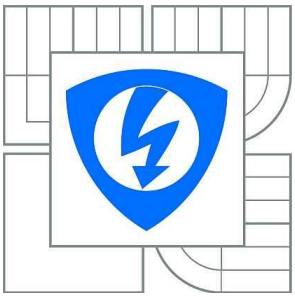
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

OPEN IMS CORE A IP MULTIMEDIA SUBSYSTEM

THE OPEN IMS CORE AND THE IP MULTIMEDIA SUBSYSTEM

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

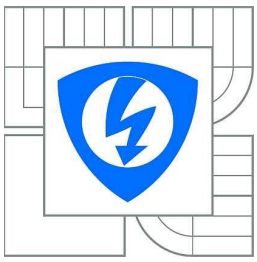
AUTOR PRÁCE — Bc. MARTIN BOŽEK

AUTHOR

VEDOUCÍ PRÁCE — Ing. ĽUBOŠ NAGY

SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Martin Božek	***ID:***	98024
Ročník:	2	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Open IMS Core a IP Multimedia Subsystem

POKYNY PRO VYPRACOVÁNÍ:

Základním cílem diplomové práce je prostudovat a popsat technologii IMS (IP Multimedia Subsystem) se zaměřením se na možnost testování této platformy v Open source nástrojích. Výsledkem práce bude funkční experimentální sít umožňující testování IMS technologie.
Body zadání:
- vytvoření a konfigurace experimentální sítě IMS v školní laboratoři na jednom PC,
- nainstalovaná architektura IMS bude obsahovat minimálně: S/I/P/E-CSCF, HSS, DNS, desktopové klientské aplikace (např. UCTIMSCLIENT, Monster, atd.),
- nainstalování pobočkové ústředně Asterisk na druhém PC,
- konfigurace architektury IMS a PBX Asterisk pro jejich vzájemné propojení,
- navrhnutí minimálně dvou laboratorních úloh se zaměřením na otestování různých služeb poskytovaných vytvořenou IMS sítí pomocí dostupných klientských aplikací (např. UCTIMSCLIENT, Monster, SIPdroid, atd.).

DOPORUČENÁ LITERATURA:

[1] POIKSELKA, M., MAYER, G. The IMS: IP Multimedia Concepts and Services. V. Británie: WILEY, 2009. 560 s. Třetí vydání. ISBN 978-0-470-72196-4.
[2] RUSSELL, T. The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations. V. Británie: Mc Graw-Hill OSBOURNE, 2008. 242 s. ISBN 0071488537.

Termín zadání:	7.2.2011	***Termín odevzdání:***	26.5.2011

Vedoucí práce: Ing. Ľuboš Nagy

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

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

ANOTACE

Tato Diplomová práce se zabývá popsáním architektury IMS a jejím testováním.

V první části práce je popsán vrstový model IMS a jeho jednotlivé části. Následuje prostudování IMS z hlediska hlavních entit, propojení referenčních bodů a funkce protokolů používaných v rámci IMS.

Praktická část práce řeší nejprve seznámení se s projektem Open IMS Core, který byl zvolen pro testování IMS technologie, a jeho nastavením nutným pro uskutečnení testování a propojení s PBX Asterisk. Po seznámení se s desktopovými IMS klienty je uskutečněna instant messaging komunikace v rámci IMS sítě. Následnou analýzou zachycené komunikace pomocí aplikace Wireshark je popsán způsob předávání zpráv SIP protokolu uvnitř IMS.

Po stručném úvodu do PBX Asterisk, rozebrání předpokladů k propojení s IMS a potřebných nastavení, se přistoupí k samotnému otestování komunikace. Nejprve je uskutečněn přenos hlasu mezi desktopovým IMS klientem a IP telefonem registrovaným k PBX Asterisk. Průběh komunikace je zachycen a následně analyzován ve smyslu sestavení, průběhu a ukončení relace. Po úspěšné realizaci audio hovoru byl navázán video hovor, který byl podrobně rozebrán včetně statistik řídících signálů a přenesených paketů.

V příloze je návrh dvou laboratorních úloh, které byly vypracovány za účelem seznámení studentů s IMS technologií a možnostmi komunikace v rámci IMS sítě.

KLÍČOVÁ SLOVA: IP Multimedia Subsystem, Open IMS Core, PBX Asterisk

ABSTRACT

This thesis describes architecture of IMS and shows possibilities of IMS platform testing.

Theoretical part describes layer model of the IMS as a whole and then describes it's individual layers. Next chapters analyse key entities of the IMS, interconnection between reference points and features of protocols used in the IMS.

Practical part deals with the introduction of Open IMS Core, which was chosen for the IMS technology testing. Settings necessary to carry out testing and interconnection between PBX Asterisk are shown in next chapters. After introduction of IMS desktop clients is carried out an instant messaging communication within the IMS network. The communication is captured and analysed by Wireshark application. Afterwards there is described how SIP protocol sends messages within the IMS.

After a brief introduction to the PBX Asterisk, there are discussed assumptions for the interconnection between Asterisk and IMS. There are also described necessary settings needed for implementation and communication testing itself. The first test is an audio session carried out between the desktop IMS client and IP phone registered to the PBX Asterisk. Communication is captured for the analysis of preparation, conduction and termination of the session. After the successful realization of the audio call, video session has been made. The session was analysed in detail, including statistics of control signals and transmitted packets.

There are two laboratory excercises in attachement of this thesis, which will help students to understand the IMS technology and communication options within the IMS network.

KEYWORDS: IP Multimedia Subsystem, Open IMS Core, PBX Asterisk

BIBLIOGRAFICKÁ CITACE

BOŽEK, M. *Open IMS Core a IP Multimedia Subsystem.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 70 s., 4 přílohy. Vedoucí diplomové práce Ing. Ľuboš Nagy.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Testování sítě IP Multimedia Subsystem“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce Ing. Lubošovi Nagyovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne …… ……..

(podpis autora)

OBSAH

Úvod 1

1 Architektura IMS 2

1.1 Vrstvy IMS 3

1.1.1 Device Layer – Vrstva koncových zařízení 3

1.1.2 Transport Layer – Transportní vrstva 3

1.1.3 Control Layer – Řídicí vrstva 4

1.1.4 Service Layer – Aplikační vrstva 4

1.2 Prvky IMS 4

1.2.1 CSCF – Call Session Control Function 6

1.2.2 HSS – Home Subscribe Server 8

1.2.3 SLF – Subscription Locator Function 9

1.2.4 PDF – Policy Decision Function 10

1.2.5 AS – Application server 10

1.2.6 MRF – Media Resource Function 12

1.2.7 BGCF – Breakout Gateway control function 12

1.2.8 PSTN/CS GW – Public Switched Telephony Network/ Circuit Switched Gateway 12

1.2.9 CF – Charging Function 14

1.3 Referenční body IMS 15

1.4 Protokoly v IMS 19

1.4.1 SIP – Session Initiation Protocol 20

1.4.2 SDP – Session Description Protocol 20

1.4.3 RTP – Real-Time Transport Protocol 21

1.4.4 DIAMETER 21

1.4.5 COPS – Common Open Policy Service 21

1.4.6 MEGACO – Media Gateway Control Protocol 21
2 Testování IMS 22
2.1 Open IMS Core 22
2.2 Zprovoznění IMS sítě 23
2.3 IMS desktopové klientské aplikace 26
2.3.1 UCT IMS Client 26
2.3.2 myMONSTER-TCS 26
2.3.2 IMS Communicator 27
2.3.3 Analýza komunikace IMS klientů 27
2.4 PBX Asterisk 1.4 32
2.4.1 Instalace PBX Asterisk 33
2.5 Propojení PBX Asterisk s Open IMS Core 33
2.5.1 Testování propojení IMS a PBX Asterisk 35
2.6 Shrnutí 42
Závěr 44
LITERATURA 46
SEZNAM ZKRATEK 48
SEZNAM OBRÁZKŮ 50
Příloha A 51
Příloha B 52
Příloha C 53
Příloha D 62

Úvod

IMS neboli the IP Multimedia Subsystem je sada specifikací a protokolů popisující architekturu *Next Generation Network* pro implementaci IP telefonie a multimediálních služeb. Tato *all-IP* architektura představuje výsledek společné snahy *3rd Generation Partnership Project* a *Internet Engineering Task Force*, tedy vůdčích organizací ve svém oboru působnosti. *IETF* poskytla základní technologie a většinu standardů, zatímco *3GPP* vytvořila architekturu rozhraní a integraci protokolů tak, aby IMS splňovala nároky na špičkový mobilní systém světové třídy. IMS byl poprvé uveden v roce 2000 ve specifikaci *3GPP release 5* [2].

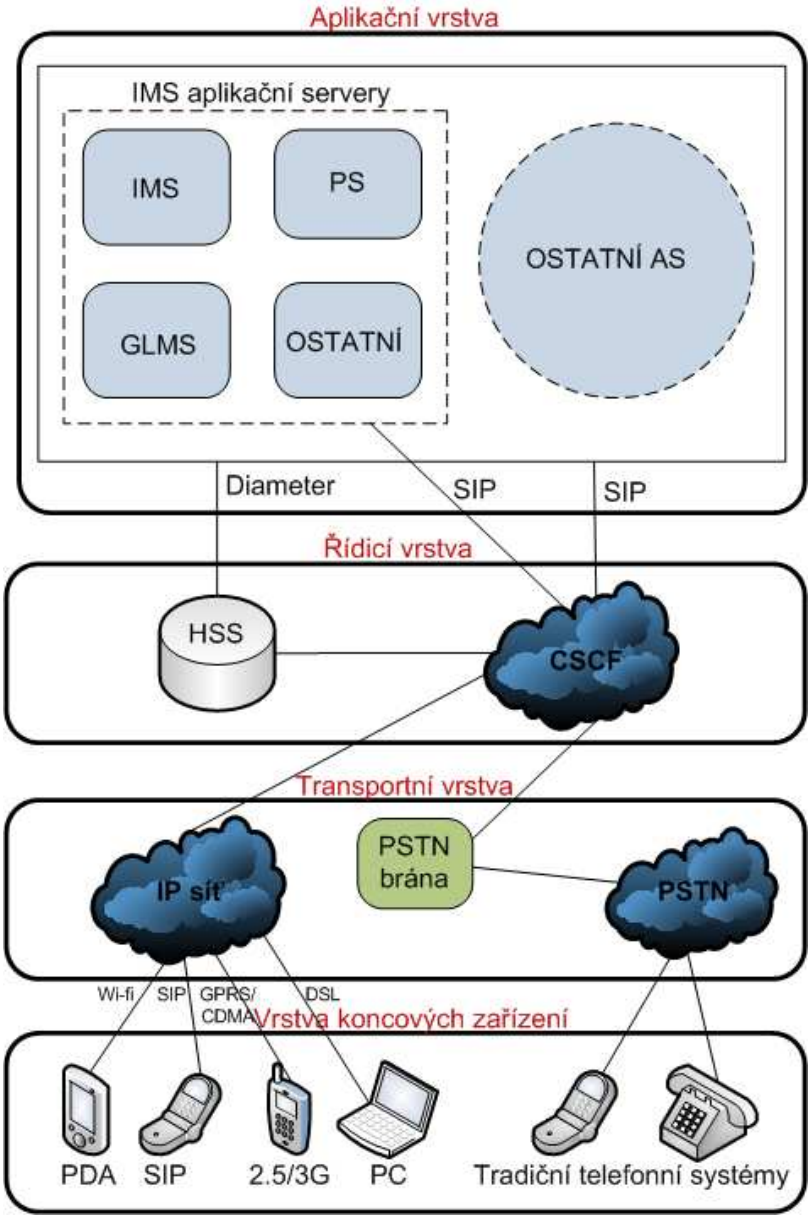
Technologie IMS propojuje dvě vůbec nejrozšířenější komunikační paradigmata – mobilní a internetovou technologii. Umožňuje tak přístup k internetovým službám jako je web, e-mail, instant messaging nebo videokonference téměř kdekoliv. IMS kromě propojení mobilních a internetových služeb také sjednocuje rozdělení telefonních sítí na okruhově (CS) a paketově spínané (PS). Bývá proto také označován jako služba fixně/mobilní konvergence. Přenos hlasu a dat je tedy sjednocen na paketovou bázi (all-IP), čímž je zjednodušena práce s přenášenými daty [1].

V této práci je první – teoretická část – věnována popisu architektury IMS. Nejprve je IMS analyzován z pohledu čtyřvrstvého modelu, včetně popisu vrstev a jejich spolupráce. Dále byly popsány jednotlivé prvky, služby a jejich vzájemné propojení a spolupráce v rámci IMS sítě. Poslední část první kapitoly se věnuje základním protokolům, se kterými IMS pracuje.

Druhá část práce je zaměřena na zprovoznění a využití open-source systému Open IMS Core, který díky implementaci IMS technologie umožňuje testování a analýzu komunikace v této síti. Ve vytvořené IMS síti lze komunikovat pomocí IMS desktopových klientů a smart phonů s aplikací IMSDroid. Po propojení Open IMS Core s pobočkovou ústřednou Asterisk je umožněno začlenění IP telefonů do IMS sítě. V rámci vytvořené topologie jsou otestovány služby Instant messaging, přenos hlasu a videohovor, které jsou podrobně analyzovány.

1 Architektura IMS

Architektura IMS podporuje široké spektrum služeb založených na protokolu SIP (pro bližší popis viz. kapitola 4.1). Tato struktura IMS umožňuje uživateli přístup přes rozdílná zařízení a to jak přes IP sítě nebo klasický telefonní systém. Na architekturu IMS můžeme z hlediska rozdělení na logické vrstvy nahlížet jako na model čtyřvrstvý nebo trojvrstvý (rozlišuje vrstvu aplikační, řídicí, uživatelskou). Pro větší rozšířenost a přehlednost čtyřvrstvého modelu bude popsán právě tento model, viz. obr.1.1, kde je názorně zobrazen diagram struktury IMS [1], [2].



Obrázek 1.1- Diagram IMS architektury [1]

1.1 Vrstvy IMS

Rozdělení IMS do vrstev přináší výhodu v podobě možnosti implementace různých funkcí a služeb bez závislosti na jejich typu. Specifikace a standardy IMS popsané v 3GPP projektu jsou v podstatě souhrnem služeb, které jsou propojeny řadou standartních rozhraní. 3GPP konkrétně řeší funkce logických prvků, popisuje, jak jsou tyto prvky propojeny a které protokoly a procedury jsou použity. Neřeší tedy popis uzlů - to umožňuje umístit více služeb na jeden uzel nebo naopak umístit jednu službu na více uzlů. Nejčastěji se však setkáme s umístěním služby na samostatný uzel. Z hlediska propojení služeb i jednotlivých vrstev je hlavní, aby použité technologie byly sjednoceny a pracovali s přenášenými informacemi bez ohledu na jejich typ [1], [2].

Podobně jako např. u modelu TCP/IP, rozdělení IMS do vrstev znázorňuje hierarchii činností a zjednodušuje tak pohled na výměnu informací. Komunikace mezi jednotlivými vrstvami je přesně definovaná, všechny vrstvy využívají funkce nižších vrstev a poskytují služby vrstvám vyšším.

1.1.1 Device Layer – Vrstva koncových zařízení

Jak už bylo zmíněno, struktura IMS nabízí uživatelům možnost volby z širšího spektra koncových zařízení. IMS zařízení jako jsou např. počítače, mobilní telefony, PDA a digitální telefony se do IMS infrastruktury připojují přes IP síť. Jiné typy zařízení, jako například tradiční analogové telefony, nejsou schopny se k IP síti připojit přímo, ale jsou schopny navázat spojení skrz PSTN bránu [1]. Pro názornost viz. obr. 1.1.

1.1.2 Transport Layer – Transportní vrstva

Transportní vrstva odpovídá za navazování a ukončování relací a zároveň zajišťuje konverzi dat přenášených mezi analogovými/digitálními formáty a paketovým formátem používaným v IP sítích. IMS zařízení se připojují k IP síti na transportní vrstvě přes různá přenosová média, nejčastěji: Wifi, DSL,

kabel, SIP, GPRS a WCDMA. Tato vrstva také umožňuje IMS zařízením vytvářet a navazovat hovory s PSTN sítí nebo jinou okruhově spínanou (CS) sítí přes PSTN bránu [1].

1.1.3 Control Layer – Řídicí vrstva

V této vrstvě se nachází hlavní prvky jádra IMS sítě – CSCF a HSS. CSCF, nebo-li Řídicí funkce hovorových relací (The Call Session Control Function, viz. kapitola 1.2.1), obecně zahrnuje SIP a proxy servery a je základním prvkem Řídicí vrstvy. CSCF zajišťuje SIP registraci koncových zařízení a zpracovává předávání SIP signálů příslušnému aplikačnímu serveru v Aplikační vrstvě. Druhým klíčovým prvkem je HSS (Home Subscribe server, viz. kapitola 1.2.2), což je databáze údajů a profilů každého koncového uživatele [1].

