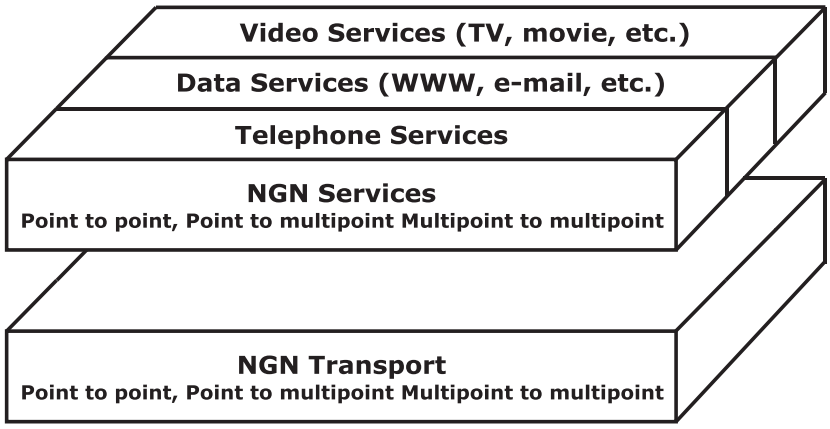
10. Síť nové generace NGN a její obecné principy

Ve druhé polovině devadesátých let začala vznikat koncepce sítě nové generace NGN (Next Generation Network), která byla postavena na myšlence oddělení transportní úrovně telekomunikačních sítí a orientace na technologie s přepojováním zpráv a garancí QoS. Možnost přenášet různé služby v jediné transportní síti s garantovanou kvalitou je pochopitelně efektivnější než provozování separátních sítí pro rozdílné služby [wil], [loj2].



Obr. 10.1 Oddělení služeb a přenosu v NGN dle ITU-T Y.2011

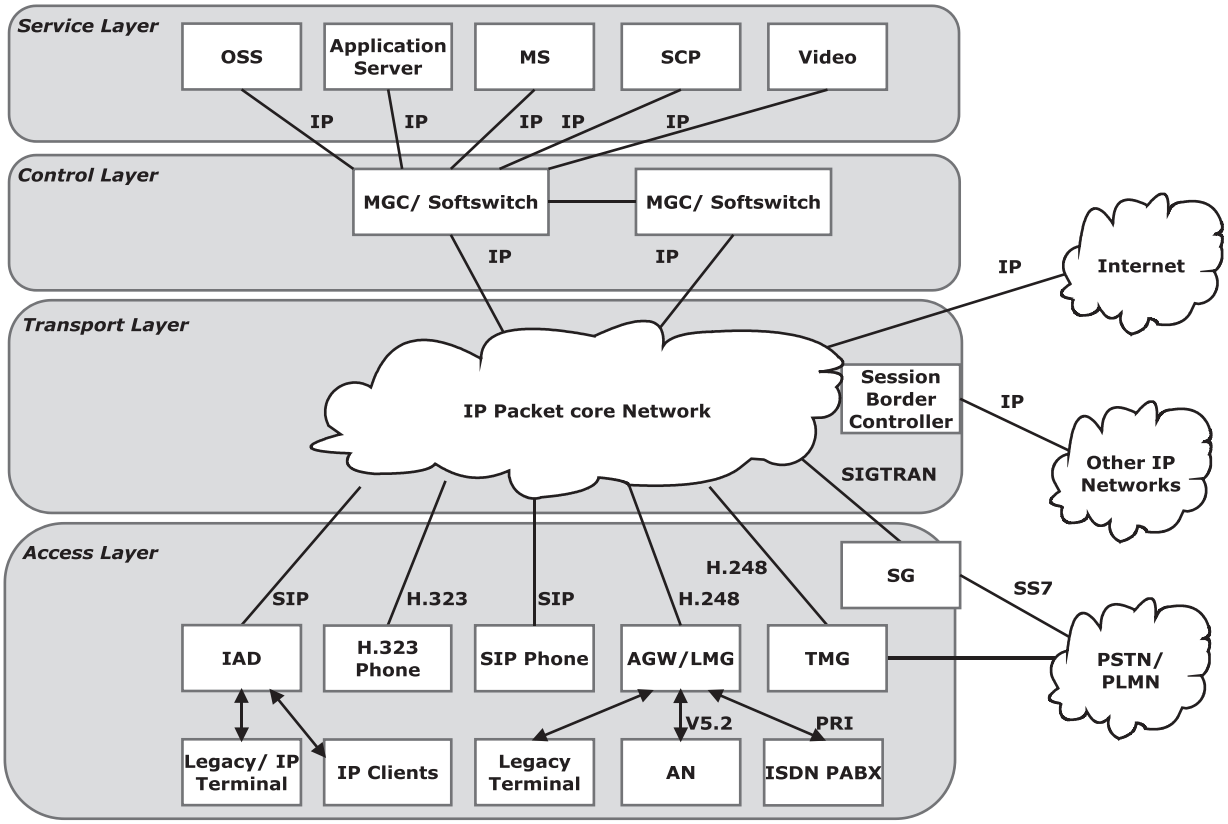
Největší šanci na úspěch měla technologie ATM, ale v dalších letech bylo zřejmé, že propracovanost ATM se příliš odrazila v ceně a flexibilitě, což mělo fatální důsledky na její reálné použití. První systém NGN a zatím jediný, který je v době vydání této publikace standardizován, je IMS (IP Multimedia Subsystem), který byl specifikován koncem roku 2006 studijní skupinou SG 13 v ITU-T Y.2021 (IMS for Next Generation Networks).

10.1 Architektura NGN

Definice NGN dle ITU-T Y.2001 (z prosince 2004):

„NGN je paketově orientovaná síť schopná poskytovat telekomunikační služby a zajistit přístup k širokopásmovým přenosovým technologiím umožňujícím QoS, ve které služby nejsou vázány na použité transportní technologie. NGN poskytuje uživatelům neomezený přístup k poskytovatelům služeb, podporuje mobilitu uživatelů a umožňuje jim zajistit trvalé a všestranně dostupné služby.“

I přes snahu integrovat služby v jedné síti (ISDN) byl v devadesátých letech nepřehlédnutelný trend odděleného vývoje datových sítí. S raketovým rozvojem Internetu bylo koncem 20 st. zřejmé, že počet uživatelů Internetu (4 mld. v roce 2008) jednou překročí počet uživatelů telefonních linek (1,5 mld. v roce 2008) a hlas by měl proto být integrován jako služba v sítích paketově orientovaných. Navzdory revolučním vizím některých společností (např. Cisco Systems) se v praxi ukázala potřeba postupné evoluce, která znamenala dalších deset let práce na standardech a až dnes dochází k masovému nasazování NGN. Byla vyvinuta řada signalizačních protokolů, z nichž se v NGN používají SIP, H.323, MGCP, Megaco/H.248 a Sigtran.



Obr. 10.2 NGN architektura

Zkratky v obr. 10.2:

- AGW Access Gateway, AN Access Network, IAD Integrated Access Gateway,
- LMG Line Media Gateway, MGC Media Gateway Controller, MS Media Server,

- OSS Operation Support Systems,SG Signaling Gateway,SCP Service Control Point
- TMG Trunk Media Gateway, SBC Session Border Controller.

10.1.1 Přístupová úroveň

Přístupová úroveň (Access Layer) NGN architektury obsahuje následující funkce:

- připojení účastníků (Legacy/IP),
- přístupových sítí a pobočkových ústředen (AN/PBX),
- propojení s tel. sítí pevnou a mobilní (PSTN a PLMN).
- zajišťuje konverzi mezi sítěmi s přepínáním paketů a propojováním okruhů

Prvky na přístupové úrovni jsou:

- IP koncová zařízení jako H.323 a SIP telefony či IP PBX (připojené přes SIP nebo H.323 trunk),
- IAD Integrated Access Device je prvek, který poskytuje přístup účastníkům na ADSL/ IPtelefon, analog,
- AGW Access Gateway poskytuje přístup pro analogové účastníky, ISDN, přístupové sítě V5 a ISDN PBX,
- SG Signaling Gateway zabezpečuje signalizační rozhraní mezi IP sítí a SS7 signalizační sítí,
- TMG Trunk Media Gateway zabezpečuje konverzi hlasu pro přenos v IP síti (RTP protokol) a v PSTN/PLMN (PCM), prvek může být integrován v jednom zařízení společně s SG.

