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

SÍŤOVÉ SLUŽBY V IMS

NETWORK SERVICES IN IMS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE MATĚJ MIKULEC
AUTHOR

VEDOUCÍ PRÁCE Ing. ĽUBOŠ NAGY
SUPERVISOR

BRNO 2010

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Matěj Mikulec	***ID:***	106644
Ročník:	3	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Sítové služby v IMS

POKYNY PRO VYPRACOVÁNÍ:

Cílem projektu je prostudovat a popsat architekturu IMS (IP Multimedia Subsystem) se zaměřením na podrobný popis sítových služeb (základních entit, signalizace, atd.). Na základě získaných poznatků realizujte aplikaci pro poskytování sítové služby uživatelům registrovaných v systému IMS pomocí SDS Ericsson. Následně proveďte podrobnou analýzu SIP komunikace v realizovaném projektu.

DOPORUČENÁ LITERATURA:

[1] RUSSELL, Travis. The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations. V. Británie: Mc Graw-Hill OSBOURNE, 2008. 242 s. ISBN 0071488537.
[2] POIKSELKA, Miikka, MAYER, Gregor, KHARTABIL, Hisham, NIEMI, Aki. The IMS: IP Multimedia Concepts and Services. V. Británie: WILEY, 2006. 466 s. Second edition. ISBN 978-0-470-01906-1.

Termín zadání:	29.1.2010	***Termín odevzdání:***	2.6.2010

Vedoucí práce: Ing. Ľuboš Nagy

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

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské 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 práce je zaměřena na služby, které lze provozovat v architektuře IP Multimedia Subsytem. V první kapitole jsou popsány hlavní entity v architektuře IMS. Druhá kapitola je zaměřena na služby - Presenční služba, Posílání zpráv v reálném čase, Push to Talk over Celluar a IPTV. U každé služby je popsána architektura a základní signalizace. Ve třetí kapitole jsou popsány jednotlivé protokoly využívané v IMS, podrobněji je popsán protokol SIP. Čtvrtá kapitola obsahuje popis prostředí aplikace SDS Ericsson v němž byla prováděna praktická část. Pátá a poslední kapitola se zabývá službou IPTV v SDS a komunikací SIP s IMS jádrem. Jsou analyzovány přenosy zpráv v jednotlivých případech komunikace klienta s IMS jádrem pomocí integrované možnosti sledovaní zpráv procházejících přes CSCF, HSS a DNS v programu SDS. Důležité poznatky jsou shrnuty v závěru.

Klíčová slova

Technologie IMS, služby, SDS Ericsson, protokol SIP, IPTV

Abstract

This thesis is focused on services that can be used in the architecture IP Multimedia Subsytem. The first chapter describes the main entities in the IMS architecture. The second chapter is focused on services - Presence, Instant Messaging, Push to Talk over Cellular and IPTV. For each service is described architecture and basic signaling. The third chapter describes the various protocols used in IMS, protocol SIP is described in more details. The fourth chapter contains a description of the application environment SDS Ericsson in which was implemented practical part. The fifth and final chapter deals with the IPTV service in SDS and SIP communications with IMS core. Traffic reports are analyzed in each case the client communication with IMS core with integrated tracking of messages passing through the CSCF, HSS and DNS in program SDS. Important findings of the work are summarized in the conclusion.

Keywords

IMS technology, services, SDS Ericsson, SIP protocol, IPTV

Bibliografická citace mé práce

MIKULEC, M. Sítové služby v IMS. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 63 s. Vedoucí bakalářské práce Ing. Ľuboš Nagy.

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma „Síťové služby v IMS“ jsem vypracoval samostatně pod vedením vedoucího bakalářské 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 bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této 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 práce Ing. Ľubošovi Nagyovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování bakalářské práce.

V Brně dne …….. ..……

podpis autora

Seznam zkratek

3G	Third Generation
AAA	Authentification Authorization and Accounting
AS	Appliction Server
BGCF	Breakout Gateway Control Function
CS	Circuit Switched
CS CN	Circuit Switched Core Network
CSCF	Call Session Function Control
DNS	Domain Name Server
ECF	Elementary Control Function
EDGE	Enhanced Data Rate for Global Evolution
EFF	Elementary Forwarding Function
EPG	Electronic Program Guide
ETSI	European Telecommunications Standards Institute
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IAP	IPTV Application Platform
ICP	IMS Client Platform
IETF	Internet Engineering Task Force
iFC	Initial Filter Criteria
IJCU	IMS JME Client Utility
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
IPTV	Internet Protocol TV
IRC	Internet Relay Chat
MEGACO	Media Gateway Control Protocol
MGCF	Media Gateway Control Function
MGW	Media Gateway Function
MHP	Multimedia Home Platform
MPEG	Motion Picture Expert Group
MRF	Media Resource Function
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MSCF	Multimedia Service Control Function
MSRP	Message Session Relay Protocol
NASS	Network Attachment Subsystem
OCS	Online Charging System
OMA	Open Mobile Alliance
PA	Presence Agent
PDF	Policy Decision Function
PES	Packet Elementary Stream
PGM	Presence and Group list Management
PoC	Push to talk Over Cellular
PQoS	Perceived Quality of Service

PS	Packet Switched; Presence Server
PSTN	Public Switched Telephone Network
PUA	Presence User Agent
QoS	Quality of Service
RACS	Resource Admission and Control Subsystem
RAN	Radio Access Network
RSL	Resource list
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SCF	Session Control Function
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SEE	Service Execution Environment
SEG	Security Gateway
SGW	Signalling Gateway
SIP	Session Initiation Protocol
SMG	Special Mobile Group
SMS	Short Messaging Service
SMTP	Simple Mail Transfer Protocol
SS7	Signaling System No.7
TCP	Transmission Control Protocol
TD-CDMA	Time Division Code Division Multiple Access
TISPAN	Telecom and Internet converged Services and Protocols for Advanced Network
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UIQ	User Interface Quartz
URI	Uniform Resource Identfier
UTRAN	Universal Mobile Telecommunications System Terrestrial Radio Access Network
VCC	Voice Call Continuity
VHE	Virtual Home Environment
VLR	Visitors Location Register
VoD	Video on Demand
VOIP	Voice Over IP
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XDMS	XML Document Management Sever
XML	Extensible Markup Language

Obsah

Úvod **13**

1 Architektura IMS **14**

1.1 IMS entity **15**

1.1.1 Prvky CSCF (Call Session Control Function) 15

1.1.2 Databáze 16

1.1.3 Služební funkce 17

1.1.4 Mezisíťové služby 17

2 Síťové služby **19**

2.1 Presenční služby (Presence) **19**

2.1.1 Entity v Presenční službě 19

2.1.2 Signalizace 20

2.2 Posílání zpráv v reálném čase (Instant Messaging) **23**

2.2.1 Architektura posílání zpráv 23

2.3 Služba PoC (Push to talk Over Cellular) **26**

2.4 IPTV **28**

3 Protokoly **32**

3.1 SIP (Session Initiation Protocol) **32**

3.1.1 SIP zařízení a servery 32

3.1.2 Formát zprávy 33

3.1.3 Hlavičky (header files) 34

3.2 SDP (Session Description Protocol) **35**

3.3 DIAMETER **35**

3.4 MEGACO (MEdia GAteway COntrol protocol) **35**

3.5 XCAP (eXtensible Markup Language Configuration Access Protocol) **36**

3.6 RTP (Real-time Transport Protocol) **36**

4 Prostředí SDS (Service Development Studio) **37**

4.1 Popis prostředí **37**

4.1.1 SDS komponenty: 38

4.1.2 Pracovní prostředí 39

5 IPTV v prostředí SDS Ericsson **40**

5.1 CSCF **40**

5.2 DNS **41**

5.3 HSS **41**

5.4 Sailfin **42**
5.5 XML konfigurační soubory **42**
5.6 Prostředí IPTV klienta v SDS **42**
5.7 SIP komunikace **44**
5.7.1 Přihlášení uživatele k serveru a ke sledování programu 44
5.7.2 Přepnutí programu 49
5.7.3 Video na vyžádání 50
5.7.4 Odhlášení uživatele od serveru IPTV 52
5.7.5 Vypršení času přihlášení (expires time) 54
5.7.6 Chyba pokud uživatel není v seznamu HSS 55
5.7.7 Chyba při přihlašování (ověřování) uživatele 55
5.8 Zachycení multicastového přenosu pomocí Wireshark **56**
Závěr **59**
Literatura **61**
Seznam příloh **63**
Příloha A: Obsah CD **63**

Seznam obrázků

Obr. 1: Konvergence služeb v IMS [14] ... 14
Obr. 2: Propojení HSS z CSCF [4] ... 16
Obr. 3: Zobrazení architektury Presenční služby [3] ... 20
Obr. 4: Úspěšná registrace statusu [2] ... 21
Obr. 5: Zveřejnění statusu [2] ... 21
Obr. 6: Zapsání do zdrojového seznamu [2] ... 22
Obr. 7: Zapsání informace pro watcher [2] ... 22
Obr. 8: Interakce presentity a watcher [2] ... 22
Obr. 9: Přenos zpráv v pager módu [4] ... 23
Obr. 10: Spojení MSRP začátek – konec [4] ... 25
Obr. 11: Spojení více účastníků (Chat server) [4] ... 26
Obr. 12: Služba PoC [2] ... 27
Obr. 13: PoC architektura [2] ... 27
Obr. 14: Architektura PoC serveru [2] ... 28
Obr. 15: Architektura pro IPTV s podporou IMS [6] ... 30
Obr. 16: Inicializace spojení (živé vysílání) [6] ... 31
Obr. 17: Ukončení spojení [12] ... 31
Obr. 18: Ukázka propojení Serverů a UA [2] ... 33
Obr. 19: Propojení prvků IPTV s IMS ... 40
Obr. 20: Prostředí IPTV klienta ... 43
Obr. 21: Registrace k serveru až po spuštění přenosu ... 45
Obr. 22: Zaregistrování uživatele a jeho UA ... 46
Obr. 23: Detail zprávy REGISTER ... 46
Obr. 24: Detail zprávy [3] SUBSCRIBE ... 47
Obr. 25: Detail zprávy NOTIFY ... 48
Obr. 26: Detail SDP v INVITE zprávě ... 49
Obr. 27: Přepnutí programu ... 49
Obr. 28: Detail SIP zprávy [1] INFO ... 49
Obr. 29: Zprávy při službě video na vyžádání ... 50
Obr. 30: Detail první INVITE zprávy ... 51
Obr. 31: Detail zprávy BYE ... 53
Obr. 32: Odhlášení uživatele ... 53

Obr. 33: Detail poslední zprávy 200 OK 53
Obr. 34: Vypršení času přihlášení 54
Obr. 35: Detail odpovědi 481 55
Obr. 36: Uživatel není v HSS 55
Obr. 37: Chyba při ověřování uživatele 56
Obr. 38: Detail odpovědi 401 56
Obr. 39: Zobrazení přenosu v programu Wireshark 57
Obr. 40: IPTV klient při příjmu vysílání 58

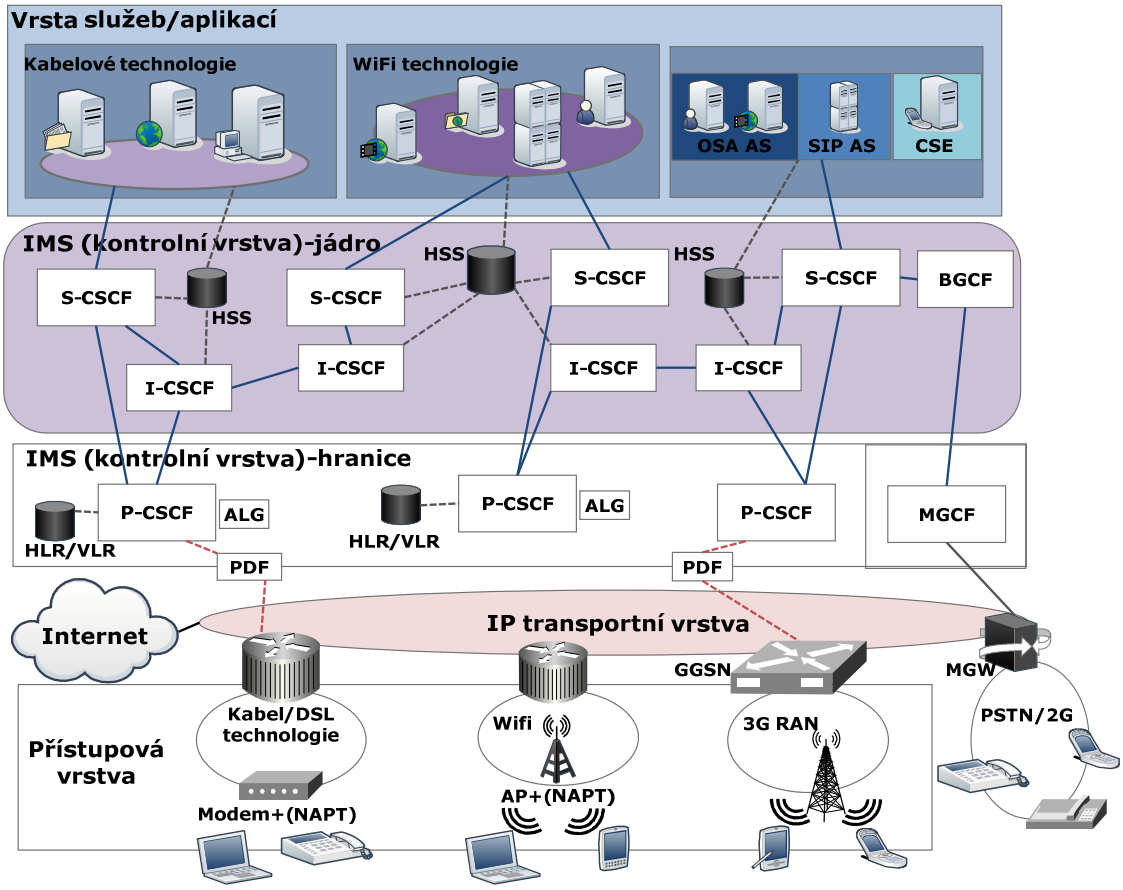
Úvod

Systém IP Multimedia Subsystem vznikal na požadavku dnešních sítí, kde je komunikačním vzorem utváření sítě založené na IP protokolu provozovaném na mobilních zařízeních. IMS je standardem sítí nové generace sloužící k provozování mobilních a fixních zařízení. Architektura IMS je konvergencí služeb dat, hlasu fixních a mobilních sítí, podporuje jak paketově spínané telefonní systémy tak i okruhově spínané a je tedy zajištěna spolupráce s existujícími sítěmi (např. PSTN, ISDN, 3G). IMS je globální a přístupově nezávislé. Podporuje schopnost doručit multimediální obsah (hlas, video, text, obrázky, atd.) a sdílení dat mezi koncovými uživateli za použití běžného internetově založeného protokolu. Je založeno na SIP službách, jež jsou vhodným nástrojem pro zajištění komunikace. Obsahuje nástroje a schopnosti zacházet s mnoha službami standardní cestou. Pod což spadá schopnost systému užívat části jiného systému a práci s nimi, přístup, uplatňování „politiky“ operátorů, kontrola poplatků, zabezpečení a kvalitu služeb. Hlavním zaměřením IMS je sbližování, vytvoření a doručení služeb. Umožnit jedné síti integrovat všechny typy přístupu je obrovskou výhodou IMS. IMS definuje, jak budou požadavky služeb směrovány, které protokoly jsou podporovány, jak se budou účtovat služby a jaká skladba služeb je vůbec povolena.

V první kapitole je seznámení s IMS a jsou popsány jednotlivé prvky architektury, jež je rozdělena do šesti skupin. V druhé kapitole jsou rozebrány služby, které lze provozovat v IMS, nezávisle na tom jak je uživatel připojen (mobilní, bezdrátová nebo pevná síť). V této kapitole jsou uvedeny: presenční služby, posílání zpráv v reálném čase, PoC a IPTV. U služeb je popsána architektura a signalizace. Třetí kapitola je zaměřena na protokoly používané v této architektuře. Hlavním signalizačním protokolem IMS je SIP, ten je podrobněji rozebrán. U ostatních protokolů jsou uvedeny základní vlastnosti. Ve čtvrté kapitole je uveden úvod k používanému pracovnímu prostředí SDS Ericsson, v kterém je prováděna praktická část s IPTV. Umožňuje vytvořit experimentální IMS síť s určitými prvky a také provozovat služby IPTV, Presenční služba, posílání zpráv a PoC. V páté poslední kapitole je popsáno prostředí IPTV a hlavní důraz je kladen na analýzu SIP komunikace v projektu.

1 Architektura IMS

První specifikace této sítě se objevila v roce 1999 a na vývoji se podíleli 3GPP (The 3rd Generation Partnership Project) a ETSI SMG (European Telecommunications Standards Institute Special Mobile Group). Velkou výhodou IMS je možnost uživatele přistupovat z jakékoliv sítě. Podporuje široký rozsah služeb, jež řídí hlavní protokol SIP. Skládá se z několika částí, ve kterých jsou propojeny jednotlivé entity. Architektura se je navržena k horizontálnímu rozdělení služeb (snadnější správa při vývoji nových služeb) a ne jako dříve vertikálním. Jelikož je eliminována závislost na přístupové síti, dochází ke snižování nákladů a zjednodušení systému. Každá služba, kterou bude chtít uživatel využít, bude spojena standardizovaným rozhraním. IMS se stará o zajištění QoS, účtování, bezpečnost, atd. Pracuje se službami, jako jsou např. presenční služba, posílání zpráv v reálném čase. Vše je propojeno IP protokolem, jak pevné tak i mobilní sítě, je to znázorněno na Obr. 1. Poslední verzí IMS je release 7 a vývoj neustále pokračuje.



Obr. 1: Konvergence služeb v IMS [14]

1.1 IMS entity

Jednotlivé prvky mohou být rozděleny do šesti kategorií dle [2].

