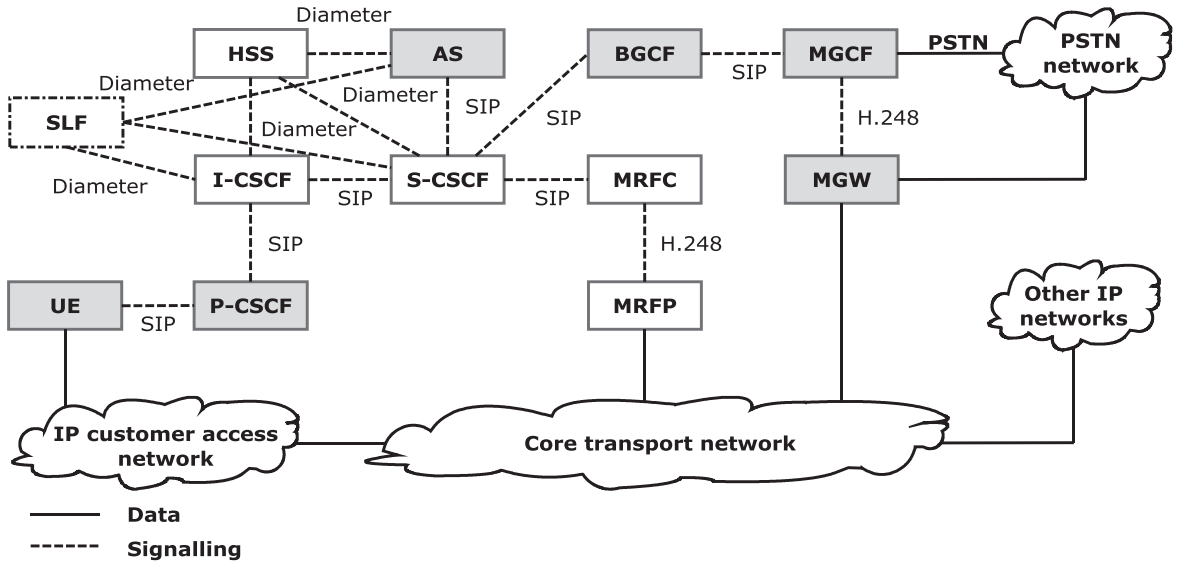
12. IP Multimedia Subsystem

Koncept IMS původně vznikl v projektu 3GPP (3rd Generation Partnership Project) kolem roku 2000 a byl navržen pro mobilní sítě, počítalo se s UMTS. Později byl představen jako koncept NGN, a tedy dle filozofie NGN oddělitelný od přenosové technologie a použitelný jak pro pevné, tak i mobilní sítě. Základním rysem IMS je, že staví na IETF standardech. Stěžejním protokolem v IMS je **SIP** (Session Initiation Protocol) a architektura je navržena tak, že v maximální míře podporuje mobilitu uživatele. Jednotlivé komponenty jsou popsány v následující kapitole a zobrazeny na obr. 12.1, klíčovými prvky v IMS jsou SIP servery označované jako CSCF (Call session Control Function). Pro komunikaci s databázemi se využívá protokol Diameter a pro sestavení, modifikaci či ukončení spojení se využívá SIP.



Obr. 12.1 IMS architektura

12.1 Koncept IMS

Koncept IMS je popsán pomocí entit, realizujících různé funkce:

- AS Application Server, aplikační server poskytují nástavbové služby pro IMS,
- BGCF Gateway Control Function, funkce řízení GW přijímá žádosti relací

přeposílané S-CSCF (nebo jiným BGCF) a vybírá síť, ve které je umístěn přípojný bod v PSTN,

- CSCF Call Session Control Function, funkce řízení relace jsou odpovědné za řízení vlastností spojení, směrování a alokaci zdrojů ve spolupráci s jinými síťovými prvky,
- HSS Home Subscriber Server, Domácí účastnický server obsahuje účastnickou databázi pro IMS (slouží ke zjištění, kde se uživatel nachází),
- MGCF Media Gateway Control Function, funkce řízení médií GW podporuje spoluprácí mezi IMS a PSTN,
- MGW Media Gateway, ukončuje nosné kanály sítě s propojováním okruhů a RTP toky IP sítě, vykonává tedy konverzi médií a transkódování,
- MRFC Media Resource Function Controller, řídí zdroje toků z MRFP ,
- MRFP Media Resource Function Processor, podporuje funkce jako mixování médií, generování tónů, audio hlášek, transkódování a analýzu médií,
- SLF Subscription Locator Function, slouží jako přístup k HSS systémům (jejich front-end a je nezbytně nutný, pokud je více HSS),
- UE User Equipment, představuje funkcionalitu uživatelských terminálů (koncové zařízení).

