt/OpenIMSCore/
2 mkdir /opt/OpenIMSCore/ser_ims
3 mkdir /opt/OpenIMSCore/FhoSS
```

Výpis 5.2: Príprava miesta na disku pre inštaláciu

```
1 cd /opt/OpenIMSCore/
2 svn checkout http://svn.berlios.de/svnroot/repos/openimscore/
    ser_ims/trunk ser_ims
3 svn checkout http://svn.berlios.de/svnroot/repos/openimscore/
    FHoSS/trunk FhoSS
```

Výpis 5.3: Stiahnutie najnovšej verzie IMS

```
1 sudo apt-get install mysql-server libmysqlclient15-dev
    libxml2 libxml2-dev bison flex front bind9 libcurl build-
    essential libcurl4-gnutls-dev
```

Výpis 5.4: Inštalácia potrebných balíčkov potrebných pre kompiláciu IMS

```
1 sudo add-apt-repository ppa:webupd8team/java
2 sudo apt-get update
3 sudo apt-get install oracle-java7-installer
```

Výpis 5.5: Inštalácia Javy

```
1 cd ser_ims
2 sudo make install-libs all
3 cd FhoSS
4 sudo ant compile deploy
```

Výpis 5.6: Kompilácia a inštalácia komponentov OpenIMS: IMS a HSS

5.2.3 Konfigurácia

```
/opt/OpenIMSCore/ser_ims/cfg/configurator.sh
# zadať doménu na ktorej bude IMS fungovať
# zadať IP na ktorej bude IMS počúvať
```

Výpis 5.7: Nastavenie domény a IP adresy

```
cp /opt/OpenIMSCore/ser_ims/cfg/open-ims.dnszone /etc/bind/
```

Výpis 5.8: Nastavenie DNS servera

Ďalej je nutné vykonať úpravy v nejakých súboroch.

```
# namiesto volgof zadat doménu, ktorú ste zadali v bode 1
zone "volgof" {
            type master;
            file "/etc/bind/open-ims.dnszone";
};
```

Výpis 5.9: Pridané riadky do súboru /etc/bind/named.conf

V súbore /etc/bind/open-ims.dnszone je nutné prepísať origin na

```
$ORIGIN volgof.
```

a IP adresy pre pcscf, icscf, scscf, trcf, bgcf, hss, ue, presence, pcrf, clf analogicky podľa príkladu uvedeného nižšie.

```
pcscf                   1D IN A         147.175.xxx.xxx
# kde IP je IP interface-u, na ktorom bude prebiehať komuniká
   cia
```

Výpis 5.10: Ukážkový riadok IP adresy zo súboru /etc/bind/open-ims.dnszone

```
/etc/init.d/bind9 restart
```

Výpis 5.11: Reštart DNS servera

5.2.4 Vytvorenie úvodného obsahu SQL databázy

```
/opt/OpenIMSCore/ser_ims/cfg/icscf.sql
/opt/OpenIMSCore/FhoSS/scripts/hss_db.sql
/opt/OpenIMSCore/FhoSS/scripts/userdata.sql
mysql -uroot -p < /opt/OpenIMSCore/ser_ims/cfg/icscf.sql
```

```
5 mysql -uroot -p < /opt/OpenIMSCore/FhoSS/scripts/hss_db.sql
6 mysql -uroot -p < /opt/OpenIMSCore/FHoSS/scripts/userdata.sql
```

Výpis 5.12: Zmena pôvodnej IP na IP interface-u a vytvorenie úvodného obsahu SQL databázy

Potom treba nastaviť v súbore FhoSS-deploy/hss.properties IP adresu a v súbore FhoSS/deploy/DiameterHSSproperties IP adresu a doménu. V súbore FHoSS/deploy/conf/tomcat-users je možné nastaviť používateľké údaje pre administrátorské konto do HSS.

Aby server reagoval na požiadavky zo sveta, musí mať odomknutú komunikáciu vo firewalle.

```
1 iptables -A INPUT -i eth0 -s 0/0 -m state --state NEW,
    ESTABLISHED -m tcp -p tcp --dport 8080 -j ACCEPT
```

Výpis 5.13: Nastavenie iptables

5.2.5 Inštalácia a konfigurácia RTPProxy

```
1 git clone https://github.com/sippy/rtpproxy.git
2 cd rtpproxy
3 ./configure
4 make
```

Výpis 5.14: Inštalácia

```
1 rtpproxy -l 147.175.204.50 -s udp:147.175.204.50:34999 -f
```

Výpis 5.15: Spustenie

Komponent musí byť povolený v IMS. To sa dosiahne úpravou súboru pcsf.cfg.