1.1.4 Service Layer – Aplikační vrstva

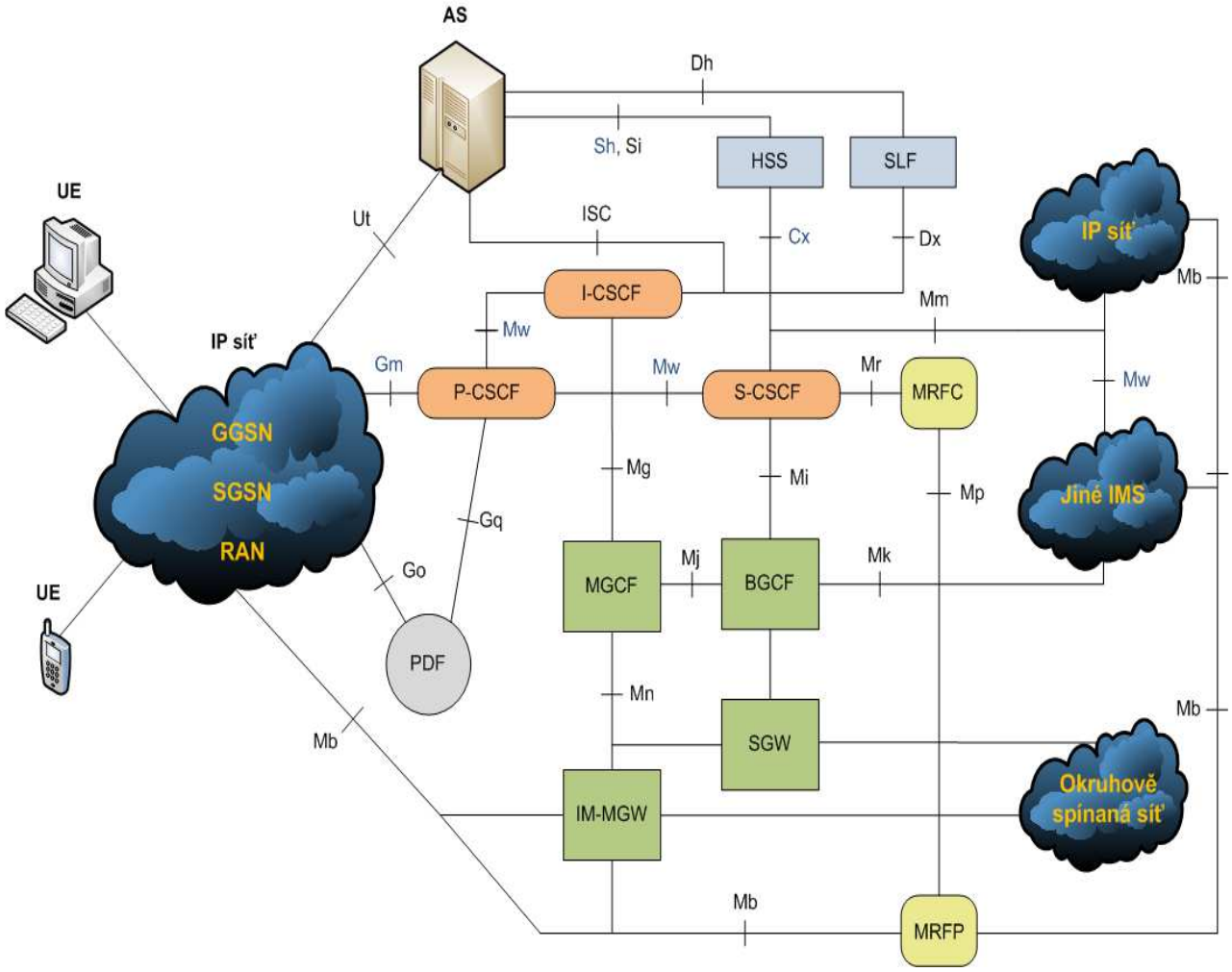
Na vrcholu architektury IMS sítě je Aplikační vrstva. Tři výše popsané vrstvy, ležící pod Aplikační vrstvou, poskytují jednotnou a standartizovanou síťovou platformu, která umožňuje poskytovatelům služeb nabízet na Aplikační vrstvě množství multimediálních služeb. Tyto služby jsou provozovány aplikačními servery (AS – application server, viz. kapitola 1.2.5), které nejen zodpovídají za hostování a vykonávání služeb, ale také za použití SIP a Diameter protokolu poskytují rozhraní Řídicí vrstvě. Jeden aplikační server může hostovat více služeb, což přináší flexibilitu a umožňuje snížení zátěže Řídicí vrstvy [1].

1.2 Prvky IMS

Přehled a propojení klíčových prvků IMS je zobrazen na obr. 1.2 [2], [3] a to včetně referenčních bodů (více v kap. 1.3). Z pohledu funkce lze prvky

rozdělit do několika skupin, nejčastěji se setkáme s rozdělením do šesti skupin, uvedeným např. v [2]:

- Řízení relací a směrování (*CSCF*).
- Databáze (*HSS, SLF*).
- Prvky komunikace mezi propojenými entitami (*BGCF, MGCF, IM-MGW*).
- Služby (*AS, MRF*).
- Podpůrné entity (*THIG, PDF*).
- Funkce poplatků (*charging*).



Obrázek 1.2– IMS architektura z hlediska prvků a referenčních bodů [2], [3]

1.2.1 CSCF – Call Session Control Function

CSCF je souhrnné označení funkcí pro zpracování SIP signalizačních paketů v IMS síti. Dělí se na čtyři druhy: P-CSCF, S-CSCF, I-CSCF, E-CSCF [2].

P-CSCF – Proxy Call Session Control Function

Proxy CSFC je prvním kontaktním bodem pro uživatele IMS sítě. Veškerá SIP signalizace směřující od uživatelského zařízení nebo k němu jde přes tuto entitu. Jak už název napovídá, P-CSCF se chová jako proxy server – obdrží požadavek, přepošle ho k cíli a poté přepošle zpět odpověď. Může být umístěn v domácí síti nebo v navštívených sítích (*visited networks*). Hlavní funkce, ke kterým slouží, jsou [2]:

- Ochrana integrity SIP signalizace na základě IPsec.
- Ochrana spojení mezi UE a P-CSCF, předchází útokům typu spoofing a replay.
- Komprese a dekomprese SIP zpráv pro rádiová rozhraní.

S-CSCF – Serving Call Session Control Function

Jedná se o tzv. Obsluhující CSCF a je centrálním uzlem celé IMS, vždy umístěným v domácí síti. Dohlíží na spojení a registrační služby uživatelských rozhraní. Když je UE obsazen relací, tak S-CSCF udržuje stav relace a vzájemně komunikuje s řídicími platformami (případně i funkcemi poplatků) tak, jak síťový operátor vyžaduje. S-CSCF může mít mnoho funkcí na základě nastavení operátora síťě, mezi ty hlavní patří [2], [4]:

- Zpracováva SIP registrace.
- Komunikuje s HSS serverem, stahuje si data o uživatelích a nahrává asociace typu *user-to-S-CSCF.*
- Na základě poskytovaných služeb rozhoduje, na jaký aplikační server budou přeposlány SIP zprávy.
- Poskytuje směrovací služby.

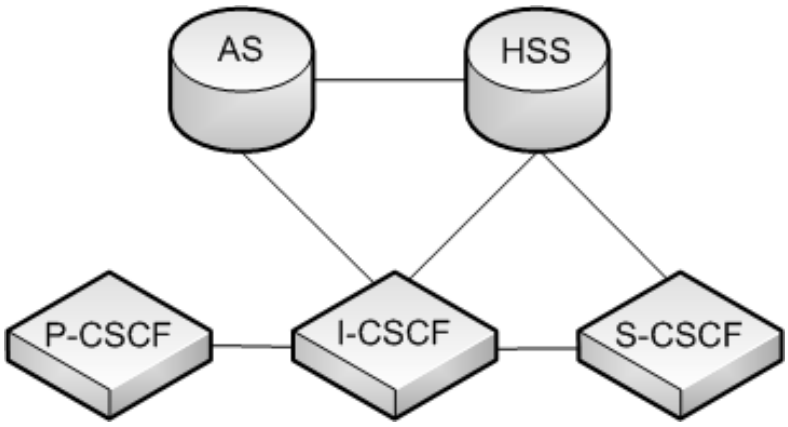
- Prosazuje pravidla síťového operátora.

I-CSCF – Interrogating Call Session Control Function

Dotazovací CSCF slouží jako kontaktní bod v síti operátora a nejčastěji je umístěn v domovské síti. Jeho IP adresa je uveřejněna v *DNS* domény, takže ho vzdálené servery mohou kontaktovat a použít jako přeposílací bod pro SIP pakety určené této doméně. V síti operátora může být několik I-CSCF. Hlavní funkce jsou [2], [4]:

- Kontaktovat HSS pro obdržení jména konkrétního S-CSCF pro obsluhu uživatele. Přiřazení S-CSCF probíhá na základě údajů o kapacitě a vlastnostech zaslaných od HSS.
- Přeposílání SIP dotazů a odpovědí od S-CSCF.
- Přeposílá CCF (Charging Collection Function) údaje vztahujícím se k poplatkům.

Pro lepší názornost propojení P/S/I-CSCF a HSS viz. obr. 1.3 [5]



Obrázek 1.3– Propojení P/S/I-CSCF, HSS a AS [5]

E-CSCF – Emergency Call Session Control Function

Nouzová CSCF zajišťuje zpracování nouzových IMS požadavků, jako je například relace s policií, záchrannou službou nebo hasiči. Hlavním úkolem E-CSCF je zvolení vhodného nouzového centra, které se nazývá *Public Safety*

Answering Point (Centrum odpovídající za veřejnou bezpečnost). Tomuto centru jsou pak doručovány nouzové požadavky pro zpracování.

1.2.2 HSS – Home Subscribe Server

HSS je hlavním úložištěm dat o uživatelích a uživatelských nastaveních v rámci IMS. V této databázi jsou především ukládána data jako: uživatelské identity, registrační údaje, přístupové parametry, IP informace, informace o poloze uživatele, čísla atd. [2]. Pro komunikaci s ostatními prvky sítě HSS využívá protokol DIAMETER (podrobněji viz. kapitola 1.4.4).

Uživatelské identity se dělí na dvě skupiny: privátní (IMPI – IP Multimedia Private Identity) a veřejné (IMPU – IP Multimedia Public Identity). Obě identity nejsou ve formě telefonního čísla, ale jako URI (Uniform Resource Identifier)[4].

- Privátní identita je unikátní a pevně přidělená globální identita, kterou přiřadí operátor domácí sítě. Používá se k registraci, autorizaci, administraci a účetním účelům. Každý uživatel má jednu nebo více IMPI [2], [4].
- Veřejnou identitu používají uživatelé k vyžádání komunikace s jiným uživatelem v síti. K jedné privátní identitě může být přiřazeno více identit veřejných a zároveň IMPU může být sdílena na více koncových zařízeních [2], [4].

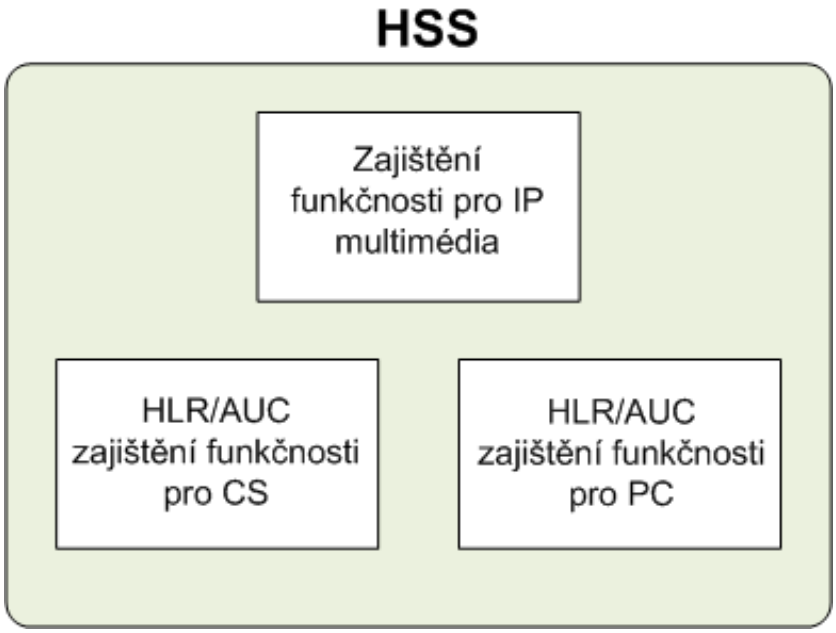
K navázání spojení slouží přístupové parametry jako je autorizace uživatele, autorizace roamingu a jména přidělená S-CSCF. HSS také poskytuje údaje o specifických požadavcích každého uživatele na vlastnosti S-CSCF. Na základě těchto informací I-CSCF volí pro uživatele nejvhodnější S-CSCF.

HSS neposkytuje informace S-CSCF umístěným v jiných sitích, což je důležité k zabezpečení uložených uživatelských dat před přístupem z nedůvěryhodných sítí. Tuto ochranu realizují entity P-CSCF a I-CSCF [6].

Kromě funkcí týkajících se funkčnosti IMS, HSS také obsahuje podskupinu HLR/AUC (Home Location Register and Authentication Center, viz. obr. 1.4). HLR neboli domovský lokalizační registr je prvek nezbytný pro přístup

do paketově spínaných sítí (nutnost pro funkčnost entit SGSN a GGSN), tak i do sítí okruhově spínaných (zejména MSC/MSC servery). To uživateli umožňuje přístup k CS službám a podporuje roaming do GSM/UMTS CS sítí [2].

Autentizační centrum (AUC) zajišťuje řízení autentizace každého mobilního uživatele pomocí autentizační funkce ACF, která pro každého uživatele generuje dynamická zabezpečovací data. Data jsou použita pro vzájemnou autentizaci IMSI (International Mobile Subscriber Identity) a sítě. Tato data jsou zároveň i použita pro poskytování ochrany integrity a šifrování komunikace skrz rádiovou přenosovou cestu mezi UE a sítí.



Obrázek 1.4– Struktura HSS [2]

1.2.3 SLF – Subscription Locator Function

SLF je rozlišovací mechanismus, který entitám I-CSCF, S-CSCF a AS umožnuje určit adresu HSS v případech, kdy je v síti více HSS na odlišných adresách.

1.2.4 PDF – Policy Decision Function

Odpovídá za tvorbu pravidel pro rozhodování, která jsou generována na základě informací o relaci a multimediálním toku. Od *Release 5* je přímo součástí P-CSCF. Je založena na mechanismu SBLB *(Service Based Local Policy*), který plní funkce jako jsou [2]:

- Ukládání informací o relaci a multimédiích (IP adresa, čísla portů, šířka pásma atd.).
- Na výzvu GGSN poskytovat rozhodnutí o autorizaci založené na těchto informacích.
- Aktualizovat rozhodnutí o autorizaci po změně těchto informací a případně autentizaci odebrat.
- Generování znaku *Media Authorization Token*, jenž identifikuje relaci a PDF.

1.2.5 AS – Application server

Jak je patrné z obr. 1.2, Aplikační servery (AS) nejsou přímo IMS entita, ale spíše jde o funkce na vrcholu IMS struktury. Protože ale poskytují v rámci IMS sítě důležité multimediální služby, jsou zařazeny mezi její prvky. Mohou být umístěny v domácí či jiné síti nebo také jako samostatný AS. Hlavními funkcemi jsou [2]:

- Možnost zpracování příchozích SIP relací z IMS sítě.
- Schopnost vytvářet SIP dotazy.
- Schopnost zasílat účetní údaje CCF (Charging Collection Function) a ECF (Event Charging Function).

Dle specifikací [ETSI TS 123 078] a [3GPP TS 23.228] poskytované služby AS nejsou omezeny jen na služby založené na SIP, ale uživatelé IMS také mohou také využívat CAMEL (Customized Applications for Mobile network Enhanced Logic) a OSA (Open Service Architecture). AS se dělí na tři druhy:

SIP AS (*SIP Application Server*)

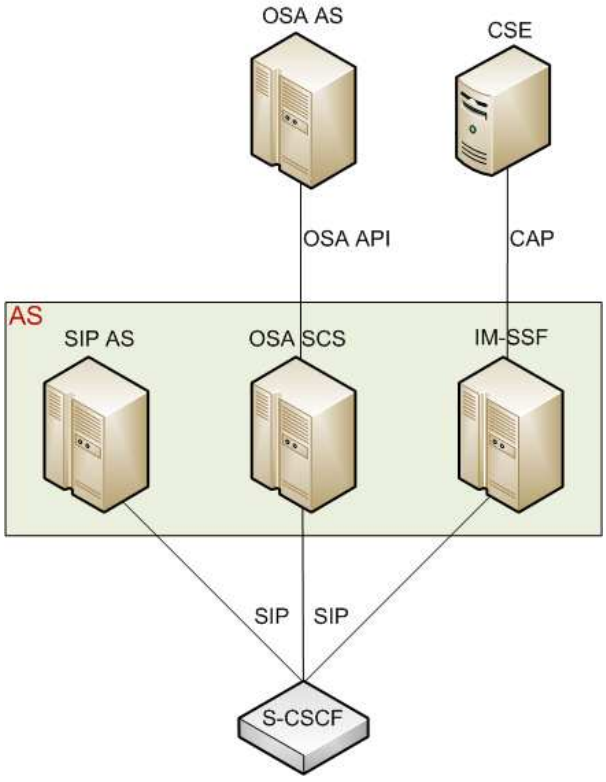
Aplikační server založený na protokolu SIP, který může hostit široké spektrum multimediálních služeb – nejčastěji konferenční a prezenční služby nebo zasílání zpráv [2].