12.2 Funkce SIP Proxy v IMS

X-CSCF představuje vždy SIP Proxy a IMS zná tři typy: P-CSCF, S-CSCF a I-CSCF. jak již bylo zmíněno, pro signalizaci se používá SIP, pro přenos užitečné zátěže RTP a pro komunikaci s databázemi protokol Diameter (následovník Radius protokolu). Nejdůležitějšími prvky IMS jsou CSCF (jsou to SIP servery, vždy SIP Proxy + případné další funkcionality, např. Registrar).

12.2.1 P-CSCF (Proxy-Call Session Control Function)

P-CSCF (Proxy-Call Session Control Function) je prvním bodem kontaktu koncového zařízení UE. Prvek P-CSCF zajišťuje:

- směrovací funkce na SIP protokolu (směruje volání),
- je schopen inicializovat a rušit SIP dialogy (vytváří, udržuje, ukončuje volání),
- autentizuje uživatele (databáze je v HSS),
- podporuje klienty za NATem a zajišťuje zabezpečený přístup do IMS (čili SBC – Session Border Controller).

Přítomnost funkce P-CSCF je v síti IMS povinná, vykazuje chování koncových SIP-Proxy (Outbound a Inbound), čili přijímá vzniklé požadavky na volání, které směruje na další prvky (I-CSCF) a zároveň je cílovou SIP Proxy, na kterou je volání terminováno.

12.2.2 I-CSCF (Interrogating-Call Session Control Function)

Základní funkcí I-CSCF je nalezení HSS serveru uživatele pomocí přístupové entity SLF (přístup do HSS) a na základě informací z HSS potom určit příslušné S-CSCF, kam bude SIP žádost směrována. I-CSCF vykazuje chování SIP Proxy, stěžejními úkoly jsou:

- nalezení správného S-CSCF,
- dotazování do HSS,

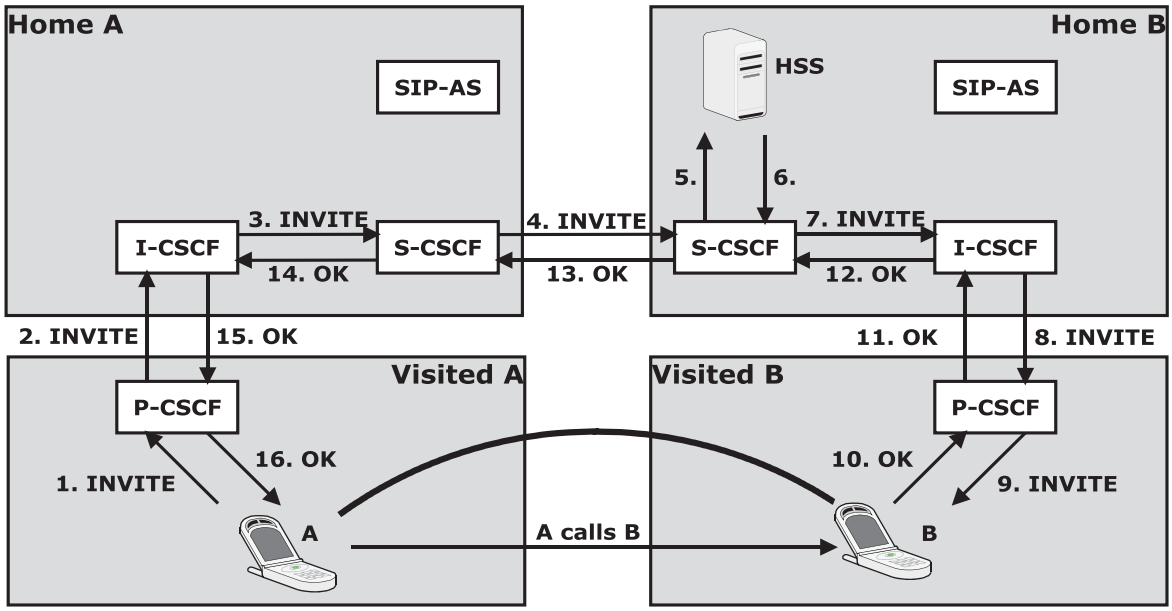
12.2.3 S-CSCF (Serving Call Session Control Function)