10.1.2 Transportní úroveň

Na transportní úrovni by měla NGN nabídnout:

- vysokou spolehlivost,
- propustnost (kapacitu),
- a garanci QoS.

Prvek SBC (Session Border Controller) je hraniční prvek, který poskytuje:

- bezpečné propojení signalizací i médií včetně skrytí infrastruktury důvěryhodné části sítě za jedinou IP adresu (adresu SBC, tzn. nejsou nikde propagovány IP adresy IP core sítě IMS a komunikace probíhá přes SBC)
- podporu klientům za NATem,
- bezpečnost proti útokům (především DoS),
- CAC (Call Admission control) a správu pásma BW Management,
- normalizaci CDR záznamů (Call Detail Record) a podporu systémům pro účtování.

10.1.3 Řídící úroveň

Řídící úroveň na obrázku 10.2 zabezpečuje Softswitch, pro který se používá označení jako MGC (Media Gateway Controller), CS (Call Server) a CA (Call Agents), protokoly, kterými komunikuje, jsou znázorněny na obr. 10.3. Softswitch je klíčovým prvkem v NGN architektuře zajišťuje tyto funkce:

- řízení volání,
- řízení přístupu a komunikace s MG (Media Gateway), SBC a SG,
- alokuje zdroje v síti,
- zpracování signalizace,
- Autentizace a autorizace,
- Směrování,
- Generování záznamů o spojeních (CDR - Call Detail Record).

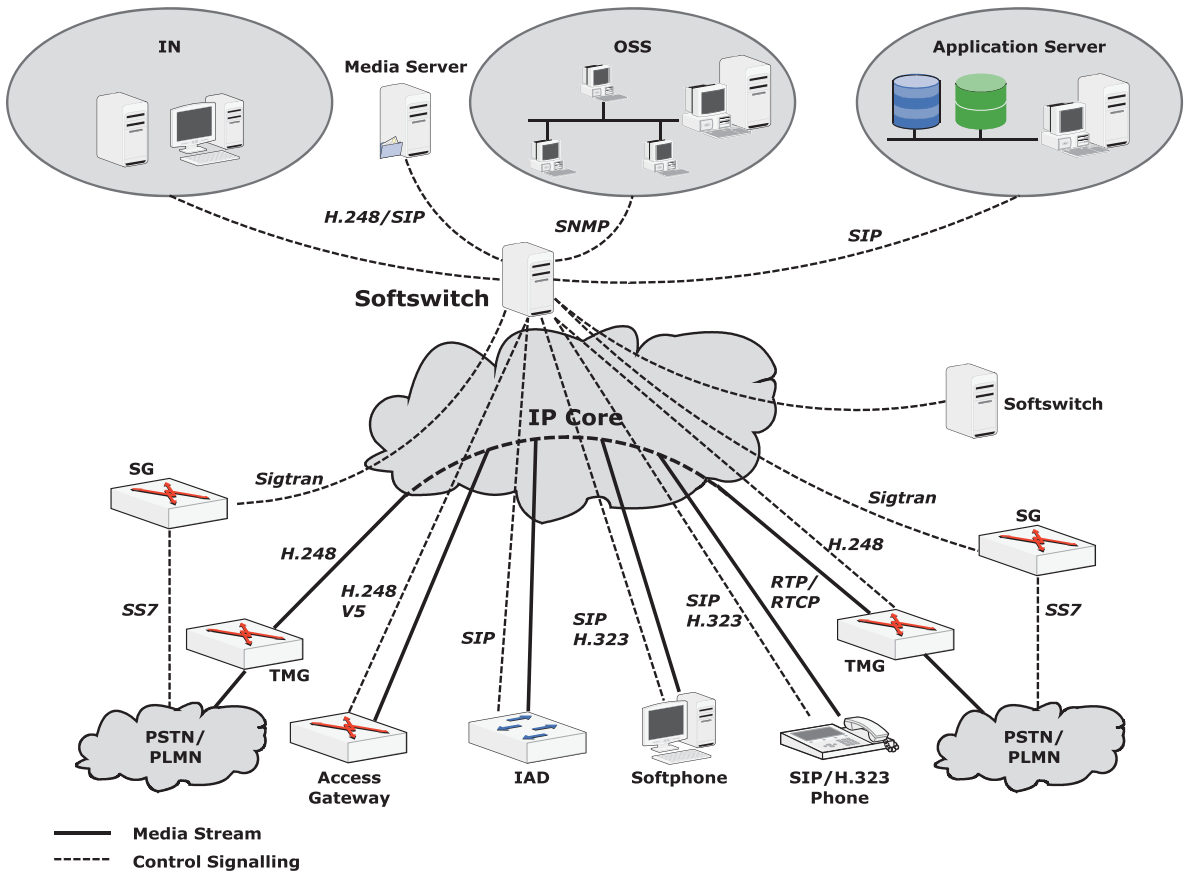
10.1.4 Úroveň služeb

Tato úroveň poskytuje služby s přidanou hodnotou a podpůrné provozní funkce. Obsahuje následující komponenty:

- OSS Operation Support System zahrnuje integrovaný systém účtování (charging

system) a systém síťové správy a provozu (Network Operation & Management System),

- Application server poskytuje aplikační rozhraní API pro služby inteligentní sítě (IN) a pokročilé služby, API musí být otevřené, aby bylo možné použít aplikace i třetí strany,
- MS Media Server zpracovává toky médií, umožňuje audio ohlášky, vytváření IVR stromů (Interactive Voice Response), konference, tóny,
- SCP Service Control Point je klíčovou komponentou inteligentní sítě zodpovědnou za data účastníků a logiku služeb,
- Video server je prvek poskytující videokonference a jejich management.



Obr. 10.3 Komponenty a protokoly NGN

10.2 Portfolio služeb NGN

Portfolio služeb NGN můžeme ukázat na konkrétním případu implementace u telekomunikačního operátora Telefónica O2, spuštění služeb proběhlo v roce 2008. Původně bylo vybráno řešení firmy Siemens, ale projekt byl ukončen po problémech s implementací služeb a jako dodavatel byl vybrán Ericsson.

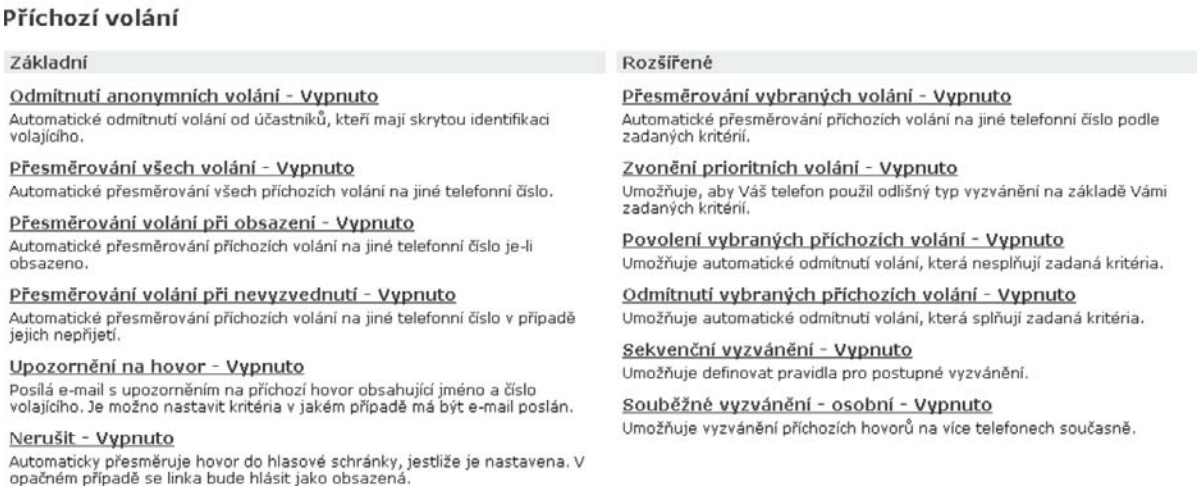
V současné době TO2 nabízí dvě řešení, a to VoIP Connect a VoIP Centrex. První z nich nabízí hlasovou službu simulující služby PSTN sítě s rozšířením portfolia o VoIP a umožňuje:

- připojení PBX se sign. DSS1 na PRI , BRI, se signal. K+MFC, K+DEC na E1,
- POTS (signalizace U),
- připojení IP PBX signalizací H.323 a SIP,
- připojení koncových zařízení (telefonů, IP telefonů, Faxů, Terminal adapterů) na analogovém rozhraní, BRI a IP koncových zařízení protokolem SIP,

VoIP Centrex je privátní hlasová služba zajišťovaná poskytovatelem sítě s využitím kombinace datových a internetových produktů a nabízí služby:

- Hostovaná PBX s privátním číslovacím plánem,
- Web portál a Hlasový portál,
- Unified Messaging a Instant Messaging,
- Presence (identifikace stavu uživatele),
- Videokonference,
- Telefonní seznamy, s využitím LDAP, adresář přátel (Buddy list),
- Call centra,
- Integrace komunikačních prvků do MS Outlook,

TO2 implementovala v NGN přes padesát doplňkových služeb.



