ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta riadenia a informatiky

28360320122175

DIPLOMOVÁ PRÁCA

Študijný odbor:
Informačné systémy, 9.2.6.
Zameranie:
Informačno-komunikačné siete

Bc. Ľubomír Troják

Prototyp IMS komunikačnej platformy

IMS platform prototype

Vedúci práce: Ing. Pavel Segeč, PhD.

Reg. č. 175/2011 reg. dňa 21. 10. 2011

Žilina, 2012

ŽILINSKÁ UNIVERZITA V ŽILINE, FAKULTA RIADENIA A INFORMATIKY.

ZADANIE TÉMY DIPLOMOVEJ PRÁCE.

Študijný program : Informačné systémy

Zameranie: Informačno-komunikačné siete

Meno a priezvisko	**Osobné číslo**
Ľubomír Troják	552827

Názov práce v slovenskom aj anglickom jazyku

Prototyp IMS komunikačnej platformy

IMS platform prototype

Zadanie úlohy, ciele, pokyny pre vypracovanie (Ak je málo miesta, použite opačnú stranu)

Cieľ diplomovej práce:
Cieľom práce je štúdium, návrh a implementácia IMS platformy. Platforma bude použitá za účelom analýzy protokolov, prevádzkovaných služieb, komunikačného správania entít a experimentovania.

Obsah:
Pri riešení práce sa zamerajte:

- Architektúra a protokoly IMS subsystému z pohľadu ETSI a 3GPP.
- Prieskum, návrh a realizácia IMS komunikačnej platformy.
- Technické aspekty realizácie, systém DNS, prechod cez NAT, IPv4 a IPv6.
- Medzi doménová komunikácia.
- Mechanizmy zabezpečenia komunikácie.
- Analýza správania implementovaného riešenia a vyhodnotenie výsledkov realizácie.

Témy z predmetov študijného zamerania 5SI031: 3, 4, 5
Meno a pracovisko vedúceho DP: Ing. Pavel Segeč, PhD.
Meno a pracovisko tútora DP:

vedúci DP	tútor	vedúci katedry	garant
21.10.2011		21.10.2011	
(dátum a podpis)	(dátum a podpis)	(dátum a podpis)	(dátum a podpis)

Zadanie zaregistrované dňa 21. 10. 2011 pod číslom 175/2011 podpis

ABSTRAKT

TROJÁK, Ľubomír: *Prototyp IMS komunikačnej platformy*. [Diplomová práca] – Žilinská univerzita v Žiline. Fakulta riadenia a informatiky; Katedra informačných sietí. – Vedúci: Ing. Pavel Segeč, PhD. – Stupeň odbornej kvalifikácie: Inžinier v študijnom programe Informačné systémy. Žilina: FRI ŽU v Žiline, 2012. – 59 s.

Cieľom diplomovej práce bolo navrhnúť a implementovať prototyp IMS komunikačnej platformy založenej na základe existujúcich produktov s otvoreným zdrojovým kódom. Práca poskytuje prehľad NGN a IMS architektúry. Analyzuje otvorené riešenia vhodné pre vytvorenie IMS testovacej platformy. Tiež sa zaoberá technickými aspektmi riešenia a realizuje inštaláciu a konfiguráciu platformy. Hlavným cieľom práce je analyzovať správanie klientov a ich komunikáciu s komponentmi IMS a porovnať ju so špecifikáciou 3GPP IMS.

Kľúčové slová: NGN, 3GPP IMS, SIP, komunikačná platforma, Kamailio

ABSTRACT

TROJÁK, Ľubomír: *IMS platform prototype*. [Master's of Engineering thesis] – The University of Žilina. Faculty of Management Science and Informatics. Department of InfoComm Networks – Supervisor: Ing. Pavel Segeč, PhD. – Qualification level: Master of Engineering in the study programme Information systems. Žilina: FRI ŽU in Žilina, 2012. – 59 p.

An aim of the thesis was to design and implement IMS platform prototype, based on available open source products. Thesis provides the overview of the NGN and IMS architecture. Thesis analyzes the open source solutions suitable for the creation of an IMS testbed. It also deals with technical aspects of the solution and performs installation and configuration of the platform. Main focus is to analyze the behavior of clients and their communication with IMS components and compare it to the 3GPP IMS specifications.

Key words: NGN, 3GPP IMS, SIP, communication platform, Kamailio

PREDHOVOR

Siete novej generácie (NGN) vznikli na základe nových skutočností, ktoré nastali v oblasti telekomunikácií. Vznikla potreba konvergencie sietí, optimalizácia riadenia sietí a mimoriadny nárast digitálnej prevádzky, ktorý predstavuje rastúci dopyt po nových multimediálnych službách, po mobilite používateľov a podobne.

IP Multimedia Subsystem (IMS) poskytuje vrstvu riadenia pre NGN, ktorá poskytuje IP multimediálne služby v novom telekomunikačnom prostredí.

Práca navrhuje IMS komunikačnú platformu, ktorá bude využívaná na výskum a analýzu protokolov, komunikačného správania entít a experimentovania.

Práca predpokladá, že čitateľ disponuje aspoň základnými vedomosťami o IP (Internet Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol) protokoloch a operačnom systéme Linux.

Chcel by som sa poďakovať vedúcemu práce Ing. Pavlovi Segečovi, PhD. za cenné rady a pomoc pri spracovávaní tejto témy. Ďalej ďakujem kolegovi Bc. Marekovi Melišovi za bezproblémovú spoluprácu pri realizácii komunikačnej platformy.

V neposlednom rade chcem poďakovať mojej rodine za trpezlivosť a podporu počas tvorby tejto práce i počas celého štúdia.

OBSAH

1. ÚVOD

Myšlienka vytvorenia sietí novej generácie (NGN) vznikla snahou vytvoriť a prevádzkovať univerzálnu komunikačnú platformu ako náhradu pre paletu existujúcich sietí. Táto platforma by podporovala množstvo služieb, protokolov a prístupových technológií. Fungovala by na báze IP a poskytovala by veľké množstvo multimediálnych služieb.

Internet Protocol (IP) Multimedia Subsystem (IMS) je založený na špecifikácii protokolu SIP (Session Initiation Protocol). IMS je viac ako protokol, je to architektúra. IMS poskytuje služby reálneho času nad sieťami založenými na prepínaní paketov [1]. Pre NGN predstavuje IMS riadiacu kostru (framework), ktorá zabezpečuje poskytovanie základných služieb.

Prototypovanie a poskytovanie multimediálnych služieb alebo konceptov je náročná úloha, ktorá vyžaduje testovacie prostredie, ktoré umožní pochopenie a hodnotenie správania a vplyvu navrhovaných riešení. Čo bolo jedným z faktorov zrýchlenia adaptácie IMS [8]. Jednou z komunít, ktoré prijímajú rozvíjajúce komunikačné normy do svojich produktov sú komunity vyvíjajúce produkty s otvoreným zdrojovým kódom. Tieto komunity umožňujú vybudovať IMS testovacie prostredia, ktoré podporujú učenie modelov, služieb a vývoj komponentov. Táto práca sa zaoberá skúmaním produktov s otvoreným zdrojovým kódom, ktoré implementujú prvky IMS a umožňujú vybudovanie IMS komunikačnej platformy.

V kapitole číslo dva práca uvádza stručný pohľad na architektúru NGN a IMS. Opisuje vlastnosti a schopnosti základných komponentov IMS, protokolov a služieb, ktoré táto architektúra poskytuje.

Nasledujúca kapitola sa zaoberá prieskumom IMS komunikačných platforiem, analyzuje technické aspekty riešenia a ponúka prehľad klientov, ktorých možno využiť na pripojenie do IMS architektúry.

V štvrtej kapitole je v práci navrhnutá a realizovaná inštalácia vybranej platformy založenej na riešení Kamailio. V kapitole popisujeme konfiguráciu a spomíname potrebné technické aspekty, ktoré treba brať do úvahy pri realizácii IMS platformy. Ďalej sú v práci spomenuté problémy, ktoré nastali počas implementácie tohto riešenia.

Piata kapitola sa venuje analýze správania klientov a komponentov IMS. Skúma ich vzájomnú komunikáciu a porovnáva ju so špecifikáciou 3GPP TS 24.229.

2. ARCHITEKTÚRA A PROTOKOLY IMS

Táto kapitola stručne popisuje architektúru NGN a IMS. Prezentuje vlastnosti základných komponentov IMS, protokolov a služieb, ktoré táto architektúra poskytuje.

2.1. NGN

NGN medzinárodná telekomunikačná únia ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) definuje ako sieť [15]:

„A Next Generation Networks (NGN) is a packet-based network able to provide Telecommunication Services to users and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and services of their choice. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users.“ [ITU-T Recommendation Y.2001 (12/2004) - General overview of NGN]

Z čoho vyplývajú aj základné vlastnosti NGN definované v [15] a to, že NGN využíva paketový prenos, oddeľuje funkcie riadenia a funkcie služieb od funkcií prenosu. NGN sieť podporuje veľké množstvo služieb, aplikácií a mechanizmov založených na základných blokoch služieb. Zároveň sieť NGN poskytuje širokopásmový prenos s garantovanou koniec-koniec kvalitou služby (Quality of Service – QoS). NGN dokáže spolupracovať so staršími sieťami cez otvorené rozhrania a umožňuje všeobecnú mobilitu používateľov. Sieť poskytuje neobmedzený prístup pre používateľov k rôznym poskytovateľom služieb. Taktiež má NGN množstvo identifikačných schém, ktoré môžu byť adresované v IP za účelom smerovania v IP sieťach, nezávisle od použitých prístupových technológií. V NGN sú charakterizované unifikované služby pre služby očakávané používateľmi. Špecifikácia NGN definuje konvergované služby medzi pevnými aj mobilnými sieťami. V rámci siete sú podporované viaceré technológie poslednej míle. NGN sieť vyhovuje všetkým regulačným požiadavkám, napríklad poskytuje núdzové volania, bezpečnosť, ochranu súkromia a podobne.

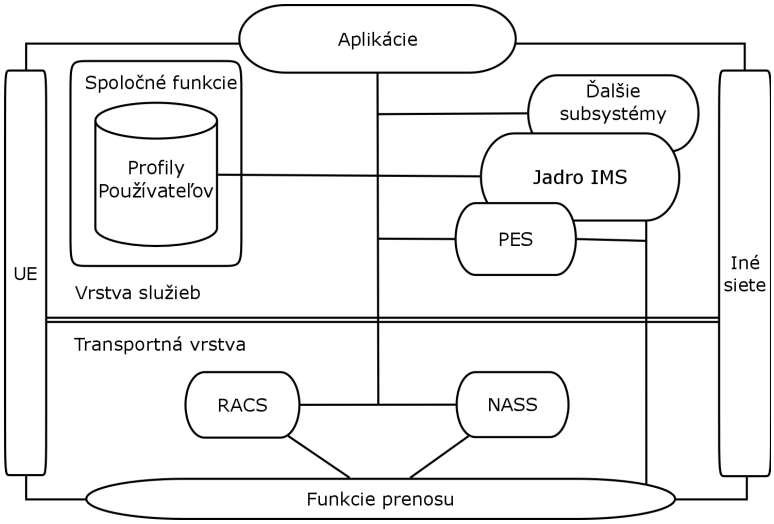
NGN architektúra je špecifikovaná odporúčaniami ITU-T (hlavne NGN Focus

Group) a ETSI (European Telecommunications Standards Institute), hlavne TC TISPAN (Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking).

Cieľom NGN je konvergencia rôznych fixných a mobilných sietí, ktorých centrálnym komponentom je IMS. Referenčná funkčná architektúra NGN je navrhnutá ako systém horizontálnych vrstiev skladajúcich sa z niekoľkých spolupracujúcich subsystémov [8]. Tento dizajn umožňuje pridávanie ďalších subsystémov a rozširovať tak hlavné funkcionality a služby. Základná NGN špecifikácia definuje transportnú vrstvu NGN a vrstvu služieb NGN (Obr. 2.1).

Transportná vrstva NGN poskytuje IP konektivitu pre NGN používateľov, označovaných ako UE (User Equipment). Zároveň skrýva použité transportné technológie prístupovej siete pod IP vrstvou.

Transportná vrstva je rozdelená na dve podvrstvy: *transport processing functions sub-layer* a *transport control sub-layer*. Podvrstva *transport processing functions sub-layer* poskytuje smerovanie a doručovanie paketov. Plní aj špecifickejšie funkcie ako je spracovanie médií, presmerovanie (relaying), prepojovanie na úrovni IP, riadenie zdrojov a podobne. Podvrstva *transport control sub-layer* poskytuje kontrolu pripojenia (napríklad adresovanie, autentifikácia prístupu, autorizácia, riadenie určovania polohy), ktorú poskytuje Network Attachment Subsystem (NASS). Funkcie zodpovedné za implementáciu procedúr, mechanizmov na manipuláciu rezervácie zdrojov (napríklad QoS, Network Address Translation (NAT)) a funkcia riadenia prístupu, sú poskytované Resource and Admission Control Subsystem (RACS) [8].



Obr. 2.1: Vrstvy NGN

Vrstva služieb NGN sa skladá z množstva subsystémov ako sú jadro IP Multimedia Subsystem (IMS), emulácia pevnej linky PSTN/ISDN emulation subsystem (PES), IPTV subsystém, ďalšie subsystémy a spoločné komponenty, ktoré navzájom zdieľajú funkcionality. Nakoniec je tu user equipment (UE) subsystém, čo je jedno alebo viacej zariadení, ktoré umožňujú používateľom prístup k sieťovým službám [8].

2.1.1. IMS

IMS bol pôvodne špecifikovaný štandardizačnou organizáciou 3rd Generation Partnership Projects (3GPP) ako vrstva služieb nad mobilnými sieťami tretej generácie (3G). Zahrňuje unikátne poskytovanie služieb na tejto platforme a umožňuje jej rýchly vývoj. IMS poskytuje bezpečnú, spoľahlivú a zúčtovateľnú infraštruktúru [11].

Riešenie 3GPP IMS zohralo ústrednú úlohu vo vývoji sietí novej generácie, zjednocovaním multimediálnych aplikácií medzi rôznymi prístupovými sieťami. Poskytuje cestu od tradičného telekomunikačného modelu, ktorý sa vyhýba rýchlemu nasadzovaniu nových stratégií [11].

ETSI TISPAN NGN prijala 3GPP IMS pre architektúru NGN sietí [8]. NGN IMS subsystém tvorí jadro IMS (Core IMS), ktoré spracováva signalizáciu (riadenie) relácií a skupina ďalších entít, napríklad aplikačných serverov (AS), entít týkajúcich sa transportu a médií (Multimedia Resource Function Processor function (MRFP) a IP Multimedia Gateway Functions (IM-MGW)), ktoré sú radené mimo jadra IMS.

IMS jadro sa skladá z viacerých entít, ako sú Call Session Control Functions (CSCF), Breakout Control Gateway Functions (BGCF), Media Gateway Control Function (MGCF), Multimedia Resource Function Controller (MRFC) a Interconnection Border Control Function (IBCF).

ETSI TISPAN a 3GPP navzájom zosúlaďujú všetky zmeny a vylepšenia potrebné pre NGN/IMS [8].

2.2. Požiadavky na architektúru

V [1] sú definované požiadavky na IMS architektúru:

- IMS relácie – používatelia môžu zapojiť hlas, video, text, zdieľanie obsahu, prezencia stavu ako súčasť ich komunikácie a majú umožnené kedykoľvek pridať, či odobrať službu.

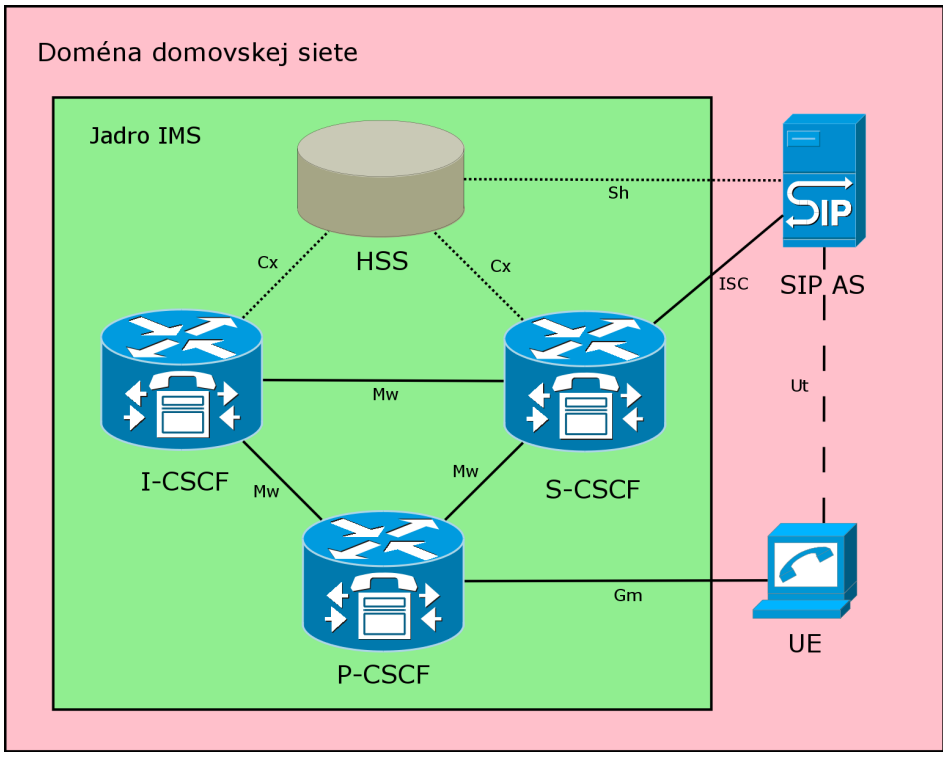
- IP konektivita – od každého UE sa vyžaduje IP konektivita.
- Zaručenie kvality služby (QoS) pre multimediálne služby.
- Kontrola prístupu – na zabezpečenie korektného použitia prostriedkov.
- Zabezpečenie komunikácie – medzi UE a IMS sieťou a komponentami IMS siete navzájom.
- Zariadiť spoplatnenie – umožniť operátorom alebo poskytovateľom služby spoplatňovať používateľov.
- Podpora roamingu – prístup pre používateľov k službám bez ohľadu na geografickú polohu. Čo je umožnené aj ak sa používateľ nenachádza v oblasti služby domovskej siete.
- Spolupráca s inými sieťami – byť schopný pripojiť do siete čo najviac používateľov bez ohľadu na druh terminálu.
- Model riadenia služby – v roamingu entity priamo interagujú s platformou umiestnenou v domovskej sieti.
- Vrstvový dizajn a nezávislosť prístupu – všetky vrstvy sú navrhnuté, aby pracovali nezávisle od prístupu do siete.

2.3. IMS entity

IMS entity môžu byť všeobecne rozdelené do šiestich kategórií [1]:

- riadenie relácie a funkcie smerovania (*-CSCF);
- databázy (HSS, SLF);
- služby (aplikačný server, MRFC, MRFP);
- funkcie vzájomnej spolupráce (BGCF, MGCF, IMS-MGW, SGW);
- podporné funkcie (PCRF, SEG, IBCF, TrGW, LRF);
- spoplatnenie.

Na nasledovnom obrázku 2.2 sú zobrazené IMS entity potrebné na poskytovanie základných služieb. Zároveň zobrazuje doménu domovskej siete operátora (home network). V prípade, že sa používateľ nachádza mimo domovskej siete, môže využiť služby roamingu a pripojiť sa zo siete iného operátora (tzv. *visited network*).



Obr. 2.2: IMS entity

Poznáme štyri rôzne druhy CSCF funkcií: Proxy-CSCF (P-CSCF), Serving-CSCF (S-CSCF), Interrogating-CSCF (I-CSCF) a Emergency-CSCF (E-CSCF). Každé plnia funkcie definované v [4]. Spoločné pre P-CSCF, S-CSCF a I-CSCF je, že zohrávajú úlohu počas registrácie, vytvárania relácie a smerovaní SIP správ.

2.3.1. Proxy Call Session Control Function (P-CSCF)

P-CSCF je prvým kontaktným bodom v rámci IMS. Čo znamená, že všetka SIP signalizácia od UE bude posielaná na P-CSCF [1]. P-CSCF sa správa ako Proxy server (definovaný v [6]), to znamená, že prijíma požiadavky a obsluhuje ich, alebo posiela ďalej. Nesmie meniť *Request URI* v SIP INVITE správe. P-CSCF sa môže správať ako User Agent (UA) (definovaný v [6]), to znamená, že môže za mimoriadnych podmietok ukončovať a samostatne vytvárať SIP transakcie [4].

V 3GPP TS 23.228 [4] sú definované nasledujúce funkcie vykonávané P-CSCF:

- Smerovať SIP register požiadavky od UE k vstupnému bodu poskytovateľa (I-CSCF) získaného z doménového mena domovskej siete poskytnutého UE.

- Smerovať SIP správy od UE k SIP serveru (napríklad S-CSCF), ktorého meno P-CSCF získalo ako výsledok registračnej procedúry.
- Zaručiť, že SIP správy prijaté od UE sú smerované k SIP serveru (S-CSCF) a obsahujú správne, alebo aktualizované informácie o type prístupovej siete aktuálne používanej UE, pokiaľ sú tieto údaje dostupné od prístupovej siete. V závislosti od politiky operátora P-CSCF môže do SIP správ (požiadaviek alebo odpovedí) vkladať získane údaje o prístupovej sieti. Taktiež pokiaľ sú informácie dostupné, môže vkladať časovú zónu UE získanú z prístupovej siete.
- Smerovať SIP požiadavky a odpovede k UE.
- Detegovať a obslúžiť tiesňové volania.
- Generovať CDR (Call Detail Record) záznamy.
- Udržiavať bezpečnostnú asociáciu medzi sebou a UE.
- Vykonávať kompresiu a dekompresiu SIP správ.
- Autorizovať nosné prostriedky a riadiť QoS.
- Detegovať a obslúžiť začínajúce alebo končiace IMS MPS (Multimedia Priority Service) požiadavky zostavenia relácie.

2.3.2. Interrogating Call Session Control Function (I-CSCF)

I-CSCF je kontaktným bodom v rámci siete operátora, určený pre všetky pripojenia účastníkov v tejto sieti. Alebo používateľov v roamingu, ktorý sa aktuálne nachádzajú v rámci oblasti služby siete operátora [4].

V sieti operátora sa môže nachádzať viacero I-CSCF. Funkcie vykonávané na I-CSCF, sú popísané v [4]:

- Pri registrácii pre používateľa, ktorý vykonáva SIP registráciu priraďovať S-CSCF, na základe zistení z HSS.
- Smerovať SIP požiadavky prijaté z inej siete k S-CSCF serveru priradenému danému používateľovi.
- Prekladať E.164 adresy, vo všetkých *Request-URI*, ktoré majú *user=phone* parameter na tel URI formát definovaný v RFC 3966, pred posielaním dotazu na HSS. Pokiaľ taký používateľ neexistuje I-CSCF preloží *Request-URI* na smerovateľný SIP URI formát.
- Získavať z HSS adresu S-CSCF obsluhujúceho používateľa, ktorého SIP URI sa

nachádza v *To* hlavičke SIP požiadavky.

- Smerovať SIP požiadavky a odpovede k S-CSCF, určeného v predchádzajúcom kroku.

2.3.3. Serving Call Session Control Function (S-CSCF)

S-CSCF je ústredným bodom IMS. Je zodpovedný za spracovanie registrácie, vykonáva smerovacie rozhodnutia, udržuje stavy relácie a ukladá Profil služieb (service profile) [1]. Keď používateľ odošle požiadavku na registráciu, tá bude smerovaná k S-CSCF, ktorý si stiahne autentifikačné údaje používateľa z HSS. Po dokončení registračnej procedúry je používateľ oprávnený zahájiť a prijímať IMS služby.

V sieti operátora, môže byť viacero S-CSCF, každý z nich môže plniť rôzne funkcionality. Funkcie vykonávané S-CSCF počas relácie sú [4]:

- Môže sa správať ako Registrar (definovaný v [6]), to znamená akceptovať požiadavky na registráciu a sprístupňuje informácie cez server určovania polohy (location server), napríklad HSS.
- Pokiaľ registračná požiadavka obsahuje *Instatnce ID* s kontaktom, ktorý je registrovaný a oznamuje podporu GRUU (Globally Routable User Agent URI), S-CSCF musí priradiť unikátne P-GRUU (Public GRUU) a nové unikátne T-GRUU (Temporary GRUU) v kombinácii s verejnou používateľskou identitou a *Instance ID*.
- Pokiaľ registračná požiadavka oznamuje podporu pre GRUU, S-CSCF musí vrátiť množinu GRUU priradenú k aktuálne registrovanému *Instance ID*.
- S-CSCF musí informovať účastníkov o zmenách v registrácii, zahŕňajúc množinu GRUU priradenú registrovanej inštancii.
- Počas registračného procesu musí S-CSCF poskytovať informácie o politike pre verejnú požívateľskú identitu. Ak sú dostupné poskytnúť ich pre P-CSCF a UE.
- Riadiť reláciu pre registrované koncové body relácií. Musí odmietnuť komunikáciu pre a od verejnej používateľskej identity, ktorá je zablokovaná (barred) pre IMS komunikáciu.
- Môže sa správať ako Proxy Server (definovaný v [6]), to znamená, že prijíma požiadavky a obsluhuje ich, alebo posiela ďalej, po prípadnom preklade.
- Môže sa správať ako User Agent (UA) (definovaný v [6]), to znamená, že môže

ukončovať a samostatne vytvárať SIP transakcie.

