

Příloha D

Laboratorní úloha č. 2 – IP Multimedia Subsystem

Cíl

Cílem úlohy je seznámení studentů s architekturou IP Multimedia Subsystem, jejím účelem, principy a vlastnostmi. V této úloze budou studenti pracovat s platformou Open IMS Core implementující IMS technologii, jenž je propojena pobočkovou ústřednou Asterisk, umožňující začlenění IP telefonů do IMS sítě.

Požadavky na pracoviště

- PC 1 s operačním systémem Linux (Ubuntu, Gentoo...), nainstalovaný a funkční Open IMS Core se všemi prvky nutnými pro jeho provoz, nainstalovaný IMS desktopový klient myMONSTER, aplikace Wireshark.
- PC 2 s operačním systémem Linux (CentOS, Suse, RedHat...), nainstalovaná PBX Asterisk a nakonfigurovaná pro propojení s IMS.
- Videotelefon Yealink VP-2009.
- Webkamera, sluchátka.

Úkoly

- 1) Spuštění jednotlivých serverů Open IMS Core.
- 2) Seznámení se s testovacími účty.
- 3) Konfigurace IMS klienta a videotelefonu.
- 4) Uskutečnění přenosu hlasu mezi desktopovým IMS klientem a IP telefonem, zachycení relace.
- 5) Uskutečnění videohovoru mezi desktopovým IMS klientem a IP telefonem, zachycení relace.
- 6) Analýza a porovnání zachycených dat.

Teoretický úvod

IMS neboli the *IP Multimedia Subsystem* je sada specifikací a protokolů popisující architekturu *Next Generation Network* pro implementaci IP telefonie a

multimediálních služeb. Tato all-IP architektura představuje výsledek společné snahy 3rd Generation Partnership Project a Internet Engineering Task Force, tedy vůdčích organizací ve svém oboru působnosti. IETF poskytla základní technologie a většinu standardů, zatímco 3GPP vytvořila architekturu rozhraní a integraci protokolů tak, aby IMS splňovala nároky na špičkový mobilní systém světové třídy. IMS byl poprvé uveden v roce 2000 specifikací 3GPP release 5. Technologie IMS propojuje dvě vůbec nejrozšířenější komunikační paradigmaty – mobilní a internetovou technologii. Umožňuje tak přístup k internetovým službám jako je web, e-mail, instant messaging nebo videokonference téměř kdekoli. IMS kromě propojení mobilních a internetových služeb také sjednocuje rozdělení telefonních sítí na okruhově (CS) a paketově spínané (PS). Bývá proto také označován jako služba fixně/mobilní konvergence. Přenos hlasu a dat je tedy sjednocen na paketovou bázi (*all-IP*), čímž je zjednodušena práce s přenášenými daty.

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

Architektura IMS podporuje široké spektrum služeb založených na protokolu SIP. Tato struktura IMS umožňuje uživateli přístup přes rozdílná zařízení a to jak přes IP sítě nebo klasický telefonní systém. Architekturu IMS můžeme z hlediska rozdělení na logické vrstvy nahlížet jako na čtyřvrstvý model

Device Layer – Vrstva koncových zařízení

Struktura IMS nabízí uživatelům možnost volby z širšího spektra koncových zařízení. IMS zařízení jako jsou např. počítače, mobilní telefony, PDA a digitální telefony se do IMS infrastruktury připojují přes IP síť. Jiné typy zařízení, jako jsou třeba tradiční analogové telefony nejsou schopny se k IP síti připojit přímo, ale jsou schopny navázat spojení skrz PSTN bránu [1].

Transport Layer – Transportní vrstva

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

vytvářet a navazovat hovory s PSTN sítí nebo jinou okruhově spínanou (CS) sítí přes PSTN bránu [1].

Control Layer – Řídící vrstva

Jednou z hlavních entit IMS je CSCF nebo-li Řídící funkce hovorových relací. Obecně zahrnuje SIP a proxy servery a je základním prvkem Řídící vrstvy. CSCF zajišťuje SIP registraci koncových zařízení a zpracovává předávání SIP signálů příslušnému aplikačnímu serveru v Aplikační vrstvě. Druhým klíčovým prvkem je HSS (Home Subscriber server) což je databáze údajů a profilů každého koncového uživatele [1].

Service Layer – Aplikační vrstva

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

CSCF – Call Session Control Function

CSCF je souhrnné označení funkcí pro zpracování SIP signalizačních paketů v IMS síti. K dispozici jsou 4 druhy CSCF: P-CSCF, S-CSCF, I-CSCF a E-CSCF [2].