```
1 modparam("pcscf","rtpproxy_enable", 1)
```

Výpis 5.16: Pridané riadky do súboru pcsf.cfg

5.2.6 Spustenie IMS

```
1 cd /opt/OpenIMSCore
2 cp ser_ims/cfg/* .
```

Výpis 5.17: Agregácia spustiteľných súborov do hlavnej zložky

```
1 ./pcscf.sh
2 ./icscf.sh
3 ./scscf.sh
4 FhoSS/deploy/startup
```

Výpis 5.18: Spustenie jednotlivých komponentov

5.2.7 Informácie o serveri

IP	147.175.204.50
Port 5060	scscf
Port 4060	pcsf
Port 3868	HSS diameter port
Port 8080	Webové rozhranie pre administráciu HSS

5.3 HSS

HSS (Home Subscriber Server) je server, ktorý zabezpečuje autentizáciu používateľov do telefónnej siete. Jeho postavenie v sieti LTE je znázornené na obr. 5.1.

Existuje niekoľko implementácií servera HSS, avšak žiadna z voľne dostupných nie je plne funkčná verzia. Niektoré implementácie majú chýbajúce komponenty, iné sú neudržiavané a niekedy dokonca nie je možné skompilovať ich zdrojové kódy s nástrojmi aktuálnych verzií.

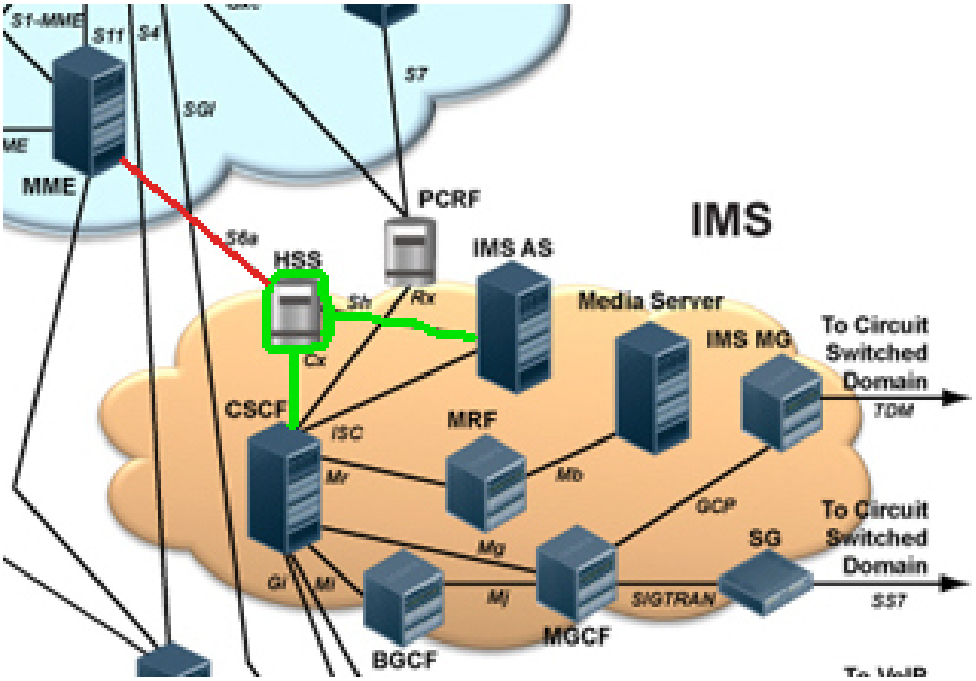
Ako hlavný server HSS sme sa rozhodli použiť FHoSS, čo je zjednodušený HSS server zahrnutý v projekte OpenIMS, implementovaný v jazyku Java. Projekt už je previazaný s IMS, čo uľahčuje ich integráciu. Ako je znázornené na obr. 5.1, projekt implementuje dve z troch rozhraní, ktoré v našom projekte potrebujeme. Rozhranie S6a bohužiaľ v projekte nie je.

Najprv sme sa pokúšali rozhranie doimplementovať, ukázalo sa však, že zdrojový kód projektu bol príliš zložitý a nie veľmi prispôsobený na testovanie. Z toho dôvodu sme rozhodli vytvoriť vlastný čiastkový server HSS pre rozhranie S6a, pričom by bežali oba naraz.

Vzhľadom k rozsiahlosti špecifikácie funkcií HSS sme usúdili, že kompletná implementácia funkcionality je nad naše sily. Preto náš server HSS má iba obmedzenú funkcionalitu, ktorá je nevyhnutne vyžadovaná pre uskutočnenie hovoru. Správy, ktoré náš server HSS obsluhuje, sú vypísané v tab. 5.1.

HSS, ktoré sme takto vytvorili avšak nie je súčasťou EPC(Evolved packet core), ako to

môžeme vidieť na obrázku č.4.3 v predchádzajúcej kapitole ale je umiesntené podobne ako FHoSS na rovnakom viruálnom stroji. So samotným EPC je prepojený privátnou adresou. V rámci testovania HSS sme vytvorili aj klienta, ktorý zasiela požiadavky podobne ako mobilné zariadenie pripojené cez eNodeB.



Obr. 5.1: Znázornenie HSS v architektúre LTE. Zelenou farbou sú zvýraznené implementované rozhrania implementácie FHoSS, červenou farbou chýbajúce rozhrania.

Názov správy	Popis
3GPP-Authentication-Information	slúži na získanie autentifikačných informácií
3GPP-Notify	slúži na ukladanie adresy PDN a ďalších pripájacích informácií
3GPP-Update-Location	slúži na ukladanie identity MME do HSS a na získavanie predplatiteľských infrmácií
Device-Watchdog	slúži na skoré detegovanie chyby spojenia

Tabuľka 5.1: Správy obsluhované našim serverom HSS

6. SIM karty

Sim karty použité v tomto tímovom projekte boli od firmy Sysmocomo, konkrétne model sysmoUSIM-SJS1. Tieto SIM karty sú určené na použitie v GSM sieťach, ale možno ich použiť aj v ľubovoľnej UMTS a LTE sieti[1].
Vlastnosti sim karty sysmoUSIM-SJS1 sú nasledovné:

- GSM autentifikácia: COMP128v1, COMP128v2, COMP128v3, XOR, MILENAGE
- UMTS autentifikácia: MILENAGE, XOR
- Programovateľné ICCID
- Programovateľné MSISDN
- Programovateľné Ki / K / OP
- Kompatibilita s GSM TS 11.11
- 64 kB flash uložisko
- Podpora JAVA nástrojov (Card Manager, OTA, STK / SAT)
- Unikátny ADM kľúč
- Unikátne OTA kľúče (3DES)