Obr. 10.4 Web portál NGN služby TO2

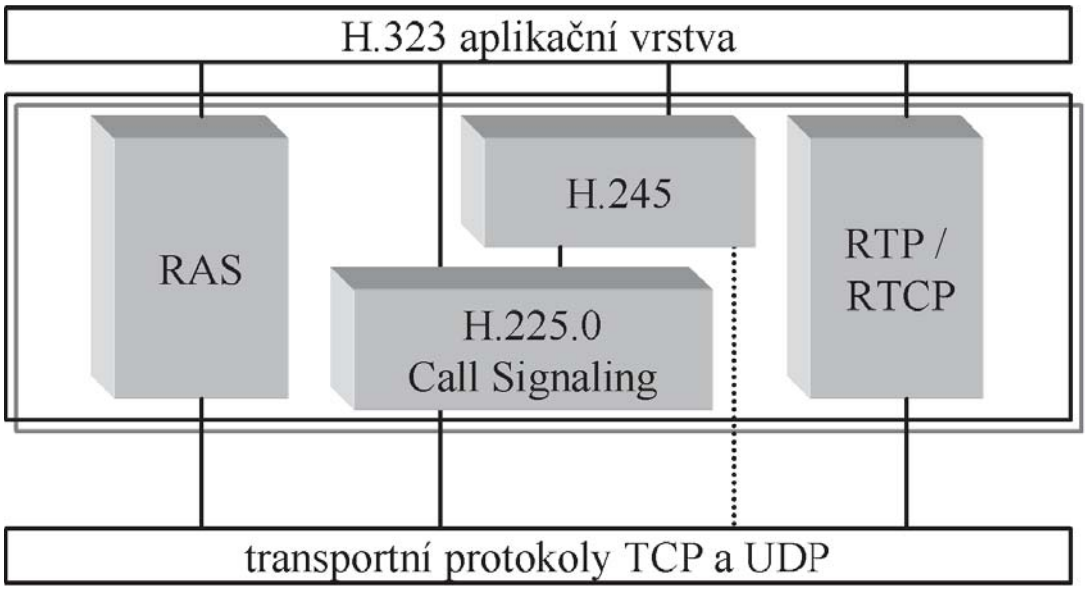
Implementace NGN je aktuální u mnoha velkých telekomunikačních operátorů, jejich investice jsou dlouhodobé a lze očekávat, že NGN technologie budou tématem minimálně dalších deseti let. Na trhu se již profilovali různí výrobci a vize. Například strategická vize firmy Siemens se jmenuje LifeWorks a vystihuje další směr komunikací. V jejich vizi vyvíjejí nástroje, se kterými by uživatelé měli absolutní kontrolu nad hranicemi pracovního a soukromého života. Zabezpečená komunikace integrovaná do jediného nástroje (jedno zařízení – fixed/mobile, home/work) umožňující univerzální způsoby komunikace (Unified Messaging – hlas. vzkaz do emailu, fax odeslaný emailem, atd..) a možnost stanovovat, kdy a kdo se na uživatele bude moci dovolat (buddy list, presence management), ať bude kdekoliv (mobilita), to jsou vize, které budou motorem dalších inovací..

11. Signalizační protokoly v NGN

Následující kapitola přináší pouze letmý přehled vlastností signalizačních protokolů v NGN, neboť jsou obsahem předmětu Voice over IP přednášeného v zimním semestru, ke kterému byly vydány skripta se stejným názvem [voz_142].

11.1 ITU-T H.323

Standard H.323 zastřešuje řadu doporučení a je určen pro Multimediální komunikaci na sítích s přepojováním paketů. První verze byla uvolněna roku 1996, aktuálně je vydávána sedmá verze (rok 2009). Média jsou přenášeny RTP protokolem (Real Time Protocol), který je postaven nad nespolehlivým UDP.



Obr. 11.1 H.323 protokolový koncept

Signalizace, s výjimkou RAS, je přenášena spolehlivě přes TCP. Pro řízení spojení jsou důležité protokoly:

- RAS (Registration, Admission and Status) je komunikační protokol pro Gatekeeper (dále jen GK), pokud jakékoliv zařízení (terminál, brána, další gatekeeper) komunikuje s GK, tak používá RAS zprávy,
- H.225.0/Q.931 protokol v H.323 je nazýván jako signalizace volání (Call signaling)

a obsahuje zprávy pro inicializaci i ukončení spojení (SETUP, ALERTING, CONNECT, RELEASE COMPLETE, atd..), koncepce byla převzata z ISDN,

- H.245 je označován jako protokol řízení médií (media control), obsahuje procedury pro vyjednání kodeků a portů pro RTP toky, pro každý směr zvlášť.

11.1.1 H.323 architektura

H.323 infrastruktura je logicky rozdělena do zón. Zóna je množina zařízení řízených jedním GK [col]. V H.323 rozeznáváme následující komponenty:

- Endpoint (koncový bod, zařízení), tím může být MCU (Multiconference Unit), brána GW nebo terminál TE,
- Gatekeeper (řídící prvek sítě).

11.1.2 Gatekeeper

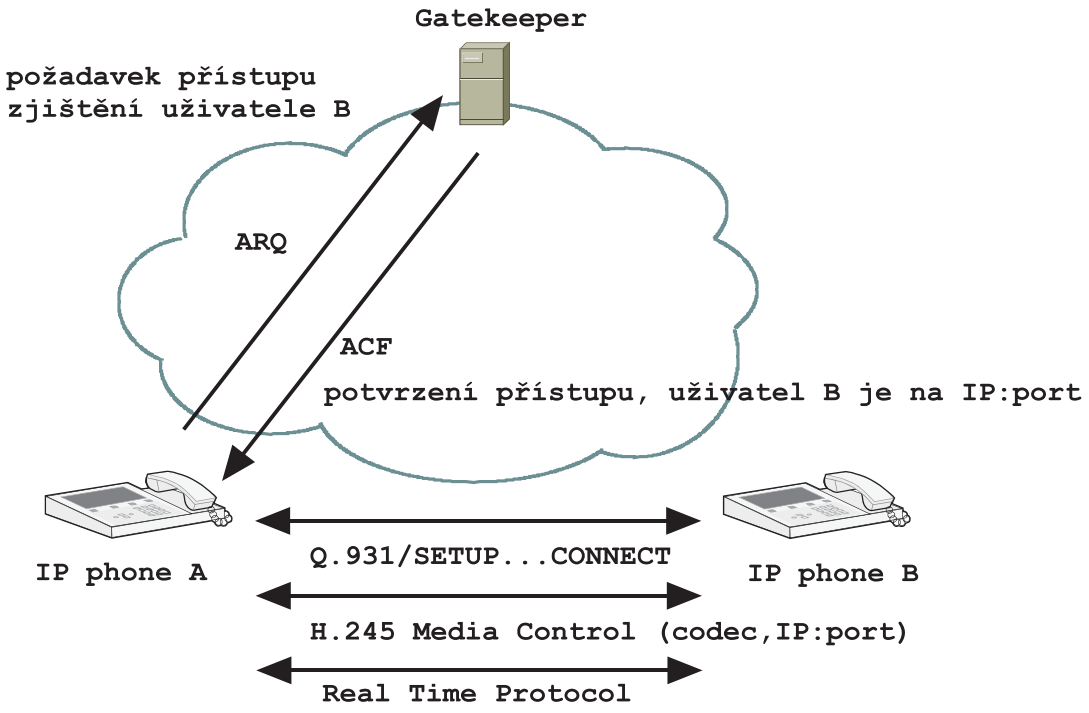
Gatekeeper je řídicím prvkem H.323 koncových bodů (terminal, gateway, MCU). Dle standardu H.323 musí zajišťovat následující funkce:

- podpora signalizace RAS (Registration/Administration/Status). Pomocí signalizace RAS se realizuje řízení přístupů k prostředkům sítě,
- řízení přístupu (Admission Control), zajišťuje autorizovaný přístup pomocí zpráv ARQ/ACF/ARJ (Admission Request/Confirm/Reject) definovaných v signalizaci RAS (Registration, Admission and Status Signaling),
- překlad adres (Address Translation) mezi E.164 číslem a IP síťovou adresou nebo mezi jmenným identifikátorem URI (jméno@doména) a IP,
- řízení přidělování kapacity pásma (Bandwidth Control). Řízení pásma dle požadavků z koncových bodů pomocí zpráv BRQ/BCF/BRJ signalizace RAS,
- řízení spojení (Call Control), zpracování zpráv nebo jejich směrování,
- řízení zón (Zone Management) zajišťuje řídicí funkce pro všechny registrované koncové body H.323 zóny. Koncové terminály a VoGW jsou rozděleny do zón, které představují distribuovanou strukturu GK.