- Na podporu služieb určeného obsluhovaného používateľa interaguje s platformou služieb.
- Poskytuje koncovým bodom informácie o udalostiach služieb (napríklad oznamovacie správy, oznámenie o poplatkoch a podobne).
- Pre požiadavky od zdrojového zariadenia (originating endpoint) (napríklad UE):
  - Pokiaľ je cieľový používateľ zákazníkom siete iného operátora, je potrebné získať adresu vstupného bodu, kam smerovať požiadavky. Zisťuje ju na základe volaného čísla alebo SIP URI cieľového používateľa. A smeruje SIP požiadavky alebo odpovede ku vstupnému bodu.
  - Pokiaľ je cieľový aj zdrojový používateľ zákazníkom operátora tej istej siete, smeruje SIP požiadavky a odpovede na I-CSCF v rámci siete operátora.
  - V závislosti od politiky operátora, smeruje SIP požiadavky alebo odpovede inému SIP serveru, ktorý sa nachádza mimo domovskej siete operátora.
  - Smerovať SIP požiadavky alebo odpovede k BGCF pre hovory smerované do PSTN alebo do inej siete založenej na prepájaní okruhov.
  - Zabezpečiť, aby zdrojový koncový bod mal predplatenú určenú IMS komunikačnú službu.
  - Zabezpečiť, aby obsah SIP požiadavky alebo odpovede (napríklad hodnota *Content-Type* v SIP hlavičke, popis médií v SDP) prijímanej alebo posielanej zdrojovým koncovým zariadením zodpovedal učenej IMS komunikačnej službe, ktorú si predplatil.
- Ak požiadavka pochádza z aplikačného servera (AS):
  - Overiť, či požiadavky prichádzajúce z AS, sú požiadavky určené obsluhovaným používateľom. V súlade s tým uplatňuje ďalšie postupy.
  - Spracovať a postúpiť ďalej požiadavky obsluhovaného používateľa, v mene ktorého AS vygeneroval požiadavky, aj keď nie je registrovaný. Ak obsluhovaný používateľ nie je registrovaný, S-CSCF musí pred smerovaním tejto požiadavky vykonať logiku služby pre neregistrovaného pôvodcu v mene obsluhovaného používateľa.
  - Spracovať a postúpiť ďalej ďalšie požiadavky pre a od obsluhovaného používateľa v ktorého mene AS vygeneroval požiadavky.

- Zohľadniť informácie o poplatkoch pre relácie, ktoré AS vygeneroval v mene obsluhovaného používateľa.

- Pre požiadavky pre koncové zariadenia (destination endpoint) (napríklad UE):
  - Smerovať SIP požiadavky alebo odpovede k P-CSCF.
  - Modifikovať SIP požiadavky pre smerovanie prichádzajúcich relácií zo siete založenej na prepájaní okruhov.
  - Smerovať SIP požiadavky alebo odpovede k BGCF pre hovory smerované do PSTN alebo do inej siete založenej na prepájaní okruhov.
  - Zabezpečiť, aby ukončujúci koncový bod mal predplatenú určenú IMS komunikačnú službu.
  - Zabezpečiť, aby obsah SIP požiadavky alebo odpovede (napríklad hodnota *Content-Type* v SIP hlavičke, popis médií v SDP) prijímanej alebo posielanej cieľovým koncovým zariadením zodpovedal učenej IMS komunikačnej službe, ktorú si predplatil.

- Pre požiadavky obsahujúce *Request URI* v tvare E.164 adresy, sa S-CSCF pokúsi o preklad E.164 adresy na formát SIP URI. Pokiaľ bude úspešný aktualizuje *Request URI* a smeruje správu na základe neho. Ak preklad E.164 adresy zlyhá, bude požiadavka smerovaná k BGCF, aby bola smerovaná do PSTN.

2.3.4. Home Subscriber Server (HSS)

HSS je hlavným dátovým úložiskom pre všetkých účastníkov a dát IMS služieb. Obsahuje používateľské identity, registračné informácie, či prístupové parametre. Tiež obsahuje autentifikačné a autorizačné informácie, má pridelené mená S-CSCF serverov. Poskytuje špecifické požiadavky používateľov, na základe ktorých I-CSCF vyberá najvhodnejší S-CSCF server pre používateľa [1].

Používateľské identity sú dvoch druhov, privátne a verejné [1]:

- Privátne používateľské identity (private user identity) sú priradené operátorom domácej siete, aby identifikovali používateľa v sieti. Používajú sa na účely registrácie a autorizácie. Privátna identita je identifikovaná formátom NAI (Network Access Identifier), napríklad v tvare *privátny_používateľ1@home1.operator.net*. Táto identita nie je určená na smerovanie SIP správ. Býva trvalo uložená na čipovej karte, ktorú UE nie je umožnené modifikovať.

- Verejná používateľská identita (public user identity) je taká, pod ktorou môžu daného používateľa ostatní používatelia kontaktovať. Môže byť verejne publikovaná, napríklad v telefónnom zozname, na webovej stránke, či vizitke. Verejnou identitou je identifikovaná buď SIP URI (SIP Uniform Resource Identifier), napríklad: *sip:meno.priezvisko@operator.com* alebo tel URI, napríklad *tel:+421-41-1234567*. Telefónne číslo je možné uviesť aj v SIP URI formáte, napríklad *sip:+421-41-1234567@operator.com; user=phone* [2]. Minimálne jedna verejná používateľská identita býva trvalo uložená na čipovej karte, ktorú UE nie je umožnené modifikovať. Musí byť najskôr registrovaná, pred vytváraním IMS relácií. Verejnú používateľskú identitu sieť neautentifikuje počas registrácie [1].

V HSS je uložený aj Profil služieb, čo je zoznam špecifických informácií používateľa. S-CSCF sa z týchto informácií dozvie pre určenú verejnú používateľskú identitu, aký aplikačný server má byť kontaktovaný, keď používateľ prijíma alebo posiela požiadavky. Tiež môže obsahovať ďalšie inštrukcie, napríklad obmedzenia vytvorené operátorom pre používateľa, ktorý smie použiť len audio ale nie video [1].

Pokiaľ je väčší počet predplatiteľov ako kapacita jedného HSS je možné v domácej sieti umiestniť viacero HSS. V tom prípade je potrebné využiť funkciu SLF (Subscription Locator Function), ktorá poskytuje vyhľadávací mechanizmus, umožňujúci I-CSCF, S-CSCF, či AS nájsť adresu konkrétneho HSS, v ktorom sa nachádzajú dáta danej používateľskej identity [1].

2.3.5. Aplikačný server (AS)

Aplikačný server (AS) je entita, nachádzajúca sa na vrstve služieb nad IMS. AS sú entity, ktoré poskytujú pridanú hodnotu pre multimediálne služby, ako napríklad prezencia stavu. AS sa môže nachádzať v domovskej sieti operátora, alebo mimo nej ako samostatný AS [1].

Hlavné funkcie AS sú [1]:

- Schopnosť spracovávať a ovplyvňovať prichádzajúce SIP relácie prijaté z IMS.
- Schopnosť vytvárať SIP požiadavky.
- Schopnosť posielať účtovacie informácie.

AS nemusí byť čisto na báze SIP, operátor môže použiť napríklad architektútu OSA (Open Service Architecture), ktorá umožňuje využívať také funkcie ako kontrola hovorov, interakcia s používateľom, kontrola dát, vedenie účtu, zúčtovanie a podobne [1].

SIP AS je SIP server, ktorý ponúka celý rad multimediálnych služieb. Môže byť využitý napríklad na prezenciu stavu, správy, *Push-To-Talk*, alebo konferenčné služby.

Zatiaľ čo AS môže byť priradený k jednej službe, používateľ môže požadovať viacero služieb, preto môže mať jeden účastník priradených viac AS. Napríklad operátor môže mať jeden AS na riadenie prevádzky podľa želaní používateľových preferencií, a to presmerovanie prichádzajúcich hovorov do odkazovej schránky od 17:00 do 7:00. A druhý AS slúžiaci na úpravu obsahu rýchlych správ podľa veľkosti obrazovky UE, počtu farieb a podobne [1].

2.4. Protokoly IMS

IMS je špecifikované množstvom rôznych dokumentov 3GPP a ETSI. IMS využíva širokú škálu existujúcich otvorených protokolov, z ktorých väčšina je vyvíjaná IETF (Internet Engineering Task Force). Umožňujú plniť požiadavky poskytovateľov služieb a flexibilitu koncových zariadení (UE) [1].

2.4.1. SIP

Jedným z takýchto protokolov, definovanom IETF v [6], je protokol SIP (Session Initiation Protocol). SIP je určený na vytváranie, ukončovanie a modifikovanie multimediálnych spojení medzi klientmi v sieti. Napríklad telefónny hovor, videohovor alebo komunikácia pomocou správ.

SIP poskytuje možnosť pohybu používateľov medzi koncovými bodmi, môžu byť adresované viacerými menami a môžu komunikovať súčasne viacerými druhmi médií. SIP umožňuje koncovým bodom UA (User Agents) sa navzájom objaviť v sieti a dohodnúť charakteristiky danej relácie. SIP slúži na vytváranie infraštruktúry počítačov, zvaných proxy servery, ktorým UA môžu posielať registrácie, požiadavky na vytvorenie relácie a ďalšie požiadavky. SIP je univerzálny nástroj na spracovanie relácií, no zároveň nie je závislý od jej druhu.

SIP podporuje tieto aspekty vytvorenia a ukončovania multimediálneho spojenia:

- Lokalizácia používateľa – určenie koncového systému, ktorý bude použitý

na komunikáciu.

- Dostupnosť používateľa – určenie ochoty volaného zapojiť sa do komunikácie.
- Schopnosti používateľa – určenie médií a ich parametrov, ktoré budú použité.
- Nastavenie relácie – stanovenie parametrov relácie na oboch volanej aj volajúcej strane.
- Riadenie relácie – vrátane prenesenia a ukončenia relácie, modifikácie jej parametrov a vyvolania služieb.

SIP je textovo orientovaný protokol založený na HTTP (Hypertext Transfer Protocol) a SMTP (Simple Mail Transfer Protocol). Využíva rovnaký formát hlavičiek ako HTTP. Pracuje s oboma IPv4 aj IPv6 protokolmi. SIP dokáže pracovať nad protokolmi TCP, UDP, či SCTP (Stream Control Transmission Protocol).

SIP protokol používa dva druhy správ, a to požiadavky a odpovede. V [6] sú definované základné požiadavky:

- REGISTER – používa sa registráciu UA na server, určí sa aktuálna IP adresa a ochota prijímať hovory.
- INVITE – používa sa na vytvorenie multimediálneho spojenia medzi UA.
- ACK – slúži na spoľahlivé potvrdenie prijatia správy.
- CANCEL – ruší prebiehajúcu požiadavku.
- BYE – požiadavka o ukončenie spojenia.
- OPTIONS – vyžiadanie možností volaného bez uskutočnenia hovoru.

Definované odpovede SIP protokolu, ktoré sú reprezentované číselnými kódmi:

- 1xx – informačné správy – požiadavka bola doručená a je spracovávaná.
- 2xx – úspech – akcia bola úspešne doručená, porozumená a bola akceptovaná.
- 3xx – presmerovanie – ďalšia akcia je potrebná na dokončenie požiadavky.
- 4xx – chyba na strane klienta – požiadavka má chybnú syntax, alebo nemôže byť splnená na serveri.
- 5xx – chyba na strane servera – server zlyhal pri plnení platnej požiadavky.
- 6xx – globálne zlyhanie – požiadavku nie je možné splniť na žiadnom serveri.

2.4.2. Rozšírenia SIP pre IMS

IETF definuje rôzne rozšírenia pre protokol SIP. Napríklad pre zlepšenie spoľahlivosti siete bolo vytvorené RFC 3262, ktoré definuje metódu PRACK (Provisional Response ACKnowledgement), ktorá je posielaná ako odpoveď na informačné správy 1xx.

Pre IMS protokol SIP predstavoval mnoho technologických problémov [26]. Preto bolo potrebné prekonať množstvo nedostatkov medzi pôvodným SIP definovaným IETF v [6] a funkciami potrebnými pre plnú podporu IMS. Pre vyriešenie tohto problému 3GPP definuje desiatky SIP rozšírení, ktoré dodávajú špecifiká pre IMS sieť. Rozšírenia SIP používané v IMS sú definované v štandarde 3GPP TS 24.229 [5].

Hlavné rozšírenia SIP použité v IMS sú [26]:

- SigComp (RFC 3320) – toto rozšírenie definuje kompresiu textových dát SIP správ, ktoré môžu byť veľmi veľké a problematicky prenášané, čo spôsobuje oneskorenie.
- P-headers (RFC 3455 a 3325) – k štandardným SIP hlavičkám pridáva ďalšie, ktoré riešia špecifické problémy IMS siete.
    - RFC 3455 definuje tieto hlavičky:
        - *P-Associated-URI* hlavička – používaná v správe 200 OK ako odpoveď na správu REGISTER. Obsahuje zoznam URI asociovaných s daným UE.
        - *P-Called-Party-ID* hlavička – posielaná pri INVITE správe, obsahuje *Request-URI* volaného používateľa.
        - *P-Visited-Network-ID* hlavička – obsahuje identifikátor siete, v ktorej sa používateľ nachádza, aby v domácej sieti bolo možné identifikovať, že je používateľ mimo domovskej siete, t. j. v roamingu.
        - *P-Access-Network-Info* hlavička – obsahuje informáciu o prístupovej sieti UE, slúži na optimalizáciu služieb.
        - *P-Charging-Function-Addresses* hlavička – využíva sa pri účtovaní, obsahuje adresy funkcií Charging Collection Function (CCF) a Event Charging Function (ECF).
        - *P-Charging-Vector header* hlavička – využíva sa pri účtovaní, obsahuje zozbierané účtovacie informácie.
    - RFC 3325 definuje nasledovné hlavičky:
        - *P-Asserted-Identity* hlavička – obsahuje identitu používateľa odosielajúceho

SIP správy, ktorá bola overená pri autentifikácii.

        - *P-Preferred-Identity* hlavička – obsahuje identitu (SIP URI) používateľa posielajúceho SIP správy, ktorú si želá overiť a následne použiť v hlavičke *P-Asserted-Header*.
- Security Agreement (RFC 3329) – špecifikuje, ako dohadovať bezpečnostné možnosti pre viacero koncových zariadení.
- AKA-MD5 (RFC 3310) – určuje ako sú terminály a siete overované pomocou definovaných mechanizmov, tiež definuje konkrétne výmeny kľúčov.
- IPSec [18] – popísaný v kapitole 3.2.6.
- Media Authorization (RFC 3313) – zabezpečuje, že budú využívané len autorizované mediálne zdroje.
- Mobile Registration (RFC 3327 a 3608) – definuje syntax a použitie SIP *Path* a *Service-route* hlavičiek.
    - *Path* hlavička – poskytuje mechanizmus na rozlíšenie medzi viacerými proxy vyskytujúcimi sa v sieti. Používa sa v REGISTER požiadavke na nájdenie a zaznamenanie poradia proxy serverov pre ďalšiu komunikáciu.
    - *Service-Route* hlavička – používa sa v odpovedi na REGISTER požiadavku. Poskytuje možnosť oznámiť UA trasu k službám (service route), na ktorej môže požadovať služby.
- Reg-event Package (RFC 3680) – využívaný terminálmi a P-CSCF na zistenie stavu registrácie.
- Preconditions (RFC 4032) – špecifikuje spôsob dohadovania QoS, zabezpečenia a ďalšieho správania volania medzi dvoma terminálmi.
- IMS Resource Reservation (RFC 3312) – definuje ako robiť rezervácie zdrojov pre hovory alebo relácie.

2.4.3. SDP

Na popísanie parametrov relácie sa používa ďalší protokol a to SDP (Session Description Protocol) [10]. Popisuje napríklad typ média, transportný protokol, typ kodeku alebo prenosovú rýchlosť. Média môžu byť pridané alebo odobrané aj z existujúcej relácie.

Pri začatí multimediálnych telekonferencií, VoIP hovorov, odosielaní video toku, alebo ďalších relácií je tu požiadavka na sprostredkovanie detailov o médiu, transportnej

adrese a ďalších metadát popisujúcich reláciu účastníkom.

SDP poskytuje štandardnú reprezentáciu informácií, bez ohľadu na to, ako sú informácie prenášané. Popisuje výlučne formát relácie, nezahrňuje transportný protokol, je určený na použitie transportného protokolu podľa potreby.

Je navrhnutý na všeobecné použitie tak, aby mohol byť použitý v celej rade sieťových prostredí a aplikácií. V IMS sieti je nesený vo vnútri SIP správ.

Popis relácie obsahuje nasledovné informácie o médiu [10]:

- Typ média – napríklad video, audio a podobne.
- Transportný protokol – RTP, UDP, IP a podobne.
- Formát média – MPEG video, G.711 audio a podobne.
- Informácie o adrese a porte
  - IP multicast relácie – adresa multicast skupiny a jej port.
  - IP unicast relácia – vzdialená adresa pre médium a jej port.

2.4.4. Diameter

Diameter je protokol určený na AAA (authentication, authorization, accounting), teda na autentifikáciu, autorizáciu a účtovanie. Diameter je následníkom protokolu Radius.

Protokol Diameter pridáva ďalšie vlastnosti, ktoré vyplynuli z rastu internetu a príchodu nových prístupových technológií, vrátane bezdrôtového prístupu, DSL, či mobilného internetu. Zahrňuje [7]:

- Zotavenie – poskytuje potvrdzovanie na úrovni aplikačnej vrstvy a definuje algoritmy na zatavenie pri zlyhaní a s tým súvisiaci stavový automat.
- Bezpečnosť prenosu – podpora IPsec je povinná a podpora TLS je voliteľná.
- Spoľahlivý prenos – oproti protokolu Radius, ktorý beží nad UDP, podporuje spoľahlivé protokoly ako napríklad TCP alebo SCTP.
- Podpora agentov – definuje explicitne správanie pre agentov, zahŕňajúc *Proxy, Redirect* a *Relay.*
- Overiteľnosť – implementuje bezpečnostné mechanizmy, ktoré umožňujú overiť pravosť prichádzajúcich paketov.
- Podpora prechodu – umožňuje spätnú kompatibilitu s Radius protokolom, aby bolo možné nasadzovať postupne nové zariadenia pri prechode na nový protokol.
- Dohadovanie schopností – diameter podporuje spracovanie chybových správ,

dohadovanie schopností medzi klientom a serverom, a podporu párov atribút-hodnota, ktoré môžu byť voliteľné alebo povinné.

- Objavovanie a konfigurácia zariadení – pomocou DNS umožňuje dynamicky objavovať zariadenia a odľahčiť tak manuálnu konfiguráciu mien alebo adries.
- Podpora roamingu – poskytuje explicitnú podporu pre mimo doménový roaming.

Diameter poskytuje nasledujúce možnosti [2]:

- pripojenie a riadenie relácií,
- autentifikácia používateľov a možnosť dohadovania parametrov,
- spoľahlivé doručenie párov atribút-hodnota,
- rozšíriteľnosť o pridanie nových príkazov a párov atribút-hodnota,
- základné účtovacie služby.

Všetky dáta nesené týmto protokolom sú doručované v páre atribút-hodnota, ktoré sú definované samotným protokolom Diameter. Alebo môže niesť dáta súvisiace s konkrétnou aplikáciou. Takýto prístup umožňuje jeho ďalšie rozširovanie [7].

2.4.5. Využitie protokolov

Entity v IMS sieti komunikujú cez definované rozhrania a na komunikáciu využívajú spomínané protokoly. Rozhrania a použitý protokol sú zobrazené aj na obr. 2.2.

V nasledovnej tabuľke 2.1 uvádzame prehľad využitia IETF protokolov v IMS komunikačnej sieti.

Meno rozhrania	IMS entity	Protokol
Gm	UE <-> P-CSCF	SIP
Mw	P-CSCF, I-CSCF, S-CSCF	SIP
ISC	S-CSCF <-> AS	SIP
Ma	I-CSCF <-> AS	SIP
Cx	(I-CSCF, S-CSCF) <-> HSS	Diameter
Sh	AS <-> HSS	Diameter
Mm	(I-CSCF, S-CSCF) <-> externá IP sieť	SIP
Ut	UE <-> AS	HTTP

Tab. 2.1: Využitie protokolov [1]

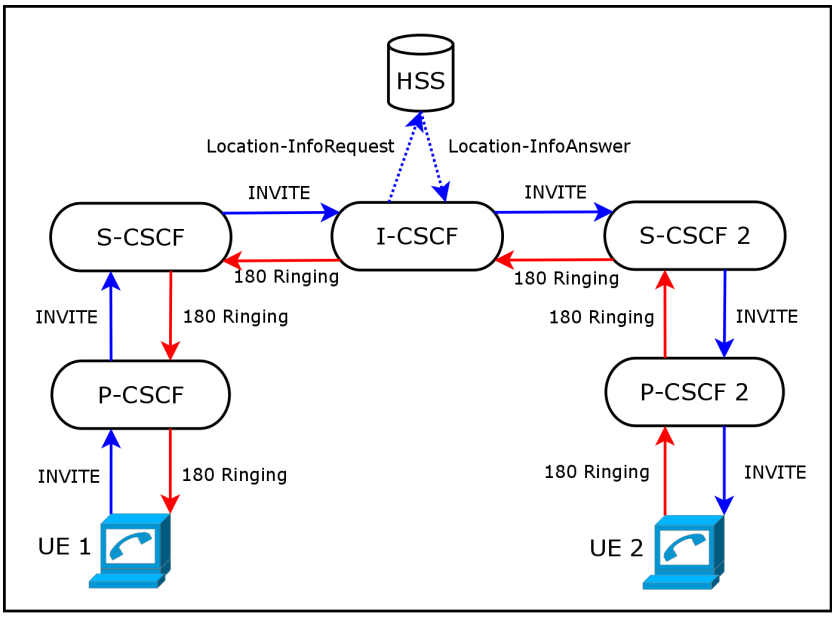
2.5. Služby

IMS komunikačná platforma poskytuje používateľom rôzne multimediálne služby. Medzi najzákladnejšie patria hlasový a video hovor, prezencia stavu a posielanie rýchlych textových správ.

2.5.1. Hlasové a video služby

Služba hlasového hovoru poskytuje možnosť vytvorenia SIP relácie, pomocou ktorej umožní prenos hlasovej komunikácie medzi dvoma UE.

Na obrázku 2.3 je znázornený tok signalizácie správy INVITE v rámci IMS komunikačnej siete.



Obr. 2.3: Tok správ signalizácie hovoru

INVITE správa sa používa na začatie hovoru pomocou SIP signalizácie. UE 1 posiela túto správu na svoj P-CSCF. UE 1 na ňu dostáva informačnú odpoveď 100 TRYING. Taktiež všetky IMS entity touto správou potvrdzujú prijatie INVITE správy. P-CSCF server INVITE správu pošle na S-CSCF obsluhujúci volajúce UE 1, ktorého adresu sa dozvedel počas registrácie UE 1. S-CSCF pošle správu na I-CSCF (adresu ktorého zistí cez DNS z doménového mena daného poskytovateľa podľa SIP adresy volaného), ktorý musí v databáze HSS vyhľadať S-CSCF server, obsluhujúci volané UE 2. Vykonáva to pomocou Diameter správy *Location-Info-Request*, odpoveď dostane v správe *Location-Info-Answer*. Podľa získanej adresy doručí správu na S-CSCF 2 volaného UE 2. S-CSCF 2

správu doručí proxy serveru P-CSCF 2 a ten volanému UE 2. Pokiaľ je prihlásený a je ochotný prijímať hovory, UE 2 odošle o tom informačnú správu 180 Ringing P-CSCF 2 serveru a začne oznamovať túto udalosť používateľovi napríklad zvonením. P-CSCF 2 server doručí správu 180 volanému UE 1 spätne po trase ako je to znázornené na obrázku 2.3. Pokiaľ sa volaný používateľ na UE 2 rozhodne prijať hovor, odošle potvrdzujúcu správu 200 OK. Volaný UE 1 na správu 200 OK odpovie správou ACK.

Hlasový a video hovor, je z pohľadu signalizácie je totožný. Rozdiel je v SDP správe, kde k záznamu `m=audio 23004 RTP/AVP 0 8 14 101` a vymenovanými podporovanými audio kodekmi pridá napríklad záznam `m=video 23008 RTP/AVP 34 96 32 97` spolu s podporovanými video kodekmi.

2.5.2. Presence

Prezencia stavu (presence) je služba, ktorá poskytuje možnosť riadiť informácie o dostupnosti používateľských zariadení, služieb alebo služieb médií. Jej obsluha pre IMS je definovaná v špecifikácii 3GPP TS 23.141.

Prezencia stavu môže obsahovať [1]:

- dostupnosť terminálu a používateľa,
- preferencie komunikácie,
- možnosti terminálu,
- polohu,
- aktuálne dostupné služby.