S-CSCF představuje v síti IMS registrační SIP Registrar server a SIP Proxy, pracuje s profilem uživatele získaného z HSS a kontroluje, zda probíhající transakce jsou v souladu s profilem. Funkce S-CSCF je v IMS povinná. Základní charakteristika S-CSCF:

- umožňuje registraci čili vykazuje chování SIP Registrar serveru,
- umožňuje aktivně zrušit registraci uživatele v IMS,

- je postaven do cesty probíhajících SIP transakcí (žádost a odpověď) a vykonává nad nimi dohled, zda probíhají v rámci uživatelského profilu, čili vykazuje chování Statefulll SIP –Proxy,
- S-CSCF prvků je obvykle více a uživatel IMS musí být registrován minimálně na jeden.

Na obrázku 8.10 je průběh sestavení spojení v IMS, volající A odesílá INVITE na Outbound SIP-Proxy (P-CSCF), ten je přeposlán na další SIP-Proxy, která ověří, zda požadavek je validní vzhledem k uživateli a odsměruje jej na domovskou SIP Proxy uživatele B (S-CSCF), která zjistí z lokalizační databáze HSS, kde se uživatel B nachází. Následně je INVITE přeposlán na I-CSCF a poté na Inbound SIP-Proxy (P-CSCF), která již žádost o spojení doručí přímo na volaného B. Odpověď je zaslána stejnou cestou jako žádost, ale vlastní spojení již může probíhat napřímo, což závisí na dalších okolnostech (jak je řešen peering mezi operátory a zda je některou ze SIP Proxy použit record-routing, viz. [voz_142]).



Obr. 12.2 Sestavení spojení v IMS

12.3 Ostatní funkce IMS

HSS (Home Subscriber Server) je databáze profilů domácích uživatelů sítě IMS, je to nástupce HLR (Home Location Register) známého z GSM sítí.

SLF (Subscription Locator Function) je jednoduchá databáze pomáhající nalézt správný HSS, který náleží k dotyčnému uživateli. Jeho implementace je nepovinná a je užitečná tehdy, pokud je v IMS síti více HSS serverů.

AS (Application Server) jsou aplikační servery poskytující jednak služby s přidanou hodnotou a nástavbové aplikace k IMS (např. charging, Operation&Maintenance).

MRFC+MRFP (Media Resource Function Control / Processor) poskytují prostředky pro práci s médii (především transcoding). MRFC vykazuje chování jako SIP UA. Komunikuje pomocí SIPu s S-CSCF a řídí MRFP protokolem H.248, může generovat záznamy pro vyúčtování. MRFP zajišťuje zpracování médií (mixování toků, jejich transkódování) a chová se jako Slave ve vztahu k MRFC, jenž jeho řídícím prvkem.

BGCF (Border Gateway Control Function) zajišťuje bezpečné propojení s non-IMS, čili je to prvek zodpovědný za vzájemnou komunikaci IMS s jinými sítěmi a za bezpečnostní opatření (šifrování, obrana proti útokům).

MGCF+MGW (Media Gateway Control Function) a MGW (Media Gateway) je podobná dvojice jako MRFC+MRFG, tentokrát ale MGW navíc disponuje prostředky pro konverzi médií do jiného typu sítě (např. MGW je osazena E1 a umožňuje peering s PSTN).

12.4 Aspekty nasazení IMS

IMS vychází z evoluce telekomunikačních sítí, nepřichází tedy s kompletní výměnou komponentů zajišťujících dnešní hlasové služby, ale s možností nasazení nových technologií bez nutnosti radikální přestavby stávajících sítí. IMS síť by měla umožnit snadnější implementaci služeb jako např. Presence, CTI, Instant Messaging.