OSA-SCS (*Open Service Access - Service Capability Server*)

Tento server zprostředkovává vykonávání OSA služeb v IMS síti – slouží jako gateway (brána) a pomocí standartizovaného rozhraní umožňuje komunikaci IMS s externími OSA AS [7].

IM-SSF (*IP Multimedia Service Switching Function*)

Třetím typem je AS sloužící jako gateway pro spojení se sítěmi implementujícími služby CAMEL, hojně využívanými v GSM sítích. Chová se jako brána mezi SIP a CAMEL službami umožňující CAMEL službám být volány z IMS sítě.



Obrázek 1.5– Diagram vazeb mezi Aplikačními servery [2]

1.2.6 MRF – Media Resource Function

Entita MRF je soubor funkcí pro obsluhu a zpracování médií. Zajišťuje například real-time převod multimediálních dat, rozpoznání hlasu, multimediální konference, přehrávání tónů a oznámení [7]. Dále se dělí na:

- MRFC (*MRF Controller*) – interpretuje informace a zpracovává signalizaci mezi AS a S-CSCF, ovládá MRFP pomocí rozhraní H.248.
- MRFP (*MRF Processor*) – zpracovává, vytváří a slučuje toky médií, implementuje všechny funkce pro jejich zpracování a sdílení.

1.2.7 BGCF – Breakout Gateway control function

Tato řídicí funkce, pracující vpodstatě jako SIP proxy, rozhoduje, jakým způsobem bude probíhat směrování hovorů do CS sítí. Pokud má být hovor uskutečněn v rámci domácí sítě, kde je umístěn daný BGCF, je vybrán Media Gateway Control Function (MGCF), který se postará o zpracování požadavku. Jestliže hovor směřuje do jiné sítě, je požadavek předán jinému BGCF ve vybrané síti [2].

1.2.8 PSTN/CS GW – Public Switched Telephony Network/ Circuit Switched Gateway

Prvek fungující jako brána mezi IMS a PSTN (popř. jinou sítí založenou na přepínání kruhů), jenž pracují na odlišných sadách protokolů. Okruhově spínané sítě používají pro signalizaci protokol ISUP *(ISDN User Part*) popř. BICC *(Bearer Independent Call Control)* přenášený přes MTP *(Message Transfer Part)*, zatímco IMS využívá SIP přes IP. Pro přenos médií používají CS sítě PCM (Pulse-Code Modulation), zatímco IMS využívá RTP (pro podrobnější popis viz. kap. 1.4.3) [2].

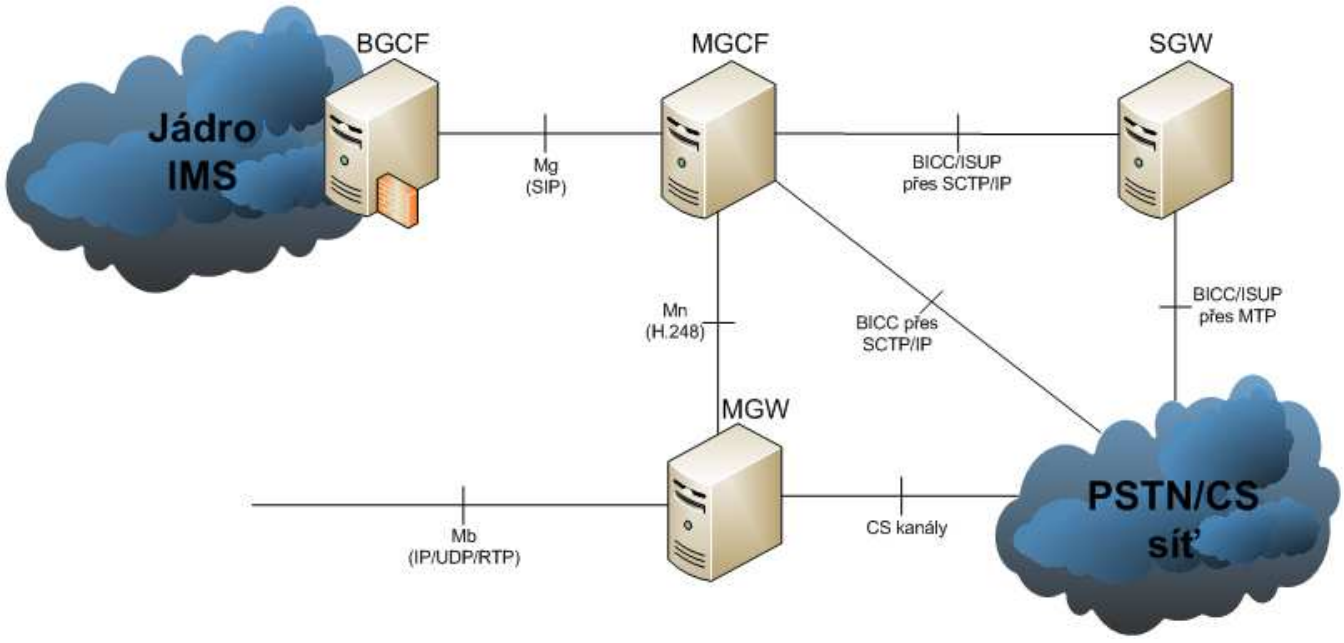
Z hlediska funkcí se tato brána dělí na tři části [6]:

- SGW (*Signalling Gateway*) – propojuje sítě s odlišnou signalizací, v našem případě sítě se signalizací založenou na protokolech SCTP/IP a

SS7. Provádí konverzi signálů nižších vrstev oběma směry, signály vyšších vrstev (např. zprávy Aplikační vrstvy) neinterpretuje.

- MGCF (*Media Gateway Controller Function*) - je hlavním uzlem PSTN/CS GW, implementuje stavový automat provádějící samotnou konverzi protokolů a rozděluje SIP na ISUP přes IP nebo BICC přes IP. Také pomocí H.248 rozhraní ovládá zdroje MGW.
- MGW (*Media Gateway*) - slouží jako gateway pro média - provádí konverzi mezi RTP a PCM, spravuje kodeky a zajišťuje jejich převod v případě, že terminál daný kodek nepodporuje či obě sítě pracují s rozdílným typem kodeku (pro IMS nejčastěji kodek AMR, pro PSTN G.711).

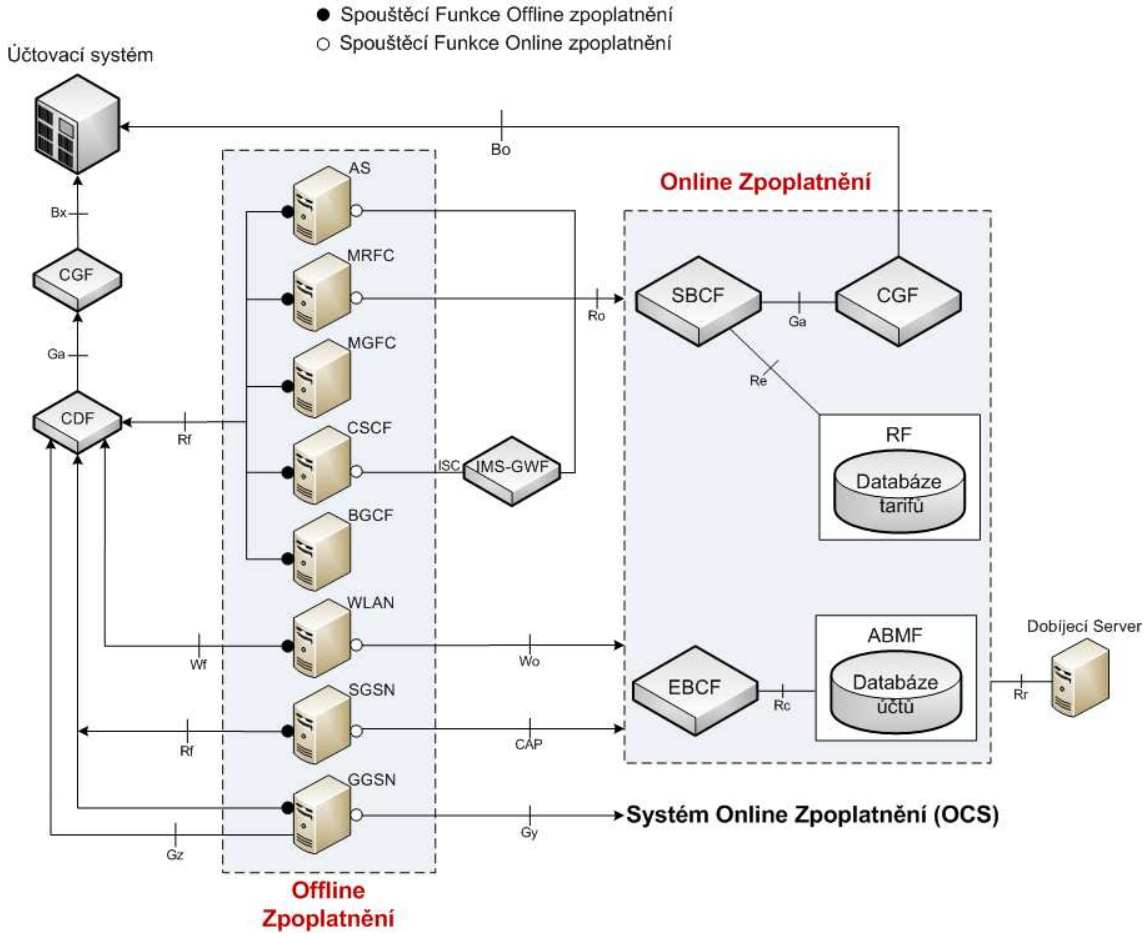
Pro lepší přehlednost a shrnutí předchozích dvou kapitol viz. obr. 1.6 znázorňující propojení architektury IMS s CS sítí.



Obrázek 1.6- Diagram propojení IMS a CS sítě [6]

1.2.9 CF – Charging Function

Charging function neboli Funkce zpoplatnění je důležitým standartem IMS architektury a nedílnou součástí ,,péče o zákazníka‘‘ ve smyslu přizpůsobování zpoplatnění jeho potřebám a poskytování jisté míry diverzity možnosti poplatků za poskytované služby. Zpoplatnění služeb je účtováno dvěma způsoby - Online a Offline Charging. Oba způsoby budou dále popsané, pro lepší přehlednost viz. obr. 1.7 zobrazující architekturu a tok informací Offline a Online účtování podle specifikace 3GPP verze 6. Terminologie je vysvětlena pod obrázkem.



BGCF - Breakout Gateway Control Function
CAP - CAMEL Application part
CDF - Charging Data Function
CGF - Charging Gateway Function
CSCF - Call Session Control Function
GSGN - Gateway GPRS Support Node
IMS-GWF - IMS Gateway Function
ISC - IMS Service Control
MRFC - Media Resource Function Controller
MGCF - Media Gateway Control Function
SGSN - Serving GPRS Support Node

Obrázek 1.7 - Struktura Offline a Online zpoplatnění [8]

Offline Charging *(Offline zpoplatnění)*

Hlavním prvkem u Offline zpoplatnění je Charging Gateway Function (CGF), která získává a zpracovává informace o účtech. Tyto informace jsou CGF doručeny od Charging Data Function (CDF), která shromažďuje a předzpracovává data získaná od jednotlivých entit pomocí Rf, Wf a Gz rozhraní. Výstup CGF je vygenerovaný Call Detail Record (CDR), který je pomocí Bx rozhraní předán Účtovacímu systému (*Billing System*). Tento způsob můžeme definovat jako mechanismus zpoplatnění, kde účetní informace v reálném čase neovlivňují právě poskytovanou službu. Tyto informace jsou shromažďovány až po ukončení relace. Tento typ zpoplatnění je určen uživatelům, kteří platí účty periodicky [8].

Online Charging *(Online zpoplatnění)*

Online Charging je zpoplatnění založené na kreditu, který si zákazník musí předplatit. Jedná se o mechanismus, kde účetní informace mohou v reálném čase ovlivnit právě poskytovanou službu nebo funkci - je vyžadována přímá interakce mezi mechanismem zpoplatnění a řízením poskytované služby, účetní informace jsou shromažďovány v průběhu relace. Tím je operátor/poskytovatel služeb chráněn před podvodem či zneužitím kreditu.

Použití síťových zdrojů se nejprve musí autorizovat u Online Charging Service (OCS), který rozhodne na základě tarifu/ceny vyžadované služby a stavu uživatelova účtu. OCS podporuje dva typy funkcí zpoplatnění: Session-Based a Event-Based. Obě funkce shromažďují z uzlů potřebné informace a komunikují s příslušnou databází. Jsou generovány CDR, které opět putují do Účtovacího systému [8].

1.3 Referenční body IMS

V této kapitole je podrobněji rozebráno propojení entit popsaných v předešlých kapitolách. Různé způsoby propojení jsou zajištěny referenčními body, které se odlišují funkcemi i protokoly, na nichž jsou postaveny. Diagram

propojení a referenčních bodů je na obr. 1.2. V této kapitole jsem vycházel ze zdrojů [2], [3], [4].

Názvosloví referenčních bodů nemá žádný konkrétní význam - komise 3GPP použila k jejich označení neobsazené názvy rozhraní přidělené od ITU. Názvosloví referenčních bodů používá velká a malá písmena, kde velká slouží k označení skupin funkcí a malá k odlišení konkrétního funkčního bodu.

Rozhraní Cx

Jak už bylo řečeno, HSS je odpovědný za ukládání uživatelských a servisních dat. Tyto informace jsou shromažďovány v okamžiku přihlášení uživatele a jsou používány entitami I-CSCF a S-CSCF když uživatel vytváří nebo přijímá relace. Referenčním bodem mezi HSS a CSCF je Cx, který pracuje na protokolu Diameter. Jdou přes něj tři hlavní procedury: manipulace s uživatelskými daty, autentizace, správa polohy.

Rozhraní Dh

Pokud je v síti použito více HSS a každý má svou adresu, AS neví, který z nich potřebuje kontaktovat. Pro tento případ byl v UMTS release 6 uveden ref. bod Dh. Tento bod vždy spolupracuje s bodem Sh. Aby AS získal adresu HSS, kontaktuje SLF se Sh žádostí určenou pro HSS. Po obdržení HSS adresy od SLF AS ví, kam zaslat svoji žádost. Referenční bod Sh je založen na protokolu DIAMETER a v podstatě se jedná o směrovací mechanismus poskytovaný upraveným DIAMETER Redirect Agentem.

Rozhraní Dx

Funkce tohoto bodu je velmi podobná jako u Dh. Při výskytu více HSS v síti entity I-CSCF a S-CSCF nedokáží identifikovat, kde leží uživatelská data. Pro získání adresy HSS používají body Dx a Cx ve spolupráci s SLF.

Rozhraní Go

Tento bod byl vytvořen k zajištění toho, aby QoS a zdrojová/cílová adresa IMS zařízení splňovala požadavky vyjednané na servisní úrovni. Je

zapotřebí komunikace mezi řídicí vrstvou a uživatelskou vrstvou pomocí GPRS. Toto spojení zajišťuje Go pracující na protokolu COPS.

Rozhraní Gm

Gm propojuje UE a P-CSCF - přenáší veškerou SIP signalizaci mezi koncovým zařízením a IMS sítí. Procedury, které přenáší, se dají rozdělit do tří skupin: *registrace, řízení relace a transakce*.

Rozhraní Gq

Gq je zaveden mezi P-CSCF a PDF a funguje na DIAMETER protokolu. Je určen k přenášení informací o nastavení relace *(policy setup information).* Tyto informace jsou PDF zasílána v každé SIP zprávě obsahující SDP protokol. Nesou údaje jako je IP adresa a číslo portu, šířka pásma, druh protokolu, druh přenášených dat atd.

Rozhraní ISC

Referenční bod ISC *(IMS service control)* slouží k přijímání a odesílání SIP zpráv mezi AS a CSCF. Tyto zprávy se dělí do dvou kategorií: žádosti pro služby poskytované AS a SIP žádosti inicializované AS.

Rozhraní Mg

Mg propojuje okraj CS domény tvořené MGCF s IMS entitou I-CSCF. Tento referenční bod umožňuje MGCF přeposílat signalizaci z CS do I-CSCF. Jak již bylo zmíněno v kap. 1.2.6, MGCF převádí signalizaci ISUP na SIP, Mg tedy pracuje s protokolem SIP.

Rozhraní Mi

Když entita S-CSCF zjistí, že relace má být směrována do CS domény, použije ref. bod Mi k přeposlání relace k BGCF. Mi používá SIP protokol.

Rozhraní Mj

Referenční bod Mj propojuje BGCF a MGCF, využívá SIP protokol. Je využíván v případě, kdy BGCF zjistí, že CS doména je součástí stejné sítě jako daná IMS.

Rozhraní Mk

Mk propojuje entitu BGCF s BGCF v jiné IMS v případě, kdy cílová CS doména není součástí dané sítě. Mk pracuje na SIP protokolu.