Prezenciu stavu vykonáva Presence server (PS), čo je SIP AS, ktorý je popísaný v kapitole 2.3.5. PS dokáže spracovávať PUBLISH (RFC 3903), SUBSCRIBE a NOTIFY (RFC 3265) požiadavky od UA.

Informácie o prezencii stavu sú obsiahnuté v zozname zdrojov (resource list), čo je XML (eXtensible Markup Language) dokument. Klient môže odoberať zoznam zdrojov, ktorý je uložený v RLS (Resource List Server). Je mu to umožnené cez XCAP (XML Configuration Access Protocol) protokol. XCAP server ho poskytuje cez URI. Napríklad *http://presence.exapmle.com:8080/xcap-root*.

Prihlásiť sa k odberu zoznamu zdrojov môže používateľ pomocou správy SUBSCRIBE. Následne ho PS informuje správou NOTIFY o prezencii stavu používateľov,

ktorých zoznam zdrojov odoberá. Používatelia svoju prezenciu stavu a jej zmeny informujú PS správami PUBLISH.

Klient si môže uložiť dáta v sieti, aby ich nemusel nastavovať na každom z jeho zariadení. Napríklad zoznam kontaktov a skupín, históriu chatu a hovorov. Tieto informácie vrátane iných možností pre klienta, ako je presmerovanie hovorov, dostupnosť a preferencie terminálov podľa rôznych druhov komunikácie sú uložené na XDM (Xml Document Management) serveri a sú konfigurované cez XCAP protokol [3].

2.5.3. Textové služby

Textové služby umožňujú komunikáciu pomocou rýchlych správ (Instant Messaging – IM). Mechanizmus IM pre IMS je definovaný v 3GPP TS 24.247. Kde sú popísané metódy a funkcie ako má systém obsluhovať page-mode a session-mode IM [3].

2.5.3.1. Page-mode

Page-mode je starší spôsob posielania IM správ fungujúci podobne ako SMS (Short Message Service). Posielať umožňuje jednu správu. Teda je vhodný na jednoduché odkazy.

Vykonáva sa pomocou SIP správy MESSAGE. S-CSCF by mal túto správu doručiť aplikačnému serveru (AS) na spracovanie. Ten by mal rozhodnúť, či správu je možné doručiť, a ku akému koncovému zariadeniu. Prijímacie zariadenie musí mať registrovanú podporu pre MESSAGE v HSS. Pokiaľ správu nie je možné doručiť hneď, môže sa doručenie odložiť na neskôr.

Odpoveď oznamujúca správne doručenie je 200 OK. Pokiaľ by sa AS rozhodol rozvetviť správu na viacero koncových zariadení, odpovie stále iba jednou potvrdzujúcou správou.

2.5.3.2. Session-mode

Session-mode je to univerzálny spôsob na vykonávanie textovej komunikácie. Používa chatovaciu reláciu medzi dvoma účastníkmi. Vytvára sa pomocou SIP relácie medzi oboma koncovými zariadeniami. Obaja sú prepojený priamo, takže veľa posielaných správ nezaťažuje servery signalizáciou, čo je výhodou oproti page-mode.

Na IM konverzácie sa v Session-mode využíva protokol MSRP (Message Session Relay Protocol) bežiacim nad TCP. Tento dialóg je veľmi podobný hlasovému dialógu, len namiesto RTP prúdu je použitý MSRP prúd.

3. IMS KOMUNIKAČNÁ PLATFORMA

Pred samotnou realizáciou komunikačnej platformy bolo potrebné vykonať prieskum existujúcich produktov s otvoreným zdrojovým kódom, ktoré poskytujú možnosť nasadenia a otestovania IMS platformy.

3.1. Prieskum implementácií

Profesionálne riešenie komunikačnej platformy by sme mohli zveriť do rúk špecializovanej firmy. Väčšinou sú to uzavreté implementácie, ku ktorým nemáme prístup. V našom riešení chceme použiť voľne dostupné riešenie s otvoreným zdrojovým kódom (open source). Tieto požiadavky spĺňajú nasledovné implementácie.

3.1.1. Open IMS Core

Fraunhofer Institute for Open Communication Systems (FOKUS) vyvíjal jadro (core) IMS systému na účely výskumu a vývoja a založil Open IMS testovaciu platformu (testbed) – miesto na testovanie IMS [11]. Je nasadená v oblasti testovania otvorených technológií, ktorých cieľom je vytváranie a overovanie existujúcich a vznikajúcich NGN/IMS štandardných komponentov.

Nápad založiť Open Source IMS riešenie vznikol zo skúseností inštitútu FOKUS, ktoré získali pri vývoji produktu SIP servera SER (SIP Express Router). SER bol vyvíjaný mnoho rokov ako SIP server s otvoreným zdrojovým kódom, ktorý je založený na voľnej licencii GPL (GNU Public License). Bol tak umožnený jeho rýchly výskum a vývoj. Táto implementácia IMS je práve založená na základoch riešenia SER [11].

Open Source jadro IMS systému nie je určené na komerčné použitie. Jeho účelom je poskytnúť IMS ako základnú referenčnú implementáciu. A umožniť tak možnosť otestovať technológiu a vývoj prototypov aplikácií, typicky v IMS testovacej platforme.

University of Cape Town (UCT) a FOKUS spolu založili akademickú spoluprácu v rámci rozvoja IMS. UCT umiestnila IMS platformu v Juhoafrickej republike s cieľom prepojenia na testovacie miesto Open IMS v Nemecku. Na UCT bol vyvinutý UCTIMSClient, ktorý bol navrhnutý špeciálne pre túto architektúru.

Open Source IMS Core sa skladá z CSCF funkcií, konkrétne P-CSCF, I-CSCF a S-CSCF a servera HSS [19].

3.1.2. Kamailio IMS

Túto implementáciu popisuje spoluzakladateľ projektu Kamailio [20] na svojom blogu [12]. Na konci roku 2010 čoraz viac ľudí malo záujem o IMS a jeho rozšírenie pre Kamailio. Aktuálna sprístupnená verzia je nad verziou Kamailio 3.1.1. Tvorcovia projektu pracujú na novšej verzii, ktorá by poľa odhadov mala byť uvoľnená v júni až júli 2012, pravdepodobne spolu s verziou Kamailio 3.3.0.

Veľkou výhodou pre firmy, ktoré chcú IMS používať, je možnosť za nízke náklady otestovať, čo im táto platforma prinesie. Hoci IMS rozšírenia boli dlho prístupné cez projekt OpenIMSCore, teraz vďaka riešeniu Kamailio sú k dispozícii na vrchole jedného z veľmi stabilných a populárnych VoIP systémov. Rozšírenia IMS sú dodávané ako samostatné moduly, preto stabilitu Kamailio nenarušia.

Okrem hlasových služieb Kamailio, ktoré je jadrom IMS riešenia, ponúka aj doplnkové služby ako napríklad prezencia stavu a IM, ktoré sú jednoducho dostupné aj pre túto platformu.

Výhody IMS rozšírenia nad Kamailio [12]:

- Ponúka otvorený, voľne dostupný systém, ktorý môže ktokoľvek vyskúšať pred tým, ako sa rozhodne investovať do profesionálneho riešenia.
- Umožňuje prístup k stovkám RTC (Real-Time Communication) rozšíreniam, napríklad služby IM, chat, telekonferencie, videokonferencie a podobne.
- Poskytuje služby nad rámec hlasu.
- Podporuje zabudované skriptovacie jazyky, napríklad Lua, Perl alebo Python.
- Má otvorený zdrojový kód, neuzatvorené obchodné prostredie, s množstvom firiem, ktoré sú ochotné ponúknuť profesionálne poradenské služby.

Kamailio IMS riešenie ponúka servery Proxy-CSCF, Interrogating-CSCF, Serving-CSCF a Home Subscriber Server – HSS. Posledný menovaný databázový server je prevzatý celý z riešenia OpenIMScore.

3.1.3. Výber

Pre našu komunikačnú platformu sme sa rozhodli využiť implementáciu Kamailio IMS. Je pokračovateľom projektu OpenIMSCore a jeho vývoj stále napreduje.

Kvalita tohto projektu bola ocenená ITSPA Awards 2012 [21], za skupinu Open

Source VoIP Projects, zastupujúcu Kamailio/SER, Asterisk a FreeSwitch, ktoré sa používajú na vytváranie veľkých VoIP systémov a poskytujú širokú škálu služieb.

3.2. Technické aspekty realizácie

Nasadzovaná komunikačná platforma bude zahŕňať nasledovné technické aspekty.

3.2.1. Komponenty IMS

Pre našu komunikačnú platformu bolo potrebné vybrať servery, ktoré budú zabezpečovať základné služby, potrebné pre účely tejto práce.

Je potrebné použiť tri entity CSCF, konkrétne P-CSCF, S-CSCF a I-CSCF. Tiež databázový server HSS. Keďže naša platforma nepredpokladá masové využívanie, kde jej primárnym nasadením bude výskumný a vzdelávací proces Katedry informačných sietí FRI, odporúčame nasadiť len jeden databázový server. Z tohto dôvodu nie je SLF server potrebný.

Pre potreby testovania pokročilých služieb sme sa rozhodli implementovať aj aplikačný server, no vzhľadom na šetrenie zariadeniami je zlúčený so serverom HSS. Čo bolo možné aj preto, že HSS nemá vlastnú Kamailio inštanciu. Ako aplikačný server sme zvolili PS (presence server), ktorý nám zabezpečuje aktuálna verzia Kamailio 3.2.0. Návrhom a implementáciou PS sa zaoberá kolega vo svojej diplomovej práci s názvom *Riešenia komunikačných platforiem pre služby SIMPLE*.

3.2.2. DNS

DNS (Domain Name System) je hierarchický distribuovaný zoznam, ktorý mapuje doménové mená na IP adresy. Na účely lokalizácie zariadení a služieb po celom svete. Slúžia na to DNS servery s hierarchickou štruktúrou. Tento protokol je popísaný v [16].

Používateľom stačí vedieť meno servera, nemusia poznať jeho adresu, ktorá je takto oddelená od jeho trvalého identifikátora. V rámci lokalizácie SIP služieb používatelia môžu mať identifikátor *používateľské.meno@doména* zhodný s tým, ktorý používajú napríklad na email: *mailto:Janko.Hraško@uniza.sk* a *sip:Janko.Hraško@uniza.sk*.

Lokalizačné služby pre SIP sú definované v RFC 3263, ktoré popisuje ako je umožnené klientom prekladať SIP URI (Uniform Resource Identifier) na IP adresu, port a transportný protokol, na ktoré majú posielať SIP požiadavky. Pre tieto účely nám DNS poskytuje dva druhy zdrojových záznamov (Resource Record - RR): SRV a NAPTR.

SRV (Service) záznam je špecifikovaný v RFC 2782, ktorý umožňuje klientovi cez DNS lokalizovať server ponúkajúci danú službu. SRV RR má nasledovný formát:

```
_Service._Proto.Name TTL Class SRV Priority Weight Port Target
```

Príklad využitia pre SIP:

```
_sip._udp.uniza.sk 43200 IN SRV 10 10 5060 sipserver.uniza.sk.
```

Tento záznam klientovi poskytne nasledovné informácie: *Služba (Service)* je SIP, *transportný protokol (Proto.Name)* je UDP, kde môže byť aj TCP, SCTP či TLS. Možnosť ponechať vo vyrovnávacej pamäti *(TTL)* na 12 hodín (43 200 sekúnd). *Trieda (Class)* je IN (Internet), typ záznamu SRV. *Priorita (Priority)* je 10, v prípade viacerých záznamov sú nižšie hodnoty dopytované ako prvé.

Váha (Weight), tu 10, sa pri viacerých záznamoch s rovnakou prioritou určuje proporčne, ako často budú dané záznamy dopytované. Vyššie hodnoty sú dopytované častejšie. Napríklad *váha* 20 by bola dopytovaná dva krát častejšie ako 10. *Port* je 5060.

C*ieľ (Target)* je plne kvalifikované doménové meno FQDN (Fully qualified domain name) servera, teda *sipserver.uniza.sk*, v DNS ukončované bodkou.

Ďalším záznamom je NAPTR (Name Authority Pointer), ktorý je definovaný v RFC 3263. Poskytuje mechanizmus, ktorý pre danú doménu špecifikuje, aký transportný protokol je preferovaný v rámci SIP požiadavky.

NAPTR má nasledovný tvar:

```
domain-name TTL Class NAPTR order preference flags service regexp target
```

Napríklad:

```
uniza.sk. IN NAPTR 60 50 "s" "SIP+D2U" "" _sip._udp.uniza.sk.
```

Tento záznam bude použitý pri prihlasovaní *sip:Janko.Hraško@uniza.sk*, kde sa nájde zhoda podľa *doménového mena (domain-name) uniza.sk*. *Životnosť záznamu (TTL)* je 12 hodín, *trieda (Class)* je IN, typ záznamu NAPTR. *Poradie (order)* je 60 a *preferencia (preference)* 50. Ich význam je odlišný od polí v SRV zázname. Taktiež nižšie hodnoty

majú vyššiu prioritu. *Poradie* určuje poradie, v akom sa budú záznamy čítať.

Ak sú ostatné polia zhodné, prejde sa na rozhodovanie podľa *preferencie*. Nižšie hodnoty majú vyššiu prioritu, ale volajúce strany môžu potlačiť preferencie volanej domény a vybrať si vyššiu hodnotu.

Príznak (flag) je *„s“* v tomto prípade špecifikuje, že všetky informácie treba hľadať vo vhodnom SRV zázname v *regxp* alebo *cieľ* poli. *Služba (service)* je SIP+D2U, čo znamená SIP protokol cez UDP. Možno definovať SIP+D2T (SIP cez TCP), SIP+D2S (SIP cez SCTP) a SIPS+D2T (SIP cez TLS cez TCP).

Použitý môže byť len jeden z *regxp* (regular expression – regulárny výraz) a *cieľ (target)*, druhý musí ostať prázdny. V tomto prípade je *cieľ _sip._udp.uniza.sk*.

NAPTR záznamy nie sú nevyhnutné, no ak sú použité, odporúča sa poradie SIPS+D2T, SIP+D2T a SIP+D2U.

Klient najprv posiela DNS NAPTR požiadavku na požadovanú doménu získanú z *Request-URI* SIP požiadavky. Podľa poradia a preferencie vyberie príslušný NAPTR záznam a pošle na adresu zo záznamu požiadavky DNS SRV a následne DNS A, pokiaľ ich DNS server neposlal v *additional section* časti odpovede NAPTR. Ak klient nedostane v odpovedi žiaden NAPTR záznam, vyskúša poslať DNS SRV požiadavku, ak dostane odpoveď podľa potreby pošle DNS A požiadavku a následne môže poslať SIP požiadavku na získanú IP adresu preferovaného SIP proxy servera. Ak nie je úspešný ani so SRV, tak posiela DNS A požiadavku s doménou zo SIP požiadavky. Ak dostane platnú IP adresu, posiela požiadavku cez UDP [16].

Pre návrh platformy pokrývajúci touto prácou bola pridelená doména *ims3.sip.uniza.sk*. V rámci nej boli serverom priradené nasledovné IP adresy:

Server	IPv4 (A)	IPv6 (AAAA)
pcscf2	158.193.139.22	2001:4118:300:122:7056:5dff:fe0e:b144
scscf2	158.193.139.23	2001:4118:300:122:8450:a3ff:fe65:8379
pcscf	158.193.139.25	2001:4118:300:122:8401:52ff:fe4c:484e
icscf	158.193.139.26	2001:4118:300:122:b89a:acff:fea9:db9a
scscf	158.193.139.27	2001:4118:300:122:2ca1:5dff:fef8:8430
hss/presence	158.193.139.28	2001:4118:300:122:a0d1:c5ff:fe28:cf34

Tab. 3.1: Priradenie IP adries severom

Konfiguračný súbor DNS pre doménu *ims3.sip.uniza.sk* vyzerá nasledovne:

```
$ORIGIN ims3.sip.uniza.sk.

@               NAPTR 10 100 "S" "SIP+D2T"  "" _sip._tcp.pcscf
@               NAPTR 20 100 "S" "SIP+D2U"  "" _sip._udp.pcscf
@               NAPTR 10 100 "S" "SIP+D2T"  "" _sip._tcp.pcscf2
@               NAPTR 20 100 "S" "SIP+D2U"  "" _sip._udp.pcscf2

pcscf             IN      A       158.193.139.25
pcscf             IN      AAAA    2001:4118:300:122:8401:52ff:fe4c:484e
_sip.pcscf        IN      SRV 0 0 5060 pcscf
_sip._udp.pcscf   IN      SRV 0 0 5060 pcscf
_sip._tcp.pcscf   IN      SRV 0 0 5060 pcscf
_sips._tcp.pcscf  IN      SRV 0 0 5061 pcscf
pcscf2            IN      A       158.193.139.22
pcscf2            IN      AAAA    2001:4118:300:122:7056:5dff:fe0e:b144
_sip.pcscf2       IN      SRV 0 0 5060 pcscf2
_sip._udp.pcscf2  IN      SRV 0 0 5060 pcscf2
_sip._tcp.pcscf2  IN      SRV 0 0 5060 pcscf2
_sips._tcp.pcscf2 IN      SRV 0 0 5061 pcscf2
icscf             IN      A       158.193.139.26
icscf             IN      AAAA    2001:4118:300:122:b89a:acff:fea9:db9a
_sip              IN      SRV 0 0 5060 icscf
_sip._udp         IN      SRV 0 0 5060 icscf
_sip._tcp         IN      SRV 0 0 5060 icscf
scscf             IN      A       158.193.139.27
scscf             IN      AAAA    2001:4118:300:122:2ca1:5dff:fef8:8430
_sip.scscf        IN      SRV 0 0 5060 scscf
_sip._udp.scscf   IN      SRV 0 0 5060 scscf
_sip._tcp.scscf   IN      SRV 0 0 5060 scscf
scscf2            IN      A       158.193.139.23
scscf2            IN      AAAA    2001:4118:300:122:8450:a3ff:fe65:8379
_sip.scscf2       IN      SRV 0 0 5060 scscf2
_sip._udp.scscf2  IN      SRV 0 0 5060 scscf2
_sip._tcp.scscf2  IN      SRV 0 0 5060 scscf2
hss               IN      A       158.193.139.28
hss               IN      AAAA    2001:4118:300:122:a0d1:c5ff:fe28:cf34
presence          IN      CNAME   hss
```

Tento DNS záznam umožňuje napríklad UE zistiť podporovaný transportný protokol a adresu servera, na ktorý má posielať SIP požiadavky, pokiaľ to UE podporuje. Tiež umožňuje vyhľadanie vstupného bodu do domény, ktorým je I-CSCF.

3.2.3. Prechod cez NAT

V dôsledku pridanej kompatibility IMS pre IPv4 siete, je potrebné sa vysporiadať s prechodom cez NAT (Network Address Translator), nakoľko existujú používatelia, ktorí nemajú prístup na internet s verejnou IP adresou. Vychádzame z predpokladu, že pri IPv6 je momentálne definovaná plná globálna konektivita. V prípade pridania funkcionality NAT aj pre IPv6 by bolo tento problém potrebné riešiť.

Problém prechodu cez NAT spôsobuje fakt, že SIP a SDP nie sú navrhnuté *NAT friendly* [9]. SIP nedodržuje odporúčanie, aby aplikačné protokoly nepoužívali IP adresy a čísla portov vo svojich aplikačných správach. Tento fakt v prípade prechodu SIP cez NAT spôsobuje problémy. Napríklad SIP správa INVITE obsahuje privátnu adresu v dôležitých

hlavičkách *Via:* a *Contact:* a v obsahujúcom SDP poli *c=*, preto správy a RTP prúd nemôžu byť správne doručované.

Prechod cez NAT je možné riešiť nasledovnými metódami:

- RTPproxy je to vysokovýkonný *media relay* softvér pre SIP proxy server slúžiaci na spracovanie RTP prúdu (stream) [13]. Pôvodne bol navrhnutý na umožnenie komunikácie SIP klientov za NAT. Existujú však prípady, kedy nemôže byť priame spojenie dvoch klientov možné, a musia byť presmerované cez iný server. RTPproxy sa dá využiť aj na tieto účely, ako *relay* server. Neskôr boli pridané ďalšie funkcionality, vďaka ktorým sa stáva neodmysliteľnou súčasťou pri budovaní VoIP sietí. Pri tomto riešení je potrebná práca SIP servera, ktorý prepíše privátnu adresu v SDP na verejnú adresu RTPproxy, a tým cez neho presmerováva RTP prúd. Nevyžaduje od klienta znalosť, že sa nachádza za NAT.
- Ďalšou možnosťou je riešiť NAT problém na strane klienta. Možnosti sú STUN, TURN alebo ICE [9].
  - STUN (Simple Traversal of UDP through NAT) umožňuje klientovi zistiť, či sa nachádza za NAT, akým typom NAT a hlavne zistiť svoju verejnú IP adresu a port. STUN riešenie využíva špeciálny STUN server, ktorý musí byť umiestnený na verejnom Internete. UA musí podporovať tento protokol a musí vedieť verejnú IP adresu STUN servera, alebo byť schopný si ju vyhľadať. Princíp je jednoduchý. Klient pošle na STUN server správu a on odpovie z akej adresy a portu mu prišla. Pokiaľ sa adresa aj port zhodujú, nie je tu žiaden NAT. Ak sú rozdielne, je medzi nimi NAT. Pokiaľ je UA za NAT a chce s niekým komunikovať musí správne modifikovať všetky časti SIP a SDP správy. STUN nepracuje v situáciách, pokiaľ je použité symetrické NAT, kde pri novej komunikácii je mapovaná vnútorná IP adresa a port na vždy unikátnu IP adresu a port. Čo znamená, že iná IP adresa a port, je medzi UA a STUN, a iná je medzi UA navzájom. Toto riešenie tiež nefunguje správne, pokiaľ sú oba UA za tým istým NAT. Pri použití UDP komunikácie je treba brať na vedomie, že toto mapovanie sa po určitom čase pri nečinnosti môže UA z NAT zmazať, preto je potrebné použiť niektorú z tzv. *keepalive* techník, ktorá udrží NAT mapovanie aktívne.
  - TURN (Traversal Using Relay around NAT) je protokol, ktorý umožňuje

komunikovať s ďalšími účastníkmi za NAT. Za týmto účelom je vytvorený špeciálny TURN server, ktorý musí byť umiestnený na verejnom segmente a je používaný na presmerovanie komunikácie. Klient, ktorý podporuje TURN, musí byť nakonfigurovaný s jeho verejnou IP adresou. Na ňu posiela TURN príkazy, a alokuje IP adresu a port, na ktorom bude TURN server vykonávať *relaying* médií.

- ICE (Interactive Connectivity Establishment) mechanizmus využíva oba protokoly STUN a TURN. Umožňuje UA odhaliť dostatok informácií o topológii siete a vybrať najvhodnejší spôsob komunikácie.

3.2.4. IPv4 a IPv6

IPv6 (Internet Protocol Version 6) je protokolom novej generácie pre Internet [17]. Základná špecifikácia je popísaná v RFC 2460. Je nástupcom aktuálne používaného IPv4 (Internet Protocol Version 4). Oba IP protokoly sú protokolmi sieťovej vrstvy, teda určujú ako sú dáta posielané z počítača na počítač v paketových sieťach ako je Internet.

IPv6 rieši hlavný problém IPv4 a to vyčerpanie adries. Oproti 32 bitom používa adresy 128 bitov dlhé. Preto je možné vytvoriť 2^{128} unikátnych IP adries. Vďaka čomu odpadá potreba NAT. Podporuje mobilitu, ktorá umožňuje dosiahnuteľnosť bez ohľadu na jeho umiestenie v IPv6 sieti.

Ďalej pridáva schopnosť auto-konfigurácie koncových zariadení, hneď po pripojení do smerovanej IPv6 siete. Implementuje na sieťovej vrstve šifrovanie a overenie totožnosti cez IPsec.

3GPP navrhlo, aby IMS podporovalo výhradne protokol IPv6 [1]. Vzhľadom na jeho pomalý nástup bolo nevyhnutné nasadiť podporu aj IPv4. Prechod medzi týmito protokolmi zabezpečuje komponent IMS zvaný IBCF (Interconnection Border Control Function). Modifikuje SIP a SDP informácie, aby mohli navzájom UE komunikovať správnymi protokolmi IP.

3.2.5. TLS

TLS (Transport Layer Security) a jeho predchodca SSL (Secure Sockets Layer) sú protokoly, ktoré bežia medzi spoľahlivým transportným protokolom ako je napríklad TCP a aplikačnou vrstvou, v IMS sieti napríklad SIP, respektíve SIPS. Umožňujú bezpečnú komunikáciu využitím kryptografie [14].

TLS má nasledovné základné fázy:

- Dohoda účastníkov na podporovaných algoritmoch.
- Výmena kľúčov založená na asymetrickom šifrovaní (napríklad RSA, či Diffie-Hellman) a autentifikácia vychádzajúca z certifikátov.
- Šifrovanie prevádzky silnou symetrickou šifrou (napríklad AES).

