

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2016

Bc. Michal Duda



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY

A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

RÁDIOVÁ PŘÍSTUPOVÁ SÍŤ MOBILNÍ SÍŤE

RADIO ACCESS NETWORK OF A CELLULAR NETWORK

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Michal Duda

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Radko Krkoš

BRNO 2016



Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**

Ústav telekomunikací

Student: Bc. Michal Duda

ID: 146812

Ročník: 2

Akademický rok: 2015/16

NÁZEV TÉMATU:

Rádiová přístupová síť mobilní sítě

POKYNY PRO VYPRACOVÁNÍ:

Popište rádiovou přístupovou síť mobilní sítě a diskutujte přístup k servisním zásahům do produkční rádiové přístupové sítě. Zaměřte se na vytvoření všeobecného postupu, kde vlastní servisní zásah může být například změna aktivního segmentu jádra sítě pro základnovou stanici, konverze transportního protokolu z IPv4 na IPv6, testování nouzových služeb či ověřování vzájemného rušení s jinými rádiovými technologiemi, například systémy satelitního rádia Sirius XM. Analyzujte existující postupy pro servisní zásahy do RAN, identifikujte problematické části a vypracujte metodiku, která je zlepší, zejména se věnujte řízení kolizí v servisních zásazích a zajištění dostatečné kapacity rádiového okolí při odstávce buňky kvůli servisnímu zásahu.

DOPORUČENÁ LITERATURA:

[1] MISHRA, Aray R. Advanced Cellular Network Planning and Optimisation: 2G/2.5G/3G. Evolution to 4G. Chichester. John Wiley, 2007, 521 p. ISBN 04-700-1471-7.

[2] FCC.gov: 9-1-1 and E9-1-1 Services [online]. 2015. USA: Federal Communications Commission, 9. říjen 2015. Dostupné z: <https://www.fcc.gov/encyclopedia/9-1-1-and-e9-1-1-services>

Termín zadání: 1.2.2016

Termín odevzdání: 25.5.2016

Vedoucí práce: Ing. Radko Krkoš

Konzultant diplomové práce:

doc. Ing. Jiří Mišurec, CSc., předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Cieľom práce bolo vyskúšať a diskutovať servisné zásahy do produkčnej rádiovkej prístupovej siete. Zamerať sa na vytvorenie všeobecného postupu testovania služby tiesňového hovoru, odstránenia rušenia sa rádiových technológií, konverzie transportného protokolu základňovej stanice a zmenu aktívneho segmentu jadra siete základňovej stanice. Následne identifikovať problematické časti a vypracovať návrh ich zlepšenia.

KLÚČOVÉ SLOVÁ

LTE, E-UTRAN, EPC, 4G, E911, servisný úkon, transportný protokol, rušenie, základňová stanica

ABSTRACT

The aim of the work was to try and discuss service interventions into the production of the radio access network. Focus on the creation of the testing procedure call emergency services, removing the interference of radio technologies, transport protocol conversions of eNodeB and server migration for eNodeB. Then identify problem areas and make proposals to improve them.

KEYWORDS

LTE, E-UTRAN, EPC, 4G, E911, service maintenance operation, interference, transport protocol, eNodeB

PREHLÁSENIE

Prehlasujem, že som svoju diplomovú prácu na tému „Rádiová přístupová síť mobilní sítě“ vypracoval(a) samostatne pod vedením vedúceho diplomovej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/nebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o právu autorskom, o právoch súvisajúcich s právom autorským a o zmene niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávných dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno

.....

podpis autora(-ky)

POĎAKOVANIE

Rád by som poďakoval vedúcemu diplomovej práce pánovi Ing. Radkovi Krkošovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno

.....

podpis autora(-ky)



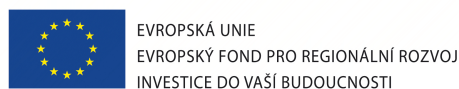
Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
<http://www.six.feec.vutbr.cz>

POĎAKOVANIE

Výzkum popsaný v tejto diplomovej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno

.....
podpis autora(-ky)



OBSAH

Úvod	10
1 Štvrtá generácia (4G)	11
1.1 Architektúra systému LTE	12
1.1.1 E-UTRAN	12
1.1.2 Paketové jadro EPC	14
2 Služba tiesňového volania	16
2.1 Služba E911	16
2.1.1 Fáza 1	16
2.1.2 Fáza 2	16
2.2 Architektúra služby E911 v 4G	18
2.3 Testovanie služby E911	22
2.3.1 Kontrola základňovej stanice	22
2.3.2 Príprava základňovej stanice na testovanie	26
2.3.3 Obnovenie pôvodných nastavení základňovej stanice	28
3 Rádiové technológie a ich rušenie	29
3.1 Odstránenie rušenia rádiových technológií	30
4 Konverzia transportného protokolu	40
5 Zmena aktívneho prvku	49
6 Záver	56
Literatúra	57
Zoznam symbolov, veličín a skratiek	60
Zoznam príloh	63
A Výpis KPI pred konverziou	64
B Výpis KPI po konverzii	65
C Definícia základňovej stanice	66
D Vymazanie základňových staníc	69
E Obsah priloženého CD	70

ZOZNAM OBRÁZKOV

1.1	Architektúra EPS	12
1.2	Protokolová výbava používateľskej roviny	13
2.1	E911 Fáza 1	17
2.2	E911 Fáza 2	18
2.3	Architektúra zapojenia tiesňovej služby	19
2.4	Náhľad prvkov základňovej stanice	23
2.5	Príklad alarmov na zariadení Alcatel	24
2.6	Náhľad na živé frekvenčné pásmo základňovej stanice Alcatel-Lucent	26
3.1	Frekvenčný náhľad WCS a jeho susedných spektier [12]	29
3.2	Diagram odstránenia rušenia rádia Sirius XM spektrom WCS	31
3.3	A: mechanické natočenie antény, B: elektrické natočenie antény	35
3.4	Názorná ukážka jemného blokovania sektorov	38
3.5	Názorná ukážka kontroly vyťaženia sektorov	39
4.1	Názorná ukážka zapojenia základňovej stanice	40
4.2	Mobilita transportnej vrstvy [15]	45
5.1	Vytváranie skupiny s následným pridávaním základňových staníc	50
5.2	Exportovanie serverových nastavení základňových staníc	51
5.3	Odstraňovanie základňových staníc z profilu na zdrojovom serveri	53
5.4	Vytvorenie novej konfigurácie pre aktivovanie nových základňových staníc	54
5.5	Aktivácia konfigurácie nových základňových staníc	54

ÚVOD

Systémy mobilnej komunikácie urobili zásadný prevrat v spôsobe, akým ľudia komunikujú, keď združili dokopy komunikáciu a mobilitu. V histórii bezdrôtovej komunikácie sme prešli dlhou cestou vývoja za úctihodne krátky čas. Evolúciou bezdrôtových prístupových technológií sme dospeli k štvrtej generácii (4G) mobilných sietí, ktorá sa začína skúšobne nasadzovať v posledných rokoch. Pri pohľade do minulosti, bezdrôtové prístupové technológie nasledovali rôzne evolučné cesty s jedným cieľom, a to výkon a efektivita v oblasti mobilného prostredia.

Táto diplomová práca sa venuje popisovaniu praktických úkonov a zásahov do rádiovkej prístupovej siete mobilnej siete. Teoretický časť je venovaná stručnému oboznámeniu sa s problematikou. Môžete sa tu dočítať o systéme štvrtej generácie mobilných sietí, o jeho architektúre, protokolovej výbave a popise jednotlivých prvkov siete. Ďalšia časť je venovaná službe tiesňového volania, ktorá tvorí dôležitú časť mobilných sietí.

Praktická časť práce sa venuje popisu vykonaných servisných úkonov v prístupovej sieti mobilných sietí. Opisované sú úkony testovania služby tiesňového hovoru, odstránenie rušenia sa rádiových technológií, konverzia transportného protokolu základňovej stanice a zmena aktívneho segmentu jadra siete pre základňovú stanicu.

Cieľom tejto práce bude priblížiť čitateľom servisné zásahy vykonávané v mobilných sieťach a vytvorenie všeobecného návodu na vykonanie týchto úkonov, zistenie problematických častí úkonov a návrh ich riešenia.

1 ŠTVRTÁ GENERÁCIA (4G)

Predchádzajúci systém tretej generácie (3G) UMTS (Universal Mobile Telecommunication System - univerzálny mobilný telekomunikačný systém) nespĺnil požiadavky IMT-2000 (International Mobile Telecommunications - medzinárodný telekomunikačný úrad) ihneď po jeho nasadení v praxi. Bolo potrebné ho zlepšiť, aby spĺňal alebo prekračoval stanovené normy. Kombinácia HSDPA (High Speed Downlink Packet Access - vysokorýchlostný prenos paketov v smere downlink) a následné pridanie HSUPA (High Speed Uplink Packet Access - vysokorýchlostný prenos paketov v smere uplink) viedlo k vytvoreniu technológie známej ako HSPA (High Speed Packet Access - vysokorýchlostný prenos paketov) tiež známej ako 3,5G.

Motiváciou zvyšovania sa dopytu po mobilných službách s vyššími prenosovými rýchlosťami a kvalitou služieb 3GPP začalo pracovať na dvoch projektoch, LTE (Long Term Evolution) a SAE (System Architecture Evolution), ktoré mali v úmysle definovať rádiovú prístupovú sieť RAN a jadro siete. LTE/SAE tiež známe ako EPS (Evolved Packet System - vyvinutý paketový systém), sa stal dôležitým krokom v bezdrôtových technológiach. Poskytuje vysoko efektívnu, bezpečnejšiu službu s nízkym oneskorením. Hlavné rádiové prístupové technológie sú OFDMA (Orthogonal Frequency Division Multiplexing - ortogonálny multiplex s frekvenčným delením) a MIMO (Multiple Input Multiple Output - viac vstupov viac výstupov). Na sieťovej vrstve bola definovaná čisto IP architektúra s podporou kvality služieb. Po nasadení prvých 4G systémov sa ale zistilo, že nespĺňajú všetky 4G požiadavky ITU (International Telecommunication Union - medzinárodná telekomunikačná únia) a kvôli tomuto sa tieto systémy označujú ako 3,9G.

Kandidátom na 4G systém je rádiová technológia LTE-Advanced (pokročilé LTE), ktorá je spätne kompatibilná s LTE. Spätnou kompatibilitou sa myslí možnosť nasadenie LTE-Advanced v spektre LTE bez akéhokoľvek dopadu na už existujúce LTE terminály. Ďalšími kandidátmi sú technológie IEE 802.16m a TD-LTE-Advanced.

IMT-Advanced (International Mobile Telecommunications-Advanced štandard) požiadavky na 4G systém sú:

- Vysoká zhodnosť funkčnosti systému na celom svete pri zachovaní flexibility podpory širokej škály služieb a aplikácií nákladovo efektívnym spôsobom;
- Kompatibilita služieb s pevnými sieťami;
- Kompatibilita spolupráce s inými rádiovými prístupovými systémami;
- Vysoko kvalitné mobilné zariadenia;
- Schopnosť celosvetového roamingu;
- Vylepšené špičkové prenosové rýchlosti (100 Mbit/s v prípade vysokej mobility)

a 1 Gbit/s v prípade nízkej mobility používateľa).

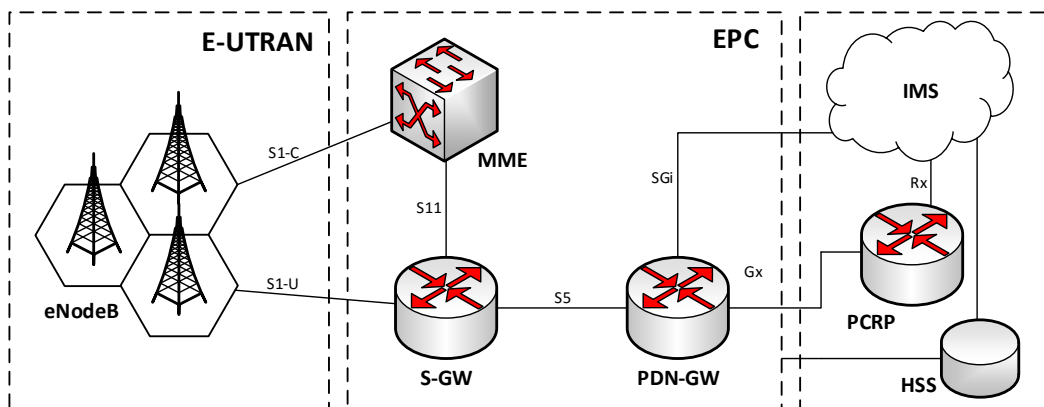
1.1 Architektúra systému LTE

Táto práca sa zameriava na servisné úkony vykonávané v prístupovej časti (LTE) mobilnej siete, a preto bude následne opísaný systém 3,9G, ktorý je momentálne nasadený celosvetovo. Systém 4G je momentálne stále v testovacej fáze.

3GPP špecifikovalo prvky a požiadavky na EPS architektúru, ktoré budú slúžiť ako základ pre siete ďalšej generácie. Táto špecifikácia Release 8[5] ustanovila dva hlavné podsystémy, LTE a SAE, ktoré viedli k špecifikácii EPC (Evolved Packet Core - vyvinuté paketové jadro), E-UTRAN (Evolved Universal Terrestrial Radio Access Network - vyvinutá univerzálna rádiová prístupová sieť) a E-UTRA (Evolved Universal Terrestrial Radio Access - vyvinuté rádiové rozhranie). Každé odpovedá jadrú systému, rádiovéj prístupovej časti systému a rádiovému rozhraniu systému. EPS poskytuje IP konektivitu medzi používateľom a externou paketovou dátovou sieťou za použitia E-UTRAN.

V súvislosti so 4G systémami, rádiové rozhranie a rádiová prístupová sieť boli vylepšené alebo predefinované, no jadro systému, EPC, neprešlo veľkými zmenami od už štandardizovanej architektúry SAE. V tejto sekcii sa môžete dočítať o prehľade E-UTRAN architektúry a o hlavných funkciách prvkov EPC.

1.1.1 E-UTRAN

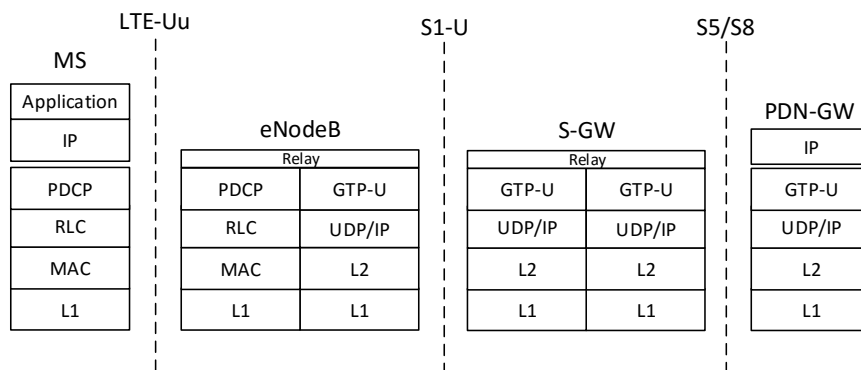


Obr. 1.1: Architektúra EPS

Na obrázku 1.1 môžete vidieť architektúru E-UTRAN pre systém LTE. Hlavnou časťou v architektúre je eNodeB (enhanced NodeB), ktorý poskytuje rádiové

rozhranie s protokolmi používateľskej a riadiacej roviny. Každý eNodeB je logický komponent, ktorý obsluhuje jednu alebo viacero buniek, rozhranie spájajúce jednotlivé eNodeB nazvané rozhranie X2. Do EPC môžu byť tiež pripojené HeNodeBs (Home eNodeB - domáca eNodeB tiež nazvané femtocell), nízko nákladové eNodeB pre domáce alebo vnútorné použitie, ktoré byť pripojené priamo alebo prostredníctvom brány, ktorá poskytuje dodatočnú podporu pre veľké množstvo HeNodeB.

Ako už bolo spomenuté, eNodeB poskytuje E-UTRAN s potrebnými protokolmi používateľskej a riadiacej roviny. Na obrázku 1.2 môžete vidieť protokolovú výbavu E-UTRAN. V používateľskej rovine sa nachádzajú PDCP (Packet Data Convergence Protocol), RLC (Radio Link Control - protokol riadenia rádiovej linky) a MAC (Medium Access Control - protokol riadenia prístupu k médiu) protokoly.



Obr. 1.2: Protokolová výbava používateľskej roviny

Hlavné funkcie jednotlivých vrstiev sú:

- NAS (Non-Access Stratum)
 - Správa spojenia medzi používateľom a jadrom siete;
 - Overenie používateľa;
 - Registrácia používateľa;
 - Aktivácia a deaktivácia nosičov;
 - Správa lokácie používateľov.

- RRC (Radio Resource Control)
 - Nadviazanie, udržiavanie a uvoľnenie RRC spojenia;
 - Funkcia bezpečnosti vrátane správy kľúčov;
 - Funkcia mobility používateľov;
 - Priamy prenos NAS správ medzi používateľom a NAS.

- PDCP (Packet Data Convergence Protocol)
 - Kompresia hlavičky paketu;
 - Doručenie dát v poradí a preposielanie dát;
 - Šifrovanie a ochrana integrity dát.

- RLC (Radio Link Control)
 - Oprava chýb pomocou ARQ (Automatic Repeat reQuest - žiadosť automatického opakovania);
 - Segmentácia podľa veľkosti transportného bloku;
 - Protokolová detekcia chýb a ich obnova;
 - Doručovanie v poradí.

- MAC (Medium Access Control)
 - Multiplexing a demultiplexing RLC dát;
 - Oprava chýb pomocou HARQ (Hybrid ARQ);
 - Prioritizácia lokálnych kanálov;
 - Hlásenie plánovaných informácií.

1.1.2 Paketové jadro EPC

EPC je sieť založená čisto na protokole IP a môže byť prístupná cez 3GPP rádiové prístupy (UMTS, HSPA, HSPA+, LTE) a nie 3GPP rádiové prístupy (WiMAX, WLAN). Dovoľuje prenos procedúry handover vo vnútri jedného alebo medzi oboma typmi rádiových prístupov. Práve táto flexibilita prístupu k EPC je atraktívna pre operátorov, pretože im umožňuje používať jedno jadro, podporujúce rôzne služby. Hlavnými prvkami EPC a ich funkciami sú:

- MME (Mobility Management Entity - prvok pre správu mobility)
MME je kľúčový prvok riadiacej roviny. Mimo ostatných funkcií, MME poskytuje funkciu zabezpečenia (autentifikácia, autorizácia), NAS signalizáciu, riadi mobilitu v stave nečinnosti, roaming a handovery. Taktiež vyberá pre používateľov S-GW a PDN-GW.

- S-GW (Serving Gateway)
S-GW je ukončujúci bod EPC, ktorý je pripojený do E-UTRAN cez rozhranie S1-U. Každý používateľ má pridelené jedno S-GW, ktoré slúži ako spojovací bod pre lokálne handovery a mobilitu v rámci technológií 3GPP. Vykonáva účtovanie medzi operátormi a tiež smeruje i preposiela pakety.

- PDN-GW (Packet Data Network Gateway)

Tento prvok poskytuje používateľovi prístup do dátovej paketovej siete pridelením IP adresy. ePDG (evolved PDG - vyvinuté PDG) poskytuje bezpečné spojenie medzi používateľmi pripojenými z nedôveryhodných prístupových sietí a EPC použitím tunelu IPsec (IP security - bezpečný internetový protokol).

Z pohľadu používateľskej roviny sú v systéme štvrtej generácie iba prvky eNodeB a brány (gateway), čo redukuje zložitosť tohto systému v porovnaní s predchádzajúcimi architektúrami. [7]

2 SLUŽBA TIESŇOVÉHO VOLANIA

Služba 911¹ je už nevyhnutnou súčasťou reakcie na mimoriadne udalosti a pripravenosť každého štátu na katastrofy. V októbri 1999, zákon 911² (zákon o bezdrôtovej komunikácii a verejnej bezpečnosti) nabral platnosť za účelom zlepšenia verejnej bezpečnosti podporou a uľahčením nasadenia celoštátnej jednotnej komunikačnej infraštruktúry pre záchranné služby. Jedným z ustanovení bolo, aby služba 911 používala univerzálne číslo tiesňového volania pre všetky telefónne služby a aby bola služba bezplatná z ktorejkoľvek pevnej linky, mobilného telefónu (aj bez odomknutia alebo použitia SIM karty) alebo verejného telefónu. V prípade Európskej únie vznikli potrebné predpisy v roku 2003. [13]

Na rýchlejšie a účinnejšie dosiahnutie pomoci boli modernizované nosiče a prvky sietí verejnej bezpečnosti. Napríklad väčšina záchranných systémov už automaticky hlási telefónne číslo a polohu volajúceho z pevnej siete, čo je schopnosť nazývaná E911 (Enhanced 911 - rozšírená služba 911). [11]

2.1 Služba E911

V roku 1999, FCC (Federal Communications Commission - federálna komisia pre komunikáciu) ustanovila nariadenia, ktoré vyžadujú, aby bezdrôtové nosiče poskytovali službu E911 na žiadosť PSAP (Public Safety Answering Point - verejná záchranná služba). Presnosť lokalizácie požadovaná FCC je rozdelená na dve fázy.