Ako čítačku pre nami zvolené SIM karty sme si vybrali model s názvom „4World čítačka kariet SIM, USB 2.0“. Tento model je kompatibilný so softvérom SIM Utility verzie 9.0, ktorý je dostupný pre platformu MS Windows . Z Linuxových riešení je na výber program pySim, ktorý podporuje zariadenia PS/SC (Personal Computer / Smart Card) ale aj ACS (Advanced Card System). Program je napísaný v jazyku Python a je vydaný pod licenciou GLPv2 a je primárne určený pre operačný systém Ubuntu[2].

[1] http://shop.sysmocom.de/products/sysmousim-sjs1

[2] http://openbts.org/w/index.php?title=ProgrammingSIMcards

7. Testovanie systému

Vzhľadom k druhu projektu, kde našou úlohou nie je písanie zdrojového kódu, ale prepájanie komponentov, ich nastavovanie a zabezpečovanie ich behu, jednotkové testy (unit tests) majú pre nás len malú použiteľnosť. Na pretestovanie nášho produktu sú vhodnejšie testy na vyššej úrovni abstrakcie, tzv. systémové testy (system tests). Tie testujú kompletne zostavený systém a overujú rôzne veci - existuje niekoľko podkategórií systémových testov. Konrétne pre nás sú zaujímavé koncové testy (end-to-end tests).

Koncové testy majú za úlohu simulovať reálne používateľské scenáre od začiatku do konca a overiť, či celý tok prebehol podľa požiadaviek.

Na testovanie sme využili niekoľko programov.

Packet sender[1] je program na odosielanie TCP paketov. Využívali sme ho na nízkoúrovňové testovanie.

Pri testovanie vyššej úrovne sme používali klientov IMS, konkrétne Boghe[2] a Monster[3].

Jednotlivé testovacie scenáre sú vypísané v nasledovných sekciách.

7.1 IMS - IP Multimedia Subsystem

Potrebné nakonfigurovať parametre IMS servera. Je potrebne zadať prihlasovanie údaje vo forme SIP. Taktiež je potrebné nastaviť port a ip adresu P-CSCF komponentu. V tomto prípade, náš P-CSCF komponent fungoval na porte *4060* a ip adrese *147.175.204.50*.

Príklad testovanej konfigurácie pre Monster IMS klienta je možné vidieť na obrázku(Obr. 7.1). Daný IMS klient je implementovaný v jazyky JAVA, čo umožňuje daného klienta používať aj na iných platformách ako na MS Windows.

Obr. 7.1: Nastavenie konfigurácie pre Monster IMS klienta

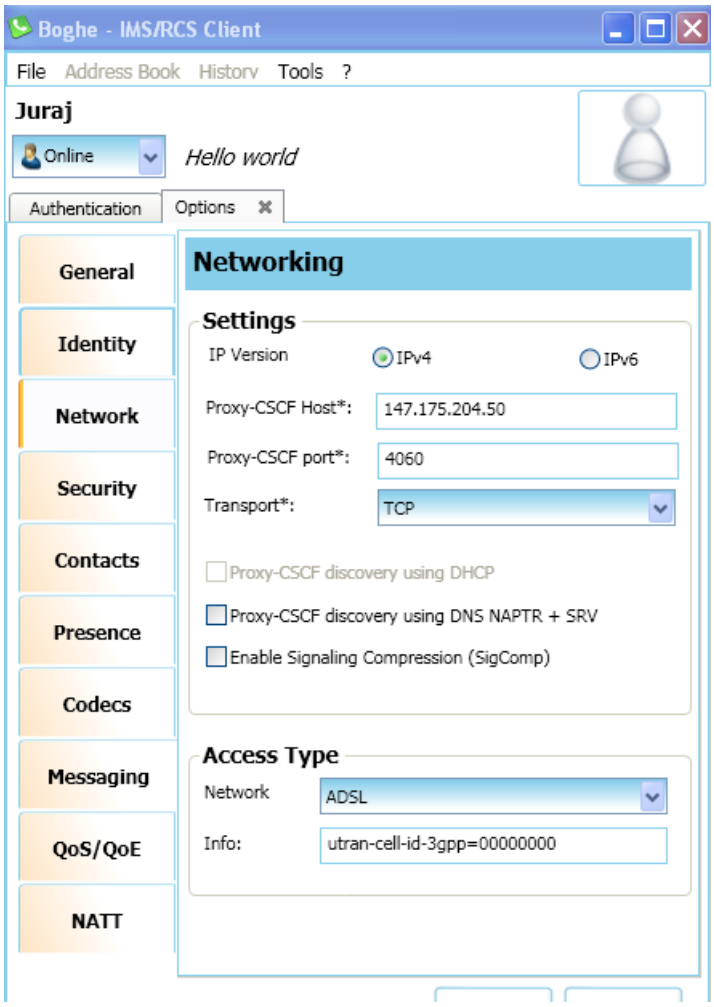
Príklad testovanej konfigurácie pre Boghe IMS klienta je možné vidieť na obrázku(Obr. 7.2). Daný IMS klient je implementovaný v jazyky C. Daný klient je možné využívať len

[1] `https://packetsender.com/`

[2] `https://github.com/DoubangoTelecom/boghe`

[3] `http://www.monster-the-client.org/index.html`

zo systémov MS windows.



Obr. 7.2: Nastavenie konfigurácie pre Boghe IMS klienta

Otestovali sme funkčnosť oboch IMS klientov pri klasických VoIP hovoroch. Obidva klienti vedia fungovať bez ohľadu či sa používajú boghe - boghe komunikácia alebo monster - boghe komunikácia.

7.1.1 Autentifikácia

Autentifikáciu sme testovali prihlásením do IMS cez IMS klienta. Pri správnych údajoch očakávame úspešné prihlásenie, zatiaľ čo pri nesprávnych údajoch očakávame chybovú hlášku.

7.1.2 Hovor

Hovor sme testovali pomocou IMS klientov spomenutých vyššie priamym napojením na IMS. Testovali sme všetky kombinácie klientov. Očakávaním bolo úspešné spojenie hovoru a prenos zvuku medzi zariadeniami.

7.2 EPC - Evolved Packet Core

7.2.1 Prihlásenie do systému

Testovanie prihlásenia sme testovali vysielaním paketov programom Packet Sender na MME a čítaním odpovedí. Test zahŕňa postupné vysielanie nasledovných paketov:

Odoslanie paketu S1AP Attach na MME
Očakávané prijatie správy S1AP Authentication request

Odoslanie paketu S1AP Authentication response na MME
Očakávané prijatie správy S1AP Security mode command

Odoslanie paketu S1AP Security mode complete na MME
Očakávané prijatie správy S1AP Attach accept, Initial context setup request, Activate default EPS context request

Odoslanie paketu S1AP Initial context setup response na MME
Odoslanie paketu S1AP Attach complete, Activate default EPS context response na MME