11.1.3 RAS

RAS signalizace zajišťuje komunikaci s GK pomocí zpráv (pouze vybrané):

- RRQ/RCF/RRJ Registration Request/Confirm/Reject, Registrace,
- URQ/UCF/URJ Unregister Request/Confirm/Reject, Odregistrování,
- ARQ/ACF/ARJ Admission Request/Confirm/Reject, Přístup,
- LRQ/LCF/LRJ Location Request/Confirm/Reject, Lokalizace mezi zónami,
- BRQ/BCF/BRJ Bandwidth Request/Confirm/Reject, Rezervovat pásmo,
- DRQ/DCF/DRJ Disengage Request/Confirm/Reject, Ukončení spojení .



Obr. 11.2 Mechanizmus navázání spojení v H.323

Uživatel A (IP phone A) odesílá ARQ a žádá GK (Gatekeeper) o sdělení informace, kam má zaslat SETUP pro uživatele B (IP phone B). GK ověří uživatele A a v databázi zjistí, na které IP adrese a portu je registrován uživatel B, informaci pošle zpět v ACF. Následně už probíhá Q.931 (Call signaling) standardním způsobem SETUP, CALL

PROCEEDING, ALERTING, CONNECT. Vyjednání médií zajistí signalizace H.245, která může být přenášena odděleně od Q.931 (Slow Start) nebo částečně v Q.931 (Fast Connect / procedura Open Logical Channel uvnitř Fast Start prvků) anebo celá tunelována v Q.931 (v případě potřeby se použijí zprávy FACILITY). Při ukončení spojení se nejdříve zavře relace na H.245, potom Q.931 pomocí RELEASE COMPLETE a nakonec RAS pomocí DRQ/DCF.

11.2 IETF SIP

SIP (Session Initiation Protocol) byl vyvíjen od roku 1996, v roce 1999 byl předložen ve formě navrhovaného standardu (Proposed Standard) v RFC 2543 a ihned zaujal svou jednoduchostí. V květnu roku 2002 byl uvolněn standard RFC 3261, který obsahuje jádro dnes používaného SIPu, kde je specifikováno použití šesti základních metod. Další rozšíření jsou obsahem více než osmdesáti RFC, které se SIPem souvisejí. **SIP dnes už jednoduchý není**, jednoduchostí vynikal před šesti lety.

SIP je signalizační protokol umožňující sestavení, modifikaci a ukončení relace s jedním nebo více účastníky. Pro popis vlastností relace se používá ve spojení se SIPem nejčastěji SDP (Session Description Protocol) a samotný hlas se přenáší v RTP. SIP je textově orientovaný protokol s rysy podobnými HTTP a SMTP protokolu. Klient posílá požadavky na server, který zasílá odpovědi jako u HTTP, v hlavičkách najdeme položky From, To či Subject jako u mailové komunikace pomocí SMTP. Zatímco u H.323 jsou entity rozděleny do zón obsluhovaných GK (Gatekeeperem) a spojení tedy probíhá buď uvnitř zóny anebo mezi zónami (mezi GK), tak SIP entita je vázána k doméně obsluhovanou SIP Proxy [bar], [sin].

Pro aplikační protokol SIP se standardně používá UDP transport na portu 5060, ale lze použít i TCP nebo TLS. SIP entity jsou identifikovány použitím SIP URI (Uniform Resource Identifier), řekli bychom jednoduše jmennými identifikátory, jejich obecný tvar je uveden níže.

sip:user:password@host:port;uri-parameters?headers

11.2.1 Prvky SIP architektury

Ačkoliv v nejjednodušší konfiguraci je možné použít dva UA (v terminologii H.323 jde o Endpoint) posílající si navzájem SIP zprávy, typická SIP síť bude obsahovat více než jeden typ prvků. Základními SIP prvky jsou:

- UA, user agent složený z klientské UAC (odesílá žádosti a přijímá odpovědi) a serverové části UAS (přijímá žádosti a odesílá odpovědi),
- SIP Proxy (směruje), Registrar (registruje), Redirect (pomáhá při přesměrování) a Location (lokalizační databáze) servery.

Je zřejmé, že návrh SIPu umožňuje dekompozici úloh do jednotlivých prvků, v praxi jsou ale zmíněné komponenty většinou použity jako logické části **SIP serveru**, jelikož je často efektivní je provozovat společně na jednom HW. Často je v SIP serveru použit speciální typ **B2BUA** (Back to Back User Agent), jenž na rozdíl od SIP Proxy, která jen směruje zprávy s minimálními úpravami v hlavičkách, provede konstrukci nové hlavičky a defacto vytvoří nové spojení k cíli. Takovéto chování je výhodné pro poskytovatele IP telefonie, neboť B2BUA mu umožňuje absolutní kontrolu nad konstrukcí SIP zpráv, na druhou stranu znamená podstatně nižší výkonnost oproti SIP Proxy.

11.2.2 SIP žádosti a odpovědi

Žádost a odpověď jsou dva základní typy SIP zpráv. Žádosti neboli metody jsou obvykle užívány k inicializaci procedury (sestavení, aktualizaci či ukončení spojení). V jádru SIP protokolu je dle RFC 3261 specifikováno šest metod, které jsou následující:

- INVITE je žádost o inicializaci spojení nebo změnu parametrů již probíhajícího spojení (re-INVITE),
- ACK je metoda potvrzující přijetí konečné odpovědi na žádost INVITE,
- BYE je zpráva užívána k ukončení sestaveného spojení,
- CANCEL se používá ke zrušení sestavovaného spojení,
- REGISTER je žádost k registraci či odregistrování, váže se logická URI uživatele s

jeho fyzickým umístěním (IP adresa a port), konkrétně jde o položky FROM a CONTACT ze SIP hlavičky,

- OPTIONS je speciální typ metody k zjištění vlastností (možností) SIP entity.

Kromě výše uváděných šesti základních metod existují i další žádosti, které byly definovány dodatečně v některých následujících RFC:

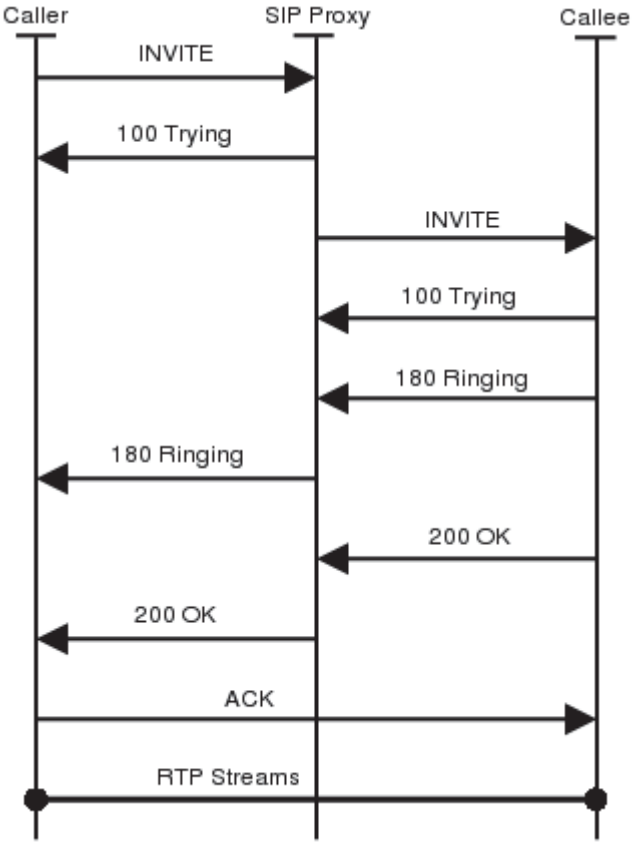
- přenos informací během relace INFO, RFC 2976,
- potvrzení dočasné (1xx) odpovědi PRACK, RFC 3262,
- přihlášení k upozornění na událost SUBSCRIBE, RFC 3265,
- informace o události NOTIFY, RFC 3265,
- aktualizace stavu relace UPDATE, RFC 3311,
- pro instant messaging byla definována metoda MESSAGE, RFC 3428,
- pro řízení spojení třetí stranou slouží REFER, RFC 3515,
- aktualizaci prezence zajišťuje PUBLISH, RFC 3903.