- Pro zajištění a řízení spojení (CSCF)
- Databáze (HSS)
- Služební funkce (MRFC, MRFP)
- Mezisíťové služby (BGCF, MGCF, …)
- Funkce podpory (PDF, SEG)
- Účtování

1.1.1 Prvky CSCF (Call Session Control Function)

CSCF je základní funkcí síťového jádra IMS. Jeho funkcí je zařídit registraci, založit spojení a udržovat síť v optimálním stavu.

P-CSCF (Proxy Call Session Control Function)

Je to první kontaktní prvek uživatele s IMS. Slouží tedy k autentizaci a kontrole důvěryhodnosti uživatele. Veškerá data prochází přes něj. Jeho úkolem je kontrolovat SIP signalizaci jak do IMS tak opačným směrem. Zaručuje směrování žádostí a odpovědí. Pro zrychlení sestavení spojení obstarává kompresi a dekompresi SIP protokolu mezi uživatelem a P-CSCF, kvůli délce zprávy normálního SIP protokolu, jež je velká pro práci v IMS. Sleduje čas spojení a vytváří data o účtování.

I-CSCF (Interrogating Call Session Control Function)

Zatímco P-CSCF je vstupním bodem do IMS, I-CSCF slouží jako brána do každé určité IMS sítě. Rozhoduje, jestli je nebo není povolen přístup do jiných sítí. Pro tento důvod může být použito ke skrytí detailů o síti pro jiné sítě. Pomáhá chránit S-CSCF a HSS proti nepovolenému přístupu z cizích sítí. Získává jména S-CSCF z HSS za účelem obsluhy uživatele, který spadá do patřičného S-CSCF a to se přiřazuje buď na základě podporovaných služeb nebo geografické polohy. Je možné ho považovat za firewall IMS sítě, zabrání přístupu z jiné sítě do naší. Hraje důležitou roli v bezpečnosti IMS a také provádí směrování mezi dvěma sítěmi.

S-CSCF (Serving Call Session Control Function)

Lze ho nazvat jádrem IMS. Zodpovídá za ovládání registračních procesů, směrování, udržování statusu spojení a za ukládání profilů. S-CSCF stahuje data z HSS (Home

Subscriber Server) a po ověření odešle data uživateli a ten může nyní začít používat služby IMS. Poskytuje data o stavu registrace ostatním aplikacím a přebírá kontrolu nad službami po dobu, co je zařízení registrováno. Taky si stahuje profil služeb (je neustále uložen v HSS) daného zařízení. To může mít například povoleno pouze audio služby. Kontroluje zasílání zpráv a provádí kontrolu obsahu.

E-CSCF (Emergency Call Session Control Function)

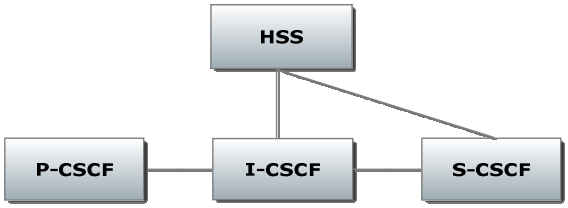
Tato entita je specializovanou funkcí sloužící k vyřizování tísňových volání na policii, hasiče nebo záchrannou službu. Dříve musel být tento požadavek směrován vždy do CS sítě. Hlavním úkolem E-CSCF je vybrat tísňové centrum PSAP (*Public Safety Answering Point*). Kritériem výběru je poloha uživatele, a podle toho se směřuje požadavek. E-CSCF je vždy umístěno ve stejné síti jako P-CSCF.

1.1.2 Databáze

IMS obsahuje dvě základní databáze hlavní databáze HSS a databáze SLF (Subcription Locator Function), která pomáhá lokalizovat data v HSS. Obě dvě používají protokol Diameter.

HSS (Home Subscriber Server)

Obsahuje hlavní databázi, v níž jsou uživatelská data např. uživatelova identita, registrační informace, přístupové parametry ke službám. Uživatelská identita se skládá ze dvou typů: soukromé a veřejné. Při registraci do IMS domény se uživatelský profil stahuje z HSS do CSCF pro zřízení spojení HSS poskytuje informace, na kterém CSCF je uživatel obsluhován (Obr. 2). Při každé změně HSS odesílá data, za účelem jejich stále aktuálnosti. Úkolem registrace je poskytnout uživatelovu pozici (v bezdrátových sítích např. GPS, v pevných např. IP). Obsahuje HLR (Home Location Register) a AAA (Authentification Authorization and Accounting), toto stejné spojení se vyskytuje v mobilních GSM sítích, umožňuje spolupráci s pevnými i bezdrátovými sítěmi. AAA uchovává bezpečnostní klíče pro každého uživatele



Obr. 2: Propojení HSS z CSCF [4]

SLF (Subscription Locator Function)

Může být zabudována do jiné funkce nebo fungovat jako samostatný server. Jeho účelem je v případě více HSS určit to, které obsahuje data konkrétního uživatele. Používá mechanismy, jež dovolují I-CSCF a S-CSCF najít HSS.

1.1.3 Služební funkce

AS (Application server)

Je to víceúčelová funkce v IMS, ale není přímo součástí IMS jádra. Komunikuje protokoly SIP, DIAMETER a je v přímém spojení s CSCF a HSS . Hlavními funkcemi AS je: schopnost vytvořit SIP požadavek a zpracovat příchozí SIP spojení z IMS, poslat informace o účtu do funkce účtování. Používá se jako aplikace, doručovatel služeb a obsahu i jako videokonference. Služby provozované AS jsou identifikovány „služebními identifikátory“ (uložené v HSS).

MRF (Multimedia Resource Function)

Dělí se na dvě další funkce MRFC a MRFP. MRFP řídí různé typy médií pod kontrolou MRFC. Příkladem ovládání médií může být: konferenční komunikace, generace a detekce tónu, fax, atd.

MRFC (Multimedia Resource Function Control)

Řídí tok médií na základě povelů zaslaných AS nebo S-CSCF. Umožňuje vytváření statistiky o mediálních tocích.

MRFP (Multimedia Resource Function Processor)

Procesor řízený MRFC. Dochází zde k zpracování a řízení toku. Může provádět i analýzu médií.

1.1.4 Mezisíťové služby

Jsou potřebné pro výměnu signalizace a médií mezi IMS a CS CN (Circuit Switched Core Network).

PSTN (Public Switched Telephony Network Gateway)

Slouží k propojení IMS s ostatními typy sítí. Obsahuje tyto prvky:

BGCF (Breakout Gateway Control Function)

BGCF vybírá místo, kde dochází k přepojení do CS domény nebo propojení na další BGCF pokud se nachází v jiné síti. Pokud se přístupový bod nachází v domácí síti, předává řízení MGCF.

MGCF (Media Gateway Control Function)

Řídí proud médií, které jsou propojeny mezi dvěma různými sítěmi, typicky paketově a okruhově spínané sítě. Spolupracuje s CSCF.

MGW (Media Gateway)

Je zodpovědná za propojení PSTN a IMS sítí, kontroluje ji MGCF. Podle potřeby také provádí zpracování médií (hlas, video).

SGW (Signaling Gateway)

Provádí obousměrnou konverzi na transportní vrstvě mezi signalizací založenou na IP a signalizací SS7.

PDF (Policy Decision Function)

Získává informace z CSCF a na jejich základě řídí tok dat. Kontroluje autorizaci jednotlivých uživatelů.

Funkce zpoplatnění služeb (Charging)

Je jednou z důležitých funkcí IMS a umožňuje dva způsoby účtování online a offline.

Offline – účtovací proces je založen na účtování až po ukončení spojení. Neprobíhá v reálném čase (během komunikace). Uživatel obdrží vyúčtování služeb po nějaké době. Například od mobilního operátora dostane měsíční vyúčtování.

Online – předplacené služby vyžadují účtování v reálném čase. IMS entity potřebují zjistit, jestli může uživatel využít služeb, které požaduje. K tomu slouží OCS, které má informace o uživatelově účtu.

2 Síťové služby

Dostupnost a rozsah služeb v posledních letech výrazně vzrostl. Díky použití IP protokolu může být nabídka služeb velmi rozsáhlá. Mezi služby patří: Presenční služba (Presence), posílání zpráv v reálném čase (Instant Messaging), Konference (Conferencing), PoC, IPTV a další.

2.1 Presenční služby (Presence)

Slouží k aktuálnímu zobrazení uživatelova statusu ostatním uživatelům a ten zároveň může vidět statusy ostatních. Obsahuje různé informace: jak je uživatel připojen (PC, Mobil,…), co právě dělá, jeho status (Online, Pryč, Zaneprázdněn, atd.) a další položky. Může být používán jako samostatný server (Presenční server) i jako přímé propojení účastníků nebo být zakomponován v dalších službách (např. posílání zpráv v reálném čase). Využívá SIP, který byl rozšířen balíčkem nazvaným „Presence“, k přenosu a kontrole statusů.

2.1.1 Entity v Presenční službě

Presentita – neboli presenční entita, zdroj který poskytuje data presenční službě

Watcher – entita dotazující se na dostupnost nějakého uživatele

SIP entity:

PA (Presence Agent) – umožňuje ukládat přihlášení a generuje oznámení

PUA (Presence User Agent) – pracuje s presenčními informacemi a zveřejňuje je. Získává informace např. z HLR v CS doménách.

Architektura Presenční služby

Presenční informace mohou být získány buď PUA v cizí síti, PUA v terminálu a PUA jako samostatné jednotky v síti. Architektura je naznačena na Obr. 3.

PUA (Presence User Agent) – shromažďuje a poskytuje presenční informace serveru

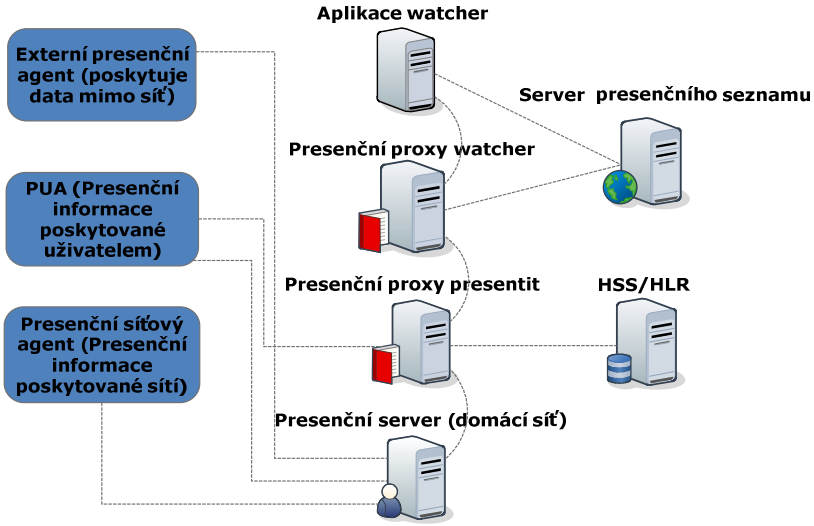
Presenční server – řídí presenční informace posílané PUA a řeší podepisovací požadavek

Presenční proxy watcher – identifikuje, kde se nachází uživatel. Může se vyskytovat buď v domácí nebo cizí síti.

Presenční proxy presentit – je v něm uloženo spojení určitého presenčního serveru s určitým uživatelem.

Seznam Presentit

Poté co se uživatel přihlásí do sítě, může chtít zjišťovat stavy ostatních přátel. Není limitovaný počtem kontrolovaných stavů přátel. Avšak kvůli ochraně proti zahlcení a překročení šířky pásma nedochází k tomu, že uživatel zjišťuje statusy svých přátel „po jednom“. K tomu slouží zdrojový seznam (*Resource List*), kde jsou uloženy všechny statusy. Při práci s tímto seznamem se využívá protokol XCAP.



Obr. 3: Zobrazení architektury Presenční služby [3]

2.1.2 Signalizace

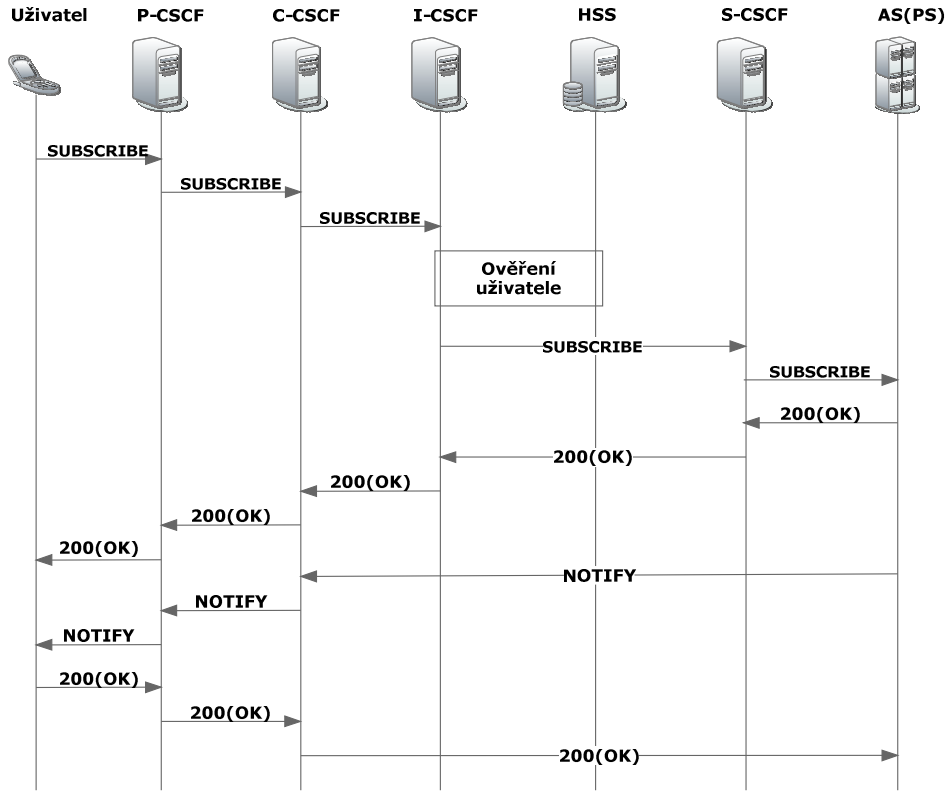
Příklady signalizace v Presenční službě:

Registrace statusu

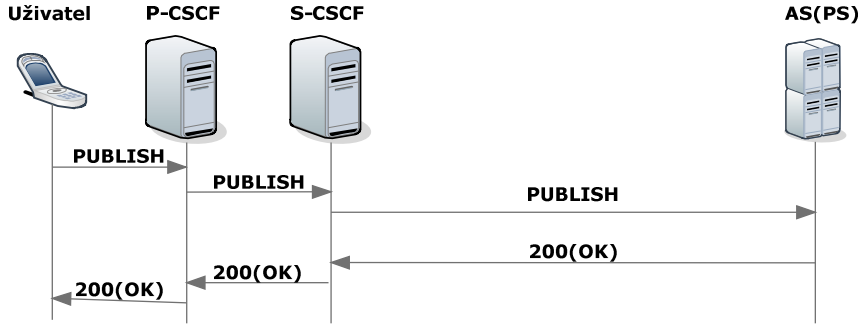
Na Obr. 4 je zobrazeno úspěšné získání statusu entitou watcher, která se nachází v jiné síti než presentita. Signalizace zobrazuje stav od počátečního požadavku NOTIFY až po SUBSCRIBE požadavek.

Zveřejnění statusu

Na Obr. 5 je znázorněn příklad úspěšného zveřejnění statusu. V tomto případě se UE stává PUA. Je to typický případ pro PS domény, kde se generují oznámení pro watchery.



Obr. 4: Úspěšná registrace statusu [2]

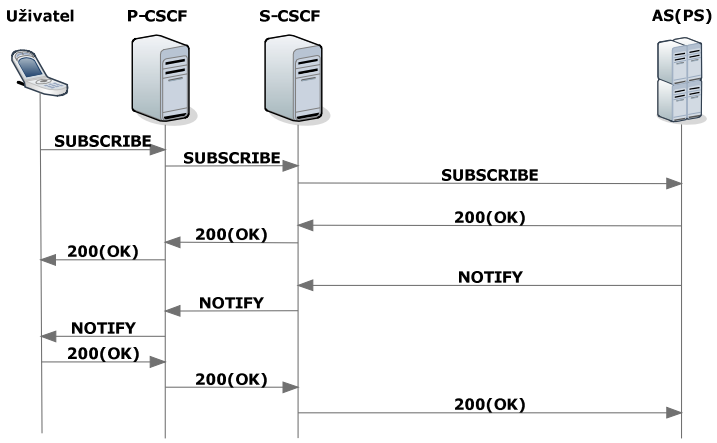


Obr. 5: Zveřejnění statusu [2]

Zapsání do zdrojového seznamu

Na následujícím obrázku (Obr. 6) je zobrazen příklad, kdy uživatel zapíše svůj status do zdrojového seznamu, který byl vytvořen dříve. Seznam zdrojů (presentit) využívá SIP URI adresy. Požadavek NOTIFY je odeslán po obdržení SUBSCRIBE požadavku.

Pokud RLS nemá žádné informace o zdrojích v seznamu, NOTIFY může mít prázdný obsah.

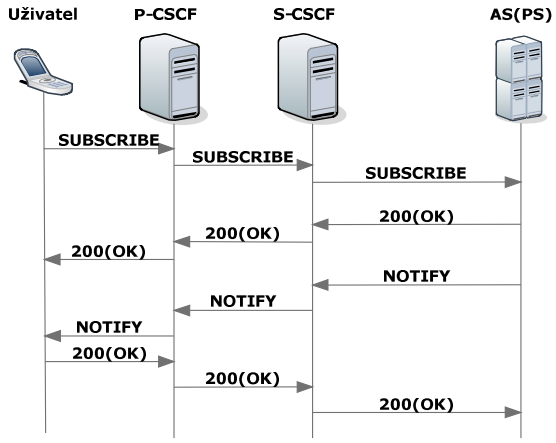


Obr. 6: Zapsání do zdrojového seznamu [2]

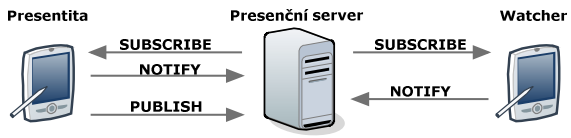
Zapsání informace pro watcher

Na Obr. 7 je zobrazen komunikace mezi PUA a PS doménou. Uživatel se zapíše k příjmu upozornění, pokud dojde ke změně statusu watcher. Cesta zpráv je stejná jako při požadavku PUBLISH. Po upozornění okamžitě následuje úspěšné přijetí požadavku.