Odoslanie paketu S1AP Detach request na MME
Očakávané prijatie správy S1AP Detach accept
Očakávané prijatie správy S1AP UE context release command

Odoslanie paketu S1AP UE context release complete na MME

Zoznam použitej literatúry

[1] *Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1*, 3rd Generation Partnership Project Std., Rev. 13.3.0, June 2015. [Online]. Available: http://www.3gpp.org/DynaReport/22228.htm

[2] *IP Multimedia Subsystem (IMS); Stage 2*, 3rd Generation Partnership Project Std., Rev. 13.4.0, September 2015. [Online]. Available: http://www.3gpp.org/DynaReport/23228.htm

[3] *IMS Profile for Voice and SMS*, GSM Association Std., Rev. 7.0, March 2013. [Online]. Available: http://www.gsma.com/newsroom/wp-content/uploads/2013/04/IR.92-v7.0.pdf

[4] palo73, "Extending pcscf of the kamailio ims platform with nat traversal," Apr 2011. [Online]. Available: http://nil.uniza.sk/ngnims/kamailio-ims/extending-pcscf-kamailio-ims-platform-nat-traversal

[5] Minggu, "Installing openimscore with ipv6 capability on ubuntu 10.04," Nov 2013. [Online]. Available: http://rakaperbawa.blogspot.sk/2013/11/installing-openimscore-with-ipv6.html

[6] Mickey, "Openimscore : Installation and configuration guide," Dec 2011. [Online]. Available: http://mehic.info/2011/12/openimscore-installation-and-configuration-guide/

[7] *OpenIMSCore Installation Guide*, Dec 2011. [Online]. Available: http://www.openimscore.org/documentation/installation-guide/

[8] H. Kniberg, *Scrum and XP from the Trenches: Enterprise Software Development*. Lulu.com, 2007.

[9] *APM30H Quick Installation Guide*, Issue: 06 ed., Huawei.

[10] *BBU3900 Instalattion Guide*, Issue: 07 ed., Huawei.

[11] *GPS Satellite Antenna System*, Issue: 08 ed., Huawei, part Number: 31504601.

[12] *RRU3938 Instalation Guide*, Issue: 07 ed., Huawei.

Príloha A: Technická dokumentácia

Technická dokumentácia k projektu

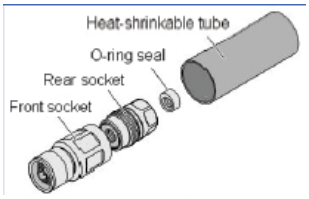
Príloha B: Príručka k vyrobeniu koncoviek na RF káble

Úvod

Koaxiálny RF konektor (konektor rádiovej frekvencie) je elektrický konektor určený pre prácu v prípade rádiových frekvencií v rozsahu viacerých Hertzov. RF konektory sa zvyčajne používajú s koaxiálnymi káblami a sú navrhnuté tak, aby zachovali tienenie. Lepšie modely tiež minimalizujú zmeny prenosových liniek a impedanciu na spojenie. Mechanicky poskytujú upevňovací mechanizmus a pružiny pre nízky ohmový elektrický kontakt a zároveň šetrí zlatý povrch, čo umožňuje veľmi vysoké párovanie. Výskumná činnosť v oblasti rádiofrekvenčných (RF) obvodov v tomto storočí vzrástla v priamej reakcii na obrovské trhové dopyty po lacných, vysokých dátových rýchlostiach bezdrôtového vysielača.

Obr. B.1: Hotový RF konektor

Tento dokument informuje o návode ako správne vytvoriť koncovku na RF kábel. Návod obsahuje aj obrázky pre lepšie pochopenie textu.



Obr. B.2: RF konektor rozložený na súčiastky

Prerezanie izolácie

Prvou vecou je správne narezanie vonkajšej izolácie, pričom musíme dávať pozor, aby sme nepoškodili kábel. Prvý úsek narežeme asi 8 mm od konca kábla.

Obr. B.3: Prerezanie izolácie

Odobratie izolácie

Pomocou kombinačiek opatrne odoberieme vrchnú izoláciu.

Obr. B.4: Odobratie izolácie

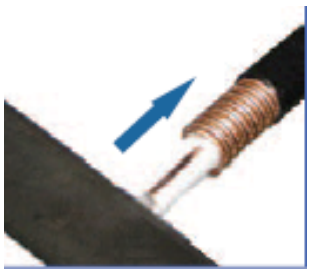
Odobratie ďalšieho kusu izolácie

Odoberieme ďalší kus izolácie no v tomto prípade už zanecháme aj pozlátenú časť kábla. Pri rezaní dávame veľký pozor. Narezávame asi 28 mm od konca kábla.

Obr. B.5: Narezanie ďalšieho kusu kábla

Odstránenie bielej izolácie

Opatrne narežeme bielu izoláciu a pomocou kombinačiek ju odstránime. Dávame pozor, aby sme nepoškodili hlavný vodič.

