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

VÝVOJ ARCHITEKTURY IP MULTIMEDIA SUBSYSTEM

DEVELOPMENT ARCHITECTURE IP MULTIMEDIA SUBSYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE VLADIMÍRA HLADÍKOVÁ
AUTHOR

VEDOUCÍ PRÁCE DOC. ING. VÍT NOVOTNÝ, PH.D.
SUPERVISOR

BRNO 2008

Cíle, kterých má být dosaženo:
Seznamte se s problematikou správy multimediálních služeb v IP sítích (IMS). Prostudujte důvody vedoucí k potřebě IMS a rozeberte architekturu systému. Zaměřte se na organizaci subsystému IMS spolupracujícího se současnými a přicházejícími mobilními sítěmi. Posuďte přínos IMS pro zavádění nových služeb, zatraktivnění nových mobilních technologií pro nové uživatele a tím i pro zrychlení zavádění nejnovějších architektur a řešení paketových mobilních sítí do praktického nasazení. Pokuste se zjistit u některých našich operátorů zájem o nasazení IMS.

LICENČNÍ SMLOUVA

POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Vladimíra Hladíková

Bytem: Rudíkov 151, 67505, Rudíkov

Narozen/a (datum a místo): 22.4.1968, Třebíč

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 602 00, Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc.

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - ☐ disertační práce
   - ☐ diplomová práce
   - ☑ bakalářská práce
   - ☐ jiná práce, jejíž druh je specifikován jako .....

   (dále jen VŠKP nebo dílo)

Název VŠKP: Vývoj architektury IP Multimedia Subsystem

Vedoucí/ školitel VŠKP: doc. Ing. Vít Novotný, Ph.D.

Ústav: Ústav telekomunikací

Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v*:

- ☑ tištěné formě – počet exemplářů 1
- ☑ elektronické formě – počet exemplářů 1

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☑ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

…….. ……
Nabyvatel Autor

Anotace:

Bakalářská práce je vypracována se zaměřením na konvergenci sítí a služeb v mobilním prostředí s implementací IMS.

V první části jsem se věnovala důvodům vzniku nového systému, kterým je IMS (Internet Protocol Multimedia Subsystem) a jaké možnosti tato architektura přináší uživatelům. Jsou zde samozřejmě zmíněny instituce a organizace, které se vývojem tohoto systému zabývají. V této kapitole je stručně popsána historie jednotlivých standardizačních částí.

V další části je popsána architektura IMS, její hlavní části a funkce. Je zde popsáno, které služby je možno pomocí tohoto systému poskytovat.

Pro zajištění kvalitního přenosu v sítích založených na IP protokolu je nutno také zajistit určitou kvalitu služeb QoS (Quality of Service), proto je tomuto tématu věnována jedna z dalších kapitol. Jsou zde popsány principy zajištění kvality. Hlavním faktorem ovlivňujícím kvalitu přenosu je, jaký typ dat je po IP sítích přenášen.

Další kapitola je věnovaná autentizaci a autorizaci v IMS sítích. Zejména objasnění spojení s protokolem Diameter.

V další částí jsem se věnovala VoIP (Voice over IP), přenos hlasu po IP sítích. Je zde popsána základní myšlenka přenosu hlasu IP sítěmi. Pro přenos hlasu IP sítěmi jsou důležité kodeky, proto je zde uveden jejich přehled.

Na to navazuje kapitola věnovaná použitým protokolům, bez nichž by celý systém nemohl fungovat. Jedná se o protokoly SDP (Session Description Protocol), protokoly pro přenos dat v reálném čase RTP (Real-time Transport Protocol), RTCP (RTP Control Protocol), RTSP (Real-Time Streaming Protocol) a nakonec nejdůležitější signalizační protokol SIP (Session Initiation Protocol) a jeho propojení se strukturou IMS.

V závěru jsou zhodnoceny možnosti IMS v mobilních komunikačních sítích a jejich využití pro VoIP. Mimo jiné jsou vzaty v úvahu i ekonomické vlivy na rozšíření zařízení podporujících služby s implementací IMS pro širokou veřejnost.

Klíčová slova:
konvergence, multimedia, mobilní sítě, 3GPP, protokol, kvalita služeb, VoIP

ABSTRACT

Bachelor thesis topic is focused on convergence of networks and services in the environment of mobile networks with implementation of Internet Protocol Multimedia Subsystem (IMS).

The first part is, devoted to reasons of design of new system, such as IMS (Internet Protocol Multimedia Subsystem) and which possibilities this architecture brings to users. I mentioned institutions and organizations, which are involved in the development of this system. In this chapter is shortly defined history of single standardised parts.

In the next part is defined the IMS architecture its main part and functions. I defined which services of this system are possible to offer.

To guarantee the high-quality transfer in the sites based on IP protocol is very important to guarantee quality of QoS (Quality of Service) services. So I take the aim to that in one of the next chapters. I mentioned quality assurance principles. The main factor that influences the quality of the transfer is which type of data is being transferred in IP network.

The next charter is devoted authentication and authorisation in IMS network. I described the integration with Diameter protocol.

The main part is devoted to VoIP (Voice over IP), the transfer of voice in IP networks. I defined the main idea of transfer of voice in IP networks. Codecs are very important for the voice transfer in IP networks, so I give a conspectus here.

The next chapter gives attention to used protocols. The system could not work without them. It goes around SDP (Session Description Protocol), protocols for real-time data transfer RTP (Real-time Transport Protocol), RTCP (RTP Control Protocol), RTSP (Real-Time Streaming Protocol) - and the most important signalling protocol SIP (Session Initiation Protocol) and its integration with IMS.

Finally I rated possibilities of IMS in mobile communication network and their use for VoIP. Among others I take into consideration also economical influences over the expansion of equipment supporting services with implementation IMS for general public.

KEYWORDS

convergence, multimedia, mobile network, 3GPP, protocol, quality of services, VoIP

HLADÍKOVÁ, V. Vývoj architektury IP Multimedia Subsystem. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 56 s. Vedoucí bakalářské práce doc. Ing. Vít Novotný, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Vývoj architektury IP Multimedia Subsystem jsem vypracovala 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 semestrální 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)

Děkuji **doc. Ing. Vítu Novotnému Ph.D.** za odborné a organizační vedení při zpracování této práce.

Obsah:

ÚVOD **1**
1 IMS ARCHITEKTURA **2**
1.1 Organizace 3GPP **2**
1.2 Základní architektura IMS **3**
1.2.1 Služby v architektuře IMS 4
1.2.2 Přístupová a transportní úroveň 6
1.2.3 Jádro sítě IMS 6
2 ZAJIŠTĚNÍ KVALITY QOS **9**
2.1 Kvalita v IP sítích **9**
2.1.1 Technologie DiffServ 10
2.1.2 Technologie IntServ 10
2.1.3 Technologie QoS v sítích s implementací IMS 12
3 AUTENTIZACE A AUTORIZACE (AAA) **14**
3.1 Možnosti zabezpečení **14**
3.2 Protokol Diameter **15**
3.2.1 Hlavní data protokolu Diameter 15
3.2.2 Diameter v IMS 16
4 VOIP **20**
4.1 Kódování hlasu **21**
4.2 Architektury VoIP **23**
4.2.1 Architektura H.323 23
4.3 Protokoly VoIP **24**
4.3.1 Protokol SDP 24
4.3.2 Protokoly pro přenos dat v reálném čase 25
4.3.3 Architektura protokolu SIP 31
5 PODPORA IMS V SOUČASNÝCH MOBILNÍCH SÍTÍCH **38**
5.1 Možnosti stávajících mobilních sítí **39**
ZÁVĚR **42**
POUŽITÁ LITERATURA: **43**

Seznam obrázků:

Obrázek 1-1. Základní rozdělení vrstev architektury IMS 3
Obrázek 1-2. Rozdělení služeb v architektuře IMS 4
Obrázek 1-3. Architektura IP Multimedia Core Network Subsystem 6
Obrázek 1-4. Dotaz do SLF databáze 8
Obrázek 2-1. Buffer jitter 9
Obrázek 2-2. Architektura QoS v sítích UMTS/GPRS 12
Obrázek 3-1. Diameter hlavička 15
Obrázek 3-2. Hlavička AVP 16
Obrázek 3-3. SIM, USIM a ISIM v UICC pro 3GPP IMS terminal 17
Obrázek 3-4. Prvotní registrace uživatele v síti IMS 19
Obrázek 4-1. Princip přenosu hlasu IP sítěmi 20
Obrázek 4-2. Zjednodušený model protokolové sady 20
Obrázek 4-3. Architektura H.323 23
Obrázek 4-4. Formát RTP hlavičky 26
Obrázek 4-5. Příklad zprávy vysílače 28
Obrázek 4-6. Příklad výměny RTSP zpráv 30
Obrázek 4-7. SIP přímá komunikace 35
Obrázek 4-8. SIP komunikace dvou účastníků se serverem proxy 35
Obrázek 4-9. SIP komunikace se serverem Redirect 36
Obrázek 4-10. SIP dotaz 36
Obrázek 4-11. Rozlišování adres 37
Obrázek 5-1. Procedura PDP kontextu v síti GPRS. 38
Obrázek 5-2. Spojení dvou IMS terminálů 39
Obrázek 5-3. Obrázek realizace řešení v zákaznické lokalitě [6] 40

Seznam tabulek:

Tabulka 1-1. Přehled služeb zajišťovaných sítěmi 3G s implementací IMS 4
Tabulka 1-2. Rozhraní IMS CN Subsystem 7
Tabulka 1-3. Základní bloky jádra IMS 7
Tabulka 2-1. Typy RSVP zpráv 11
Tabulka 2-2. Základní vlastnosti QoS UMTS/GPRS tříd [13] 12
Tabulka 3-1. Přehled Cx zpráv protokolu Diameter v IMS 17
Tabulka 3-2. Přehled parametrů Cx AVP Diameteru 18
Tabulka 4-1. Kodeky s přenosovými rychlostmi a hodnocením MOS 21
Tabulka 4-2. Kodeky pro GSM a UMTS 22
Tabulka 4-3. SDP popis 25
Tabulka 5-1. Srovnání možností připojení operátorů. 41
Tabulka 5-2. Pevné připojení vs. mobilní připojení pro operátora O2. 41

Seznam použitých zkratek:

3GPP	Third Generation Partnership Project
ADSL	Asymetric Digital Subscriber Line
AAA	Authentication, Authorization and Accounting
AVP	Attribute-Value Pair
BSC	Base Station Controller
BTS	Base Transceiver Station
CN	Core Network
CSCF	Call Session Control Function
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communication
HSS	Home Subscribe Server
I-CSCF	Interrogating CSCF
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMS	Internet Protocol Multimedia Subsystem
ISDN	Integrated Services Digital Network
MSC	Mobile Switching Centre
NDS	Network Domain Security
NMT	Nordic Mobile Telephone
P-CSCF	Proxy Call Session Control Function
PDP	Packet Data Protocol
PSTN	Public Switched Telephone Network
RFC	Request For Comments
RSVP	Resource reSerVation Protocol
RTP/RTCP	Real Time Protocol/Real Time Control Protocol
RTSP	Real Time Streaming Protocol
S-CSCF	Serving CSCF
SCTP	Stream Control Transport Protocol
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLF	Server Location Function
TCP/IP	Transmission Control Protocol /Internet Protocol
TMSI	Temporary Mobile Subscriber Identity
UA	User Agent
UCS	Universal Character Set
UMTS	Universal Mobile Telecommunication System
URL	Uniform Resource Locator
UTF	UCS Transformation Formats

Úvod

Přeprava informací ať již v analogové nebo dnes především v digitální podobě je hlavní náplní telekomunikací. Cílem je výměna informací - znalostí mezi lidmi, případně i dalšími zařízeními, která umí produkovat, odeslat, a na druhé straně přijmout a zpracovat informace. Dnešním uživatelům již nestačí „pouze telefonovat“, komunikační sítě tak zajišťují přenos různých uživatelských dat. Sítěmi obecně tak projde obrazový materiál pro příjem televize, ať již jde o přenos klasickými rádiovými kanály, nebo přes satelit nebo kabelovou televizí. Do popředí se dostává též příjem TV pomocí datových sítí. Datové sítě pracují na principu IP protokolu, jehož základem je přepojování paketů. Začaly se tedy budovat nové telekomunikační pevné i bezdrátové sítě. Je zde k dispozici možnost, kdy pomocí jedné linky (myšlen jeden přípojný kabel do domácnosti) lze provozovat telefonní hovor, být připojen k Internetu a zároveň sledovat televizní program. Tuto technologii například nabízí jeden z telefonních operátorů na pevných linkách pomocí technologie ADSL/VDSL. S vývojem elektroniky nezůstaly pozadu ani mobilní sítě. Za první datovou mobilní síť lze pokládat technologii GSM, ta ovšem ještě používá princip přepojování okruhů. Mobilní sítě s přepojováním paketů jsou až sítě 2,5G (technologie GPRS) a výše. Aby byla možná komunikace mezi různými typy sítí, je nutné tzv. sbližování telekomunikačních sítí s komutací okruhů s IP sítěmi a sdružování telekomunikačních služeb do služeb multimediálních toto všechno se dá shrnout jedním slovem konvergence. Koordinaci konvergence a technickou specifikaci zajišťuje ETSI TISPAN (Telecoms & Internet Converged Services & Protocols for Advanced Networks). Systém, který zastřešuje všechny tyto služby je systém IMS (IP Multimedia Subsystem).

Cílem této práce je zpracovat možnosti a využití architektury IMS a jaké možnosti tato architektura nabízí v zavádění nových služeb pro uživatele, a také jaké důvody vedly ke vzniku této architektury. Pro zpracování principů architektury IMS bylo nutné se seznámit s použitými protokoly, způsoby autentizace a zajištění kvality.

Toto téma jsem si vybrala z důvodu vytvoření textu s celkovým pohledem na tuto architekturu v češtině. Takovýto text s celkovým přehledem nebyl doposud v češtině publikován. Dále jsem se chtěla zaměřit na využití mobilních sítí s implementací IMS pro VoIP. Součástí práce je i posouzení ekonomických vlivů na rozšíření této technologie mezi širokou veřejnost. S architekturou na bázi IMS se můžeme setkat v pevné i mobilní síti poskytovatele O2, jež v současné době nabízí „Triple Play“ jako jednu z posledních novinek. Proto jsem se zaměřila i na nasazení IMS v sítích ostatních mobilních operátorů.

Informace k této práci jsem čerpala v zahraniční literatuře, z internetových zdrojů organizací IETF, 3GPP a odborných zpráv, které zpravidla popisují pouze úzkou část celé problematiky.

1 IMS architektura

V dnešní době zákazník očekává od „spojů“ širokou nabídku služeb. Dříve se služba orientovala na účastnické zařízení a pro dané zařízení byly zřízeny sítě. Pro hovor byly zřízeny telefonní sítě, pro textové zprávy nebo-li dálnopis, byli sítě pro přenos dálnopisných zpráv. Do těchto samostatných speciálních sítí patří také rozhlas a televize. Samostatnou kapitolou byly datové sítě. V současné době probíhají radikální změny v tomto směru. Všechny sítě jsou digitalizovány a propojovány. Dochází k tzv. konvergenci a to v celosvětovém měřítku. Na rozšíření spektra služeb je potřeba nové vybavení a to jak na straně předplatitele služby, tak na straně poskytovatelů.

Operátor je nucen, pro udržení zákazníka, zdokonalovat služby. Proto se jeví jako nejvhodnější alternativa řešení komunikační infrastruktura na principu IP. Je zapotřebí všestranné technologické prostředí, které zabezpečuje integraci odlišných komunikačních připojení. Takové prostředí dokáže podpořit personální komunikaci v reálném čase, může se jednat např. o služby hlasové nebo videokonference. Ovšem sloučení všech těchto služeb nelze provozovat na komunikacích založených na principu přepojování okruhů, je nutno všechny sítě převést na princip přepojování paketů. Pro realizaci takovéhoto prostředí byla navržena architektura IMS. Vyjdeme-li pouze z názvu IMS (Internet Protocol Multimedia Subsystem), tak vyvodíme, že se jedná o poskytování multimediálních služeb na bázi IP protokolu. Pod pojmem multimediální služby si můžeme představit prakticky cokoli, co lze převést do podoby digitálního signálu. Pro další rozvoj telekomunikačních technologií nastala jistá potřeba koordinace budování těchto nových služeb a sítí. Z těchto důvodů vznikla organizace 3GPP, kde se všechny kroky pro konvergenci koordinují.