Výhodou TLS je, že je nezávislý od aplikačného protokolu. Jeho výhody sú:

- Kryptografické zabezpečenie – TLS by mal byť použitý na vytvorenie zabezpečeného spojenia.
- Súčinnosť – Nezávislí programátori by mali byť schopní vyvíjať aplikácie využívajúce TLS, ktoré môžu úspešne vymieňať kryptografické parametre bez znalosti kódu toho druhého.
- Rozšíriteľnosť – TLS sa snaží poskytnúť kostru (framework), podľa ktorej môže byť do TLS pridaný nový verejný kľúč a šifrovacie metódy. Vďaka čomu nebude nutné vytvárať nový protokol, s možnými novými hrozbami. Preto nie je potrebné implementovať ďalšiu bezpečnostnú knižnicu.
- Relatívna efektívnosť – kryptografické operácie bývajú veľmi náročné na CPU, najmä operácie s verejnými kľúčmi. Preto TLS zavádza schému, ktorá redukuje počet spojení, ktoré je potrebné vykonať. Navyše tým šetrí aj sieťovú prevádzku.

3.2.6. IPsec

IPsec (IP security) je bezpečnostné rozšírenie IP protokolu založené na autentifikácii a šifrovaní obsahu každého IP paketu [18]. Pracuje už na sieťovej vrstve, kde na rozdiel od TLS a iných protokolov, pracujúcich na transportnej vrstve, nevyžaduje podporu od aplikácie.

Je navrhnutý poskytovať spolupracujúcu, vysoko kvalitnú, kryptograficky založenú bezpečnosť pre IPv4 a IPv6. IPsec protokoly sú navrhnuté, aby boli nezávislé od kryptografických algoritmov.

Implementovaný je v koncovom zariadení, kde vystupuje ako bezpečnostná brána (SG – security gateway) alebo ako nezávislé zariadenie poskytujúce ochranu IP prevádzky. Na to využíva dva protokoly AH (Authentication Header) a ESP (Encapsulating Security Payload).

3.3. IMS klienti

IMS klienti a UE sú objekty, ktoré ineragujú s IMS entitami a vykonávajú signalizačné procedúry a vyvolanie služieb. IMS klienti sa môžu líšiť podľa toho, či podporujú iba registráciu a hlasové hovory, alebo klientov, čo podporujú aj videohovory, písanie IM, prezenciu stavu, IPTV a podobne [8].

3.3.1. RCS

RCS (Rich Communication Suite) je priemyselná iniciatíva vytvorená členmi GSMA (GSM Association), združenia mobilných operátorov a príbuzných spoločností. Zameriava sa na podporu štandardizácie, nasadzovania a propagácie mobilného telekomunikačného systému GSM (Global System for Mobile Communications) [30]. Pojmem RC (Rich Communication) „bohatá komunikácia“ označuje použitie viacerých komunikačných služieb ako len hlasu.

Aktuálna verzia špecifikácie je RCS 5.0, ktorá je spätne kompatibilná s RCS-e (RCS-enhanced) V1.2 a RCS 4. Podporuje oba OMA (Open Mobile Alliance) CPM (Converged IP Messaging) a OMA SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions) IM štandardy. Charakterizuje klienta, ktorý má nasledovné vlastnosti [30]:

- Širokopásmový prístup, ponúka hlasové hovory, zdieľanie obsahu počas hovoru, prenos súborov počas hovoru alebo počas posielania správ, umožňuje vytvorenie chatovej relácie.
- Podporuje LTE, zdieľanie videa s hovorom alebo bez hovoru, manipuláciu so zdieľanými obrázkami, zdieľanie videa s možnosťou pozastavenia a obnovenia.
- Poskytuje prezenciu stavu, informácie o možných službách, hyper dostupnosť, čiernu listinu používateľov (Blacklist), obohatenú podporu obsahu, zálohu a synchronizáciu kontaktov.
- Prináša zdokonalené správy, schopnosť posielať a prijímať SMS a MMS správy, ponúka konverzačné správy, definuje jednotného tvorcu SMS a MMS, poskytuje možnosť vláknového náhľadu správ, definuje chat službu, správy jeden jednému a jeden viacerým, dáva zoznam pozvaných účastníkov na skupinovú komunikáciu.
- Obohacuje obsah spracovaním médií, napríklad ponúka jazykový preklad.
- Podporuje viacero zariadení, jedno primárne a až dve sekundárne.

- Zavádza sieťové kontakty NAB (Network Address Book), ktoré spravuje a udržiava operátor, zahŕňa všetky zariadenia vo vlastníctve používateľa. Poskytuje konfiguráciu pre RCS zaradenia, ktorá je vykonávaná bez ich zásahu.
- Umožňuje vymieňať geografickú polohu.

3.3.2. Prehľad klientov

V nasledovnej tabuľke 3.2 uvádzame prehľad voľne dostupných klientov a ich vlastností.

IMS Klienti	Boghe IMS/RCS client	iDoubs	IMSDroid	myMonster TCS	UCT IMS client	IMS Communicator
Web stránka	code.google.com/p/boghe	code.google.com/p/idoubs	code.google.com/p/imsdroid	www.monster-the-client.org	uctimsclient.berlios.de	imscommunicator.berlios.de
Licencia	GPLv3	GPLv3	GPLv3	free, own	GPLv2	LGPL
Verzia	2.0.97.687	2.0.184	2.0.484	0.9.25 TCS	1.0.13	0.70.605
Dátum vydania	15.3.2012	20.9.2011	15.3.2012	20.3.2012	13.2.2009	8.7.2007
Operačný systém	Win	iOS,Mac OS X	Android	Multiplatform (Java)	Linux	Multiplatform (Java)
Viacero účtov	Nie	Nie	Nie	Áno	Nie	Nie
Registrácia	AKAv1/v2-MD5, MD5, basic	AKAv1/v2-MD5, MD5, basic	AKAv1/v2-MD5, MD5, basic	AKAv1-MD5, MD5	AKAv1-MD5, MD5	AKAv1-MD5, MD5
IMS signalizácia	Áno	Áno	Áno	Áno	Áno	Áno
SigComp	Áno	Áno	Áno	Nie	Nie	Nie
Audio	Áno PCMA, PCMU, GSM, AMR-NB-OA, AMR-NB-BE, iLBC, Speex-NB	Áno G.722, G.729AB, AMR-NB, iLBC, GSM, PCMA, PCMU, Speex-NB, Speex-WB, Speex-UWB	Áno G729AB1, AMR-NB, iLBC, GSM, PCMA, PCMU, Speex-NB	Áno PCMA, PCMU, MCA	Áno GSM, PCMA, PCMU, MP2	Áno JMF codecs
Video	Áno MP4V-ES, Theora, H264, H263/+/++	Áno VP8, H264, MP4V-ES, Theora, H263/+/++	Áno VP8, H264, MP4V-ES, Theora, H.263, H.263-1998, H.261	Áno H.263, MP2T, H.263-,MPV, MP4V-ES	Áno -	Áno JMF codecs
Správy	Page / Session mode	Page / Session mode	Page / Session mode	Page / Session mode	Page mode	-
Presence	Áno OMA, IETF	Áno OMA, IETF	Áno OMA, IETF	Áno OMA, IETF	Áno -	Áno -
XDMS/XCAP	Áno	Áno	Áno	Áno	Áno	Nie
Bezpečnosť	TLS, IPSec	-	TLS, IPsec	-	Nie	IPSec
IPv6	Áno	Áno	Áno	Áno	Áno	Áno
Prechod cez NAT	Áno STUN/TURN	Áno STUN/TURN	Áno STUN/TURN	Nie	Nie	Áno STUN
P-CSCF vyhľadanie	Pevné, DNS NAPTR+SRV	Pevné, DNS NAPTR+SRV	Pevné, DNS NAPTR+SRV	Pevné, SRV DNS	Pevné	Pevné
Ďalšie vlastnosti	Zdokonalený zoznam adries, zdieľanie obsahu, prenos súborov	-	Prenos súborov, zdieľanie obrazu, zdieľanie videa	Prenos súborov, manažment skupín	IPTv (RTSP)	-

Tab. 3.2: Prehľad IMS klientov [27]

V práci ďalej testujeme klientov, ktorí sú stále vyvíjaní a boli aktualizovaní v poslednej dobe. Konkrétne klienta Boghe na OS Windows, klienta Monster na OS Windows a Linux. Na odporúčanie kolegov zo Slovenskej technickej univerzity sme tiež otestovali UCT IMS klienta na OS Linux. Klient Boghe z časti spĺňa požiadavky RCS definované v kapitole 3.3.1.

4. REALIZÁCIA KAMAILIO IMS PLATFORMY

Cieľom diplomovej práce je implementovať prototyp IMS komunikačnej platformy, ktorá bude poskytovať základné služby a umožní otestovať jej funkcionality. IMS platforma bude využívaná na výskum a analýzu správania protokolov a entít. V tejto kapitole popíšeme postup pri prebiehajúcej implementácii a riešení jej technických aspektov.

4.1. Inštalácia IMS jadra

Inštalácia bola vykonaná na virtuálne servery s neustálym prístupom na internet. Ako operačný systém sme zvolili Debian GNU/Linux 6.0 Squeeze. Volili sme 32 bitový variant, nakoľko sú dostupné len 32 bitové inštalačné balíčky IMS platformy, a tým nie je potrebná ich manuálna kompilácia. Podrobný návod inštalácie možno nájsť v [22].

Balíčky sú dostupné v repozitári s adresou *http://repository.ng-voice.com*. Tento je potrebné priradiť do systémových repozitárov Debianu. Balíček obsahujúci IMS implementáciu sa nazýva *kamailio-ims-modules*. Zatiaľ je kompatibilný len s verziou Kamailio 3.1.1. Obsahuje moduly CSCF, vzorové konfiguračné súbory, ktoré je potrebné pre správnu funkčnosť serverov upraviť na pridelené adresy a parametre platformy. Konfiguračné súbory našej platformy možno nájsť v prílohe D.

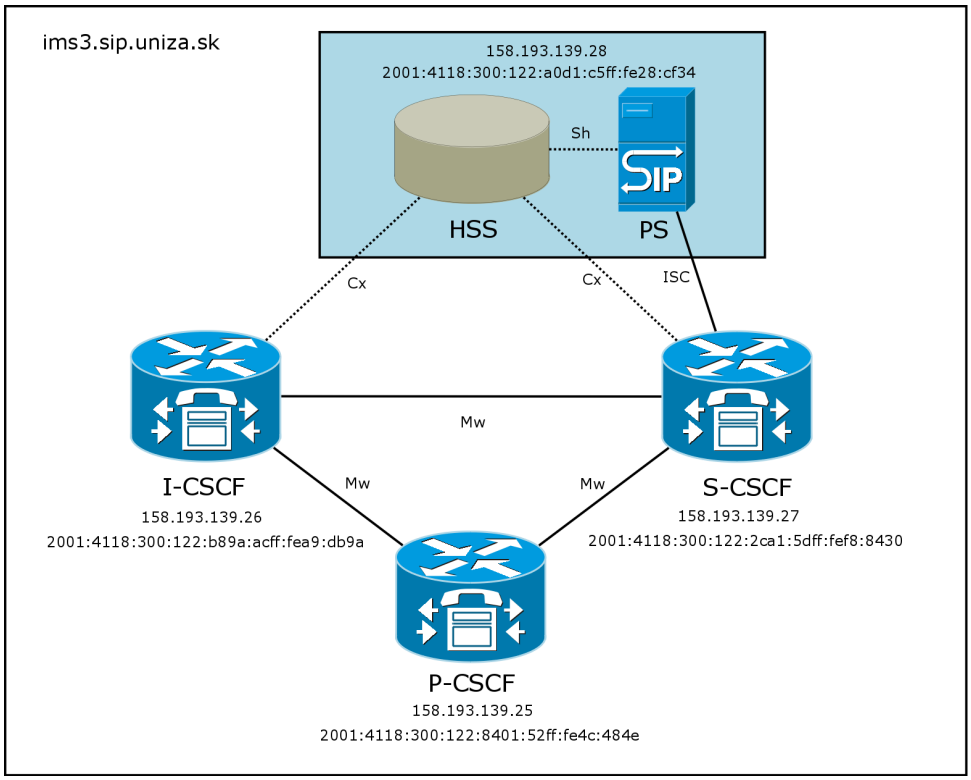
Pre potreby ukladania dát bolo nutné nainštalovať databázové servery, konkrétne MySQL. Databázu potrebuje napríklad I-CSCF, kde ukladá URI smerujúce na obsluhujúci S-CSCF server *sip:scscf.ims3.sip.uniza.sk:5060*.

Repozitár tiež obsahuje balíček obsahujúci funkcionalitu HSS. Využíva implementáciu OpenIMSCore HSS vyvíjanú inštitútom FOKUS nazvanú FHoSS (FOKUS Home Subscriber Server).

Balíček sa nazýva *openimscore-fhoss*. Na ukladanie dát využíva MySQL server. K svojej funkčnosti vyžaduje Javu, nachádzajúcu sa v *non-free* repozitároch Debianu, ktorú potrebuje na vytvorenie web servera poskytujúceho webovské konfiguračné rozhranie. V ňom je možná administrácia používateľských kont, ich privátnych a verejných identít, priraďovanie obslužných a aplikačných serverov a podobne. Návod na pridanie nového používateľa možno nájsť v [23].

4.1.1. Topológia platformy

Na obrázku 4.1 možno vidieť topológiu komunikačnej platformy, nevyhnutnej pre poskytovanie základných služieb. Obsahuje komponenty IMS jadra P-CSCF, I-CSCF, S-CSCF a HSS, spolu s ich IP adresami (Tab. 3.1). Na serveri, na ktorom beží HSS je nainštalovaný aj SIP server Kamailio, ktorý plní funkciu PS. Súčasťou PS je aj XCAP s nasledovnou URI: *http://presence.ims3.sip.uniza.sk:5060/xcap-root*.



Obr. 4.1: Topológia platformy

4.1.2. Topológia rozšírenej platformy

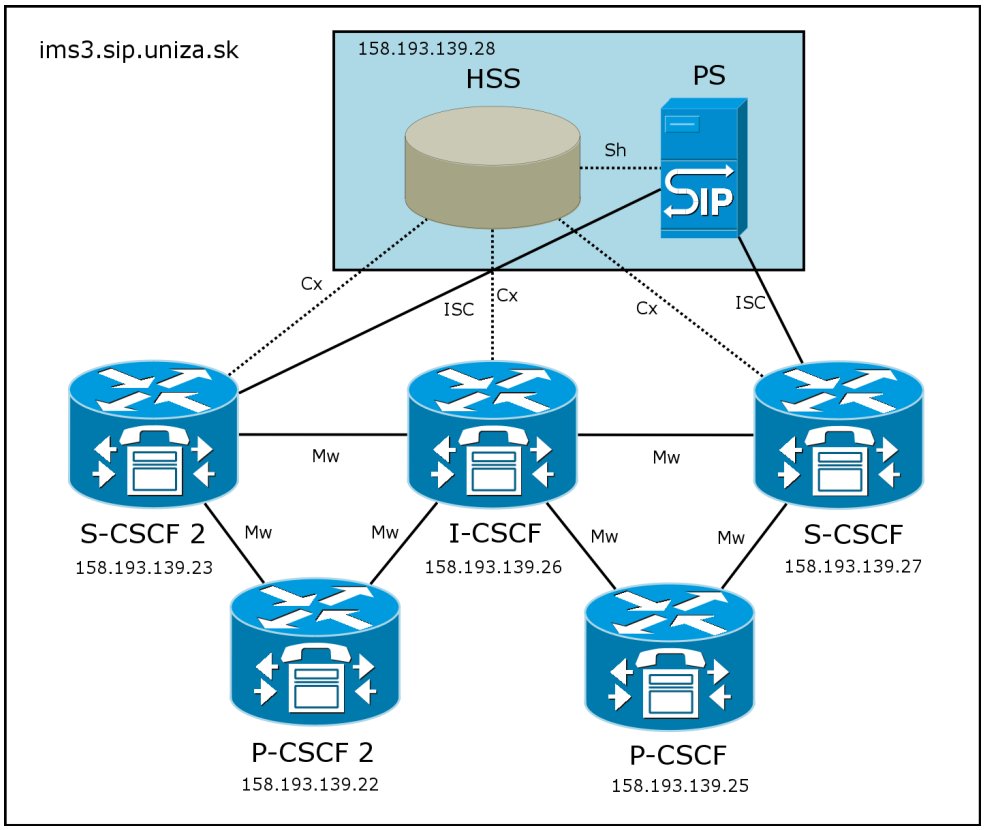
V komunikačnej platforme sme pre potreby pokročilejších scenárov pridali ďalší P-CSCF a S-CSCF server (Obr. 4.2).

Inštalácia týchto serverov prebieha rovnako podľa návodu [22]. Len vo všetkých konfiguračných súboroch je potrebné namiesto *pcscf* použiť *pcscf2* a podobne namiesto *scscf* odpovedajúce *scscf2,* podľa vybraných doménových mien pre tieto servery (Tab. 3.1).

Ďalej je potrené na serveri HSS pridať cestu k novému S-CSCF 2. Pridaním nasledovného riadku do súboru */etc/fhoss/DiameterPeerHSS.xml*:

```
<Peer FQDN="scscf2.ims3.sip.uniza.sk" Realm="ims3.sip.uniza.sk" port="3870" />
```

Pre využívanie S-CSCF 2 je potrebné podľa návodu [31] pridať do databázy HSS cez webovské konfiguračné rozhranie nový záznam *Preferred S-CSCF Set* odkazujúci na SIP URI tohto servera *sip:scscf2.ims3.sip.uniza.sk:5060*. Následne je ho potrebné priradiť používateľom.



Obr. 4.2: Topológia rozšírenej platformy

4.2. Riešenie technických aspektov

V tejto platforme bolo potrebné riešiť technické aspekty opísané v kapitole 3.2.

4.2.1. NAT

Ako prvé riešenie sme testovali použitie *relay* servera, ktorý poskytuje úplné riešenie prechodu cez NAT. Z dostupných riešení bol vybratý produkt RTPproxy.

4.2.1.1. RTPproxy

Inštalácia je pomerne jednouchá. Podrobný návod možno nájsť v [24]. Je potrebné nainštalovať balíček *rtpproxy* z repozitára. Je nevyhnutné nastaviť port, na ktorom bude spolu s P-CSCF komunikovať a verejnú IP adresu, na ktorej bude presmerovávať RTP

prúd.

S konfiguráciou P-CSCF však nastávajú problémy. Do konfigurácie P-CSCF je potrebné pridať direktívu *WITH_NAT* a nastaviť správne číslo portu na komunikáciu s RTPproxy. Podľa návodu [24] by táto konfigurácia mala byť postačujúca. Riešenie sa počas testovania ukázalo ako nefunkčné.

Pri našom testovaní bol jeden klient na verejnej IP adrese a druhý za NAT, ktorý sme vytvorili na Cisco smerovači. Testovali sme volania jeden druhému s rôznymi klientmi, no ani v jednom hovor nebol smerovaný cez RTPproxy.

Po dôkladnejšom prezretí konfiguračného súboru P-CSCF servera sme zistili, že neobsahuje smerovacie (routing) položky, ktoré sa nachádzajú v SIP Kamailio konfiguračnom súbore. Ako sú napríklad *route[RELAY]*, či *route[RTPPROXY]*. Rozhodli sme sa tieto položky pridať do konfiguračného súboru P-CSCF. Bolo potrebné vyriešiť správy o chybách, ktoré tieto zmeny spôsobili, pridaním chýbajúcich knižníc. Táto zmena spôsobila, že registrácia klienta bola úspešná, ale pokiaľ bol hovor cez NAT, tak signalizácia skončila v smerovacej logike P-CSCF servera.

Po kontaktovaní používateľského fóra *User Mailing List* Kamailio, nám tento postup odobril aj jeden z tvorcov. Radil nám ako má správna konfigurácia vyzerať. A aký je postup INVITE správy v smerovacej logike Kamailio. No zároveň nás upozornil, že by nám to mal potvrdiť odborník z IMS vetvy Kamailio. Zistili sme, že smerovacie logiky zo SIP Kamailio konfiguračného súboru nebudú správne fungovať, nakoľko P-CSCF nemá žiadnu databázu, databázový server je HSS. Preto sme sa vrátili k pôvodnej P-CSCF konfigurácii bez SIP Kamailio smerovacích logík.

Zmenili sme testovací scenár umiestnením oboch klientov za to isté NAT. Počas testovania tohto scenára sme zistili, že RTPproxy je funkčný a klienti dostanú upravenú SDP správu tak, aby posielali RTP prúd na proxy. Pôvodný scenár, kde je jeden klient za NAT a druhý je verejný nie je stále funkčný. Po vykonaní hlbšieho testovania sme zistili, že keď je volajúci klient za NAT (druhý klient verejný), tak nenastane žiadna zmena v SDP, a preto je RTP prúd posielaný na privátnu IP adresu.

Naopak, keď je volaný klient za NAT, je v SDP správne zmenená privátna IP adresa na verejnú adresu proxy. Ale nie je na ňu zmenená verejná IP adresa volajúceho. Preto RTP prúd nie je posielaný na proxy, ale na verejnú IP adresu UE. V konečnom dôsledku toto riešenie nie je funkčné, pretože RTPproxy na *relaying* potrebuje obojsmerný RTP prúd.

Pri testovaní sme zistili, že prepisovanie IP adries v SDP správach je funkčné len pri použití Monster IMS klienta. Ukázalo sa, že v správach posielaných z Boghe IMS klienta a UCT IMS klienta žiadne IP adresy v SDP nie sú prepisované.

Z používateľského fóra Kamailio, sme zatiaľ nedostali odpoveď, ktorá by nám pomohla tento problém vyriešiť.

4.2.1.2. STUN

Vzhľadom na neúplnú funkcionalitu RTPproxy sme rozhodli pridať do našej topológie aj STUN/TURN server. Použili sme Restund server, dostupný na katedrovej IP adrese 158.193.139.47, na porte 3478. Riešenie je voľne dostupné a je ho možno nainštalovať a nakonfigurovať podľa návodu [25].

Z našich testovaných klientov podporuje STUN/TURN jedine Boghe IMS klient. Vyriešil sa tým problém, keď volajúci z verejnej IP adresy volá druhého, ktorý je za NAT. Klient za NAT v odpovedi 200 OK správne nastaví v SDP správnu verejnú IP adresu a port, ktoré pred tým získa zo STUN servera.

Problém nastáva, keď klient za NAT chce volať. Na požiadavku INVITE dostáva odpoveď *403 Forbidden - Not Registered! You must register first with a S-CSCF*. Zistili sme, že problém spôsobuje funkcia *P_is_registered()*, ktorá má za úlohu zistiť, či správa prišla od registrovaného UE. Overuje to funkcia *r_is_registered* na základe hodnôt vo *Via* hlavičke. V nej klient Boghe posiela privátnu IP adresu, a server má uloženú ako registrovanú verejnú IP adresu. Klient ju získal zo STUN požiadavky získanej pred registráciu, ktorú uvádza v *Contact* hlavičke.

4.2.2. IPv6

Sfunkčniť IPv6 protokol bolo pomerne jednoduché, nakoľko IMS platforma natívne podporuje tento protokol. Potrebné je mať vytvorené správne DNS záznamy AAAA ukazujúce na IPv6 adresy serverov.

Je potrebné pridať do konfigurácie direktívu prikazujúcu serveru počúvať na týchto adresách. Či už UDP alebo TCP. Tým sme získali platformu podporujúcu oba IP protokoly súčasne. Klient s IPv4 sa bez problémov dovolá klientovi s tiež IPv4 adresou. Podobne, keď majú obaja IPv6 adresy.

Problém nastáva, keď je pripojený jeden klient z IPv4 a druhý z IPv6. Vtedy nemôžu spolu navzájom priamo komunikovať. Na riešenie sme použili RTPproxy server.

Podobne ako pri NAT, by mal presmerovávať komunikáciu medzi týmito dvoma sieťami.

Do konfigurácie RTPproxy popísanej v [24] je potrebné pridať *relay* aj na IPv6 adrese.

```
LISTEN_ADDR=158.193.139.25
LISTEN_ADDR6=2001:4118:300:122:8401:52ff:fe4c:484e
EXTRA_OPTS="-l ${LISTEN_ADDR} -6 /${LISTEN_ADDR6}"
```

Podľa návodu pre Kamailio SIP server [28] by táto konfigurácia mala byť postačujúca. Toto riešenie sa ukázalo ako nefunkčné. Problém bude pravdepodobne na strane P-CSCF, od ktorého požadujeme, aby presmerovával RTP prúd na RTPproxy. Je potrebné prepísať IPv4 klientovi IPv6 kontaktnú adresu v SDP správe na IPv4 a naopak IPv6 klientovi prepísať IPv4 adresu na IPv6. P-CSCF správy nemodifikuje vôbec, preto klienti nie sú schopní navzájom doručovať RTP prúd.

4.2.3. TLS

Pre správnu funkcionalitu konfigurácie s TLS je potrebné vytvoriť DNS SRV záznam so *_sips._tcp* predponou. Tiež sme vygenerovali certifikát lokálnej certifikačnej autority, ktorým sme potom podpísali certifikát *pcscf* servera podľa postupu popísaného v [32].

Vygenerovali sme 1024 bitové RSA certifikáty za pomoci nástroja *openssl*, otvorenej implementácie SSL a TLS protokolov. Neodporúča sa vyšší počet bitov, aby nebol server zbytočne zaťažovaný šifrovaním no zároveň nie menší, aby poskytoval dostatočnú bezpečnosť.