Na Obr. 8 je zobrazena interakce mezi presentitou a watcherem přes Presenční server.



Obr. 7: Zapsání informace pro watcher [2]



Obr. 8: Interakce presentity a watcher [2]

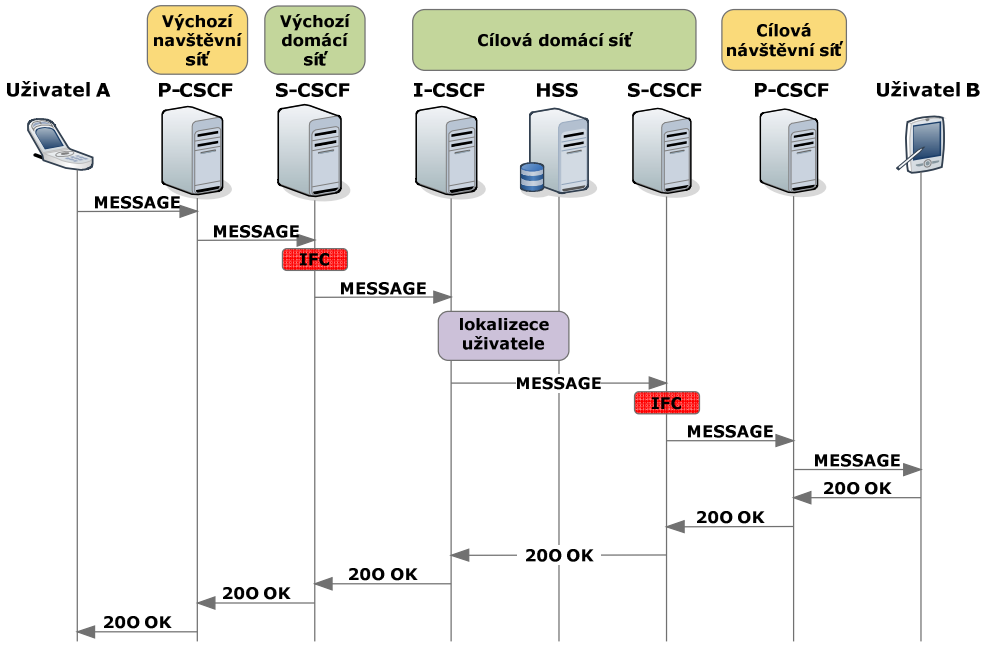
2.2 Posílání zpráv v reálném čase (Instant Messaging)

Dnes je komunikace pomocí posílání zpráv velmi oblíbená, ať už jsou to SMS nebo PC programy (ICQ, Jabber). Zprávy nemusí obsahovat pouze text, ale také např. video, audio a být doručena různými cestami. Posílání zpráv se dělí na dva druhy, každý má jinou charakteristiku. Pager mód má charakteristiku SMS v mobilních sítích. Chatovací mód se dá přirovnat k používání IRC, kdy se uživatel připojí do určité místnosti, která již byla vytvořena a zde může komunikovat s ostatními účastníky místnosti.

2.2.1 Architektura posílání zpráv

Pager mód (Immediate mode)

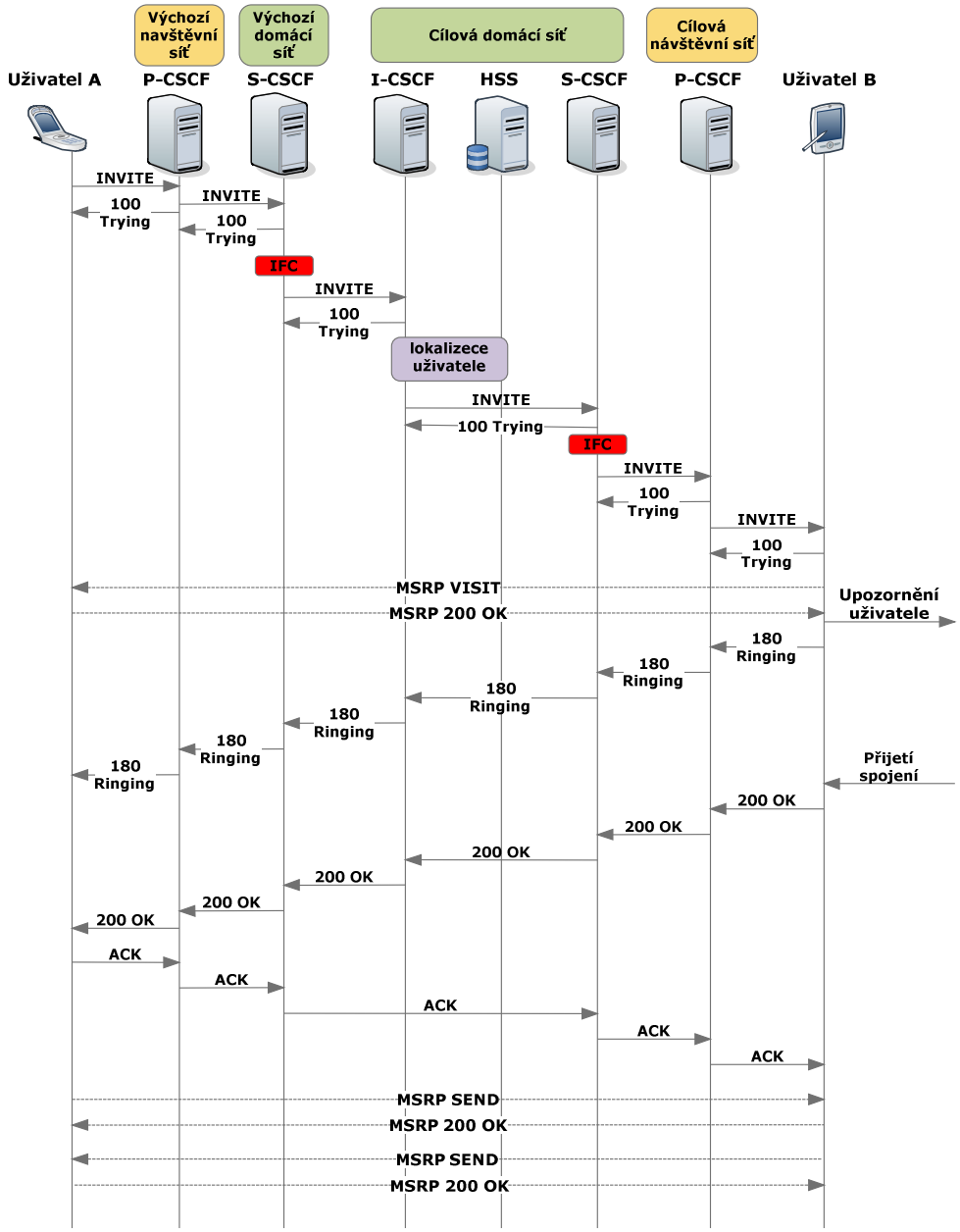
Je dobře známé posílání zpráv v reálném čase zapracované do IMS systému. Používá SIP metodu MESSAGE k posílání zpráv mezi uživateli. V pager módu každý uživatel generuje požadavek MESSAGE, který je vložen do požadovaného obsahu, jež je obvykle text, ale mohou to být multimédia - obrázek, zvuk, video. Vyhledání příjemce probíhá pomocí požadavku na URI. Požadavek je potom směrován přes IMS stejně jako INVITE do doby, než se najde cesta k příjemci. Není zde žádný spojový protokol. Každá zpráva je nezávislou transakcí a není spojena s předchozím požadavkem. Pokud je uživatel nepřihlášen, je zpráva poslána AS a ten jej uloží. Pokud se příjemce přihlásí do sítě, je mu zpráva doručena. Signalizace přenosu zpráv je na Obr. 9.



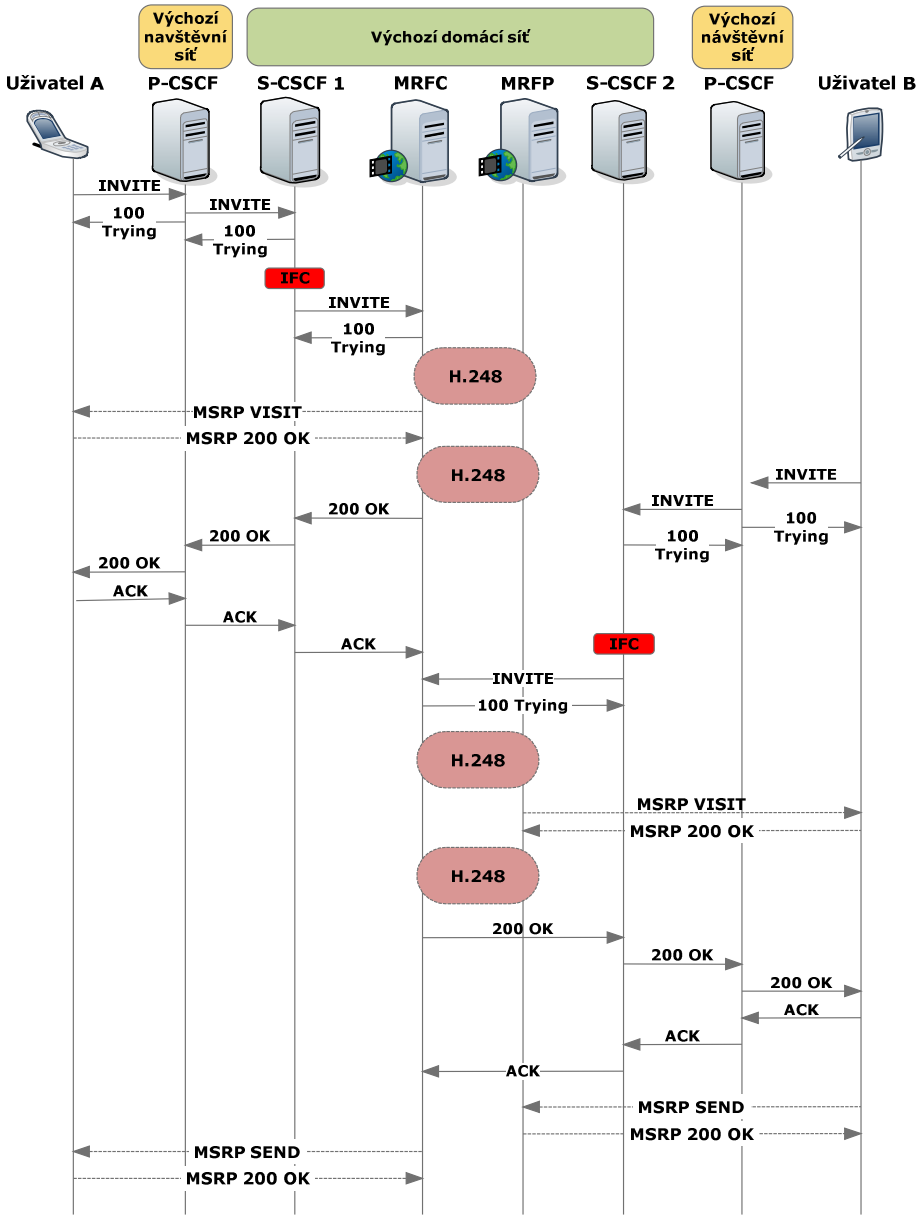
Obr. 9: Přenos zpráv v pager módu [4]

Chatovací mód (Session-based Mode)

Tento mód je založen na SIP požadavku INVITE. K přenosu zpráv se používá MSRP, jež je implementováno v každém IMS zařízení. Přenos může být uživatel-uživatel, v tom případě se přenos podobá hlasovému hovoru. Navíc MRFP může implementovat MSRP. Existují dva různé scénáře pro zřízení spojení. První na Obr. 10 kde je zobrazeno spojení k jinému koncovému bodu. MSRP je posíláno od začátku na konec. Rozdíl oproti běžnému přenosu je rozšíření INVITE požadavku, které je definované v SDP (Session Description Protocol). V druhém případě jsou MRFC a MRFP prostředníky v síti. Může to být kvůli operátorovi, aby mohl zpoplatnit zprávy např. na základě jejich velikosti nebo obsahu. Dalším důvodem může být úloha MRF vystupujícího jako jednotka pro konferenci více účastníků (známé jako chatovací místnost). Na Obr. 11 je zobrazen přenos dat konference více účastníků. Pro zjednodušení počítáme s tím, že oba účastníci se nachází v síti jednoho operátora. Na obrázku (Obr. 10) uživatel pošle žádost INVITE přes jeho P-CSCF a S-CSCF. S-CSCF přepošle INVITE do MRFC. MRFC kontroluje MRFP pomocí protokolu H.248 a vytváří nová ukončení pro uživatele. MRFP zahajuje TCP spojení pro IMS terminál a posílá MSRP VISIT požadavek. IMS terminál odpovídá MSRP kladnou odpovědí 200 (OK). Protokol H.248 informuje MRFC, že bylo navázáno nové MSRP spojení a v tomto místě MRFC posílá 200 (OK) k dokončení spojení. Později se připojí druhý uživatel a zřídí se další spojení s MRFC. Kdykoliv může některý uživatel poslat zprávu, která je přenášena požadavkem MSRP SEND.



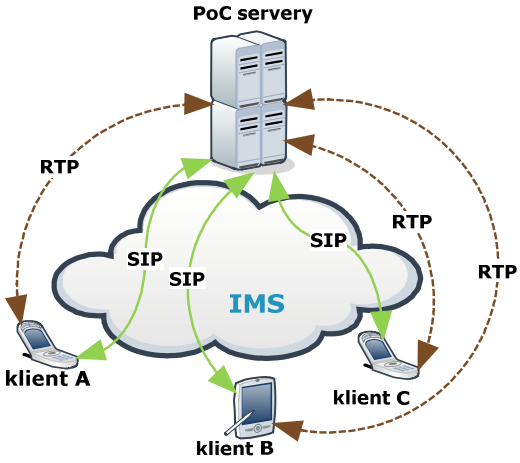
Obr. 10: Spojení MSRP začátek – konec [4]



Obr. 11: Spojení více účastníků (Chat server) [4]

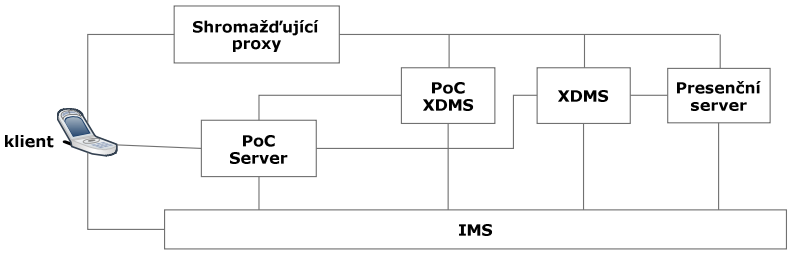
2.3 Služba PoC (Push to talk Over Cellular)

Tato služba slouží ke komunikaci uživatele s jiným uživatelem nebo skupinou uživatelů. V PoC spojení může hovořit v jednom okamžiku pouze jeden účastník spojení, ostatní pouze poslouchají (poloduplexní přenos). Pokud chce účastník hovořit, zmáčkne tlačítko na svém přístroji a může komunikovat s ostatními (nikdo jiný nemluví). Služba je založena na principu „kdo dřív zmáčkne, ten dřív mluví“. Spojení se dá přirovnat k vysílačkám. Řízení spojení a další signalizace je založena na SIP, hlas se přenáší pomocí RTP/RTCP (Realtime Transfer Protocol/ Realtime Transfer Control Protocol), zobrazeno na Obr. 12.



Obr. 12: Služba PoC [2]

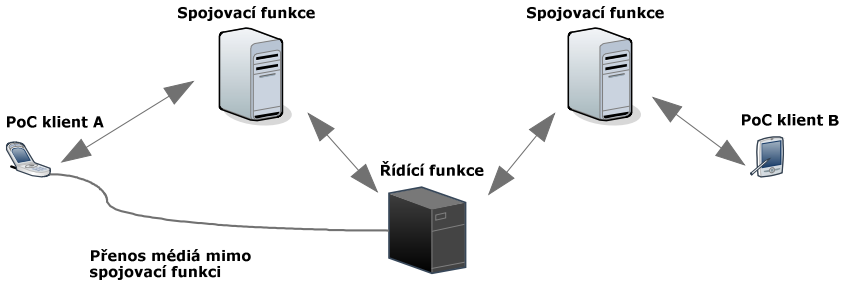
Standard PoC byl navržen OMA (Open Mobile Alliance). Architektura PoC se skládá z: PoC serverů (aplikační, XDMS server) a PoC klienta. XDMS servery obsahují konfigurační nastavení aplikací. PoC server je do IMS připojen přes přístupový bod řízení služeb. IMS zajišťuje funkce služby jako autorizaci, směrování spojení a zpoplatnění. PoC klient je softwarová aplikace v uživatelově zařízení. PoC služba může být propojena i s presenční službou, jak je vidět na Obr. 13.



Obr. 13: PoC architektura [2]

PoC servery

PoC server je aplikační server, který poskytuje služby uživatelům. Kontroluje procedury spojení, uživatele (zdali se smějí připojit od PoC skupiny) a poskytuje informace o uživatelích. OMA definuje dvě funkce serverů: spojovací a řídící. Během spojení je jedna řídící funkce a ostatní jsou spojovací (záleží na počtu uživatelů). SIP signalizace jde vždy jako první do spojovací funkce, který posílá data řídící. Avšak média a jejich signalizace mohou být posílána přímo do řídící funkce. Propojení funkcí je na Obr. 14.