1.1 Organizace 3GPP

IP Multimedia Core Network Subsystem v sobě obsahuje podpůrné prostředky , které jsou potřeba pro multimediální mnoho přístupovou síť založenou na principu přepojování paketů. Celý tento systém zahrnuje signalizaci a principy přenosové sítě jak byla specifikována v TS23.002. V roce 1998 vznikla organizace 3GPP/3GPP2 (Third Generation PartnershipProject). Prvním projektem této organizace se stal standard R99 (Vydání 1999) [1], [2] z prosince 1999. V tomto vydání vyspecifikovala 3GPP vývoj služeb, architektury sítí a obecný základ přístupu k radiovým sítím. ETSI SMG se zaměřili na vývoj GSM – Enhanced Data Rates for Global Evolution (EDGE).

V roce 2000 začala 3GPP pracovat na specifikaci Release 2000. Do tohoto Vydání bylo zahrnuto i tzv. All-IP, to známe dnes jako IP Multimedia Subsystem (IMS). Vyvinout však systém za pouhý jeden rok se ukázalo jako nemožné. Proto bylo rozděleno na Release 4 a Release 5. Vydání 4 bylo dokončeno bez IMS v březnu 2001. IMS bylo specifikováno jako součást standardu 3GPP až v Release 5.

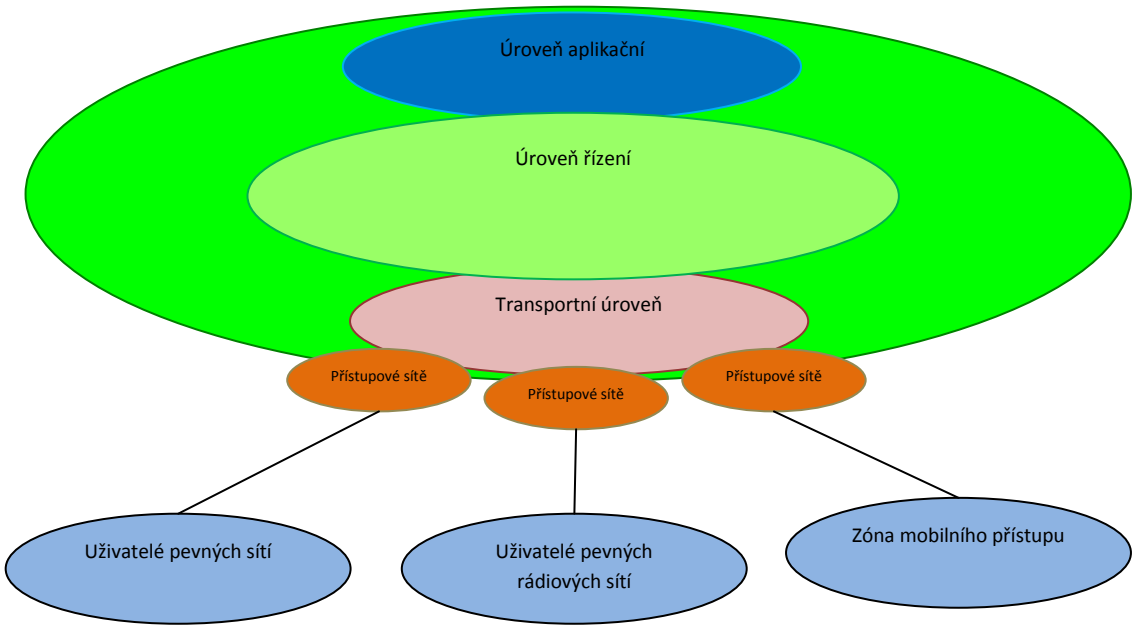
Dle standardu 3GPP je IMS subsystém standardizován jako architektura založená na IP principu, která spolupracuje s již existujícími hlasovými a datovými sítěmi, a to včetně sítí mobilních. Tento standard platí pro pevné linky (PSTN, ISDN …) i pro mobilní sítě (GSM,..UMTS…). Takto postavená architektura umožňuje navázat IP spojení bod-bod („peer-to-peer“) se všemi typy klientů. Je zde zajištěna i nezbytná kvalita přenosu služeb (QoS). Release 5 bylo uzavřeno v březnu 2002 po velkých diskusích.

Mnoho nových návrhů se objevilo až v Release 6., které bylo dokončeno v září 2005. Hlavním stavebním kamenem IMS architektury se stal signalizační protokol Session Initiation Protocol (SIP).

Na toto vydání pak navazuje Vydání 7, které bylo uzavřeno v září 2007. Toto vydání se zaměřilo na zlepšení QoS a Real-time aplikace jako např. VoIP.
Zároveň v říjnu téhož roku byly spuštěny práce na Vydání 8, které se zaměřilo na zvyšování přenosové kapacity (rychlosti), ale současně za snižování nákladů na jednotku přenosové informace.

1.2 Základní architektura IMS

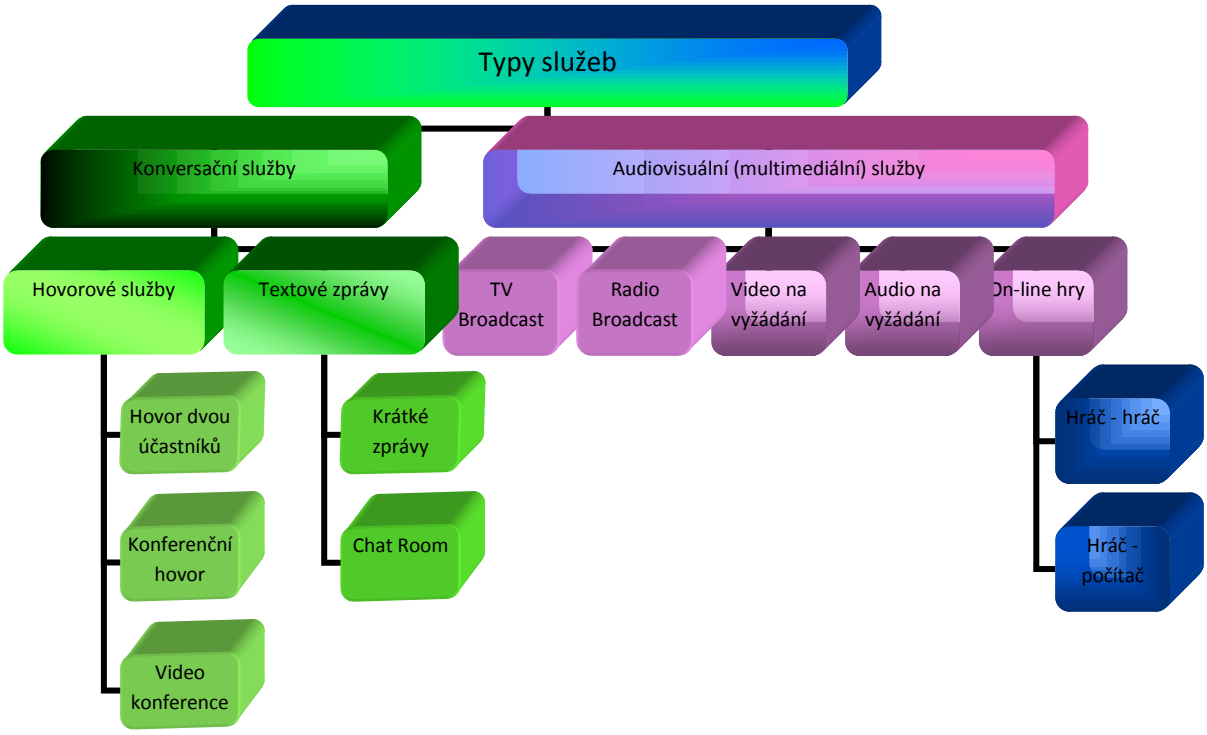
Architektura IMS zajišťuje vzájemnou souvislost řady funkčních prvků. Základní rozdělení architektury je třívrstvé, můžeme ji rozdělit na vrstvu aplikační, řídicí a transportní nebo také přístupovou.