2.1.1 Fáza 1

V tejto fáze musia nosiče poskytnúť PSAP nasledujúce údaje:

- Číslo volajúceho;
- Polohu základňovej stanice;
- Sektor základňovej stanice.

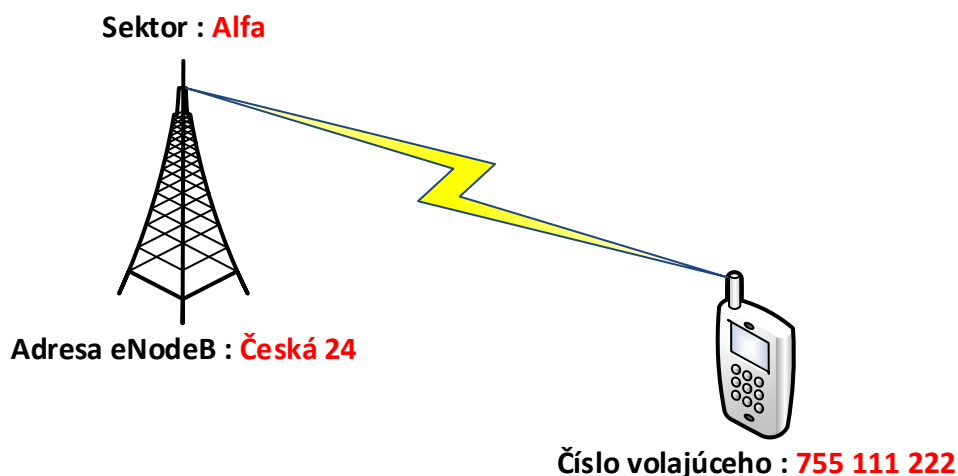
2.1.2 Fáza 2

V tejto fáze, oproti fáze 1, musia nosiče navyše poskytnúť PSAP:

- Určenie polohy volajúceho.

¹Americká obdoba celoeurópskej linky 112 slúžiaca na privolanie zložiek integrovaného záchranného systému.

²Zákon 911 americkej legislatívy.



Obr. 2.1: E911 Fáza 1

Lokalizačné techniky

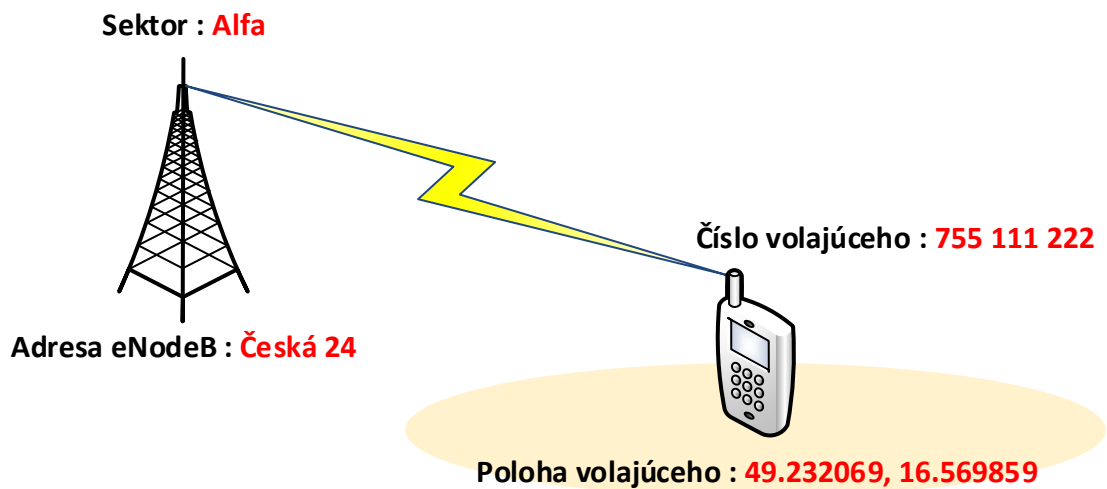
Fáza 1 je relatívne jednoduchá, používa jednoduché vyhľadávanie v databáze. Fáza 2 však musí navyše určiť polohu volajúceho, jeho zemepisnú dĺžku a šírku, na čo sa používajú dve techniky určenia polohy:

- Lokalizácia cez mobilné zariadenie: AGPS;
- Lokalizácia cez mobilnú sieť: UTDOA.

Lokalizácia cez mobilné zariadenie (AGPS)

AGPS (Assisted Global Position System - asistovaný globálny pozičný systém) je lokalizačná technika, ktorá vylepšuje klasickú GPS. Mobilné zariadenie používa GPS satelity na stanovenie svojej lokácie a získané dáta odošle do PSAP. Presnosť tejto metódy veľmi závisí na prostredí, v ktorom sa volajúci nachádza. Na výpočet svojej polohy musí GPS prijímač v mobilnom zariadení prijať merania aspoň zo štyroch GPS satelitov. Táto metóda môže, kvôli relatívne pomalému rozhraniu, trvať dve až dvanásť minút. Tento čas je však príliš dlhý pre tiesňovú službu a taktiež znižuje výdrž batérie v zariadení.

V momente, keď príde tiesňový hovor z mobilného zariadenia, podporujúceho AGPS, asistenčné dáta sú doručené cez mobilnú sieť na oznámenie mobilnému zariadeniu, kde sa nachádzajú GPS satelity. S týmito pomocnými dátami sa čas lokalizácie skrúti na 20 a menej sekúnd.



Obr. 2.2: E911 Fáza 2

Lokalizácia cez mobilnú sieť (UTDOA)

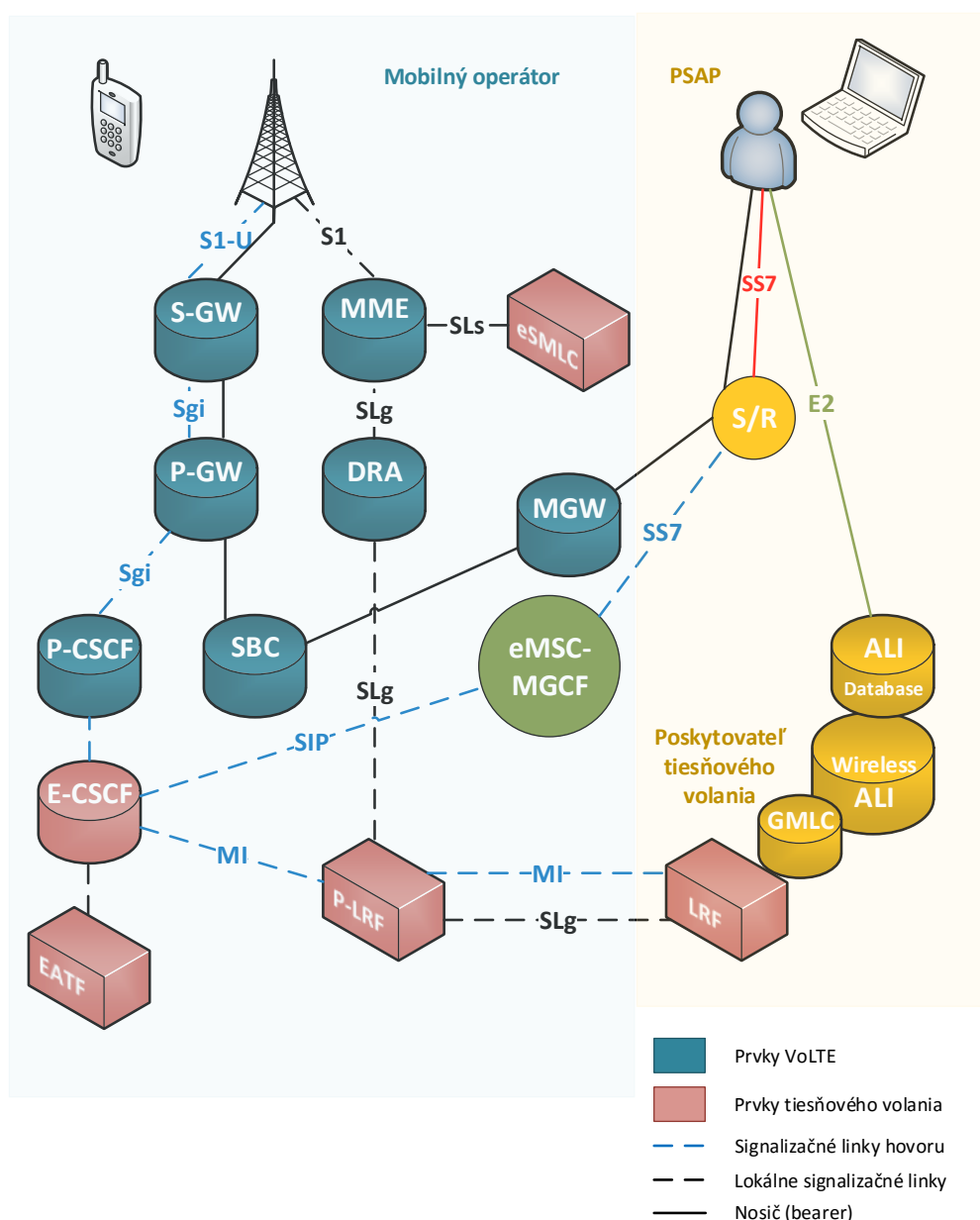
UTDOA lokalizuje mobilné zariadenia pomocou času, za ktorý sa dostane signál na viacero základňových staníc. Použitím rýchlosti šírenia rádiového signálu (rýchlosť svetla) je lokácia mobilného zariadenia odhadnutá na základe vzdialenosti zariadenia od každej základňovej stanice prijímajúcej jeho signál. Táto metóda sa využíva v systémoch GSM. V systéme UMTS je lokalizačný proces pre zariadenia nepodporujúce AGPS predaný sieti GSM.

2.2 Architektúra služby E911 v 4G

LTE (Long Term Evolution) je 4. generácia bezdrôtovej technológie, podporuje vyššie prenosové rýchlosti internetových aplikácií. Napríklad VoIP (Voice over IP - prenos hlasu cez protokol IP), mobilná televízia a mnoho ďalších. Obrázok 2.3 zobrazuje architektúru tiesňovej služby v sieťach 4G a nasledujúca sekcia sa bude venovať opisu jednotlivých prvkov.

Nasadenie LTE sa zvyčajne uskutočňuje v troch fázach, pričom každá fáza má iný dopad na službu tiesňového volania:

- Fáza 1: Zariadenia podporujúce iba prenos dát: Zariadenia podporujúce hlasové služby neboli podporované, a preto neboli potrebné žiadne zmeny v sieti služby tiesňového volania;



Obr. 2.3: Architektúra zapojenia tiesňovej služby

- Fáza 2: Táto fáza priniesla použitie hlasovej služby pomocou techniky prepnutia používateľa do siete 3G alebo 2G. S komerčným a tiesňovým hovorom je zachádzané rovnako, oba sú prepnuté do siete 3G alebo do siete 2G v prípade, že je sieť 3G nedostupná;
- Fáza 3: Tiež nazývaná ako VoLTE (Voice over LTE - prenos hlasu cez LTE), je posledným krokom v nasadení LTE. VoLTE umožňuje súčasné využívanie hlasovej a dátovej služby na plne integrovaných zariadeniach LTE. Implemen-

tácia VoLTE vyžaduje nasadenie nových prvkov aj nových rozhraní potrebných na prepojenie týchto prvkov ako zobrazuje obrázok 2.3.

Operátor PSAP

Operátor PSAP alebo agent prijíma tiesňový hovor a lokalizačné dáta.

Informácie o hovore sa zobrazia na počítači po prijatí hovoru. Agent si môže vyžiadať aktualizácie alebo opakovaný prenos druhej fázy lokalizačných informácií [14].

SR (Selective Router - výberový smerovač)

Výberový smerovač SR je smerovač s E911 smerovacou databázou, ktorá smeruje tiesňové hovory. Jeho úlohou je smerovať tiesňové hovory do správneho PSAP na základe ESRK (Emergency Services Routing Key - smerovací kľúč tiesňovej služby) prijatého od MSC.

eMSC (Enhanced Mobile Switching Center - vylepšený MSC)

Úlohy prvku eMSC sú prebraté z technológie UMTS, ale navyše navyše podporovať službu VoLTE. eMSC je zvyčajne spojené s prvkom MGCF (Media Gateway Control Function), ktorý riadi MGW (Media Gateway) a poveruje ho vytváraním cesty zmenou IP/RTP nosiča na TDM/SS7 nosič. Taktiež doručuje tiesňový hovor do SR.

E-CSCF (Emergency-Call Session Control Function - prvok riadenia tiesňového hovoru)

E-CSCF má tri hlavné úlohy potrebné na spracovanie tiesňového hovoru:

- Žiada smerovacie informácie od P-LRF;
- Priraduje SIP reláciu EATF;
- Smeruje hovor do PSAP na základe vrátenej hodnoty ESRK a preposiela tiesňové žiadosti cez BGCF. [2]

EATF (Emergency Access Transfer Function)

Hlavnou funkciou EATF je podporovať SRVCC handover (Single Radio Voice Call Continuity handover - zabezpečenie continuity hlasového hovoru) pre tiesňové hovory. Po prijatí tiesňovej žiadosti od E-CSCF, EATF pracuje ako back-to-back user agent relácie SIP.

P-LRF - (Proxy-Location Retrieval Function)

Jeho hlavnou úlohou je pracovať ako proxy server pre prvky GMLC rôznych poskytovateľov a poskytovať nasledujúce funkcie:

- Identifikovanie poskytovateľa GMLC;
- Poskytovanie rozhrania SLg pre lokalizáciu;
- Poskytovanie rozhrania Mi pre funkciu stanovenia smerovania;
- Informovanie GMLC v prípade SRVCC handoveru pre zbieranie koncových KPI dát používaných na výkonnostné monitorovanie.

P-CSCF (Proxy-Call Session Control Function)

P-CSCF je vstupný bod do IMS (IP Multimedia Subsystem - podsystém doručovania IP multimediálnych služieb) domény a slúži ako proxy server pre mobilné zariadenia. Mobilné zariadenie je priradené k špecifickému P-CSCF na základe IMS registrácie a inicializácie SIP (Session Initiation Protocol - protokol pre zahájenia relácie) relácie. Po prijatí tiesňového hovoru od PGW (PDN Gateway - brána do paketovej dátovej siete), P-CSCF identifikuje tento tiesňový hovor a vyšle tiesňovú INVITE požiadavku E-CSCF v rovnakej IMS doméne.[10]

SBC (Session Border Controller)

SBC je zariadenie alebo aplikácia, ktorá upravuje spôsob zahajovania, vykonávania a ukončovania hovorov VoIP. To znamená, že na SBC môžeme nastaviť a definovať kategórie aj priradovať priority pre tiesňové hovory, čo sa prevádza nastavením priority v hlavičke protokolu SIP. SBC je umiestnené na hraničnom bode s verejnou sieťou. [8][22]

PGW (PDN Gateway)

Pre službu E911, PGW poskytuje IP adresy špecificky pre tiesňové IMS relácie.

eNodeB (Evolved NodeB)

Po prijatí tiesňového hovoru od používateľa základňová stanica eNodeB zaháji procedúru tiesňového hovoru. Prenáša lokalizačné dáta medzi používateľom a eSMLC cez MME, udržiava všetky potrebné spojenia a signalizáciu, pokiaľ nie je tiesňový hovor ukončený.

eSMLC (Evolved Serving Mobile Location Center)

eSMLC je nový prvok, ktorý riadi celkovú koordináciu a plánovanie prostriedkov potrebných na výpočet približnej polohy mobilného zariadenia.

DRA (Diameter Routing Agent)

DRA uskutočňuje správu smerovania pre spojenia SLg a správu koncových relácií medzi MME i P-LRF. Tieto spojenia sú používané na podporu relácií pre SLR (Subscriber Location Report) a PSL (Provide Subscriber Location) potrebné pre službu tiesňového hovoru E911. [19]

2.3 Testovanie služby E911

V prvom rade pred samotným spustením služby E911 je potrebné sa uistiť o správnej funkcii celého smerovacieho systému, a to pre každý sieťový prvok eNodeB podporujúci práve túto službu. Testovanie sa prevádza pre každé frekvenčné pásmo, z čoho vyplýva, že v prípade už úspešne otestovaného eNodeB, ktorému bolo následne pridané nové LTE frekvenčné pásmo podporujúce taktiež službu E911, je potrebné toto testovanie vykonať znovu.

Na samotné testovanie služby tiesňového hovoru je potrebný technik, ktorý sa nachádza v dosahu testovaného eNodeB a inžinier so vzdialeným prístupom na potrebné eNodeB, ktorí potrebujú navzájom komunikovať v reálnom čase na prípadné riešenie nadbytočných problémov. Postup testovania spolu s bežnými problémami budú opísané v tejto kapitole.

Testovanie môžeme rozdeliť do troch fáz:

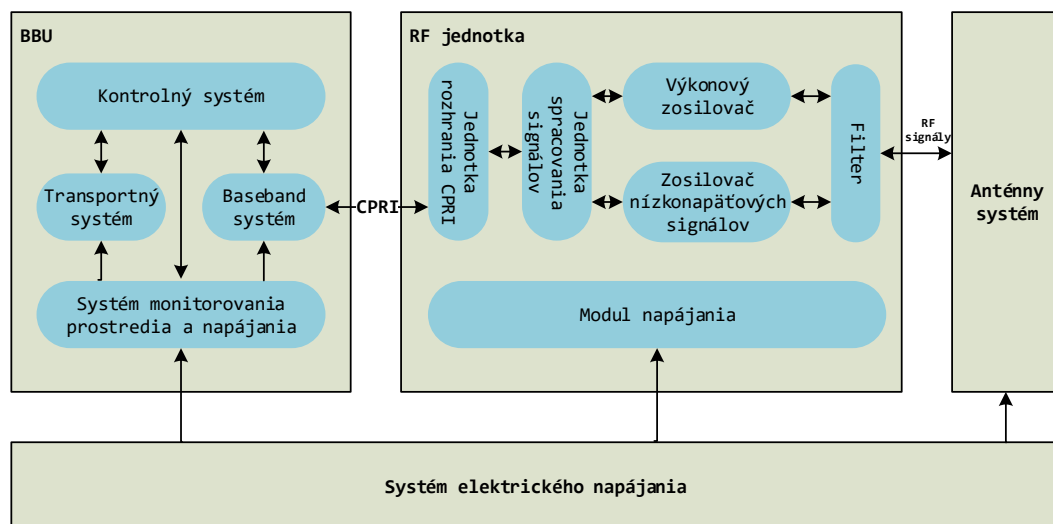
- Kontrola zariadenia pred samotným testovaním;
- Príprava zariadenia do požadovaného stavu na testovanie;
- Uvedenie zariadenia do počiatočného stavu a vykonanie kontroly zariadenia po testovaní.

Nasledujúce úkony sú opísané zo strany inžiniera vykonávajúceho prípravu zariadenia na testovanie.

2.3.1 Kontrola základňovej stanice

Samotné testovanie začína po prijatí hovoru, kedy technik oznámi prvky a sektory potrebné pripraviť na testovanie služby E911. Všetky úkony vykonávané na prvkoch eNodeB sa uskutočňujú pri ich plnom nasadení v sieti. V prvom rade je potrebné overiť, či sa požadované sektory nachádzajú na jednom eNodeB alebo sú rozdelené na viaceré kabinety.

Pod pojmom kabinet si môžeme predstaviť jadro prvku základňovej stanice, ktoré spracováva signály. Kabinet tvorí BBU (Baseband unit - jednotka spracovania frekvenčného pásma v telekomunikačných systémoch), zodpovedná za komunikáciu cez fyzické rozhranie eNodeB a RF Unit (Radio frequency unit - RFU/RRU¹ - jednotka spracovania komunikácií medzi UE a sieťou) zodpovedná za bezdrôtovú komunikáciu medzi UE a sieťou LTE, UMTS či GSM. BBU a RRU sú prepojené rozhraním CPRI realizované optickým spojom.



Obr. 2.4: Náhľad prvkov základňovej stanice

Základňové stanice pracujúce v samostatnom a viacnásobnom režime môžeme klasifikovať podľa poskytovaných služieb ako:

- Základňová stanica v samostatnom režime poskytuje služby len pre jeden mobilný systém GSM, UMTS alebo LTE;
- Základňová stanica vo viacnásobnom režime poskytuje služby pre viaceré mobilné systémy:
 - Režim dvoch mobilných systémov môže pracovať s GSM a UMTS, GSM a LTE alebo UMTS a LTE systémami;
 - Režim troch mobilných systémov, kedy základňová stanica poskytuje služby pre všetky tri systémy súčasne.