Obr. 14: Architektura PoC serveru [2]

PoC klient

Je standardem OMA označováno jako zařízení, které je schopné připojit se do sítě IMS a používat PoC služby, označení PoC verze v požadavku SIP REGISTER a další. Musí také být schopné nastavovat PoC službu.

PoC komunikace

PoC podporuje několik komunikačních typů. Hlavní rozdíly mezi těmito typy jsou spojeny s politikou přístupu a vytváření spojení. Pozvání mohou být do: předem připravené skupiny, dočasné skupiny (může být spojení 1-1), otevřené skupiny (Chat), uzavřené skupiny. Spojení mohou trvat i hodiny avšak samotný hovor z toho času může zabrat pouhé minuty. Uživatel může využívat několika nezávislých spojení v jeden okamžik. Pro připojení do otevřených skupin musí uživatel znát jejich SIP URI.

Modely zřízení spojení v PoC

Existují dva modely spojení: na vyžádání a předem zřízené. Hlavním rozdílem mezi nimi je vyřizování spojení. Při předem zřízeném spojení uživatel zřídí spojení svou spojovací funkcí a vyjedná všechny parametry spojení před samotným zahájením relace s jinými uživateli. V modelu na vyžádání se využívá základních SIP metod. Parametry přenosu dat jsou vyjednávány během zřizování PoC spojení. První způsob má výhodu v tom, že PoC klient může pozvat další klienty nebo přijmout PoC spojení bez opětovného vyjednávání parametrů.

2.4 IPTV

IPTV nepředstavuje nic víc, než přenos obsahu jako je TV a video na vyžádání (Video on Demand). Tato služba se v dnešní době může přenášet přes pevné, bezdrátové i mobilní sítě. IPTV poskytuje zpětný kanál, takže zákazník může „komunikovat“ s obsahem. IMS IPTV navíc nabízí např. komunikaci mezi jednotlivými uživateli.

Předchůdcem IPTV byla interaktivní TV postavená na MHP (Mobile Home Platform), ale ta měla např. nepěkný vzhled a nebyl u ní standardem zpětný kanál. Neustále zvyšování potenciálních zákazníků nutí operátory a prodejce optimalizovat síťovou strukturu, kontrolní mechanismy a umožnit uživatelům jednoduše využívat služby. K tomu právě slouží provozování IPTV přes síťovou architekturu IMS. IPTV založená na IMS je tedy službou, která je kontrolována a řízena jádrem IMS a doručována nezávisle přes IP síť. IPTV je specifikována standardem ETSI TISPAN (Telecom and Internet converged Services and Protocols for Advanced Network).

Podle lit. [6] existují tři druhy evoluce IPTV:

- IPTV architektura – v drtivé většině dnes používaný standard. Založená na obvyklých protokolech (např. RTP, RTCP).
- NGN IPTV architektura – je schopná pracovat s existujícími prvky v NGN. Jsou v ní komponenty pro kontrolu RACS (Resource Admission and Control Subsystem) a NASS/NACF (Network Attachment Subsystem/ Network Attachment Control Function). Tento přístup využívá specializovaný IPTV subsystém uvnitř NGN.
- NGN IMS IPTV architektura – přenosová část je založena na IMS funkcích. IMS jádro provádí také navázání a kontrolu služeb pomocí SIP protokolu.

Dále se mohou služby dělit na další tři hlavní skupiny [6]:

- Broadcastové vysílání – plošné živé TV nebo rádiové vysílání
- Obsah na vyžádání – obvykle unicastová služba, založená na požadavcích uživatele (vyžádání filmu, písně, atd.)
- Služby nahrávání videa – obsahuje možnosti nahrávání, pauzy nebo posunutí času (*time shift*).

Výhody IPTV založené na IMS:

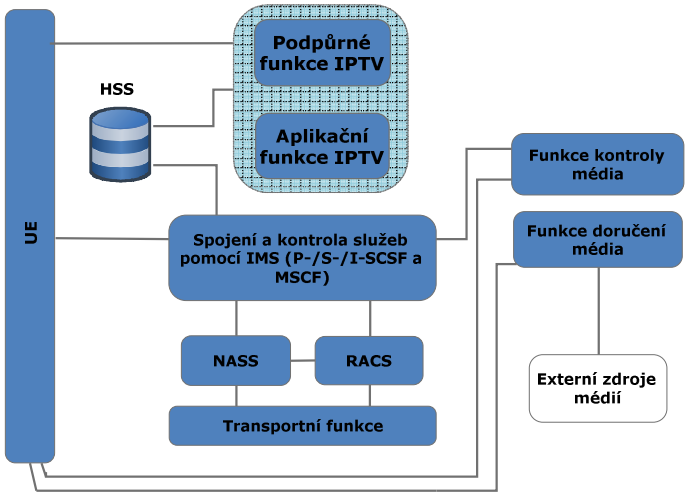
- integrace umožňující registraci a ověření uživatele,
- řízení spojení, směrování a další,
- spolupráci s dalšími službami (Presenční služba, Posílání zpráv v reálním čase, atd.).
- kontrola QoS,

- sjednocuje poplatky a účtování,
- podpora mobility a roamingu.

IMS architektura pro IPTV službu je znázorněna na Obr. 15. Zařízení uživatele komunikuje s funkcemi kontroly služby IPTV přes jádro IMS za účelem řízení spojení. Také může přímo přistupovat ke konfiguraci uživatelova profilu nebo interakci s aplikačním serverem IPTV. V této architektuře se využívá MSCF, jež je zodpovědné za spolupráci IMS jádra na vrstvě kontroly služeb. Hlavními úkoly MSCF jsou: navázání spojení a kontrola služeb IPTV aplikací, ověření uživatelem vybraných služeb podle jeho profilových informací a další. MSCF lze použít jako kontrolní prvek pro jakoukoliv jinou multimediální službu nejen pro IPTV. Tento prvek dovoluje rozšířit IMS jádro bez speciálních změn. MSCF se používá pro kontrolní účely napříč architekturou kontroly a doručení média. Každé uživatelské zařízení má alespoň čtyři propojení s funkcí kontroly média a doručení média. Stejně tak je propojeno s IMS a funkcemi IPTV. Funkce kontroly média může kontrolovat funkci doručení média, což dovoluje vybudovat skutečně škálovatelnou doručovací infrastrukturu. Externí obsah může být přenesen z externího zdroje médií (např. obsah poskytovatele).

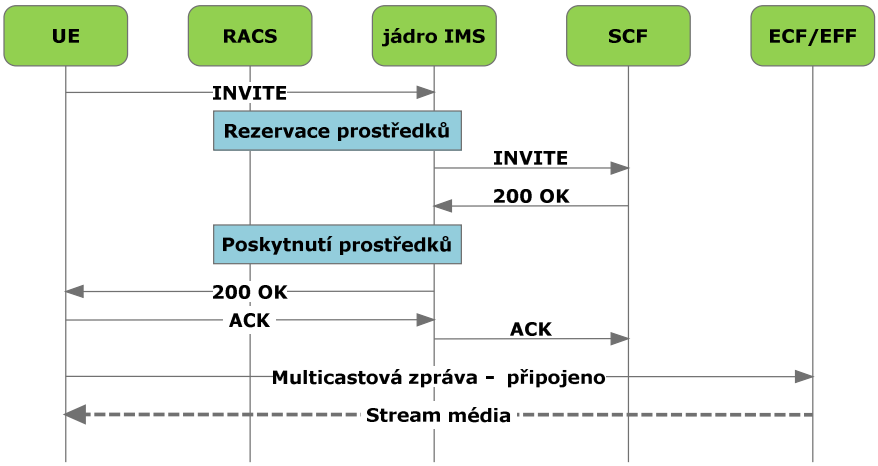
NASS/NACF - mají na starosti dynamické přidělování IP adresy, uživatelovu autorizaci a správu uživatelovi polohy

RACS - je zodpovědný za kontrolu QoS, vyjednávání prostředků přidělení služební a transportní vrstvy.



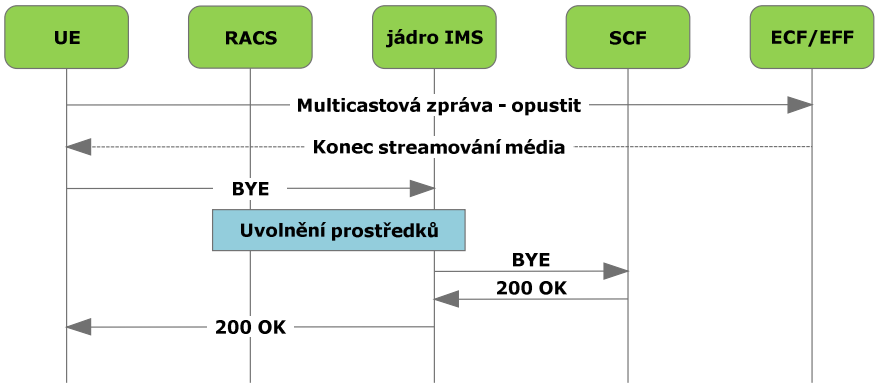
Obr. 15: Architektura pro IPTV s podporou IMS [6]

Příklad signalizace pro živé vysílání TV je uveden na Obr. 16. Uživatel (UE) si vybere obsah a pošle zprávu INVITE do jádra IMS pro sestavení spojení. RACS zajistí rezervaci prostředků. Jádro IMS pošle zprávu INVITE kontrolní funkci SCF, která ověří uživatelův profil, jestli může používat dané služby nebo ne. Pokud je vše v pořádku tak SCF odešle zprávu 200 OK a uživateli je poskytnut obsah. Uživatel potvrdí zprávou ACK, poté se připojí multicastovou zprávou a je zahájen přenos média přes ECF/EFF (transportní funkce).



Obr. 16: Inicializace spojení (živé vysílání) [6]

Na Obr. 17 je zobrazeno ukončení spojení TV vysílání. Kdy uživatel pošle multicastovou zprávu opustit. Transportní funkci ECF/EFF, jež ukončí přenášení média a informuje o tom uživatele. Uživatel (UE) to přijme a pošle do jádra sítě IMS zprávu BYE. RACS uvolní prostředky, jež byly potřebné pro přenos. Jádro IMS pošle zprávu BYE kontrolní funkci SCF a ta ji potvrdí odpovědí 200 OK. Jádro IMS ještě pošle odpověď 200 OK k uživateli.



Obr. 17: Ukončení spojení [12]

3 Protokoly

V IMS se vyskytuje mnoho protokolů, které slouží k zajištění spojení, přenosu dat atd. mezi jednotlivými entitami. Mezi hlavní protokoly patří SIP, DIAMETER, RTP, SDP.

3.1 SIP (Session Initiation Protocol)

Vzešel z protokolů SMTP (Simple Mail Transfer Protocol) a HTTP (Hyper Text Transfer Protocol). Je to textově orientovaný signalizační protokol. SIP protokol je jedním z nejdůležitějších protokolů v IMS. Využívá se pro vytvoření, řízení a ukončení spojení v IP sítích. Byl vybrán, protože podporuje všechny formy médií a díky různým modifikacím může být robustnější a zabezpečený.

3.1.1 SIP zařízení a servery

Uživatelský agent (SIP UA)

Je to koncové zařízení v SIP architektuře. Přijímají a posílají SIP požadavky a odpovědi. Nejčastěji je to uživatelův přístroj (např. SIP telefon). UA se skládá ze dvou částí:

- UAC (User Agent Client) – strana, která vytváří požadavek
- UAS (User Agent Server) – přijímá, přesměrovává, odmítá a posílá odpovědi na příchozí požadavky jménem uživatele

Servery

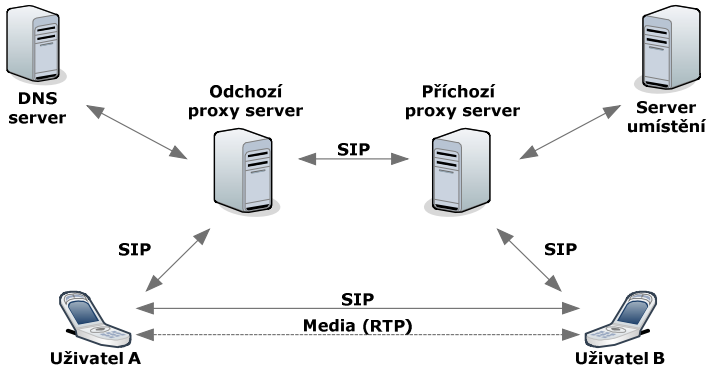
Jsou to logické entity, které zabezpečují přenos mezi jednotlivými UA. Dělí se na:

Proxy server – přijímá žádosti i odpovědi a ty posílá dalším serverům, taky provádí směrování.

Přesměrovací server (Redirect Server) – informuje o nové adrese, kam má být zaslána zpráva.

Server umístění (Location Server) – sleduje umístění uživatelů

Registrační server (Registrar Server) – přijímá žádosti REGISTER. Používá se pro ukládání spojení SIP adresy s adresou hostitele, kde se právě uživatel nachází. Ukázka propojení serverů zobrazuje Obr. 18.



Obr. 18: Ukázka propojení Serverů a UA [2]

3.1.2 Formát zprávy

SIP zpráva se skládá ze tří částí: záhlaví, hlavičky, tělo zprávy.

Záhlaví (Start Line) – jeho obsah se mění podle toho, zda se jedná o SIP požadavek nebo odpověď.

Požadavek (Request)

Obsahuje tři komponenty: typ metody, požadavek URI a verzi protokolu.

Typ metody *(Method name)* – určuje typ požadavku. Je definováno šest základních metod v RCF 3261: INVITE, CANCEL, ACK, BYE, REGISTER, OPTIONS.

Požadavek URI *(Request URI)* – slouží k označení klienta, kterému je požadavek adresován.

Verze protokolu *(Protocol version)* – zde je obsažena verze použitého protokolu. Pro SIP verzi 2.0 tam bude „SIP/2.0“.

Odpověď (Response)

Stejně jako požadavek obsahuje tři komponenty: verzi protokolu, kód odpovědi, text odpovědi.

Verze protokolu – je to totožné s verzí protokolu u požadavku.

Kód odpovědi *(Status code)* – je to trojciferné číslo, kterým se vyjadřuje podstata odpovědi.

Text odpovědi *(Reason phrase)* – textové pole krátce popisující kód odpovědi.

Kódy odpovědí – 1xx - informační

2xx - úspěšná odpověď

3xx - přesměrování

4xx - chyba na straně klienta

5xx - chyba na straně serveru

6xx - obecná chyba

3.1.3 Hlavičky (header files)

Obsahují informace spojené s požadavkem např. iniciátora požadavku.

Každá hlavička musí obsahovat položky - To - To:SIP-URI(;parametry)

- From - From:SIP-URI(;parametry)
- Call-ID - Call-ID:unikátní id
- Cseq - Cseq:číslo metoda
- Via - Via: SIP/2.0/[transportní protokol], kým posláno(;parametry)
- Max-Forwards - Max-Forwards: číslo
- Contact - Contact: SIP-URI(;parametry)

Může obsahovat i další řadu nepovinných položek např. *Event*, *Server*, *Content-Length*.

Tělo zprávy

Může obsahovat jakoukoliv textovou informaci. Nejčastěji se při spojení SIP využívá SDP zpráv popisujících multimediální přenos.

SIP URI

Slouží k identifikaci uživatele v SIP, je jako běžná emailová adresa. Mohou být dvojího typu:

sip:josef@vut.cz – běžná adresa

sips:josef@vut.cz – nový typ adresy vyžadující TLS zabezpečení při přenosu přes TCP [2]

Tvar SIP URI:

sip:infouživatele@hostport[parametry][hlavičky] [2]

3.2 SDP (Session Description Protocol)

SDP protokol je protokolem na aplikační vrstvě sloužícím k popisu multimediálního spojení. Při popisu spojení musí volaný i volající udat své možnosti, formát média a adresu (port). Tyto data se mohou měnit během přenosu. Například při popisu normálního hovoru musí být uvedeny použité kodeky, které jsou potřeba k převedení hlasu do digitální podoby rozpoznány SDP, jež ví, jak je dekódovat na druhé straně. Je tím definováno jakým způsobem bude přenos probíhat. Obsah SDP má tři části – popis spojení, času a média.

V popisu spojení jsou obsaženy informace jako – v = verze protokolu, s = název spojení, b = šířka pásma.
Popis času obsahuje informace jako – t = čas zahájení přenosu, r = kolikrát se spojení opakovalo.
Popis média obsahuje informace jako – c = informace o spojení, i = název přenášeného média (např. filmu).

Formát SDP zprávy: *<znak>=<hodnota parametru>* [2]

3.3 DIAMETER

Je protokolem AAA, který byl vyvinut IETF. Jeho předchůdcem byl RADIUS. DIAMETER je rozdělen na dvě části: DIAMETR protokol a DIAMETR aplikace. Pokračování je zaměřeno jen na Diametr protokol. Využívá pro přenos dat TCP a SCTP protokol. Používanější je SCTP, jelikož umožňuje zařadit několik nezávislých toků do jednoho SCTP. Zabezpečení tohoto protokolu zajišťuje TLS a IPsec. Obsahuje tři typy síťových prvků: klient, server a agent. Hlavní úkolem je propojení CSCF a HSS.

DIAMETER zpráva

Slouží k přenosu požadavků nebo oznámení. Používají se kódy zpráv podobně jako v SIP pro označení účelu zprávy. Zpráva se skládá z hlavičky (verze, ID aplikace,…) a z volitelného počtu atributů nesoucích data (AVPs – Attribute Value Pairs). Definovány jsou např. zprávy pro data spojená s účtem nebo schopností výměny dat.

3.4 MEGACO (MEdia GAteway COntrol protocol)

MEGACO se používá mezi MG a MGC k ovládání signalizace a spojení během multimediální konference. Komunikace je zprostředkována dvěma prvky: koncový –

fyzické připojení (tel. linka) a abstraktní (přenášení např. zvukového souboru), kontext – popisuje spojení mezi koncovými prvky. Protokol používá sadu příkazů, určených k řízení právě popsaných logických entit. Příklady příkazů – Add, Move, Notify, atd.