Obrázek 1-1. Základní rozdělení vrstev architektury IMS

1.2.1 Služby v architektuře IMS

V aplikační vrstvě jsou umístěny všechny dostupné služby. Tyto služby jsou uživateli přidělovány na základě toho, které z těchto služeb má předplaceny. Služby v architektuře IMS můžeme rozdělit následovně:



Obrázek 1-2. Rozdělení služeb v architektuře IMS

Tabulka 1-1. Přehled služeb zajišťovaných sítěmi 3G s implementací IMS

- veřejný informační servis,
- surfování na Webu,
- on-line alternativa tištěných médií (noviny, časopisy),
- on-line překlady,
- výchovné a zábavné služby,
- virtuální škola (e-learning),
- on-line výzkumné laboratoře,
- on-line knihovna,
- školení,
- audio na vyžádání (alternativa k CD a kazetám),
- hra na vyžádání,
- obchodní informace,
- video telefonie,
- video konference,
- reakce a rozeznání hlasu – identifikace mluvčího,
- obchod a finance,
- electronic commerce na síti – elektronické obchodování,
- virtuální bankovnictví, virtuální SIM a kreditní karty,
- inteligentní vyhledávače,
- speciální servis a služby,
- lékařské služby,
- služby rychlé pomoci,
- služby monitoringu zabezpečení

Komunikační služby lze rozdělit na základní a doplňkové nebo na hlasové a datové služby. Po případě můžeme služby dělit na telematické, doručovatelské a podpůrné.

Mezi základní služby patří služby doručovatelské a telematické. Doručovatelské služby zajišťují přenos dat mezi rozhraními síťových terminálů. Tyto služby jsou implementovány jako spojované služby a jsou poskytované jak sítí s přepojováním okruhů tak i sítí s přepojováním paketů. Telematické služby jsou aplikačně orientované služby, typická aplikace je přenos hlasu. Tyto služby jsou zavedeny jako koncové služby mezi dvěma terminály (end-to-end). Telematické služby se podřizují buňkové struktuře mobilních sítí. Primární cíl je hlasová komunikace. Dále jde o bezplatná tísňová volání např. jednotné číslo pro Evropu 112. Tato služba musí být podporována všemi operátory mobilních služeb. Toto spojení má samozřejmě nejvyšší prioritu. Dále do telematických služeb patří i nehlasová komunikace jako jsou SMS, MMS. SMS (Short Message Service) zajišťuje přenos alfanumerických znaků řídicím kanálem. To umožňuje souběžné používání hlasových telematických služeb s SMS. MMS (Multimedia Message Service) zajišťuje přenos obrázků v komprimovaných souborech jako GIF, JPG, … nebo přenos videa.

Další službou je hlasová schránka. Ta zajišťuje možnost zanechat vzkaz volanému nelze-li ho zastihnout přímo. Důvodem může být jiný hovor nebo vypnutá mobilní stanice aj.

Podpůrné nebo taky doplňkové služby se nenabízejí samostatně, ale jako podpora služeb základních. Mezi důležité doplňkové služby patří např. identifikace volajícího, potlačení dodávání čísla volajícího (skryté číslo), automatické zpětné volání (call-back), konference několika účastníků dále se může jednat o uzamčení (zablokování) mobilního terminálu pro některé ať už příchozí či odchozí hovory.

Dalšími novými službami jsou služby multimediální. Tyto nové služby lze provozovat pouze v sítích 3G. Pro tyto nové služby musí být vybaveny i mobilní terminály. Mezi tyto služby patří real-time aplikace jako TV broadcast nebo radio broadcast, video na přání (video on deman), hudba na přání nebo on-line hry. Hry mohou být typu hráč-hráč nebo hráč-počítač.

Mezi další služby patří elektronické obchodování. Jedná se on-line objednávky zboží a elektronické platby (převody kapitálu mezi jednotlivými účastníky obchodu).

Sítě s podporou IMS nabízejí přenositelnost čísla. Pod pojmem telefonní číslo si nemusíme představit skutečně jen devíti místné číslo (s mezinárodní předvolbou 12 míst) tak jak je známe. Může se jednat i o čísla v tzv. nemezinárodním formátu. Pod tímto pojmem si představme například přihlašovací jména do Skype nebo číslo do ICQ. V síti potom pracují „překladače“, které takovéto adresy přeloží do srozumitelné podoby pro tu kterou síť. V UE (User Equipment) jsou uloženy všechna uživatelská nastavení – všechna uživatelská jména, přihlašovací hesla a adresy. Takový uživatel se může tedy do sítě připojit jako UA (User Agent) SIP telefonu nebo pomocí mobilní stanice nebo přes pevnou síť. Všechny tyto možnosti jsou zajištěny pomocí zpráv signalizačního protokolu SIP (Session Initiation Protocol).

Po přihlášení do systému je na základě SIP dotazu ze S-CSCF do UE zjištěno jaké služby a jakou adresaci uživatel využívá a je-li uživatel v domovské síti či nikoli. P-CSCF pošle SIP požadavek směrem S-CSCF na SIP URI adresu.

Roaming je založen na tom, že uživatel, který sice momentálně není v domovské síti, má ovšem řádnou smlouvu s domovským operátorem. Veškeré spojení se uskutečňuje přes CSCF v domovské síti.

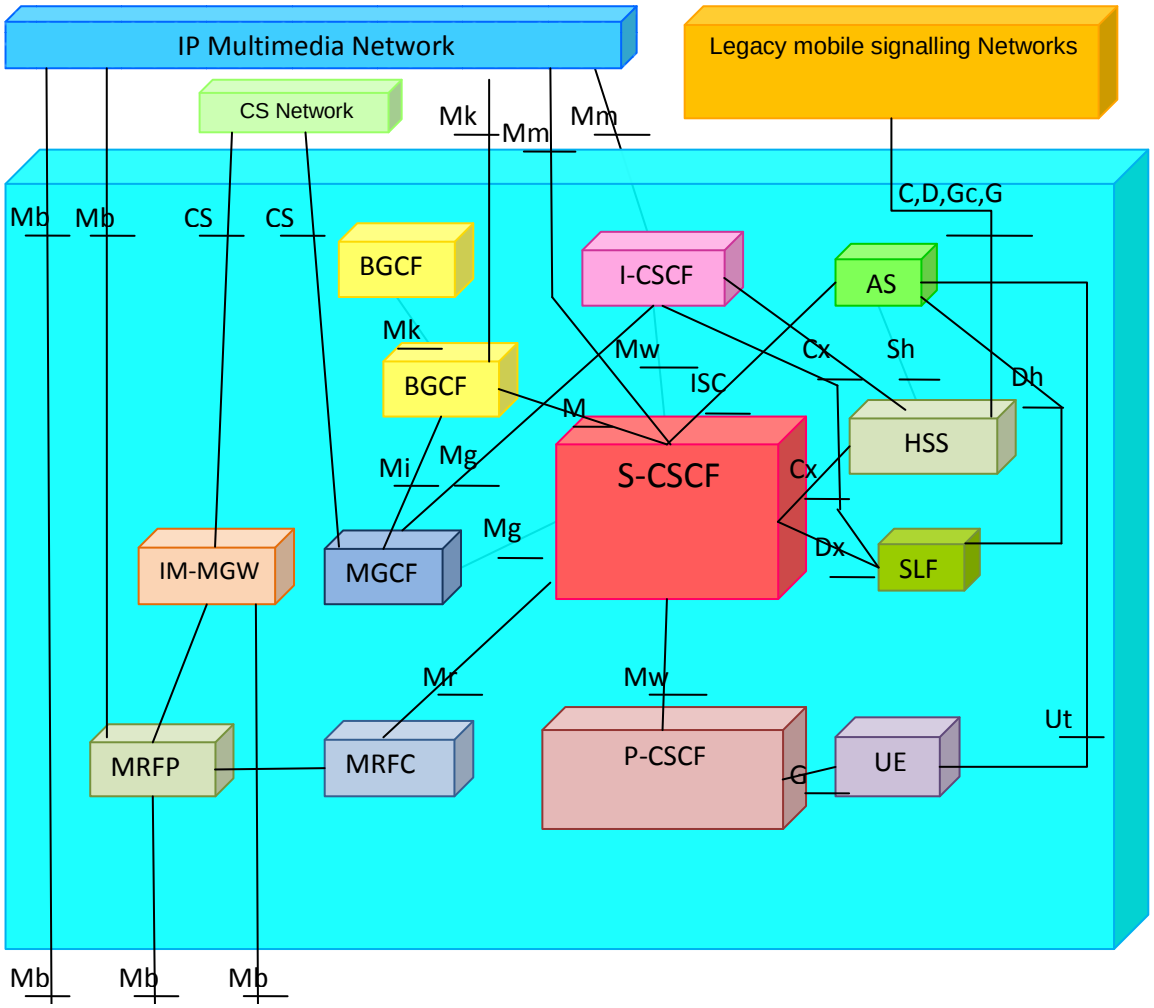
1.2.2 Přístupová a transportní úroveň

Základní myšlenka IMS je přístup k síti a službám odkudkoli to znamená, do sítě je možno se připojit pomocí pevné linky (xDSL, PSTN), pevných radiových sítí (WLAN, DOCSIS®, WiMAX™) nebo mobilních sítí (E-UTRAN, UTRAN, GERAN a cdma2000®) popřípadě pomocí rozvodů kabelové televize nebo satelitního vysílání.