P-CSCF – Proxy Call Session Control Function

Proxy CSFC je prvním kontaktním bodem pro uživatele IMS sítě. Veškerá SIP signalizace směřující od uživatelského zařízení nebo k němu jde přes tuto entitu. Hlavní funkce, ke kterým slouží, jsou [2]:

- Ochrana integrity SIP signalizace na základě IPsec.
- Ochrana spojení mezi UE a P-CSCF, předchází útokům typu spoofing a replay.
- Komprese a dekomprese SIP zpráv pro rádiová rozhraní.
- Komunikace s PDF (Policy Decision Function).

S-CSCF - Serving Call Session Control Function

Jedná se o tzv. Obsluhující CSCF a je centrálním uzlem celé IMS, vždy umístěným v domácí síti. Dohlíží na spojení a registrační služby uživatelských

rozhraní. S-CSCF může mít mnoho funkcí na základě nastavení operátora sítě, mezi ty hlavní patří [2],[4]:

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

I-CSCF (Interrogating Call Session Control Function)

Dotazovací CSCF slouží jako kontaktní bod v síti operátora a nejčastěji je umístěn v domovské síti. Hlavní funkce jsou [2]:

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

E-CSCF (Emergency Call Session Control Function)

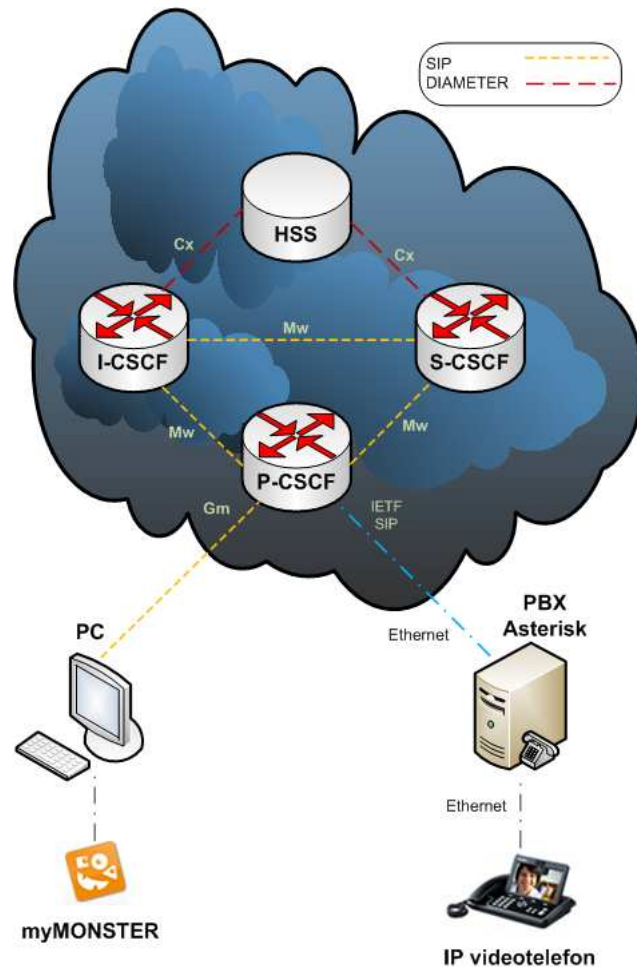
Nouzová CSCF zajišťuje zpracování nouzových IMS požadavků, jako je například relace s policií, záchrannou službou nebo hasiči. Hlavním úkolem E-CSCF je zvolení vhodného nouzového centra, které se nazývá *Public Safety Answering Point* (Centrum odpovídající za veřejnou bezpečnost). Tomuto centru jsou pak doručovány nouzové požadavky pro zpracování [2].

HSS – Home Subscribe Server

HSS je hlavním úložištěm dat o uživateli a uživatelských nastaveních v rámci IMS. V této databázi jsou především ukládána data jako: uživatelské identity, registrační údaje, přístupové parametry, IP informace, informace o poloze uživatele, čísla atd. Pro komunikaci s ostatními prvky sítě HSS využívá protokol DIAMETER. K navázání spojení slouží přístupové parametry jako je autorizace uživatele, autorizace roamingu a jména přidělená S-CSCF. HSS také poskytuje údaje o specifických požadavcích každého uživatele na vlastnosti S-CSCF. Na základě těchto informací I-CSCF volí pro uživatele nejvhodnější S-CSCF. HSS neposkytuje informace S-CSCF umístěným v jiných sítích, což je důležité k zabezpečení uložených uživatelských dat před přístupem z nedůvěryhodných sítí. Tuto ochranu realizují entity P-CSCF a I-CSCF [2],[4].