3.5 XCAP (eXtensible Markup Language Configuration Access Protocol)

V XCAP je uživateli umožněno nahrávat informace na XCAP server, který poskytuje tato data aplikačním serverům, jež poskytují data uživatelům. Uživatel může pracovat s daty, přidávat a mazat je. Příkladem je nahrání uživatelova zdrojového seznamu (RSL) pro presenční službu. Používá HTTP k nahrávání a čtení informací od uživatelů a informace se zobrazují v XML. Využívá se u presenční služby, posílání zpráv a konference.

3.6 RTP (Real-time Transport Protocol)

Je definován jako mezi koncový protokol doručující data v reálném čase (video, audio). RTP neposkytuje QoS, avšak QoS zajišťuje RTCP, které taky přenáší informace o účastnících přenosu a má i další funkce. K rozpoznání chyby přenosu, jsou v RTP přenosu pakety označovány pořadovými čísly. Nejčastěji ve spojení s UDP protokolem.

RTP záhlaví paketu obsahuje:

V (Version) – verze RTP.

P (Padding) – doplňky, mohou být využity k šifrování dat nějakým algoritmem.

X (Extension) – rozšíření RTP hlavičky.

CC (CSRC count) – počet podílejících se zdrojů.

M (Marker) – jeho vysvětlení je definováno v profilu.

PT (Payload Type) – identifikuje používaný kodek.

SN (Sequence Number) – sekvenční číslo paketu. Je inkrementováno o 1 pro každý RTP paket. Přijímač podle něj zjišťuje, zda nepřišel paket mimo pořadí nebo se neztratil.

SL (Timestap) – časová značka přenášených dat. Pomáhá odstranit jitter.

SSRC (Synchronization source) – slouží k identifikaci zdroje paketů.

CSRC (Contributing source) – seznam zdrojů dat.

4 Prostředí SDS (Service Development Studio)

SDS je volně šířitelným programem pro registrované uživatele, který vytvořila firma Ericsson k simulaci a testování IMS aplikací pro klienty i servery. Stáhnout lze z: http://www.ericsson.com/developer/sub/open/technologies/ims_poc/tools/sds_40. Je založeno na platformě Eclipse IDE. Lze v něm vytvořit základní IMS síť s prvky CSCF (S,P,I), HSS, DNS (Domain Name Server) a aplikační servery. Podporuje klienty a zařízení pro mobilní, pevné a WLAN (Wireless Locan Area Network) sítě. Umožňuje pracovat se službami, jako jsou: presenční služba, posílání zpráv, IPTV. Verze prostředí SDS 4.1 FD1 potřebuje pro správné fungování nainstalování Javy verze 6, ta je součástí instalačního balíku. Pro IPTV emulátor založený na IAP 2.0 (což je aplikační platforma pro IPTV) a běžícím na SailFin serveru, je potřeba nainstalovat program VLC media player verze 0.8.6.i, který je možné stáhnout na adrese: http://download.videolan.org/pub/videolan/vlc/0.8.6i/win32/. Pokračování práce bude probíhat v operačním systému Windows 7. I když tato verze ještě není plně podporována pro tento systém. Je možné v ní vytvořit experimentální síť pro IMS IPTV.

Jelikož IPTV je perspektivní, neustále se vyvíjející služba a je připravena k provozování ve spolupráci se sítí IMS, pokračování této práce bude zaměřeno právě na službu IPTV. Nové spolupráce se sítěmi NGN a IMS začínají využívat operátoři a snaží se tyto služby zakomponovat do svých nabídek. Je to vhodné jelikož IMS dovoluje propojovat pevné a mobilní služby a nabízí možnost spravování celé sítě, bez značného zásahu do ní.

4.1 Popis prostředí

SDS prostředí slouží k návrhu a realizaci SIP aplikací, jež zde mohou být navrhovány, rozšiřovány a testovány. SDS obsahuje řadu nástrojů pro vývoj koncových aplikací IMS služeb na straně serverů i klientů. Služby serverů jsou tvořeny SIP, HTTP a Java komponenty. Nová služba je vyvíjena v SIP kontejneru bez závislosti na ostatních službách. Moduly pro klienty je možné vyvíjet jako Java aplikace, využívající SIP, MSRP a jiné protokoly.

V SDS jsou hlavními komponentami:

- Prostředí pro návrh
- Vizuální síť
- ICP

- IJCU
- Emulátor pro přenosná zařízení
- Simulátor jádra IMS sítě
- Testovací prostředí
- Vizuální znázornění přenosu zpráv

4.1.1 SDS komponenty:

Prostředí pro návrh

Je grafické integrované vývojové prostředí (IDE), pracující na systému Eclipse. Rozšiřuje Eclipse např. těmito prvky [12]:

- Možnost vytvářet projekty SIP aplikací, SIP servletů, HTTP servletů a klientské aplikace
- Spouštěč prostředí realizace služeb (SEE)
- Editor pro SIP a HTTP rozmístění popisovačů

Vizuální síť

Poskytuje pohled na simulované uzly CSCF, DNS servery, PoC servery a emulátor Symbian z pohledu sítě. Můžeme vidět, zdali uzel běží, rychle provádět jeho konfiguraci a pouštět ho nebo zastavovat.

ICP (IMS Client Platform)

Používá se k vývoji klientských aplikací pro platformu Windows (verze 2000, XP a Vista) a Symbian. ICP je implementací architektury klientské platformy definované firmou Ericsson pro IMS, jež dovoluje vývoj klientských aplikací pro již existující služby. Podporuje všechny základní služby IMS. Funguje jako UA pro všechny klienty.

Simulátor jádra IMS sítě

SDS poskytuje simulační prostředí pro prvky IMS sítě. To umožňuje SDS chovat se jako virtuální IMS síť pro vývojáře. Entity v simulované doméně se chovají jako jádro IMS sítě, směřují SIP signalizaci do realizačního prostředí a spouští požadovanou logiku služeb. SDS podporuje v jádru IMS sítě operace, jako jsou: vyřízení registrace, ověření, směrování a další. Každá funkce je reprezentována jedním prvkem což logicky představuje jiné IMS entity.

Testovací prostředí

SDS obsahuje dva nástroje k testování služeb: testovacího agenta pro testování chování vaší aplikace s jakýmkoliv druhem zpráv a automatický testovací systém, což je nástroj, dovolující psát, upravovat a spouštět skripty pro otestování aplikace. Testovací prostředí také obsahuje možnost sledovat přenos SIP zpráv v reálném čase nebo ze souboru.

4.1.2 Pracovní prostředí

Pracovní prostředí je sada logických funkcí důležitých pro vývojáře služby, jež v ní může simulovat služby v průběhu vývoje. Všechny prvky služby je možno vyzkoušet bez reálného systému nebo přístupové sítě.

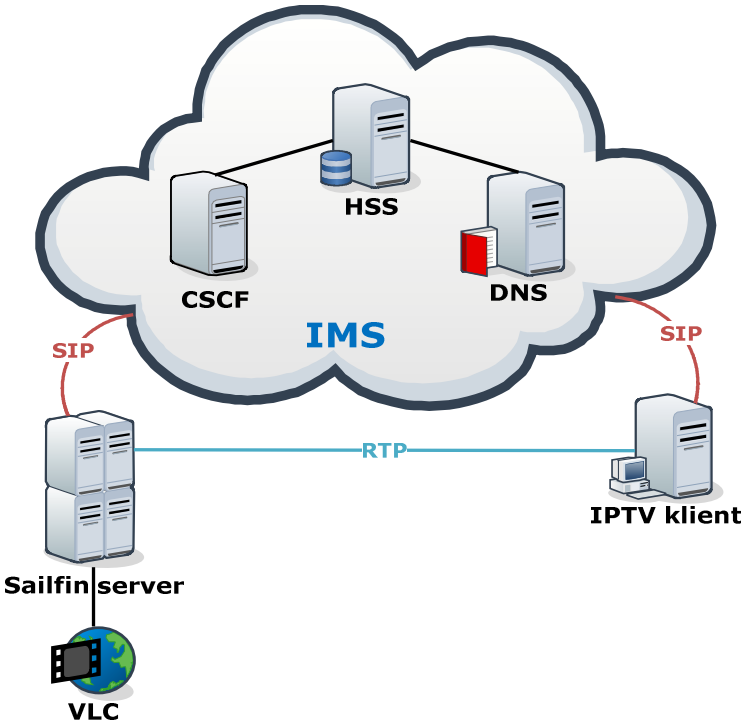
Pracovní prostředí se skládá z prvků:

- HSS – hlavní úložiště dat služeb.
- CSCF – vykonává kontrolu spojení pro registrovaná koncová zařízení. P-CSCF se chová jako SIP proxy. Posílá zprávy do I-CSCF, ale SDS neumí simulovat I-CSCF, takže data jsou přímo směrována do S-CSCF.
- DNS – CSCF využívá jeho procedury k rozložení SIP URI na IP adresu, port a transportní protokol dalšího skoku (*hop*) ke kontaktu.
- Emulátor Symbianu – je grafické rozhraní a testovací prostředí, umožňující simulovat chování zařízeních používajících Symbian.
- PGM – dovoluje klientům spravovat presenční skupinu
- PoC – PoC simulátor poskytuje klienty se schopností implementovat PoC v IMS.
- IMS-M – simulátor posílání zpráv poskytuje schopnost používat IM nebo pozdržet zprávu neregistrovaným uživatelům.
- IPTV – umožňuje interakci mezi IPTV klientem a CSCF, HSS, DNS. Podporuje řešení od firmy Ericsson IAP 2.0. Pro přenášení média využívá RTP a RTSP protokoly, pro řízení relace SIP. Síť je tvořena jádrem IPTV a VLC programem běžícím na Sailfin serveru. VLC se chová jako vysílací server. Používá RTSP protokol pro požadavky služby video na vyžádání. Jádro IPTV řídí požadavky pro IPTV experimentální síť skrze HTTP a SIP. V síti lze provádět akce – spouštět všesměrové vysílání, získávat VoD a poskytnout EPG.

Jediným podporovaným video formátem je MPEG-2 (Motion Picture Expert Group), tudíž všechna používaná videa musejí být převedena do tohoto formátu.

5 IPTV v prostředí SDS Ericsson

Jak již bylo řečeno v programu SDS je možno vytvořit experimentální síť pro IPTV s IMS jádrem. Základními prvky, které tvoří jádro, jsou P/S/I-CSCF, HSS a DNS, ty jsou spojeny s aplikačním server Sailfin na němž je spuštěn přehrávač VLC media player, jež slouží jako server pro vysílání videa a Sailfin server ho řídí. A jako poslední vystupuje IPTV klient, sloužící k ovládání a sledování přenosu ze serveru (připojen přes fiktivní set-top box). Je nutná konfigurace IMS prvků a také úprava XML konfiguračních souborů platformy IAP. Celé zapojení je zobrazeno na Obr. 19.



Obr. 19: Propojení prvků IPTV s IMS

Jednotlivé prvky, které jsou potřebné pro provoz experimentální sítě:

5.1 CSCF

Základní prvek v síti IMS zařizující registraci a spojení. V programu je potřeba nastavit IP adresy (adresa používaného počítače) a porty prvků P/S/I-CSCF. Přístup k nastavení se nachází na horní liště nabídky programu Window→Preferences→Ericsson SDS→Server. Položka CSCF zahrnuje několik možností úprav nastavení. Například jestli má docházet k ověření uživatele při přihlašování ke službám na základě algoritmu MD5 (jediný podporovaný v programu), dále jak dlouho má být uživatel připojen do

systému (min. a max. doba) a možnost roamingu uživatele. Chová se jako SIP proxy a registrační SIP spolu s uživatelským agentem SIP. P-CSCF (používá port 5081) posílá dále REGISTER požadavky přijaté od UA do I-CSCF pokud uživatel není v domácí síti (SDS prostředí neumí simulovat I-CSCF, zpráva jde tedy přímo do S-CSCF), v případě pokud je, jde požadavek přímo do S-CSCF (používá port 5082) domácí sítě. P-CSCF také schovává identitu před vnějšími sítěmi. I-CSCF pracuje se seznamem DNS a při provádění SIP procedur P/S-CSCF hledá další SIP skok v cílové doméně zprávy, je také schopno přeložit číslo ve formátu E.164 do URI a získat informace o uživateli z HSS. S-CSCF komunikuje s HSS za účelem získání profilu uživatele (může obsahovat iFC (Initial Filter Criteria)).

5.2 DNS

Nastavení tohoto prvku se nachází v programové části SDS - Provisioning. Jeho úkolem je řešit spojení mezi dvěma uživateli pomocí doménové adresy, telefonního čísla, IP adresy a transportního protokolu. Můžeme definovat virtuální domény pro CSCF. Tím, že dáme každému aplikačnímu serveru doménové jméno, můžeme posílat všechny požadavky jinému aplikačnímu serveru, jednoduše tím, že změníme IP adresu pro toto doménové jméno. Spolupracuje s CSCF, pro něž provádí rozklad SIP URI na IP adresu, port a transportní protokol a také podporuje možnost přeložit číslo ve formátu E.164 na SIP URI. V programu SDS je využíván BIND (Berkley Internet Name Domain) DNS server, což je DNS server vytvářený jako open source, který vznikl na univerzitě v Berkley. DNS také slouží ke směrování dat pro uživatele, kdy CSCF vytvářející spojení musí najít transportní adresu pro CSCF v jiné doméně. Přenos dat může probíhat pomocí TCP nebo UDP protokolu, klienti musí být schopni automaticky určit protokol.

5.3 HSS

Se také nachází v části Provisioning. 1Obsahuje několik položek, z nichž byla využita pouze položka User Profile sloužící k vytvoření a úpravě dat uživatele, všechny další části zůstaly nastaveny beze změny. V HSS jsou uchovány data obsahující identity uživatelů, přístupové parametry a informace o službách, které uživatel může používat. Přístupové parametry jsou používány pro sestavení spojení (může docházet i k ověření uživatele). Požadovanými vlastnostmi HSS jsou autentizační procedura (uložení autentizačních dat na server), přístup do profilu služeb a poskytnutí těchto dat S-CSCF.

5.4 Sailfin

Server Sailfin je postaven na otevřeném projektu stejnojmenného názvu, spadající pod projekt GlassFish. V prostředí SDS se nachází v položce Servers. Je založen na technologii Java a škálovatelnosti SIP servletů (umožňuje pracovat se žádostmi a odpověďmi typu HTTP). V SDS slouží jako aplikační server, ke spouštění námi vytvořených projektů nebo aplikací, v tomto případě je na něm provozován program VLC. Na něj se pomocí IPTV klienta uživatel připojuje za účelem sledování „televizního“ přenosu. Nastavení Sailfinu se provádí přes webové rozhraní na adrese http://localhost:4848/ kam se můžeme přihlásit jako administrátor pomocí jména a hesla (admin, adminadmin).

5.5 XML konfigurační soubory

Ke konfiguraci IAP platformy slouží XML soubory nacházející se ve složce serveru Sailfin. Jsou to config, config_vclEpg, config_vodList a log4j. Pomocí nich se nastavují například IP adresy RTSP, VLC serveru, dále umístění VLC programu, kanály televize, cesty k souborům, které mají být přehrávány, atd.

Config – konfiguruje IPTV emulátor – jsou v něm umístěny IP adresy a porty serverů (RTSP, VLC a další), umístění VLC přehrávače.

Config_vlcEpg – konfiguruje EPG data o vysílaném kanálu – v něm jsou obsaženy cesty k přehrávaným kanálům. Každý kanál musí obsahovat cestu k souboru, IP adresu, port a data kanálu (název, EPG číslo, počáteční bod přehrávání, čas začátku programu a další). Je důležité, aby každý kanál měl jinou IP adresu, ale je i možnost aby více kanálu sdílelo jednu IP adresu za předpokladu, že každý bude mít jiný port.

Config_vodList – obstarává data k VoD (video na vyžádání) – obsahuje VoD prvky popisující film nebo ukázku. Každý VoD element musí mít jiné id. Opět musí být uvedeny cesty k souborům, jež mají být přehrány.

log4j – nastavuje úroveň informování v konzolovém zobrazení. Například aby se místo běžných informací zobrazovaly ladící zprávy.

5.6 Prostředí IPTV klienta v SDS

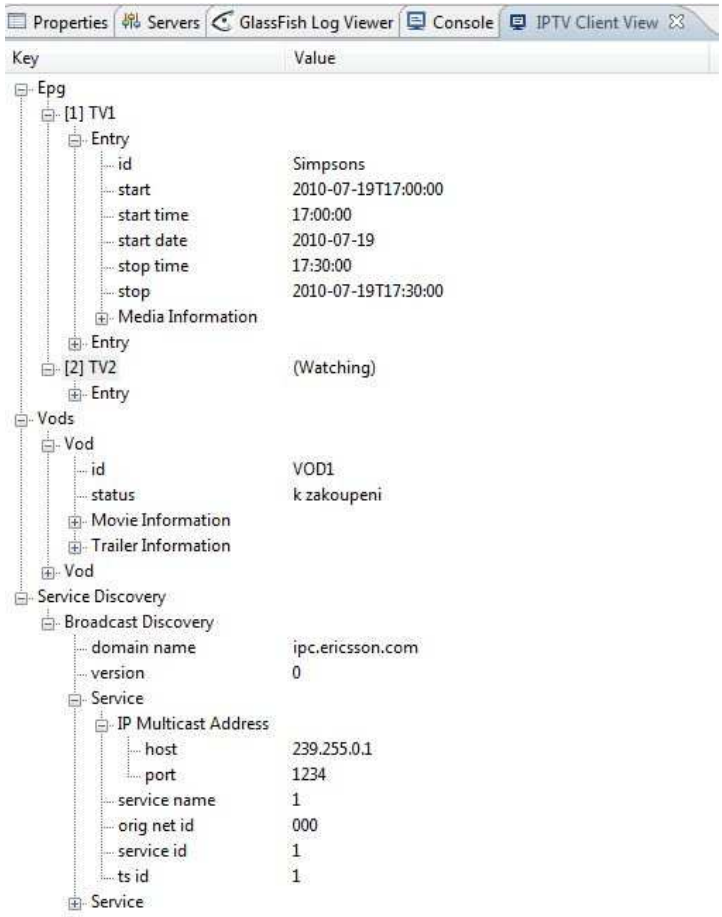
Nastavení se provádí podobně jako u CSCF přes nabídku horního panelu Window→Preferences→Ericsson SDS→Client→IPTV Client. Pokud budeme brát

popis zobrazený na Obr. 20 od vrchu, je zde možnost prohlédnout si EPG, VoD a zjištění poskytovatele služby.