Do konfigurácie je potrebné pridať direktívu definujúcu *WITH_TLS*. A podľa [32] upraviť niektoré parametre v konfiguračnom súbore. Napríklad je potrebné nastaviť cesty k súborom vygenerovaného certifikátu a privátnemu kľúču. Taktiež prikázať serveru počúvať na porte 5061 protokolom TLS.

Túto konfiguráciu sa nám nepodarilo odskúšať, nakoľko sa s ňou server nepodarilo spustiť. Server vracia správu o chybe, oznamujúcu problém nájsť internú funkciu *pcscf.so* modulu. Nepodarilo sa nám nájsť riešenie, s ktorým nepomohli ani samotní autori projektu Kamailio IMS, s odkazom, že riešenie bude zapracované v novšej verzii Kamailio IMS.

V záznamoch o chybách sme našli, že P-CSCF nemôže nájsť funkciu *get_tls_session_hash,* ktorú sa pokúša vyhľadať funkcia *find_export.* Tá volá funkciu *find_export_record,* tá následne funkciu *find_mod_export_record,* ktorá by mala vyhľadať

zoznam modulov v module *mod* a vrátiť smerník podľa zadaného mena. Alebo v prípade nenájdenia vráti *0*, čo je aj v našom prípade.

4.2.4. IPsec

Z našich testovaných klientov podľa tabuľky 3.2 podporuje IPsec jedine klient Boghe. Testovali sme podporu pre IPsec zvolením voľby IPsec na karte *Security* v nastaveniach klienta. Z nášho testovania vyplynulo, že Boghe IPsec nepodporuje, nakoľko sa klient nepokúsi vytvoriť žiadnu bezpečnostnú asociáciu so serverom.

V prípade potreby použitia IPsec odporúčame použiť vytvorenie bezpečnostnej asociácie na úrovni operačného systému, nezávislom od aplikácie. Napríklad pomocou nástroja IPsec-Tools na OS Linux.

4.3. Riešenie čiastkových problémov

V tejto platforme bolo potrebné riešiť rôzne problémy. Od triviálnych, ako je medzera navyše v databázovom zázname mena S-CSCF na HSS, vytvorenom inštalačným skriptom [29]. Až po tie, čo sú nahlásené ako chyby a sami autori sa ich snažia opraviť.

Väčšina problémov sa dá odhaliť pomocou chybových správ vrátených zo serverov. Určité chybové správy sú popísané v [29]. Okrem niektorých z nich sme museli riešiť aj nasledovné chybové správy

Chybová správa *600 Busy everywhere - Forwarding to S-CSCF failed* bola posielaná ako odpoveď na INVITE správu. Zistili sme, že S-CSCF bolo preplnené záznamovými súbormi (/var/log/*). Vyriešili sme to pomocou nástroja *logrotate*, v ktorého konfiguračnom súbore sme nastavili dennú archiváciu a častejšie mazanie starých záznamových súborov.

Stav používateľa je uložený na serveri HSS v databáze *hss_db* tabuľke *impu* stĺpci *user_state*. V stave registrovaný *(Registered)* je nastavený *user_state == 1*. Keď nie je registrovaný odpovedá na INVITE správy chybovou správou *600 Busy everywhere - Empty list of S-CSCFs*, pri registračnom stave *Not-Registered (user_state == 0)*. Správna správa by mala byť *404 Not Found - destination user not found on this S-CSCF*, posielaná pri registračnom statuse *Unregistered (user_state == 2)*. Nepodarilo sa nám zistiť, prečo je niekedy *user_state* pri odhlásení používateľa nastavovaný na nesprávnu hodnotu.

Vo vnútri SIP správ sme niekedy dostávali nasledovnú varovnú správu:

```
Warning: 392 158.193.139.27:5060 "Noisy feedback tells:  pid=14914
req_src_ip=158.193.139.26 req_src_port=5060
in_uri=sip:scscf.ims3.sip.uniza.sk:5060
out_uri=sip:scscf.ims3.sip.uniza.sk:5060 via_cnt==3"
```

Zistili sme, že je to len ladiaca správa a dá sa vypnúť v konfigurácii S-CSCF nastavením nasledovného parametra:

```
sip_warning=no
```

Ďalší problém, s ktorým sme sa museli vysporiadať bolo, že S-CSCF neposielal prijaté požiadavky na I-CSCF, ako je v popise jeho správania v kapitole 2.3.3. Sám ich hneď spracovával a obsluhoval priamo. Pre nápravu je potrebné nastaviť IP adresu I-CSCF namiesto adresy S-CSCF podľa vzorového konfiguračného súboru.

```
# Do not loop through the I-CSCF if the terminating user is here
# might not work if other routes are present
    if (S_term_registered()){
            t_relay_to_udp("158.193.139.26",5060);
            exit;
    }
```

S-CSCF sa s touto konfiguráciou správa podľa špecifikácie a smeruje SIP požiadavky na I-CSCF server, ako je to znázornené napríklad na obr. 2.3.

Pokiaľ sa chce používateľ zaregistrovať v roamingu, teda z iného P-CSCF, ako je jeho domovský, môže dostať chybovú správu *403 Forbidden - HSS Roaming not allowed* ako odpoveď na REGISTER správu. Táto chyba znamená, že používateľ nie je oprávnený sa zaregistrovať v danej sieti iného operátora. Túto sieť oznamuje P-CSCF, cez ktoré sa používateľ registruje pridaním *P-Visited-Network-Id* hlavičky. Danú doménu siete je potrebné pridať do databázy HSS, a následne ju prideliť verejnej používateľskej identite, podľa krokov popísaných v [33]. Používateľ tak bude mať povolený roaming v sieti daného operátora a môže sa úspešne zaregistrovať.

V prípade zlej voľby autentifikačnej schémy na HSS pre privátnu používateľskú identitu na Early-IMS-Security alebo NASS-Bundled, dostane UE na počiatočnú register správu chybovú odpoveď *500 Server Internal Error - while packing auth vectors*. V prípade tejto chyby je potrebné vybrať inú autentifikačnú schému a reštartovať Kamailio inštanciu, inak bude odpovedať stále tou istou chybovou správou.

5. ANALÝZA SPRÁVANIA

Cieľom práce je využiť realizovanú IMS komunikačnú platformu na analýzu správania klientov a P-CSCF. V tejto časti práca skúma ich vzájomnú komunikáciu a porovnáva, či je v súlade so špecifikáciou IMS 3GPP TS 24.229, verzia 11.3.0.

5.1. Požiadavky zo špecifikácie

V špecifikácii 3GPP TS 24.229 [5] sú definované správania a povinnosti, ktoré musia byť vykonávané na strane UE a jednotlivých IMS entitít. My sa zameriavame na špecifikácie správ a povinnosti vyplývajúce z ich spravovania medzi UE a P-CSCF.

5.1.1. Strana UE

UE môže zaregistrovať jednu zo svojich verejných používateľských identít z ľubovolnej IP adresy, ktorou je pripojený na verejný internet. Tá istá identita môže byť viazaná na viacej IP adries. Tiež UE môže registrovať ďalšie verejné používateľské identity pre svoje IP adresy.

5.1.1.1. Registrácia

Počiatočná registračná procedúra spočíva v poslaní nechránenej REGISTER správy. UE môže začať novú registráciu, keď bola prijatá finálna odpoveď od registrátora prebiehajúcej registrácie, alebo už predchádzajúca požiadavka vypršala.

UE môže zahájiť registráciu aj v minulosti zaregistrovanej verejnej používateľskej identity na niektorú z jeho kontaktných adries a asociovanej bezpečnostnej alebo TLS relácii, kedykoľvek po skončení počiatočnej registrácie.

5.1.1.1.1. Nechránená REGISTER správa

Pri posielaní nechránenej REGISTER správy musí UE naplniť pole hlavičiek nasledovne:

- *From* hlavička – ak podporuje registráciu viacerých telefónnych čísel v SIP (RFC 6140), tak toto pole naplní adresou PBX (Private Branch Exchange), inak použije verejnú používateľskú identitu, ktorou sa chce zaregistrovať.
- *To* hlavička – obsah rovnaký ako hlavička *From*.

- *Contact* hlavička – musí obsahovať SIP URI obsahujúce IP adresu alebo FQDN daného UE. Pokiaľ UE podporuje GRUU, podporuje viacero registrácií, má IMEI (International Mobile Equipment Identity) alebo MEID (Mobile Equipment Identifier), tak musí UE pridať *"+sip.instance"* parameter hlavičky, obsahujúci *Instance ID*. Pokiaľ UE podporuje viacero registrácií súčasne, musí zahrnúť aj *"reg-id"* parameter hlavičky, s obsahom určeným v RFC 5626. UE musí zahrnúť všetky ICSI (IMS Communication Service Identifier) hodnoty *g.3gpp.icsi-ref* a IARI (IMS Application Reference Identifier) hodnoty *g.3gpp.iari-ref*.
- *Via* hlavička – obsahuje IP adresu alebo FQDN daného UE a port, na ktorom chce prijímať odpoveď na túto správu, čo platí pre UDP. Pri TCP bude odpoveď prijatá na TCP spojení, na ktorom bola požiadavka poslaná. UE tiež musí pridať bezparametrový parameter hlavičky *"rport"*. Ktorým klient požaduje, aby server odoslal odpoveď späť na zdrojovú IP adresu a port, z ktorého požiadavka naozaj prišla, čo je vhodné hlavne, ak sa UE nachádza za NAT. Pokiaľ je za NAT, tak by mal pridať bezparametrový parameter hlavičky *"keep"*, ktorým označí podporu posielania *keep-alives* správ, definovaných v RFC 6223.
- Tiež musí obsahovať interval vypršania registrácie *Expires* s hodnotou 600 000 sekúnd ako požadovanú dĺžku trvania registrácie. Túto hodnotu môže S-CSCF zamietnuť odpoveďou 423 (Interval Too Brief).
- *Request-URI* musí nastaviť na SIP URI doménového mena domovskej siete, na ktorú posiela túto požiadavku. Napríklad *sip:ims3.sip.uniza.sk*.
- V *Supported* hlavičke uvedie *"path"* značku, ak podporuje GRUU uvedie aj *"gruu"* značku a ak podporuje viacero registrácií uvedie *"outbound"* značku.
- V prípade podpory TLS u UE, musí obsahovať *P-Access-Network-Info* hlavičku.
- *Security-Client* hlavička – slúži na oznámenie plánu médií bezpečnostných mechanizmov, ktoré UE podporuje. Tieto bezpečnostné mechanizmy sa odlišujú *"mediasec"* parametrom hlavičky.
- Ak podporuje registráciu viacerých telefónnych čísel v SIP (RFC 6140), tak UE musí pridať hlavičky *Require* a *Proxy-Require* obsahujúce voliteľný parameter *"gin"* .

5.1.1.1.2. Odpoveď 200 OK

Keď príjme 200 OK správu ako odpoveď na REGISTER požiadavku, UE musí:

- Uložiť čas uplynutia registrácie verejnej používateľskej identity nachádzajúcej sa v *To* hlavičke. A priradiť ju k príslušnej kontaktnej adrese UE alebo registračnému toku a asociovanej adrese, ak je viacero registrácií.
- Ak sa jedná o počiatočnú registráciu UE musí prvú URI, ktorá sa nachádza v hlavičke *P-Associated-URI* uložiť ako implicitnú verejnú používateľskú identitu. Následne ju priradiť k príslušnej kontaktnej adrese UE a súvisiacej bezpečnostnej alebo TLS relácii. Pokiaľ *P-Associated-URI* hlavička nie je zahrnutá, musí zaobchádzať s registrovanou identitou ako zablokovanou (barred) verejnou používateľskou identitou.
- Uložiť zoznam trás služieb nachádzajúcich sa v *Service-Route* hlavičke.
- Nájsť v *Contact* hlavičke pole zhodujúce sa poľom v požiadavke REGISTER. Ak podporuje GRUU uloží si parametre z *"pub-gruu"* a *"temp-gruu"*.
- Pokiaľ REGISTER obsahoval *"reg-id"* a *"+sip.instanc*e*"* paremetre v *Contact* hlavičke a *"outbound"* značku, UE musí skontrolovať, či prichádzajúca správa obsahuje *"outbound"* značku v *Require* hlavičke. Následne musí konať podľa RFC 5626 .
- Uložiť plán médií bezpečnostných mechanizmov, ktoré P-CSCF podporuje z *Security-Server* hlavičky.
- Ak hlavička *Via* obsahuje *"keep"* parameter, začne posielať *keep-alives* registrácie k P-CSCF.

5.1.1.1.3. Ostatné odpovede

Keď prijme správu 305 Use Proxy ako odpoveď, UE musí vybrať ďalšie P-CSCF, ak má predkonfigurovaných viac IP adries alebo doménových mien, inak sa UE pokúsi P-CSCF vyhľadať. Na vybrané P-CSCF pošle novú počiatočnú registráciu.

Keď prijme 423 Interval Too Brief správu, UE musí poslať inú REGISTER správu s hodnotou vypršania registrácie menšou alebo rovnou ako *Min-Expires* hodnota hlavičky 423 odpovede.

Po prijatí odpovedí 408 Request Timeout, 500 Server Internal Error, 504 Server Time-Out alebo 600 Busy Everywhere UE sa môže pokúsiť o opätovnú registráciu.

5.1.1.2. Autentifikácia

Autentifikácia sa vykonáva počas počiatočnej registrácie. V prípade, že server vyžaduje autentifikáciu od UE pošle 401 Unauthorized správu ako odpoveď na REGISTER požiadavku. Server môže požadovať nasledovné druhy autentifikácie.

5.1.1.2.1. IMS AKA

Pri použití REGISTER správy musí pridať UE k pôvodným hlavičkám popísaných v 5.1.1.1.1. kapitole *Authorization* hlavičku s nasledovnými parametrami:

- Parameter *"username"* – nastavený na privátnu používateľskú identitu.
- Parameter *"realm"* – v prípade počiatočnej registrácie nastaviť na doménové meno domovskej siete, inak nastaviť na *"realm"* z *WWW-Authenticate* hlavičky.
- Parameter *"uri"* – nastaviť na SIP URI doménového mena domovskej siete.
- Parametere *"nonce"* a *"response"* – nastaviť na prázdne hodnoty, v prípade počiatočnej registrácie, inak na naposledy prijaté *"nonce"* a *"response"* hodnoty.

Po prijatí 401 Unauthorized správy ako odpovede na REGISTER, UE musí extrahovať RAND (Random) a AUTN (Authentication Token) parametre z *"nonce"* hodnoty. Skontrolovať platnosť správy podľa 3GPP TS 33.203. Pokiaľ je platná, podľa tejto špecifikácie vyrátať RES (Response) parameter.

Následne UE musí poslať ďalšiu REGISTER správu, obsahujúcu *Authorization* hlavičku, ktorá bude obsahovať parametre:

- Parameter *"realm"* – nastaviť na *"realm"* z *WWW-Authenticate* hlavičky.
- Parameter *"username"* – nastavený na privátnu používateľskú identitu.
- Parameter *"response"* – obsahujúci vyrátaný RES parameter.
- Parameter *"uri"* – nastaviť na SIP URI doménového mena domovskej siete.
- Parametre *"algorithm"* a *"nonce"* – nastavené na na hodnoty prijaté v 401 Unauthorized odpovedi.

V prípade, ak klient podporuje bezpečnostné mechanizmy, môže vložiť *Security-Client* a *Security-Server* hlavičky. UE musí nastaviť *Call-ID* hlavičku na rovnakú hodnotu, aká bola hodnota *Call-ID* v 401 Unauthorized správe.

Pokiaľ nie je prijatá správa 200 OK pred vypršaním životnosti bezpečnostnej

asociácie alebo je prijatá odpoveď 403 Forbidden, UE musí považovať registráciu za neúspešnú.

5.1.1.2.2. SIP Digest

Pri použití registrácie so SIP Digest autorizáciou musí pridať UE k pôvodným hlavičkám popísaných v 5.1.1.1.1. kapitole aj *Authorization* hlavičku s nasledovnými parametrami:

- Parameter *"username"* – nastavený na privátnu používateľskú identitu.
- Parameter *"realm"* – doménové meno domovskej siete.
- Parameter *"uri"* – nastaviť na SIP URI doménového mena domovskej siete.
- Parametere *"nonce"* a *"response"* – nastaviť na prázdne hodnoty.

Po prijatí 401 Unauthorized správy ako odpovede na REGISTER, v ktorom je použitý algoritmus autorizácie MD5 (Message-Digest algorithm), UE musí vybrať parametre *digest* výzvy z *WWW-Authenticate* hlavičky podľa špecifikácie RFC 2617. Podľa tejto špecifikácie musí UE vypočítať *digest* odpoveď.

Následne UE musí poslať ďalšiu REGISTER správu, obsahujúcu *Authorization* hlavičku, ktorá bude obsahovať parametre vyskladané podľa špecifikácie RFC 2617. K parametrom spomínaným vyššie pridá napríklad *"cnonce"*, *"qop"* a *"nonce-count"*. UE musí nastaviť *Call-ID* hlavičku nastaviť na rovnakú hodnotu, aká bola hodnota *Call-ID* v 401 Unauthorized správe.

Po prijatí 200 OK odpovede na REGISTER požiadavku, musí UE v prípade použitia *Authentication-Info* hlavičky s parametrom*"algorithm*" nastaveným na *"MD5"*, autentifikovať S-CSCF použitím *"rspauth"* parametru hlavičky *Authentication-Info*.

V prípade prijatia 403 Forbidden odpovede, UE musí považovať registráciu za neúspešnú.

5.1.1.2.3. NASS-IMS Bundled

Pri použití NASS-IMS bezpečnostného mechanizmu k hlavičkám popísaných v 5.1.1.1.1. kapitole pridá *Authorization* hlavičku s nasledovným parametrom:

- Parameter *"username"* – nastavený na privátnu používateľskú identitu.

Po prijatí 200 OK ako odpovedi na register správu nie sú na UE žiadne dodatočné požiadavky. V prípade NASS-IMS Bundled autentifikácie sa na REGISTER správu neočakáva odpoveď 401 Unauthorized.

Je určený pre klientov, ktorí majú čipovú kartu. Preto nie je potrebná osobitná autentifikačná procedúra.

5.1.1.3. Odhlásenie

Akúkoľvek verejnú používateľskú identitu, ktorú má UE zaregistrovanú, môže odhlásiť (deregister) prostredníctvom jednoduchej registračnej procedúry.

Pred odoslaním REGISTER požiadavky na odhlásenie musí UE zrušiť všetky dialógy alebo tok pre kontaktné adresy alebo verejné používateľské identity, ktoré sa chystá odhlásiť. Pokiaľ používateľ odoberá balík *reg event* k používateľskej identite, ktorú ide odhlásiť a tento dialóg je jediný zostávajúci *reg event* používateľa, to znamená, že neexistujú ďalšie kontaktné adresy asociované s *reg event* balíkom používateľa, potom UE nesmie tento dialóg zrušiť.

Pri posielaní REGISTER požiadavky UE odstráni mapovanie medzi verejnou používateľskou identitou a jednou z jeho kontaktných adries alebo niektorých z tokov.

UE vyskladá polia hlavičiek REGISTER ako v 5.1.1.1.1. kapitole s použitím adries verejnej používateľskej identity, ktorú chce odhlásiť. Vo *Via* hlavičke nemusí uvádzať ďalšie parametre. Interval vypršania registrácie nastaví na hodnotu *0*, podľa požiadaviek odhlásenia používateľa.

UE môže odhlásiť všetky kontaktné adresy viazané s verejnou používateľskou identitou a asociované s privátnou používateľskou identitou. UE musí poslať samostatnú REGISTER správu, s použitím jednej kontaktnej adresy a verejnej používateľskej identity, ktorú ide odhlásiť v *To* hlavičke. A samostatnú *Contact* hlavičku s hodnotou *"*"*, a *Expires* hlavičku nastavenou na *"0"*. UE nesmie zahrnúť *"instance-id"* a *"reg-id"* parametre hlavičky v *Contact* hlavičke v tejto REGISTER požiadavke.

V prípade prijatia správy 401 Unauthorized sa UE musí správať podľa krokov popísaných v kapitole 5.1.1.2.

Po prijatí 200 OK ako odpoveď na odhlasovaniu správu REGISER UE musí zmazať všetky detaily o registrácii odhlasovanej verejnej používateľskej identity a asociovanej kontaktnej adresy. UE si uloží plán médií od P-CSCF, ktoré prijal v *Security-*

Server hlavičke. Pokiaľ neostala žiadna verejná používateľská identita registrovaná, UE musí zmazať všetky plány médií a pridružené kľúče bezpečnostných asociácií, tiež sa UE odhlási sa z asociovaného *reg event* balíka.

5.1.1.4. Inicializácia hovoru

Pre začatie signalizácie hovoru musí UE odoslať požiadavku INVITE. Detailný priebeh signalizácie hovoru je popísaný v kapitole 2.5.1.

UE musí po prijatí 200 OK odpovede na INVITE správu potvrdiť prijatie odoslaním ACK požiadavky. Na ukončenie dialógu musí UE poslať BYE požiadavku.

Ak koncové UE vyžaduje spoľahlivé vyzváňanie zo zdrojovej strany, UE musí poslať odpoveď 180 Ringing spoľahlivo.

5.1.2. Z pohľadu P-CSCF

P-CSCF musí podporovať *Path* a *Service-route* hlavičky. Keď P-CSCF posiela požiadavky alebo odpovede k UE, pred ich odoslaním musí zmazať *P-Charging-Function-Addresses* a *P-Charging-Vector* hlavičky správ, ak existujú.

Keď P-CSCF prijme požiadavky alebo odpovede od UE, P-CSCF musí:

- Musí zmazať *P-Charging-Function-Addresses* a *P-Charging-Vector* hlavičky správ, ak existujú a ignorovať obsah týchto hlavičiek.
- Môže vložiť hodnoty uložených *P-Charging-Function-Addresses* a *P-Charging-Vector* hlavičiek pred odosielaním správy.
- Musí zmazať *P-Access-Network-Info* hlavičku, ak požiadavka alebo odpoveď obsahuje *P-Access-Network-Info* hlavičku s parametrom *"network-provided"*.
- Môže vložiť *P-Access-Network-Info* hlavičku ak sú odpovede a požiadavky odosielané použitím:
  - xDSL – pole *access-type* naplní príslušným typom, vloží parameter *"network-provided"* a naplní parameter *"dsl-location"*.
  - Ethernet – pole *access-type* naplní príslušným typom, ak je použitý NASS subsystém, tak vloží parameter *"network-provided"* a naplní parameter *"eth-location"*.
  - Fiber (optika) – pole *access-type* naplní príslušným typom, ak je použitý NASS subsystém, tak vloží parameter *"network-provided"* a naplní parameter *"fiber-*

location".

- DOCSIS – pole *access-type* naplní typom *"DOCSIS"*, a vloží parameter *"network-provided"*.
- 3GPP – pole *access-type* naplní príslušným typom a vloží parameter *"network-provided"*.

Keď P-CSCF príjme požiadavky alebo odpovede obsahujúce *P-Media-Authorization* hlavičku, P-CSCF ju musí zmazať.

P-CSCF môže pridať, odobrať alebo modifikovať *P-Early-Media* hlavičku, v rámci smerovania požiadaviek a odpovedí podľa RFC 5009.

5.1.2.1. Registrácia

P-CSCF musí byť pripravený prijať nechránené REGISTER požiadavky na predvolenom SIP porte definovanom v [6]. P-CSCF tiež musí byť pripravený prijať požiadavky na porte, ktorý sa UE dozvedel počas vyhľadávania P-CSCF.

P-CSCF musí rozlišovať medzi bezpečnostnými mechanizmami pomocou *Security-Client* hlavičky a *Authorization* hlavičky.

Keď P-CSCF príjme od UE REGISTER požiadavku, P-CSCF musí:

- Vložiť *Path* hlavičku obsahujúcu SIP URI identifikujúce P-CSCF.
- Vložiť *Require* hlavičku obsahujúcu voliteľnú značku *"path"*.
- Vložiť *P-Charging-Vector* hlavičku s parametrom *"icid-value"* podľa špecifikácie 3GPP TS 32.260. P-CSCF tiež musí vložiť *"orig-ioi"* parameter hlavičky, ktorý musí nastaviť na hodnotu, ktorá identifikuje odosielajúcu sieť požiadavky. P-CSCF nesmie pridať *"term-ioi"* parameter hlavičky.
- Vložiť *P-Visited-Network-ID* hlavičku na hodnotu reťazca, ktorý identifikuje sieť iného operátora v domovskej sieti.
- Pokiaľ REGISTER požiadavka obsahuje v *Authorization* hlavičke *"integrity-protected"* parameter musí ho P-CSCF zmazať.
- Pokiaľ REGISTER požiadavka obsahuje *Authorization* hlavičku aktualizuje parameter *"integrity-protected"*.
- Pokiaľ v REGISTER požiadavke *Via* hlavička obsahuje IP adresu, ktorá sa líši od zdrojovej adresy IP paketu, P-CSCF musí pridať *"received"* parameter do *Via* hlavičky v súlade s postupom definovaným v [6].