Každá žádost musí být zodpovězena, výjimkou je metoda ACK, což je žádost, která má význam potvrzení doručení odpovědi na INVITE. Kód odpovědi je celé číslo z rozsahu 100 až 699 a označuje typ odpovědi. Odpovědi začínající 1xx jsou pouze informativní a po nich následuje formální odpověď z rozsahu 2xx-6xx. Celkem je definováno 6 tříd odpovědí:

- 1xx jsou dočasné informativní odpovědi, (100 Trying, 180 Ringing, 183 Session Progress),
- 2xx jsou pozitivní finální odpovědi, (200 OK, 202 accepted),
- 3xx odpovědi jsou užívány k přesměrování (301 Moved Permanently, 302 Moved Temporarily),
- 4xx jsou negativní konečné odpovědi indikující problém na straně klienta (401 Unauthorized, 407 Proxy Authentication Required, 415 Unsupported Media Type,

486 Busy Here),

- 5xx znamenají problém na straně serveru (501 Not Implemented, 503 Service Unavailable),
- 606 Not Acceptable (600 Busy Everywhere, 603 Decline, 604 Does Not Exist Anywhere).



Obr. 11.3 Typické sestavení spojení v SIP signalizaci

UAC inicializuje spojení odesláním žádosti INVITE na SIP Proxy, ta je přeposlána adresátovi, 100 Trying indikuje zahájení zpracování žádosti INVITE a 180 Ringing vyzvánění u volaného. Odpověď 200 OK je zaslána při přihlášení volaného a následně je potvrzena metodou ACK. Vlastnosti médií jsou vyjednány pomocí SDP protokolu, jeho položky jsou přenášeny v těle SIP zpráv, obvykle INVITE (návrh SDP) a 200 OK (odpověď SDP), ale existují i jiné způsoby (např. Early media, SDP již ve 183 nebo 180).

Pokud jde o volání mezi různými doménami, tak při vyhledávání cílové příchozí

SIP Proxy (Inbound) se zpravidla používají SRV záznamy v DNS, které uchovávají informaci, který konkrétní stroj poskytuje hledanou službu v doméně. Lze se tedy DNS např. dotázat, kdo poskytuje službu SIP na protokolu UDP v doméně vsb.cz a dostaneme odpověď, že se jedná o stroj asterisk.vsb.cz, na který SIP Proxy odešle INVITE adresující v cílové URI uživatele z dané domény.

11.2.3 Popis polí SIP žádosti

Žádosti jsou obvykle užívány k registraci uživatele, sestavení, modifikaci či ukončení spojení anebo může jít o další služby (presence, instant messaging). Odpovědi jsou užívány k potvrzení přijetí žádosti a její vyřízení, obsahují konkrétní status. Typická SIP žádost vypadá následovně:

Request-Line: INVITE sip:0738331699@asterisk.vsb.cz SIP/2.0
Via: SIP/2.0/UDP 158.196.192.32;branch=z9hG4bK9ec4c0248acd48724710d7;rport
From: "SJphone" <sip:7002@asterisk.vsb.cz>;tag=27df31582de
To: <sip:0738331699@asterisk.vsb.cz>
Contact: <sip:7002@158.196.192.32>
Call-ID: C317880624584EB9B1443F8B448CC2830x9ec4c020
CSeq: 2 INVITE Max-Forwards: 70
User-Agent: SJphone/1.65.377a (SJ Labs) Content-Length: 321
Content-Type: application/sdp

(v): 0
(o): - 3428274950 3428274950 IN IP4 158.196.192.32 (s): SJphone
(c): IN IP4 158.196.192.32 (t): 0 0
(m): audio 49162 RTP/AVP 18 3 8 0 (a): rtpmap:18 G729/8000
(a): rtpmap:3 GSM/8000 (a): rtpmap:8 PCMA/8000 (a): rtpmap:0 PCMU/8000

První řádek nám říká, že se jedná o zprávu INVITE, jež je užívána k sestavení spojení. URI na prvním řádku *sip:0738331699@asterisk.vsb.cz* se nazývá Request URI a obsahuje URI dalšího skoku zprávy (next hop, směruje se dle **RURI**). V tomto případě bude hostitelem *asterisk.vsb.cz* a hledá se uživatel 0738331699.

SIP žádost obsahuje v hlavičce jedno nebo více polí ***Via***, jež jsou použity k záznamu cesty žádosti. Následně jsou užívány ke směrování SIP odpovědí přesně takovou cestou, jakou byly odeslány. Naše INVITE zpráva obsahuje jedno pole Via, to bylo vytvořeno UA, který odeslal žádost. Z pole Via můžeme říct, že odpověď bude

doručena UA na IP adresu 158.196.192.32 a port 5060.

Pole hlavičky ***From*** **a** ***To*** identifikuje iniciátora volání (volající) a příjemce (volaného). Pole From obsahuje parametr *tag*, který slouží jako identifikátor dialogu a bude popsán později.

Pole hlavičky ***Call-ID*** je identifikátor dialogu a jeho cílem je identifikovat zprávy náležející jednomu volání. Takovéto zprávy mají stejný identifikátor Call-ID.

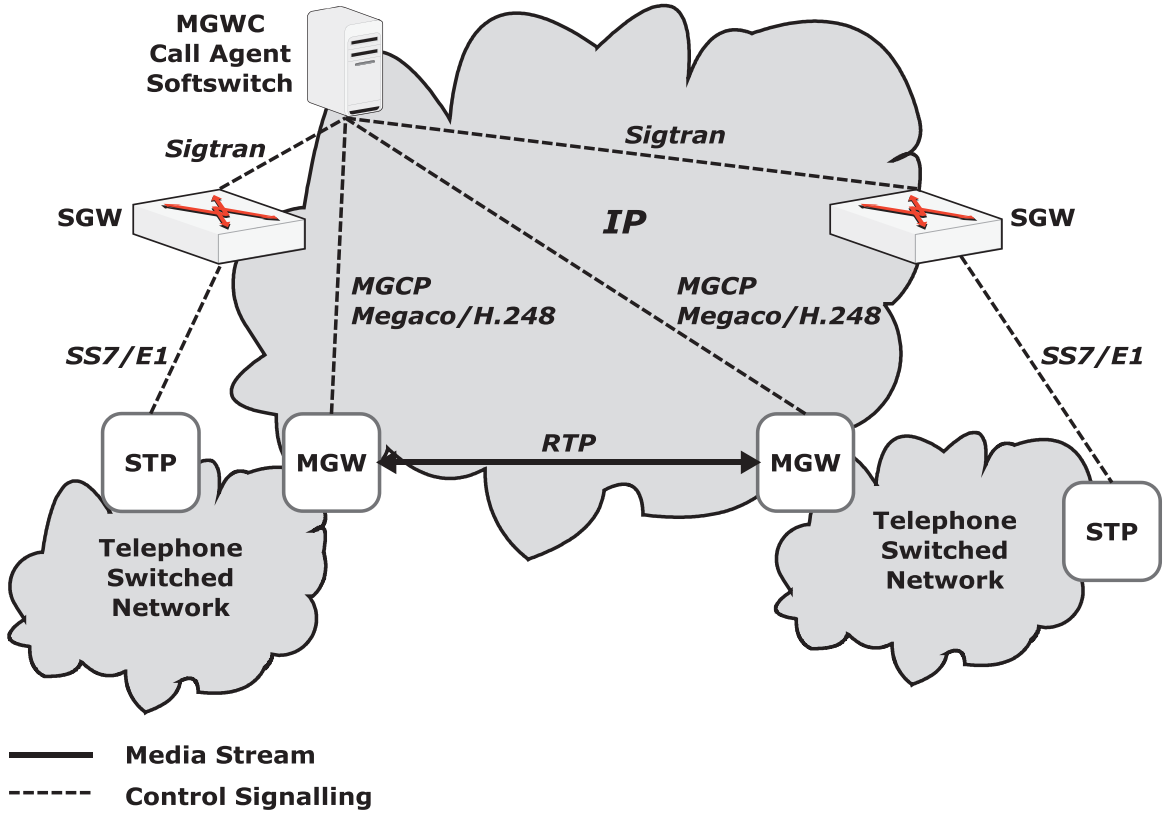
V rámci dialogu jsou jednotlivé žádosti očíslovány v poli ***CSeq***. Protože žádosti mohou být odeslány nespolehlivým přenosem, může docházet k opakováním a pořadové číslo je nutné, aby příjemce mohl detekovat opakování a správně tak selektovat žádosti.