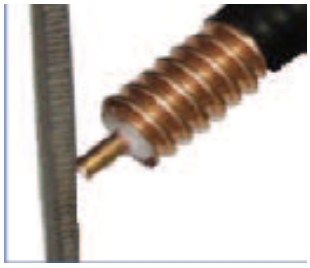


Obr. B.6: Odstránenie plastovej bielej izolácie

Skrátenie hlavného vodiča
Hlavný vodič skrátime na dĺžku 8 mm.

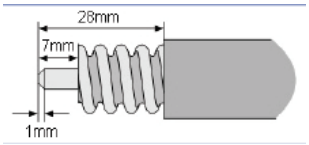
Obr. B.7: Skrátenie hlavného vodiča

Zabrúsenie hlavného vodiča
Posledný 1 mm z hlavného vodiča zabrúsime, aby lepšie zapadol do koncovky



Obr. B.8: Zabrúsenie hlavného vodiča

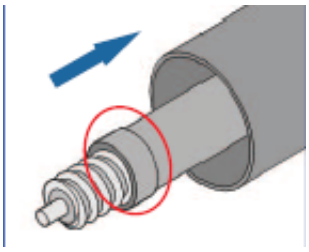
Predpripravený kábel
Takto sa nám podarilo pripraviť kábel na nasadenie koncovky. Teraz si ešte raz skontrolujeme vzdialenosti jednotlivých úsekov.



Obr. B.9: Rozmery predpripraveného kábla

Nasadenie izolačného prvku

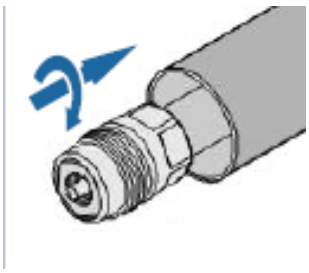
Nasadíme izolačný prvok, pričom dávame pozor, aby sme ho nepretrhli. Nasadíme ho až po úroveň, kde začína pôvodná izolácia kábla.



Obr. B.10: Nasadenie izolačného prvku

Zatiahnutie zadnej časti koncovky

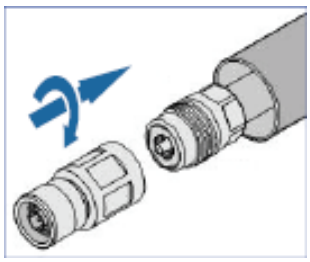
V tomto bode sa dostávame už k samotnému nasadeniu koncovky. Najskôr sa nasadzuje zadná koncovka, ktorá sa zaťahuje v smere hodinových ručičiek.



Obr. B.11: Zatiahnutie zadnej časti koncovky

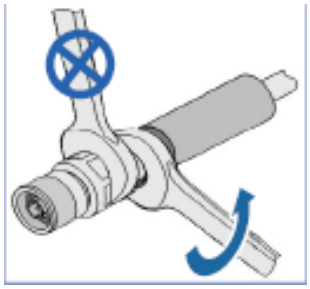
Zatiahnutie prednej časti koncovky

Nasunieme aj prednú koncovku a zaťahujeme taktiež v smere hodinových ručičiek. Ak nastane problém, že závit sa nezachytí, musíme zadnú koncovku trochu povytiahnúť.



Obr. B.12: Zatiahnutie prednej časti koncovky

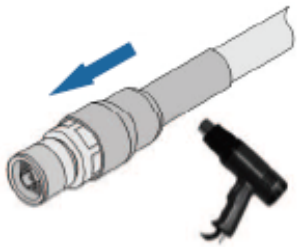
Následne zoberieme potrebné kľúče. Prednú a zadnú koncovku poriadne dotiahneme.



Obr. B.13: Poriadne zatiahnutie koncovky

Izolácia pomocou teplovzdušnej pištole

Nakoniec nasadíme poslednú izoláciu a pomocou teplovzdušnej pištole ju prichytíme o kábel a koncovku.



Obr. B.14: Posledné zaizolovanie celého konektoru pomocou teplovzdušnej pištole

Príloha C: Technická dokumentácia

Konfigurácia PGW

//S5S8
configure
context pgw -noconfirm
interface s5s8_int tunnel
ipv6 address fdb5:915e:710a::2/64
tunnel-mode ipv6ip //po dohode sme tunel nepoužili
source interface s5s8_int
destination address 147.175.204.85
exit
interface s5s8_int2
ip address 192.168.0.10 255.255.255.0
exit
exit
policy accounting rf_pol -noconfirm
accounting-level flow
accounting-event-trigger interim-timeout action stop-start
operator-string pgw_local
exit
subscriber default
exit
exit
port ethernet 1/18
no shutdown
bind interface s5s8_int_2 pgw
end

//APN
configure
context pgw -noconfirm
apn apn
accounting-mode radius
ims-auth-service gx_ims
aaa group rf_rad
dns primary 8.8.8.8
dns secondary 147.175.99.1
ip access-group access_in in
ip access-group access_out out
mediation-device context-name pgw
ip context-name pdn
ipv6 access-group accessv6_in in
ipv6 access-group accessv6_out out
active-charging rulebase rule
end

//AAA
configure
context pgw -noconfirm

aaa group rf_rad
radius attribute nas-identifier 1
radius accounting interim interval 180
radius dictionary standard
diameter authentication dictionary aaa-custom1
diameter accounting dictionary aaa-custom1
diameter authentication endpoint s6b_cfg
diameter accounting endpoint rf_cfg
diameter authentication server s6b_cfg priority 1
diameter accounting server rf_cfg priority 1
exit
aaa group default
radius attribute nas-ip-address address 192.168.4.10 //tu som si vymyslel
radius accounting interim interval 180
diameter authentication dictionary aaa-custom1
diameter accounting dictionary aaa-custom1
diameter authentication endpoint s6b_cfg
diameter accounting endpoint rf_cfg
diameter authentication server s6b_cfg priority 1
diameter accounting server rf_cfg priority 1
end

//LMA
configure
context pgw
lma-service lma -noconfirm
no aaa accounting
revocation enable
bind ipv4-address 192.168.0.10