Rozhraní Mm

Referenční bod Mm je založený na SIP protokolu a slouží k propojení IMS s mutimediálními sítěmi pracujícími na IP protokolu. I-CSCF skrz Mm přijímá SIP žádost o navázání relace od jiného SIP serveru a přeposílá ji terminálu. Obdobně S-CSCF využívá Mm k přeposlání žádostí o navázání relace z IMS sítě do IP sítí.

Rozhraní Mn

Tento referenční bod využívá entita MGCF pro řízení signalizace a komunikaci s MGW. Narozdíl od většiny ref. bodů s označením M, pracuje na protokolu H.248.

Rozhraní Mp

Referenční bod Mp propojuje MRFC a MRFP. Slouží k přenosu řídících zpráv pro ovládání multimediálních toků, takže je založen na protokolu H.248.

Rozhraní Mr

Mr je využíván, když S-CSCF předává MRFC SIP signalizaci pro navázání relací doručitelského typu *(bearer-related session),* jako jsou např. konference nebo oznámení uživateli. Tento referenční bod není přesně standartizován.

Rozhraní Mw

Rozhraní Mw slouží k vzájemnému propojení entit CSCF - a to jak v rámci propojení uvnitř IMS sítě, tak i v rámci propojení mezi dvěmi IMS sítěmi. Stejně tak jako u ref. bodu Gm se vykonávané procedury rozdělují do tří skupin: *registrace, řízení relace a transakce.* Referenční bod Mw pracuje na protokolu SIP.

Rozhraní Sh

Referenční bod Sh propojuje AS s HSS a je založen na protokolu DIAMETER. Je využíván v případě, když AS požaduje data o uživatelích nebo kterému S-CSCF má zasílat SIP požadavky. Tato data jsou uložena na HSS, který má seznam AS oprávněných přistupovat k uloženým datům. Zpracovávané procedury se dělí do dvou hlavních skupin: *manipulace s daty* a *upozornění/zápis uživatelů.*

Rozhraní Si

Si poskytuje AS pracujím na platformě CAMEL stejné služby jako referenční bod Sh. Tento ref. bod ovšem pracuje na protokolu MAP (součást protokolové sady SS7) a přenáší mezi HSS a IM-SSF uživatelská data vyhovující tradičnímu telefonnímu systému PSTN.

Rozhraní Ut

Referenční bod Ut, založený na HTTP protokolu, propojuje AS s UE a umožňuje uživatelům správu informací využívaných AS. Uživatel si pomocí tohoto bodu může vytvořit PSI *(Public Service Identity)* identifikující služby hostované AS. PSI může mít formát SIP nebo URI, je uložena na HSS.

1.4 Protokoly v IMS

V předchozích kapitolách jsme se setkali s celou řadou protokolových sad, které jsou v rámci IMS využívány. Pro ucelení popisu IMS architektury si popíšeme ty nejdůležitější z nich.

1.4.1 SIP – Session Initiation Protocol

SIP neboli Protokol pro inicializaci relací je široce využívaný internetový protokol pro přenos signalizace a řízení multimediálních komunikačních relací přenášených přes IP. Počátky tohoto protokolu sahají do roku 1996, kdy jej IETF začala využívat k distribuci multimediálního obsahu jako např. přenosy jejich konferencí a seminářů. Díky jednoduchosti a rozšířitelnosti, byl později SIP přijat jako signalizační protokol pro VoIP, když byl v roce 1999 standartizován jako RFC2543. Začal tak postupně nahrazovat doporučení H.323, které svou složitostí nemohlo SIP konkurovat. SIP oproti H.323 zvládá doručování zpráv na větší vzdálenosti a to i přes body s NAT. SIP, zakládající si na své jednoduchosti, ve velké míře vychází z osvědčeného internetového protokolu HTTP - jde tedy o textový protokol fungující na principu dotaz-odpověď [2].

V roce 2000 byl SIP přijat jako signalizační protokol pro 3GPP a trvalý prvek IMS. V rámci IMS jsou jeho hlavní funkce: vytváření, změny a ukončování multimediálních relací a doručování popisu relace uživateli v jeho okamžité poloze. Z hlediska protokolů má IMS na UE jen dva nároky - aby byly kompatibilní s IP a mohly provozovat SIP UA [9].

SIP, jakožto pružný a rozšiřitelný protokol drží krok s vývojem IMS. Naposledy byl upraven v RFC 3261 v roce 2002, ale postupně dal vzniknout několika další protokolům, jako třeba SIMPLE nebo MSRP.

1.4.2 SDP – Session Description Protocol

Jedná se o textový protokol aplikační vrstvy určený k popisu vlastností relace multimediálního přenosu dat. Nepřenáší se pomocí něj vlastní data, ale slouží pro vyjednání parametrů, jako je typ média (video, audio, atd.), transportní protokol (RTP/UDP/IP, H.320, atd.), typ kodeku nebo přenosová rychlost. V IMS je úzce spjatý se SIP [10], [6].

1.4.3 RTP – Real-Time Transport Protocol

RTP standardizuje paketové doručování zvukových a obrazových dat po IP. Používá se pro multimediální streamy (ve spojení s RTSP), jako je telefonie, videokonference a push to talk systémy. Přenáší pro ně datové toky vyjednané SIP, čímž je jedním z technických základů VoIP technologií. Data RTP jsou nejčastěji přenášena pomocí UDP protokolu. Služby pracující s RTP zahrnují určení užitečného zatížení, číslování sekvencí, časové razítkování a sledování přenosu [11], [2].

1.4.4 DIAMETER

DIAMETER je AAA protokol *(authentication, authorization and accounting)* používaný pro širokou řadu přístupových technologií. Hlavní koncept tvoří základní protokol, který může být rozšířen pro poskytování AAA služeb novým přístupovým technologiím. Může pracovat jak lokálně tak i v roamingu. Nahrazuje protokol RADIUS, ze kterého zároveň i vychází. Dělí se na dvě samostatně standartizované části *Diameter Base Protocol* a *Diameter Application* [12].

1.4.5 COPS – Common Open Policy Service

Jde o protokol typu dotaz-odpoveď sloužící k administraci, upravám a vynucování pravidel stanovených PDF, používá se ke komunikaci mezi entitami P-CSCF a GGSN. COPS specifikuje poměrně jednoduchý model výměny informací o pravidlech mezi klientem-serverem pomocí příslušného signalizačního protokolu [13].

1.4.6 MEGACO – Media Gateway Control Protocol

Megaco neboli H.248 se obecně používá pro řízení multimediálních bran v IP sítích a PSTN. Je používám mezi multimediální branou a jejím řízením pro zpracování signalizace a řízení multimediální relace [14].

2 Testování IMS

Testování IMS technologie a jejího propojení s PBX Asterisk probíhalo na počítačových stanicích umístěných v Laboratoři spojovacích systémů, koncových zařízení a konvergovaných síťových technologií (PA-427) na Ústavu telekomunikací fakulty FEKT.

Platformu IMS lze zprovoznit a testovat více způsoby, existují nejméně 4 nástroje, které simulují funkčnost IMS technologie:

1.) IMS Model for Opnet Modeler – model IMS sítě pro Opnet Modeler, známý software pro návrh, simulaci a analýzu sítí. Pracuje pod OS Windows i Linux, nejedná se o Open source software.

2.) Ericson Software Development Studio – nástroj pro vývoj IMS aplikací a testování IMS

3.) VNUML (Virtual Network User Mode Linux) – Open source virtualizační nástroj pro simulaci a testování síťového prostředí.

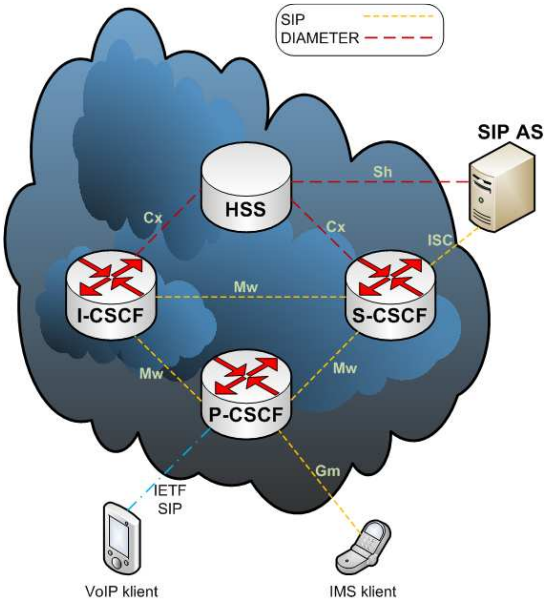
4.) Open IMS Core – Open source prostředí pro testování IMS technologie pracující pod linuxovými operačními systémy.

Z uvedených možností byl pro testování zvolen systém Open IMS Core, který byl vyvinut výhradně na Open source a volně dostupných nástrojích. Zároveň tento systém využívá k testování IMS služeb a produktů většina vývojářů a poskytovatelů [24].

2.1 Open IMS Core

Jedná se o projekt Fraunhoferova Institutu FOKUS *(Fraunhofer Institut für Offene Kommunikationssysteme),* který implementuje funkce CSCF a HSS (tedy jádro IMS, viz. Obr. 2.1) v Open source prostředí operačního systému Linux. Projekt vznikl pro vzdělávací účely a zvýšení dostupnosti principů IMS technologie. Vzhledem k otevřenosti celého projektu a faktu, že je postaven výhradně na Open source a volně dostupných nástrojích a aplikacích, se jedná o vhodný nástroj pro realizaci zadání práce.

Open IMS Core je distribuován ve dvou podobách – ve formě instalačních balíčků nebo ve formě image souboru s již nainstalovaným OS Linux a základní konfigurací Open IMS Core.



Obrázek 2.1 Struktura prostředí Open IMS Core [15]

2.2 Zprovoznění IMS sítě

Jak už bylo zmíněno, Open IMS Core (OIC) je navržen tak, aby pracoval pod OS Linux. Verze kernelu (jádra) musí být 2.6 a konkrétní distribuce Linuxu vhodná pro chod OIC stanovena není. Simulátor IMS prostředí by tedy měl fungovat na všech distribucích, které splňují softwarové požadavky uvedené v [16]. V našem případě byla zvolena distribuce Ubuntu (verze 10.4).

Po nainstalování OS se přistoupilo k samotnému stáhnutí zdrojového kódu OIC a jeho kompilaci - stručný návod je uveden v [16]. Návod pro instalaci *E-CSCF* a *LRF* je popsán v [17]. Oproti stáhnutí již předinstalovaného obrazu disku je tento postup výhodnější v tom, že zdrojový kód je vždy z nejaktuálnější revize podporované vyvojáři. Uživatel také touto cestou získá přehled o nainstalovaných balíčcích, službách a jejich konfiguraci.

V základu je Open IMS Core nastaven tak, aby pracoval na lokální smyčce *127.0.0.1*. Pro další postup bylo nutné toto nastavení změnit a u

jednotlivých služeb přepsat IP adresy, aby fungovaly na síťové adrese stanice *192.168.110.34.* Síťové adresy jednotlivých uzlů bylo nutné přepsat *ve složce /opt/OpenIMSCore* v souborech: *icscf.cfg, icscf.xml, pcscf.cfg, pcscf.xml, scscf.cfg a scscf.xml.* Pro HSS se editovaly soubory *DiameterPeerHSS.xml* a *hss.properties* v podsložce .../*FhoSS/deploy.*

Podobný postup se musel vykonat i pro nastavení DNS a přidružené síťové služby. Přeadresovány byly:

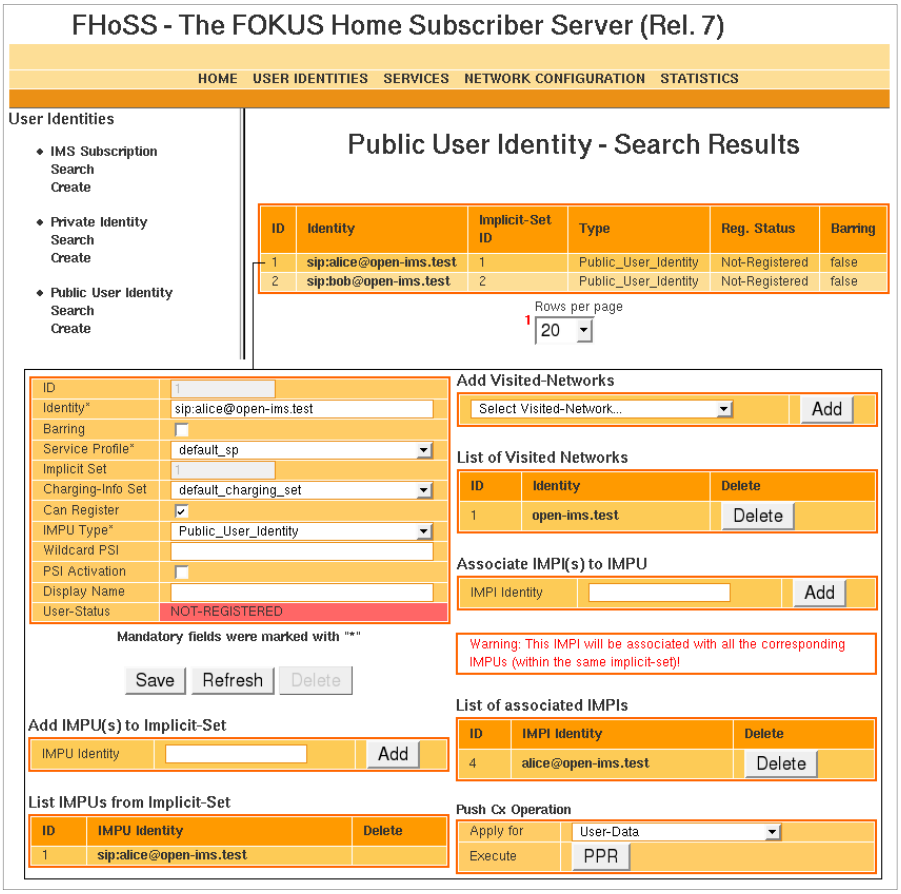
- soubor */etc/resolv.conf* kvůli přístupu k DNS
- soubor */etc/hosts* pro korektní adresaci definovaných domén
- DNS zóna definovaná v */etc/bind/open-ims.test*
- nastavení síťových rozhraní */etc/network/interfaces,* kde bylo nutné nastavit místo automatického přidělování IP adres statické údaje:

```
auto eth0
iface eth0 inet static
address 192.168.110.34
netmask 255.255.255.0
```

Nyní se mohlo přistoupit k samotnému spuštění služeb *P-CSCF I-CSCF, S-CSCF* a *HSS* (v rámci OIC pojmenován jako *FHoSS*). Každou službu je nutné spustit s právy *root* nebo *sudo* v jednotlivých oknech terminálu, ve kterých pak lze sledovat chod i chybová hlášení. Po spuštění jmenovaných služeb je přístup k *FHoSS* umožněn přes webové rozhraní, v našem případě z adresy *http://192.168.110.34:8080* (přístupové jméno: *hssAdmin* a heslo: *root*). Druhou možností správy OIC jsou konzolové příkazy využívající konfigurační skripty umístěné v */opt/OpenIMSCore/ser_ims/cfg.* Webové rozhraní umožňuje rychlejší a efektivnější správu, proto byla při testování využívána jen tato možnost. Administrátorská webová konzole je rozdělena na 4 sekce:

- User Identities – slouží k manipulaci s uživatelskými účty a jejich nastaveními
- Services – sekce určená pro správu servisních profilů, aplikačních serverů a přidružených funkcí

- Network Configuration – nastavení navštívených sítí, sad zpoplatňovacích funkcí, preferovaných *S-CSCF* atd.
- Statistics – umožňuje logování činnosti HSS v informativním a debug módu



Obrázek 2.2 – Ukázka webového rozhraní a uživatelských účtů

Jak už bylo zmíněno, v sekci User Identities lze vytvářet, měnit a mazat uživatelské identity. V základním nastavení OIC jsou již předem vytvořeny dva testovací účty Alice a Bob, které byly použity pro otestování komunikace a funkčnosti IMS sítě. Testování proběhlo pomocí dvou mobilních smart telefonů HTC s operačním systémem Android a aplikací IMSDroid. Po nastavení odpovídajících uživatelských a síťových parametrů v aplikaci IMSDroid (*IMPU*, *IMPI*, adresa *P-CSCF a* port, název realmu, tajný klíč/heslo) se uživatelé Alice a Bob skrz *AP* a počítačovou síť v laboratoři připojili k IMS síti a úspěšně se registrovali. Následovalo navázání komunikace mezi uživateli v podobě instant

messagingu, přenosu hlasu a videohovoru. Tímto bylo ověřeno, že je operační systém i Open IMS Core správně nakonfigurován a mohlo se přistoupit k další práci.

2.3 IMS desktopové klientské aplikace

V současné době existuje několik IMS klientů pro prostředí OS Linux. Pro testování byli vybráni 3 nejrozšířenější. Každý se liší podporovanými funkcemi a možnostmi nastavení, proto si je jednotlivě přiblížíme a následně uvedeme ukázky testování a analýzy komunikace.