V SIP hlavičce je dále pole ***Contact*** obsahující IP adresu a port, na kterém odesílatel očekává další žádosti odesílané volaným, obě strany si vymění své kontakty v žádosti a odpovědi a pokud bude chtít jedna ze stran poslat další požadavek, např. ukončení spojení BYE, tak nemusí posílat žádost na SIP Proxy, ale pošle ji přímo. Samozřejmě že je možnost ovlivnit i cestu dalších žádostí v dialogu, ale to si vysvětlíme v dalších kapitolách.

Hlavička zprávy je oddělena od těla zprávy prázdným řádkem. Tělo zprávy žádosti INVITE obsahuje popis médií vyhovující odesílateli a kódované v ***SDP***. Z SDP jsme se dozvěděli, kdo poslal nabídku SDP a na které IP má být tok médií ukončen. A co se týče vlastní nabídky, tak ta obsahuje čtyři kodeky seřazené dle preferencí G.729, GSM, PCM (A-law) a PCM (μ-law).

11.3 MGCP a Megaco/H.248

MGCP je IETF protocol, který byl vydán v roce 1999 jako informativní RFC 2705 a dotažen do finální podoby standardního doporučení byl až v roce 2003 v RFC 3435. Z MGCP vychází protokol Megaco/H.248, přičemž Megaco je označení IETF a H.248 je značení ITU-T pro stejný standard. První verze H.248 byla uvolněna v roce 2000, nyní je třetí verze z roku 2005.



Obr. 11.4 Obecný model použití protokolů MGCP či Megaco/H.248

Na obr. 8.8 je znázorněno typické použití protokolu MGCP či Megaco/H.248. MGCP se využívá k ovládání MGW, signalizace SS7 je přenesena pomocí protokolu Sigtran ze signalizační brány SG, řídícím prvkem je MGWC, přes který procházejí veškeré signalizační toky [col].

11.3.1 Prvky MGCP architektury

Protokoly MGCP a Megaco/H.248 jsou typu Master/slave (na rozdíl od H.323 či SIPu) a z toho vychází i koncepce prvků:

- Media Gateway (MGW) konvertuje média na formát vyžadovaný jinou sítí,
- MGWC (Media Gateway Controller) řídí prvky MGCP architektury, používají se i termíny Call Agent (CA) nebo Softswitch, entita zajišťuje zpracování volání, řízení komunikace a ovládá veškeré dalších prvky, se kterými má vztah Master/Slave,
- Signaling Gateway (SGW) umožňuje připojení do signalizační sítě SS7.

11.3.2 Zprávy MGCP

Protokol používá zprávy typu command/response CMD/ACK (NACK) na transportním UDP protokolu. Zprávy typu CMD jsou následující:

- EPCF (Endpoint Configuration), CA>MG, dává GW instrukce k nastavení kódování na straně linkového rozhraní (směrem do PSTN, ISDN, ...),
- RQNT (Notification Request), CA>MG, dává GW instrukce k dohledu specifických událostí a instruuje jak k těmto událostem generovat signály,
- NTFY (Notify), MG>CA, MG dává CA instrukce k dohledu specifických událostí,
- CRCX (Create Connection), CA>MG, CA požaduje vytvořit spojení přes GW mezi dvěma endpointy,
- MDCX (Modify Connection), CA>MG, CA vyžaduje změnit parametry týkající se sestaveného spojení,
- DLCX (Delete Connection), CA>MG a MG>CA, umožňuje zrušit existující spojení, ACK vrací statistiky volání,
- AUEP (Audit EndPoint), CA>MG, monitoruje status endpointu,
- AUCX (Audi Connection), CA>MG, monitoruje status spojení,
- RSIP (RestartInProgress), MG>CA, MG sděluje CA o stavu v provozu a mimo provoz.

Každý příkaz musí být zodpovězen, odpověď vrací návratový kód indikující stav vyřízení příkazu. Tyto kódy jsou součástí RFC 3661 a mají rozsah 000-999:

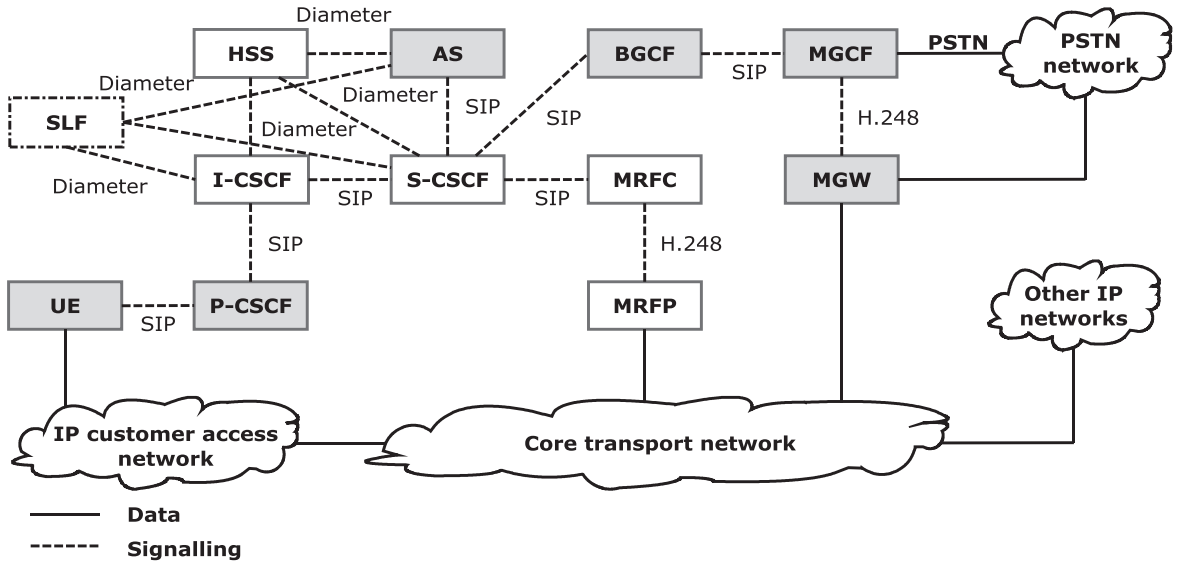
- 000-099 Response acknowledgement, potvrzení odpovědi, (např. 000 - jde o potvrzení po přijetí dočasné odpovědi, je použit 3-way handshake),
- 100-199 Provisional response, dočasná neboli prozatímní odpověď informující o průběhu vyřizování požadavku (např. 100 – transaction in progress oznamující vyřizování anebo 101 – transaction has been queued oznamující zařazení požadavku do fronty),
- 200-299 Successful completion je úspěšné dokončení, tuto odpověď vidíme

nejraději,

- 400-499 Transient error, jedná se o přechodnou chybu, kterou může být např. 401 – phone allready off-hook oznamující stav obsazeno anebo 404 – insufficient bandwith indikující nedostatek pásma,
- 500-599 Permanent error, trvalá chyba např. 500 – unknown endpoint oznamující neznámý cíl anebo 504 – unknown or unsupported command indikující neznámý či nepodporovaný příkaz,
- 800-899 Package specific response codes oznamuje specifické kódy (nestandardní),
- 900-999 Reason codes, jedná se o důvody chyb např. 901 – endpoint taken out of service oznamující, že koncový terminál je mimo provoz anebo 903 – QoS resource reservation was lost indikuje nemožnost garantovat kvalitu.