Open IMS Core

Jedná se o projekt Fraunhoferova Institutu FOKUS (*Fraunhofer Institut für Offene Kommunikationssysteme*), který implementuje funkce CSCF a HSS (tedy jádro IMS, viz. Obr. 1.1) v Open source prostředí operačního systému Linux. Projekt vznikl pro vzdělávací účely a zvýšení dostupnosti principů IMS technologie. Vzhledem k otevřenosti celého projektu a faktu, že je postaven výhradně na Open source a volně dostupných nástrojích a aplikacích, se jedná o vhodný nástroj pro testování.



Obrázek 1.1 Struktura prostředí Open IMS Core [5]

2.4 PBX Asterisk

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

modulů a tedy rozšiřitelnost, podpora širokého spektra audio kodeků a jejich vzájemných převodů. Asterisk dovede pracovat s několika protokoly, zejména VoIP, SIP, H.323, MGCP, IAX a zvládá převody signalizace mezi nimi. Může tedy sloužit i jako multimediální brána pro převod signalizace mezi sítěmi pracujícími na odlišných protokolech

Vypracování

1) Spuštění jednotlivých entit Open IMS Core

Po spuštění PC1 bude vyžadováno zadání loginu a hesla do OS Linux, sdělí vám je vyučující. Spusťte zároveň i PC2 s PBX Asterisk, jako login zadejte *root* a heslo vám sdělí vyučující. Nyní jste přihlášení pod administrátorským účtem, proto nikterak nezasahujte do nastavení systému! Do konzole zadejte příkaz *ifconfig* a poznačte si IP adresu stanice. Pak zadejte do konzole příkaz *asterisk -rvvv* pro inicializaci Asterisku a vraťte se k PC1.

Po spuštění systému otevřete terminál a pomocí příkazu *cd /opt/OpenIMSCore* přejděte do složky Open IMS Core. V této složce jsou nakopírovány skripty pro spuštění jednotlivých serverů IMS. Pro každý server je nutné otevřít nové okno terminálu a příkazy vykonávat s oprávněním *root* nebo *super* uživatele (*sudo*). Servery spustíte následujícími příkazy:

```
./pcscf.sh
./icscf.sh
./scscf.sh
```

Potom příkazem *cd /opt/OpenIMSCore/FHoSS/deploy* přejděte do složky, kde je umístěna Open IMS Core verze databáze HSS nazvaná FHoSS. Spustíte ji příkazem: *./startup.sh*. Nyní by mělo běžet jádro IMS a vy v jednotlivých terminálech můžete sledovat činnost prvků tvořících jádro IMS. Pokud se vyskytla nějaká chybová hlášení, ověřte, že máte potřebná uživatelská oprávnění a příkazy jste zadávali ve správném pořadí.

2) Seznámení se s testovacími účty

Nyní pomocí příkazu *ifconfig* v konzoli zjistěte, jakou IP adresu používá PC1. IP adresu si poznačte, spusťte internetový prohlížeč a jako adresu do prohlížeče zadejte IP adresu stanice a port 8080 (na kterém běží HSS server). Adresa bude vypadat např. takto: *http://192.168.110.34:8080*. Jako přístupové jméno zadejte *hssAdmin* a jako heslo *hss*. Dostanete se do administrátorského rozhraní HSS serveru. Přejděte do sekce *User Identities*, kde máte na výběr sekce *IMS Subscription*, *Private Identity* a *Public User Identity*. Pomocí možnosti *Search* můžete dohledat dvě uživatelské identity Alice a Bob, které

byly předem vytvořeny pro testovací účely. Jednu z identit si prohlédněte podrobně a poznačte si *IMPU*, *IMPI*, *Secret Key* a *Visited Networks*.

3) Konfigurace IMS klienta a videotelefonu

Na ploše najdete zástupce pro spuštění desktopového IMS klienta myMONSTER. Nyní je potřeba nastavit údaje pro úspěšnou registraci vámi zvoleného uživatele do IMS sítě.

V rámci myMONSTER klienta je nutné po spuštění vytvořit nový profil - položka *New*. V menu zvolíme položku *IMS Network* a sekci *Connection Settings* vyplníme údaji, které jste si poznačili v bodě 3). Do položky *PCSCF* zadejte *pcscf.open-ims.test*, port: *4060*. *PCSCF Discovery* nastavíme jako *Fix IP*, jako *Local IP* zadáme IP adresu stanice a zbytek hodnot ponecháme. Po uložení údajů se přihlašte na uživatelský účet, pokud se objevila nějaká chybová hlášení, zkontrolujte správnost zadaných nastavení a ověřte, že jste správně zadali údaje zjištěné z webového rozhraní.