Prvky, z ktorých pozostáva základňová stanica, môžeme vidieť na obrázku 2.4. V prípade menej obývaných oblastí sa stretávame so základňovými stanicami pracujúcimi v samostatnom režime, a teda všetky sektory pracujúce v danom frekvenčnom pásme využívajú práve jednu BBU. V prípade husto zaľudnených oblastí sa využívajú eNodeB s viacerými kabinetmi. V tomto prípade má každý kabinet jedinečnú

¹môže byť pre každý kabinet samostatná, ale väčšinou ju zdieľa niekoľko základňových staníc

IP adresu a je potrebné každý kabinet nastaviť a pripraviť na testovanie zvlášť. Toto riešenie sa využíva hlavne kvôli veľkému zatažovaniu daných sektorov s možným zahltením fronty. Z tohto dôvodu sa stretávame s riešením použitia dvoch alebo troch kabinetov, pričom každý kabinet spracováva dáta len z jedného alebo dvoch sektorov.

Po zistení počtu kabinetov už môžeme pristúpiť ku kontrole jednotlivých kabinetov, resp. základňových staníc eNodeB. Po pripojení sa na server spravujúci žiadané eNodeB si najprv zobrazíme aktívne alarmy na zariadení. Alarmy sú podľa svojej dôležitosti rozdelené na alarmy menšie, väčšie (hlavné) a kritické. V tomto kroku by sme nemali na žiadanom frekvenčnom pásme (sektore) vidieť žiadny alarm. V prípade, že sa na žiadanom sektore budú nachádzať alarmy ovplyvňujúce funkčnosť samotného sektoru, sme nútení celý proces predčasne ukončiť a informovať technika o nájdených alarmoch.

Alarmy ovplyvňujúce funkčnosť sektorov môžu vyzeráť nasledovne:

2016-02-09 16:33:45 M Service Degraded EUtranCellFDDILL00948_3A_1

2016/03/17 02:18:07 355 CDT	IAL03544	ENBEquipment	eNBEquip	ENBEquipmentDegradedOrFaulty	equipmentAlarm	equipmentMalfunction
2016/03/17 00:54:09 642 CDT	IAL03544	Cell	cell-IAL03544_3B_1	LTECellDown	equipmentAlarm	equipmentMalfunction
2016/03/17 00:54:09 626 CDT	IAL03544	Cell	cell-IAL03544_3C_1	LTECellDown	equipmentAlarm	equipmentMalfunction
2016/03/17 00:54:09 626 CDT	IAL03544	Cell	cell-IAL03544_3A_1	LTECellDown	equipmentAlarm	equipmentMalfunction
2016/03/16 20:19:41 623 CDT	IAL03544	NetworkElement	IAL03544	BootableConfigBackupFailed	configurationAlarm	fileTransferFailure

Obr. 2.5: Príklad alarmov na zariadení Alcatel

V prvom výpise môžeme vidieť z ľava, dátum a čas vzniknutého alarmu, nasleduje skratka závažnosti alarmu. Skratka *M* vyjadruje závažný alarm (z anglického slova *major*), stretnúť sa ešte môžeme s *C* ako kritický alarm a *m* ako menší alarm (z anglického slova *minor*). Nasleduje názov sektoru, na ktorom vznikol daný alarm a z ktorého je možné zistiť aj frekvenčné pásmo. Tento typ výpisu poskytujú zariadenia Ericsson, kde skratka *3A* znamená frekvenčné pásmo 2300 MHz a sektor Alfa. Stretnúť sa môžeme aj s LTE frekvenčnými pásmami 2100 MHz so skratkou *2*, 1900 MHz so skratkou *9*, 850 MHz so skratkou *8* a pásmom 700 MHz so skratkou *7*. Väčšina operátorov využíva systém s tromi sektormi na bunku, teda sektory Alfa, Beta a Gamma. Ojedinele sa môžeme stretnúť so systémom šiestich antén na bunku, ktorý síce poskytuje dvojnásobné zväčšenie kapacity bunky, ale prináša aj zvýšené prekrývanie sa susedných sektorov. To činí až 60°, v porovnaní so systémom troch antén to je 40°. Preto sa systémy so šiestimi anténami využívajú iba na miestach s veľmi vysokým vyťažením sektorov.[16]

Na druhom obrázku 2.5 môžeme vidieť z ľava taktiež dátum a čas vzniknutého alarmu, nasleduje identifikátor základňovej stanice a objekt, na ktorom vznikol

alarm. Následne môžeme vidieť názov objektu, v našom prípade vidíme názvy sektorov. Nakoniec nasleduje názov alarmu, typ alarmu a pravdepodobná príčina alarmu.

V prípade, že sa na sektoroch nenachádza žiadny alarm, pokračujeme s výpisom aktuálneho stavu sektorov. Nové základňové stanice, sektory žiadané technikom by mali byť zablokované, pretože musia byť najskôr otestované a až následne uvedené do prevádzky. Už nasadené základňové stanice môžu mať sektory odblokované, takýmto sektorom hovoríme živé. Spracúvajú používateľské dáta a je potrebné overiť, či sú sektory nastavené na stav Barred¹. Len v tomto prípade môžeme ukončiť testovanie, pretože základňová stanica sa nachádza v stave, kedy je technik schopný pripojiť sa na potrebné sektory.

Názorná ukážka možných stavov sektorov na zariadení Ericsson:

- Novo pridané neotestované frekvenčné pásmo

```

=====
administrativeState cellBarred operationalState PlmnReserved
=====
1 (LOCKED)          1 (BARRED) 0 (DISABLED)    true
1 (LOCKED)          1 (BARRED) 0 (DISABLED)    true
1 (LOCKED)          1 (BARRED) 0 (DISABLED)    true
=====

```

- Živé frekvenčné pásmo

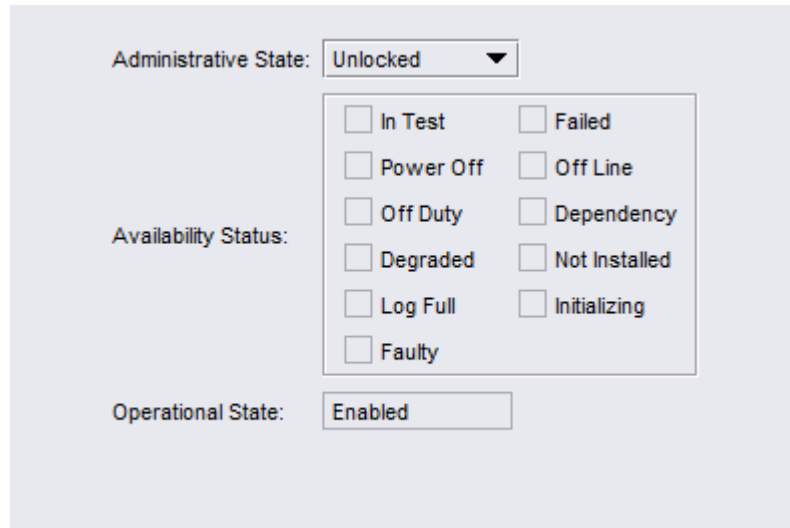
```

=====
administrativeState cellBarred      operationalState PlmnReserved
=====
1 (UNLOCKED)        1 (NOT_BARRED) 0 (ENABLED)     false
1 (UNLOCKED)        1 (NOT_BARRED) 0 (ENABLED)     false
1 (UNLOCKED)        1 (NOT_BARRED) 0 (ENABLED)     false
=====

```

Na otestovanie potrebného sektora technik potrebuje poznať jeho identifikátor. Ak mu tento identifikátor nebol zdelaný jeho nadriadeným pracovníkom, vyžiada si spolu s potvrdením o pripravenosti eNodeB aj takzvané PCI (Physical-layer Cell Identifier - fyzický identifikátor bunky). V ďalšom kroku je potrebné si overiť, či nebude zariadenie eNodeB v najbližšej dobe vykonávať vlastnú kontrolu, ktorá by mohla negatívne ovplyvniť výsledok testovania. Po zistení, že sa v čase testovania bude vykonávať vlastná kontrola, musíme technika o tejto kontrole informovať a testovanie dočasne odložiť. Nasledujúci krok je veľmi dôležitý, pretože musíme overiť, či budeme schopní vytvoriť zálohu zariadenia pred uskutočnením zmien na samotnom

¹je stav, v ktorom sa dokáže pripojiť iba používateľ so špeciálnou (barred) SIM kartou



Obr. 2.6: Náhľad na živé frekvenčné pásmo základňovej stanice Alcatel-Lucent

zariadení pre možnosť opätovného vrátenia do pôvodného stavu po spôsobení kritickej chyby. V prípade zariadenia Ericsson je maximálny možný počet záloh nastavený na hodnotu 51. V dôsledku tejto skutočnosti ak zistíme, že sa na zariadení nachádza už daný počet záloh, musíme pred vytvorením novej zálohy vymazať práve tú najstaršiu. Po vykonaní základnej kontroly zariadenia môžeme pristúpiť k vytvoreniu zálohy, ktorú tiež nastavíme ako primárnu, aby pri nútenom alebo samovoľnom reštartovaní základňovej stanice sa zariadenie spustilo s aktuálnymi nastaveniami.

2.3.2 Príprava základňovej stanice na testovanie

Po vytvorení zálohy môžeme pristúpiť k uskutočneniu potrebných zmien na testovanie. Na začiatku prípravy základňovej stanice by sme mali uviesť potrebné sektory do stavu *reserved*, rezervovať ich pre testovanie. Význam tohto stavu je zväčša informatívny, oznamuje ostatným inžinierom pracujúcim na danom eNodeB že sa na rezervovaných sektoroch vykonáva diagnostický zásah a nemali by meniť ich stav. Tento krok nie je súčasťou bežnej procedúry avšak bez nastavenia rezervovanosti zariadenia vznikajú na stanicach konflikty, kedy v jednom čase pracujú na základňovej stanici viacerí inžinieri a navzájom menia stav sektorov alebo ovplyvňujú testovanie zmenou iného parametra. Po rezervovaní sektorov ich musíme uviesť do stavu *barred*. Sektor v stave *barred* neumožňuje používateľom pripojiť sa. Pripojí sa iba technik, ktorý využíva špeciálnu tzv. *barrovanú* sim kartu. Po nastavení sektoru do stavu *barred* môžeme uskutočniť poslednú zmenu. Odblokovať sektor, čím ho uvedieme do stavu, v ktorom začne vysielat signál. Je dôležité, aby sme odblokovanie sektora uskutočnili až ako posledný krok. V opačnom prípade by mohlo dojsť k situácii, kedy

sa na ešte nepripravený sektor pripoja používatelia. Tí následne môžu uskutočniť tiesňový hovor ktorý by mohol byť neúspešný a mohlo by dôjsť k strate na životoch. Taktiež by mohli uskutočniť hovor v čase, kedy by bol sektor nastavený do stavu *barred*, a tým pádom by používateľov okamžite odpojilo zo siete. Po dokončení prípravy základňovej stanice na testovanie by sa zariadenie malo nachádzať v nasledujúcom stave:

=====			
administrativeState	cellBarred	operationalState	PlmnReserved
=====			
1 (UNLOCKED)	1 (BARRED)	0 (ENABLED)	true

Lenže vo väčšine prípadov technik nie je schopný sa pripojiť na dané sektory. Po konzultácii s technikom nasleduje zistenie, že technik nepoužíva špeciálnu sim kartu a teda sa nemôže pripojiť na barrované sektory. Jediná možnosť, ako môže technik otestovať sektory, je uviesť ich do stavu *not_barred*. Toto riešenie však prináša ďalší problém. Na odomknuté sektory, ktoré sú v režime *not_barred* sa môžu pripojiť všetci používatelia, nie iba technik. Po dokončení testovania je potrebné uviesť zariadenie do pôvodného stavu, v akom sme ho našli. V prípade *not_barred* sektorov sú na bunku pripojení aj iní používatelia, ako ukazuje ľavá strana nasledujúceho výpisu. Tých po uzamknutí sektorov odpojí a preruší všetku ich komunikáciu, či už uskutočňovali hovor alebo využívali iné služby. Na pravej strane výpisu môžeme vidieť žiadaný počet pripojených používateľov, inak povedané, aby nebol žiadny používateľ pripojený na eNodeB počas testovania.

SectorId	#UE:s	#Bearers	SectorId	#UE:s	#Bearers
ILL00948_3A	3	8	ILL00948_3A	0	0
ILL00948_3B	7	13	ILL00948_3B	0	0
ILL00948_3C	7	13	ILL00948_3C	0	0
ILL00948_2A	17	28	ILL00948_2A	17	28
ILL00948_2B	18	36	ILL00948_2B	18	36
ILL00948_2C	18	31	ILL00948_2C	18	31

Opísanou úpravou vznikajú neúspešné relácie, ktoré negatívne vplývajú na koncových používateľov. Ako riešenie tohto problému by sme mohli použiť namiesto tzv. tvrdého vypínania sektorov (hard block) vypínanie jemné (soft block). Princíp jemného vypínania spočíva v tom, že sektor postupne znižuje svoj vysielač výkon, UE vyhodnotí signál zo susednej bunky ako lepší a uskutoční handover. V ostatných situáciách, kedy technik nie je schopný sa pripojiť na sektory je na príčine nedostatočný vysielač výkon bunky. Ten je zväčša nastavený na 7% výkonu. Na takúto stanicu sa nie je možné pripojiť, a to ani v prípade, že sa bude technik nachádzať priamo pri nej. Riešením je zvýšenie výkonu na čas potrebný pre otestovanie sektorov.

2.3.3 Obnovenie pôvodných nastavení základňovej stanice

Po dokončení testovania uvedieme zariadenie do počiatočného stavu. Ako prvé zablokujeme odblokované sektory a až následne ich vrátime do stavu `not_barred`. V prípade opačného postupu by znova nastala situácia, kedy by sa na sektory pripojili používatelia. Ich relácie by boli zrušené v momente zablokovania sektorov. Následne skontrolujeme alarmy na zariadení. Výskyt nového alarmu musíme eskalovať ako problém špeciálnemu tímu ktorý, sa zaoberá riešením alarmov na danom type zariadenia. V poslednom kroku vytvoríme zálohu po otestovaní a nastavíme ju znova ako primárnu, pretože zariadenie funguje správne a budúcim výpadkom sa zariadenie obnoví s aktuálnymi nastaveniami.

Jedným z častých problémov je zablokovanie testovaných sektorov iným inžinierom. Tento problém sa vyskytuje, pretože základňové stanice, na ktorých prebieha testovanie nie sú označené. Riešením by mohlo byť vyššie zmienené nastavenie sektoru do stavu *reserved*. Každý inžinier by si mal pred uskutočnením zmien na zariadení overiť tento stav, a v prípade už spomínaného rezervovaného stavu nevykonávať žiadnu akciu na zariadení, prípadne kontaktovať inžiniera, ktorý uviedol zariadenie do tohto stavu a informovať sa, aké zmeny vykonáva na zariadení. Zistenie identity používateľa, ktorý uskutočňoval príkazy na zariadení vykonáme zobrazením histórie použitých príkazov. Pri každom príkaze sa nachádza identifikátor používateľa. Z tohto dôvodu má každý používateľ jedinečný identifikátor, podľa ktorého vieme dodatočne zistiť, ktorý používateľ zadal konkrétny príkaz. História príkazov sa v zariadeniach výrobcov Ericsson a Alcatel-Lucent ukladá po dobu jedného mesiaca. Táto doba sa však dá meniť a rozhoduje o nej iba vlastník zariadenia.

Otestovaním základňovej stanice sme zistili či služba E911 pracuje správne tým spôsobom, že sa technik dovoľá do najbližšieho centra verejnej záchranej služby. Samotný hovor prebieha ako tiesňový hovor. Technik na začiatku oznámi operátorovi, že sa jedná o testovací hovor a opýta sa na miesto, na ktoré sa dovoľal. Po uskutočnení hovoru technik prijme e-mail obsahujúci údaje o hovore. V prípade neúspešného hovoru sa musí táto skutočnosť oznámiť tímu zodpovednému za riešenie daných problémov. Po odstránení problému sa základňová stanica znova otestuje. Samotná služba E911 je veľmi dôležitou súčasťou mobilných sietí. Je to služba zachraňujúca životy a preto sektory, ktoré ešte neboli otestované nemusia pracovať správne a nemôžu byť uvedené do prevádzky.

3 RÁDIOVÉ TECHNOLOGIE A ICH RUŠENIE

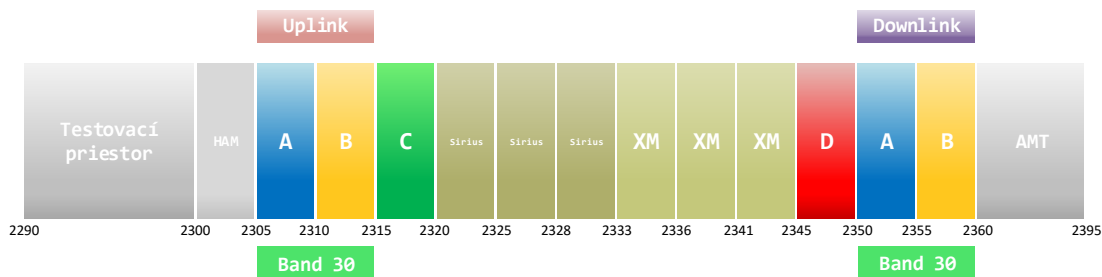
Mobilní operátori si zakupujú nové frekvenčné spektrá pre uspokojenie zvyšujúcej sa potreby kapacity a následne možnosti nasadenia súčasnej technológie LTE na nových frekvenčných pásmach bez zrušenia ostatných poskytovaných služieb a technológií. Výhodou rozšírenia frekvenčného spektra je tiež použitie dvoch, troch, štyroch alebo piatich nosičov konfigurovaných na poskytovanie zlepšených rýchlostí agregovaných nosičov.

Agregácia nosičov sa používa pre zväčšenie kapacity a zvýšenie dátového toku pre používateľa. Agregácia sa môže použiť v prípade frekvenčného oddelenia kanálov FDD (Frequency-Division Duplex) a v prípade časového oddelenia TDD (Time-Division Duplex). Agregovaných môže byť maximálne päť nosičov, keďže maximálna kapacita spomínaných nosičov je 100 MHz a každý nosič môže disponovať maximálne 20 MHz. Podrobnejšie informácie si môžete prečítať na stránkach 3GPP [1].

V ďalšej sekcii sa zameriame na konkrétny problém rušenia rádiových technológií Sirius XM¹ a AMT (Aeronautical Mobile Telemetry - letecká mobilná telemetria) so spektrom WCS (Wireless Communication Service - bezdrôtová komunikačná služba), ktoré bolo spočiatku používané pre iný účel. Susedné frekvenčné spektrá neboli pripravené na poskytovanie novej mobilnej služby v pásme WCS a dôsledkom toho je rušenie susedných frekvenčných spektier Sirius XM a AMT spektrom WCS.

WCS spektrum sa skladá zo štyroch kanálov, z čoho dva sú uvoľnené pre použitie mobilných hlasových a dátových služieb. Ako môžete vidieť na obrázku, jedná sa o kanály A a B vo frekvenčných pásmach 2305 - 2015 MHz v smere Uplink a 2350 - 2360 MHz v smere downlink, pásma tiež známe ako Band 30 (B30).

Ako je ilustrované na obrázku 3.1, vysielacie WCS v aktívnom režime môžu generovať rušenie, pri prenose dát v smere downlink, ktoré ovplyvňuje AMT v hornej hranici spektra a Sirius XM v dolnej hladine spektra WCS.



Obr. 3.1: Frekvenčný náhľad WCS a jeho susedných spektier [12]

¹je satelitné rádio v Spojených štátoch amerických

Toto rušenie by mohlo negatívne ovplyvniť meranie AMT ovplyvňujúce civilné a vojenské testovanie lietadiel a ich prevádzku. Rušenie prijímačov satelitného rádia Sirius XM, obzvlášť starších jednotiek XM sa prejaví ako stlmenie zvuku, ku ktorému dôjde v tesnej blízkosti WCS-B30 vysielaču aj napriek 5 MHz kanálu D medzi spektrami WCS a Sirius XM.

WCS vysielače môžu taktiež vytvárať určitú hladinu rušenia pri prenose dát v smere uplink. Toto rušenie sa vytvára najmä pri starších jednotkách typu Sirius. Môže byť zaznamenané, keď používateľ WCS vysiela vedľa antény Sirius XM (bližšie ako 10 cm) alebo keď sa používateľ WCS nachádza na okraji bunky, vysiela pri plnom výkone 23 dBm a zároveň sa nachádza pri anténe Sirius XM (bližšie ako 1 m). Tieto scenáre však nie sú v praxi veľmi pravdepodobné. Ak by sa používateľ nachádzal na mieste s extrémne nízkym RSRP, zariadenie by sa pripojilo pomocou IntraFrekvenčného¹ alebo InterFrekvenčného handoveru² na lepšiu obsluhujúcu bunku.