2.3.1 UCT IMS Client

Tento komplexní klient byl navržený přímo pro použití v Open IMS Core, jeho vývoj stále probíhá ve Fraunhoferově Institutu FOKUS a je pod licencí GNU GPL. Podporuje širokou řadu funkcí, jako jsou video/audio hovory, instant-messaging, prezenční služby, IPtv, XCAP a další. Vývoj tohoto projektu dal vzniknout i několika souvisejícím vedlejším projektům týkajících se např. podpory QoS, Funkce zpoplatnění, IPtv streaming serveru atd. Pro podrobné informace a návod k instalaci viz. oficiální stránky [18]. V rámci této práce byl klient využíván pro audio/video hovory a IM.

2.3.2 myMONSTER-TCS

Jedná se o multiplatformní telekomunikační aplikaci ***M**ultimedia **O**pen InterN**e**t **S**ervices and **T**elecommunication **E**nvi**R**onment* taktéž vyvíjenou ve Fraunhoferově Institutu FOKUS. Vyvinul se z IMS klienta známého jako OpenIC a podporuje rozsáhlé spektrum protokolů a služeb jako např. chat a IM, polohovací služby, sdílení souborů, prezenční služby, GLM, audio/video hovory a také několik doplňků (Add-ons). Ve zpoplatněné verzi klienta jsou k dispozici i další rozšířené funkce, nicméně pro testování OIC plně postačuje klient ve volně dostupné verzi určené pro nekomerční a vzdělávací účely. Stejně jako

UCT IMS Client se tento klient používal pro IM a audio/video hovory. Pro podrobnější dokumentaci viz. stránky projektu [19].

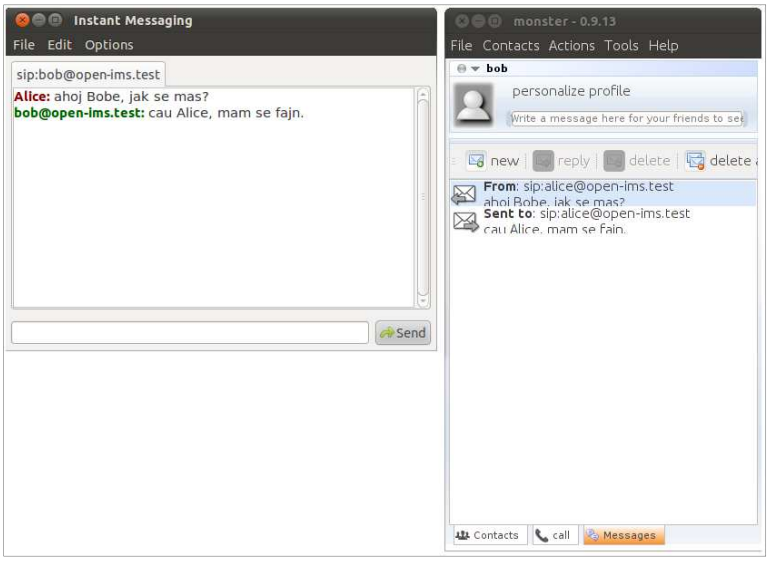
2.3.2 IMS Communicator

Ve srovnání se dvěmi předešlými klienty jde o méně rozsáhlý produkt, který vzniknul za účelem vývoje a testování NGN sítí, zejména IMS a projektu Open IMS Core. Klient je volně šiřitelný pod licencí GNU GPL a umožňuje využívání prezenčních služeb, IM, audio/video hovorů a několika přidružených funkcí. Při testování OIC byl tento klient používán pro IM a hlasovou komunikaci. Video hovory nebylo možné uskutečnit, protože tento klient nebyl schopen detekovat webovou kameru. Příčinu se nepodařilo identifikovat. Dokumentace k projektu a informace jsou dostupné z [20].

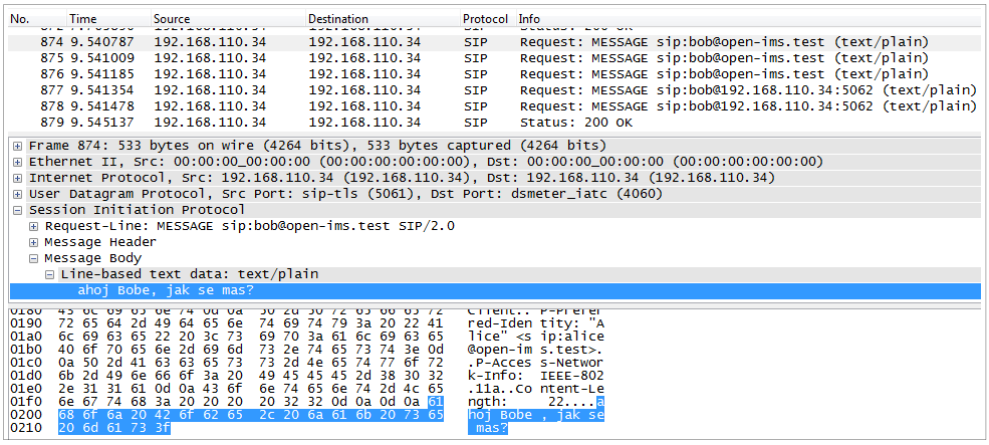
2.3.3 Analýza komunikace IMS klientů

Po úspěšném nainstalování klientů, se mohlo přistoupit k otestování jejich funkčnosti. Pro registraci uživatele k *HSS* jako Alice/Bob se v klientovi vyplní příslušné *IMPU*, *IMPI*, adresa *P-CSCF* serveru a jeho port, název realmu a tajný klíč/heslo. Klienti nabízí i další nastavení, ale pro otestování IM komunikace mezi klienty stačí zadat jen tyto údaje. Pro otestování byli zvoleni klienti UCT IMS Client a myMONSTER.

Po spuštění klientů, registraci uživatelů a zahájení vzájemné IM komunikace následovala analýza předávání SIP signalizace a zpráv v rámci IMS sítě. K podrobné analýze byla použita aplikace Wireshark, která na zvoleném síťovém zařízení dokáže zachytávat pakety, dešifrovat je a na základě použitého protokolu analyzovat a vyhodnotit. Wireshark je k dispozici pod GNU GPL licencí a lze používat pod operačními systémy Windows, Unix, Linux i Mac OS X.



Obrázek 2.3 – Ukázka IM komunikace mezi klienty UCT IMS Client a myMonster



Obrázek 2.4 – Ukázka zachycení zprávy přes Wireshark

Z Obr. 2.4 je patrné, že zpráva byla předávána pomocí protokolu SIP a putovala přes několik entit. Podrobnější analýzou zpráv s příznakem *Request: MESSAGE* zjistíme, o které entity se jedná. Stačí u každé této zprávy dohledat UDP část, kde je popsán zdrojový a cílový port.

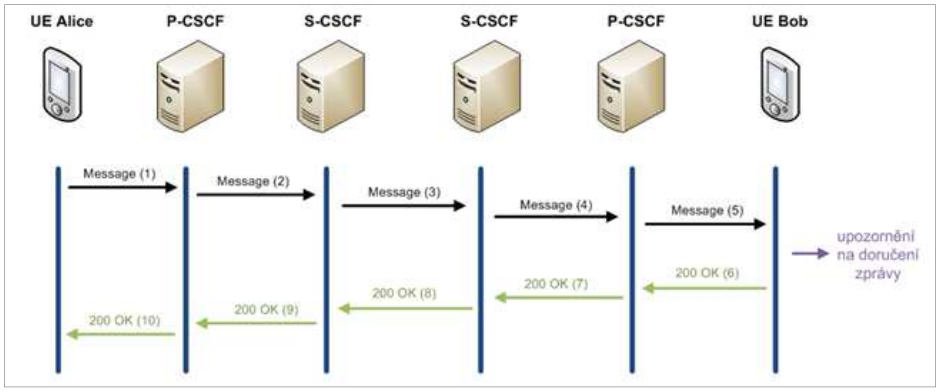
Informace o portech lze zjistit i ze SIP hlaviček, které se při průchodu každou entitou mění a zaznamenávají trasu, kterou zpráva prošla (viz. Obr. 2.5). Dle [9] každou transakci označuje parametr *Branch,* který se vždy při dalším kroku mění. Pole hlavičky *Via* dle [25] může obsahovat parametr *rport*, který při nespolehlivém přenosu umožňuje klientovi požadovat po serveru, aby

zaslal odpověď zpět na zdrojovou IP adresu a port, ze kterého požadavek pochází.

```
▼ Session Initiation Protocol
  ▶ Request-Line: MESSAGE sip:bob@192.168.110.34:5062 SIP/2.0
  ▼ Message Header
    ▶ Via: SIP/2.0/UDP 192.168.110.34:4060;branch=z9hG4bKeef1.0c67ba3.0
    ▶ Via: SIP/2.0/UDP 192.168.110.34:6060;rport=6060;branch=z9hG4bKeef1.27c7faf7.0
    ▶ Via: SIP/2.0/UDP 192.168.110.34:6060;branch=z9hG4bKeef1.17c7faf7.0
    ▶ Via: SIP/2.0/UDP 192.168.110.34:4060;branch=z9hG4bKeef1.fb67ba3.0
    ▶ Via: SIP/2.0/UDP 192.168.110.34:5061;rport=5061;branch=z9hG4bK1374509750
    ▶ From: "Alice" <sip:alice@open-ims.test>;tag=2133501934
    ▶ To: <sip:bob@open-ims.test>
```

Obrázek 2.5 – Ukázka SIP hlavičky

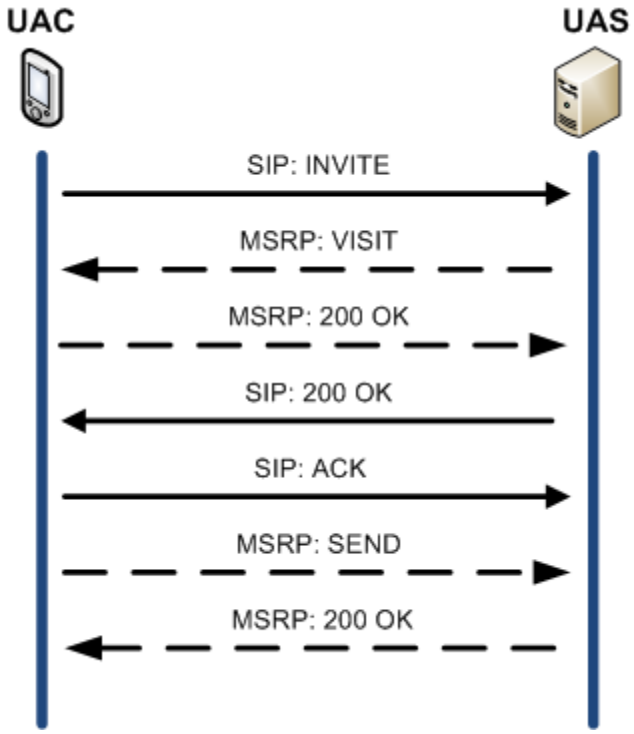
Zdrojový port 5061 je portem klienta Alice - ten předává zprávu portu 4060, který náleží *P-CSCF*. Zpráva dále putuje z portu 4060 na port 6060 (*S-CSCF*), ten ji předá opět portu 6060, ovšem zde je již zpráva na straně uživatele Alice. Dále proběhne předání zprávy na port 4060, odkud směřuje na port klienta Bob 5062. Bob je IM klientem upozorněn na novou zprávu a mezitím je Alici vyslána zpráva *200 OK*, která potvrzuje úspěšné doručení zprávy. Pro názornost viz. Obr. 2.6.



Obrázek 2.6 – Flow diagram zaslání zprávy v Pager módu

Z analýzy vyplývá, že komunikace probíhala v tzv. *Pager módu*, kdy mezi koncovými uživateli nedochází k navázání relace, ale pouze zaslání zprávy a potvrzení jejího doručení. Druhou možností výměny zpráv v IMS síti je *Session-based Instant Messaging* nebo-li IM založený na relaci. V tomto případě je

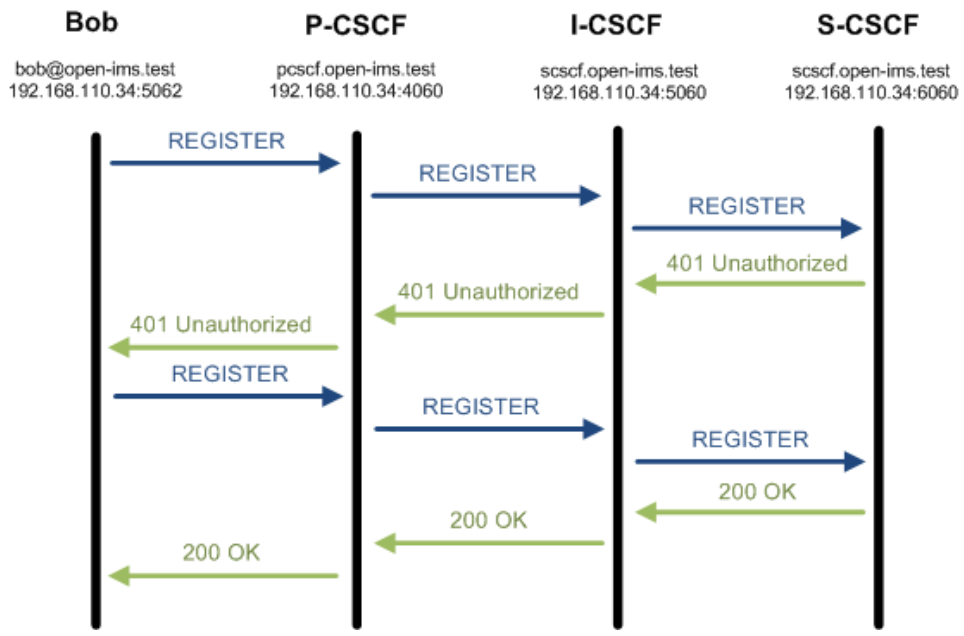
relace navázána pomocí metody SIP INVITE a přenos zpráv je uskutečněn pomocí protokolu *MSRP (The Meesage Session Relay Protocol)* [6].



Obrázek 2.7 – Zaslání zprávy při Session Based IM [6]

Na Obrázku 2.7 vidíme postupně jdoucí zaslání žádosti SIP: INVITE (která zároveň obsahuje SDP informující o typu média a podpoře MSRP), odpověď v podobě MSRP: VISIT sloužící k navázání spojení mezi dvěmi MSRP koncovými body. UAC potvrzuje pomocí MSRP: 200 OK, následně obdrží SIP:200 OK a relace je zahájena pomocí odpovědi SIP: ACK. Po zahájení relace lze mezi koncovými body zasílat zprávy pomocí zaslání MSRP: SEND a potvrzení MSRP: 200 OK.

Po analýze IM komunikace byl zachycen proces registrace uživatele do IMS sítě. Výměnu SIP zpráv mezi jednotlivými entitami ilustruje Obr. 2.8. IMS UAC zasílá žádost *REGISTER* do své domovské sítě, přes P-CSCF a I-CSCF je zpráva přeposlána S-CSCF. Tato entita řeší autorizaci a autentizaci, zasílá zpět odpověď *401 Unauthorized*, která v poli *WWW-Authenticate* obsahuje použitý kódovací algoritmus (AKAv1-MD5), zakódovaný autentizační token (*AUTN*) a náhodnou výzvu (*RAND*), viz Obr. 2.9.



Obrázek 2.8 – Proces registrace

```
WWW-Authenticate: Digest realm="open-ims.test", nonce=
    Authentication Scheme: Digest
    realm="open-ims.test"
    nonce="+AXmZeZz6vHx0ZPNclCcq/PDUtUZ8AAAL/LQyCHnmJU="
    algorithm=AKAv1-MD5
    ck="99fbb010f54846d187e401cc033b7f77"
    ik="9addc7b8c298452231f07e3ea2291ec9"
```

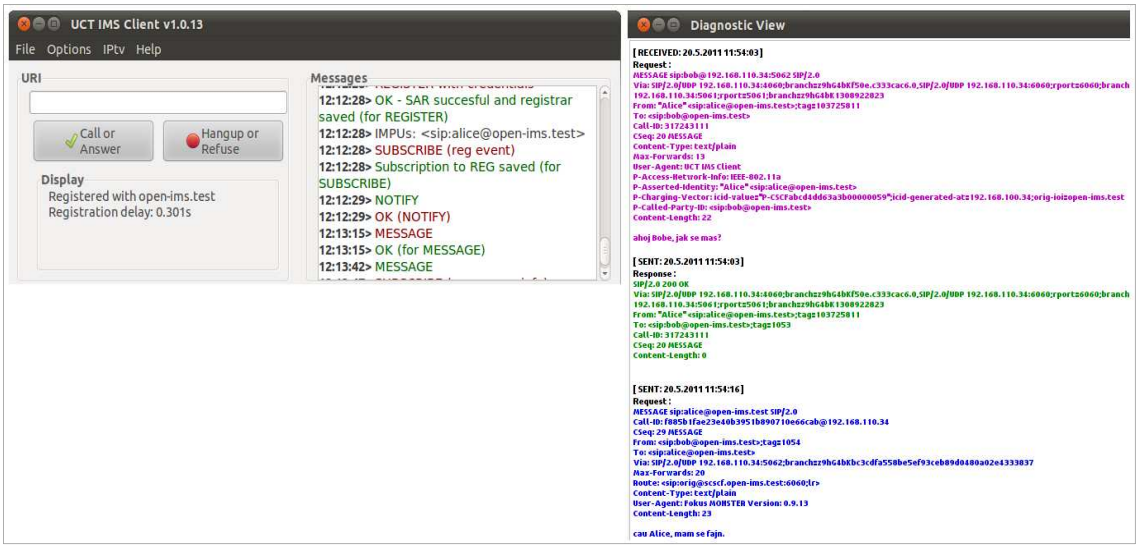
Obrázek 2.9 – Pole WWW-Authenticate

Terminál po obdržení zprávy *401 Unauthorized* vypočítá z hodnoty *nonce* odpovídající *AUTN* a *RAND.* Dojde k odeslání žádosti *REGISTER*, která v poli *Authorization* obsahuje vygenerovanou odpověď RES. Ta je na straně S-CSCF porovnána s očekávanou hodnotou (XRES) a pokud hodnoty vzájemně odpovídají, uživatel je autentizován a dostává odpověď *200 OK.*

```
Authorization: Digest username="bob@open-ims.test",rea
    Authentication Scheme: Digest
    username="bob@open-ims.test"
    realm="open-ims.test"
    nonce="+AXmZeZz6vHx0ZPNclCcq/PDUtUZ8AAAL/LQyCHnmJU="
    uri="sip:open-ims.test"
    algorithm=AKAv1-MD5
    response="1b95571b18d1ba7aebaf7e28111cacbf"
    integrity-protected="no"
```

Obrázek 2.10 – Pole Authorization

Aplikace Wireshark je sice nejkomplexnějším nástrojem pro zachytávání a analýzu komunikace, nicméně existují i další možnosti jak monitorovat činnost IMS klienta. V UCT IMS Client lze činnosti a hlášení sledovat v okně *Messages.* Oproti tomu aplikace myMONSTER nabízí v sekci *Tools–Diagnostics* mnohem podrobnější výpis činnosti klienta, viz Obr. 2.11.