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,

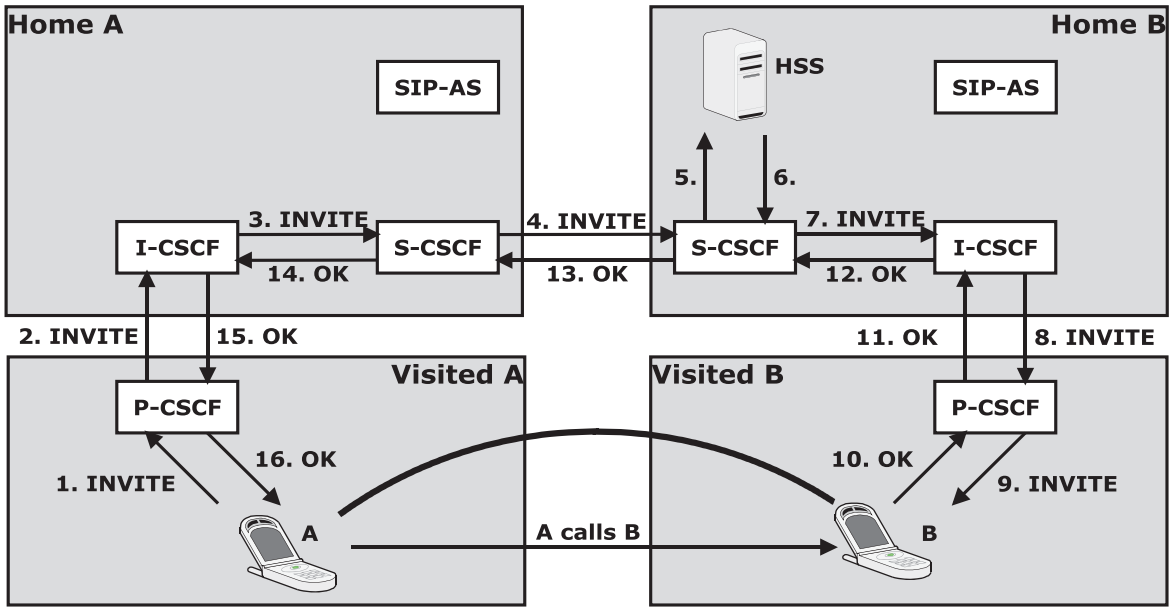
12.2.3 S-CSCF (Serving Call Session Control Function)

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].

13. Spojování v mobilních sítích

Koncept buňkové (celulární) sítě byl vytvořen v Bellových v laboratořích v šedesátých letech, přesto první rozsáhlejší nasazení započalo až v osmdesátých letech v analogovém systému NMT (Nordic Mobile Telephony) označovaném jako 1G (první generace) a v devadesátých letech s příchodem digitálního systému GSM (2G) již můžeme hovořit o masovosti využívání. V roce 2012 při populaci 7 mld. obyvatel byl evidován přibližně stejný počet SIM karet.

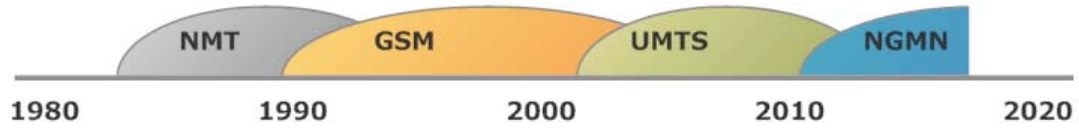
GSM is now in more countries than McDonalds.

(Mike Short, 1996)

V sítích 2G bylo umožněno zasílání SMS a data byly řešeny pomocí CSD (Circuit Switched Data) s max. rychlostí 9,6 kbit/s, datové přenosy byly zpoplatněny dle doby sestaveného spojení. Platba dle objemu přenesených dat anebo paušálem za datovou službu se objevila se zavedením GPRS technologie (General Packet Radio Service) marketingově označované jako 2,5G s rychlostí 20 kbit/s na slot, při konfiguraci mobilní stanice 4+1 (4 sloty downnlink a 1 slot uplink) lze dosáhnout 80 kbit/s.

Další vylepšení GSM přinesla 2,75G s technologií EDGE (Enhanced Data Rates for GSM Evolution), zatímco při použití GMSK modulace (Gaussian Minimum Shift Keying) v GPRS je rychlost modulační rovna přenosové, tak u EDGE je zavedeno osmifázové klíčování 8-PSK (8 Phase Shift Keying), kde tři po sobě následují bity mapovány do jednoho symbolu. EDGE poskytuje na jeden timeslot přenosovou rychlost maximálně 59,2 kbit/s, tzn. v konfiguraci mobilní stanice 4+1 by to bylo 236,8 kbit/s.

Třetí generace 3G je označována síť s technologií UMTS (Universal Mobile Telecommunication System), která původně nabízela přenosové rychlosti pro data 384 kbit/s, podstatné vylepšení přináší HSDPA (High-Speed Downlink Packet Access) s modulací QPSK a 16-QAM s teoretickou rychlostí přenosu 14,4 Mbit/s (3,5G) a s možností s možností povýšení na HSDPA+ (s využitím Multiple Input Multiple Output (MIMO) s rychlostí až 84,4 Mbps. Aktuálně se nasazuje nová generace 4G NGMN (Next Generation Mobile Networks) s technologií LTE (Long Term Evolution), evoluce je zachycena na obr.13.1.



Obr. 13.1 Evoluce technologií.

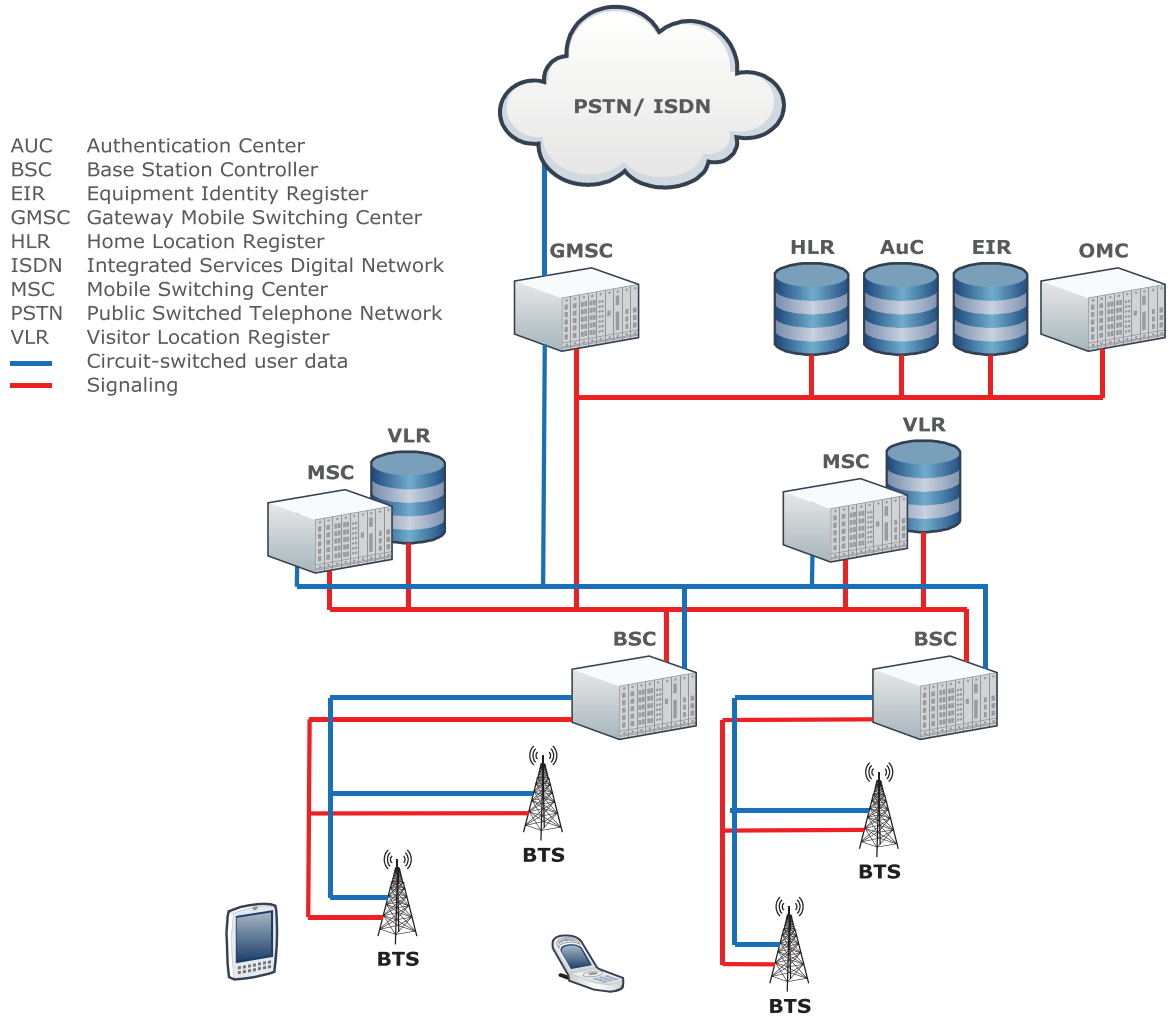
Princip buňkové sítě spočívá v rozdělení území na mnoho dílčích částí (buněk) se základnovými stanicemi, mezi které se rozdělí dostupné frekvence tak, aby bylo možné stejnou frekvenci základnové stanice použít vícekrát, tzn. podmnínkou je dodržet určitou vzdálenost mezi buňkami se stejnými kmitočty z důvodu interference. V buňkových sítích se obecně používají tři metody přístupu:

- FDMA (Fequency Division Multiplex Access), frekvence je rozdělena do pásem a každé z nich je přiřazeno určité stanici, mezi těmito stanicemi není zapotřebí žádné koordinace či synchronizace, na druhou stranu je FDMA neefektivní, ačkoliv stanice nevysílá, tak její část spektra nemůže být použita jinými stanicemi.
- TDMA (Time Division Multiple Access), každé stanici je povoleno vysílat pouze v přiřazeném časovém intervalu, přiřazování se děje periodicky a tato perioda se nazývá cyklus (rámec). V rámci jednoho cyklu může být stanici přiřazen jeden i více časových intervalů TSL (timeslot). Stanice musí být synchronizovány a každá stanice musí mít fixní alokaci TSL, ať již vysílá či nikoliv.
- CDMA (Code Division Multiple Access), každá stanice má přiřazenou určitou kódovou sekvenci modulovanou na nosné (ortogonální kódy), všechny využívají identickou frekvenci, dobrá odolnost proti rušení i odposlechu.

13.1 Komponenty GSM/GPRS sítě

GSM síť se skládá z následujících prvků, viz. obr. 13.2: MS (Mobile Station), SIM (Subscriber Identity Module), BTS (Baset Transiever Station), BSC (Base Station Controller), MSC (Mobile service Switching Center), HLR (Home Location Register), VLR (Visitor Location Register), EIR (Equipment Identity Register), AuC (Authentication Center), OMC (Operation and Maintenance Center) a GMSC (Gateway Mobile Switching Center). Buňková síť obsahuje desítky až tisíce buněk pokrývajících oblast s dosahem

obvykle mezi 500m až 35km. Rádiová část GSM sítě obsahuje základnové stanice BTS, ty ovšem nemají logiku, která by zasahovala do řízení sítě, logika kompletně podléhá BSC spravující sadu základnových stanic.



Obr. 13.2 Komponenty v GSM/GPRS sítích.

BSC ná kompletní přehled, co se na které BTS děje, rozhoduje o handoveru, sbírá informace o úrovních signálů jednotlivých mobilních stanic a řídí BTS. Rozhraní mezi BSC a BTS se nazývá Abis, jde o E1 TDM s protokolem LAPD, který vyl již prezentován v části věnované ISDN (viz. linková vrstva, Q.921, kap. 4.2.1).

Provoz z mobilních stanic je směrován přes switch, který je označován jako MSC (Mobile Switching Center). Tento switch nabízí obdobné funkce jako u ISDN ústředen, navíc zahrnuje alokaci a administraci rádiových zdrojů a mobility uživatelů. V buňkové síti

je obvykle několik MSC a propojení s pevnou síti PSTN/ISDN je zajištěno pomocí brány GMSC (Gateway MSC).

GSM obsahuje několik databází, HLR a VLR obsahují aktuální umístění uživatele, které umožňuje terminovat volání na správnou BTS a navíc tyto registry obsahují profily uživatelů, což je důležité pro tarifikaci a další administrativní záležitosti. Další databáze AUC (Authentication Center) uchovává klíče pro autentizaci a šifrování a nakonec architektura obsahuje databázi EIR (Equipment Identity Register) obsahující účastnická data. Správa je oragnizována pomocí prvku OMC, což umožňuje konfiguraci síťových prvků, monitoring, administraci účastníků a jejich účtování.

Celá síť je rozdělená do MSC regionů a každý z nich je složen z nejméně jedné oblasti LA (Location Area), každá oblast se skládá z několika skupin buněk. Každá skupina buněk je přiřazena konkrétní BSC. V každé oblasti LA existuje alespoň jedna BSC. Dle úloh jednotlivých systémů může být GSM síť rozdělena do třech logických úrovní:

- rádiová přístupová síť BSS (Base Station Subsystem),
- jádro sítě NSS (Network Switching Subsystem),
- a dohledová síť OMSS (Operation nad Maintenance Subsystem).

13.2 Adresace

Mobilní stanice je jednoznačně identifikována pomocí **IMEI** (International Mobile Station Equipment) přidělené výrobcem, obdoba sériového čísla či MAC adresy zařízení. Identita uživatele je uložena v SIM (Subscriber Identity Module).

13.2.1 Identifikátory účastníka

Při registraci obdrží každý uživatel jedinečný identifikátor **IMSI** (International Mobile Subscriber Identity), IMSI je uloženo v SIM a jedná se max. 15-ti místné číslo, které se skládá z následujících částí:

- Mobile Country Code MCC, třímístný kód (230 pro ČR),
- Mobile Network Code (MNC), dvoumístný kód pro identifikaci sítě v rámci země (01 - TMobile, 02 - Telefónica O2, 03 - Vodafone, 04 - MobileKom, 99 - Testovací

ČVUT),

- Mobile Subscriber Identification Number (MSIN), max. 10 čísel, identifikace účastníka v jeho domácí mobilní síti.

Další adresou je **MSISDN** (Mobile Subsrciber ISDN Number) přidělené účastníkovi, jedná se o tel. číslo, pod kterým je dosažitelný a jedna mobilní stanice může mít i více MSISDN. Oddělení identifikátoru uživatele IMSI a jeho tel.č. MSISDN je provedeno záměrně, aby bylo IMSI skryto, narozdíl od MSISDN, adresa IMSI není veřejná. Asociace MSISDN a IMSI je provedeno v registru HLR. Struktura MSISDN je v souladu se standardem ITU-T E.164 a skládá se z CC (Country Code), NDC (National Destination Code) a SN (Subscriber Number), např. 420603123456.

V případě roamingu se pracuje s adresou **MSNR** (Mobile Station roaming Number), která má stejnou strukturu jako MSISDN a je přiřazeno registrem VLR. Otázkou je, jak se dozví domácí HLR potažmo MSC, informace důležité k sestavení příchozího volání, to se děje dvěmi možnými způsoby:

- buď je MSNR přiřazeno při každé registraci, když mobilní stanice vstoupí do jiné oblasti LA, v tomto případě MSNR je předáno z VLR do HLR, kde je uloženo, tím pádem je možné směrovat volání na uživatele na příslušné MSC, kde propojovací prvek MSC získá dodatečné lokalizační informace z příslušného VLR,
- anebo pokaždé, když HLR vyžaduje sestavení příchozího volání, v tomto případě MSNR není uloženo v HLR, ale k uživateli je v tabulce známa pouze adresa aktuální VLR a HLR sama žádá po VLR na základě jedinečné identifikace účastníka (MSISDN a IMSI) platnou roamingovou adresu MSRN, na jejím základě je proveden routing.

VLR registr odpovědný za aktuální umístění účastníka může přiřadit identifikátor TMSI (Temporary Mobile Subscriber Identity), který má pouze lokální význam v oblasti obsluhovanou daným VLR. Rovněž VLR může přiřadit dodatečný vyhledávací klíč LMSI (Local Mobile Station Identity) každé mobilní stanici v jeho oblasti k urychlení vyhledávání v databázi. Klíč LMSI je přiřazen, pokud se mobilní stanice registruje ve VLR rovněž je zaslán do HLR.