IMS je skupina serverů a databází s definovanými funkcemi a otevřenými protokoly. Jelikož staví na otevřených standardech, objevil se koncept IMS už i jako otevřené řešení Open-Source IMS, se kterým přišel berlínský FOKUS (výzkumný institut pro otevřené

komunikační systémy). Koncept IMS otevírá telekomunikačním operátorům cestu k NGN, tato cesta je nutná a pokud v devadesátých letech vznikl zásadní rozdíl mezi operátory, kteří nabízeli mobilní služby a těmi, co je neměli, tak v dalších letech bude signifikantní rozdíl mezi těmi, kteří budou mít a nebudou mít IMS. Lze předpokládat, že uživatelé si velmi rychle na služby IMS zvyknou, budou ovládat nastavení svých komunikačních služeb přes webové portály, řídit svou dostupnost a nedostupnost kalendářem v Outlooku, nastavovat profily umožňující jim efektivněji využívat jejich čas. IMS není produkt, je to otevřená architektura, ve které je potenciál dlouhodobého vývoje, dnes jsme teprve na začátku a hodilo by se říct Caesarovo "*Alea iacta est.*"

V aplikační úrovni je možné vidět budoucí potenciál především v rozvoji služby *Presence*. Provázání plánování činností uživatele a logiky spojování se označuje jako Presence Management, ten dovoluje řízení komunikace na základě uživatelem definovaných profilů anebo naplánovaných aktivit. V praxi to vypadá tak, že naplánování schůzky zanesené v kalendáři MS Outlook způsobí, že veškeré hovory budou končit v hlasové schránce uživatele, v případě naplánované služební cesty budou hovory do kanceláře přesměrovány na mobilní telefon, uživatel bude moci automaticky přepnutý profil pochopitelně ovládat i manuálně z koncového zařízení. Řízení spojovacího systému na základě Presence skýtá rozsáhlé možnosti, jeho výsledkem je zefektivnění komunikace a lze očekávat vývoj nástrojů pro Presence Management.

Obdobně lze najít i další aplikace, které již nalezly uplatnění, budou se tedy rozvíjet a nechybí v portfoliu produktů výrobců IMS, uvedu tři dle mého soudu nejzajímavější. První je *Unified Messaging*, což je vzájemná konverze různých druhů komunikace, např. příchozí fax je konvertován do pdf a odeslán na email uživatele. Druhou aplikací je *CRM* (Customer Relationship Management), která řeší vztahy se zákazníky, například na základě identifikace čísla volajícího zobrazí z databáze důležité informace o volajícím a nabídne přístup na detailnější údaje. Třetí aplikace je stejně jako druhá rovněž typická pro centra volání, a je to *IVR* (Interactive Voice Response), tato aplikace umožňuje průchod informačním hlasovým stromem nejen pomocí tónové volby, ale může být i doplněna systémem pro rozpoznání řeči a ovládána tak lidským hlasem.

Budoucí komunikace se budou potýkat s problémy zabezpečení více než dnes. Klasická

telefonie založena na propojování okruhů nebyla pro útoky tak exponovaná jako IP telefonie. Dosud nejznámější registrovaný útok provedl 23-letý Edwin Pena z Miami, odhadovaná škoda se vyšplhala na 4,5 mil. USD, největší jeho obětí byl VoIP poskytovatel z New Jersey, který v roce 2006 přes svou síť registroval půl miliónu neautorizovaných volání provedených útočníkem, posléze se zjistilo, že jeho obětí bylo dalších 15 VoIP operátorů a Edwin Pena dostal přezdívku „VoIP bandita“. V roce 2008 byly na univerzitách v ČR registrovány dva úspěšné útoky, ve kterých byly útočníky zneužity klíčové komponenty IP telefonie k terminování volání na Kubu. Bezpečnostími aspekty IP telefonie se budeme zabývat snad v další publikaci, autor se této oblasti nyní intenzivně věnuje [voz_147], [voz_146], [voz_145], [voz_143], [voz_138] a [voz_124].