Obrázek 2.11 – Ukázka výpisu klientů UCT IMS Client a myMONSTER

Základní úkony klientů jako registrace/deregistrace nebo přijetí/odeslání zprávy můžeme sledovat přímo z konzole nebo také z logu webového rozhraní *FHoSS*, což se může hodit například při špatné konfiguraci, kdy se v konzoli objeví chybové hlášení.

2.4 PBX Asterisk 1.4

Asterisk je softwarová open source implementace telefonní ústředny (PBX) pro PC. Pracuje pod linuxovými a unixovými operačními systémy, nabízí rozsáhlé možnosti propojení pro telefonní hardware i software a přidružené telefonní aplikace. Umožňuje spojení s vnějšími telefoními službami, přepojování hovorů, správu linek, propojování uživatelů s veřejným telefonním systémem přes IP, analogová a digitální spojení. Velkou výhodou je podpora modulů a tedy rozšiřitelnost, podpora širokého spektra audio kodeků a jejich

vzájemných převodů. Asterisk dovede pracovat s několika protokoly, zejména VoIP, SIP, H.323, MGCP, IAX a zvládá převody signalizace mezi nimi. Může tedy sloužit i jako multimediální brána pro převod signalizace mezi sítěmi pracujícími na odlišných protokolech [21].

2.4.1 Instalace PBX Asterisk

Nároky na počítačovou stanici provozující PBX Asterisk se různí dle předpokládaného vytížení ústředny, počtu uživatelů a klapek (extensions), použitých prvků/modulů Asterisku a také typu využitých kodeků. Za předpokladu, že bude Asterisk nainstalován pod distribucí OS s nevelkými hardwarovými nároky (základní Linuxové/Unixové instalace bez grafického rozhraní), měl by bez problémů pracovat na stanicích s procesory o taktu 500MHz a operační pamětí 128MB RAM. Jedná se tedy o další výhodu, kterou využití Asterisku nabízí – lze používat na počítačích, které jsou v dnešní době považovány za zastaralé.

V našem případě byla pro nainstalování OS a Asterisku použita stanice s parametry: *CPU 733MHz, 320MB RAM, 10GB HDD, IP adresa: 192.168.110.35*. Jako operační systém byla vybrána Linuxová distribuce CentOS 5.5. Verze Asterisku byla zvolena verze 1.4, která plně dostačuje pro testování propojení Asterisku s IMS. Po úspěšném nainstalování OS a zprovoznění PBX Asterisk, se mohlo přistoupit k řešení samotného problému propojení s OIC.

2.5 Propojení PBX Asterisk s Open IMS Core

Na základě předešlých pokusů o propojení Asterisku a OIC [22] bylo předpokládáno, že hlavním problémem při propojení bude nestandartní implementace SIP použitá v OIC. OIC přidává dodatečný příznak v SIP hlavičce pro směrování a multimediální prostupnost, kterou Asterisk nezpracuje. Na SIP metodu *INVITE* reaguje statusem *420 Bad extension*, který se dle standardu [9] generuje vždy v případech, kdy *UAS* (User Agent Server) nezná označení

možnosti (*option-tag*) uvedené v části hlavičky s požadavky (*Require header field*).

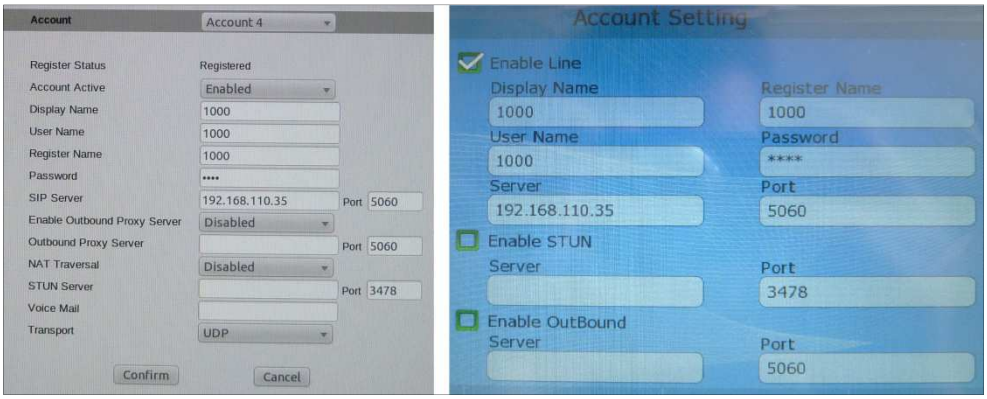
Ukázalo se, že k přidávání nestandartního option-tagu do hlavičky dochází v případě, pokud je na straně klienta nastavena hodnota QoS vyšší než žádná. V tomto případě klient vyžaduje rezervaci zdrojů pro QoS před samotným sestavením spojení. Do SIP hlavičky je proto dle standardu [23] přidán příznak *Require:precondition*, který Asterisk v souladu se základním SIP protokolem [9] neumí rozeznat.

Řešení tohoto problému uvedené v [22] spočívá v modifikaci zdrojového kódu Asterisku, konkrétně souboru *asterisk/channels/chan_sip.c* (viz příloha A). Nejedná se tedy přímo o řešení problému, ale spíš vynucení jeho ignorování na straně Asterisku – jak už bylo zmíněno, Asterisk se v tomto případě chová dle standardu. Druhým řešením je nastavení klientů/UE tak, aby nebylo používáno QoS. Toto řešení bylo upřednostněno a použito pro další postup.

Propojení Asterisku a OIC předpokládá plně funkční konfiguraci obou entit a přidruženého klientského softwaru i hardwaru. Nyní tedy jako poslední bod si zbývá přiblížit konfiguraci *VoIP* koncového zařízení a přidruženého uživatelského účtu.

Jako UE byl použit IP videotelefon Yealink VP-2009, tedy zařízení vhodné pro testování přenosu hlasu i videa v rámci *IMS-to-SIP* relace. Videotelefonu byla přidělena IP adresa *192.168.110.141*, která zároveň sloužila i jako adresa pro přístup do konfiguračního rozhraní telefonu přes webový prohlížeč (uživatel: *admin*, heslo: *admin*). V sekci s uživatelskými účty byl vytvořen testovací účet s názvem *1000* a jako *SIP server* byla uvedena IP adresa PC s PBX Asterisk (pro přesná nastavení viz. Obr. 2.12.) Nastavení účtů lze provádět i přímo ve videotelefonu v sekci *Settings – Account Settings.*

Po nastavení uživatelského účtu na IP telefonu bylo třeba definovat uživatelský kanál v PBX Asterisk. Konfigurační soubor Asterisku *sip.conf* slouží k nastavení SIP kanálů pro příchozí i odchozí hovory. Cílem jeho úprav bylo zajistit co nejjednodušší funkční konfiguraci kanálu pro realizaci spojení *IMS-SIP* (viz. Příloha B). Prvním ukazatelem správného nastavení uživatelského účtu i kanálu byl status videotelefonu *Registered.*



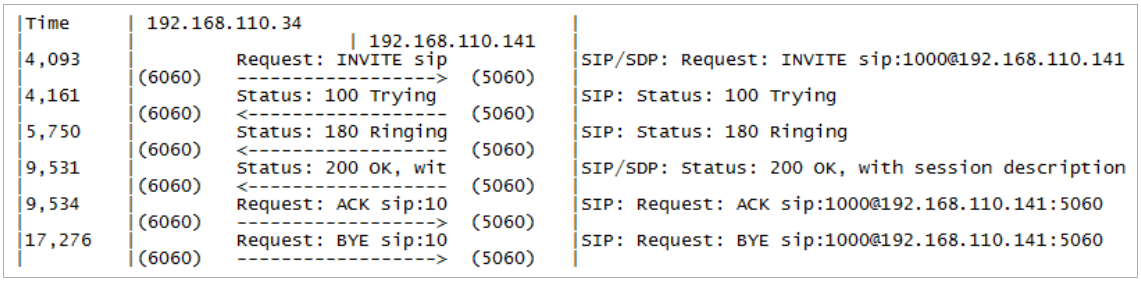
Obrázek 2.12 – Nastavení uživatelského účtu přes webové rozhraní a videotelefon

2.5.1 Testování propojení IMS a PBX Asterisk

Po nakonfigurování všech potřebných prvků, se mohlo přistoupit k uskutečnení komunikace mezi IMS desktopovým klientem a IP telefonem. Z pochopitelných důvodů stanice s desktopovým klientem vyžadovala připojení sluchátek, mikrofonu a webkamery.

2.5.1.1 Audio hovor

První fáze testování bylo uskutečnění hlasového hovoru pomocí klienta myMONSTER, který inicioval relaci s uživatelem *1000* – *URI sip: 1000@192.168.110.141* (uživatel@IP adresa). Pomocí programu Wireshark byla zachytávána komunikace na síťovém rozhraní *eth0.* Vygenerovaný flow diagram vypadá následovně:

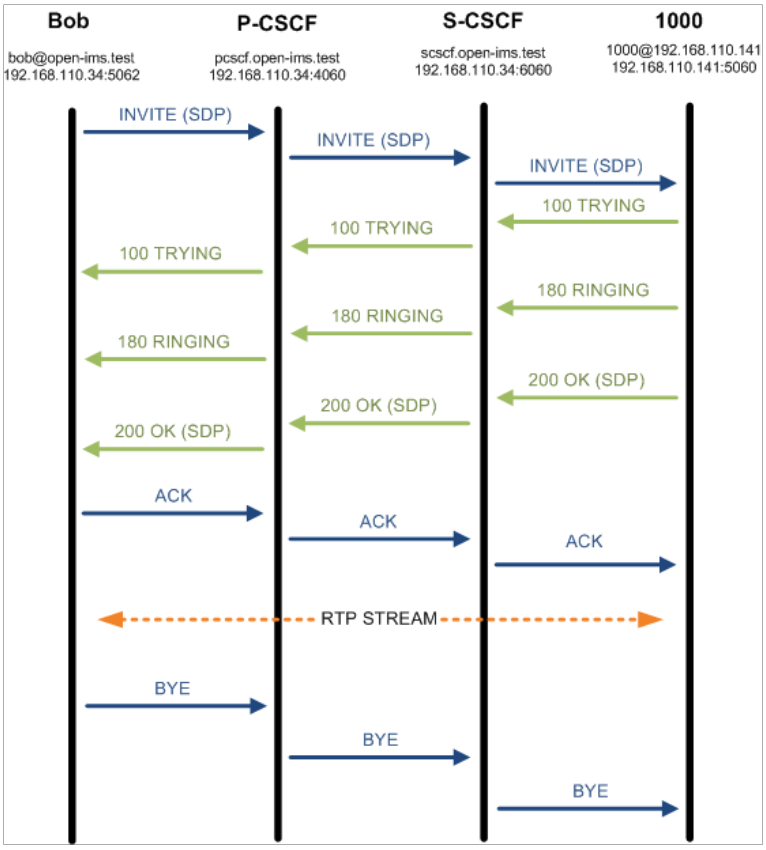


Obrázek 2.13 – Flow diagram mezi síťovým rozhraním eth0 a IP telefonem

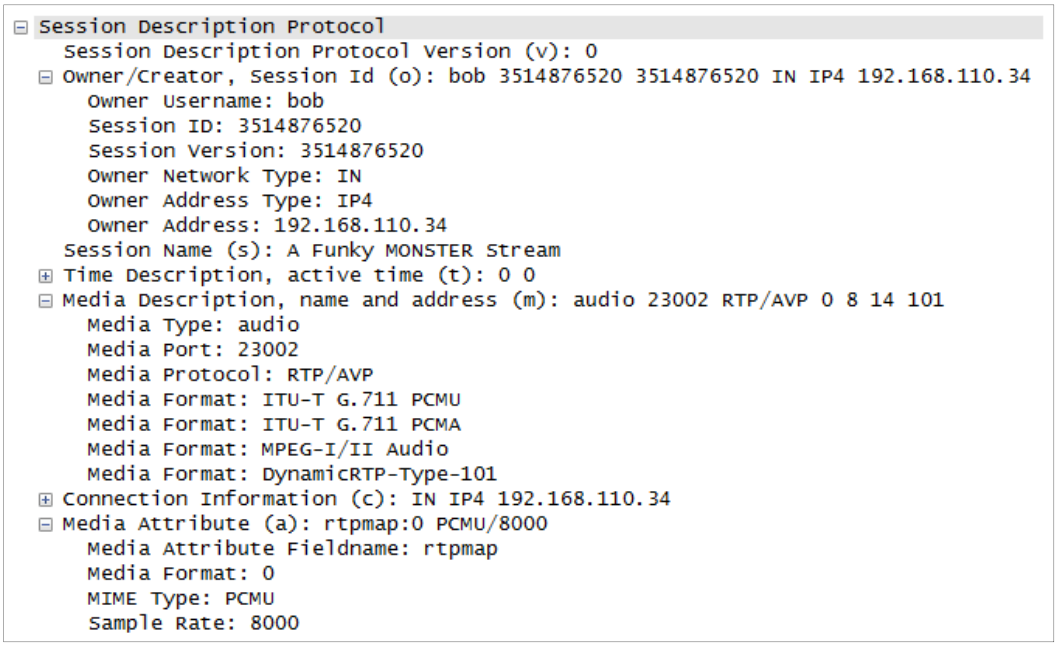
Zde je zachycena ovšem pouze SIP signalizace mezi rozhraním *eth0* a IP telefonem, nikoliv však signalizace, která probíhala uvnitř IMS sítě.

Podrobnou analýzou zachycených paketů lze úplný flow diagram znázornit tak, jak ukazuje obr 2.14.

Klient uživatele Bob vygeneruje požadavek *INVITE,* kterým zahajuje komunikaci o plánované relaci. Požadavek současně obsahuje i protokol SDP s popisem parametrů streamového toku dat, jako např. druh média, port, podporované protokoly, kodek, vzorkovací rychlost atd. (viz. Obr. 2.15). Požadavek předává dál P-CSCF, odkud pokračuje přes S-CSCF na port 5060 uživatele 1000. Ten obratem zpět zasílá Status: *100 TRYING* indikující přijetí požadavku *INVITE*. Následně zasílá zpět *Status: 180 RINGING*, který informuje o zvonění UE. Poté uživatel 1000 přijímá hovor a dochází k zaslání zprávy *200 OK,* inforumující protější stranu, že je připraven k výměně multimediálních dat. Zároveň se v těle zprávy zasílá SDP obsahující informace o možnostech audia, které dané zařízení podporuje. Uživatel Bob odpovídá metodou ACK, potvrzující zahájení relace. Tím je zahájen audio stream realizovaný pomocí RTP protokolu a audio kodeku G.711. Hovor je ukončen metodou BYE, která v jiných případech může znamenat i zamítnutí hovoru.



Obrázek 2.14 - Úplný flow diagram audio relace



Obrázek 2.15 – SDP s popisem audio relace

Zaznamenané statistiky RTP streamů jsou uvedeny na Obr. 2.16. Během relace nedošlo ke ztrátě paketů, maximální hodnota zpoždění byla 108ms (běžné hodnoty u VoIP jsou stovky ms) a kolísání zpoždění (*Jitter*) bylo řádově v jednotkách ms (u VoIP bývá běžně v desítkách až stovkách ms).