1.2.3 Jádro sítě IMS

Základním stavebním kamenem celého systému IMS je CSCF (Call Session Control Function). Tento blok zpracovává signalizační zprávy protokolu SIP (Session Initiation Protocol), které přicházejí od uživatelských aplikací, aplikačních serverů AS (Application Server) nebo dalších bloků v IMS architektuře. Tato část CSCF se dělí na další bloky a to na blok obsluhující S-CSCF (Serving-CSCF), blok P-CSCF (Proxy-CSCF) a I-CSCF (Interrogating-CSCF).

1.2.3.1 Základní bloky jádra IMS



Obrázek 1-3. Architektura IP Multimedia Core Network Subsystem

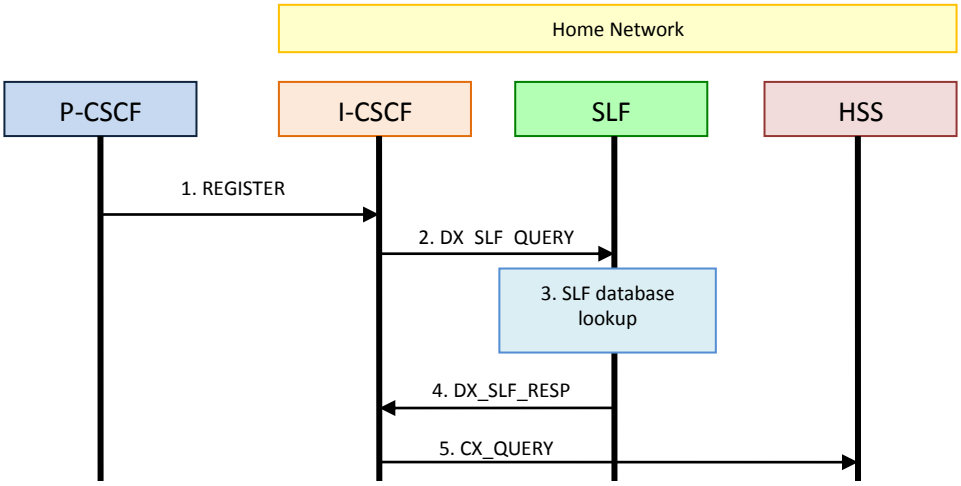
Tabulka 1-2. Rozhraní IMS CN Subsystem

Rozhraní	Význam:
Cx	rozhraní mezi CSCF a HSS
Dx	rozhraní mezi I-CSCF a SLF
Gi	rozhraní mezi GPRS a vnější paketovou sítí
Gm	rozhraní mezi UE a P-CSCF
ISC	rozhraní mezi CSCF a AS (aplikačním serverem)
Ma	rozhraní mezi AS a GMLC
Mb	rozhraní služeb IP sítě
Mg	rozhraní mezi MGCF a CSCF
Mi	rozhraní mezi S-CSCF a BGCF
Mj	rozhraní mezi BGCF a MGCF
Mk	rozhraní mezi BGCF a jiné BGCF
Mm	rozhraní mezi CSCF/BGCF/IMS ALG a vnější IP multimediální sítí
Mr	rozhraní mezi S-CSCF a MRFC
Mw	rozhraní mezi jednotlivými vnitřními částmi CSCF
Mx	rozhraní mezi CSCF/BGCF a IBCF
Sh	rozhraní mezi AS a HSS
Ut	rozhraní mezi UE a AS

Tabulka 1-3. Základní bloky jádra IMS

Zkratka	Název	Funkce
CSCF	Call Session Control Function	Centrum jádra IMS
P-CSCF	Proxy-CSCF	Proxy odvozuje svou funkci ze SIP architektury, je prvním kontaktním místem v IM CN. Přijímá žádosti o spojení, přesměrovávání žádostí a odpovědí. Kontroluje identitu uživatele a ověřuje důvěryhodnost, proto další části již autentizaci uživatele neprovádějí. Jeho další funkcí je komprese a dekomprese zpráv na rádiovém rozhraní.
I-CSCF	Interrogating-CSCF	Jeho základní funkcí je dotaz na HSS k získání jména S-CSCF pod jehož správu patří uživatel. Je to styčný bod vnitřní struktury sítě pro volající účastníky z jiných sítí.
S-CSCF	Serving-CSCF	Jedná se o hlavní blok jádra IMS. Vykonává dohled nad spojením, evidence a na základě profilu v HSS směruje spojení s AS.
AS	Application Server	Aplikační servery SIP AS – aplikační server se službami na bázi protokolu SIP. Předpokládá se, že všechny nové služby budou na bázi SIP protokolu OSA-SCS (Open Service Access – Service Capability Server) – server se službami, které bazírují na otevřeném přístupu. IM-SSF (IP Multimedia- Service Switching Function) – server s komutovanými službami

Zkratka	Název	Funkce
BGCF	Breakout Gateway Control Function	Provádí směrování pro bod přestupu do jiných sítí nebo do jiného BGCF.
HSS	Home Subscribe Server	Hlavní databáze uživatelů je to obdoba HLR a AuC z architektury GSM. Zde jsou uloženy informace o předplacených službách uživatele, údaje o registraci, přístupové parametry aj.
SLF	Subscription Locator Function	zajišťuje přiřazení určitého HSS pro uživatele
MGCF	Media Gateway Control Function	zajišťuje vzájemnou signalizaci mezi IP sítí a sítí s přepojováním okruhů
IM-MGW	IMS – Media Gateway	zajišťuje spojení mezi IP sítěmi a sítěmi CS
MRFP	Media Resource Function Processor	vykonává např. multiplexování příchozích datových toků tento blok je řízen MRFC
MRFC	Media Resource Function Control	řídí služby konference a interaktivní hlasové odezvy, které jsou realizované přes MRFP na základě informací poskytnutých AS a S-CSCF
UE	User Equipment	Uživatelské vybavení



Obrázek 1-4. Dotaz do SLF databáze

1. I-CSCF přijme žádost o registraci a vyžádá si uživatelská data
2. I-CSCF odešle žádost na SLF o uživatelská data
3. SLF prohledává databázi s uživatelskými daty
4. SLF odesílá jméno HSS kde jsou uloženy uživatelovy parametry
5. I-CSCF zasílá dotaz přímo konkrétnímu HSS

2 Zajištění kvality QoS

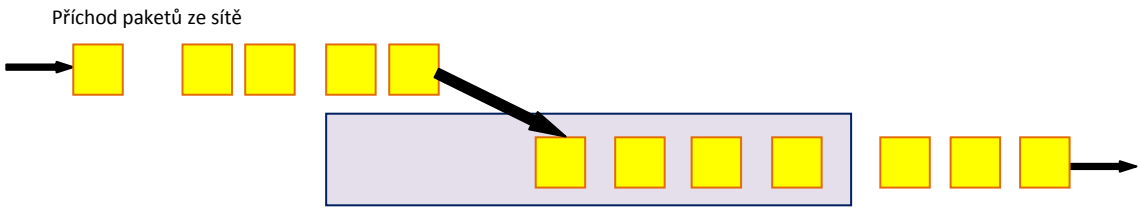
Při přenosu informací od volajícího účastníka k účastníku volanému dochází k různým procesům, které probíhají v různých prostředcích a vše dohromady vytváří službu. Samotná realizace služby se děje v časových úsecích, kde v každém tomto úseku probíhá nějaká fáze při poskytování této služby. Sledování jakosti QoS (Quality of Service) je velice důležité. Abychom mohli kvalitu nějakým způsobem posuzovat, musí být definována. V doporučení E.800, je jakost definována jako: „ Celkový účinek poskytnutí služby, který určuje stupeň uspokojení uživatele služby“.