RSRP (Reference Signal Received Power - sila prijímaného signálu) je priemer prichádzajúcich signálov cez celú šírku pásma kanálu, ktorý poskytuje informáciu o sile signálu. Používateľ musí pravidelne merať silu signálu aktuálnej bunky, na ktorú je pripojený a taktiež silu signálu buniek susediacich, aby si udržal konštantnú kvalitu signálu. Pre túto skutočnosť sa meria parameter RSRP. Na základe tohto parametra sa následne vypočíta RSRQ (Reference Signal Received Quality - kvalita prijímaného signálu) [4].

3.1 Odstránenie rušenia rádiových technológií

Na odstránení rušenia spektra WCS so satelitným rádiom Sirius XM pracuje technik, ktorý sa fyzicky nachádza pri samotnej základňovej stanici eNodeB a zisťuje rušenia rádia Sirius XM. Súčasne sa spolupracujúci inžinier vzdialene pripája na eNodeB a nastavuje požadované hodnoty. Diagram celého úkonu je zobrazený na obrázku 3.2.

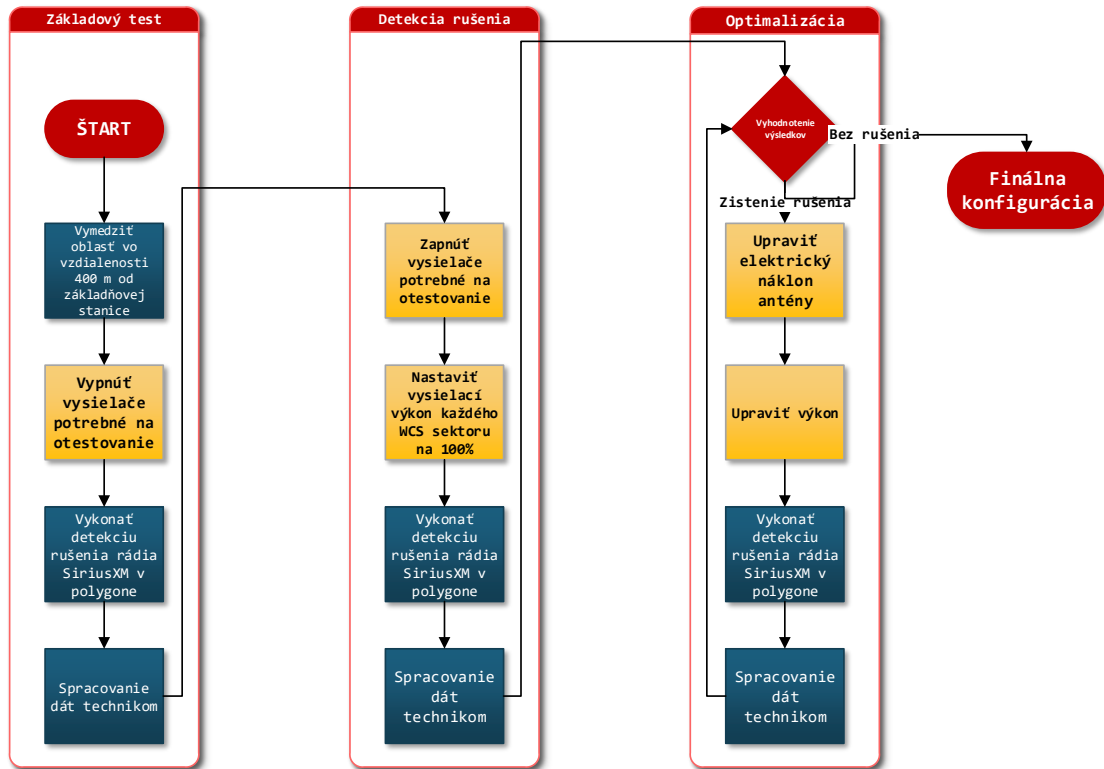
Celý úkon je rozdelený na 7 krokov. Pri každom kroku je potrebné, aby technik komunikoval s inžinierom v reálnom čase kvôli riešeniu nadbytočných problémov.

KROK 1

Na začiatku celého úkonu spolupracujúci technik oznámi inžinierovi identifikátory základňových staníc, s ktorými sa bude pracovať. Inžinier si musí následne overiť v tzv. CIQ (databáza základňových staníc, na ktorých je povolené pracovať), či

¹je typ handoveru, pri ktorom používateľ naďalej využíva rovnaký LTE kanál, zmení iba obsluhujúce eNodeB.

²je typ handoveru, kedy používateľ mení obsluhujúce eNodeB aj používaný LTE kanál.



Obr. 3.2: Diagram odstránenia rušenia rádia Sirius XM spektrom WCS

sa v ňom nachádza žiadaná stanica. Často nastáva situácia, kedy technik oznámi inžinierovi ID stanice, ktorá neobsahuje všetky sektory na testovanie. V tom prípade musí inžinier vyhľadať druhý kabinet stanice, na ktorom sa nachádza potrebný sektor. Toto dohľadávanie sa musí vykonávať z dôvodu testovania všetkých sektorov súčasne. Pri zisťovaní rušenia musí technik dookola obísť základňovú stanicu vo vzdialenosti 400 m, čo je vzdialenosť stanovená FCC.

Po pripojení na základňovú stanicu najskôr skontrolujeme, či sa na testovaných sektoroch nenachádzajú alarmy, ktoré by neumožnili odblokovanie sektorov a im príslušných objektov, o ktorých sa môžete dočítať nižšie v práci. V nasledujúcom výpise môžete vidieť príklad alarmu ovplyvňujúceho funkčnosť sektoru.

M ResourceConfigurationFailure ARL02645-3C (Required resource disabled)

V prípade čo i len jedného alarmu na jednom zo žiadaných sektorov musíme o tejto skutočnosti informovať technika a testovanie odložiť, pretože ako už bolo vyššie spomenuté, technik testuje rušenie na všetkých sektoroch zároveň. To znamená, že sektor, ktorý je momentálne odstavený by mohol po odstránení alarmu a uvedenia sektoru do funkčného stavu rušiť satelitné rádio Sirius XM naďalej. V prípade žiadneho alarmu alebo len alarmu neovplyvňujúceho funkčnosť žiadaného sektoru si následne vytvoríme zálohu (podobne ako pri projekte testovania tiesňovej

služby E911), aby sme v prípade nastávajúceho problému vedeli vrátiť základňovú stanicu do pôvodného stavu. Cieľom prvého kroku je zablokovanie sektorov pracujúcich v spektre WCS a objektov tzv. SectorEquipmentFunction, aby mohol technik overiť správne fungovanie samotného satelitného rádia Sirius XM.

SectorEquipmentFunction je manažovateľný objekt, ktorý reprezentuje skupinu buniek vo vnútri jedného geografického územia, so spoločnými funkciami vzťahujúcimi sa k objektom AntennaFunction, TMA Function (Tower Mounted Amplifier - vežový zosilovač) a podporujúcim zariadeniam ako napr. výkonový zosilovač. Objekt SectorEquipmentFunction teda reprezentuje skupinu zariadení, ktoré môžu byť bunkou používané. Jeden sektor môže mať iba jeden objekt SectorEquipmentFunction. AntennaFunction je manažovateľný objekt, ktorý predstavuje rad vysielačích elementov, ktoré môžu byť naklonené pre úpravu rádiových frekvencií pokrývajúcej bunku. Viac informácií sa môžete dočítať tu [18].

Pred samotným zablokovaním sektorov musíme v prvom rade skontrolovať počiatočný stav WCS sektorov. WCS sektory by mali byť odblokované, no využívať by mali iba hodnotu pod 10% z celkového vysielačieho výkonu. To v praxi znamená, že žiadny používateľ sa na sektory nepripojí ani z tesnej blízkosti samotnej základňovej stanice. Avšak občas nastane situácia, kedy sa WCS sektory nachádzajú v zablokovanom stave už pred prvým krokom. V tomto prípade vytvoríme poznámku o danej skutočnosti, aby inžinier vykonávajúci posledný krok nastavil základňovú stanicu do pôvodného stavu. Ak sú všetky vyššie uvedené požiadavky splnené, pristúpime k samotnému zablokovaniu sektorov a objektov SectorEquipmentFunction korešpondujúce s danými sektormi. Samotné blokovanie sektorov v tomto projekte na rozdiel od projektu tiesňového volania uskutočňujeme pomocou jemného blokovania sektorov. Po zablokovaní sektorov technik nie je schopný pripojiť sa na základňovú stanicu. Tým môžeme overiť správne fungovanie WCS sektorov a tiež skutočnosť, či rádio Sirius XM nie je rušené inou technológiou alebo inou príčinou než vysielačím sektorom v spektre WCS. Po zablokovaní by mala byť základňová stanica v nasledujúcom režime.

administrativeState	operationalState	MO
1 (LOCKED)	0 (DISABLED)	EUtranCellFDD-ARL02645-3A
1 (LOCKED)	0 (DISABLED)	EUtranCellFDD-ARL02645-3B
1 (LOCKED)	0 (DISABLED)	EUtranCellFDD-ARL02645-3C
1 (LOCKED)	0 (DISABLED)	SectorEquipmentFunction=6
1 (LOCKED)	0 (DISABLED)	SectorEquipmentFunction=7
1 (LOCKED)	0 (DISABLED)	SectorEquipmentFunction=8

Pokiaľ technik overí vyššie uvedené skutočnosti, pripravíme základňovú stanicu na ďalší krok. Keďže v ďalšom kroku, kroku č. 2, technik potrebuje otestovať rušenie rádia WCS sektormi. K tomu potrebuje aspoň 80 % vyťaženie týchto sektorov, preto potrebujeme na základňovej stanici definovať nový profil. Nutnosť definovania nového profilu je však iba pri zariadeniach Ericsson.

```
crn ENodeBFunction=1,AirIfLoadProfile=4
ailgChangePeriod 1
ailgHighPrio 2
ailgLoadType 2
ailgLowPrioModType 0
dlPrbLoadLevel 100
minLoadLevelPdcch 100
```

Tento profil môžeme vnímať ako predlohu nastavení pre sektory, ktorý využíva generátor dát implementovaný v softvéri základňových staníc. Generátor vytvorí potrebné zaťaženie sektorov na ich otestovanie. Vo vyššie zmienenom výpise môžeme vidieť najdôležitejšiu časť skriptu, v ktorej definujeme potrebné parametre profilu. Prvý riadok označuje názov profilu, príkazom *ailgChangePeriod 1* nastavujeme vzor periodickej zmeny pre generovanie umelej záťaže na 1 ms. Táto perióda sa aplikuje na oba PDSCH (Physical Downlink Shared Channel – zdielaný downlink kanál) a PDCCH (Physical Downlink Control Channel - riadiaci downlink kanál) umelo zaťažené kanály. Príkazom *ailgHighPrio* nastavujeme metódu použitú na generovanie umelej záťaže s vysokou prioritou. V tomto prípade nastavujeme hodnotu 2, teda nepoužívame záťaž s vysokou prioritou. Príkazom *ailgLoadType* nastavujeme typ záťaže, ktorá sa bude generovať. S použitím hodnoty 2 nastavujeme záťaž kanálu PDSCH bez priestorového filtrovania¹ (beamforming) a záťaž PDCCH kanálu. Príkazom *dlPrbLoadLevel* nastavujeme minimálnu úroveň zaťaženia sektoru spojenú

¹je v zjednodušenom význame smerovanie rádiových signálov špecifickým smerom

²je alokovaný špecifický počet subnosičov pre používateľa na vopred stanovený čas

s použitím jedného bloku downlink PRB² (Physical Resource Block - fyzický zdrojový blok). Nami nastavená hodnota je 100%. To znamená, že v prípade záťaže s vyššou prioritou než je priorita stanovená príkazom *algHighPrio* (záťaž generovaná pripojeným používateľom) nedosahuje 100% zataženie bloku PRB, bude tento blok doplnený vygenerovanou záťažou s nižšou prioritou aby splnil nastavenú hodnotu vyťaženia. Príkazom *minLoadLevelPdcch* nastavujeme minimálnu úroveň zataženia dostupných CCE (Control Channel Elements - riadiace prvky kanálu) kanálu PDCCH. Ak je zataženie kanálu PDCCH od používateľa pod úrovňou 100%, zataženie s nižšou prioritou bude vygenerované pre dosiahnutie nami stanovenej úrovne využitia.

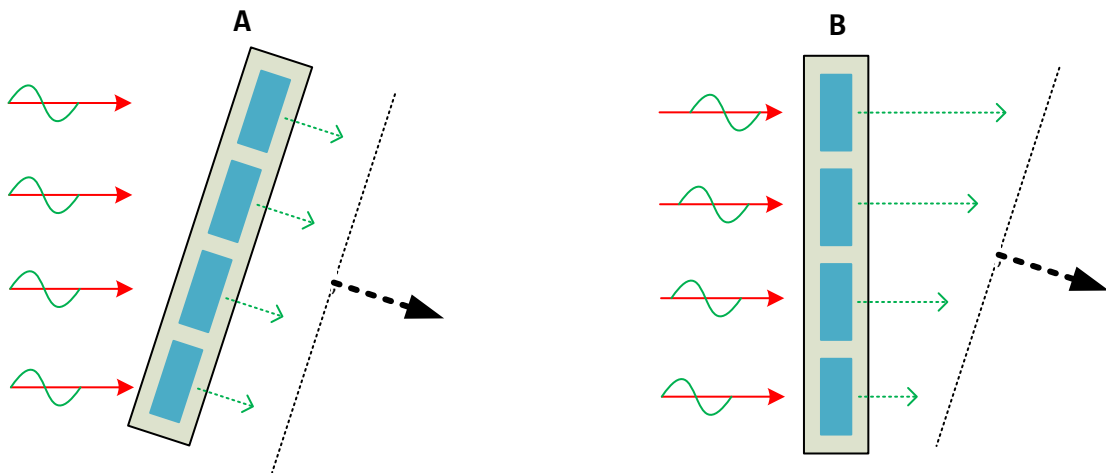
Po nadefinovaní profilu je ešte potrebné ho priradiť k žiadaným sektorom. Nakoniec prvého kroku je potrebné aktivovať vyššie zmienený generátor.

KROK 2

Po otestovaní správnej funkčnosti samotného satelitného rádia Sirius XM (aj po vylúčení možnosti rušenia inou príčinou než sú sektory WCS) si technik vyžiada nasledujúci krok. Krok č. 2 slúži na nastavenie prvotných parametrov, ktoré sú inžinierovi poskytnuté prostredníctvom vytvorených tiketov. Každá testovaná základňová stanica musí mať vytvorený tiket. Pokiaľ tento tiket vytvorený nie je, inžinier nemôže na danej základňovej stanici pracovať a testovanie musí byť odložené. Keďže samotné testovanie trvá určitú dobu, tak je veľmi pravdepodobné, že na nasledujúcom kroku bude pracovať iný inžinier z rovnakého tímu. Preto je potrebné si ešte pred začatím nastavovania samotných parametrov overiť, či sa na zariadení nachádza vytvorená záloha z kroku č. 1. Z tohto dôvodu je nutné používať rozumné názvy a popisy všetkých úkonov. Ďalším dôležitým úkonom je overenie stavu WCS sektorov, ktoré by mali byť zablokované. V prípade odblokovaného stavu sektorov je nutné ihneď ukončiť testovanie a informovať technika o skutočnosti, že iný inžinier práve pracuje na danom zariadení, a preto nemôže byť otestované. Narážame tak na rovnaký problém ako v prípade projektu testovania núdzovej služby E911. V prípade sektorov WCS v blokovanom stave môžeme pristúpiť k samotnému nastavovaniu parametrov. Vykonáva sa zmena troch parametrov: maximálny výstupný výkon, vysielačový výkon a natočenie vysielačovej antény. Maximálny výstupný výkon sa nastavuje iba v kroku č. 2 pre každý sektor osobitne. Hodnota je nastaviteľná v rozsahu 0 až 250000 mW pre zariadenia Ericsson. Hodnota vysielačového výkonu je nastaviteľná v rozsahu 10 až 100 % pre zariadenia Ericsson a určuje, aká časť vysielačového výkonu bude alokovaná pre daný sektor. Z toho faktu vyplýva, že sa bude hodnota nastavovať pre každý sektor osobitne. Posledným parametrom je elektrické natočenie vysielačovej antény, ktoré je nastaviteľné v prípade zariadenia Ericsson

v rozsahu -900 až 900. Jedná sa o elektricky kontrolované natočenie lúčov antény v jednotkách 0.1°.

V prípade elektrického natočenia antény sa modifikácia výsledného natočenia vytvára zmenou charakteristík signálových fází každého prvku antény (ako môžete vidieť na obrázku 3.3), ktorý znázorňuje rozdiel medzi mechanickým a elektrickým natočením antény.



Obr. 3.3: A: mechanické natočenie antény, B: elektrické natočenie antény

Elektrické natočenie môže mať fixnú hodnotu alebo sa môže rôzne meniť. Táto zmena môže byť prevedená buď manuálne na mieste alebo vzdialene. V druhom prípade sú antény označované ako RET (Remote Electrical Tilt - antény so vzdialeným elektrickým natočením). Obvykle sa využíva malý motor pripojený k regulátorom, ktoré vykonávajú prácu nastavenia náklonu antény [21].

Po vykonaní týchto zmien si skontrolujeme nastavenia z vytvoreného profilu, pretože môže nastať situácia, kedy už tento profil je na základňovej stanici vytvorený. Môže sa tak stať v prípade, keď sa nepodarí nájsť správne nastavenia sektorov v siedmich krokoch a testovanie je odložené pretože tiket ku každej základňovej stanici umožňuje iba sedem krokov. A ako bude opísané neskôr v kroku 7, po otestovaní sa sítě testované sektory nechávajú pridelené vytvorenému profilu, ale parametre *dlPrbLoadLevel* a *minLoadLevelPdcch* sa nastavujú na nižšiu hodnotu. Preto je potrebné overiť správne nastavenie profilu.

Následne je potrebné odomknúť zamknuté WCS sektory a objekty *SectorEquipmentFunction*, a to v opačnom poradí, v akom sme ich zamykali v kroku č.1. V prvom rade odomkneme objekty *SectorEquipmentFunction* a následne WCS sektory. Ako posledný krok skontrolujeme stav generátoru, ktorý musí byť aktivovaný. Informujeme technika o ukončení prípravy a možnosti začať s testovaním rušenia satelitného rádia Sirius XM.

Krok 3 - 6

Kroky 3 až 6 slúžia na hľadanie správnych parametrov výkonu a naklonenia antény pre odstránenie rušenia satelitného rádia Sirius XM. Postup týchto krokov je podobný predchádzajúcim krokom. V prvom rade si overíme existenciu zálohy z prvého kroku a zobrazíme si aktuálny stav WCS sektorov, ktoré by mali byť odomknuté (unlocked) a aktivované (enabled). Následne môžeme prísť k blokovaniu sektorov a objektov SectorEquipmentFunction v poradí: 1. WCS sektory, 2. príslušné objekty SectorEquipmentFunction. Po vykonaní blokovania si overíme aktuálne nastavenie vysielacieho výkonu WCS sektorov a hodnoty natočenia príslušných antén za účelom zistenia prípadnej manipulácie s hodnotami iným inžinierom. V prípade očakávaného stavu môžeme prísť k zmene vysielacieho výkonu a naklonenia antény na hodnoty, ktoré si technik vyžiadal po ukončení testovania prvotných parametrov. K prvotnému zablokovaniu sektorov dochádza z dôvodu nastavenia daných parametrov, ktoré sa aplikujú až po reštarte WCS sektorov. Po nastavení žiadaných parametrov následne odomkneme sektory a príslušné objekty SectorEquipmentFunction v rovnakom poradí ako v kroku č.2, skontrolujeme správne nastavenie profilu na WCS sektoroch a informujeme technika o ukončení prípravy a možnosti pokračovať v testovaní.