Src IP addr	Src port	Dst IP addr	Dst port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
192.168.110.141	11800	192.168.110.34	23002	0xB8C301DF	g711U	2418	0 (0,0%)	32,71	10,49	5,99
192.168.110.34	23002	192.168.110.141	11800	0x6665B416	g711U	2624	0 (0,0%)	108,22	9,29	6,21

Obrázek 2.16 – Statistiky RTP

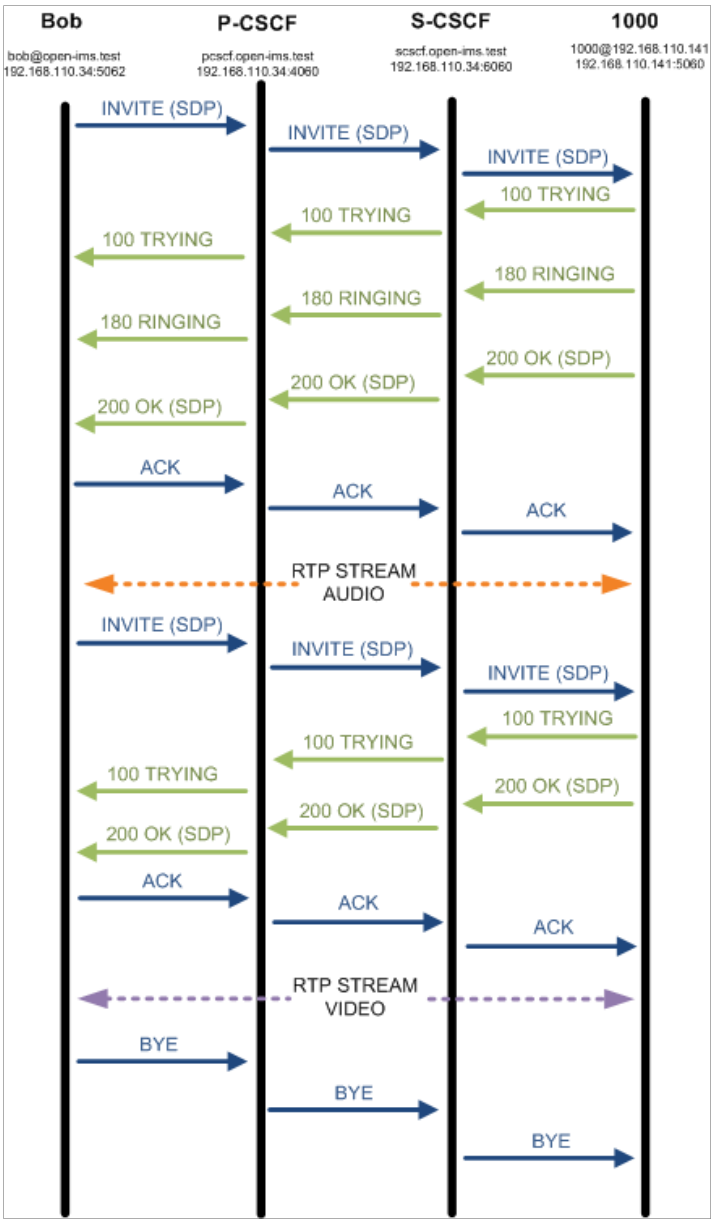
2.5.1.2 Video hovor

Po úspěšné realizaci přenosu hlasu mezi desktopovým klientem a IP telefonem se přistoupilo k otestování audio/video relace. Konfigurace stanic, zařízení a softwaru zůstala stejná jako u audio relace. Průběh relace ilustruje flow diagram Obr. 2.17.

Stejně jako u předešlého audio hovoru, relace začíná vygenerováním metody *INVITE* na straně uživatele Bob a jejím postupným předáváním přes *P-CSCF* a *S-CSCF* k *UE* uživatele 1000. Následuje zaslání metod *100 TRYING, 180 RINGING* a *200 OK* uživateli Bob, který odpovídá metodou *ACK* a zahajuje se audio stream. V další fázi hovoru, kdy uživatel Bob aktivuje vysílání videa

z webkamery, dochází generování další metody *Request: INVITE.* SDP část zprávy tentokrát obsahuje kromě informací o audiu i informace o videu – protokol, podporované formáty, port, kodek, vzorkovací frekvence atd. (viz. Obr. 2.18). Uživatel 1000 odpovídá postupně zprávami *100 TRYING* a *200 OK.*

V SDP části zprávy *200 OK* specifikuje u videa možnosti podporované zařízením, port, použitý kodek *(h.263)*, rychlost vzorkování (90000), použití *CIF/QCIF* atd. Po obdržení příznaku *ACK* od uživatele Bob je zahájen RTP/h.263 video stream. Hovor je po 35s ukončen metodou *BYE.*

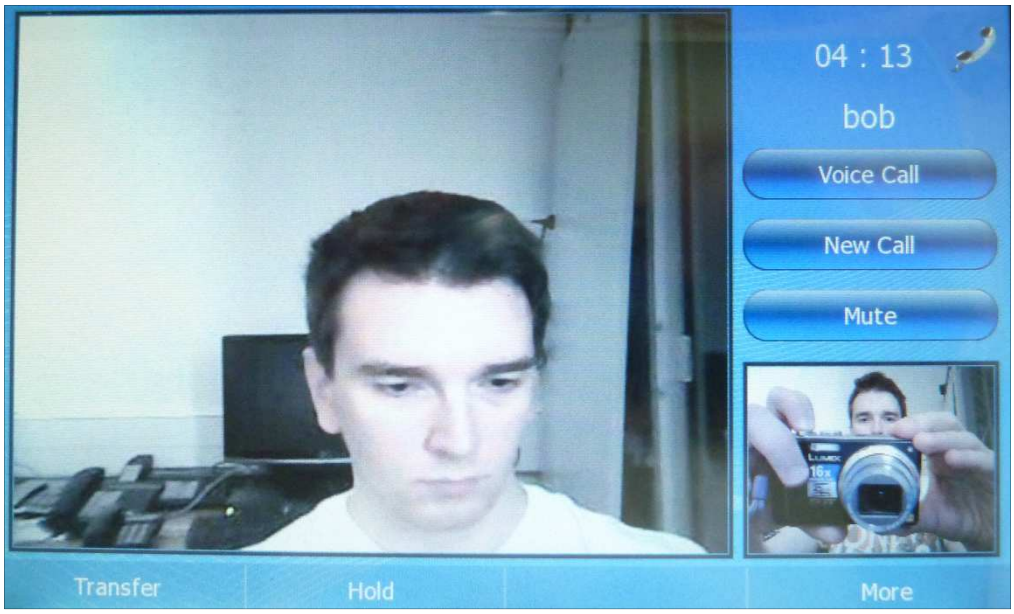


Obrázek 2.17 – Flow diagram video hovoru

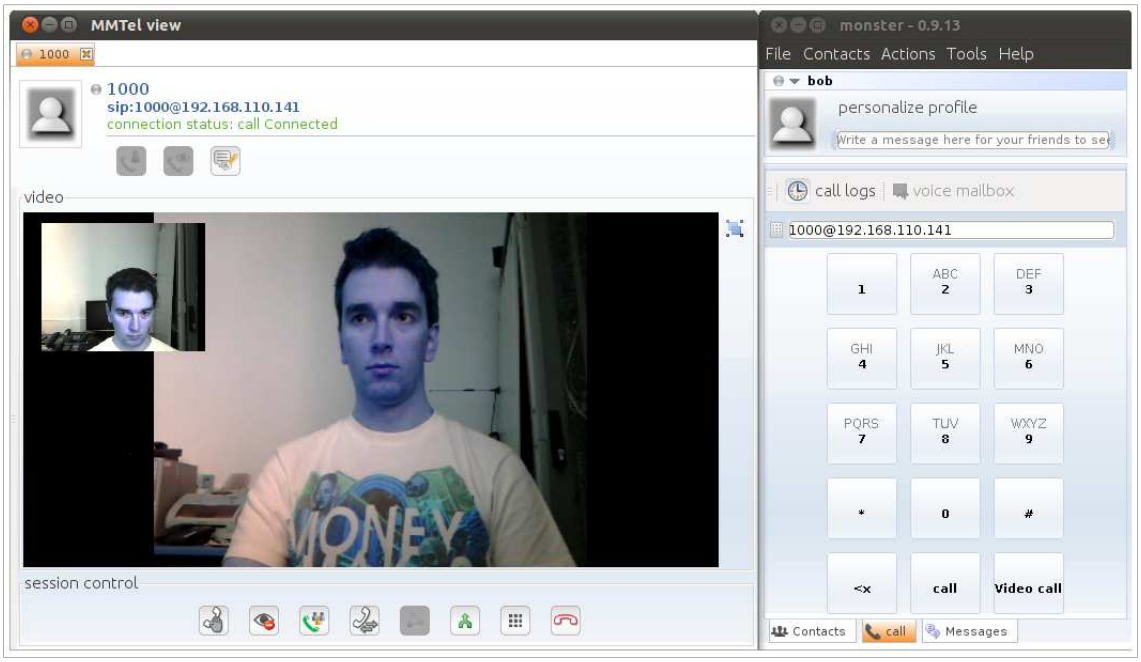
```
Session Description Protocol
    Session Description Protocol Version (v): 0
  ⊞ Owner/Creator, Session Id (o): bob 3514876627 3514876632 IN IP4 192.168.110.34
    Session Name (s): A Funky MONSTER Stream
  ⊞ Time Description, active time (t): 0 0
  ⊞ Media Description, name and address (m): audio 23004 RTP/AVP 0 101
  ⊞ Connection Information (c): IN IP4 192.168.110.34
  ⊞ Media Attribute (a): rtpmap:0 PCMU/8000
  ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
  ⊟ Media Description, name and address (m): video 23006 RTP/AVP 34 96 32 97
      Media Type: video
      Media Port: 23006
      Media Protocol: RTP/AVP
      Media Format: ITU-T H.263
      Media Format: DynamicRTP-Type-96
      Media Format: MPEG-I/II Video
      Media Format: DynamicRTP-Type-97
  ⊞ Connection Information (c): IN IP4 192.168.110.34
  ⊟ Media Attribute (a): rtpmap:34 H263/90000
      Media Attribute Fieldname: rtpmap
      Media Format: 34
      MIME Type: H263
      Sample Rate: 90000
  ⊞ Media Attribute (a): rtpmap:96 H263-1998/90000
  ⊞ Media Attribute (a): rtpmap:32 MPV/90000
  ⊞ Media Attribute (a): rtpmap:97 MP4V-ES/90000
```

Obrázek 2.18 – SDP popisující video relaci

Při přenosu zvuku během relace nebyl zaznamenán žádný problém ani zkreslení. Přenos videa byl plynulý a na straně uživatele 1000 bez viditelného zkreslení příchozího i odchozího toku, viz Obr. 2.19. U desktopového klienta došlo k viditelnému zkreslení barev u obou směrů videa (viz. Obr 2.20). Analýzou obrazu bylo zjištěno, že byla zkreslena složka barevného tónu (Hue). I když se přesnou příčinu nepodařilo dohledat, spočívá pravděpodobně v kodecích videa desktopového klienta.

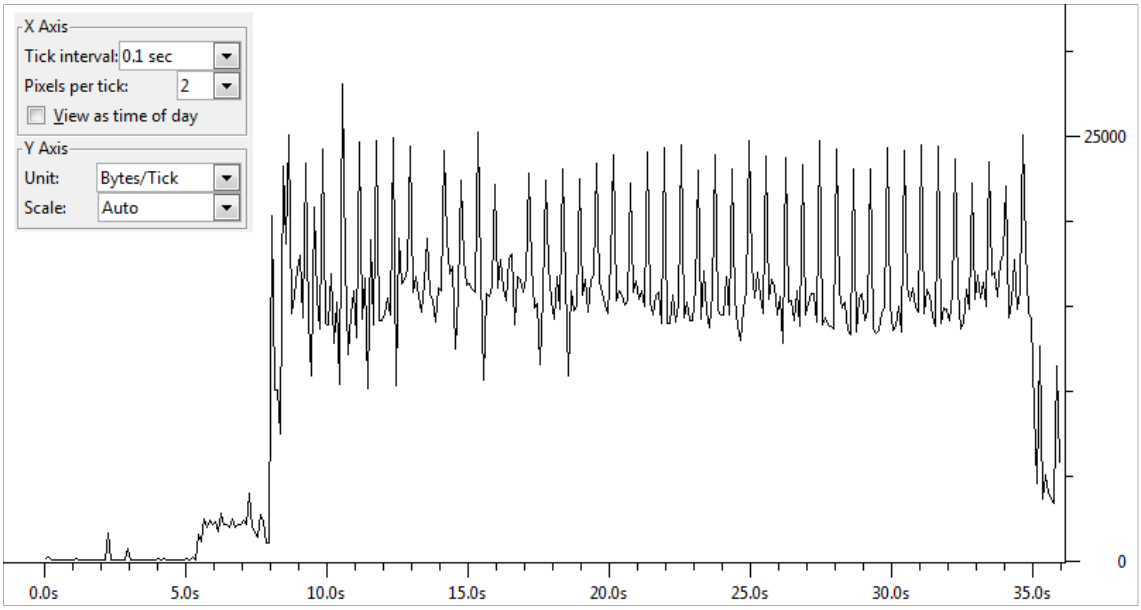


Obrázek 2.19 – Video relace z pohledu videotelefonu



Obrázek 2.20 – Video relace z pohledu desktopového klienta

Pro video hovor byly zpracovány i statistiky přenesených paketů. Graf zachycující průběh datového toku v čase je na Obr. 2.21. Z grafu je patrný rozdíl mezi objemem samotných audio dat (přibližně pátá až osmá sekunda) a objemem dat zahrnujících i video (8-35 s).



Obrázek 2.21 – Graf znázorňující přenos datového toku v čase

Statistiky paketů RTP streamů jsou vyhodnoceny na Obr. 2.22. Důležitými údaji jsou:

- 0% ztrátovost paketů ve všech směrech
- Maximální zpoždění (Delta) nepřesahující 100 ms v žádném směru. V Telekomunikacích jsou tyto hodnoty běžně v řádech stovek ms.
- Poměrně vyrovnané hodnoty maximálního a průměrného rozptylu zpoždění (Jitter). Hodnoty bývají běžně v řádech desítek až stovek ms.

Src IP addr	Src port	Dst IP addr	Dst port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
192.168.110.34	23004	192.168.110.141	11780	0x60D8D8BB	g711U	1523	0 (0,0%)	91,72	10,67	9,43
192.168.110.34	23006	192.168.110.141	11782	0xDFA5051F	h263	1381	0 (0,0%)	98,21	1,34	0,48
192.168.110.141	11780	192.168.110.34	23004	0xB8C4A44D	g711U	1334	0 (0,0%)	34,99	8,44	6,02
192.168.110.141	11782	192.168.110.34	23006	0xB8C4A457	h263	2151	0 (0,0%)	59,99	3,29	3,13

Obrázek 2.22 – Statistiky uskutečněných RTP streamů během video hovoru

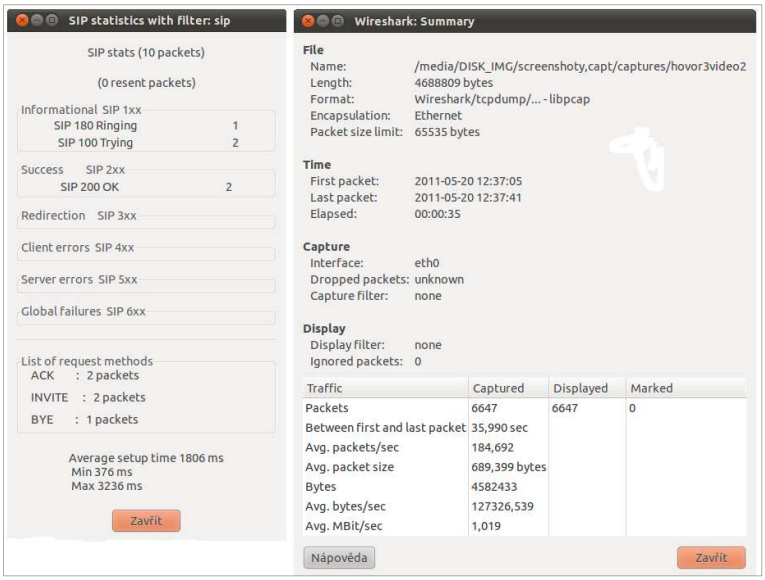
Srovnání klíčových parametrů uskutěčněného audio a audio/video přenosu je na Obr. 2.23

Typ relace	UE	Max. Jitter [ms]	Průměrný Jitter [ms]	Max. Zpoždění [ms]	Packet loss [%]
Audio	myMonster	9,29	6,21	108,22	0
	Yealink VP-2009	10,49	5,99	32,71	0
Audio a video	myMonster	10,67	9,43	91,72	0
	Yealink VP-2009	8,44	6,02	34,99	0
	myMonster	1,34	0,48	98,21	0
	Yealink VP-2009	3,29	3,13	59,99	0

Obrázek 2.23 – Porovnání hodnot RTP streamů naměřených u audio a audio/video relace

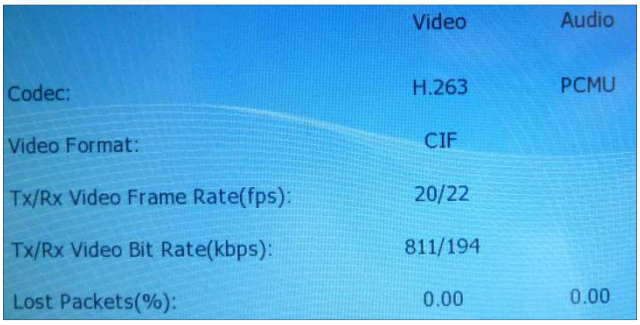
Na Obr. 2.24 jsou uvedeny statistiky SIP signalizace a celkové shrnutí relace, podstatnými údaji jsou:

- 0 opakovaně poslaných paketů značí neztrátovost
- 0 chyb klienta (*Client-error*, třída hlášení 4xx), 0 chyb serveru (*Server-error*, třída hlášení 5xx), 0 globálních chyb (*Global failure*, třída hlášení 6xx)
- Průměrný čas odezvy (*setup time*) 1806 ms.
- Průměrně bylo přeneseno 184,7 paket/s
- Průměrná rychlost přenosu 1,019 Mbit/s



Obrázek 2.24 – Statistiky přenosu SIP signalizace a celkové shrnutí relace

Základní statistiky relace bylo možné sledovat v reálném čase při audio/video hovoru i na IP telefonu, viz. Obr. 2.25. Toto shrnutí odpovídá údajům zachyceným přes aplikaci Wireshark.