- Ak P-CSCF pridal *"received"* parameter a transportný protokol je požitý UDP, P-CSCF tiež pridá *"rport"* parameter do *Via* hlavičky so zdrojovým číslom portu prijatej REGISTER správy.

Keď P-CSCF príjme 200 OK odpoveď na REGISTER požiadavku, P-CSCF musí skontrolovať hodnotu vypršania registrácie. Pokiaľ je rôzna od *0* P-CSCF musí:

- Uložiť zoznam trasy k službám zo *Service-Route* hlavičky. P-CSCF musí tento zoznam trasy použiť na overenie platnosti smerovacích informácií požiadaviek od UE. Pokiaľ zoznam zo *Service-Route* hlavičky existuje pre danú kontaktnú adresu, potom P-CSCF musí nahradiť existujúci zoznam trasy k službám hodnotami *Service-Route* hlavičky prichádzajúcej 200 OK odpovede.
- Asociovať zoznam trasy k službám s registrovanou verejnou používateľskou identitou, jej asociovaných kontaktných adries a asociovaných bezpečnostných asociácií lebo TLS relácií.
- Uložiť verejnú používateľskú identitu, ktorú nájde v *P-Associated-URI* hlavičke.
- Uložiť predvolenú používateľskú identitu, pre použitie procedúr s hlavičkou *P-Asserted-Identity*, ktorá bude slúžiť pre požiadavky od UE v rámci bezpečnostnej asociácie alebo TLS relácie. Predvolená používateľská identita je tá, ktorá je prvá v zozname SIP URI v hlavičke *P- Associated-URI* hlavičke.
- Uložiť hodnotu z *P-Charging-Function-Addresses* hlavičky.
- Uložiť hodnotu *"term-ioi"* parametra hlavičky *P-Charging-Vector*, ak existuje.
- Ak P-CSCF deteguje, že sa UE nachádza za NAT a *Via* hlavička od UE obsahovala *"keep"* parameter, potom P-CSCF musí pridať hodnotu k tomuto parametru, aby naznačil, že si praje posielať *keep-alive* správy asociované s registráciu daného UE, ako je definované v RFC 6223.

Ak P-CSCF deteguje, že sa UE nachádza za NAT a požiadavka bola prijatá cez TCP spojenie, P-CSCF nesmie uzatvoriť TCP spojenie počas trvania registrácie.

5.1.2.2. Odhlásenie

Keď P-CSCF prijme odpoveď 200 OK na REGISTER požiadavku poslanú UE, P-CSCF musí skontrolovať každú *Contact* hlavičku zahrnutú v odpovedi. Pokiaľ *Contact*

hlavička obsahuje kontaktnú adresu registrovanú cez toto P-CSCF cez bezpečnostnú asociáciu alebo TLS reláciu a hodnota vypršania registrácie je rovná *nule,* potom P-CSCF musí:

- Ak *Contact* hlavička neobsahuje *"reg-id"* parameter musí odstrániť všetky mapovania medzi verejnou používateľskou identitou nájdenou v *To* hlavičke a kontaktnou adresou v *Contact* hlavičke.
- Ak *Contact* hlavička obsahuje *"reg-id"* parameter musí P-CSCF odstrániť všetky mapovania medzi verejnou používateľskou identitou nájdenou v *To* hlavičke a tokom identifikovaným *"reg-id"* parametrom.
- Ak nie je použitých viacero registrácií, musí P-CSCF skontrolovať, či existujú ďalšie registrácie verejnej používateľskej identity. Keď sú všetky verejné používateľské identity, ktoré zaregistroval tento P-CSCF odhlásené, P-CSCF musí zmazať všetky bezpečnostné asociácie, TLS relácie alebo IP asociácie voči UE, po skončení transakcie vzťahujúcej sa k tomuto odhláseniu.

5.1.2.3. Inicializácia hovoru

P-CSCF musí odpovedať na všetky INVITE požiadavky informačnou správou 100 Trying.

P-CSCF musí pridať *access-network-charging-info* parameter *P-Charging-Vector* hlavičky do prvej požiadavky od UE.

Po obdržaní informácie, že QoS alebo prenosové prostriedky už nie sú k dispozícii pre aktuálne vytváranú multimediálnu reláciu, P-CSCF musí zrušiť dialóg nasledovnými krokmi:

- Odošle správu CANCEL na zrušenie INVITE požiadavky volanému UE obsahujúcu *Reason* hlavičku so statusom 503 (Service Unavailable).
- Na prijatú požiadavku INVITE pošle chybovú odpoveď 503 Service Unavailable.

V prípade, že prenosové prostriedky nie sú dostupné počas existujúcej relácie, alebo P-CSCF deteguje, že SDP nesie v SIP odpovedi parametere, ktoré nevyhovujú politike operátora, potom P-CSCF musí vygenerovať BYE požiadavku volanému používateľovi.

5.2. Klienti

Porovnanie správania IMS klientov. Testovali sme Monster IMS, Boghe IMS a UCT IMS klientov.

5.2.1. Monster IMS klient

Testovanie vlastností Monster IMS klienta, verzia 0.9.25.

5.2.1.1. Registrácia

Porovnanie s požiadavkami zo špecifikácie popísaných v kapitolách 5.1.1.1. a 5.1.1.2 a zachytenou komunikáciu v prílohe A.1.

Pri počiatočnej REGISTER správe sú tieto nedostatky:

- Vo Via hlavičke neuvádza "rport" parameter.
- Neuvádza interval vypršania registrácie (Expires) na hodnotu 600000, ale 3600 sekúnd. Túto hodnotu má používateľ možnosť zmeniť.
- V *Contact* hlavičke uvádza *"+sip.instance"* parameter, no nepridáva *Supported: gruu* hlavičku.
- Nepridáva *Supported* hlavičku s *"path"* značkou.
- Neobsahuje *Security-Client* a *P-Access-Network-Info* hlavičky.

Odpoveď REGISTER na 401 Unauthorized správu:

- Verzia Monster 0.9.13 neobsahovala rovnaké *Call-ID* ako 401 Unauthorized správa. Vo verzii Monster 0.9.25 je tento problém už odstránený.
- Inak vyhovuje požiadavkám zo špecifikácie.

5.2.1.2. Podpora autentifikačných schém

Overenie podpory autentifikačných schém u klienta Monster. Uvádzame ukážky *Authorization* hlavičiek, ktoré posiela v REGISTER správach.

Ukážka *Authorization* hlavičky REGISTER správy s AKAv1-MD5:

```
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="iQvaFMVrByYxCqNENskDB
++CBdWw3AAAWWCKr8z9BHE=",uri="sip:ims3.sip.uniza.sk",algoritm=AKAv1-
MD5,response="29524966c77da7b296ea509219e08955",qop=auth-
int,nc=00000001,cnonce="48519848525554102"
```

Túto autentifikáciu podporuje, odpoveď dostáva 200 OK.

Authorization hlavička REGISTER správy s AKAv2-MD5:

```
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="ogk/As1xq0vZ2ErL1OjL8
BsVylHR5QAAtCVdXtko+uQ=",uri="sip:ims3.sip.uniza.sk",algoritm=AKAv2-
MD5,response="3be6083db5f7b7c79a1bc783a83c96f5",qop=auth-
int,nc=00000001,cnonce="10210254571011015549"
```

Túto autentifikáciu nespracuje klient správne, odpoveď dostáva 401 Unauthorized.

Authorization hlavička REGISTER správy s MD5 digest autentifikáciou:

```
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="559cf4f3ae42725d4c81b
b6bfb6575a4",uri="sip:ims3.sip.uniza.sk",algoritm=MD5,response="1a6823ccfd69b6a14966184ab98
6fb4e",qop=auth-int,nc=00000001,cnonce="1005456102102485351"
```

Autentifikáciu MD5 podporuje, odpoveď dostáva 200 OK.

5.2.1.3. Odhlásenie

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.1.3. a zachytenou komunikáciu v prílohe A.4.

Nedostatky rovnaké ako pri REGISTER správach popísaných v kapitole 5.2.1.1. Interval vypršania registrácie (Expires) uvádza správne na hodnotu 0. Ďalším nedostatkom je, že prvej REGISTER správe v *Authorization* hlavičke posiela naplnené parametere *"nonce"* a *"response"*, namiesto prázdnych.

5.2.1.4. Inicializácia hovoru

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.1.4. a zachytenou počiatočnou správou INVITE v prílohe A.7.

Klient pridáva *Supported* hlavičku s podporou spoľahlivého doručovania správ parametrom *"100rel"* iba po zapnutí tejto voľby používateľom.

5.2.2. Boghe IMS klient

Testovanie vlastností Boghe IMS klienta, verzia 2.0.97.687.

5.2.2.1. Registrácia

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.1.1. a 5.1.1.2 a zachytenou komunikáciu v prílohe A.2.

Počiatočná REGISTER správa má nasledovný nedostatok:

- Neobsahuje *Security-Client* hlavičku.

Odpoveď REGISTER na 401 Unauthorized správu vyhovuje špecifikácii.

5.2.2.2. Podpora autentifikačných schém

Overenie podpory autentifikačných schém u klienta Boghe. Uvádzame ukážky *Authorization* hlavičiek, ktoré posiela v REGISTER správach.

Ukážka *Authorization* hlavičky REGISTER správy s AKAv1-MD5:

```
Authorization: Digest
username="jano@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="2B6YQRI5BFtSfQgLg7KwnfGd
OrB7FwAAWGCm1NSX9x8=",uri="sip:ims3.sip.uniza.sk",response="6813b449e6de618262847dedf3673ab
a",algorithm=AKAv1-MD5,cnonce="a6bd5c5f00781209142ff6412b540174",qop=auth-int,nc=00000001
```

Túto autentifikáciu podporuje, odpoveď dostáva 200 OK.

Authorization hlavička REGISTER správy s AKAv2-MD5:

```
Authorization: Digest
username="jano@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="0BehZuaHv8jzfY4+orJtMltt
B4sz7QAA41fiX0xxZfM=",uri="sip:ims3.sip.uniza.sk",response="7025bba791a6957d665bb9be802e59a
a",algorithm=AKAv2-MD5,cnonce="83f53ad5984554fd357d3d5104bec531",qop=auth-int,nc=00000001
```

Aj túto autentifikáciu podporuje, odpoveď dostáva 200 OK.

Authorization hlavička REGISTER správy s MD5 digest autentifikáciou:

```
Authorization: Digest
username="jano@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="d8c8ff31a50c7600a8a1d608
e500d62b",uri="sip:ims3.sip.uniza.sk",response="275182bcd0dc036fdbac5118934a77ed",algorithm
=MD5,cnonce="2f99f32e9e4bc32371289decfcc4f638",qop=auth-int,nc=00000001
```

Klient podporuje aj MD5, odpoveď dostáva 200 OK.

5.2.2.3. Odhlásenie

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.1.3. a zachytenou komunikáciu v prílohe A.5.

Nedostatky rovnaké ako pri REGISTER správach popísaných v kapitole 5.2.2.1. Ďalším nedostatkom je, že prvej REGISTER správe v *Authorization* hlavičke posiela naplnené parametere *"nonce"* a *"response"*, namiesto prázdnych a navyše pridáva *"cnonce", "qop"* a *"nc"* parametre.

5.2.2.4. Inicializácia hovoru

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.1.4. a zachytenou počiatočnou správou INVITE v prílohe A.8.

Správa INVITE posielaná klientom Boghe vyhovuje špecifikácii.

5.2.3. UCT IMS klient

Testovanie vlastností UCT IMS klienta, verzia 1.0.13, upravená kolegami z Fakulty informatiky a informačných technológií Slovenskej technickej univerzity v Bratislave.

Upravené boli závislosti knižníc na spoluprácu s novými knižnicami libVLC 2.0.

5.2.3.1. Registrácia

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.1.1. a 5.1.1.2 a zachytenou komunikáciu v prílohe A.3.

Počiatočná REGISTER správa má nasledovné nedostatky:

- V *Authorization* hlavičke nenastavuje *nonce* a *response* na prázdne reťazce ale na medzery.
- Neobsahuje *Security-Client* a *P-Access-Network-Info* hlavičky.

Odpoveď REGISTER na 401 Unauthorized správu:

- Nepridáva do *Authorization* hlavičky parametre *"qop"* a *"nonce-count"*.

5.2.3.2. Podpora autentifikačných schém

Overenie podpory autentifikačných schém u klienta Boghe. Uvádzame ukážky *Authorization* hlavičiek, ktoré posiela v REGISTER správach. Klient nepridáva žiadne dodatočné parametre okrem *"nonce"* a *"response"*.

Ukážka *Authorization* hlavičky REGISTER správy s AKAv1-MD5:

```
Authorization: Digest username="student@ims3.sip.uniza.sk", realm="ims3.sip.uniza.sk",
nonce="O3OWbuntozEeLfSot+7J7PU2oL3l+gAAGr80PmdMU5M=", uri="sip:ims3.sip.uniza.sk",
response="7fe608af898ff7a29c71c9f0af5f4350", algorithm=AKAv1-MD5
```

Túto autentifikáciu UTC klient podporuje, odpoveď dostáva 200 OK.

Authorization hlavička REGISTER správy s AKAv2-MD5:

```
Authorization: Digest username="student@ims3.sip.uniza.sk", realm="ims3.sip.uniza.sk",
nonce="Brnzp0uAW8AFb6+Fa5PFpAb6STU5MQAAzypkuM0sODo=", uri="sip:ims3.sip.uniza.sk",
response="e321d05b686c7369617d532e91e3b043", algorithm=AKAv2-MD5
```

Túto autentifikáciu nespracuje klient správne, odpoveď dostáva 401 Unauthorized.

Authorization hlavička REGISTER správy s MD5 digest autentifikáciou:

```
Authorization: Digest username="student@ims3.sip.uniza.sk", realm="ims3.sip.uniza.sk",
nonce="13f58928731f440ef30f83f6c0cfc08a", uri="sip:ims3.sip.uniza.sk",
response="0eeda3a5a69f598c114dc808db47aa3d", algorithm=MD5
```

Autentifikáciu MD5 podporuje, odpoveď dostáva 200 OK.

5.2.3.3. Odhlásenie

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.1.3. a zachytenou komunikáciu v prílohe A.6.

Nedostatky rovnaké ako pri REGISTER správach opísaných v kapitole 5.2.3.1.

5.2.3.4. Inicializácia hovoru

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.1.4. a zachytenou počiatočnou správou INVITE v prílohe A.9.

Správa INVITE posielaná UCT klientom vyhovuje špecifikácii.

5.2.4. Zhrnutie klientov

Ani jeden z klientov nepodporuje viacnásobnú registráciu, z toho dôvodu táto funkcionalita nemohla byť otestovaná.

V nasledovnej tabuľke 5.1 uvádzame prehľad nedostatkov zistených pri testovaní správania klientov.

Klienti	Monster	Boghe	UCT
Registrácia			
REGISTER	Vo Via neuvádza "rport", Expires iná hodnota, nepridáva Supported: gruu ani Supported: path, neobsahuje Security-Client a P-Access-Network-Info	Neobsahuje Security-Client	V Authorization "nonce" a "response" nie prázdne, Neobsahuje Security-Client a P-Access-Network-Info
REGISTER (odpoveď na 401)	Vyhovuje špecifikácii	Vyhovuje špecifikácii	V Authorization chýbajú "qop" a "nonce-count"
Ohlásenie	Rovnaké ako pri registrácii, nie prázdne "nonce" a "response"	Neobsahuje Security-Client, V Authorization nie prázdne "nonce" a "response" , navyše "cnonce", "qop" a "nc"	Rovnaké ako pri registrácii
Inicializácia hovoru	Voliteľné Supported: 100rel	Vyhovuje špecifikácii	Vyhovuje špecifikácii

Tab. 5.1: Hodnotenie IMS klientov

Z nášho testovania vyplynulo, že najmenej nedostatkov má klient Boghe, ktorý nevyhovel jedine v bezpečnostných požiadavkách. Preto odporúčame požívať Boghe IMS klienta na OS Windows v rámci IMS komunikačnej platformy. Na OS Linux odporúčame používať Monster IMS klienta, ktorý napriek chýbajúcim hlavičkám ponúka oproti UCT IMS klientovi prívetivejšie používateľské rozhranie a viacero funkcionalít popísaných v tabuľke 3.2.

5.3. P-CSCF

Správanie P-CSCF servera vo vytvorenej Kamailio IMS komunikačnej platforme.

5.3.1. Registrácia

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.2.1. a zachytenou komunikáciu medzi P-CSCF a I-CSCF v prílohe B.1., počas registrácie UE.

Pridanie hlavičiek do správy REGISTER vyhovuje špecifikácii. Spáva 200 OK ako odpoveď na REGISTER správu neobsahuje *P-Charging-Vector* hlavičku s parametrom *"term-ioi"*.

5.3.2. Odhlásenie

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.2.2. a zachytenou komunikáciu medzi P-CSCF a I-CSCF v prílohe B.2., počas registrácie UE.

Správanie pri odhlásení vyhovuje špecifikácii.

5.3.3. Inicializácia hovoru

Porovnanie s požiadavkami zo špecifikácie popísaných v 5.1.2.3. a zachytenou INVITE správou odoslanou z UE a posielanou z P-CSCF na S-CSCF v prílohe B.3.

P-CSCF nepridáva do hlavičky *P-Charging-Vector* parameter *access-network-charging-info*.

5.3.4. Zhodnotenie

V nasledovnej tabuľke 5.2 uvádzame prehľad nedostatkov zistených pri testovaní správania P-CSCF servera.

	P-CSCF
Registrácia	
REGISTER	Vyhovuje špecifikácii
200 OK	V P-Charging-Vector neuvádza "term-ioi"
Ohlásenie	Vyhovuje špecifikácii
Inicializácia hovoru	V P-Charging-Vector neuvádza access-network-charging-info

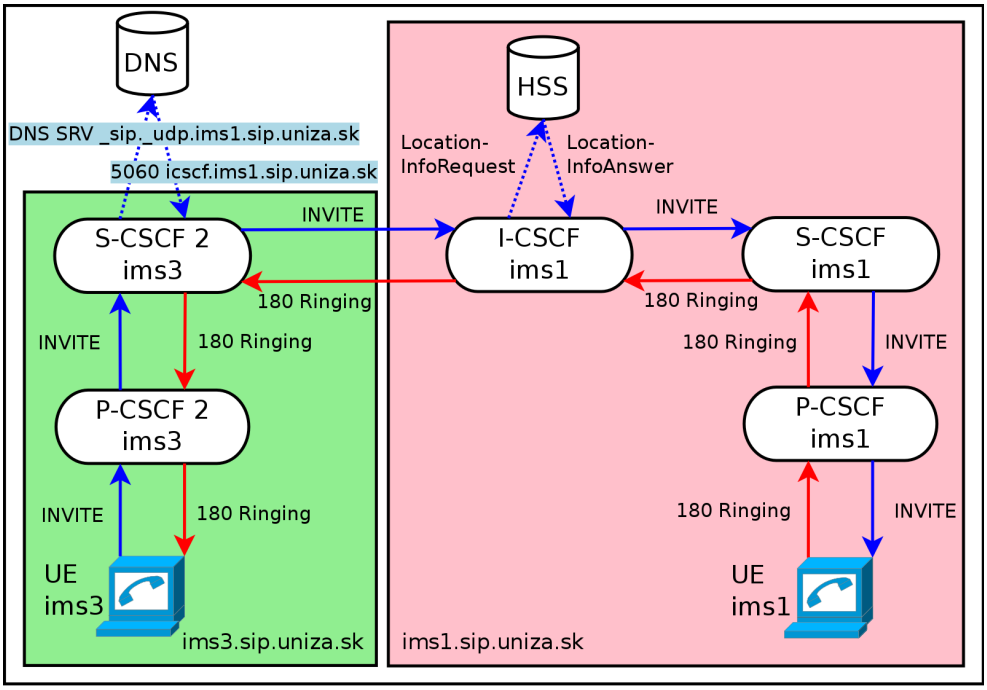
Tab. 5.2: Hodnotenie P-CSCF

5.4. Medzidoménová komunikácia

O medzidoménovej komunikácii hovoríme v prípade, keď chce používateľ pomocou UE v domácej sieti kontaktovať UE v sieti iného operátora.

UE musí vygenerovať INVITE požiadavku a poslať ju na svoj P-CSCF, ktorý ju musí poslať na obslužný S-CSCF server. S-CSCF podľa popisu v kapitole 2.3.3. musí získať adresu vstupného bodu podľa SIP URI cieľového operátora. Vykonáva to pomocou DNS SRV požiadavky na doménu daného operátora. Získa adresu I-CSCF servera, na ktorú smeruje INVITE požiadavku. I-CSCF sa správa podľa popisu v kapitole 2.5.1. a posiela INVITE na S-CSCF. Podobne S-CSCF na P-CSCF a následne P-CSCF na volané UE.

Príklad medzidoménovej komunikácie možno vidieť na obrázku 5.1, kde podľa zachytenej komunikácie v prílohe C, S-CSCF správne vyhľadá kontaktný bod a odošle INVITE požiadavku na I-CSCF z domény operátora *ims1.sip.uniza.sk*.



Obr. 5.1: Tok správ medzidoménovej signalizácie hovoru

6. ZÁVER

Témou diplomovej práce je návrh a implementácia prototypu IMS komunikačnej platformy založenej na základe existujúcich produktov s otvoreným zdrojovým kódom.

Práca poskytuje prehľad NGN a IMS architektúry, IMS entít, protokolov a služieb, podporovaných v komunikačnej platforme. Práca analyzuje vhodné otvorené riešenia pre vytvorenie IMS testovacej platformy, zaoberá sa technickými aspektmi realizácie a ponúka prehľad dostupných IMS klientov.

V práci je popísaný postup realizácie a inštalácie IMS komunikačnej platformy založenej na riešení Kamailio IMS. Práca popisuje riešenia jednotlivých technických aspektov a čiastkových problémov. Nie všetky riešenia sú plne funkčné, dôvodom je neúplná podpora zo strany modulov Kamailio IMS. Autori projektu Kamailio IMS v súčasnosti vyvíjajú novšiu verziu produktu, ktorá by mala odstrániť zistené problémy.

Vytvorená IMS komunikačná platforma poskytuje možnosť otestovať správanie jednotlivých entít, protokolov a služieb. Nad realizovanou komunikačnou platformou bola vykonaná analýza správania so zameraním na vzájomnú komunikáciu IMS klientov a P-CSCF servera a porovnanie konformnosti voči 3GPP špecifikácii 24.229. V práci detailne popisujeme správanie požadované špecifikáciou 3GPP TS 24.229 a porovnávame vlastnosti platformy analýzou zachytenej reálnej komunikácie. Výsledkom boli odhalené určité nedostatky pri vytváraní SIP požiadaviek. Z pohľadu IMS klientov najviac vyhovuje Boghe IMS klient, ktorého nedostatky sú jedine v bezpečnostných požiadavkách.