Krok 7

Krokom č. 7 končíme testovanie základňovej stanice či už v prípade úspešného alebo neúspešného nájdenia potrebných parametrov. Základňová stanica sa po skončení testovania musí nachádzať v tzv. konečných parametroch, ktoré sú stanovené v tike-toch daných základňových staníc. Ako už bolo spomenuté vyššie, pri poslednom kroku sa zariadenie nevypína, ale uvedie sa do nastavení, v ktorých sa nebude možné na základňovú stanicu pripojiť z dôvodu slabého vysielacieho výkonu. Koná sa tak z dôvodu nutnosti schválenia zistených parametrov organizáciou FCC a samotným rušeným elementom, v našom prípade rádiom Sirius XM. V tomto kroku sa postupuje rovnako ako v predchádzajúcich krokoch. Najprv skontrolujeme stav WCS sektorov, následne testované sektory zablokujeme spolu s objektami SectorEquipmentFunction. Teraz sa nachádzame vo fáze nastavenia konečných parametrov. Hodnota vysielacieho výkonu sa v prípade zariadení Ericsson nastavuje na 10%, teda základňová stanica bude využívať iba 10% z celkového nastaveného vysielacieho výkonu. Dôležité je následne nastaviť parametre *dlPrbLoadLevel* a *minLoadLevelPdcch* na hodnotu 20. Koná sa tak z dôvodu zbytočného nevyťažovania základňovej stanice, keďže môže nastať situácia, kedy bude potrebné otestovať WCS sektory napr. na funkčnosť tiesňovej služby E911. Sektory WCS budú stále využívať definovaný profil, technik sa pomocou hodnôt PCI na ne pripojí a stanica nebude zbytočne

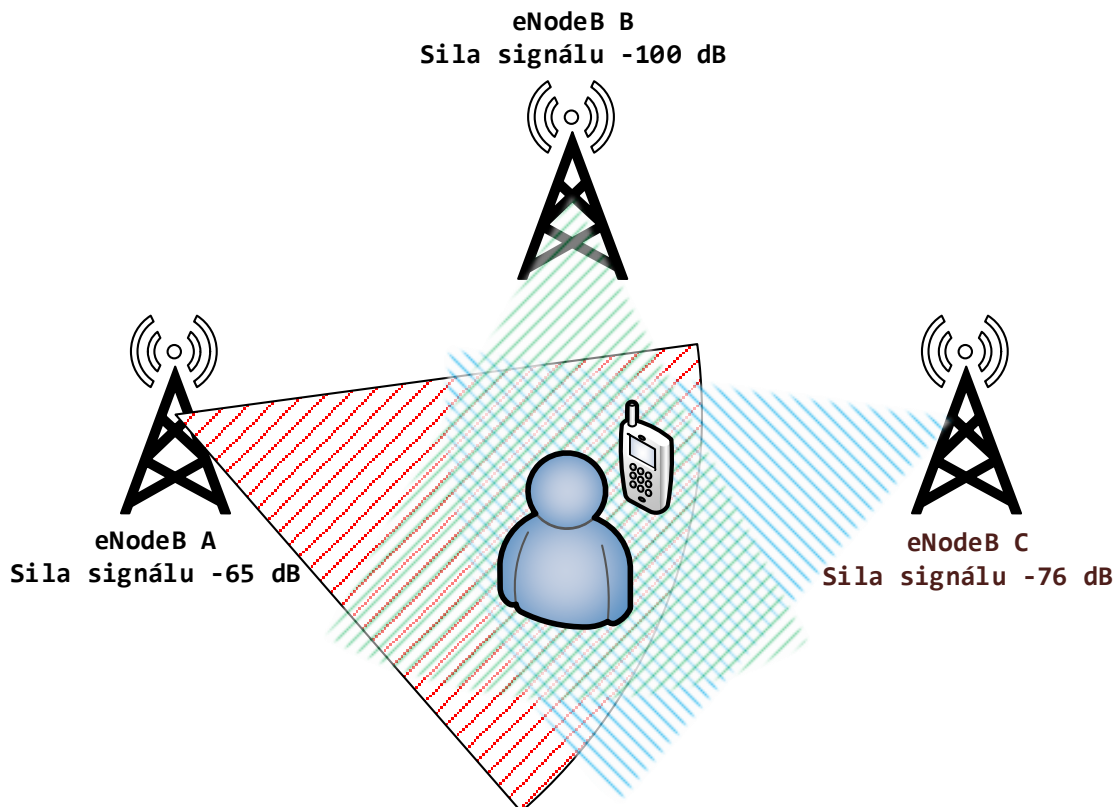
generovať príliš veľa zbytočných dát, ale bude generovať dáta iba po hladinu 20% vyťaženia. Následne, v prípade potreby, vykonáme zmeny v nastavení hodnôt naklonenia jednotlivých antén. Avšak tento krok nie je takým častým ako zmena hodnôt vysielacích výkonov. Po dokončení nastavovania koncových parametrov môžeme vykonať kontrolu zariadenia, kedy skontrolujeme alarmy, stav sektorov a príslušných objektov. Vytvoríme novú zálohu základňovej stanice, aby sme neprišli o koncové nastavenia, ak by neskôr došlo k zlyhaniu alebo chybe zariadenia.

Výstupom tohto testovania sú zistené parametre, ktoré sa budú po schválení potrebnými organizáciami následne nastavovať na základňové stanice. Počas celého testovania platí, že testované WCS sektory nemôžu byť nastavené na vysielací výkon 100% po čas dlhší ako je čas stanovený na testovanie.

Zásadným problémom pri oboch doteraz zmienených úkonoch je samotné vypínanie sektorov. Vypínanie sektorov sa vykonáva pri procese testovania tiesňovej služby pomocou tvrdého vypínania. To znamená, že sa sektor jednoducho v danom momente vypne. V prípade testovania rušenia služby sa už používa jemné blokovanie sektorov, ale starý operačný systém L14, zariadenia Ericsson, stále používa metódu tvrdého blokovania sektorov. Samotné jemné blokovanie sektorov by sa taktiež mohlo aplikovať aj na proces testovania tiesňovej služby, ale inžinier vykonávajúci tento úkon musí postupovať podľa schváleného postupu, ktorý to neumožňuje. Tu narážame na zmenu už zavedeného a fungujúceho postupu, ktorá by sa musela uskutočniť. Všeobecne každé tvrdé vypnutie sektora spôsobí okamžité prerušenie toku používateľských dát a dochádza k nutnosti handoveru. To má za následok oneskorenie používanej služby. Jednou možnosťou, ako sa vyhnúť oneskoreniu služby je práve použitie jemného blokovania sektorov, ktoré je zobrazené na obrázku. Pri použití jemného blokovania sa sektor ihneď nevypne, ale dochádza k postupnému znižovaniu vysielacieho výkonu, až kým zariadenie používateľa nevyhodnotí signál zo susednej základňovej stanice za lepšiu a uskutoční handover. To znamená, že používateľ nestratí svoje relácie a nebude negatívne ovplyvnený zásahom inžiniera do rádiových častí mobilnej siete.

Problémom však je, že samotné použitie jemného blokovania sektorov nevyrieši problém používateľa so stratou relácie. Ak susedné základňové stanice sú plne vyťažené, tým pádom používateľ bude musieť počkať na najbližší možný slot pre vysielanie. Preto by malo byť do procesu testovania tiesňovej služby zaradené pred samotné blokovanie sektorov overenie voľnej kapacity susedných základňových staníc.

Obrázok 3.5 znázorňuje situáciu, kde je potrebné zablokovať sektory na stanici A. V prípade blokovania teda musíme počítať s následkom, že 194 používateľov sa bude musieť pripojiť na jednu zo susedných základňových staníc. Pokiaľ predpokladáme LTE systém s 20 MHz šírkou pásma pre každý smer toku dát, máme k dispozícii 100 RB (resource block - zdrojový blok¹) v jednom subrámcí². Pokiaľ budeme počítať



Obr. 3.4: Názorná ukážka jemného blokovania sektorov

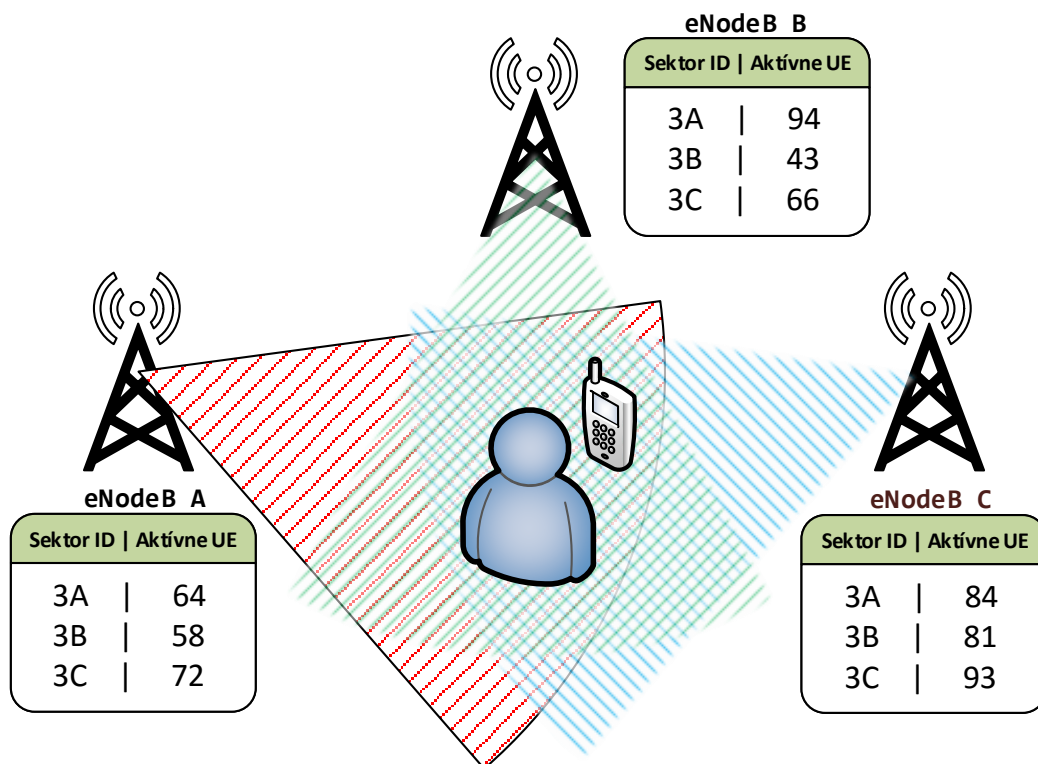
s jedným RB pre používateľa tak je základňová stanica schopná obslúžiť 100 používateľov za 1 ms. V tejto situácii by ďalšie dve základňové stanice nemali kapacitu obslúžiť všetkých používateľov v rovnakú chvíľu a niektorí používatelia by museli čakať na najbližší voľný subrámeček. Lenže v skutočnosti základňová stanica nie je schopná obslúžiť 100 používateľov za predpokladu 1 RB pre 1 používateľa v 1 subrámečeku, pretože musíme počítať s faktom, že niekoľko RB si vyžadujú PDCCH kanál, PBCH kanál, referenčný a synchronizačný signál (RS) i kódovanie. Tie môžeme odhadnúť nasledovne:

- PDCCH kanál môže zabrať 1 až 3 symboly zo 14 symbolov v subrámečeku. Ak budeme počítať s priemerným využitím 2.5 symbolu v subrámečeku, zaberie kanál PDCCH 17.86 % zo všetkých RB.
- RS signály využívajú 4 symboly v každom treťom subnosiči. To znamená vyťaženie 4.76 % v prípade konfigurácie 2x2 MIMO.
- Ostatné kanály (PSS, SSS, PBCH, PCFICH, PHICH), ktoré spolu využívajú približne 2.6 % zdrojových blokov.

V konečnom dôsledku tak len samotné vyťaženie zdrojových blokov povinnými

¹1 RB pozostáva z 12 subnosičov a každý subnosič pozostáva zo 14 symbolov

²1 subrámeček trvá 1 ms



Obr. 3.5: Názorná ukážka kontroly vyťaženia sektorov

prvkami tvorí približne 25.22 % [20]. Z pôvodného počtu 100 užívateľov sa tak dostávame na hodnotu 75 obslužených používateľov v jednom subrámcu, čo je v prípade trvania jedného LTE rámca³ 750 používateľov. Túto hodnotu 750 používateľov môžeme považovať za maximálnu kapacitu, pri ktorej vieme zaručiť jej zvládnutie základňovou stanicou.

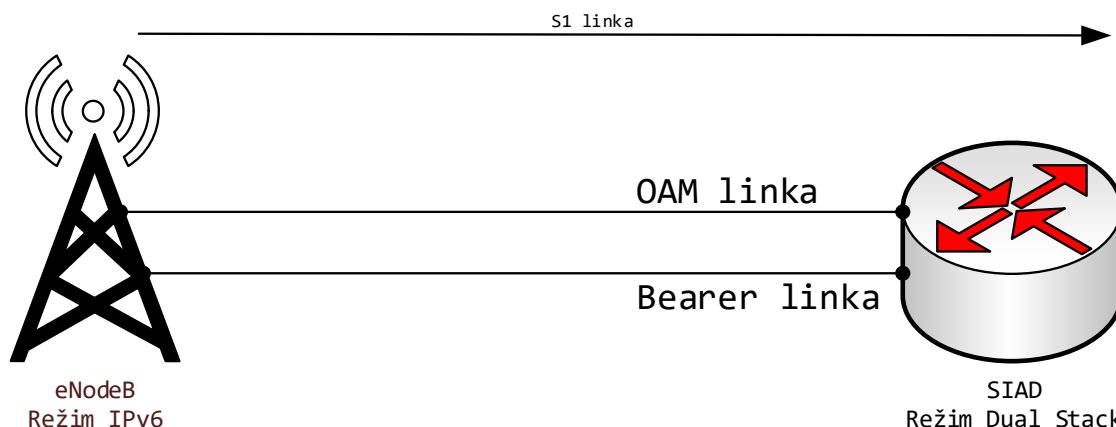
Kapacita základňovej stanice taktiež závisí na použitej výpočtovej sile, teda na výkonnosti procesoru a veľkosti pamäte použitých na danej stanici. Preto aj v prípade menšieho počtu pripojených používateľov na sektoroch je potrebné overiť zaťaženie procesoru susedných základňových staníc.

V uvedenom výpočtovom modeli na predchádzajúcich obrázkoch môžeme konštatovať, že okolité stanice majú dostatočnú rezervu v počte pripojených používateľov a teda v časovom okne LTE rámca 10 ms bude každá zo susedných základňových staníc schopná obslužiť všetkých odpojených používateľov.

³LTE rámec alebo všeobecne rádiový rámec má trvanie 10 ms

4 KONVERZIA TRANSPORTNÉHO PROTOKOLU

Príchodom nového transportného protokolu IPv6 (Internet Protocol version 6 - internetový protokol verzie 6) sa začal postupne meniť celý internet. Väčšina veľkých firiem začala postupne transformovať svoju sieť na transportný protokol IPv6. Mobilní operátori migrujú svoje siete na nový transportný protokol IPv6 hlavne z marketingového hľadiska, aby získali výhodu pred svojim konkurentom a aby neprišli o nových potencionálnych zákazníkov. Samozrejme táto konverzia má aj ďalšie dôvody. Oddalovanie konverzie svojej siete má dopad na výšku ceny samotného úkonu. Prechod na IPv6 je potrebný na poskytovanie nových služieb ako sú napríklad senzorové siete. Tento proces konverzie je však náročný a dôležité je si všetko dopredu podrobne naplánovať, aby nedošlo k ovplyvneniu samotného používateľa. V tejto kapitole sa zameriame na konverziu z transportného protokolu IPv4 na transportný protokol IPv6 základňovej stanice. Na obrázku 4.1 môžete vidieť skutočné zapojenie základňovej stanice, ktorá je pripojená na SIAD (Smart Integrated Access Device - Integrované prístupové zariadenie).



Obr. 4.1: Názorná ukážka zapojenia základňovej stanice

SIAD je prístupové zariadenie, ktoré agreguje používateľské dáta a hovory, predáva ich smerovaču pripojeného na MSC [9]. Je to posledné zariadenie v sieti pracujúce v režime Dual Stack¹. Je dôležité, aby SIAD už bol pripravený na konverziu transportného protokolu základňovej stanice, teda aby už pracoval v režime Dual Stack. Samotná príprava zariadenia SIAD však spadá pod projekt realizovaný iným tímom a musí sa vykonať s dostatočným predstihom, aby sa overila správna konfigurácia zariadenia a jeho schopnosť spracovávať dáta.

¹je režim, v ktorom je zariadenie schopné pracovať s dátami protokolu IPv4 aj IPv6

Podobne ako pri projekte rušenia rádiovkej technológie Sirius XM, pre každú zmenu transportného protokolu existuje tiket, ktorý obsahuje názvy všetkých základňových staníc priradených na migráciu. Dôležitým prvkom v tikete je CIQ, v ktorom nájdeme všetky potrebné informácie pre inžiniera: priradené IPv6 adresy základňových staníc, ich potrebný počiatkový a žiadaný koncový stav, taktiež IPv6 adresy zariadení MME a NTP (Network Time Protocol - sieťový protokol na synchronizáciu času) serverov.

V prípade, že disponujeme týmito potrebnými dátami, môžeme začať s auditom základňových staníc. Je nutné pripojiť sa na všetky pridelené základňové stanice a skontrolovať, či už náhodou nie sú vytvorené rozhrania IPv6 pre OAM a Bearer linku. Ak sú, tak skontrolovať či majú pridelené správne adresy vzhľadom k adresám na SIADe. Je dôležité, aby tieto adresy patrili do jednej podsiete kvôli správne smerovaniu a fungovaniu VLAN (Virtual Local Area Network - virtuálna lokálna sieť) podsiete. Každá z liniek OAM a Bearer tvorí samostatnú VLAN. V samotnom audite potom môžeme vidieť, že sa pripájame na základňovú stanicu pod adresou IPv4 ako je vidieť v nasledujúcom výpise zo zariadenia Ericsson.

```
amos CVL06216

Checking ip contact...OK
CVL06216> lt all
.
.
.
Connected to 203.0.113.38

CVL06216>
```

Pri audite je ešte potrebné skontrolovať nadefinované adresy pre MME a NTP servery. Každá základňová stanica má nadefinovaných 12 IPv4 MME adries a 2 adresy NTP serverov. Musíme overiť, či sa nenachádzajú už nadefinované IPv6 adresy pre MME a NTP servery na základňovej stanici, pretože ak by už stanica disponovala týmito adresami a my by sme v ďalšom kroku nadefinovali rovnakú adresu, mohlo by dôjsť k preťaženiu daného MME, pretože zariadenia MME sú prispôbené na presný počet pripojených základňových staníc. Musíme počítat s tým, že migrujeme viacero základňových staníc súčasne, zvyčajne aspoň 50. Ďalšia nutnosť je kontrola synchronizácie stanice. Základňová stanica musí používať GPS synchronizáciu. Nemôže používať IP synchronizáciu, pretože pri konverzií dochádza k vymazaniu IPv4 adries NTP serverov. V prípade, že používa IP synchronizáciu, musíme ju zmazať a aktivovať GPS synchronizáciu. Ďalšou možnosťou by bolo vytvorenie nového IPv4 rozhrania a statického záznamu v smerovacej tabuľke, ktoré by slúžilo

výlučne na IP synchronizáciu. Avšak nám ide výhrane o IPv6 sieť, a preto sa tento spôsob nepoužíva.

Teraz môžeme pristúpiť k overovaniu IPv6 spojenia so S-GW a MME. Adresy týchto zariadení sú poskytnuté inžinierovi prostredníctvom CIQ. IPv6 spojenie overíme pingom z každej základňovej stanice na každú adresu všetkých S-GW v sieti. V našom prípade má každé S-GW 4 adresy a v celej sieti sa ich nachádza 68. Každá základňová stanica musí mať spojenie s každým S-GW v sieti. V prípade MME má každé z nich 2 adresy a tentoraz overuje konektivitu len na MME v danej oblasti, kde sa nachádzajú základňové stanice. Zvyčajne je jedna geografická oblasť v rozsahu jedného štátu. Tieto pingy sme realizovali priamo z každej základňovej stanice pripravenej na koverziu. Následne musíme otestovať konektivitu Bearer aj OAM linky zo serveru. Ak sú všetky testy konektivity úspešné, môžeme pokračovať ďalej, no v prípade, že test niektorej zo základňových staníc zlyhá, musíme túto stanicu odstrániť zo skupiny.

Po kontrole konektivity sa pripojíme na každú základňovú stanicu a vykonáme kontrolu zariadenia z dôvodu možnosti vrátenia zariadenia do pôvodného stavu po dokončení konverzie. Vykonávame kontrolu nasledovných objektov:

- Stav všetkých sektorov;
- Stav všetkých MME, na ktoré má základňová stanica spojenie;
- Stav TWAMP¹ responderu, ktorý je aktívny na oboch virtuálnych linkách medzi eNodeB a SIAD, teda celkovo 4 záznamy;
- Kontrola KPI (Key Performance Indicator - kľúčový indikátor výkonu);

V prílohe A môžeme vidieť všetky kontrolované KPI na zariadení Ericsson. Vidíme časový rozostup 15 minút a všetky hodnoty sú uvedené v percentách, pokiaľ nie je uvedené v samotnom výpise inak. Tieto KPI z pred konverzie budeme porovnávať s KPI po samotnej konverzií. V prípade, že vyššie uvedená kontrola sektorov ukázala, že niektoré z nich sú zablokované, je potrebné tieto sektory zaznačiť a po dokončení konverzie transportného protokolu ich naspäť uviesť do zablokovaného stavu.

Po vykonaní všetkých kontrol musíme vytvoriť zálohu základňovej stanice, aby sme pri zlyhaní konverzie vedeli vrátiť stanicu do pôvodného stavu.