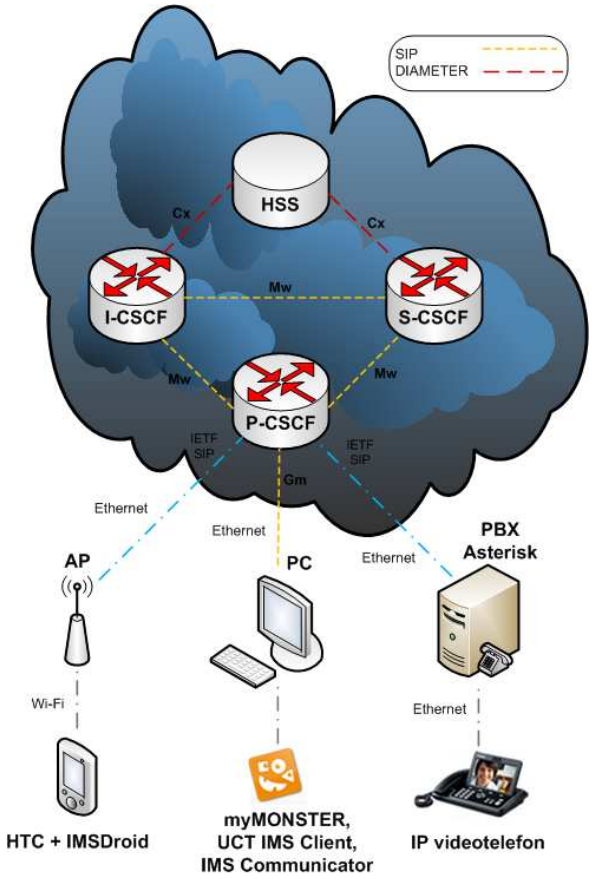
Obrázek 2.25 – Media statistics na videotelefonu

2.6 Shrnutí

V druhé kapitole této práce, zaměřené testování IMS a zprovoznění všech potřebných elementů, se podařilo dosáhnout vzájemné konvergence IMS sítě, reprezentované Open IMS Core, s pobočkovou ústřednou Asterisk. Jejich propojení proběhlo pomocí počítačové síťe v Laboratoři spojovacích systémů, koncových zařízení a konvergovaných síťových technologií. V námi vytvořené topologii lze uskutečnit komunikaci prostřednictvím IMS sítě pomocí:

- Zařízení podporujících chod aplikace IMSDroid (smart telefony) připojené k laboratorní síti přes Wi-Fi přístupový bod
- IMS desktopových klientů jako je myMONSTER, UCT IMS Client nebo IMS Communicator
- IP telefonů zaregistrovaných pomocí PBX Asterisk

Pro názornou ukázku vytvořené topologie viz. Obr. 2.26.



Obrázek 2.26 – Topologie IMS sítě a přidružených prvků

Závěr

Telekomunikační trendy v dnešní době postupně směřují k *all-IP* přenosu dat nebo-li k pojetí popsaném konceptem *Next Generation Network*. Ačkoliv je postupná transformace přístupových sítí i samotného jádra telekomunikační sítě technicky i finančně nákladný proces, většina poskytovatelů k tomuto trendu již přistoupila nebo to v následujících letech plánuje. V České Republice je možné využívat kompletní služby IMS u poskytovatele O2. Operátor T-Mobile momentálně nenabízí stejně široké spektrum služeb jako O2, přesto je v plošném zpřístupňování IMS technologie dál, než operátoři Vodafone (umožňuje zavedení implementace IMS jen firemním zákazníkům) nebo U:fon (IMS služby momentálně nepodporuje).

Pro porozumnění technologii IMS byl v počátečních kapitolách práce popsán vrstový model IMS a jeho jednotlivé vrstvy. Následovalo prostudování IMS z hlediska hlavních entit, propojení Referenčních bodů a funkce protokolů používaných v rámci IMS.

Praktická část byla zaměřena nejprve na seznámení se projektem Open IMS Core, který byl zvolen pro testování IMS technologie, jeho zprovoznění a některá jeho nastavení nutná pro testování a propojení s PBX Asterisk. Po seznámení se s desktopovými IMS klienty byla uskutečněna instant messaging komunikace v rámci IMS sítě. Následnou analýzou zachycené komunikace pomocí aplikace Wireshark byl popsán způsob předávání zpráv SIP protokolu uvnitř IMS.

Po stručném úvodu do PBX Asterisk, rozebrání předpokladů k propojení s IMS a potřebných nastavení se přistoupilo k samotnému otestování komunikace. Nejprve byl uskutečněn přenos hlasu mezi desktopovým IMS klientem a IP telefonem registrovaným k PBX Asterisk. Průběh komunikace byl zachycen a následně analyzován ve smyslu sestavení, průběhu a ukončení relace. Po úspěšné realizaci audio hovoru byl navázán video hovor, který byl podrobně rozebrán včetně statistik řídících signálů a přenesených paketů.

Výstupem této práce bylo sestavení a zprovoznění topologie IMS sítě skládající se z prvků HSS, S/I/P/E-CSCF, její začlenění do počítačové sítě

v laboratoři PA-427 a následné otestování. Ke komunikaci v rámci IMS sítě lze použít smart phone s nainstalovaným IMS klientem, PC s desktopovými IMS klienty nebo IP telefon registrovaný u pobočkové ústředny Asterisk.

V příloze C a D je návrh dvou laboratorních úloh, které byly vypracovány za účelem seznámení studentů s IMS technologií, Open IMS Core a možnostmi komunikace v rámci IMS sítě.

LITERATURA

[1] CHEN, Rebecca LJ, SU, Elisa CY, SHEN, Victor SC, WANG, Yi-Hong. *The Introduction to IP Multimedia Subsystem (IMS)* [online]. 2006. [cit. 2006-09-12]. Dostupné na WWW: <http://www.ibm.com/developerworks/webservices/library/ws-soa-ipmultisub1/>.

[2] POIKSELKA, Miikka, MAYER, Gregor, KHARTABIL, Hisham. *The IMS: IP Multimedia Concepts and Services.* England: WILEY, 2009. 560 s. Third edition. ISBN 0-470-721960.

[3] Hill2Dot. *The IP Multimedia Subsystem* [online] 2008. [cit. 2008-10-21]. Dostupné na WWW: <http://www.hill2dot0.com/wiki/index.php?title=IP_Multimedia_Subsystem>.

[4] AHSON, Syed A.; ILYAS, Mohammad . *IP multimedia subsystem (IMS) handbook*. 1. [s.l.] : [s.n.], 2008. 543 s. ISBN 978-1-4200-6459-9 .

[5] RUSSELL, Travis. *The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations*. V. Británia: Mc Graw-Hill OSBOURNE, 2008. 242 s. ISBN 0071488537.

[6] CAMARILLO, Gonzalo; GARCÍA-MARTÍN, Miguel A. *The 3G IP Multimedia Subsystem (IMS) : Merging the Internet and the Cellular Worlds*. 1. [s.l.] : [s.n.], 2004. 381 s. ISBN 0470871563.

[7] CHAKRABORTY, Shyam ; PEISA, Janne ; FRANKKILA, Tomas ; SYNNERGREN, Per . *IMS Multimedia Telephony over Cellular Systems : VoIP Evolution in a Converged Telecommunication World*. Great Britain : Wiley, 2007. 339 s. ISBN 978-0-470-05855-8(HB).

[8] A. AHSON, Syed ; ILYAS, Mohammad. *VoIP Handbook : Applications, Technologies, Reliability, and Security*. [s.l.] : [s.n.], 2009. 454 s. ISBN 978-1-4200-7020-0.

[9] *RFC 3261 - SIP: Session Initiation Protocol* [online]. 2002 [cit. 2010-12-06]. Dostupný z WWW: <http://tools.ietf.org/html/rfc3261>.

[10] RFC 4566 - SDP: Session Description Protocol [online]. 2006 [cit. 2010-12-06]. Dostupný z WWW: <http://tools.ietf.org/html/rfc4566>.

[11] *RFC 3550 - RTP: A Transport Protocol for Real-Time Applications* [online]. 2003 [cit. 2010-12-06]. Dostupný z WWW: <http://tools.ietf.org/html/rfc3550>.

[12] *RFC 3588 - Diameter Base Protocol* [online]. 2003 [cit. 2010-12-06]. Dostupný z WWW: <http://tools.ietf.org/html/rfc3588>.

[13] *RFC 2748 - The COPS (Common Open Policy Service) Protocol* [online]. 2000 [cit. 2010-12-06]. Dostupný z WWW: <http://tools.ietf.org/html/rfc 2748>.

[14] *RFC 3525 - The Gateway Control Protocol Version 1* [online]. 2003 [cit. 2010-12-06]. Dostupný z WWW: <http://tools.ietf.org/html/rfc 3525>.

[15] *OPEN SOURCE IMS CORE* [online]. 2004 , Modified: Tue, Dec 9, 2008 9:57:52 AM [cit.2010-12-10]. Dostupný z WWW: <http://www.openimscore.org/>.

[16] *OPEN SOURCE IMS CORE* [online]. 2008 [cit. 2011-05-17]. OpenIMSCore Installation Guide. Dostupné z WWW: <http://www.openimscore.org/installation_guide>.

[17] *OPEN SOURCE IMS CORE* [online]. 2008 [cit. 2011-05-19]. Installation Guide of the Emergency Services Branch of the Open IMS Core. Dostupné z WWW: <http://www.openimscore.org/emergency_installation_guide>.

[18] *UCT IMS Client* [online]. 18 Dec 2006, 1 June 2009 [cit. 2011-05-18]. UCT IMS Client. Dostupné z WWW: <http://uctimsclient.berlios.de/>.

[19] *MyMONSTER - Telco Communicator Suite* [online]. 2009, 17/02/2009 [cit. 2011-05-18]. MyMONSTER - Telco Communicator Suite. Dostupné z WWW: <http://www.monster-the-client.org/>.

[20] *IMS Communicator* [online]. 23 Jan 2007 [cit. 2011-05-18]. IMS Communicator. Dostupné z WWW: <http://imscommunicator.berlios.de/>.

[21] MEGGELEN, Jim Van; MADSEN, Leif; SMITH, Jared. *Asterisk: The Future of Telephony*. 2. 1005 Gravenstein Highway North, Sebastopol, CA 95472 : O'Reilly Media, 2007. 574 s. ISBN 0-596-51048-9.

[22] MACDONALD, Alton; CARTAS, Rodolfo; INCERA, José . Asterisk as a Public Switched Telephone Network Gateway for an IMS Test Bed : 2010 17th International Conference on Telecommunications. In . *Data Communication and Networks Papers*. Instituto Tecnológico Autónomo de Mexico : IEEE, 2010. s. 594-599. ISBN 9781424452460.

[23] CAMARILLO, G.; KYZIVAT, P. *Request for Comments* [online]. March 2005 [cit. 2011-05-19]. Update to the Session Initiation Protocol (SIP) - Preconditions Framework. Dostupné z WWW: <http://www.ietf.org/rfc/rfc4032.txt>.

[24] AL-BEGAIN, Khalid , et al. *IMS: A Development and Deployment Perspective*. Great Britain : Wiley, 2009. 316 s. ISBN 978-0-470-74034-7.

[25] *RFC 3581* - An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing [online]. 2003 [cit. 2010-12-06]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc3581.txt >.

SEZNAM ZKRATEK

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ACF	Authentication Control Function
AP	Access point
AS	Application Server
AUC	Authentication Center
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
CAMEL	Customized Applications for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CCF	Charging Collection Function
CDMA	Code-Division Multiple Access
CIF	Common Intermediate Format
CS	Circuit Switched
CSE	Camel Service Enviroment
CSCF	Call Session Control Function
COPS	Common Open Policy Service
DSL	Digital Subscribe Line
DNS	Domain Name System
E-CSCF	Emergency CSCF
FHoSS	The FOKUS Home Subscriber Server
GGSN	Gateway GPRS Support Node
GLM	Group List Management
GPL	General Public License
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HLR	Home Location Register
HSS	Home Subscribe Server
HTTP	Hypertext Transfer Protocol
IETF	Internet Engeneering Task Force
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	Internet Protocol Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
ISUP	ISDN User Part
ITU	International Telecommunication Union
LRF	Location Retrieval Function
MAP	Mobile Application Part
MSRP	Message Session Relay Protocol
MTP	Message Transfer Part
NAT	Network Adress Translation
OIC	Open IMS Core

OS	Operační systém
OCS	Online Charging System
OSA	Open Service Architecture
PBX	Private Branch Exchange
PCM	Pulse-Code Modulation
PDA	Personal Digital Assistant
PS	Presence Server
PS	Packet Switched
PSI	Public Service Identity
PSTN	The Public Switched Telephone Network
QCIF	Quarter CIF
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SBLP	Service-Based Local Policy
S-CSCF	Serving Call Session Control
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SS7	Signalling System no.7
TCP	Transmission Control Protocol
UAS	User Agent Server
VoIP	Voice over Internet Protocol
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
URI	Uniform Resource Identifier
WCDMA	Wideband Code Division Multiple Access
WiFi	Wireless local area networks technology
WLAN	Wireless Local Area Network

SEZNAM OBRÁZKŮ

Obrázek 1.1 – Diagram IMS architektury [1] 2
Obrázek 1.2 – IMS architektura z hlediska prvků a referenčních bodů [2], [3] ... 5
Obrázek 1.3 – Propojení P/S/I-CSCF, HSS a AS [5]..... 7
Obrázek 1.4 – Struktura HSS [2]..... 9
Obrázek 1.5 – Diagram vazeb mezi Aplikačními servery [2] 11
Obrázek 1.6 – Diagram propojení IMS a CS sítě [6] 13
Obrázek 1.7 – Struktura Offline a Online zpoplatnění [8] 14
Obrázek 2.1 – Struktura prostředí Open IMS Core [15] 23
Obrázek 2.2 – Ukázka webového rozhraní a uživatelských účtů 25
Obrázek 2.3 – Ukázka IM komunikace mezi klienty UCT IMS Client a myMonster 28
Obrázek 2.4 – Ukázka zachycení zprávy přes Wireshark 28
Obrázek 2.5 – Ukázka SIP hlavičky 29
Obrázek 2.6 – Flow diagram zaslání zprávy v Pager módu 29
Obrázek 2.7 – Zaslání zprávy při Session Based IM [6]..... 30
Obrázek 2.8 – Proces registrace..... 31
Obrázek 2.9 – Pole WWW-Authenticate 31
Obrázek 2.10 – Pole Authorization..... 31
Obrázek 2.11 – Ukázka výpisu klientů UCT IMS Client a myMONSTER..... 32
Obrázek 2.12 – Nastavení uživatelského účtu přes webové rozhraní a videotelefon..... 35
Obrázek 2.13 – Flow diagram mezi síťovým rozhraním eth0 a IP telefonem ... 35
Obrázek 2.14 - Úplný flow diagram audio relace..... 36
Obrázek 2.15 – SDP s popisem audio relace 37
Obrázek 2.16 – Statistiky RTP 37
Obrázek 2.17 – Flow diagram video hovoru..... 38
Obrázek 2.19 – Video relace z pohledu videotelefonu 39
Obrázek 2.18 – SDP popisující video relaci 39
Obrázek 2.20 – Video relace z pohledu desktopového klienta..... 40
Obrázek 2.21 – Graf znázorňující přenos datového toku v čase..... 40
Obrázek 2.22 – Statistiky uskutečněných RTP streamů během video hovoru . 41
Obrázek 2.23 – Porovnání hodnot RTP streamů naměřených u audio a audio/video relace 41
Obrázek 2.24 – Statistiky přenosu SIP signalizace a celkové shrnutí relace ... 42
Obrázek 2.25 – Media statistics na videotelefonu 42
Obrázek 2.26 – Topologie IMS sítě a přidružených prvků..... 43