2.1 Kvalita v IP sítích

Vzhledem k tomu, že v IP sítích současně na jednom kanále probíhá více aplikací (hovorů, přenos dat aj.) je kvalita služeb velice důležitá. U multimediálních aplikací a tím i u real-time aplikací je důležité zejména žádné nebo velice malé zpoždění. Hlasová komunikace náchylná na zpoždění a pravidelnost doručování paketů, pak může být ohrožena ostatními komunikačními kanály. Nejdůležitějšímu parametry, které určují kvalitu hovoru v IP síti, jsou hlavní tři:

- jitter – změny ve zpoždění
- latence – zpoždění
- ztráta paketů

- Ke změnám ve zpožděních dochází vlivem změn zátěže v síti či vlivem změn tras v průchodu paketů. Pro hlasovou komunikaci je důležité pravidelné vysílání a přijímání paketů, to se děje kolem 20 ms. Aby při hlasové komunikaci nedocházelo k rozdílným zpožděním, jsou zde zabudovány vyrovnávací paměti (buffer) pro příchozí pakety a zpoždění tak může kolísat mezi 20-50 ms.



Obrázek 2-1. Buffer jitter

První příchozí paket je vložen do bufferu, do jeho středu. Další příchozí pakety jsou řazeny za předchozí paket v relativním pořadí tak, jak budou přehrávány. Schopnost vyrovnávat různá zpoždění je dána velikostí (délkou) bufferu. Čím je buffer delší tím je schopen zvládat rozdílnější zpoždění. Velikost bufferu je velice důležitá, aby nedocházelo k jeho přeplňování (v případě bufferu malého) nebo k jeho vyprázdnění (úseky ticha při bufferu velkém). Měření jitteru probíhá

v přijímači na základě time-stamp (časové značky) v rámci RTP paketu.

- Zpoždění přenosu je způsobeno hned několika faktory. Ke zpoždění dochází v jitter bufferu, zpoždění při kódování hlasu, zpoždění při přepínání (routery, přepínače), zpoždění při samotném přenosu přenosovým médiem.
- Ztráta paketů představuje četnost, jakou jsou zahazovány pakety zařízeními v síti nebo přijímačem. Zahození paketů může v paketových sítích způsobit řada věcí. Častou příčinou zahození rámců je zahlcení sítě. Pokud čelí routery příliš velkému provozu, je pravděpodobné, že zahltí své vstupní buffery. Pokud k tomu dojde, jsou další příchozí pakety zahazovány. Routery mohou také pakety zahazovat v souladu se schématem kvality služby (Quality of Service), který implementují. Mohou to dělat proto, aby pustily jako první pakety, které jsou označeny za prioritní. Ztráta paketů díky číslování v RTP je přijímacím telefonem detekována a ten musí překlenout chvíli ticha během času, kdy měl být zahozený paket přehrán.
- Dalším důležitým faktorem určujícím QoS v IP sítích je její propustnost. Propustnost je definována jako možnost přenesení maximálního počtu paketů za určitý časový úsek.

Pro potřeby IP sítí a zejména sítí multimediálních byly vyvinuty principy zajištění QoS. Existují tři modely zajištění kvality v IP sítích.

- **Best-effort**
- Differentiated services – **DiffServ** , diferencované služby
- Integrated services – **IntServ**, integrované služby

První zmiňovaný způsob Best-effort je založen na principu, kdy je ke všem paketům či rámcům přistupováno se stejnou důležitostí a je s nimi zacházeno tedy stejně. Tento způsob nemá prostředky na zjišťování datových toků. Proto každý paket zpracovává bez závislosti na ostatních. Z toho plynou chyby a ztráty paketů a tedy dochází k znehodnocení např. celého přenášeného souboru. Proto se používají jiné mechanismy na zajištění potřebné kvality.

2.1.1 Technologie DiffServ

Technologie DiffServ pracuje tak, že provoz rozděluje do několika tříd. Každá třída má svou vlastní frontu a při odesílání datových jednotek jsou některé třídy upřednostňovány před jinými. Místa, ve kterých je zacházení se třídami provozu řízeno stejným způsobem, se nazývají Diffserv doménami. Pro VoIP služby bývá zpravidla nastavena nejvyšší priorita, pak je pro tuto třídu vymezena omezená část šířky pásma. Pokud přicházející provoz zařazený do této třídy překračuje přidělenou kapacitu, jsou datové jednotky zahozeny. Tento mechanismus se používá zejména v páteřních sítích.

2.1.2 Technologie IntServ

Technologie Intserv přistupuje k řešení problému řízení kvality služeb jiným způsobem. Zatímco Diffserv rozděluje veškeré přenášené datové jednotky do tříd a podle toho

s nimi zachází. IntServ pracuje na principu rezervace pásma. Rámec IntServ obsahuje čtyři části: plánovač paketů, kontrola přístupu, klasifikátor a rezervační protokol RSVP. Rezervace síťových prostředků je iniciována aplikací a rezervaci potvrzují (příp. odmítnou) všechny síťové uzly na trase mezi zdrojovým a cílovým uzlem. Pro rezervaci prostředků je využit protokol RSVP (Resource Reservation Protocol). Jestliže je nutno na trase překlenout uzly, které nepodporují technologii Intserv, je protokol RSVP přes tyto prvky sítě protunelován. Rezervaci je nutno provádět pro každý směr komunikace zvlášť. Řízení kvality služeb pomocí Intserv není vhodné pro nasazení v sítích s velkým provozem, protože silně zatěžuje síťové prvky. Proto se využívá hlavně v přístupových sítích.

Plánovač paketů řídí zasílání různých proudů paketů na základě souborů front. Musí být zařazen v místě, kde jsou pakety řazeny do front. Ve většině případů je každá služba – tok dat – řešen samostatnou frontou. Plánovač pak řídí posílání jednotlivých paketů z front na základě předem přesně daných algoritmů.

Kontrola přístupu řídí rozhodování o přidělení rezervace. Kontrola přístupu je spuštěna v každém uzlu, aby mohl rozhodnout, zda bude daná QoS přijata nebo odmítnuta.

Klasifikátor identifikuje pakety ve směrovačích pro určitou úroveň služby. Každý příchozí paket je zařazen do určité třídy. S pakety ze stejné třídy je zacházeno stejně.

2.1.2.1 Protokol RSVP

RSVP (Reource reSerVation Protocol) je protokol pro reservaci zdrojů. Je používán k získání určité kvality služeb pro jednotlivé datové proudy po celé trase na všech zařízeních a ve všech uzlech. V každém uzlu RSVP zažádá o reservaci zdrojů pro daný datový tok. Kvalita založená RSVP má dva základní prvky zdroje a cíle. Tyto dva prvky si vyměňují dva typy zpráv PATH a RESV. Typy těchto zpráv jsou v tabulce 2-1.

Tabulka 2-1. Typy RSVP zpráv

číslo	typ zprávy
1	Path
2	Resv
3	PathErr
4	ResvErr
5	PathTear
6	ResvTear
7	ResvConf

Zprávu Path zasílá zdroj pro zajištění prostředků pro určitou aplikaci. Zpráva prochází všemi uzly a směrovači, kde je uložena cesta. Stejnou cestou prochází odpověď cíle.

Zpráva Resv je odpověď cíle na Path zdroje. Zpráva prochází opačnou cestou než zpráva Path a zarezervuje prostředky. Když cílová stanice rezervaci odmítne nebo když rezervace není možná odešle zdroji zprávu ResvErr.

Pokud není reservace do určité doby obnovena tak pak zanikne.