Následne už môžeme pristúpiť k samotnej konverzií transportného protokolu, ktorú môžeme rozdeliť na 3 kroky:

- Nadefinovanie nových liniek k MME;
- Konverzia Bearer linky;
- Konverzia OAM linky;

Ešte pred prvým krokom je dôležité, aby sme celú základňovú stanicu zablokovali kvôli zabráneniu používateľmi pripojenia sa, pretože počas konverzie by Bearer linky

¹je obojsmerný protokol aktívneho merania spojenia medzi dvoma zariadeniami

stratili reláciu alebo by boli od základňovej stanice úplne odpojení. Preto najskôr pristúpime k blokovaniu všetkých sektorov.

Krok 1

V prvom rade je potrebné zablokovať všetky nadefinované linky k MME. Na nasledujúcom výpise zo zariadenia Ericsson môžete vidieť očakávaný stav týchto liniek. Číslo 1 reprezentuje odblokovaný stav a číslo 0 reprezentuje stav zablokovaný.

```

=====
Id   MO                               administrativeState      Result
=====
1949 TermPointToMme=17                 1 -> 0                   >> Set.
1950 TermPointToMme=18                 1 -> 0                   >> Set.
1951 TermPointToMme=19                 1 -> 0                   >> Set.
1952 TermPointToMme=20                 1 -> 0                   >> Set.
1953 TermPointToMme=21                 1 -> 0                   >> Set.
1954 TermPointToMme=22                 1 -> 0                   >> Set.
2066 TermPointToMme=1                  1 -> 0                   >> Set.
2067 TermPointToMme=2                  1 -> 0                   >> Set.
2068 TermPointToMme=3                  1 -> 0                   >> Set.
2069 TermPointToMme=4                  1 -> 0                   >> Set.
2070 TermPointToMme=5                  1 -> 0                   >> Set.
2071 TermPointToMme=6                  1 -> 0                   >> Set.
=====

```

Vo vyššie uvedenom výpise ste mohli vidieť celkovo 12 liniek k šiestim MME v oblasti. Každé MME má pridelené dve adresy, jednu primárnu a druhú záložnú. Po zablokovaní MME liniek, ktoré mali nadefinované IPv4 adresy pristúpime k ich vymazaniu. V prípade zariadenia Ericsson sú tieto linky vymazávané po jednej, pretože zo skúsenosti vieme že vymazaním všetkých liniek naraz dochádzalo k častému zasekávaniu a samovoľnému reštartovaniu základňovej stanice. Domnievame sa, že táto skutočnosť je spôsobená softvérovou chybou stanice. V prípade zariadenia Alcatel môžeme vymazať všetky MME linky naraz. Po vymazaní liniek môžeme pristúpiť k nadefinovaniu nových MME liniek. Týmto krokom nadefinujeme linku k rovnakým MME, avšak priradíme jej primárnu a sekundárnu adresu IPv6. Na nasledujúcom výpise zo zariadenia Ericsson môžete vidieť nadefinovanú IPv6 linku k MME.

```

=====
Id   MO                               ipv6Address1             Result
=====
2996 TermPointToMme=17                 :: -> 2600:300:3003:2:: >> Set.
=====

```

Po nadefinovaní všetkých primárnych aj sekundárnych IPv6 adries si ich ešte raz prekontrolujeme, pretože zle nadefinované dvojice adries čo len jedného MME spôsobujú preťaženie ďalších MME. MME je dôležitým riadiacim prvkom kontrolnej roviny v sieti, ktoré pracuje v skupine v tzv. poole. V jednej skupine sa nachádza viacero MME a je dôležité, aby boli na základňovú stanicu nadefinované MME z jednej skupiny, z dôvodu presmerovania hovoru na ďalšie MME v prípade preťaženia MME. Vo vnútri jednej skupiny funguje funkcia load-balancing (rozloženie záťaže), ktorá pracuje na základe faktoru váhy, ktorý je pridelený každému MME. Tieto pridelené faktory všetkých MME sú oznamované používateľom v S1-AP zprávach a vyjadrujú pravdepodobnosť, s akou si základňová stanica vyberie dané MME [6].

Krok 2

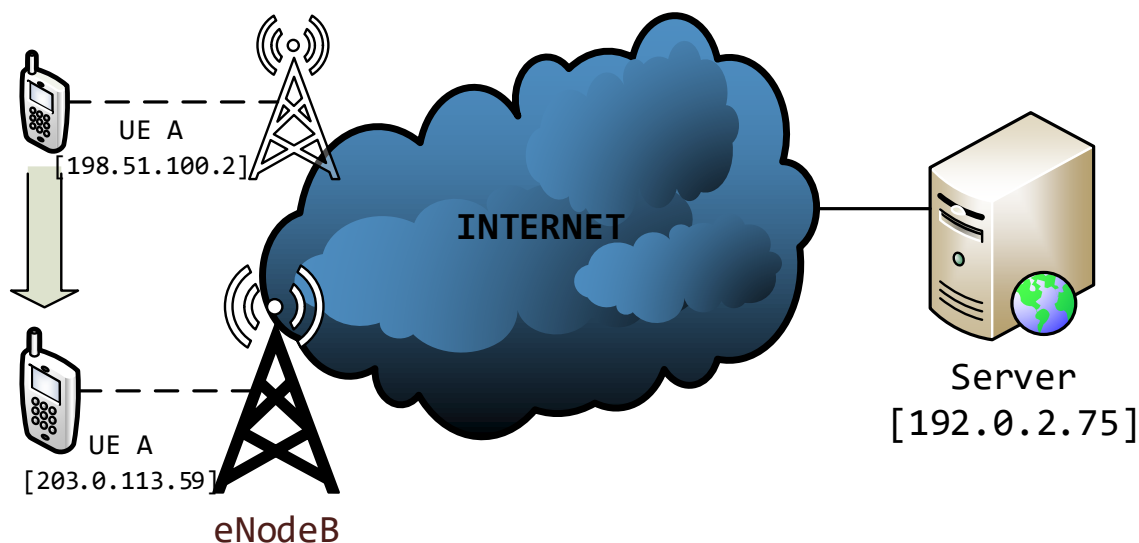
V tomto kroku budeme migrovať transportný protokol Bearer linky. Bearer linka je využívaná pre používateľské a riadiace dáta. V prvom rade si vytvoríme novú zálohu, aby sme v prípade výskytu chyby nemuseli začať celú konverziu od začiatku (vykonávanie všetkých potrebných kontrol). Následne môžeme pristúpiť k samotnému nadefinovaniu nového IPv6 rozhrania. Po vytvorení nového rozhrania nastavíme jeho preferenciu na primárnu, teda všetky dáta budú smerované cez nové rozhranie. Po nadefinovaní rozhrania je potrebné upraviť SCTP (Stream Control Transmission Protocol - riadiaci protokol streamovaného prenosu) protokol.

Protokol SCTP, nazývaný aj ako nová generácia protokolu TCP (Transmission Control Protocol - protokol riadenia prenosu), je navrhnutý na zjednodušenie podpory telefónneho spojenia cez internet. V porovnaní s TCP, SCTP zaisťuje kompletný súbežný prenos viacerých dátových tokov medzi pripojenými koncovými bodmi. SCTP taktiež podporuje funkciu tzv. multihoming, čo znamená, že používateľ môže mať viacero alternatívnych IP adries, pretože podporuje zmenu IP adresy používateľa počas prebiehajúceho spojenia bez jeho straty. Táto funkcia je veľmi potrebná v mobilných sieťach pri mobilite používateľa, ktorý mení obsluhujúcu základňovú stanicu a je mu priradená nová IP adresa [17].

Obrázok 4.2 znázorňuje koncept mobility transportného protokolu v mobilnej sieti, teda vyššie spomínanú funkciu multihoming, kedy používateľ mení obsluhujúcu základňovú stanicu a je mu priradená nová IP adresa, ale jeho prebiehajúca relácia nie je prerušená.

V našom prípade potrebujeme nastaviť maximálnu veľkosť SCTP správy, ktorá môže byť odoslaná cez nové rozhranie na 1460 bajtov. Keďže maximálna veľkosť ethernetového rámca je 1500 bajtov, 20 bajtov zaberie hlavička sieťovej vrstvy a ďalších 20 bajtov zaberie hlavička transportného protokolu.

Ako posledný krok nám ostáva priradiť rozhraniu IPv6 adresu. Preto najskôr rozhranie zablokujeme, nastavíme mu IPv6 adresu a následne ho naspäť odblokujeme. Blokácia rozhrania je potrebná z toho dôvodu, že novo definované parametre nado-



Obr. 4.2: Mobilita transportnej vrstvy [15]

budnú platnosť až po reštartovaní daného objektu. Nakoniec si overíme správnosť IPv6 adresy a vytvoríme novú zálohu, ktorú nastavíme ako primárnu. V prípade vzniku chyby sa základňová stanica obnoví do nastavení po zmigrovaní transportného protokolu Bearer linky.

Krok 3

V poslednom kroku nám teda ostáva zmeniť transportný protokol OAM linky. V prvom rade vykonáme zmenu adries NTP serverov. V tomto prípade nie je potreba nadefinovať novú linku k NTP serverom, pretože nemeníme používané servery. Meníme iba IPv4 adresu na IPv6 adresu. Z tohto faktu vieme vyvodit, že NTP servery pracujú v režime Dual Stack a podporujú súčasne obe verzie transportného protokolu IP. Ako môžete vidieť na nasledujúcom výpise zo zariadenia Ericsson, v našom prípade nadefinujeme vždy primárnu a sekundárnu adresu linky NTP serveru na každú základňovú stanicu.

```

=====
MO                               serverAddress
=====
NtpServer=1,ntpServerAddressPrimary 2600:0308:0030:0101::0079
NtpServer=2,ntpServerAddressSecondary 2600:0308:0010:0200::0097
=====

```

Po overení správnosti nových IPv6 adries liniek k NTP serverom znova overíme konektivitu s OAM linkou. Zo serveru, ktorý spravuje dané základňové stanice vyšleme ping s cieľovou adresou OAM linky, čím sa uistíme o konektivite s danou linkou. V tomto momente môžeme začať s konverziou transportného protokolu OAM linky.

Konverziu začíname nastavením časovaču na nami zvolený čas. Pri nastavení časovaču sa automaticky vytvorí záloha, na ktorú sa základňová stanica obnoví po vypršaní nastaveného času. Časovač je veľmi dôležitý, pretože budeme vykonávať zmeny na OAM linke, ktorú používame a na ktorú sme my pripojení. Z toho plynie, že v prípade chybného nastavenia (alebo inej chyby, ktorá by mohla nastať) stratíme spojenie so základňovou stanicou a už nebudeme schopní sa na ňu znova pripojiť. Časovač sa používa pre zabezpečenie obnovenia základňovej stanice pri výskyte chyby po nami nastavenom čase. Po aktivovaní a overení spustenia časovaču môžeme začať s konverziou transportného protokolu OAM linky. Samotná konverzia je podobná ako konverzia Bearer linky, v prvom rade nadefinujeme nové rozhranie. Po nadefinovaní rozhrania nastavíme jeho preferenciu na primárnu, čím zaistíme, že základňová stanica bude pre inžinierov prístupná pod IPv6 adresou.

Pri definovaní nových rozhraní počítame so skutočnosťou, že druhá strana linky, zariadenie SIAD, je už pripravené a teda tieto rozhrania už boli nadefinované spolu s IPv6 adresami. Z toho plynie, že po nadefinovaní rozhrania a priradení správnej IPv6 adresy na strane základňovej stanice bude linka okamžite funkčná.

Následne priradíme novému rozhraniu správnu IPv6 adresu, ktorá je inžinierovi poskytnutá prostredníctvom vyššie spomenutého tiketu. Po skontrolovaní správnosti nadefinovanej IPv6 adresy novému rozhraniu je už potrebné len deaktivovať časovač, aby sa po uplynutí nastaveného času stanica nevrátila do pôvodného stavu. So samotným deaktivovaním časovaču sa automaticky vytvorí záloha na zariadení.

V tomto bode sme ukončili vykonávanie zmien na zariadení a môžeme konštatovať, že sme ukončili konverziu transportného protokolu IPv4 na IPv6 základňovej stanici. V tomto stave už základňová stanica pracuje výhradne na protokole IPv6, avšak potrebné je ešte odstrániť staré rozhrania pre OAM a Bearer linku.

Na overenie celkovej konzistentnosti konfigurácie a aktualizovanie vykonaných zmien je potrebné reštartovať základňovú stanicu. Pokiaľ sa zariadenie po jeho reštartovaní uvedie do prevádzky bez problémov, a na zariadení nepribudnú žiadne nové alarmy, konverzia transportného protokolu bola úspešná.

Ďalej je potrebné odblokovať a tým uviesť do prevádzky všetky novo nadefinované IPv6 linky k MME, odblokovať všetky sektory na základňovej stanici a tým ich sprístupniť pre používateľov. Po úspešnom zmigrovaní transportného protokolu sa od stanice odpojíme a znova pripojíme, čím vykonáme overenie konektivity základňovej stanice. V nasledujúcom výpise zo zariadenia Ericsson môžeme vidieť, že sa už pripájame pomocou IPv6 adresy.

```

amos CVL06216

Checking ip contact...OK
CVL06216> lt all
.
.
.
Connected to 2001:506:4404:c068::13:10:2

CVL06216>

```

Ako predposledný krok musíme vykonať aktualizáciu smerovacej tabuľky základňovej stanice. Musíme vymazať všetky záznamy týkajúce sa starých IPv4 záznamov a pridať novú predvolenú statickú cestu s IPv6 adresou ďalšieho zariadenia SIAD.

```

=====
Proxy  MO                               Action          Nr of Param
=====
1945  Ip=1,IpRoutingTable=1                listRoutes      0
»» Return value = 7
destinationIpAddr destinationNetMask nextHopIpAddr routeMetric interface
0.0.0.0          0.0.0.0          203.0.113.37 16          lh0
::              0      2001:506:4404:c068::13:10:1 10          lh1
127.0.0.1       255.255.255.255  onlink        0           lo0
::1             128              onlink        0           lo0
169.254.1.10    255.255.0.0      onlink        1           le0
203.0.113.38    255.255.255.252 onlink        1           lh0
2001:506:4404:c068::13:10:2 64  onlink        1           lh1
=====

```

V predchádzajúcom výpise zo základňovej stanice Ericsson môžete vidieť záznamy smerovacej tabuľky po nadeinovaní nového rozhrania a pridaní nového predvoleného statického záznamu, ktorý je vyznačený zelenou farbou. Červenou farbou sú zvýraznené záznamy na odstránenie, konkrétne sa jedná zhora o záznam predvolenej statickej cesty, ktorá používa ako cieľovú adresu IPv4 adresu zariadenia SIAD a záznam siete, ktorá je tvorená linkou medzi základňovou stanicou a zariadením SIAD. Tento záznam je do smerovacej tabuľky pridávaný automaticky po uvedení spojenia do funkčnosti medzi dvoma zariadeniami.

Ako úplne posledný krok vykonáme záverečnú kontrolu zariadenia, ktorá je rovnaká ako kontrola vykonávaná pred začatím konverzie transportného protokolu základňovej stanice. Je dôležité skontrolovať alarmy na stanici, pretože očakávaný výstup je rovnaký počet alarmov ako pri prvej kontrole. V prípade nového alarmu

si zobrazíme jeho popis a uistíme sa, že sme vykonali všetko správne, no hlavne si overíme, či sme odblokovali všetky sektory a linky k MME. Táto skutočnosť býva najčastejšou chybou a príčinou nového alarmu. V prípade, že sme všetko skontrolovali, musíme túto skutočnosť nahlásiť príslušnému tímu, ktorý sa bude zaoberať daným problémom. Ďalej si skontrolujeme stav TWAMP responderu, kde by sme mali vidieť jeho štyri aktivované procesy. Jeden proces merania na jeden smer jednej linky. Prekontrolujeme smerovaciú tabuľku a novo vytvorené rozhranie. Po kontrole nastavení základňovej stanice počkáme 30 minút a po tomto časovom úseku skontrolujeme KPI už zmigrovanej základňovej stanice využívajúcej iba transportný protokol IPv6.

V prílohe B môžete vidieť zmerané KPI po samotnej konverzii transportného protokolu základňovej stanice. Je dôležité, aby sa tieto hodnoty zhodovali s hodnotami nameranými pred konverziou transportného protokolu, teda aby sa zobrazené hodnoty veľmi nelíšili od tých predchádzajúcich. Touto kontrolou si overíme celkovú správnosť vykonanej konverzie a správnu funkčnosť základňovej stanice.

Výstupom celého procesu sú základňové stanice pracujúce s IPv6 transportným protokolom. Pracuje sa naraz na väčšom počte základňových staníc, kedy sú všetky stanice rozdelené do niekoľkých skupín a každá skupina obsahuje maximálne 9 základňových staníc. Týmto postupom sa eliminuje hrozba ľudskej chyby, pretože v prípade ľudského zlyhania nastane chyba iba na 9 základňových stanicách.

5 ZMENA AKTÍVNEHO PRVKU

V tejto kapitole sa budeme venovať servisnému zásahu do rádiovkej siete, pri ktorom dochádza k zmene aktívneho prvku jadra siete pre základňovú stanicu Ericsson.

Mobilný operátor je vlastníkom niekoľkých stoviek až tisícok základňových staníc. Tieto základňové stanice však v reálnom nasadení nie sú zapojené podľa všeobecnej architektúry, ktorú môžete vidieť na obrázku 1.1, pretože by už len z logického hľadiska nebolo možné pripojiť niekoľko stoviek základňových staníc patriacich do jednej oblasti na všetky MME a S-GW v oblasti. V reálnom nasadení sú základňové stanice pripájané na spravujúce Citrix servery.

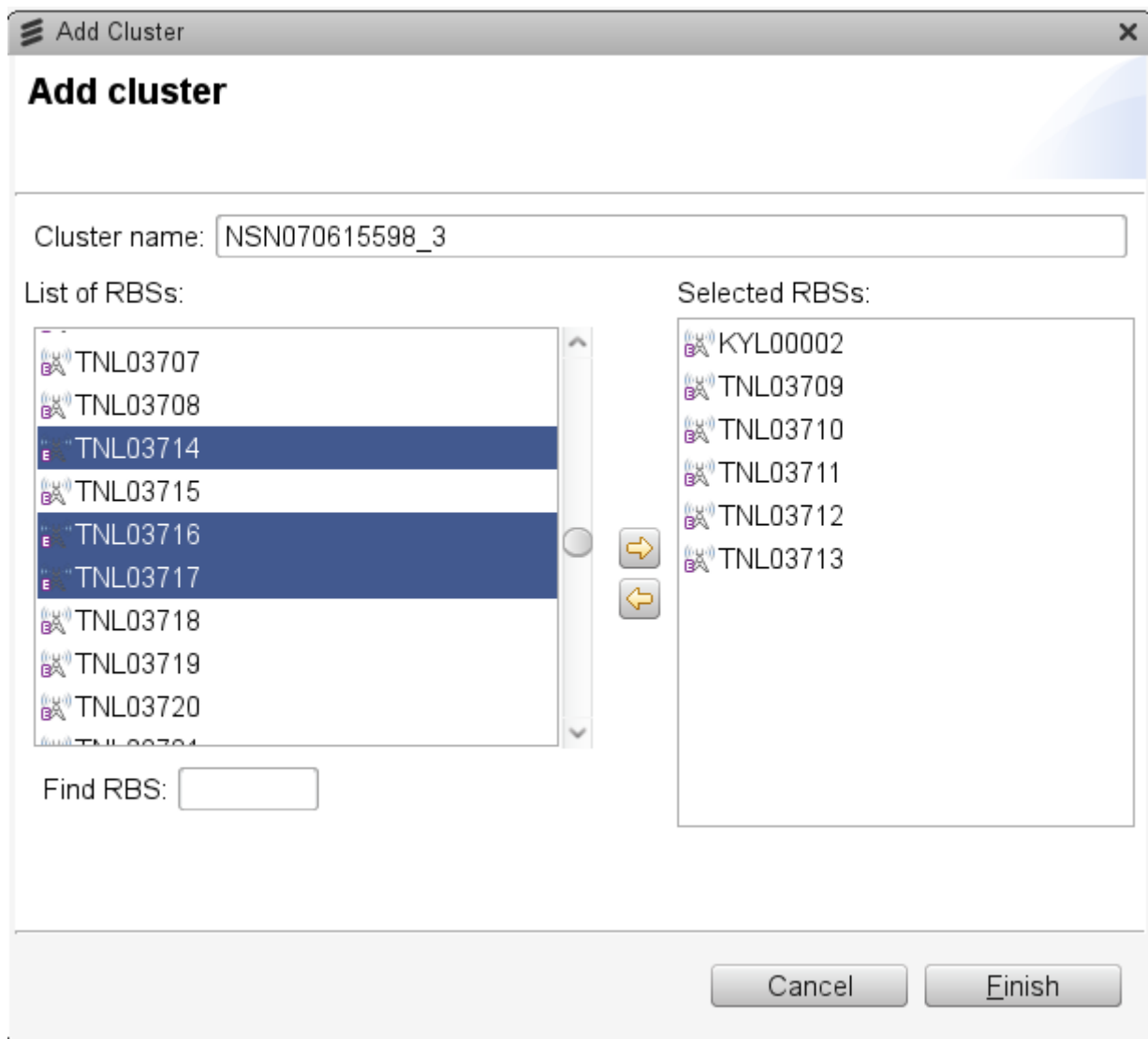
Citrix systém a služby s ním spojené umožňujú Windows aplikáciám a výpočtovým prostriedkom byť centrálné riadené v zabezpečenom dátovom centre. Taktiež umožňujú viacerým používateľom nezávisle pristupovať k serveru. Používatelia môžu pristupovať k aplikáciám z kadekoľvek a z akéhokolvek systému. Základňové stanice sú teda pripájané na servery, ktoré sú prispôbené na zvládnutie veľkého počtu pripojených zariadení a veľkého počtu pripojených používateľov.