7. ZOZNAMY

7.1. Zoznam bibliografických odkazov

[1] Piokselkä, M., Mayer, G.: The IMS: IP Multimedia Concepts and Services, Whiley, Third Edition, Jan. 2009, ISBN: 978-0-470-72196-4

[2] Yao, F., Zhang, L.: OpenIMS and Interoperability with Asterisk/Sip Express VOIP Enterprise Solutions, Agder University, Máj 2007

[3] Broman, L.: IMS platform prototype, Luleå University of Technology, 2008

[4] 3GPP: IP Multimedia Subsystem (IMS); Stage 2 , 3GPP TS 23.228, V11.4.0, Mar. 2012

[5] 3GPP: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, 3GPP TS 24.229, V11.3.0, Mar. 2012

[6] Rosenberg, J. et. al.: SIP: Session Initiation Protocol, RFC 3261, Jún 2002

[7] Calhoun, P. et al.: Diameter Base Protocol, RFC 3588, Sep. 2003

[8] Segeč, P., Kováčiková, T.: Implementation of IMS testbeds using OpenSource platforms, In: Journal of Information, Control and Management Systems, University of Žilina, 2012, ISSN 1336-1716

[9] Segeč, P.: SIP over NAT [SIP cez NAT]. In: Journal of Information, Control and Management Systems, Vol. 7, No. 1, s. 89-95., 2009, ISSN 1336-1716

[10] Handley, M. et. al: SDP: Session Description Protocol, RFC 4566, Júl 2006

[11] de Gouveia, F.C. et. al: The role of open ims testbeds in complex service delivery platforms, Fraunhofer FOKUS, Berlin, Dec. 2007, ISBN: 978-1-4244-0987-7, DOI: 10.1109/AFRCON.2007.4401492

[12] Mirela, D.-C.: Two technologies striking back in VoIP - part II, Máj 2011, <http://by-miconda.blogspot.com/2011/05/two-technologies-striking-back-in-voip.html>

[13] Sippy RTPproxy, Jún 2010, <http://www.rtpproxy.org/wiki/RTPproxy>

[14] Dierks, T. et. al.: The Transport Layer Security (TLS) Protocol, Version 1.2, RFC 5246, Aug. 2008

[15] ITU-T's Definition of NGN, Sep. 2010, <http://www.itu.int/en/ITU-T/gsi/ngn/Pages/definition.aspx>

[16] George, J.: DNS Configuration, SIP.edu Cookbook, Máj 2003, <http://mit.edu/sip/sip.edu/dns.shtml>

[17] Das, K.: IPv6 - The Next Generation Internet, 2008, <http://ipv6.com/articles/general/ipv6-the-next-generation-internet.htm>

[18] Kent, S., Seo, K.: Security Architecture for the Internet Protocol, RFC 4301, Dec. 2005

[19] Domovská stránka projektu OpenIMScore <http://www.openimscore.org/>

[20] Domovská stránka projektu Kamailio (OpenSER) <http://www.kamailio.org/>

[21] The 2012 ITSPA Awards, Mar. 2012, <http://www.itspaawards.org.uk/>

[22] Installing base Kamailio IMS platform on the debian squeeze – 32bit, Portál NIL (Network information library knowledge portal), Mar. 2011, <http://nil.uniza.sk/ngnims/kamailio-ims/installing-base-kamailio-ims-platform-debian-squeeze-32bit>

[23] Adding a new user to IMS platform using the HSS web GUI, Portál NIL (Network information library knowledge portal, Apr. 2011, <http://nil.uniza.sk/ngnims/kamailio-ims/adding-new-user-ims-platform-using-hss-web-gui>

[24] Extending PCSCF of the Kamailio IMS platform with NAT traversal, Portál NIL (Network information library knowledge portal), Apr. 2011, <http://nil.uniza.sk/ngnims/kamailio-ims/extending-pcscf-kamailio-ims-platform-nat-traversal>

[25] Installing and configuring Restund - STUN/TURN server,
Portál NIL (Network information library knowledge portal), Feb. 2012,
<http://nil.uniza.sk/sip/installing-and-configuring-restund-stunturn-server>

[26] Paz, A.: IMS SIP: For Widespread Next Generation Networks,
Enterprise Messaging News, Feb. 2007
<http://www.enterprisemessagingnews.com/enterprisemessagingnews-79-20070212IMSSIPForWidespreadNextGenerationNetworks.html>

[27] Six open-source IMS clients - features overview - February 2012,
Portál NIL (Network information library knowledge portal), Feb. 2012,
<http://nil.uniza.sk/ngnims/six-open-source-ims-clients-features-overview-february-2012>

[28] Mirela, D.-C.: Run your own SIP VoIP service on both IPv4 and IPv6,
Jún 2011, <http://kb.asipto.com/kamailio:kamailio-mixed-ipv4-ipv6>

[29] IMS - Problem troubleshooting,
Portál NIL (Network information library knowledge portal), Mar. 2011,
<http://nil.uniza.sk/ngnims/ims-problem-troubleshooting>

[30] GSMA, Rich Communications, RCS Product Specifications, 2012,
<http://www.gsma.com/rcs-product-specifications/>

[31] Installing additional serving S-CSCF server into Kamailio IMS
environment, Portál NIL (Network information library knowledge portal),
<http://nil.uniza.sk/ngnims/kamailio-ims/installing-additional-serving-s-cscf-server-kamailio-ims-environment>

[32] Configuring TLS support in Kamailio 3.1 – Howto,
Portál NIL (Network information library knowledge portal), Nov. 2010,
<http://nil.uniza.sk/network-security/tls/configuring-tls-support-kamailio-31-howto>

[33] How to enable roaming in IMS platform using the HSS web GUI,
Portál NIL (Network information library knowledge portal), Máj 2012,
<http://nil.uniza.sk/ngnims/kamailio-ims/how-enable-roaming-ims-platform-using-hss-web-gui>

7.2. Zoznam používaných skratiek

- 3G – 3rd generation
- 3GPP – 3rd Generation Partnership Project
- AAA – Authentication, Authorization, Accounting
- ACK – Acknowledgement
- AES – Advanced Encryption Standard
- AH – Authentication Header
- AKA – Authentication and Key Agreement
- AS – Aplikačný Server
- AUTN – Authentication Token
- BGCF – Breakout Control Gateway Functions
- CCF – Charging Collection Function
- CDR – Call Detail Record
- CPM – Converged IP Messaging
- CPU – Central Processing Unit
- CSCF – Call Session Control Functions
- DNS – Domain Name System
- DOCSIS – Data Over Cable Service Interface Specification
- DSL – Digital subscriber line
- E-CSCF – Emergency Call Session Control Function
- ECF – Event Charging Function
- ESP – Encapsulating Security Payload
- ETSI – European Telecommunications Standards Institute
- FhoSS – FOKUS Home Subscriber Server
- FOKUS – Fraunhofer Institute for Open Communication Systems
- FQDN – Fully qualified domain name
- FRI – Fakulta riadenia a informatiky
- GNU – GNU's Not Unix
- GPL – General Public License
- GPL – GNU Public License
- GRUU – Globally Routable User Agent URI
- GSM – Global System for Mobile Communications
- GSMA – GSM Association
- HSS – Home Subscriber Server
- HTTP – Hypertext Transfer Protocol
- I-CSCF – Interrogating Call Session Control Function
- IARI – IMS Application Reference Identifier
- IBCF – Interconnection Border Control Function
- ICE – Interactive Connectivity Establishment
- ICSI – IMS Communication Service Identifier
- ID – Identifier
- IETF – Internet Engineering Task Force
- IM – Instant Messaging

- IM-MGW – IP Multimedia Gateway Functions
- IMEI – International Mobile Equipment Identity
- IMS – IP Multimedia Subsystem
- IN – Internet
- IP – Internet Protocol
- IPSec – Internet Protocol Security
- IPSPA – Internet Telephony Services Providers Association
- IPTV – Internet Protocol television
- IPv4 – Internet Protocol Version 4
- IPv6 – Internet Protocol Version 6
- ITSPA – Internet Telephony Services Providers Association
- ITU-T – International Telecommunication Union-Telecommunication Standardization Sector
- LGPL – Lesser General Public License
- LRF – Location Retrieval Function
- LTE – Long Term Evolution
- MD5 – Message-Digest 5
- MEID – Mobile Equipment Identifier
- MGCF – Media Gateway Control Function
- MMS – Multimedia Messaging Service
- MPEG – Motion Picture Experts Group
- MPS – Multimedia Priority Service
- MRFC – Multimedia Resource Function Controller
- MRFP – Multimedia Resource Function Processor function
- MSRP – Message Session Relay Protocol
- NAB – Network Address Book
- NAI – Network Access Identifier
- NAPTR – Name Authority Pointer
- NASS – Network Attachment Subsystem
- NAT – Network Address Translation
- NGN – Next Generation Networks
- OMA – Open Mobile Alliance
- OS – Operačný Systém
- OSA – Open Service Architecture
- P-CSCF – Proxy Call Session Control Function
- P-GRUU – Public Globally Routable User Agent URI
- P-header – Private-Header
- PBX – Private Branch Exchange
- PCRF – Policy and Charging Rules Function
- PES – PSTN/ISDN emulation subsystem
- PRACK – Provisional Response ACKnowledgement
- PS – Presence server
- PSTN – Public Switched Telephone Network
- QoS – Quality of Service
- RACS – Resource and Admission Control Subsystem

- RADIUS – Remote Authentication Dial In User Service
- RAND – Random
- RC – Rich Communication
- RCS – Rich Communication Suite
- RCS-e – RCS-enhanced
- RES – Response
- RFC – Request for Comments
- RLS – Resource List Server
- RR – Resource Record
- RSA – Rivest, Shamir, Adleman
- RTC – Real-Time Communication
- RTP – Real-time Transport Protocol
- RTP/AVP – RTP audio video profile
- S-CSCF – Serving Call Session Control Function
- SCTP – Stream Control Transmission Protocol
- SDP – Session Description Protocol
- SEG – Security Gateway
- SER – SIP Express Router
- SGW – Signalling Gateway
- SigComp – Signaling compression
- SIMPLE – Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
- SIP – Session Initiation Protocol
- SIPS – Secure SIP
- SLF – Subscriber Location Function
- SMS – Short Message Service
- SMTP – Simple Mail Transfer Protocol
- SQL – Structured Query Language
- SRV – Service
- SSL – Secure Sockets Layer
- STUN – Simple Traversal of UDP through NAT
- T-GRUU – Temporary Globally Routable User Agent URI
- TC TISPAN – Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking
- TCP – Transmission Control Protocol
- tel – telephone
- TLS – Transport Layer Security
- TrGW – Translation Gateway
- TS – Technical Specification
- TTL – Time-to-live
- TURN – Traversal Using Relay around NAT
- UA – User Agent
- UCT – University of Cape Town
- UDP – User Datagram Protocol
- UE – User Equipment

- URI – Uniform Resource Identifier
- VoIP – Voice over Internet Protocol
- XCAP – XML Configuration Access Protocol
- XDM – Xml Document Management
- XML – eXtensible Markup Language
- ŽU – Žilinská univerzita

7.3. Zoznam ilustrácií

7.4. Zoznam tabuliek

7.5. Zoznam príloh

Príloha A: Zachytená komunikácia medzi UE a P-CSCF

A.1 Registrácia Monster IMS klienta

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Call-ID: 8ac6ffb8ac61d6937abb9688ae877a7d@172.16.1.99
CSeq: 1 REGISTER
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1000
To: "student" <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 172.16.1.99:5060;branch=z9hG4bK60664ac35fc7ddd3fdd47260be8cd78b363435
Max-Forwards: 20
Expires: 3600
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="",response="",uri="s
ip:ims3.sip.uniza.sk"
Contact: "student" <sip:student@172.16.1.99:5060>;+sip.instance=76a5671b-9b2d-4f1a-8f87-
a24ca4d0f0ae
User-Agent: monster Version: 0.9.25
Content-Length: 0
```

```
SIP/2.0 401 Unauthorized - Challenging the UE
Call-ID: 8ac6ffb8ac61d6937abb9688ae877a7d@172.16.1.99
CSeq: 1 REGISTER
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1000
To: "student" <sip:student@ims3.sip.uniza.sk>;tag=68988887aea29c51493f22b8b0542a94-3b54
Via: SIP/2.0/UDP 172.16.1.99:5060;rport=7164;received=158.193.139.187
;branch=z9hG4bK60664ac35fc7ddd3fdd47260be8cd78b363435
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
WWW-Authenticate: Digest realm="ims3.sip.uniza.sk",
nonce="1ba3a152f283117c24f3a28616296b64", algorithm=MD5, qop="auth,auth-int"
```

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Call-ID: 8ac6ffb8ac61d6937abb9688ae877a7d@172.16.1.99
CSeq: 2 REGISTER
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1001
To: "student" <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 172.16.1.99:5060;branch=z9hG4bKbca1e8f7e62d3fb0405fa193b8545a68363435
Max-Forwards: 20
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="1ba3a152f283117c24f3
a28616296b64",uri="sip:ims3.sip.uniza.sk",algoritm=MD5,response="bf43e03c2eea1c277f7fe73f3
cbc565e",qop=auth-int,nc=00000001,cnonce="102979952545110050"
Expires: 3600
Contact: "student" <sip:student@172.16.1.99:5060>;+sip.instance=76a5671b-9b2d-4f1a-8f87-
a24ca4d0f0ae
User-Agent: monster Version: 0.9.25
Content-Length: 0
```

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Call-ID: 8ac6ffb8ac61d6937abb9688ae877a7d@172.16.1.99
CSeq: 2 REGISTER
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1001
To: "student" <sip:student@ims3.sip.uniza.sk>;tag=68988887aea29c51493f22b8b0542a94-f419
Via: SIP/2.0/UDP 172.16.1.99:5060;rport=7164;received=158.193.139.187
;branch=z9hG4bKbca1e8f7e62d3fb0405fa193b8545a68363435
P-Associated-URI: <sip:student@ims3.sip.uniza.sk>
Contact: <sip:student@172.16.1.99:5060>;expires=3600;pub-
gruu="sip:student@ims3.sip.uniza.sk;gr=76a5671b-9b2d-4f1a-8f87-a24ca4d0f0ae"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Serving-CSCF
Content-Length: 0
```

A.2 Registrácia Boghe IMS klienta

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.187:56883;branch=z9hG4bK16831579;rport
From: <sip:student@ims3.sip.uniza.sk>;tag=16816835
To: <sip:student@ims3.sip.uniza.sk>
Contact: <sip:student@158.193.139.187:56883;transport=udp>;expires=600000;+g.oma.sip-
im;language="en,fr";+g.3gpp.smsip;+g.oma.sip-im.large-message;audio;+g.3gpp.icsi-ref="urn
%3Aurn-7%3A3gpp-application.ims.iari.gsma-vs";+g.3gpp.cs-voice
Call-ID: 456a595e-6608-a8fd-5f37-e79ed3983521
CSeq: 849 REGISTER
Content-Length: 0
Max-Forwards: 70
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="",uri="sip:ims3.sip.
uniza.sk",response=""
Allow: INVITE, ACK, CANCEL, BYE, MESSAGE, OPTIONS, NOTIFY, PRACK, UPDATE, REFER
Privacy: none
P-Access-Network-Info: ADSL;utran-cell-id-3gpp=00000000
User-Agent: IM-client/OMA1.0 Boghe/v2.0.97.687
P-Preferred-Identity: <sip:student@ims3.sip.uniza.sk>
Supported: path
```

```
SIP/2.0 401 Unauthorized - Challenging the UE
Via: SIP/2.0/UDP 158.193.139.187:56883;branch=z9hG4bK16831579;rport=56883
From: <sip:student@ims3.sip.uniza.sk>;tag=16816835
To: <sip:student@ims3.sip.uniza.sk>;tag=6ddfb0d30320d6fc6ec3c87d97cc8672-0e99
Call-ID: 456a595e-6608-a8fd-5f37-e79ed3983521
CSeq: 849 REGISTER
Path: <sip:term@pcscf.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
WWW-Authenticate: Digest realm="ims3.sip.uniza.sk",
nonce="e357300a78a402122d08eaa5e3e528e9", algorithm=MD5, qop="auth,auth-int"
```

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.187:56883;branch=z9hG4bK16839261;rport
From: <sip:student@ims3.sip.uniza.sk>;tag=16816835
To: <sip:student@ims3.sip.uniza.sk>
Contact: <sip:student@158.193.139.187:56883;transport=udp>;expires=600000;+g.oma.sip-
im;language="en,fr";+g.3gpp.smsip;+g.oma.sip-im.large-message;audio;+g.3gpp.icsi-ref="urn
%3Aurn-7%3A3gpp-application.ims.iari.gsma-vs";+g.3gpp.cs-voice
Call-ID: 456a595e-6608-a8fd-5f37-e79ed3983521
CSeq: 850 REGISTER
Content-Length: 0
Max-Forwards: 70
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="e357300a78a402122d08
eaa5e3e528e9",uri="sip:ims3.sip.uniza.sk",response="878731303df52715d7b8a08c4091336e",algo
rithm=MD5,cnonce="611ad3b93306456fd0b9ad860536c717",qop=auth-int,nc=00000001
Allow: INVITE, ACK, CANCEL, BYE, MESSAGE, OPTIONS, NOTIFY, PRACK, UPDATE, REFER
Privacy: none
P-Access-Network-Info: ADSL;utran-cell-id-3gpp=00000000
User-Agent: IM-client/OMA1.0 Boghe/v2.0.97.687
P-Preferred-Identity: <sip:student@ims3.sip.uniza.sk>
Supported: path
```

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Via: SIP/2.0/UDP 158.193.139.187:56883;branch=z9hG4bK16839261;rport=56883
From: <sip:student@ims3.sip.uniza.sk>;tag=16816835
To: <sip:student@ims3.sip.uniza.sk>;tag=6ddfb0d30320d6fc6ec3c87d97cc8672-71e4
Call-ID: 456a595e-6608-a8fd-5f37-e79ed3983521
CSeq: 850 REGISTER
P-Associated-URI: <sip:student@ims3.sip.uniza.sk>
Contact: <sip:student@158.193.139.187:56883;transport=udp>;expires=600000
Path: <sip:term@pcscf.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Serving-CSCF
Content-Length: 0
```

A.3 Registrácia UCT IMS klienta

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.227:5060;rport;branch=z9hG4bK631711245
From: <sip:student@ims3.sip.uniza.sk>;tag=652237848
To: <sip:student@ims3.sip.uniza.sk>
Call-ID: 1254754314
CSeq: 1 REGISTER
Contact: <sip:student@158.193.139.227:5060;line=4be170c9186c346>;
+sip.instance="<urn:uuid:44e0c3ee-8a15-11e1-947c-8fd61571057c>"
Authorization: Digest username="student@ims3.sip.uniza.sk", realm="ims3.sip.uniza.sk",
nonce=" ", uri="sip:ims3.sip.uniza.sk", response=" "
Max-Forwards: 70
User-Agent: UCT IMS Client
Expires: 600000
Supported: path
Supported: gruu
Content-Length: 0
```

```
SIP/2.0 401 Unauthorized - Challenging the UE
Via: SIP/2.0/UDP 158.193.139.227:5060;rport=5060;branch=z9hG4bK631711245
From: <sip:student@ims3.sip.uniza.sk>;tag=652237848
To: <sip:student@ims3.sip.uniza.sk>;tag=6ddfb0d30320d6fc6ec3c87d97cc8672-e3d4
Call-ID: 1254754314
CSeq: 1 REGISTER
Path: <sip:term@pcscf.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
WWW-Authenticate: Digest realm="ims3.sip.uniza.sk",
nonce="01b81aa4adb28d6c95e5b0d41a7431da", algorithm=MD5, qop="auth,auth-int"
```

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.227:5060;rport;branch=z9hG4bK329228830
From: <sip:student@ims3.sip.uniza.sk>;tag=652237848
To: <sip:student@ims3.sip.uniza.sk>
Call-ID: 1254754314
CSeq: 2 REGISTER
Contact: <sip:student@158.193.139.227:5060;line=4be170c9186c346>;
+sip.instance="<urn:uuid:44e0c3ee-8a15-11e1-947c-8fd61571057c>"
Authorization: Digest username="student@ims3.sip.uniza.sk", realm="ims3.sip.uniza.sk",
nonce="01b81aa4adb28d6c95e5b0d41a7431da", uri="sip:ims3.sip.uniza.sk",
response="a58407e0c5f904f0c07ebcc3fd70f7cd", algorithm=MD5
Max-Forwards: 70
User-Agent: UCT IMS Client
Expires: 600000
Supported: path
Supported: gruu
Content-Length: 0
```

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Via: SIP/2.0/UDP 158.193.139.227:5060;rport=5060;branch=z9hG4bK329228830
From: <sip:student@ims3.sip.uniza.sk>;tag=652237848
To: <sip:student@ims3.sip.uniza.sk>;tag=6ddfb0d30320d6fc6ec3c87d97cc8672-41ca
Call-ID: 1254754314
CSeq: 2 REGISTER
P-Associated-URI: <sip:student@ims3.sip.uniza.sk>
Contact: <sip:student@158.193.139.227:5060;line=4be170c9186c346>;expires=600000;pub-
gruu="sip:student@ims3.sip.uniza.sk;gr=urn:uuid:44e0c3ee-8a15-11e1-947c-8fd61571057c"
Path: <sip:term@pcscf.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Serving-CSCF
Content-Length: 0
```

A.4 Odhlásenie Monster IMS klienta

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Call-ID: 94521a7a9c9206610d71aa35f8da0b9a@192.168.1.4
CSeq: 3 REGISTER
From: <sip:student@ims3.sip.uniza.sk>;tag=1004
To: <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 192.168.1.4:5060;branch=z9hG4bKf352c127d426e231b63fc0c68f852a15373934
Max-Forwards: 20
Expires: 0
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="18c53dfc2d3a73167957
fbbe49513d21",response="2dca1dd42ebeaa728f28583485580deb",uri="sip:ims3.sip.uniza.sk"
Contact: "student" <sip:student@192.168.1.4:5060>;+sip.instance=7e10d1c0-d13d-4eb0-863e-
809b5401d2b2
User-Agent: monster Version: 0.9.25
Content-Length: 0
```

```
SIP/2.0 401 Unauthorized - Challenging the UE
Call-ID: 94521a7a9c9206610d71aa35f8da0b9a@192.168.1.4
CSeq: 3 REGISTER
From: <sip:student@ims3.sip.uniza.sk>;tag=1004
To: <sip:student@ims3.sip.uniza.sk>;tag=68988887aea29c51493f22b8b0542a94-f5e8
Via: SIP/2.0/UDP
192.168.1.4:5060;rport=5060;branch=z9hG4bKf352c127d426e231b63fc0c68f852a15373934
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
WWW-Authenticate: Digest realm="ims3.sip.uniza.sk",
nonce="d3ebca6dd5eb2ecb028b6fba563d2828", algorithm=MD5, qop="auth,auth-int"
```

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Call-ID: 94521a7a9c9206610d71aa35f8da0b9a@192.168.1.4
CSeq: 4 REGISTER
From: <sip:student@ims3.sip.uniza.sk>;tag=1005
To: <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 192.168.1.4:5060;branch=z9hG4bK6188cf46f95d269eb6ed565fcac174b6373934
Max-Forwards: 20
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="d3ebca6dd5eb2ecb028b
6fba563d2828",uri="sip:ims3.sip.uniza.sk",algoritm=MD5,response="19a1a895053718397659a5a65
c01d031",qop=auth-int,nc=00000001,cnonce="10297575157534854"
Expires: 0
Contact: "student" <sip:student@192.168.1.4:5060>;+sip.instance=7e10d1c0-d13d-4eb0-863e-
809b5401d2b2
User-Agent: monster Version: 0.9.25
Content-Length: 0
```

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Call-ID: 94521a7a9c9206610d71aa35f8da0b9a@192.168.1.4
CSeq: 4 REGISTER
From: <sip:student@ims3.sip.uniza.sk>;tag=1005
To: <sip:student@ims3.sip.uniza.sk>;tag=68988887aea29c51493f22b8b0542a94-3275
Via: SIP/2.0/UDP
192.168.1.4:5060;rport=5060;branch=z9hG4bK6188cf46f95d269eb6ed565fcac174b6373934
Contact: <sip:student@192.168.1.4:5060>;expires=0;pub-
gruu="sip:student@ims3.sip.uniza.sk;gr=7e10d1c0-d13d-4eb0-863e-809b5401d2b2"
Contact: <sip:student@172.16.1.99:5060>;expires=3015;pub-
gruu="sip:student@ims3.sip.uniza.sk;gr=76a5671b-9b2d-4f1a-8f87-a24ca4d0f0ae"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Serving-CSCF
Content-Length: 0
```

A.5 Odhlásenie Boghe IMS klienta

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.187:56883;branch=z9hG4bK16850644;rport
From: <sip:student@ims3.sip.uniza.sk>;tag=16816835
To: <sip:student@ims3.sip.uniza.sk>
Contact: <sip:student@158.193.139.187:56883;transport=udp>;expires=0;+g.oma.sip-
im;language="en,fr";+g.3gpp.smsip;+g.oma.sip-im.large-message;audio;+g.3gpp.icsi-ref="urn
%3Aurn-7%3A3gpp-application.ims.iari.gsma-vs";+g.3gpp.cs-voice
Call-ID: 456a595e-6608-a8fd-5f37-e79ed3983521
CSeq: 851 REGISTER
Content-Length: 0
Max-Forwards: 70
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="e357300a78a402122d08
eaa5e3e528e9",uri="sip:ims3.sip.uniza.sk",response="0a9b5be0ce7a7173cd939120bb930e96",algo
rithm=MD5,cnonce="611ad3b93306456fd0b9ad860536c717",qop=auth-int,nc=00000002
Allow: INVITE, ACK, CANCEL, BYE, MESSAGE, OPTIONS, NOTIFY, PRACK, UPDATE, REFER
Privacy: none
P-Access-Network-Info: ADSL;utran-cell-id-3gpp=00000000
User-Agent: IM-client/OMA1.0 Boghe/v2.0.97.687
P-Preferred-Identity: <sip:student@ims3.sip.uniza.sk>
```

```
SIP/2.0 401 Unauthorized - Challenging the UE
Via: SIP/2.0/UDP 158.193.139.187:56883;branch=z9hG4bK16850644;rport=56883
From: <sip:student@ims3.sip.uniza.sk>;tag=16816835
To: <sip:student@ims3.sip.uniza.sk>;tag=6ddfb0d30320d6fc6ec3c87d97cc8672-7471
Call-ID: 456a595e-6608-a8fd-5f37-e79ed3983521
CSeq: 851 REGISTER
Path: <sip:term@pcscf.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
WWW-Authenticate: Digest realm="ims3.sip.uniza.sk",
nonce="e67a046c89207d28f2f162d84e46ffda", algorithm=MD5, qop="auth,auth-int"
```

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.187:56883;branch=z9hG4bK16850626;rport
From: <sip:student@ims3.sip.uniza.sk>;tag=16816835
To: <sip:student@ims3.sip.uniza.sk>
Contact: <sip:student@158.193.139.187:56883;transport=udp>;expires=0;+g.oma.sip-
im;language="en,fr";+g.3gpp.smsip;+g.oma.sip-im.large-message;audio;+g.3gpp.icsi-ref="urn
%3Aurn-7%3A3gpp-application.ims.iari.gsma-vs";+g.3gpp.cs-voice
Call-ID: 456a595e-6608-a8fd-5f37-e79ed3983521
CSeq: 852 REGISTER
Content-Length: 0
Max-Forwards: 70
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="e67a046c89207d28f2f1
62d84e46ffda",uri="sip:ims3.sip.uniza.sk",response="aae89e50aa8c87c38d82653a7b0a9127",algo
rithm=MD5,cnonce="7c4be7fa00e28e1537ae7b5c6fcd3b9d",qop=auth-int,nc=00000001
Allow: INVITE, ACK, CANCEL, BYE, MESSAGE, OPTIONS, NOTIFY, PRACK, UPDATE, REFER
Privacy: none
P-Access-Network-Info: ADSL;utran-cell-id-3gpp=00000000
User-Agent: IM-client/OMA1.0 Boghe/v2.0.97.687
P-Preferred-Identity: <sip:student@ims3.sip.uniza.sk>
```