end

//PDN
configure
context pdn -noconfirm
interface sgi_ipv4_int
ip address 147.175.204.83 255.255.0.0
end

//PGW service
configure
context pgw
pgw-service pgw_service -noconfirm
plmn id mcc 231 mnc 78
associate lma-service lma_service
associate qci-qos-mapping qci_qos
authorize external
fqdn host domain realm realm
end

//Static IP route

configure
context pgw
ip route 0.0.0.0 0.0.0.0 192.168.0.20 s5s8_int_2
end

//pgw-pdn context
configure
context pdn -noconfirm
interface pdn_sgi_int
ip address 147.175.204.83 255.255.255.0
exit
ip pool pool_pdn range 192.168.3.50 192.168.3.100 public 1
subscriber default
ip access-list list
redirect css service css_service any
permit any
exit
aaa group default
exit
exit
port ethernet 1/17
no shutdown
bind interface pdn_sgi_int pdn
exit
end

//Active Charging Service Configuration
configure
require active-charging optimized-mode
active-charging service char_service
ruledef rule_def
exit
ruledef default
ip any-match = TRUE
exit
ruledef icmp-pkts
icmp any-match = TRUE
exit
ruledef qci3
icmp any-match = TRUE
exit
ruledef static
icmp any-match = TRUE
exit
charging-action char_act
exit
charging-action icmp
billing-action egcdr
exit
charging-action qci3

content-id 1
billing-action rf
qos-class-identifier 1
allocation-retention-priority 1
tft packet-filter qci3
exit
charging-action static
service-identifier 1
billing-action rf
qos-class-identifier 1
allocation-retention-priority 1
tft packet-filter qci3
exit
packet-filter pack_filt
ip remote-address = 192.168.3.20
ip remote-port = 5555
exit
rulebase default
exit
rulebase rule_base
end

//Creating and Configuring the AAA Context
configure
context aaa -noconfirm
interface s6b_int
ip address 147.175.204.87 255.255.255.0
exit
interface gx_int
exit
subscriber default
exit
ims-auth-service gx_ims
p-cscf discovery table 1 algorithm round-robin
p-cscf table 1 row-precedence 1 ipv4-address 192.168.4.10//<pcrf_adr>
policy-control
diameter origin endpoint gx_cfg
diameter dictionary dpca-custom1
diameter host-select table 1 algorithm round-robin
diameter host-select row-precedence 1 table 1 host gx_cfg
exit
exit
diameter endpoint s6b_cfg
origin realm realm
origin host host address 192.168.4.20 //aaa_ctx
peer s6b_cfg realm realm address 192.168.4.30
route-entry peer s6b_cfg
exit
diameter endpoint gx_cfg
origin realm realm

origin host host address 192.168.4.20 //aaa_ctx
peer gx_cfg realm realm address 192.168.4.30 //pcrf
route-entry peer gx_cfg
exit
diameter endpoint gy_cfg
use-proxy
origin realm realm
origin host host address 192.168.4.20 //gy
connection retry-timeout 180
peer gy_cfg realm realm address 192.168.4.40 //<ocs_ipv6_addr>
route-entry peer gy_cfg
exit
diameter endpoint <rf_cfg_name>
origin realm <realm_name>
origin host host address 192.168.4.50 //<rf_ipv4_address>
peer rf_cfg realm realm address 192.168.4.60 //<ofcs_ipv4_addr>
route-entry peer rf_cfg
exit
exit

//Configuring QCI-QoS Mapping
configure
qci-qos-mapping qci_map
qci 1 downlink user-datagram dscp-marking 0x20
qci 3 downlink user-datagram dscp-marking 0x20
qci 9 downlink user-datagram dscp-marking 0x20
end

Konfigurácia Mobility Management Entity

MME, alebo Mobility Management Entity je jednotka zodpovedná za vykonávanie riadiacej logiky v LTE architektúre. Virtuálny systém asr5000 obsahuje komponent aj pre túto entitu. Konfigurácia virtuálneho zariadenia postupovala podľa dokumentácie od spoločnosti Cisco. Každý komponent v systéme je zadefinovaný ako tzv. *context,* pod ktorým sa nachádzajú všetky funkcie komponentu. Rozhrania VirtualEthernet sú virtuálne sieťové rozhrania, ktoré slúžia na prepájanie komponentov v rámci systému ako aj s externými komponentmi siete.