V prípade, že mobilný operátor chce zvýšiť rýchlosť poskytovaného pripojenia alebo rozšíriť dosah pripojenia pre používateľov, buduje nové základňové stanice, ktoré je potrebné priradiť na zodpovedajúci server. Takisto v prípade preťaženia jedného serveru alebo potreby rýchlejšieho prístupu na základňové stanice tieto stanice migrujú z pod správy jedného serveru na iný server.

Samotná zmena aktívneho prvku jadra siete sa vykonáva v dvoch krokoch a inžinierovi sú na tento úkon poskytnuté dva dni. V prvý deň je potrebné vykonať prípravu na tento úkon, ktorá pozostáva z overenia dostupnosti všetkých základňových staníc, ktoré je potrebné zmigrovať. Zvyčajným postupom je vytvorenie skriptu ktorý využije príkaz ping a tak zistí dostupnosť všetkých základňových staníc. Lepšou variantou je však vytvorenie tzv. skupiny (cluster) v programe CEX¹ (Common Explorer - prieskumník), do ktorej pridáme všetky základňové stanice. Tento postup je zachytený na obrázku 5.1. Jeho výhodou je fakt, že po pridaní všetkých požadovaných staníc si môžeme zobrazíť ich aktuálny stav, ktorý bude potrebné v ďalších krokoch kontrolovať.

Po vytvorení skupiny a pridaní všetkých základňových staníc skontrolujeme ich aktuálny stav a všetky stanice, ktoré majú iný status ako *Connected* a *Synchronized*, teda všetky stanice, ktoré nie sú pripojené alebo plne synchronizované so serverom je potrebné vylúčiť zo skupiny. V tomto momente je príprava ukončená a potrebujeme iba vyexportovať základné nastavenie základňových staníc pre server, čo je zobrazené na obrázku 5.2. Následne môžeme začať s prevedením zmeny aktívneho prvku siete.

¹je tzv. OSS Common Explorer, teda varianta prieskumníka vo Windowse

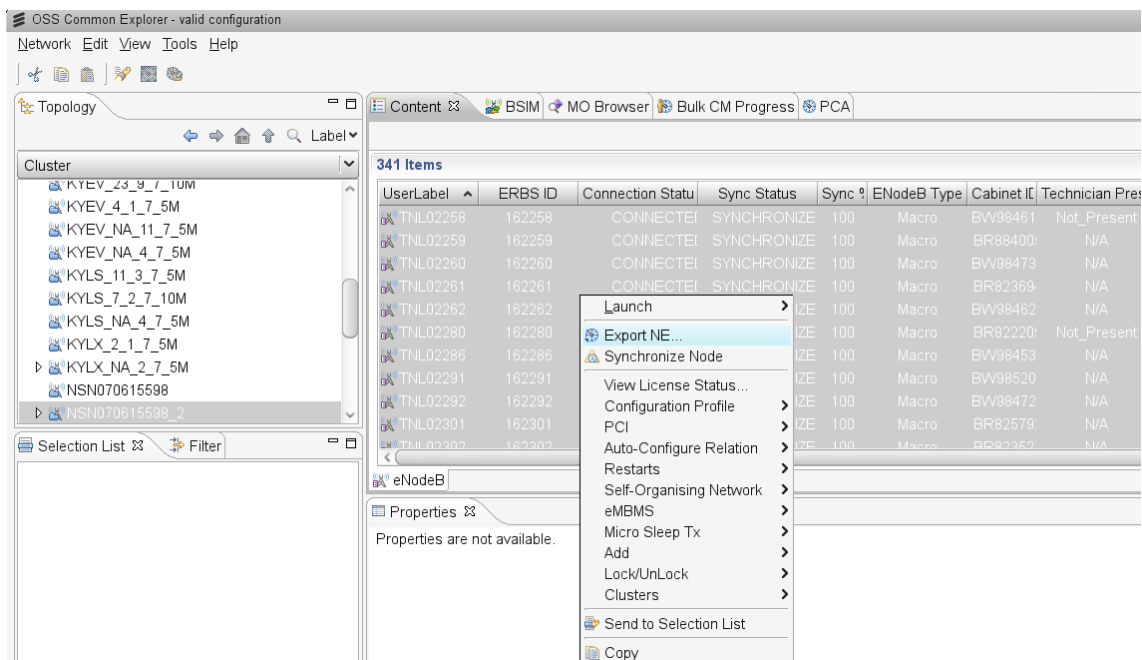


Obr. 5.1: Vytváranie skupiny s následným pridávaním základňových staníc

V prvom kroku potrebujeme získať všetky informácie zo zdrojového serveru potrebné na vytvorenie profilu pre základňové stanice na cieľovom serveri. Tieto informácie sú uložené v súbore `/home/nmsadm/scripts/mpc_arne_export.sh` ktorý si skopírujeme na naše lokálne úložisko.

Informácie ohľadom využívaných FTP (File Transfer Protocol - protokol na prenos súborov) serverov základňovými stanicami obsahujúce:

- Názvy serverov;
- Sieťová adresa serverov;
- Konkrétna cesta ku konfiguračným, softvérovým, licenčným a záložným súborom na serveroch.



Obr. 5.2: Exportovanie serverových nastavení základňových staníc

Informácie ohľadom základňových staníc, ktoré obsahujú:

- Názov základňových staníc, pod ktorým sa na ne pripájame;
- Lokalizáciu staníc v zmysle adresy a popisného čísla;
- Zemepisnú dĺžku a šírku základňových staníc;
- Sieťovú adresu základňových staníc;
- Referencie na konkrétne súbory FTP serverov;
- Svetovú časovú zónu, do ktorej základňové stanice patria.

Ako ďalší krok potrebujeme získať vyššie spomenuté informácie z cieľového serveru. Je potrebné skontrolovať, či sú vyššie spomenuté cesty ku konfiguračným, softvérovým, licenčným a záložným súborom na zdrojovom a cieľovom serveri rovnaké. V prípade, že nie sú alebo niektoré cesty chýbajú, je potrebné ich pridať alebo upraviť na cieľovom serveri aby presne korešpondovali s informáciami na zdrojovom serveri. Takto upravený súbor nahráme naspäť na cieľový server. Týmto zaistíme správne zálohovanie základňových staníc ako aj načítanie konfigurácií pri ich zapínaní.

Následne môžeme začať so samotnou zmenou aktívneho prvku základňových staníc. Všetky stanice sa zvyknú migrovať naraz a je potrebné pripraviť .xml súbor(skript) so všetkými informáciami o základňových staniach, ktoré sme získali zo zdrojového serveru. Pri kopírovaní daných informácií sme získali informácie o všetkých základňových staniach pripojených na server, a preto treba selektovať iba dáta týkajúce sa potrebných základňových staníc. Vykonávať tento servisný úkon

pre všetky stanice naraz však nie je najlepšou voľbou z hľadiska prípadnej chyby, ktorá môže nastať pri samotnej exekúcii importovania údajov. Takýto proces trvá zvyčajne až niekoľko hodín. Pri počte základňových staníc 350 je to približne 5 hodín, pri chybe vzniknutej na konci tohto úkonu by sme ho museli celý opakovať po opravení chyby alebo po vylúčení stanice, na ktorej sa chyba vyskytla. Preto je lepšie si rozdeliť stanice napr. do siedmich skupín a vytvoriť skripty pre každú skupinu zvlášť. V prílohe C môžete vidieť skript nadefinovania jednej základňovej stanice pre danú skupinu.

Po vytvorení skriptov pre nadefinovanie nových prvkov na cieľovom serveri pre všetky skupiny musíme ešte vytvoriť podobné skripty pre vymazanie už nadefinovaných prvkov zo zdrojového serveru pre všetky skupiny. Tieto skripty sú už oveľa jednoduchšie na vytvorenie, pretože sa odkazujú iba na názov základňovej stanice, všetky parametre týkajúce sa základňových staníc sa automaticky vymažú spolu s vymazaním ich primárneho objektu. V prílohe D môžete vidieť skript na vymazanie základňových staníc v jednej skupine. Môžete tu vidieť, že v prvom rade sa odstraňuje manažovateľný objekt, čím vymažeme aj všetky ostatné objekty ktoré odkazujú na tento primárny manažovateľný objekt. Až následne odstraňujeme samotnú základňovú stanicu z pamäte.

Po príprave všetkých potrebných skriptov je už potrebné iba odstrániť základňové stanice z profilu na zdrojovom serveri. Po odstránení z profilu tieto stanice nebudú priradené do žiadneho profilu. To vykonáme pomocou programu PMS¹ (Performance Measuring System - program merania výkonu), ktorý poskytuje server. Ukážka programu je zobrazená na obrázku 5.3.

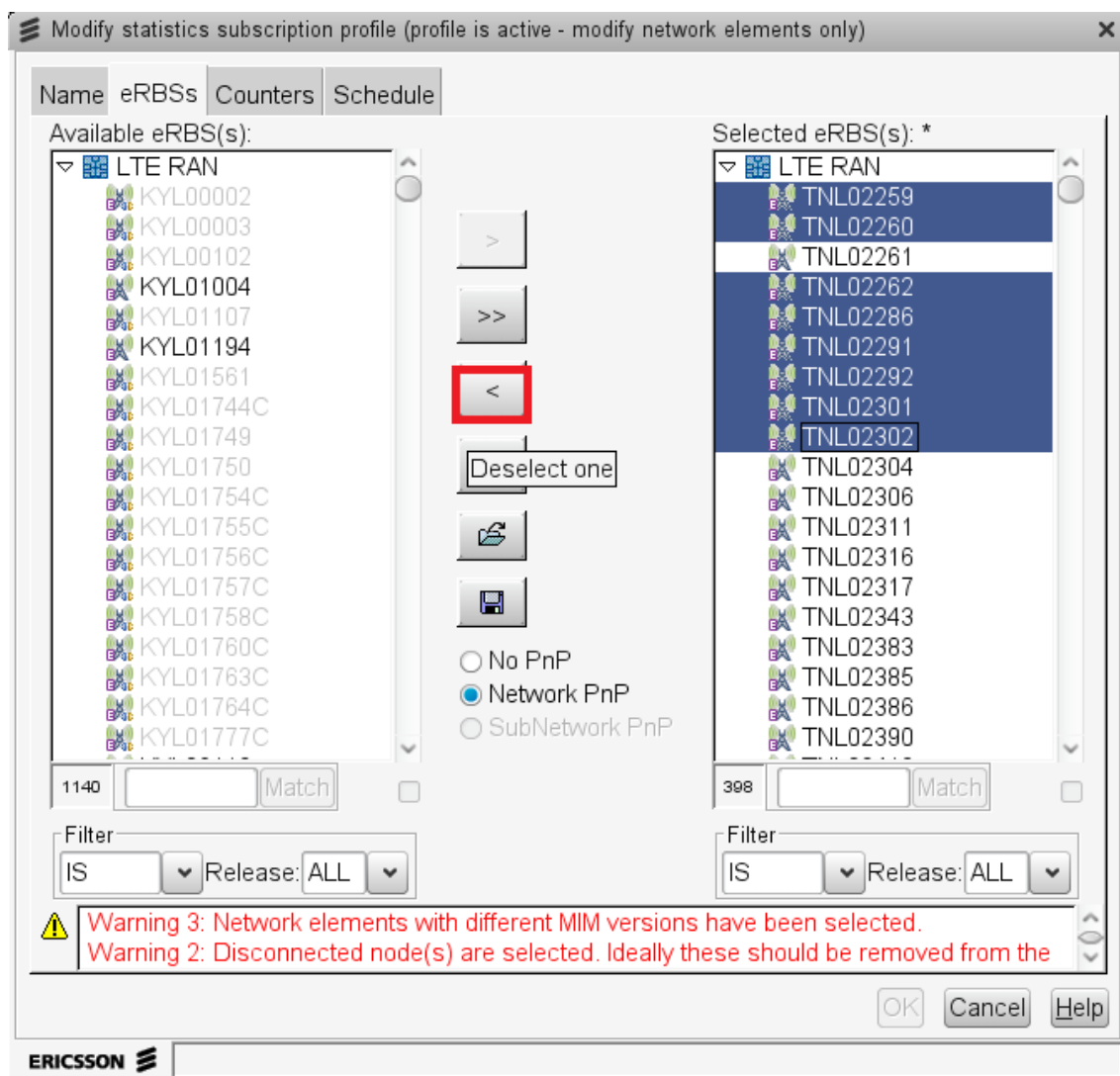
V tomto momente je už všetko pripravené a môžeme pristúpiť k samotnému spúšťaniu pripravených skriptov.

Na rozdiel od programu PMS, kvôli ktorému sme sa museli pripojiť na zdrojový server prostredníctvom webového rozhrania, aby sme mohli využívať grafické rozhranie, na spúšťanie vytvorených skriptov sa pripojíme na server prostredníctvom SSH (Secure Shell - zabezpečený prístup k príkazovému interpretovaču) spojenia. Pri spúšťaní samostatných skriptov musíme dodržať nasledujúci postup:

1. Spustiť skript pre odstránenie základňových staníc na zdrojovom serveri pre danú skupinu;
2. Spustiť skript pre nadefinovanie základňových staníc na cieľovom serveri pre danú skupinu.

Postupne spúšťame v danom poradí skripty pre všetky skupiny a zároveň kontrolujeme pomocou programu CEX správnosť skriptu určeného pre mazanie. Pri správnom priebehu sa z pôvodného počtu základňových staníc pomaly stane počet staníc

¹je proprietárny program Ericsson, ktorý slúži na správu profilov na serveroch

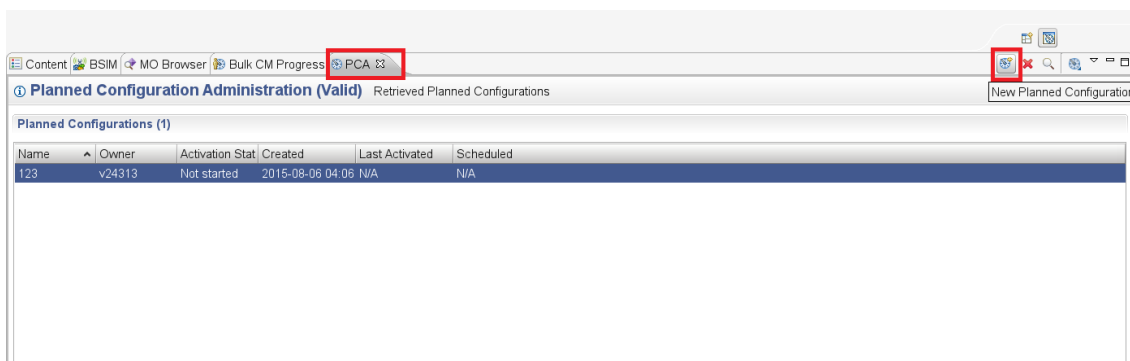


Obr. 5.3: Odstraňovanie základňových staníc z profilu na zdrojovom serveri

zmenšený o veľkosť danej skupiny. Po dokončení všetkých skupín by mala byť skupina (vytvorený cluster) úplne prázdna. V prípade, že nastane situácia, v ktorej nám po dokončení všetkých skupín ostane jedna alebo viacero základňových staníc, je potrebné sa pripojiť na každú stanicu a zistiť možnú príčinu chyby. V prípade, že na základňovej stanici prebieha jej samotný reštart, je potrebné opakovať skripty pre skupinu do ktorej základňová stanica patrila. V prípade že sú na základňovej stanici alarmy, ktoré znemožňujú jej migráciu, je potrebné vytvoriť chybový tiket¹.

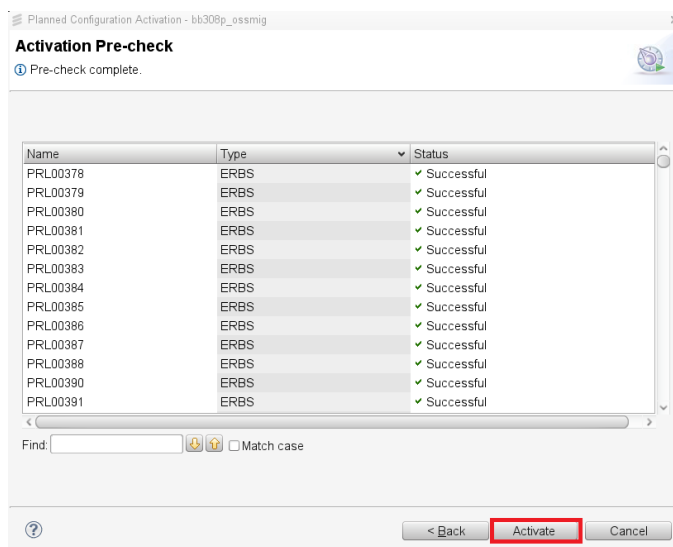
Ako posledný krok v tomto servisnom úkone nám ostáva aktivovať novú konfiguráciu základňových staníc na cieľovom serveri. V programe CEX si vytvoríme novú konfiguráciu podľa obrázku 5.4.

¹je tiket ohlasujúci nájdený problém, ktorý inžinier nemôže vyriešiť či už z dôvodu nevedomosti alebo nedostatočných práv na opravu chyby



Obr. 5.4: Vytvorenie novej konfigurácie pre aktivovanie nových základňových staníc

Následne do novovytvorenej konfigurácie importujeme serverové nastavenia, ktoré sme vyexportovali zo zdrojového serveru. Po dokončení importu server overí správnosť údajov porovnaním s údajmi, ktoré sme nadefinovali pomocou vytvorených skriptov. V prípade, že sú všetky základňové stanice overené, túto skutočnosť nám identifikuje stav *úspešný (successful)* na obrázku 5.5, aktivujeme túto konfiguráciu a zmena aktívneho prvku základňových staníc je dokončená. Nakoniec vykonáme kontrolu základňových staníc, náhodne si vybereme niekoľko staníc z každej skupiny a pripojíme sa na ne už prostredníctvom nového serveru. Pokiaľ bude prihlásenie úspešné, vykonaná zmena aktívneho prvku bola úspešná.



Obr. 5.5: Aktivácia konfigurácie nových základňových staníc

Výsledkom tohto servisného úkonu je zmena serveru, pomocou ktorého sa budú inžinieri pripájať na dané základňové stanice. V prípade tohto servisného úkonu nie je potrebné sa zaoberať kolíziami na základňových stanicach typu viacero naraz

pracujúcich inžinierov na jednom zariadení. Všetci mobilní inžinieri sú oboznámení s časom tohto úkonu a v prípade, že budú počas neho pracovať na jednej alebo viacerých spomínaných základňových staniciach, budú od týchto staníc odpojení.

6 ZÁVER

Cieľom diplomovej práce bolo popísať rádiovú prístupovú sieť mobilnej siete, diskutovať servisné zásahy vykonané pre otestovanie služby tiesňového volania, odstránenia rušenia sa rádiových technológií, konverziu transportného protokolu základňovej stanice a zmenu aktívneho segmentu jadra siete pre základňovú stanicu.

V teoretickej časti diplomovej práce boli popísané systémy štvrtej generácie rádiových sietí, ich architektúra, protokolová výbava a popis jednotlivých prvkov. Následne je popísaná služba tiesňového hovoru, jej vývojové fázy a začlenenie do mobilných sietí. Opísaný bol taktiež spôsob lokalizácie mobilného zariadenia, pretože je úzko spätý so službou tiesňového hovoru. V závere teoretickej časti sú popísané všetky prvky potrebné na uskutočnenie tiesňového hovoru.

V praktickej časti, ktorá sa venovala vytvoreniu postupov jednotlivých servisných zásahov, boli opísané servisné úkony testovania služby tiesňového hovoru, odstránenia rušenia sa rádiových technológií, konverzie transportného protokolu základňovej stanice a zmeny aktívneho segmentu jadra siete pre základňovú stanicu.