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Via: SIP/2.0/UDP 158.193.139.187:56883;branch=z9hG4bK16850626;rport=56883
From: <sip:student@ims3.sip.uniza.sk>;tag=16816835
To: <sip:student@ims3.sip.uniza.sk>;tag=6ddfb0d30320d6fc6ec3c87d97cc8672-a385
Call-ID: 456a595e-6608-a8fd-5f37-e79ed3983521
CSeq: 852 REGISTER
Contact: <sip:student@158.193.139.187:56883;transport=udp>;expires=0
Path: <sip:term@pcscf.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
```

A.6 Odhlásenie UCT IMS klienta

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.227:5060;rport;branch=z9hG4bK2085652251
From: <sip:student@ims3.sip.uniza.sk>;tag=652237848
To: <sip:student@ims3.sip.uniza.sk>
Call-ID: 1254754314
CSeq: 3 REGISTER
Contact: <sip:student@158.193.139.227:5060;line=4be170c9186c346>;
+sip.instance="<urn:uuid:44e0c3ee-8a15-11e1-947c-8fd61571057c>"
Authorization: Digest username="student@ims3.sip.uniza.sk", realm="ims3.sip.uniza.sk",
nonce=" ", uri="ims3.sip.uniza.sk", response=" "
Max-Forwards: 70
User-Agent: UCT IMS Client
Expires: 0
Supported: path
Supported: gruu
Content-Length: 0
```

```
SIP/2.0 401 Unauthorized - Challenging the UE
Via: SIP/2.0/UDP 158.193.139.227:5060;rport=5060;branch=z9hG4bK2085652251
From: <sip:student@ims3.sip.uniza.sk>;tag=652237848
To: <sip:student@ims3.sip.uniza.sk>;tag=6ddfb0d30320d6fc6ec3c87d97cc8672-0336
Call-ID: 1254754314
CSeq: 3 REGISTER
Path: <sip:term@pcscf.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
WWW-Authenticate: Digest realm="ims3.sip.uniza.sk",
nonce="48bcfd84dcd50b5e0117f59db8c085d0", algorithm=MD5, qop="auth,auth-int"
```

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.227:5060;rport;branch=z9hG4bK977824048
From: <sip:student@ims3.sip.uniza.sk>;tag=652237848
To: <sip:student@ims3.sip.uniza.sk>
Call-ID: 1254754314
CSeq: 4 REGISTER
Contact: <sip:student@158.193.139.227:5060;line=4be170c9186c346>;
+sip.instance="<urn:uuid:44e0c3ee-8a15-11e1-947c-8fd61571057c>"
Authorization: Digest username="student@ims3.sip.uniza.sk", realm="ims3.sip.uniza.sk",
nonce="48bcfd84dcd50b5e0117f59db8c085d0", uri="sip:ims3.sip.uniza.sk",
response="e434e209eb88f85777cfd525d7856fa9", algorithm=MD5
Max-Forwards: 70
User-Agent: UCT IMS Client
Expires: 0
Supported: path
Supported: gruu
Content-Length: 0
```

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Via: SIP/2.0/UDP 158.193.139.227:5060;rport=5060;branch=z9hG4bK977824048
From: <sip:student@ims3.sip.uniza.sk>;tag=652237848
To: <sip:student@ims3.sip.uniza.sk>;tag=6ddfb0d30320d6fc6ec3c87d97cc8672-b893
Call-ID: 1254754314
CSeq: 4 REGISTER
Contact: <sip:student@158.193.139.227:5060;line=4be170c9186c346>;expires=0;pub-
gruu="sip:student@ims3.sip.uniza.sk;gr=urn:uuid:44e0c3ee-8a15-11e1-947c-8fd61571057c"
Path: <sip:term@pcscf.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
```

A.7 Počiatočná INVITE správa Monster IMS klienta

```
INVITE sip:karol@ims3.sip.uniza.sk SIP/2.0
Call-ID: da4b01ef468329088a46285403981610@172.16.1.99
CSeq: 11 INVITE
From: <sip:student@ims3.sip.uniza.sk>;tag=1012
To: <sip:karol@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 172.16.1.99:5060;branch=z9hG4bK7032f122df91576840bfebafab7012d13239
Max-Forwards: 20
Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Content-Type: application/sdp
Contact: "student" <sip:student@172.16.1.99:5060>
Supported: 100rel
User-Agent: monster Version: 0.9.25
Content-Length: 247

v=0
o=student 3545372304 3545372304 IN IP4 172.16.1.99
s=A Funky MONSTER Stream
t=0 0
m=audio 23002 RTP/AVP 0 8 14 101
c=IN IP4 172.16.1.99
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:14 MPA/8000
a=rtpmap:101 telephone-event/8000
```

A.8 Počiatočná INVITE správa Boghe IMS klienta

```
INVITE sip:karol@ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.187:61276;branch=z9hG4bK16934448;rport
From: <sip:student@ims3.sip.uniza.sk>;tag=16935163
To: <sip:karol@ims3.sip.uniza.sk>
Contact: <sip:student@158.193.139.187:61276;transport=udp>;+g.oma.sip-im;language="en,fr";
+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
Call-ID: cabd8dcb-0626-00c8-da9b-82036511a9dd
CSeq: 3116 INVITE
Content-Type: application/sdp
Content-Length: 327
Max-Forwards: 70
Route: <sip:pcscf.ims3.sip.uniza.sk:5060;lr;transport=udp>
Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
Allow: INVITE, ACK, CANCEL, BYE, MESSAGE, OPTIONS, NOTIFY, PRACK, UPDATE, REFER
Privacy: none
P-Access-Network-Info: ADSL;utran-cell-id-3gpp=00000000
User-Agent: IM-client/OMA1.0 Boghe/v2.0.97.687
P-Preferred-Identity: <sip:student@ims3.sip.uniza.sk>
Supported: 100rel

v=0
o=doubango 1983 678901 IN IP4 158.193.139.187
s=-
c=IN IP4 158.193.139.187
t=0 0
m=audio 21940 RTP/AVP 3 8 0 97 101
c=IN IP4 158.193.139.187
a=ptime:20
a=rtpmap:3 GSM/8000/1
a=rtpmap:8 PCMA/8000/1
a=rtpmap:0 PCMU/8000/1
a=rtpmap:97 SPEEX/8000/1
a=rtpmap:101 telephone-event/8000/1
a=fmtp:101 0-15
a=sendrecv
```

A.9 Počiatočná INVITE správa UCT IMS klienta

```
INVITE sip:karol@ims3.sip.uniza.sk SIP/2.0
Via: SIP/2.0/UDP 158.193.139.227:5060;rport;branch=z9hG4bK658179787
Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1866450549
To: <sip:karol@ims3.sip.uniza.sk>
Call-ID: 1535449949
CSeq: 20 INVITE
Contact: <sip:student@158.193.139.227:5060>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Max-Forwards: 70
User-Agent: UCT IMS Client
Subject: IMS Call
P-Preferred-Identity: "student" <sip:student@ims3.sip.uniza.sk>
P-Preferred-Service: urn:xxx:3gpp-service.ims.icsi.mmtel
Privacy: none
P-Access-Network-Info: IEEE-802.11a
Require: sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Content-Length:   328

v=0
o=- 0 0 IN IP4 158.193.139.227
s=IMS Call
c=IN IP4 158.193.139.227
t=0 0
m=audio 32052 RTP/AVP 0 8 101
b=AS:64
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=curr:qos local none
a=curr:qos remote none
a=des:qos none local sendrecv
a=des:qos none remote sendrecv
```

Príloha B: Zachytená komunikácia odchádzajúca z P-CSCF

B.1 Registrácia Monster IMS klienta – správy medzi P-CSCF a I-CSCF

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Call-ID: 8ac6ffb8ac61d6937abb9688ae877a7d@172.16.1.99
CSeq: 1 REGISTER
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1000
To: "student" <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 158.193.139.22;branch=z9hG4bK0b37.6140faf5.0
Via: SIP/2.0/UDP 172.16.1.99:5060;rport=7164;received=158.193.139.187
;branch=z9hG4bK60664ac35fc7ddd3fdd47260be8cd78b363435
Max-Forwards: 19
Expires: 3600
Contact: "student" <sip:student@172.16.1.99:5060>;+sip.instance=76a5671b-9b2d-4f1a-8f87-
a24ca4d0f0ae
User-Agent: monster Version: 0.9.25
Content-Length: 0
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="",response="",uri="s
ip:ims3.sip.uniza.sk", integrity-protected="no"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd4f9ad84f00000002";icid-generated-
at=158.193.139.22;orig-ioi="ims3.sip.uniza.sk"
P-Visited-Network-ID: ims3.sip.uniza.sk
```

```
SIP/2.0 401 Unauthorized - Challenging the UE
Call-ID: 8ac6ffb8ac61d6937abb9688ae877a7d@172.16.1.99
CSeq: 1 REGISTER
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1000
To: "student" <sip:student@ims3.sip.uniza.sk>;tag=68988887aea29c51493f22b8b0542a94-3b54
Via: SIP/2.0/UDP 158.193.139.22;branch=z9hG4bK0b37.6140faf5.0
Via: SIP/2.0/UDP 172.16.1.99:5060;rport=7164;received=158.193.139.187
;branch=z9hG4bK60664ac35fc7ddd3fdd47260be8cd78b363435
WWW-Authenticate: Digest realm="ims3.sip.uniza.sk",
nonce="1ba3a152f283117c24f3a28616296b64", algorithm=MD5, qop="auth,auth-int"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
```

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Call-ID: 8ac6ffb8ac61d6937abb9688ae877a7d@172.16.1.99
CSeq: 2 REGISTER
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1001
To: "student" <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 158.193.139.22;branch=z9hG4bKda37.f4db8454.0
Via: SIP/2.0/UDP 172.16.1.99:5060;rport=7164;received=158.193.139.187
;branch=z9hG4bKbca1e8f7e62d3fb0405fa193b8545a68363435
Max-Forwards: 19
Expires: 3600
Contact: "student" <sip:student@172.16.1.99:5060>;+sip.instance=76a5671b-9b2d-4f1a-8f87-
a24ca4d0f0ae
User-Agent: monster Version: 0.9.25
Content-Length: 0
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="1ba3a152f283117c24f3
a28616296b64",uri="sip:ims3.sip.uniza.sk",algoritm=MD5,response="bf43e03c2eea1c277f7fe73f3
cbc565e",qop=auth-int,nc=00000001,cnonce="102979952545110050", integrity-protected="no"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd4f9ad84f00000003";icid-generated-
at=158.193.139.22;orig-ioi="ims3.sip.uniza.sk"
P-Visited-Network-ID: ims3.sip.uniza.sk
```

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Call-ID: 8ac6ffb8ac61d6937abb9688ae877a7d@172.16.1.99
CSeq: 2 REGISTER
From: "student" <sip:student@ims3.sip.uniza.sk>;tag=1001
To: "student" <sip:student@ims3.sip.uniza.sk>;tag=68988887aea29c51493f22b8b0542a94-f419
Via: SIP/2.0/UDP 158.193.139.22;branch=z9hG4bKda37.f4db8454.0
Via: SIP/2.0/UDP 172.16.1.99:5060;rport=7164;received=158.193.139.187
;branch=z9hG4bKbca1e8f7e62d3fb0405fa193b8545a68363435
P-Associated-URI: <sip:student@ims3.sip.uniza.sk>
Contact: <sip:student@172.16.1.99:5060>;expires=3600;pub-
gruu="sip:student@ims3.sip.uniza.sk;gr=76a5671b-9b2d-4f1a-8f87-a24ca4d0f0ae"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Serving-CSCF
Content-Length: 0
```

B.2 Odlásenie Monster IMS klienta – správy medzi P-CSCF a I-CSCF

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Call-ID: 94521a7a9c9206610d71aa35f8da0b9a@192.168.1.4
CSeq: 3 REGISTER
From: <sip:student@ims3.sip.uniza.sk>;tag=1004
To: <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 158.193.139.22;branch=z9hG4bKecd5.bbde37a6.0
Via: SIP/2.0/UDP 158.193.139.187 :
5060;rport=5060;branch=z9hG4bKf352c127d426e231b63fc0c68f852a15373934
Max-Forwards: 19
Expires: 0
Contact: "student" <sip:student@158.193.139.187 :5060>;+sip.instance=7e10d1c0-d13d-4eb0-
863e-809b5401d2b2
User-Agent: monster Version: 0.9.25
Content-Length: 0
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="18c53dfc2d3a73167957
fbbe49513d21",response="2dca1dd42ebeaa728f28583485580deb",uri="sip:ims3.sip.uniza.sk",
integrity-protected="no"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd4f9adb1a00000024";icid-generated-
at=158.193.139.22;orig-ioi="ims3.sip.uniza.sk"
P-Visited-Network-ID: ims3.sip.uniza.sk
```

```
SIP/2.0 401 Unauthorized - Challenging the UE
Call-ID: 94521a7a9c9206610d71aa35f8da0b9a@192.168.1.4
CSeq: 3 REGISTER
From: <sip:student@ims3.sip.uniza.sk>;tag=1004
To: <sip:student@ims3.sip.uniza.sk>;tag=68988887aea29c51493f22b8b0542a94-f5e8
Via: SIP/2.0/UDP 158.193.139.22;branch=z9hG4bKecd5.bbde37a6.0
Via: SIP/2.0/UDP 158.193.139.187 :
5060;rport=5060;branch=z9hG4bKf352c127d426e231b63fc0c68f852a15373934
WWW-Authenticate: Digest realm="ims3.sip.uniza.sk",
nonce="d3ebca6dd5eb2ecb028b6fba563d2828", algorithm=MD5, qop="auth,auth-int"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
Server: Serving-CSCF
Content-Length: 0
```

```
REGISTER sip:ims3.sip.uniza.sk SIP/2.0
Call-ID: 94521a7a9c9206610d71aa35f8da0b9a@192.168.1.4
CSeq: 4 REGISTER
From: <sip:student@ims3.sip.uniza.sk>;tag=1005
To: <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 158.193.139.22;branch=z9hG4bKbcd5.d52c6c81.0
Via: SIP/2.0/UDP 158.193.139.187 :
5060;rport=5060;branch=z9hG4bK6188cf46f95d269eb6ed565fcac174b6373934
Max-Forwards: 19
Expires: 0
Contact: "student" <sip:student@158.193.139.187 :5060>;+sip.instance=7e10d1c0-d13d-4eb0-
863e-809b5401d2b2
```

```
User-Agent: monster Version: 0.9.25
Content-Length: 0
Authorization: Digest
username="student@ims3.sip.uniza.sk",realm="ims3.sip.uniza.sk",nonce="d3ebca6dd5eb2ecb028b
6fba563d2828",uri="sip:ims3.sip.uniza.sk",algoritm=MD5,response="19a1a895053718397659a5a65
c01d031",qop=auth-int,nc=00000001,cnonce="10297575157534854", integrity-protected="no"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd4f9adb1a00000025";icid-generated-
at=158.193.139.22;orig-ioi="ims3.sip.uniza.sk"
P-Visited-Network-ID: ims3.sip.uniza.sk
```

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Call-ID: 94521a7a9c9206610d71aa35f8da0b9a@192.168.1.4
CSeq: 4 REGISTER
From: <sip:student@ims3.sip.uniza.sk>;tag=1005
To: <sip:student@ims3.sip.uniza.sk>;tag=68988887aea29c51493f22b8b0542a94-3275
Via: SIP/2.0/UDP 158.193.139.22;branch=z9hG4bKbcd5.d52c6c81.0
Via: SIP/2.0/UDP 158.193.139.187 :
5060;rport=5060;branch=z9hG4bK6188cf46f95d269eb6ed565fcac174b6373934
Contact: <sip:student@158.193.139.187 :5060>;expires=0;pub-
gruu="sip:student@ims3.sip.uniza.sk;gr=7e10d1c0-d13d-4eb0-863e-809b5401d2b2"
Contact: <sip:student@172.16.1.99:5060>;expires=3015;pub-
gruu="sip:student@ims3.sip.uniza.sk;gr=76a5671b-9b2d-4f1a-8f87-a24ca4d0f0ae"
Path: <sip:term@pcscf2.ims3.sip.uniza.sk:5060;lr>
Service-Route: <sip:orig@scscf2.ims3.sip.uniza.sk:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Serving-CSCF
Content-Length: 0
```

B.3 INVITE správa Monster IMS klienta – posielaná z P-CSCF na S-CSCF

```
INVITE sip:student@ims3.sip.uniza.sk SIP/2.0
Record-Route: <sip:mo@pcscf.ims3.sip.uniza.sk:5060;lr>
Call-ID: 02341dfeffa17d9cea20f0ccd41d1b86@172.16.1.100
CSeq: 5 INVITE
From: <sip:karol@ims3.sip.uniza.sk>;tag=1007
To: <sip:student@ims3.sip.uniza.sk>
Via: SIP/2.0/UDP 158.193.139.25;branch=z9hG4bKe532.c6039386.0
Via: SIP/2.0/UDP 172.16.1.100:5060;rport=6892;received=158.193.139.187
;branch=z9hG4bKcf01b4c1aecab43754b1efd9db9916e5343630
Max-Forwards: 19
Route: <sip:orig@scscf.ims3.sip.uniza.sk:5060;lr>
Content-Type: application/sdp
Contact: "karol" <sip:karol@172.16.1.100:5060>
User-Agent: monster Version: 0.9.25
Content-Length: 267
P-Asserted-Identity: <sip:karol@ims3.sip.uniza.sk>
P-Charging-Vector: icid-value="P-CSCFabcd4f9acda40000003e";icid-generated-
at=158.193.139.25;orig-ioi="ims3.sip.uniza.sk"

v=0
o=karol 3544534048 3544534048 IN IP4 172.16.1.100
s=A Funky MONSTER Stream
t=0 0
m=audio 36126 RTP/AVP 0 8 14 101
c=IN IP4 158.193.139.25
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:14 MPA/8000
a=rtpmap:101 telephone-event/8000
a=nortpproxy:yes
```

Príloha C: Zachytená komunikácia medzidoménovej signalizácie hovoru

P-CSCF 2 IMS3 (158.193.139.22):

No.	Time	Source	Destination	Protocol	Length	Info
10	5.388215	91.148.31.98	158.193.139.22	SIP/SDP	803	Request: INVITE sip:palo@ims1.sip.uniza.sk, with session description
11	5.390347	158.193.139.22	91.148.31.98	SIP	408	Status: 100 trying -- your call is important to us
12	5.391012	158.193.139.22	158.193.139.23	SIP/SDP	1153	Request: INVITE sip:palo@ims1.sip.uniza.sk, with session description
13	5.392506	158.193.139.23	158.193.139.22	SIP	473	Status: 100 trying -- your call is important to us
15	5.459829	158.193.139.23	158.193.139.22	SIP	716	Status: 180 Ringing
16	5.460497	158.193.139.22	91.148.31.98	SIP	659	Status: 180 Ringing
24	8.837634	158.193.139.23	158.193.139.22	SIP/SDP	919	Status: 200 OK, with session description
25	8.838784	158.193.139.22	91.148.31.98	SIP/SDP	882	Status: 200 OK, with session description
27	8.865341	91.148.31.98	158.193.139.22	SIP	578	Request: ACK sip:palo@172.16.1.100:5060
28	8.866211	158.193.139.22	158.193.139.23	SIP	665	Request: ACK sip:palo@172.16.1.100:5060

S-CSCF 2 IMS3 (158.193.139.23):

No.	Time	Source	Destination	Protocol	Length	Info
4	1.627609	158.193.139.22	158.193.139.23	SIP/SDP	1133	Request: INVITE sip:palo@ims1.sip.uniza.sk, with session description
5	1.628322	158.193.139.23	158.193.139.22	SIP	472	Status: 100 trying -- your call is important to us
6	1.628594	158.193.139.23	158.193.152.2	DNS	87	Standard query SRV _sip._udp.ims1.sip.uniza.sk
7	1.629695	158.193.152.2	158.193.139.23	DNS	277	Standard query response SRV 0 0 5060 icscf.ims1.sip.uniza.sk
10	1.633182	158.193.139.23	158.193.139.41	SIP/SDP	1201	Request: INVITE sip:palo@ims1.sip.uniza.sk, with session description
11	1.638289	158.193.139.41	158.193.139.23	SIP	733	Status: 100 trying -- your call is important to us
13	1.696961	158.193.139.41	158.193.139.23	SIP	772	Status: 180 Ringing
14	1.697444	158.193.139.23	158.193.139.22	SIP	715	Status: 180 Ringing
20	5.450109	158.193.139.41	158.193.139.23	SIP/SDP	975	Status: 200 OK, with session description
21	5.450704	158.193.139.23	158.193.139.22	SIP/SDP	918	Status: 200 OK, with session description
22	5.479686	158.193.139.22	158.193.139.23	SIP	664	Request: ACK sip:palo@172.16.1.100:5060
23	5.480034	158.193.139.23	158.193.152.2	DNS	83	Standard query A scscf.ims1.sip.uniza.sk
24	5.481276	158.193.152.2	158.193.139.23	DNS	230	Standard query response A 158.193.139.42
27	5.485351	158.193.139.23	158.193.139.42	SIP	664	Request: ACK sip:palo@172.16.1.100:5060

I-CSCF IMS 1 (158.193.139.41):

No.	Time	Source	Destination	Protocol	Length	Info
7	1.210561	158.193.139.23	158.193.139.41	SIP/SDP	1221	Request: INVITE sip:palo@ims1.sip.uniza.sk, with session description
11	1.214549	158.193.139.41	158.193.139.23	SIP	734	Status: 100 trying -- your call is important to us
14	1.216862	158.193.139.41	158.193.139.42	SIP/SDP	1327	Request: INVITE sip:palo@ims1.sip.uniza.sk, with session description
15	1.218406	158.193.139.42	158.193.139.41	SIP	791	Status: 100 trying -- your call is important to us
17	1.259479	158.193.139.42	158.193.139.41	SIP	830	Status: 180 Ringing
18	1.259656	158.193.139.41	158.193.139.23	SIP	773	Status: 180 Ringing
19	3.670453	158.193.139.42	158.193.139.41	SIP/SDP	1033	Status: 200 OK, with session description
20	3.670666	158.193.139.41	158.193.139.23	SIP/SDP	976	Status: 200 OK, with session description

S-CSCF IMS 1 (158.193.139.42):

No.	Time	Source	Destination	Protocol	Length	Info
8	4.856631	158.193.139.41	158.193.139.42	SIP/SDP	1327	Request: INVITE sip:palo@ims1.sip.uniza.sk, with session description
9	4.856959	158.193.139.42	158.193.139.41	SIP	791	Status: 100 trying -- your call is important to us
10	4.857349	158.193.139.42	158.193.139.40	SIP/SDP	1503	Request: INVITE sip:palo@172.16.1.100:5060, with session description
11	4.858523	158.193.139.40	158.193.139.42	SIP	671	Status: 100 trying -- your call is important to us
13	4.917204	158.193.139.40	158.193.139.42	SIP	898	Status: 180 Ringing
14	4.917362	158.193.139.42	158.193.139.41	SIP	830	Status: 180 Ringing
21	8.295045	158.193.139.40	158.193.139.42	SIP/SDP	1101	Status: 200 OK, with session description
22	8.295282	158.193.139.42	158.193.139.41	SIP/SDP	1033	Status: 200 OK, with session description
24	8.325990	158.193.139.23	158.193.139.42	SIP	665	Request: ACK sip:palo@172.16.1.100:5060
25	8.326265	158.193.139.42	158.193.139.40	SIP	666	Request: ACK sip:palo@172.16.1.100:5060

P-CSCF IMS1 (158.193.139.40):

No.	Time	Source	Destination	Protocol	Length	Info
9	5.906322	158.193.139.42	158.193.139.40	SIP/SDP	1503	Request: INVITE sip:palo@172.16.1.100:5060, with session description
10	5.906786	158.193.139.40	158.193.139.42	SIP	671	Status: 100 trying -- your call is important to us
12	5.907049	158.193.139.40	91.148.31.98	SIP/SDP	102	Request: INVITE sip:palo@172.16.1.100:5060, with session description
14	5.965277	91.148.31.98	158.193.139.40	SIP	889	Status: 180 Ringing
15	5.965635	158.193.139.40	158.193.139.42	SIP	898	Status: 180 Ringing
23	9.342955	91.148.31.98	158.193.139.40	SIP/SDP	1092	Status: 200 OK, with session description
24	9.343461	158.193.139.40	158.193.139.42	SIP/SDP	1101	Status: 200 OK, with session description
26	9.375192	158.193.139.42	158.193.139.40	SIP	666	Request: ACK sip:palo@172.16.1.100:5060
27	9.375532	158.193.139.40	91.148.31.98	SIP	670	Request: ACK sip:palo@172.16.1.100:5060