```
  context mme
    interface s1-mme
      ip address 147.175.204.81 255.255.255.0
    #exit
    interface s11
      ip address 192.168.1.30 255.255.255.0
    #exit
    interface s6a
      ip address 192.168.2.10 255.255.255.0
    #exit
    subscriber default
    exit
    domain show default subscriber mme_service
    aaa group default
    #exit
    hss-peer-service hss_peer_mme
      diameter hss-endpoint hss_end_new eir-endpoint eir_end
    exit
    diameter endpoint eir_end
      origin realm eir
    #exit
    diameter endpoint hss_end_new
      origin realm hss
      origin host hssko address 192.168.2.10
      peer peerko realm hss address 192.168.2.20
      route-entry realm hss peer peerko
    #exit
    mme-service mme_service
      mme-id group-id 61005 mme-code 113
      plmn-id mcc 231 mnc 78
      network-sharing plmnid mcc 231 mnc 78 mme-id group-id 61005
mme-code 113
      associate egtp-service sgw-egtp-egress-service context mme
      associate hss-peer-service hss_peer_mme context mme
      policy attach imei-query-type imei-sv verify-equipment-
identity
      pgw-address 192.168.1.20
      bind s1-mme ipv4-address 147.175.204.81
    egtp-service sgw-egtp-egress-service
```