Na základe vyskúšaných servisných zásahov a vytvorených postupov bolo vykonané vyčlenenie problematickej časti servisných úkonov a bol vytvorený návrh ich riešenia.

LITERATÚRA

- [1] 3GPP *Carrier Aggregation explained* [online]. Poslední aktualizace 6.2013 [cit. 6.3.2016]. Dostupné z URL: <<http://www.3gpp.org/technologies/keywords-acronyms/101-carrier-aggregation-explained>>.
- [2] 3GPP *Emergency Sessions* [online]. Poslední aktualizace 6.2013 [cit. 17.2.2016]. Dostupné z URL: <<http://www.qtc.jp/3GPP/Specs/23167-940.pdf>>.
- [3] 3GPP ETSI *Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode* [online]. ETSI TS 136 304 V9.1.0 07.2010 [cit. 24.2.2016]. Dostupné z URL: <https://www.etsi.org/deliver/etsi_ts/136300_136399/136304/09.01.00_60/ts_136304v090100p.pdf>.
- [4] 3GPP ETSI *Evolved Universal Terrestrial Radio Access (E-UTRA), Physical layer - Measurements* ETSI TS 136 214 V9.1.0 04.2010 [cit. 15.3.2016]. Dostupné z URL: <http://www.etsi.org/deliver/etsi_ts/136200_136299/136214/09.01.00_60/ts_136214v090100p.pdf>.
- [5] 3GPP Release 8 *Release 8* [online]. 2011, poslední aktualizace 24.9.2014 [cit. 1.3.2016]. Dostupné z URL: <http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel-08_description_20140924.zip>.
- [6] 3GPP Release 8 *Technical Specification Group Services and System Aspects* [online]. [cit. 10.4.2016]. Dostupné z URL: <http://www.3gpp.org/ftp/Specs/archive/23_series/23.401/23401-8c0.zip>.
- [7] AKYILDIZ, I. GUTIERREZ-ESTEVEZ, D. REYES, E. *The evolution to 4G cellular systems: LTE-Advanced* [online]. Broadband Wireless Networking Laboratory, Georgia Institute of Technology, 2010 [cit. 10.12.2015]. Dostupné z URL: <<http://www2.ece.gatech.edu/research/labs/bwn/surveys/ltea.pdf>>.
- [8] CISCO *Managing Emergency Calls* [online]. [cit. 30.3.2016]. Dostupné z URL: <http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book/sbc_emercall.pdf>.
- [9] CISCO *Cisco IAD2435-8FXS Business Class Integrated Access Device*. [cit. 4.4.2016]. Dostupné z URL: <http://www.cisco.com/c/en/us/products/collateral/unified-communications/iad2400-series-integrated-access-devices/data_sheet_c78-505267.html>.

- [10] CND *Emergency Services* [online]. [cit. 21. 3, 2016]. Dostupné z URL: <<http://www.openimscore.org/documentation/emergency-services/>>.
- [11] Federal Communications Commission *Služby 911 a E911* [online]. 2011, poslední aktualizace 12. 11. 2015 [cit. 2. 12. 2015]. Dostupné z URL: <<https://www.fcc.gov/encyclopedia/9-1-1-and-e9-1-1-services>>.
- [12] Federal Communications Commission *What is Antenna Electrical and Mechanical Tilt* [online]. [cit. 17. 3, 2016]. Dostupné z URL: <<https://www.fcc.gov/general/wireless-communications-service-wcs>>.
- [13] Federal Communications Commission *E911 Requirements for IP-Enabled Service Providers* [online]. poslední aktualizace 3. 6. 2015 [cit. 1. 3. 2016]. Dostupné z URL: <https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-116A1.pdf>.
- [14] Government of Canada *Telecom Regulatory Policy CRTC 2009-40* Publikované 2. 2. 2009 [cit. 2. 4. 2016]. Dostupné z URL: <<http://www.crtc.gc.ca/eng/archive/2009/2009-40.htm>>.
- [15] Internet Engineering Task Force (IETF) *IPv4 Address Blocks Reserved for Documentation* Publikované 1. 2010 [cit. 18. 5. 2016]. ISSN: 2070-1721. Dostupné z URL: <<https://tools.ietf.org/html/rfc5737>>.
- [16] Kumar, S. *Wireless Communications Fundamental & Advanced Concepts* [online]. 2015, [cit. 24. 12. 2015]. River Publishers, ISDN: 978-87-93102-80-4, 978-87-93102-81-1.
- [17] Li Ma, F. Richard, Yu. Victor, C. Leung, M. *Performance Improvements of Mobile SCTP in Integrated Heterogeneous Wireless Networks* [online]. [cit. 11. 4. 2016]. Dostupné z URL: <<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4350307>>.
- [18] Patent *Method and arrangement for configuring managed object model for combined cell* Publikované 20. 3. 2014 [cit. 15. 3. 2016]. Dostupné z URL: <<http://www.google.com/patents/WO2014042567A1?cl=en>>.
- [19] PRINCIPI, B. *Diameter routing in 3G, IMS and LTE networks: Tekelec one-on-one* [online]. poslední aktualizace 4. 10. 2011 [cit. 2. 4. 2016]. Dostupné z URL: <<http://www.telecomengine.com/article/diameter-routing-3g-ims-and-lte-networks-tekelec-one-one>>.

- [20] RAYAL, F. *LTE Peak Capacity* [online]. Poslední aktualizace 27.6.2011 [cit. 28.3,2016]. Dostupné z URL: <<https://frankrayal.com/2011/06/27/lte-peak-capacity/>>.
- [21] telecomHall *Wireless Communications Service (WCS)* [online]. [cit. 6.3,2016]. Dostupné z URL: <<http://www.telecomhall.com/what-is-antenna-electrical-and-mechanical-tilt-and-how-to-use-it.aspx>>.
- [22] Voip-info *Session Border Controller* [online]. poslední aktualizace 18.1.2016 [cit. 15.3.2016]. Dostupné z URL: <<http://www.voip-info.org/wiki/view/Session+Border+Controller>>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

AGPS	asistovaný globálny pozičný systém – Assisted Global Positioned System
AMT	letecká mobilná telemetria – Aeronautical Mobile Telemetry
CCE	riadiace prvky kanálu – Control Channel Elements
CEX	prieskumník – Common Explorer
DRA	Diameter Routing Agent
EATF	prvok tiesňovej prístupovej prenosovej funkcie – Emergency Access Transfer Function
EPS	vyvinutý paketový systém – Evolved Packet System
E-CSCF	prvok riadenia tiesňového hovoru – Emergency-Call Session Control Function
eMSC	vylepšené MSC – Enhanced Mobile Switching Center
ePDG	vyvinuté PDG – evolved PDG
eSMLC	vyvinuté mobilné lokalizačné centrum – Evolved Serving Mobile Location Center
FCC	federálna komisia pre komunikáciu – Federal Communications Commission
FDD	frekvenčné oddelenie kanálov – Frequency-Division Duplex
FTP	protokol na prenos súborov – File Transfer Protocol
HSDPA	vysokorýchlostný prenos paketov v smere downlink – High Speed Downlink Packet Access
HSPA	vysokorýchlostný prenos paketov – High Speed Packet Access
HSUPA	vysokorýchlostný prenos paketov v smere uplink – High Speed Uplink Packet Access
IMT-2000	medzinárodný telekomunikačný úrad – International Mobile Telecommunications
IPv6	internetový protokol verzie 6 – Internet Protocol version 6

ITU	medzinárodná telekomunikačná únia – International Telecommunication Union
KPI	klúčový výkonnostný indikátor – Key Performance Indicator
LTE	Long Term Evolution
MIMO	viacero vstupov viacero výstupov – Multiple Input Multiple Output
NTP	sieťový protokol na synchronizáciu času – Network Time Protocol
OFDMA	ortogonálny multiplex s frekvenčným delením – Orthogonal Frequency Division Multiplexing
PCI	identifikátor bunky - Physical-layer Cell Identifier
P-CSCF	proxy server v IMS – Proxy-Call Session Control Function
PDCCH	fyzický, riadiaci downlink kanál – Physical Downlink Control Channel
PDN-GW	brána dátových paketových sietí – Packet Data Network Gateway
PDSCH	fyzický, zdieľaný downlink kanál – Physical Downlink Shared Channel
P-LRF	prvok príjmu lokalizačnej funkcie – Proxy-Location Retrieval Function
PMS	program merania výkonu – Performance Measuring System
PRB	fyzický zdrojový blok – Physical Resource Block
PSAP	verejná záchranná služba – Public Safety Answering Point
RAN	rádiová prístupová sieť – Radio Access Network
RB	zdrojový blok – Resource Block
RET	vzdialený elektrický náklon – Remote Electrical Tilt
RSRP	sila prijímaného signálu – Reference Signal Received Power
RSRQ	kvalita prijímaného signálu – Reference Signal Received Quality
SAE	System Architecture Evolution

SBC	prvok riadenia relácií – Session Border Controller
SCTP	riadiaci protokol streamovaného prenosu – Stream Control Transmission Protocol
SIAD	integrované prístupové zariadenie – Smart Integrated Access Device
SMSS	výberový smerovač – Selective Router
SSH	zabezpečený prístup k príkazovému interpretovaču – Secure Shell
TCP	protokol riadenia prenosu – Transmission Control Protocol
TDD	časové oddelenie kanálov – Time-Division Duplex
TWAMP	dvojcestný protokol aktívneho merania spojenia– Two Way Active Measuring Protocol
UMTS	univerzálny mobilný telekomunikčný systém – Universal Mobile Telecommunication System
VLAN	virtuálna lokálna sieť – Virtual Local Area Network

ZOZNAM PRÍLOH

A Výpis KPI pred konverziou	64
B Výpis KPI po konverzii	65
C Definícia základňovej stanice	66
D Vymazanie základňových staníc	69
E Obsah priloženého CD	70

A VÝPIS KPI PRED KONVERZIOU

```

Object Counter 07:00 07:15 07:30 07:45 08:00 08:15 08:30
AddedERabEstabSuccRate 100 100 100 100 100 100 100
InitialERabEstabSuccRate 100.0 100.0 100.0 100.0 100.0 87.7 100.1 99.9
InitialERabSetupSuccRate 100.0 100 100 100.0 99.9 100.0 100.0
InitialUEContextEstabSuccRate 100.0 100 100 100.0 99.9 100.0 100.0
RrcConnSetupSuccRate 100.0 100.0 100.0 100 87.8 100.1 100.0
S1SigEstabSuccRate 100 100 100 100 100 100 100
DlPacketLossDueToHo 0 0.0 0 0 0.0 0 0
DlThroughput-kbps 9785.9 12437.8 18616.9 23769.1 18933.6 31764.2 25790.5
MacHarqDlSuccRate 93.7 94.2 94.9 94.9 94.9 97.5 96.6
MacHarqUlSuccRate 93.5 93.1 93.1 91.2 89.7 93.4 93.5
RlcArqDlSuccRate 99.9 99.9 99.8 99.9 99.9 100.0 99.9
RlcArqUlSuccRate 99.3 99.2 99.7 99.7 99.0 99.5 99.5
UlPacketLoss 0.1 0.2 0.6 0.5 0.3 0.1 0.1
UlThroughput-kbps 603.3 1472.6 494.7 451.6 462.8 1331.1 1176.8
HoExecSuccRate 99.3 99.1 100 100 99.7 99.0 100
HoPrepSuccRate 100 100 100 100 97.0 100 100
MobilitySuccRate 99.3 99.1 100 100 96.8 99.0 100
ERabDrop 0.0 0.0 0.0 0.0 0.1 0.1 0.0
ERabRelAbnormalENB 0.0 0 0 0 0.0 0.0 0
ERabRelAbnormalENBCdt 0 0 0 0 0 0 0
ERabRelAbnormalENBHoExec 0 0 0 0 0.0 0.0 0
ERabRelAbnormalENBHoPrep 0 0 0 0 0 0 0
ERabRelAbnormalENBTnFail 0 0 0 0 0 0 0
ERabRelAbnormalENBUeLost 0.0 0 0 0 0.0 0 0
ERabRelMME 0.0 0.0 0.0 0.0 0.0 0.0 0.0
ERabRelNormalENB 0.0 0.0 0.0 0.0 0.0 0.0 0.0
ERabRetainability 0.0 0.0 0.0 0.0 0.0 0.0 0.0
ERabRetainabilityRate 0.0 0 0.0 0.0 0.0 0.0 0
ERabRelAbnormal 0.0 0.0 0.0 0.0 0.0 0.0 0.0
UeCtxtRelAbnormal 0.0 0 0.0 0.0 0.0 0.0 0
UeCtxtRelAbnormalENB 0.0 0 0 0 0.0 0.0 0
UeCtxtRelAbnormalENBCdt 0 0 0 0 0 0 0
UeCtxtRelAbnormalENBHoExec 0 0 0 0 0.0 0.0 0
UeCtxtRelAbnormalENBTnFail 0 0 0 0 0 0 0
UeCtxtRelAbnormalENBUeLost 0.0 0 0 0 0.0 0 0
UeCtxtRelAbnormal-2 0.0 0 0 0 0.0 0.0 0
UeCtxtRelMME 0.0 0 0.0 0.0 0.0 0 0

```

B VÝPIS KPI PO KONVERZII

```
Object Counter 12:15 12:30 12:45 13:15 13:30 13:45 14:00
AddedERabEstabSuccRate 100 100 100 100 100 100 100
InitialERabEstabSuccRate 100.0 100.0 98.5 100 99.9 100.0 99.9
InitialErabSetupSuccRate 100.0 100 100 100 100 99.9 99.9
InitialUEContextEstabSuccRate 100.0 100 100 100 100 100.0 100.0
RrcConnSetupSuccRate 100 100.0 98.7 100 99.9 100.1 100
S1SigEstabSuccRate 100 100 99.9 100 100 100 100
DlPacketLossDueToHo 0 N/A 0.0 0.0 0 0 0
DlThroughput-kbps 24037.1 N/A 13585.1 21424.3 34860.6 28067.2 14956.5
MacHarqDlSuccRate 96.8 N/A 95.5 96.1 97.6 98.0 96.5
MacHarqUlSuccRate 95.0 N/A 96.2 92.9 96.6 95.7 95.7
RlcArqDlSuccRate 100.0 N/A 100.0 100.0 99.9 100.0 100.0
RlcArqUlSuccRate 99.5 N/A 99.9 99.5 99.9 99.9 99.9
UlPacketLoss 0.1 N/A 0.1 0.1 0.0 0.1 0.0
UlThroughput-kbps 727.1 N/A 340.3 531.1 463.4 391.5 328.9
HoExecSuccRate 100 100 100 99.6 100 100 100
HoPrepSuccRate 100 100 94.8 92.6 95.7 100 100
MobilitySuccRate 100 100 94.8 92.2 95.7 100 100
ERabDrop 0.1 0.1 0.1 0.1 0.0 0.1 0.1
ERabRelAbnormalENB 0.0 N/A 0.0 0 0 0 0
ERabRelAbnormalENBCdt 0 N/A 0.0 0 0 0 0
ERabRelAbnormalENBHoExec 0 N/A 0 0 0 0 0
ERabRelAbnormalENBHoPrep 0 N/A 0 0 0 0 0
ERabRelAbnormalENBTnFail 0 N/A 0 0 0 0 0
ERabRelAbnormalENBUeLost 0.0 N/A 0 0 0 0 0
ERabRelMME 0.0 N/A 0.0 0.0 0.0 0.0 0.0
ERabRelNormalENB 0.0 N/A 0.0 0.0 0.0 0.0 0.0
ERabRetainability 0.0 N/A 0.0 0.0 0.0 0.0 0.0
ERabRetainabilityRate 0.0 0 0.0 0.0 0.0 0.0 0.0
ErabRelAbnormal 0.0 N/A 0.0 0.0 0.0 0.0 0.0
MinPerDrop 22920 N/A 33565.7 25914 44271.4 33720 22091.2
UeCtxtRelAbnormal 0.0 N/A 0.0 0.0 0.0 0.0 0.0
UeCtxtRelAbnormalENB 0.0 N/A 0.0 0 0 0 0
UeCtxtRelAbnormalENBCdt 0 N/A 0.0 0 0 0 0
UeCtxtRelAbnormalENBHoExec 0 N/A 0 0 0 0 0
UeCtxtRelAbnormalENBTnFail 0 N/A 0 0 0 0 0
UeCtxtRelAbnormalENBUeLost 0.0 N/A 0 0 0 0 0
UeCtxtRelAbnormal-2 0.0 0 0.0 0 0 0 0
UeCtxtRelMME 0.0 N/A 0 0.0 0.0 0.0 0.0
```

C DEFINÍCIA ZÁKLADŇOVEJ STANICE

```
<Site userLabel="CCL00211">
  <altitude string="0"/>
  <location string="1826 FULTON ROAD SANTA ROSA CA"/>
  <longitude string="441972389"/>
  <latitude string="138475789"/>
  <worldTimeZoneId string="ÜS/Pacific"/>
  <freeText string=/>
  <datum string="nad83"/>
</Site>
<ManagedElement sourceType="CELL0">
  <ManagedElementId string="CCL00631"/>
  <primaryType type="ÉRBS"/>
  <managedElementType types=/>
  <associatedSite string="Site=CCL00631"/>
  <nodeVersion string=/>
  <platformVersion string=/>
  <swVersion string=/>
  <vendorName string="Éricsson"/>
  <userDefinedState string=/>
  <managedServiceAvailability int="1"/>
  <isManaged boolean="true"/>
  <neMIMVersion string="É.1.220"/>
  <connectionStatus string="ÖN"/>
  <ManagedFunction>
    <functionType string="ÉNodeB"/>
    <supportSystemControl boolean="false"/>
  </ManagedFunction>
  <Connectivity>
    <DEFAULT>
      <emUrl url="http://107.100.167.202:80/em/index-stubbed.html"/>
      <ipAddress string="107.100.167.202"/>
      <oldIpAddress string=/>
      <hostname string=/>
      <nodeSecurityState state="ÖN"/>
      <boardId string=/>
      <Protocol number="0">
        <protocolType string="CORBA"/>
        <port int="0"/>
        <protocolVersion string="V2.3"/>
      </Protocol>
    </DEFAULT>
  </Connectivity>
</ManagedElement>
```

```

    <securityName string=/>
    <authenticationMethod string=/>
    <encryptionMethod string=/>
    <communityString string=/>
    <context string=/>
    <namingUrl string="http://107.100.167.202:80/nameroot.ior"/>
    <namingPort int="0"/>
    <notificationIRPAgentVersion-string="3.2"/>
    <alarmIRPAgentVersion string="3.2"/>
    <notificationIRPNamingContext
context="NOTIFICATION-IRP-VERSION-1-1"/>
    <alarmIRPNamingContext-context="ALARM-IRP-VERSION-1-1"/>
</Protocol>
<Browser>
    <browser string=/>
    <browserURL string=/>
    <bookname string=/>
</Browser>
</DEFAULT>
</Connectivity>
<Tss>
    <Entry>
        <System string="CCL00631"/>
        <Type string="SECURE"/>
        <User string="rbs"/>
        <Password string="rbs"/>
    </Entry>
    <Entry>
        <System string="CCL00631"/>
        <Type string="NORMAL"/>
        <User string="rbs"/>
        <Password string="rbs"/>
    </Entry>
</Tss>
<Relationship>
    <AssociableNode TO-FDN="FtpServer=SMRSSLAVE-LRAN-akr1e3ds1,
FtpService=aifuser"
AssociationType="ManagedElement-to-autoIntegration"/>
    <AssociableNode TO-FDN="FtpServer=SMRSSLAVE-LRAN-akr1e3ds1,
FtpService=l-back-akr1e3ds1"

```

```
AssociationType="ManagedElement-to-ftpBackupStore"/>
<AssociableNode TO-FDN="FtpServer=SMRSSLAVE-LRAN-akr1e3ds1,
FtpService=l-key-akr1e3ds1"
AssociationType="ManagedElement-to-ftpLicenseKeyStore"/>
<AssociableNode TO-FDN="FtpServer=SMRSSLAVE-LRAN-akr1e3ds1,
FtpService=l-sws-akr1e3ds1"
AssociationType="ManagedElement-to-ftpSwStore"/>
<AssociableNode TO-FDN="ManagementNode=ONRM"
AssociationType="MgmtAssociation"/>
</Relationship>
</ManagedElement>
```

D VYMAZANIE ZÁKLADŇOVÝCH STANÍC

```
<Delete>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05657,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05657"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05658,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05658"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05661,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05661"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05665,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05665"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05666,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05666"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05668,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05668"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05669,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05669"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05670,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05670"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05672,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05672"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05673,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05673"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05674,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05674"/>
<Object="SubNetwork=ONRM-ROOT-MO,MeContext=CLL05676,ManagedElement=1"/>
<Object="SubNetwork=ONRM-ROOT-MO,Site=CLL05676"/>
</Delete>
```

E OBSAH PRILOŽENÉHO CD

Priložený disk obsahuje nasledujúce položky:

- Elektronická verzia diplomovej práce.