EPG – Nachází se v něm informace o právě vysílaném programu. Obsahuje název pořadu, čas začátku a konce pořadu a datum. V položce *Media Information* je uveden název pořadu, popis pořadu, hodnocení, číslo epizody a kategorie. Také jsou v něm uvedeny informace o dalších pořadech. U právě sledovaného programu je v závorkách uvedeno slovo *Watching*.

VoD – Poskytuje možnost výběru (zakoupení) videa uživatelem. Je zde opět název VoD, jeho status a dále informace o filmu nebo ukázce (*trailer*). V nich je obsažen např. název filmu, popis filmu a hodnocení.

Poskytovatel služby (Service Discovery) – Zde jsou údaje o poskytovateli vysílání. Vidíme název domény a verzi vysílání. Dále IP adresu a port vysílání prvního programu, jméno služby, označení sítě poskytovatele a číslo služby.



Obr. 20: Prostředí IPTV klienta

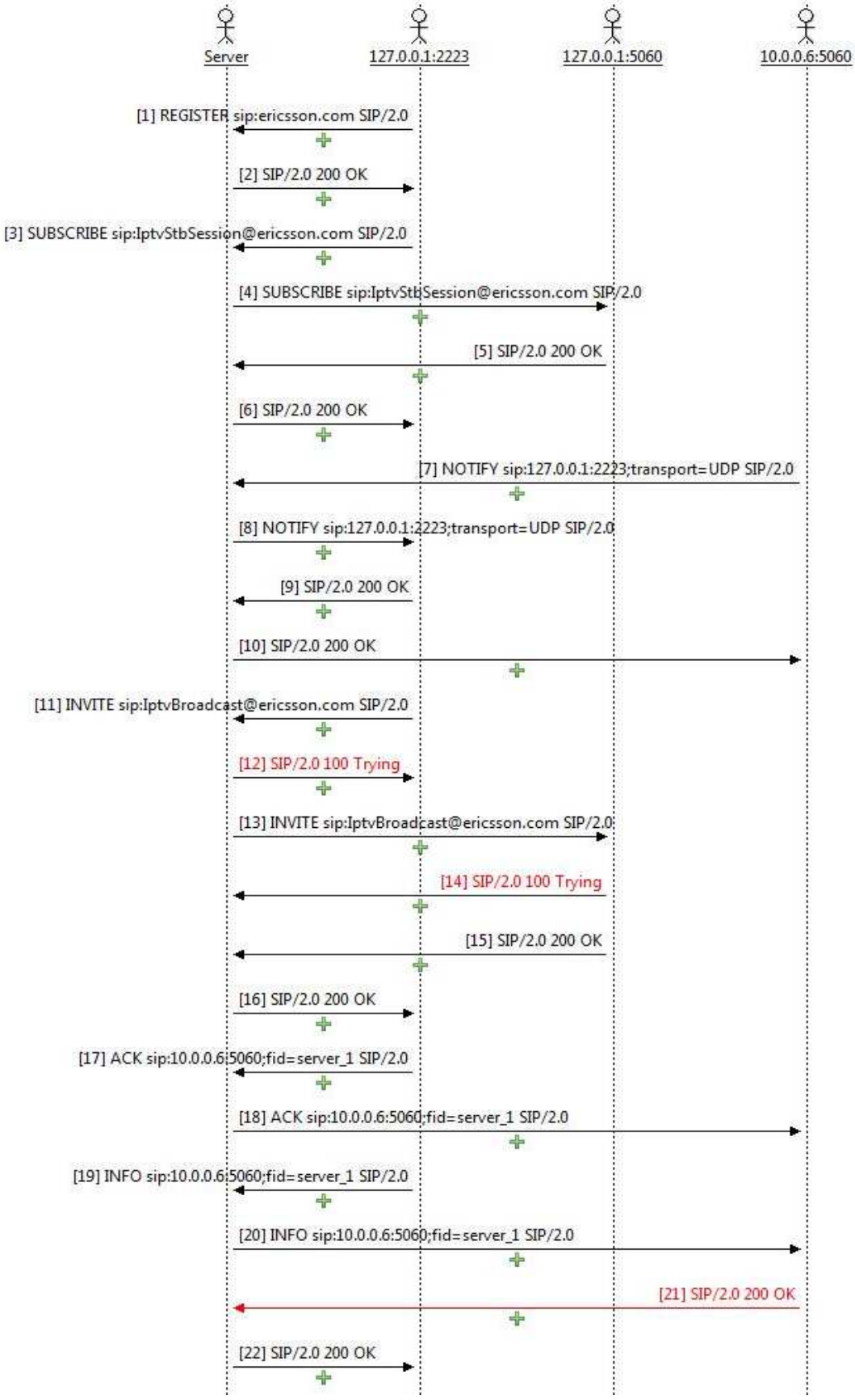
5.7 SIP komunikace

V realizované experimentální síti je možnost přímo v programu SDS sledovat SIP zprávy mezi uživatelem využívajícím IPTV klienta a CSCF entitami, HSS a DNS.

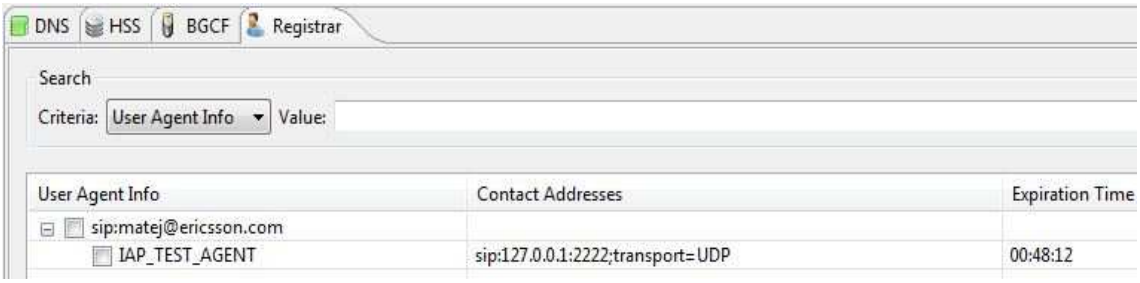
5.7.1 Přihlášení uživatele k serveru a ke sledování programu

Po zapnutí IPTV klienta se uživatel skrze uživatelského agenta přihlásí zprávou REGISTER (Obr. 23) k *Registrar* serveru, který uchovává informace o umístění klientů (IP adresa a port). Spojení uživatele a UA je na obrázku Obr. 22. Zprávy na začátku prochází přes P-CSCF prvek sítě až po čtvrtou zprávu, při které se zapojuje S-CSCF prvek dále se poté střídají, dle toho který prvek je využíván u jaké zprávy. P-CSCF při směrování a S-CSCF při řízení spojení. Uživatel může být připojen po dobu jedné hodiny. Hodnota *expires* byla předem nastavena na 3600 s. Server odpovídá kladně zprávou 200 OK na REGISTER. Třetí zpráva v pořadí je zpráva SUBSCRIBE, jež slouží k vytvoření spojení uživatele a v našem případě IPTV set-top boxu, je inicializována UA, který se jmenuje IAP_TEST_AGENT. Zpráva SUBSCRIBE je ze serveru odeslána uživateli a jím potvrzena 200 OK nazpět a 200 OK posláno serveru. Tím je provedena procedura přihlášení. Nyní je uživateli zaslána zpráva NOTIFY a ten je informován o možnosti přijímat vysílání. Dojde k potvrzení metodou 200 OK a uživatel zprávou INVITE (obsahuje i SDP protokol - Obr. 26) žádá o navázání spojení. Poté dochází k informační odpovědi 100 *Trying* k UA a DNS, která je určena k oznámení procesu zpracovávání požadavku INVITE serverem. Vše je opět v pořádku ukončeno zprávou ACK, jež se standardně používá pro potvrzení požadavku INVITE. Devatenáctou zprávou je INFO, ta slouží k výměně signalizačních informací během spojení (dá se říci, že může nahrazovat použití metody re-INVITE). Nevyužívá se ke změně SIP spojení nebo jeho parametrů. Prostě posílá informace o aplikační vrstvě spjaté se spojením. Může nést například informace o síle bezdrátového spojení nebo zůstatek na účtu a mnohé další. Vše je zakončeno zprávami 200 OK. Uživatel v tento moment sleduje vybraný kanál. Celý tento proces je zobrazen na

Obr. 21 a na dalších obrázcích jsou detaily zpráv REGISTER, SUBSCRIBE a NOTIFY.



Obr. 21: Registrace k serveru až po spuštění přenosu



Obr. 22: Zaregistrování uživatele a jeho UA

Obsah jednotlivých hlaviček zpráv:

```
REGISTER sip:ericsson.com SIP/2.0
CSeq: 1 REGISTER
Expires: 3600
Content-Length: 0
Contact: <sip:127.0.0.1:2223;transport=UDP>
User-Agent: IAP_TEST_AGENT
From: <sip:matej@ericsson.com>;tag=528
To: <sip:matej@ericsson.com>
Call-ID: 7d15b73382b2e50833c29165600156a2@127.0.0.1
Via: SIP/2.0/UDP 127.0.0.1:2223;branch=z9hG4bK2010a3d78c92a3b1b8d9926152ab0a53
```

Obr. 23: Detail zprávy REGISTER

REGISTER – název metody. Za ní následuje adresu domény, do které se uživatel registruje a verze SIP.

CSeq: Jedná se o unikátní označení žádosti v rámci relace. Každá nová žádost inkrementuje CSeq. Opakovaná žádost má stejný Cseq. Veškeré odpovědi k žádosti mají stejný CSeq.

Expires: Udává, po jak dlouho dobu bude uživatel přihlášen se stejným jménem. V tomto případě je to 3600 s (používáno jako standardní čas).

Content-Length: Zobrazuje velikost těla zprávy v decimálním tvaru, 0 značí bez obsahu.

Contact: Obsahuje aktuální adresu UA 127.0.0.1 a typ přenosového protokolu (UDP).

User-Agent: Obsahuje informace o klientově uživatelském agentu, který vytváří žádosti.

From: Zde je uveden iniciátor požadavku. Za ním je uvedena položka *tag*, která obecně slouží jako identifikátor dialogu (vhodné pokud dochází k větvení).

To: V hlavičce je uložena adresa příjemce žádosti.

Call-ID: Hlavička jednoznačně (unikátně) identifikuje skupinu zpráv klienta.

Via: Je v ní zobrazena cesta, přes kterou musí projít požadavek. *Branch* umožňuje detekovat smyčky.

Na dalším obrázku je zpráva SUBSCRIBE, kde jsou popsány pouze hlavičky, které se nevyskytují v předchozí zprávě. Tento postup bude aplikován na všechny detailně zobrazené zprávy tzn., že u každé nové zprávy budou popsány pouze před tím se nevyskytující hlavičky.

```
SUBSCRIBE sip:IptvStbSession@ericsson.com SIP/2.0
Event: eri_iptv
CSeq: 2 SUBSCRIBE
Expires: 3600
Accept: text/xml
Content-Length: 0
Contact: <sip:127.0.0.1:2223;transport=UDP>
User-Agent: IAP_TEST_AGENT
To: <sip:IptvStbSession@ericsson.com>
From: <sip:matej@ericsson.com>;tag=5911
Call-ID: 548ee14221d15b6ea78c7f43c4b1a5a7@127.0.0.1
Via: SIP/2.0/UDP 127.0.0.1:2223;branch=z9hG4bKf79e38d74b9eca94265acf234db31558
```

Obr. 24: Detail zprávy [3] SUBSCRIBE

SUBSCRIBE - název metody. Dále je uvedena adresa, na kterou směřuje požadavek a verze SIP protokolu, jež je v tomto případě 2.0.

Event: Používá se pro informování o události, která je ve zprávě přenášena, zde je to eri_iptv (Ericsson IPTV).

Accept: Tato hlavička je využívána ke specifikování určitého akceptovatelného typu odpovědi. Zde je to text a XML.

```
NOTIFY sip:127.0.0.1:2222;transport=UDP SIP/2.0
Max-Forwards: 69
Subscription-State: active;expires=3600
Event: eri_iptv
CSeq: 2 NOTIFY
Content-Length: 218
Contact: <sip:10.0.0.6:5060;fid=server_1;transport=UDP>
From: <sip:IptvStbSession@ericsson.com>;tag=g7xcbta5-1
Route: <sip:10.0.0.6:5082;from-tag=6360;lr>
To: <sip:alice@ericsson.com>;tag=6360
Call-ID: 644a7651fc8aaea9399a94dfcd609f5c@127.0.0.1
Content-Type: text/xml
Via: SIP/2.0/UDP 10.0.0.6:5060;branch=z9hG4bKdaace18ac8e7ff9444518287072d2c842e6d

<?xml version="1.0" encoding="UTF-8"?>
<iptv xmlns="http://stbsession.ipc.iptv.ericsson.com">
 <portalURL>http://127.0.0.1:9080/iap</portalURL>
 <channelURL>http://127.0.0.1:9080/iap/channels.xml</channelURL>
</iptv>
```

Obr. 25: Detail zprávy NOTIFY

Mírné odchylky ve zprávě ať už čísla portů nebo jména a další údaje jsou způsobeny jiným časem a místem zaznamenání zprávy. Pro vysvětlení jednotlivých položek ve zprávě však nemají zásadní vliv.

Max-Forwards: Uvedené číslo udává počet možných průchodů přes proxy nebo brány. Pokud se dostane na nulu, je požadavek zahozen. Slouží k tomu, aby požadavek neputoval sítí do nekonečna a nedošlo k zacyklení.

Subscription-State: Používá se k indikaci stavu, v jakém se nachází proces zapsání. Je aktivní a do jeho vypršení zbývá 3600 s.

Route: Zobrazuje cestu probíhajícího spojení. V tomto případě je to S-CSCF prvek 10.0.0.6, rozeznat to lze podle portu 5082.

Content-Type: Je v ní uveden typ přenášeného obsahu v těle zprávy k příjemci. V XML souboru, jež je v těle zprávy, je přenášena část nastavení IPTV.

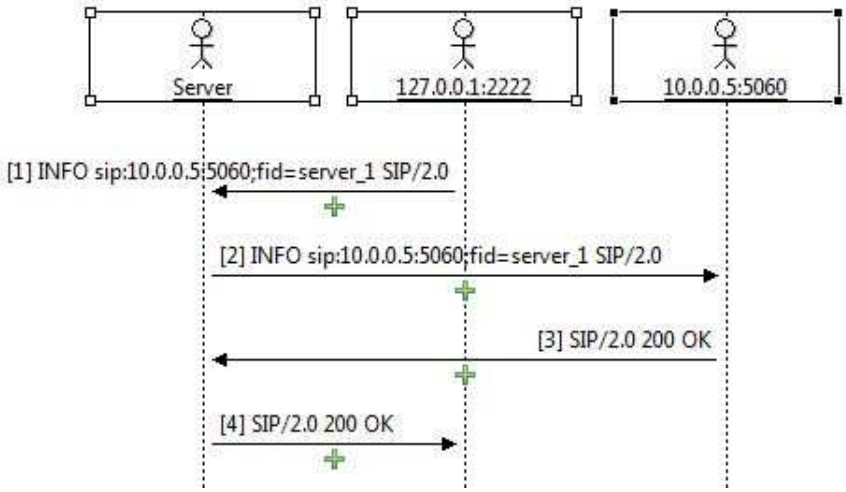
Z následujícho obrázku patřícího k INVITE zprávě lze vyčíst, že SDP protokol je verze 0. Vysílání je inicializováno Internetovou (IN) adresou IPv4 127.0.0.1. Jméno spojení je IPTV SDP. Začátek a konec spojení nejsou určeny. Probíhá přenos videa přes transportní protokol UDP na multicastové adrese. Šířka pásma je 15000 kb/s a data budou pouze přijímána.

```
v=0
o=- 0 0 IN IP4 127.0.0.1
s= IPTV SDP
c=IN IP4 127.0.0.1
t=0 0
m=video 9 RAW/RAW/UDP 33
c=IN IP4 239.0.0.0
b=AS:15000
a=recvonly
```

Obr. 26: Detail SDP v INVITE zprávě

5.7.2 Přepnutí programu

Pokud dochází k přepnutí z jednoho programu na druhý, je přes UA (127.0.0.1:2222) vyslána zpráva INFO na server vysílání označený jako IptvBroadcast a ten dále posílá zprávu na server Sailfin, na němž běží multicastové vysílání. Zpráva je nyní doručena na server a ten odpovídá kladně zprávou 200 OK. V první zprávě INFO je patrné zapojení S-CSCF entity, jež řídí spojení a to v položce *Route*. Průběh zpráv i detailní pohled na zprávu INFO jsou zobrazeny na Obr. 27 a Obr. 28.