```
    interface-type interface-mme
    gtpc bind ipv4-address 192.168.1.30
  #exit
#exit

port ethernet 1/13
  no shutdown
  bind interface s1-mme mme
#exit
port ethernet 1/14
  no shutdown
  bind interface s6a mme
#exit
port ethernet 1/15
  no shutdown
  bind interface s11 mme
#exit
```

Konfigurácia S-GW

Creating an S-GW Ingress Context

```
configure
context sgwIngressContext -noconfirm
        subscriber default
        exit
interface sgw_s1u
        ip address 147.175.204.82/16
        exit
        interface sgw_s11
        ip address 192.168.1.20/24
        exit
ip route 0.0.0.0 0.0.0.0 147.175.204.82/32 sgw_s1u
        exit
ip route 0.0.0.0 0.0.0.0 192.168.1.20/32
        exit
port ethernet 1/16
        no shutdown
        bind interface sgw_s1u sgwIngressContext
        end
port ethernet 1/11
        no shutdown
        bind interface sgw_s11 sgwIngressContext
        end
```

Creating an S-GW Ingress Service

```
configure
context sgwIngressContext
        egtp-service sgwEgtpIngressService -noconfirm
        end
```

Creating an eGTP Egress Service

```
configure
context sgwEgressContext
        egtp-service sgw_egtp_egress_service -noconfirm
        end
```

Creating an S-GW Service

```
configure
        context sgwIngressContext
        sgw-service sgw_service -noconfirm
        end
```

eGTP Configuration

Setting the System's Role as an eGTP S-GW and Configuring GTP-U and eGTP Service Settings

```
configure
context sgwIngressContext
        gtpp group default
        exit
gtpu-service sgw_gtpu_ingress_service
        bind ipv4-address 147.175.204.82
        bind ipv4-address 192.168.1.20
        exit
        egtp-service sgwEgtpIngressService
                interface-type interface-sgw-ingress
                validation-mode standard
                associate gtpu-service sgw_gtpu_ingress_service
                gtpc bind ipv4-address 147.175.204.82
                gtpc bind ipv4-address 192.168.1.20
                exit
        exit
context sgwEgressContext
        gtpu-service sgw_gtpu_egress_service
                bind ipv4-address 192.168.0.20
                exit
        egtp-service sgw_etgp_egress_service
                interface-type interface-sgw-egress
                validation-mode standard
                associate gtpu-service sgw_gtpu_egress_service
                gtpc bind ipv4-address 192.168.0.20
                end
```

Configuring the S-GW Service

```
configure
        context sgwIngressContext
                sgw-service sgw_service
                associate ingress egtp-service sgwEgtpIngressContext
                associate egress-proto gtp egress-context sgwEgressContext
                end
```