Význam zpráv protokolu RSVP:

PathTear – odstraní Path stav ze všech směrovačů

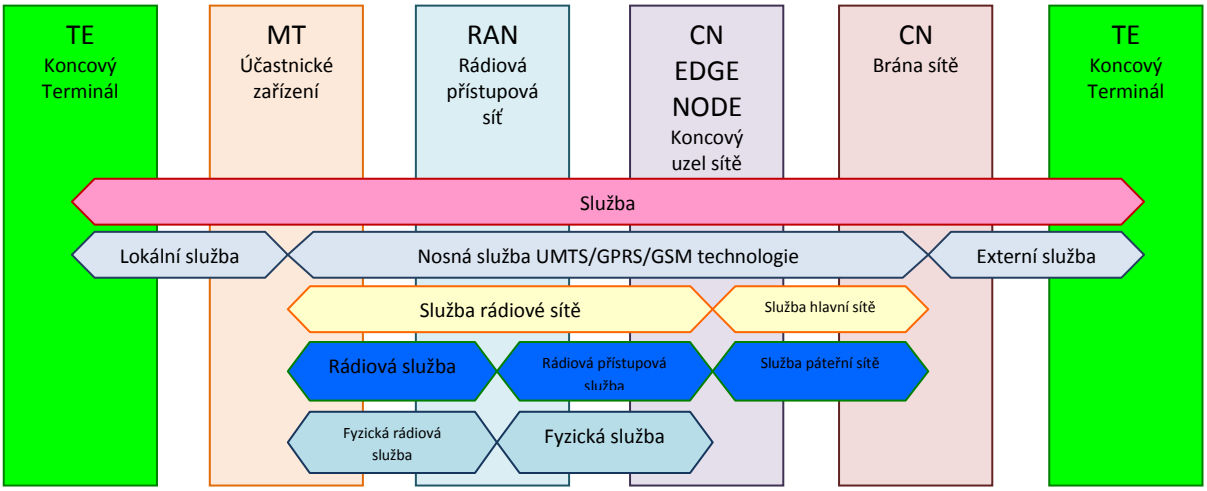
ResvTear – odstraní rezervaci ze všech měrovačů

PathErr – chyba při posílání Path zprávy

ResvErr – chyba při posílání Resv zprávy

2.1.3 Technologie QoS v sítích s implementací IMS

Principy QoS v mobilních komunikacích byly definovány v dokumentech organizací 3GPP v TS23.207 pro GSM/GPRS z června r. 2007 a v TS23.107 pro UMTS ze září 2007.



Obrázek 2-2. Architektura QoS v sítích UMTS/GPRS

V sítích s technologiemi UMTS i GPRS jsou definovány čtyři třídy služeb:

- **conversational class**, konverzační třída je určena pro real-time aplikace. Tato služba vyžaduje minimální zpoždění a minimální kolísání zpoždění. Typickým příkladem je klasický telefonní hovor.

- **streaming class,** třída proudového přenosu je určena pro jednosměrný mediální přenos. Tato služba vyžaduje minimální nebo žádné kolísání zpoždění. Typický příklad internetové radiové vysílání.

- **interactive class,** interaktivní třída je určena pro přenos typu dotaz-odpověď. Tato služba vyžaduje minimální chybovost.

- **background class,** třída přenosu na pozadí je určena pro přenos s nejnižší prioritou.

Tabulka 2-2. Základní vlastnosti QoS UMTS/GPRS tříd [13]

třída/vlastnosti	konverzační třída	třída přenosu datového proudu	interaktivní třída	přenos na pozadí
základní vlastnosti	pracující v reálném čase	pracující v reálném čase	nepracující v reálném čase	nepracující v reálném čase
	minimální, striktně omezené zpoždění	minimální kolísání zpoždění	komunikace typu dotaz-odpověď	bez časového omezení doručení odpovědi
	minimální kolísání zpoždění		minimální bitová chybovost	minimální bitová chybovost
	obousměrná komunikace	jednosměrná komunikace	obosměrná (zpravidla asymetrická komunikace)	obousměrná i jednosměrná komunikace
příklad	hovorová služba	vysílání audio či video toku	přístup na web, do databáze, atd.	stahování souborů, emailů, atd.

V každé třídě jsou různé nároky na kvalitativní parametry. Tyto parametry jsou:

- maximální rychlost [kbit/s] – aplikace může touto maximální okamžitou bitovou rychlostí posílat data po omezenou dobu. Po tuto dobu síť garantuje jejich přenos.
- garantovaná rychlost [kbit/s] – garantovaná průměrná bitová rychlost
- pořadí doručení [ano/ne] – požadavek na zachování pořadí datové jednotky během přenosu přes síť
- maximální velikost datové jednotky [oktet] – síť může garantovat sjednané parametry pro datové jednotky do této velikosti
- informace o formátu datové jednotky [bity] - specifikace možných velikostí datových jednotek, na základě této specifikace je síť schopna lépe využít rádiové prostředky
- chybovost datové jednotky – je to poměr mezi chybnými či ztracenými datovými jednotkami a celkovým provozem v síti za sjednaných podmínek
- doručení chybných datových jednotek [ano/ne/-] - způsob zacházení s chybnými datovými jednotkami. Ano určuje další zpracování a vyhodnocení na základě typu chyby. Ne určuje zahození datové jednotky. Symbol [-] určuje systém nevyužívá detekci chyb
- zpoždění přenosu – určuje maximální velikost zpoždění.
- priorita zpracování provozu – určuje relativní důležitost datových jednotek.
- Priorita alokace/pozdržení – určuje relativní důležitost služby. Je sjednávána mezi uživatelem a poskytovatelem služeb.
- statický popis zdroje – určuje charakter zdroje. V současnosti jen dva typy hovor a neznámý, dají se očekávat další.
- indikace signalizačních informací – určuje označení datové jednotky jako signalizační, taková jednotka má pak sítí zajištěno jiné zacházení.

Uživatel a operátor se dohodnou na QoS profilu uživatele. Tento profil je uložen v databázi HSS. Těchto profilů může být i více pro každou službu zvlášť. Nejčastější kvalitativní parametr pro kvalitu dnešních služeb, je přenosová rychlost. V úvahu přichází jak maximální tak garantovaná. Při žádosti o spojení jsou z HSS načteny informace o jednotlivých profilech uživatele pro jednotlivé služby. Na základě těchto parametrů jsou přiděleny síťové prostředky.

3 Autentizace a autorizace (AAA)

V datových sítích a nejen v nich je důležitá bezpečnost. Bezpečností sítě se rozumí minimalizace zranitelných míst síťových prostředků. K tomu se využívá systém založený na AAA (Authentication, Authorization and Accounting), nebo-li autentizace, autorizace a účtování.

Autentizace – znamená potvrzení, že uživatel je platným odběratelem požadovaných služeb. Ověření lze dosáhnout po představení identity. Může být jednosměrná i obousměrná. Jednosměrná je ověření uživatele vůči serveru. Obousměrná je vhodnější, protože nemůže dojít k podvrhu ze strany serveru. Obousměrná tedy umožňuje ověření obou koncových zařízení.

Autorizace – znamená ověření, zda může být specifická služba poskytnuta pro konkrétního uživatele ověřeného na základě autentizace. Autorizace může být omezena rozsahem poskytnuté služby např. časové omezení, nebo počet přihlášení jednoho uživatele.

Účtování – znamená sledování využívání poskytnutých služeb uživateli. Tyto informace jsou pak dále zpracovány poskytovatelem ať už skutečně pro vyúčtování nebo jiné účely. Tyto informace jsou uloženy na ověřovacích serverech, které jsou uvnitř sítě.

Bezdrátové sítě mají oproti sítím kabelovým jednu velkou nevýhodu z hlediska bezpečnosti. U bezdrátových sítí není technicky možné omezit prostor, ve kterém je možné signál zachytit. U kabelových sítí se musíme dostat ke kabelům, abychom byli schopni odposlouchávat komunikaci, ale u bezdrátových sítí nám stačí být jen v dosahu signálu vysílače, což v některých případech může být oblast i několik kilometrů od vysílače. Proto je nutné u těchto sítí zavést bezpečnostní opatření, které zabrání potencionálním útočníkům vniknout do sítě, nebo odposlouchávat data.

3.1 Možnosti zabezpečení

a) Jednou z možností jak zabezpečit data je šifrování. Může se jednat o symetrické nebo asymetrické šifrování. Při symetrickém šifrování obě strany sdílejí stejný šifrovací klíč. U asymetrického šifrování se data zašifrují jedním klíčem a druhým se dešifrují. Přitom oba klíče tvoří jedinečný pár.
b) Nejjednodušším typem autentizace je uživatelské jméno a heslo. Největší výhodou je jeho nenáročnost pro uživatele. Pokud se samozřejmě někomu podaří odposlechem či jiným způsobem zjistit náš login a heslo má takovýto „útočník“ plný přístup ke službám, které jsou určeny někomu jinému. Tato autentizace je zejména závislá na kvalitě (složitosti) zvoleného hesla.
c) Další typem autentizace je jednorázové heslo. Tento způsob je spolehlivější, ale také náročnější na speciální vybavení. Toto vybavení může být softwarové nebo hardwarové. Speciální vybavení pro každé spojení vygeneruje jiné heslo.
d) Dále jsou to certifikáty, ty vydává server a uživatel je má uloženy. Tento certifikát je nejlépe mít uložen na zařízení, které není trvale připojeno k síti, aby nebylo možno náhodně tento certifikát získat.

e) Jedním z dalších autentizací je zařízení autentizační kalkulátor. Toto zařízení pro každé spojení se serverem generuje nové jednorázové heslo, je zasynchronizováno se serverem.