Nyní přejdeme ke konfiguraci uživatelského účtu videotelefonu. Ze statusu na display telefonu zjistíte IP adresu, která byla telefonu přidělena. Tuto adresu zadejte do webového prohlížeče na PC1 a po zadání loginu a hesla *admin/admin* se dostanete do konfiguračního rozhraní. Toto rozhraní si projděte, žádná nastavení však neměňte. V sekci *Account* zadejte do polí *Display Name*, *User Name*, *Register Name*, *Password* hodnotu *1000*. Jako *Sip Server* uveďte IP adresu PC2, kterou jste si poznačili na počátku úlohy. Port nastavte na hodnotu *5060*, *Enable Outbound Proxy Server* nastavte na *Disabled* a stejně tak i *Nat Traversal* – překlad adres NAT ani odchozí proxy server se v našem případě nevyužívá. Jako *transportní protokol (Transport)* nastavte *UDP*. Zbytek položek nechte prázdný, protože nejsou podporovány aktuální konfigurací sítě. Nastavení potvrďte a po chvíli bude *Register Status* zařízení hlásit *Registered*.

4) Uskutečnění přenosu hlasu mezi desktopovým IMS klientem a IP telefonem, zachycení relace

Po úspěšné registraci IMS klienta i videotelefonu můžeme přistoupit k otestování přenosu hlasu. V klientovi myMONSTER v sekci *Calls* zadejte *sip URI* ve formátu *uživatel@IP.adresa* (v našem případě tedy *1000@IP.adresa.telefonu*). Před uskutečněním hovoru ale nejprve spusťte paketový analyzátor Wireshark (zástupce je na ploše) a připravte zachytávání síťového provozu na zařízení *eth0*. Po uskutečnění hlasového hovoru a jeho zachycení, si komunikaci zachycenou aplikací Wireshark uložte, budete ji později potřebovat.

5.)Uskutečnění videohovoru mezi desktopovým IMS klientem a IP telefonem, zachycení relace

Zopakujte postup z předešlého kroku s tím rozdílem, že během audio hovoru kliknete na položku *Enable Video Output* ve spodní části okna a tím aktivujete přenos videa. Po ukončení relace si opět uložte zachycená data.

6) Analýza a porovnání zachycených dat

Nyní prostudujte a analyzujte data obou relací zachycená aplikací Wireshark. Pro lepší přehlednost je doporučeno používat filtry (např. *sip*, *rtp*).

- Porovnejte SIP signalizaci u první a druhé relace - čím se liší?
- Pomocí funkce *Statistics -> Summary* porovnejte průměrnou přenosovou rychlost u audio a audio/video hovoru.
- Pomocí funkce *Telephony-> RTP->Show all streams* zjistěte hodnoty maximálního zpoždění signálu, střední a maximální hodnotu rozptylu signálu. Porovnejte rozdíly u přenosu hlasu a přenosu hlasu/video
- Určete, jaký typ kodeku byl použit pro přenos audia a který pro přenos videa. Jaká je vzorkovací frekvence pro audio a pro video?
- K čemu slouží *Session Description Protocol*? Určete, jaké informace nese pro audio, jaké pro video a v jakých typech zpráv je zde přenášen.

Na konci laboratorního cvičení vraťte pracoviště do původního stavu - smažte vámi vytvořené soubory aplikace Wireshark a vámi zadaná nastavení IMS klienta a videotelefonu.

Literatura

- [1] CHEN, Rebecca LJ, SU, Elisa CY, SHEN, Victor SC, WANG, Yi-Hong. *The Introduction to IP Multimedia Subsystem (IMS)* [online]. 2006. [cit. 2006-09-12]. Dostupné na WWW: <<http://www.ibm.com/developerworks/webservices/library/ws-soa-ipmultisub1/>>.
- [2] POIKSELKA, Miikka, MAYER, Gregor, KHARTABIL, Hisham. *The IMS: IP Multimedia Concepts and Services*. England: WILEY, 2009. 560 s. Third edition. ISBN 0-470-721960.
- [3] CAMARILLO, Gonzalo; GARCÍA-MARTÍN, Miguel A. *The 3G IP Multimedia Subsystem (IMS) : Merging the Internet and the Cellular Worlds*. 1. [s.l.] : [s.n.], 2004. 381 s. ISBN 0470871563.
- [4] AHSON, Syed A.; ILYAS, Mohammad . *IP multimedia subsystem (IMS) handbook*. 1. [s.l.] : [s.n.], 2008. 543 s. ISBN 978-1-4200-6459-9 .
- [5] *OPEN SOURCE IMS CORE* [online]. 2004 , Modified: Tue, Dec 9, 2008 9:57:52 AM [cit.2010-12-10]. Dostupný z WWW: <<http://www.openimscore.org/>>.