Obr. 27: Přepnutí programu

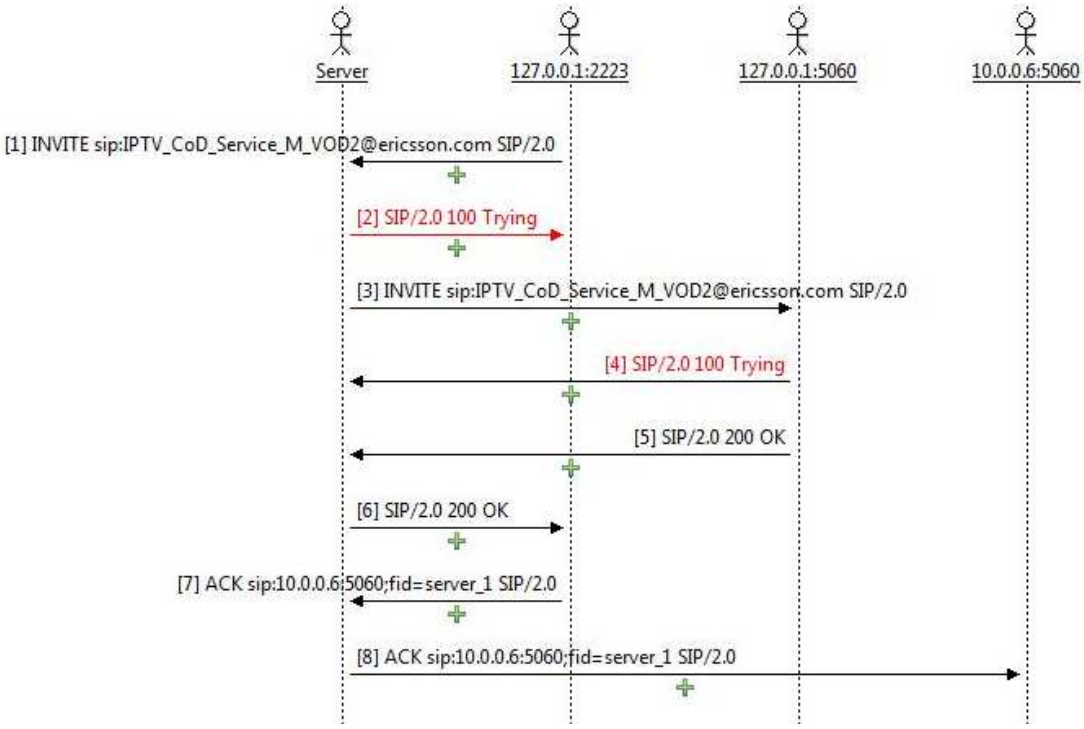
```
INFO sip:10.0.0.5:5060;fid=server_1 SIP/2.0
CSeq: 6 INFO
Content-Length: 181
Contact: <sip:127.0.0.1:2222;transport=UDP>
From: <sip:matej@ericsson.com>;tag=1974
To: <sip:IptvBroadcast@ericsson.com>;tag=g7zvnehq-2
Route: <sip:10.0.0.5:5082;from-tag=1974;lr>
Call-ID: 618803b623e76403311b8ab01ca8d8bd@127.0.0.1
Content-Type: text/xml
Via: SIP/2.0/UDP 127.0.0.1:2222;branch=z9hG4bK38b56c4b6aab8d0b9de6e510e2e8be71

<?xml version="1.0"encoding="UTF8"?><channelChange xmlns="http://channelChange.ipc.ercisson.com">
```

Obr. 28: Detail SIP zprávy [1] INFO

5.7.3 Video na vyžádání

Na Obr. 29 je zobrazen přenos SIP zpráv, pokud si uživatel vybere (zakoupí) video. UA zahajuje přenos zprávou INVITE na server, kde je uložen požadovaný obsah (video). Server mu odpovídá zprávou *Trying*, což označuje zpracovávání požadavku INVITE. Stejný postup se odehrává i u DNS. Poté jsou oba požadavky potvrzeny zprávami 200 OK. Celý proces je ukončen zprávami ACK, které potvrzují INVITE požadavek. Nyní ještě není spuštěn samotný přenos videa, bylo pouze zakoupeno. Uživatel si jej spustí v momentě, kdy bude chtít. V tomto módu je na rozdíl od předešlého vysílání možnost ovládání přenosu formou pauzy. Pokud dojde k ukončení sledování daného VoD, je uživatel automaticky přepnut na poslední sledovaný kanál.



Obr. 29: Zprávy při službě video na vyžádání

Na dalším obrázku (Obr. 30) je pohled na první zprávu INVITE. Popsány budou opět jen části, které se nevyskytují v předchozích detailně popsaných zprávách. V tomto případě je zde na první pohled patrné rozšíření o SDP protokol v těle zprávy. Prvním prvkem tohoto protokolu je v=0.

Popis jednotlivých položek SDP protokolu ve zprávě INVITE:

```
INVITE sip:IPTV_CoD_Service_M_VOD2@ericsson.com SIP/2.0
CSeq: 7 INVITE
Content-Length: 193
Contact: <sip:127.0.0.1:2223;transport=UDP>
User-Agent: IAP_TEST_AGENT
From: <sip:matej@ericsson.com>;tag=3325
To: <sip:IPTV_CoD_Service_M_VOD2@ericsson.com>
Call-ID: f14ccb33fabc11233d184f6404ed1afb@127.0.0.1
Via: SIP/2.0/UDP 127.0.0.1:2223;branch=z9hG4bK3deca61c98183130261ea37f4335023f
Content-Type: application/sdp

v=0
o=- 0 0 IN IP4 127.0.0.1
s=-
t=0 0
m=application 9 tcp eri_iptv_rtsp
c=IN IP4 127.0.0.1
a=setup:active
a=connection:new
m=video 1232 RAW/RAW/UDP 33
c=IN IP4 127.0.0.1
b=AS:17000
a=recvonly
```

Obr. 30: Detail první INVITE zprávy

v= Slouží k označení verze protokolu.

o= Označuje původce spojení. Na začátku je znaménko „-“ což označuje, že původce nepodporuje koncept uživatelských adres. Dále 0 označuje ID spojení a druhá 0 označuje číslo této zprávy (je využíváno proxy pro rozlišení, která zpráva z mnoha pro toto spojení je nejnovější). Položka IN je zkratkou pro Internet a ta je následována verzí použitého protokolu IPv4 a adresou původce.

s= Označuje jméno spojení. Zde je nevyplněno.

t= Specifikuje začátek a konec relace. Zde uvedeny neurčité hodnoty, začátek 0 a konec 0.

m= Slouží k popisu přenášeného média. Každý popis, v němž mohou být i další položky začíná „m=“ a končí dalším „m=“ nebo také na konci samotného SDP. Na začátku je definováno médium v našem případě *application* (což značí přenášení signalizace). Následované číslem portu a transportním protokolem. Na konci je označení služby.

c= Obsahuje informace o spojení v popisu média. (volitelná položka, pokud je již obsažena v popisu spojení)

a= Obecně označuje žádný nebo více atributů média. Zde je obsah položky „a“ spjatý s TCP. Atribut *setup* uvádí, který z koncových bodů mohl zahájit TCP spojení. *Active* určuje, že koncový bod bude zahajovat odchozí spojení.

a= Tato položka je spjatá s předcházející, jež slouží v kontextu SDP k zahájení přenosu. Zde je uveden atribut *connection*, který slouží k tomu, že se SDP zprávy mohou posílat v jakémkoliv stádiu přenosu mezi koncovými body jako je např. vyjednávání parametrů pro médium nebo ukončování spojení a další. Položka *new* určuje nově vytvářený přenos (opakem je *existing*).

m= Zakončení popisu média. Nachází se zde označení typu média v našem případě video, dále port přenosu a zvolený přenosový protokol, číslem 33 je označen formát média.

c= Obsahuje informace o spojení, jediný rozdíl od předchozího „c“ je, že se nachází v popisu spojení a je opět volitelná pokud je obsažena v popisu média.

b= Udává uvažovanou šířku pásma. AS (*Application-Specific Maximum*) znamená maximální hodnotu šířky pásma v kbit/s, zde je to 17000 kb/s.

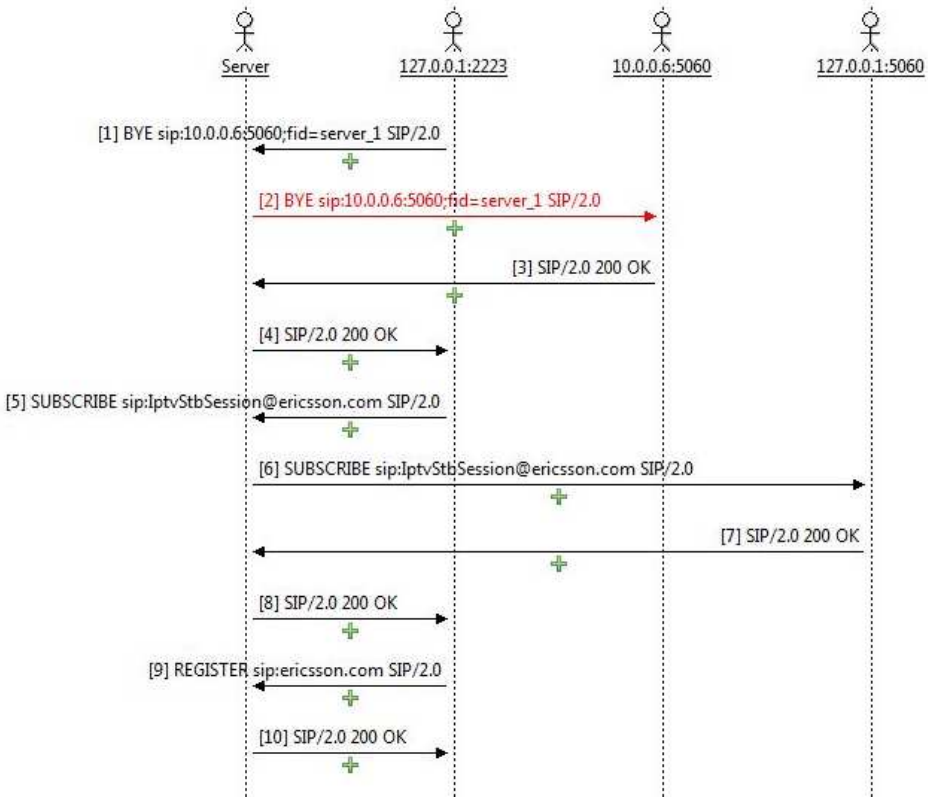
a= Hodnota *recvonly* vyjadřuje to, že aplikace bude data pouze přijímat.

5.7.4 Odhlášení uživatele od serveru IPTV

Při ukončení spojení, respektive příjmu vysílání UA vyšle standardní ukončovací požadavek BYE (Obr. 31) na adresu *sip:IptvBroadcast@ericsson.com* tedy adresu vysílání. Dále je ze serveru odeslána zpráva BYE na Sailfin server. Oba požadavky dostávají kladnou odpověď 200 OK. Pátou zprávu v pořadí je SUBSCRIBE odesílána přes UA na adresu Set-top boxu, která má ale na rozdíl od přihlašovací zprávy SUBSCRIBE v položce *expires* uvedenu hodnotu 0 (tedy nulový čas přihlášení) což značí „odhlašovací“ požadavek. Stejná zpráva je odeslána i na DNS. Přichází kladné potvrzení 200 OK jak od DNS tak i od Set-top boxu. Poslední zprávou je REGISTER, sloužící k odregistrování. Opět to lze poznat podle položky *expires* s hodnotou 0. Celý proces je zakončen odpovědí 200 OK na požadavek REGISTER. Přenos zpráv je na Obr. 32.

```
BYE sip:10.0.0.6:5060;fid=server_1 SIP/2.0
Contact: <sip:127.0.0.1:2223;transport=UDP>
CSeq: 12 BYE
Route: <sip:10.0.0.6:5082;from-tag=7938;lr>
Via: SIP/2.0/UDP 127.0.0.1:2223;branch=z9hG4bKb462e749d02f1126b97cbf7b1a69c5d5
Call-ID: 1de83a654cbe4557dc7b3e511d424e5c@127.0.0.1
From: <sip:matej@ericsson.com>;tag=7938
To: <sip:IptvBroadcast@ericsson.com>;tag=g7ypv79i-5
```

Obr. 31: Detail zprávy BYE



Obr. 32: Odhlášení uživatele

```
SIP/2.0 200 OK
CSeq: 14 REGISTER
Expires: 0
Date: Tue, 13 Apr 2010 13:14:13 GMT
Content-Length: 0
Contact: <sip:127.0.0.1:2223;transport=UDP>;expires=0
P-Associated-URI: <sip:matej@ericsson.com>,<sip:+15145550003@ericsson.com;user=phone>
To: <sip:matej@ericsson.com>;tag=1653
From: <sip:matej@ericsson.com>;tag=4381
Call-ID: 199422508e07a7b430ba4443258c9da5@127.0.0.1
Via: SIP/2.0/UDP 127.0.0.1:2223;branch=z9hG4bKc77e23ff7ba90a7452fc4aa6f45b5689;received_port_ext=5081;received=127.0.0.1
Path: <sip:term@10.0.0.6:5081;lr>
```

Obr. 33: Detail poslední zprávy 200 OK

U odpovědí je vždy na začátku uvedena verze SIP a kód odpovědi se slovním vyjádřením.

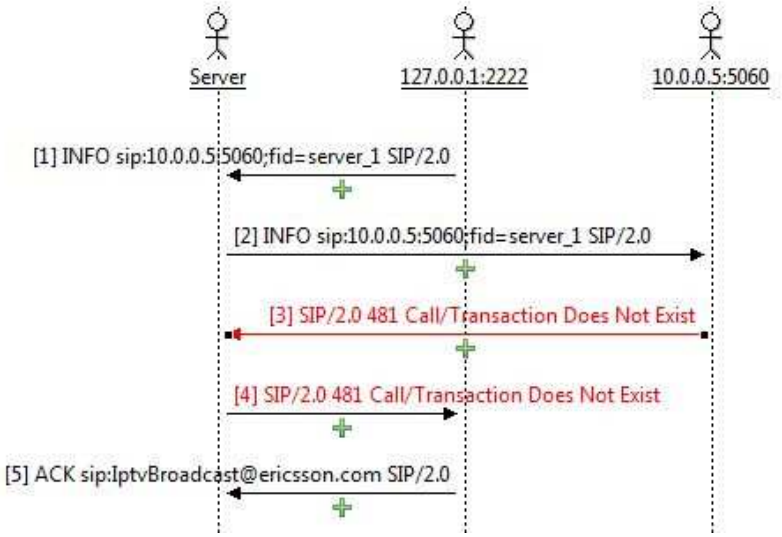
Date: Obsahuje datum a čas kdy byla poprvé odpověď poslána. Možno využít tam, kde je potřeba systému ověřit si aktuální čas. (systémy, které nemají zabezpečený neustálý chod hodin)

P-Associated-URI: Patří mezi privátní hlavičky, její účel je spjatý s konkrétním prostředím. Byla vyvinuta pro 3GPP, které ji používá. Pokud *Registrar* podporuje tuto hlavičku, musí být uvedena vždy v odpovědi 200 OK na registrační požadavek. Jsou v ní uvedeny všechny asociované adresy k registrovanému kontaktu. Nemusejí být všechny zaregistrovány.

Path: Jedná se o rozšíření SIP hlaviček (RFC 3327). Je velmi podobný hlavičce *Record-Route*. Používá se k vybudování cesty pro transakci náležející do spojení. Zde je vidět zapojení prvku P-CSCF, podle portu 5081.

5.7.5 Vypršení času přihlášení (expires time)

Pokud vyprší čas přihlášení, který byl nastaven na 3600 s od začátku připojení uživatele, není uživatel schopen například přepnout program, jak je znázorněno na Obr. 34. INFO zpráva posílaná při přepnutí programu dostává v tomto případě negativní odpověď *481 Call/Transaction Does Not Exist* (obecně odpovědi 4xx značí chybu na straně klienta). Není zde žádný existující dialog. Samotný obsah zprávy 481 je uveden na Obr. 35.



Obr. 34: Vypršení času přihlášení

```
SIP/2.0 481 Call/Transaction Does Not Exist
CSeq: 7 INFO
Via: SIP/2.0/udp 10.0.0.5:5082;branch=z9hG4bKb2fb33b0baefdfde0c3fba244d70f22c,SIP/2.0/UDP 127.0.0.1:2222;
branch=z9hG4bK03dfc5aaf82d517e58f102e4cf63bc4e;received_port_ext=5081;received=127.0.0.1
Server: Glassfish_SIP_1.0.0
Content-Length: 0
Call-ID: 618803b623e76403311b8ab01ca8d8bd@127.0.0.1
From: <sip:matej@ericsson.com>;tag=1974
To: <sip:IptvBroadcast@ericsson.com>;tag=g7zvnehq-2
```

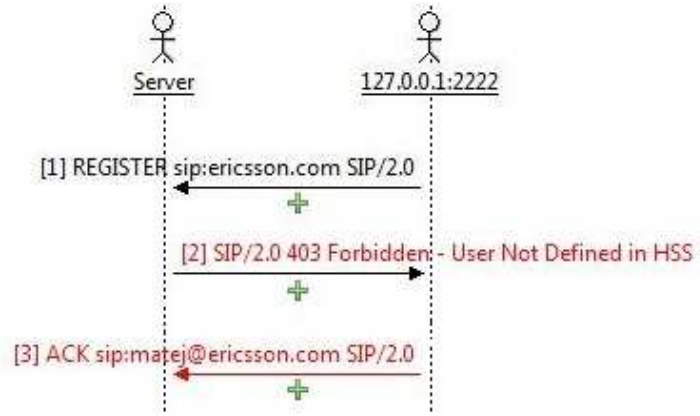
Obr. 35: Detail odpovědi 481

Zde je možné vidět další hlavičku používanou v SIP a to je *Server*.

Server: Obsahuje informace o tom jaký software (zde Glassfish pod nějž je zařazen i Sailfin) využívá UAS pro vyřizování požadavků.

5.7.6 Chyba pokud uživatel není v seznamu HSS

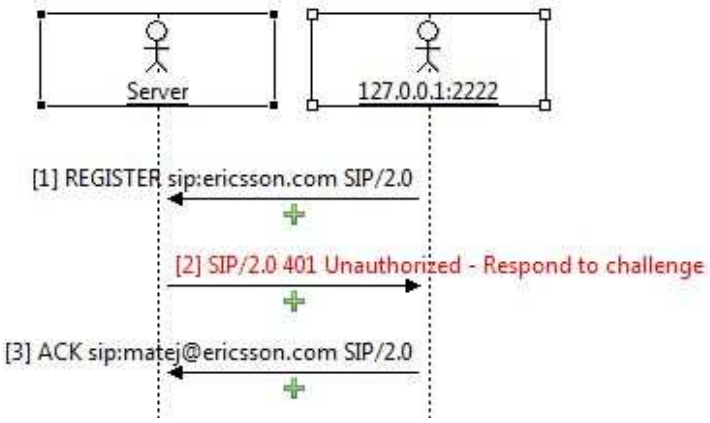
Při této chybě bylo nastaveno přihlašovací jméno IPTV klienta na matej@ericsson.com. Chyba byla vytvořena ve slově matej, jelikož v HSS bylo uvedeno matj a při pokusu o přihlášení zprávou REGISTER se UA dostalo negativní odpovědi *403 Forbidden – User Not Defined in HSS*. Požadavek je tedy chybný a nemůže být zpracován. UA potvrzuje přijetí odpovědi 403 zprávou ACK. Komunikace je uvedena na Obr. 36.



Obr. 36: Uživatel není v HSS

5.7.7 Chyba při přihlašování (ověřování) uživatele

V tomto případě byla zvolena možnost ověření uživatele v CSCF při přijetí zprávy REGISTER. Použitým algoritmem byl MD5 (jediný podporovaný). Uživatel (UA) neprošel ověřením, jelikož neposkytnul ověření ve svém požadavku REGISTER a byla mu zaslána negativní odpověď *401 Unauthorized – Respond to challenge*. Proces ověření a detail odpovědi 401 jsou zobrazeny na Obr. 37 a Obr. 38.



Obr. 37: Chyba při ověřování uživatele

```
SIP/2.0 401 Unauthorized - Respond to challenge
CSeq: 1 REGISTER
Via: SIP/2.0/UDP 127.0.0.1:2222;branch=z9hG4bKe2e00224dd5fd7275b432ef584bfda42;received_port_ext=5081;received=127.0.0.1
WWW-Authenticate: Digest realm="ericsson.com",stale=false,algorithm=MD5,nonce="4ed5d953697208007f499b916fe84b0b",
opaque="61b4ed6e5002f09493d8c77443686cc9",domain="sip:ericsson.com",qop="auth"
Content-Length: 0
Call-ID: 66b005da06f7541e74729b309505b75d@127.0.0.1
From: <sip:matej@ericsson.com>;tag=9875
To: <sip:matej@ericsson.com>;tag=3237
```

Obr. 38: Detail odpovědi 401

V této zprávě se objevuje hlavička *WWW-Authenticate* spojená s autentizací uživatele.

WWW-Authenticate: Musí být obsažena alespoň v odpovědi 401. Skládá se minimálně z jedné výzvy, která uvádí autentizační schéma a parametry aplikované na URI, která zahajuje požadavek. Využívá se při autentizaci na server, jež poskytuje nějakou službu. Nejdříve je oblast, ve které je prováděna autentizace. Dále je položka *stale* s hodnotou *false* což značí, že je uživatelské jméno nebo heslo špatné. *Algorithm* označuje použitý algoritmus. *Nonce* obsahuje specifické data serveru (může být generován pro každou odpověď 401). *Opaque* je řetězec dat, stanovený serverem, který může být nezměněný vrácen klientem. *Domain* obsahuje SIP URI domény. Poslední položka *qop* je volitelná a zajišťuje zpětnou kompatibilitu s RFC 2069. Řetězec této položky zobrazuje úroveň zabezpečení podporovanou serverem. Zde *auth* znamená *authentication*.

5.8 Zachycení multicastového přenosu pomocí Wireshark

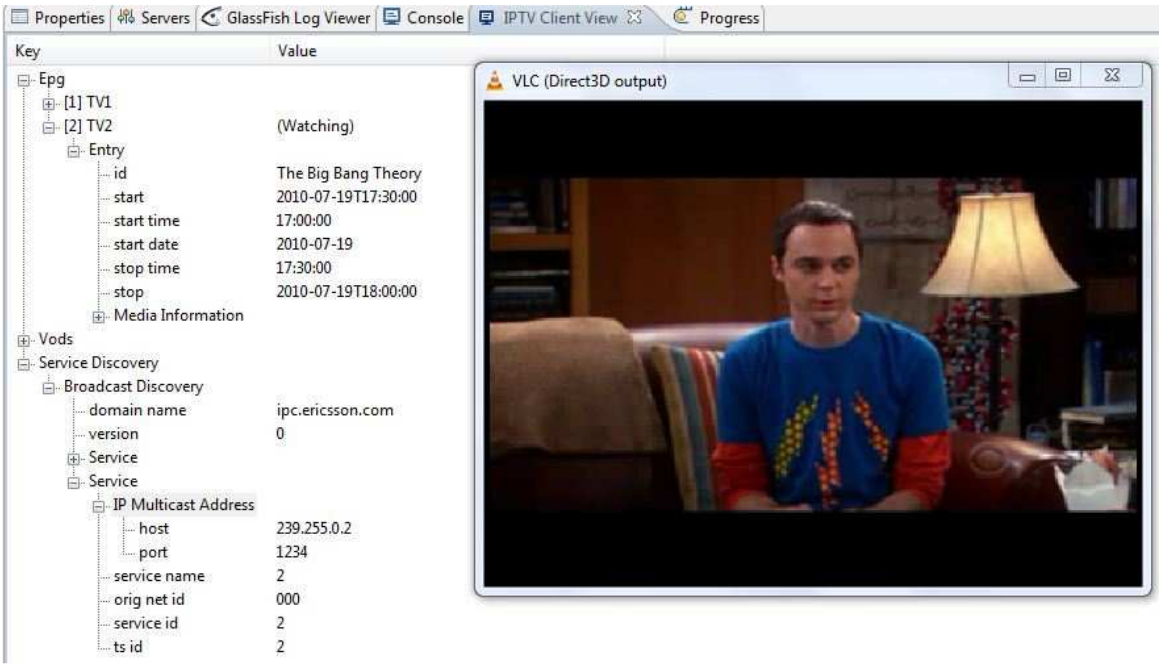
Pomocí programu Wireshark, který slouží pro sledování síťové komunikace, je zachycen multicastový přenos videa na adresách 239.255.0.1 pro první program a s koncovým číslem 2 pro druhý program vysílání (Obr. 39). Je přenášen transportním protokolem RTP, jenž je určen k přenosu multimediálního obsahu. Také je patrné

použití nejužívanějšího protokolu v SIP a to UDP protokolu (povinná podpora všech SIP zařízení). V komunikaci je možno vidět použití kodeku MPEG-II videa při transportním přenosu a zvuku MPEG-1 Audio Layer 2 s vzorkovací frekvencí 44,1 kHz a přenosovou rychlostí 128 kb/s. V zachyceném přenosu se také vyskytuje MPEG PES (Packet Elementary Stream), používaný pro přenos videa po síti. Video pro přenos bylo zvoleno s rozlišením 352x288 a snímkovou frekvencí 25 snímků za sekundu. Video není příliš kvalitní, ale je zvoleno s ohledem na zatížení sítě v domácím prostředí. Šířka pásma obsazená takto upraveným videem na kanálu 2, měla průměrnou hodnotu 711 kb/s. Spolu s prvním kanálem byla průměrná šířka pásma při vysílání 1300 kb/s. Průměrná délka jednoho přenášeného paketu byla 1355 bytů (nemají přesně určenou svoji velikost). Ztrátovost paketů vykazovala při měření nulovou hodnotu. Maximální hodnota kolísání (jitter) byla 8,51 ms a průměrná 1,54 ms. Měření maximální delty mělo hodnotu 75,58 ms (jedná se o rozdíl mezi dvěma po sobě jdoucími pakety). Tyto hodnoty jsou orientační, jelikož Wireshark neumí změřit reálné zpoždění mezi koncovými prvky. Výsledné hodnoty dopočítává dle určitého vzorce.

No..	Time	Source	Destination	Protocol	Info
1	0.000000	DTS 30853.920111111	PTS 30853.960111111	MPEG PES	sequence-header
2	0.013705	192.168.56.1	239.255.0.1	UDP	Source port: 55206 Destination port: search-agent
3	0.016603	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21822, Time=2776880951, Mark
4	0.027363	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21823, Time=2776881839, Mark
5	0.033251	192.168.56.1	239.255.0.1	UDP	Source port: 55206 Destination port: search-agent
6	0.033310	128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
7	0.048859	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21825, Time=2776883613, Mark
8	0.057634	192.168.56.1	239.255.0.1	UDP	Source port: 55206 Destination port: search-agent
9	0.057692	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21826, Time=2776884501, Mark
10	0.061549	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21827, Time=2776885388, Mark
11	0.075197	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21828, Time=2776886275, Mark
12	0.079105	192.168.56.1	239.255.0.1	UDP	Source port: 55206 Destination port: search-agent
13	0.082990	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21829, Time=2776887163, Mark
14	0.085077	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21830, Time=2776888050, Mark
15	0.097675	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21831, Time=2776888937, Mark
16	0.104570	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21832, Time=2776889825, Mark
17	0.112305	192.168.56.1	239.255.0.1	UDP	Source port: 55206 Destination port: search-agent
18	0.120128	DTS 30853.960111111	PTS 30854.000111111	MPEG PES	p-frame
19	0.126991	192.168.56.1	239.255.0.1	UDP	Source port: 55206 Destination port: search-agent
20	0.129889	128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
21	0.133858	128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
22	0.147471	128 kb/s	44,1 kHz	MPEG PES	p-frame
23	0.156261	192.168.56.1	239.255.0.2	RTP	PT=MPEG-II transport streams, SSRC=0xB1396BE9, Seq=21837, Time=2776894261, Mark

Obr. 39: Zobrazení přenosu v programu Wireshark

Na závěr je zde ukázka (Obr. 40) spuštěného multicastového vysílání a prostředí IPTV klienta při příjmu vysílání druhého kanálu.



Obr. 40: IPTV klient při příjmu vysílání

Závěr

Práce je zaměřena na architekturu sítě IMS a služeb v ní. IMS je pro dnešní sítě, ať mobilní nebo pevné velkým přínosem, jelikož umožňuje jejich konvergenci bez nutnosti velkého zásahu do přebudování sítí. Z čehož profitují jak poskytovatelé, tak i zákazníci. Jedním z prvních evropských mobilních operátorů, který implementoval IMS technologii do své sítě, bylo O2 v Británii (2005). V Česku má s IMS zkušenost například firma Vodafone (od roku 2007), jež jej využívá ke konvergenci mobilních a pevných služeb. V jeho síti je použito síťové řešení od firmy Ericsson.

V této práci je rozebrána architektura sítě IMS popisující jednotlivé entity sítě, dále služby, protokoly a aplikační prostředí SDS. Zaměření je na služby, u nichž je popsána architektura a signalizace mezi prvky sítě IMS. Převážná část signalizace je založena na protokolu SIP, který se používá v komunikaci již delší dobu hlavně u služeb VoIP. Zajišťuje kontrolní a řídící mechanismy mezi transportní a síťovou vrstvou. Je velmi vhodný pro svou univerzálnost.

Z jednotlivých služeb byla vybrána jako pokračování této práce služba IPTV provozovaná na architektuře IMS. Tato varianta IPTV poskytuje benefity ve formě spolupráce s dalšími aplikacemi jako je presenční služba nebo posílání zpráv (stále ve vývoji). Cílem IMS IPTV je umožnění používat tuto službu nezávisle na zařízení, jež uživatel používá (počítač, mobilní telefon). V práci je uvedeno i základní seznámení s prostředím aplikace SDS od firmy Ericsson, v němž je možno vytvářet experimentální síť a zkoušet služby provozované v síti IMS. Prostředí SDS umožňuje ověření provozu služby IPTV ve spojení s programem VLC, který je na straně serveru i klienta. K základnímu poznání komunikace v IPTV IMS stačí prostředí v SDS, velkou výhodou je integrované sledování SIP komunikace v IMS jádru. Jsou popsány základní komunikační procesy (*flow diagram*) jako je přihlášení se ke službě IPTV nebo přepnutí programu a další. Ze zachycených zpráv je patrné, že se během komunikace nevyužívají pouze základní metody ze specifikace RFC 3261, ale například i metody SUBSCRIBE nebo INFO. Byly vytvořeny i situace v komunikaci, kdy nastala nějaká chyba, příkladem je vypršení času přihlášení nebo pokud uživatel není uveden v HSS. Vhodné by také bylo mít další možnosti, jako je například unicastové a broadcastové vysílání, nejen multicastové. Z toho vyplívající možnost přepínat mezi těmito typy přenosů, sledovat ovlivnění přenosu (např. zatížení sítě) a průběh SIP komunikace. Práce s programem je intuitivní.

V obecné otázce IPTV je důraz kladen na personalizaci této služby. ETSI TISPAN neustále pracuje na vývoji nové standardizace (TISPAN Release 3), ve které bude možno IPTV používat s propojením služeb, například je to možnost vidět statusy ostatních přátel přímo při sledování, komunikovat s nimi a sdílet s nimi obsah svého domácího úložného média. Pro poskytovatele služby (například reklamní agentury) je zde potenciál zisku více informací o osobě sledující vysílání (je přihlášen pod svým jménem) a tudíž přesnějšího zacílení obsahu (reklamy). Pro uživatele možnost ovlivňovat vysílání např. hlasováním. Stále je potřeba zapracovat na vylepšení QoS, které ještě není implementováno v plném rozsahu. Jedním z těchto problému je neposkytování mechanismů PQoS (Perceived Quality of Service). S neustálým rozvojem je architektura komplexnější, ale také složitější. Je potřeba, aby byla řídící inteligence v IMS síti a ne na jejich okrajích. Přispívá to k jednoduššímu propojování s cizími prvky, které nejsou přímo navrženy pro IMS.

IMS technologie se neustále vyvíjí a je určitě příslibem do budoucna, jelikož vývoj komunikací směřuje ke konvergenci služeb bez závislosti na přístupové síti a používaném zařízení. Pro operátory to přináší výhody v možnosti řídit více služeb jednotnou cestou. Pro uživatele je velký přínos v tom, že může využívat stejných služeb na různých místech a zařízeních.

Literatura

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

[2] POIKSELKA, Miikka, MAYER, Gregor. *The IMS: IP Multimedia Concepts and Services*. V. Británie: WILEY, 2009. 560 s. Third edition. ISBN 978-0-470-72196-4.

[3] AL-HEMZI, Adel, et al. *IP Multimedia Subsystem (IMS): Handbook*. A. Ahson Syed, Ilyas Mohammad. Boca Raton, Florida : CRC Press, 2009. 562 s. ISBN 9781420064599.

[4] CAMARILLO, Gonzalo, GACÍA-MARTÍN, Miguel A. *The 3G IP Multimedia Subsystem (IMS) – Merging the Internet and the Cellular Worlds*. V. Británie: WILEY, 2004. 427 s. ISBN 0-470-87156-3.

[5] LIU, Jeffrey, JIANG, Steven, LIN, Hicks. *Introduction to Diameter : Get the next generation AAA protocol*. [online]. 2006 [cit. 2009-11-28]. Dostupný z WWW: <http://www.ibm.com/developerworks/wireless/library/wi-diameter/>;.

[6] MIKOCZY, Eugen, et al. *IMS based IPTV services - Architecture and Implementation*. In DAGIUKLAS, Tasos, SKLAVOS, Nicolas. 3rd international conference on Mobile multimedia communications: SESSION: Multimedia content management. Nafpaktos, Greece: [s.n.], 2007. s. 7. Dostupný z WWW: <http://portal.acm.org/citation.cfm?id=1385307>;. ISBN 978-963-06-26.

[7] Ericsson. *Service Development Studio (SDS) 4.1 Installation Instructions* [online] 2009 Dostupný z WWW: <http://www.ericsson.com/developer/developerszonedown/downloads/docs/ims_poc/Service_Development_Studio4.1FD1_inst_instruc.pdf >:.

[8] KALID, Ahmad. *IMS - Based IPTV: Today and tomorrov*. In Technology Conference at SUPERCOMM. 2009. McCormik Place, Chicago: [s.n.], c2009. s. 24. Dostupný z WWW: <http://www.blooble.com/broadbandpresentations/presentations?itemid=2730>;.

[9] BEZPALEC, Pavel. *Signalizační protokol IETF SIP/SDP:* přednáška z předmětu X32SIS. Praha: Katedra telekomunikační techniky FEL ČVUT, 2009.

[10] NICK, Williams. *SIP: Creating next-generation telecom applications. developer.* [online]. 2003 [cit. 2009-11-28]. Dostupný z WWW: <http://www.ibm.com/developerworks/wireless/library/wi-sip.html>:.

[11] CHEN, Rebecca LJ, SU, Elisa CY, SHEN, Victor SC, WANG, Yi-Hong. *The Introduction to IP Multimedia Subsystem (IMS)* [online]. 2006. [cit. 2009-11-28]. Dostupný z WWW: <http://www.ibm.com/developerworks/webservices/library/ws-soa-ipmultisub1/>:.

[12] BIKFALVI, Alex. *Iptv TISPAN overview slides* [online]. 2009. s.12. Dostupný z WWW: <enjambre.it.uc3m.es/~bikfalvi/download/IptvTispanOverviewSlides.pdf>:.

[13] *Service Development Studio (SDS) 4.1 Developer's Guide.* [online] 2009. Dostupný z WWW: <http://www.ericsson.com/developer/sub/open/technologies/ims_poc/docs/sds_40_dev_guide>:.

[14] MANI, Mehdi, CRESPI, Noel. *Adopting IMS in WiFi Technology*. In CHEOK, Adrian, CHONG, Peter. 4th international conference on mobile technology, applications, and systems and the 1st international symposium on Computer human interaction in mobile technology: SESSION: Mobility 2007: Next generation communication service. Singapur, China [s.n.], 2007. s. 7. ISBN 978-1-59593-819-0

[15] AL-HEMZI, Adel, MAGEDANZ, Thomas, RIEDE, Christian. *Session and Media Signaling for IPTV via IMS*. In TUGCU, Tuna, XIE, Linda. 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications: SESSION: IMS and multimedia. Innsbruck, Austria [s.n.], 2008. s. 6. ISBN 978-1-59593-984-5

Seznam příloh

Příloha A: Obsah CD

CD obsahuje: elektronickou verzi práce