3.2 Protokol Diameter

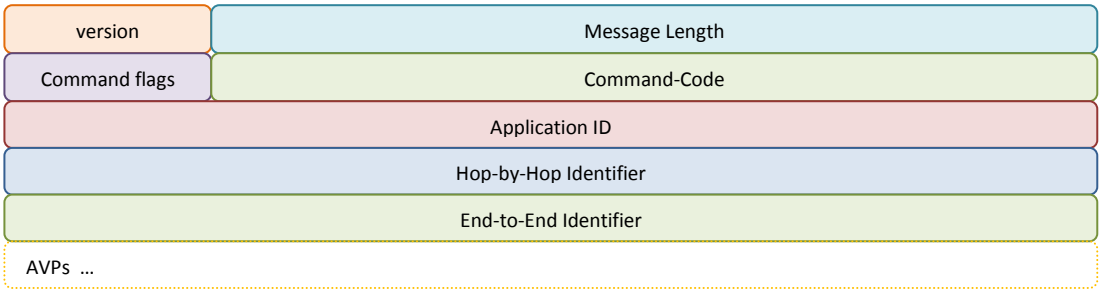
Diameter je protokol zajišťující v sítích princip AAA.
Základní vlastnosti protokolu Diameter jsou:

- pro přenos používá TCP a SCTP,
- jde výhradně o protokol pro komunikaci klient→server, s výjimkou podpory některých zpráv generovaných serverem,
- je možno použít stavový i bezstavový model,
- dynamické objevování uzlů (DNS, SRV, NAPTR),
- definuje metody odolávající chybám,
- oznamuje chyby,
- podporuje roaming,
- lze definovat nové příkazy, je snadno rozšiřitelný,

3.2.1 Hlavní data protokolu Diameter

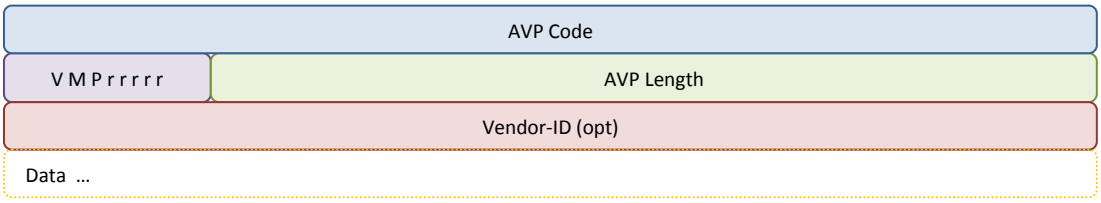
Tak jako například komunikace na bázi protokolu SIP se děje vzájemně mezi uživatelem a serverem je i komunikace protokolem Diameter komunikací mezi uživatelem a serverem.

Hlavní části při komunikaci klient server jsou Relay Agent, Proxy Agent, Redirect Agent a Translation Agent. Proxy Agent zajišťuje dopravu dotazů a odpovědí v komunikaci mezi klientem a serverem. Relay Agent zajišťuje přepojování na základě přepojovací tabulky. Redirect Agent zajišťuje přesměrování zpráv na jiného agenta nebo přímo na dotazovaný server. Translation Agent zajišťuje překlad zpráv mezi dvěma zařízeními s rozdílnými protokoly (např. Diameter - RADIUS). Účtování v protokolu je založeno na schopnosti zjišťovat stav v reálném čase. Tento model znamená, že plán účtování provádí vždy pouze jeden ze dvou oprávněných. Záleží na cestě a čase účtovacích dat. Server pomocí Acct-Interim-Interval a Accounting-Realtime-Required AVPs řídí činnost Diameter uživatele. Všechny jeho aktivity jsou zaznamenávány pomocí jednoduchých zpráv START_RECORD, STOP_RECORD, INTERIM_RECORD a ukládány na server, kde jsou pak dále využity.



Obrázek 3-1. Diameter hlavička

version – určuje verzi protokolu
Message Length – 3 oktety, určuje velikost zprávy včetně hlavičky
Command Flags – 8bitů, jsou tyto příkazy | R P E T r r r r |
R(equest) – označuje žádost
P(roxiable) – je-li nastaveno zpráva je pro Proxy nebo Relay nebo Redirect. Není-li nastaveno jedná se o lokální proceduru.
E(rror) – chybová zpráva
T(Potentially re-transmitted message) – při opakovaném zasílání požadavků, které nebyly potvrzeny
r(eserved) – volné bity pro budoucí možné rozšíření
Command Code – 3 oktety, určuje příkaz
Application ID – 4 oktety, určuje jaká zpráva je obsažena, jestli autentizací nebo účtování nebo jde o poskytnutí speciální služby.
Hop-by-Hop Identifier – 4 oktety, zajišťuje sjednocení žádostí a odpovědí, tj. přidělí identifikátor žádosti a stejný identifikátor je u odpovědi.
End-toEnd Identifier – 4 oktety, zajišťuje identifikace zpráv, aby nedošlo k jejich duplikaci
AVPs – nese informace o autentizaci, autorizaci a účtování. (AVP – Attribute-Value-Pairs)



Obrázek 3-2. Hlavička AVP

AVP Code – jedinečná čísla 1-255 jsou kompatibilní s protokolem Radius od čísla 256 jsou typická pro protokol Diameter.
AVP Flags – informuje přijímač jak přijatou zprávu zpracovat
AVP Length – určuje délku celého AVP
Vendor-ID – je nepovinný údaj a určuje specifické funkce
Dále následují AVP data.

3.2.2 Diameter v IMS

Autentizace a autorizace v IMS je zajišťována při komunikaci v jádru tohoto systému, k tomu je využíváno rozhraní Cx. Ve standardu 3GPP TS 29.228 jsou vyspecifikovány zprávy tohoto rozhraní. V následující tabulce je přehled těchto zpráv.

Tabulka 3-1. Přehled Cx zpráv protokolu Diameter v IMS

Cx zpráva	Zdroj	Cíl	Název příkazu	Kód	Zkratka
Cx-Query + Cx-Select-Pull	I-CSCF	HSS	User-Authorization-Request	300	UAR
Cx-Query Resp + Cx-Select-Pull Resp	HSS	I-CSCF	User-Authorization-Answer	300	UAA
Cx-Put + Cx-Pull	S-CSCF	HSS	Server-Assignment-Request	301	SAR
Cx-Put Resp + Cx-Pull Resp	HSS	S-CSCF	Server-Assignment-Answer	301	SAA
Cx-Location-Query	I-CSCF	HSS	Location-Info-Request	302	LIR
Cx-Location-Query Resp	HSS	I-CSCF	Location-Info-Answer	302	LIA
Cx-AuthDataReq	S-CSCF	HSS	Multimedia-Authentication-Request	303	MAR
Cx-AuthDataResp	HSS	S-CSCF	Multimedia-Authentication-Answer	303	MAA
Cx-Deregister	HSS	S-CSCF	Registration-Termination-Request	304	RTR
Cx-Deregister Resp	S-CSCF	HSS	Registration-Termination-Answer	304	RTA
Cx-Update_Subscr_Data	HSS	S-CSCF	Push-Profile-Request	305	PPR
Cx-Update_Subscr_Data Resp	S-CSCF	HSS	Push-Profile-Answer	305	PPA

Identifikace uživatele probíhá na základě informací uložených na kartě UICC (Universal Integrated Circuit Card). Je zde uloženo unikátní identifikační číslo přidělené operátorem a je jedinečné v celosvětové síti. Dále je zde uloženo vlastní telefonní číslo. Na obrázku 3-3. je SIM-karta mobilního terminálu.

Každý uživatelský terminál (např. mobilní telefon) je identifikován několika kódy.

a) IMEI identifikační číslo - identifikuje zařízení, jeho součástí jsou:
   - TAC (Type Approval Code) slouží k identifikaci typu zařízení
   - FAC (Final Assembly Code) identifikace výrobce zařízení
   - SNR (Serial number) sériové výrobní číslo, zadáno výrobcem

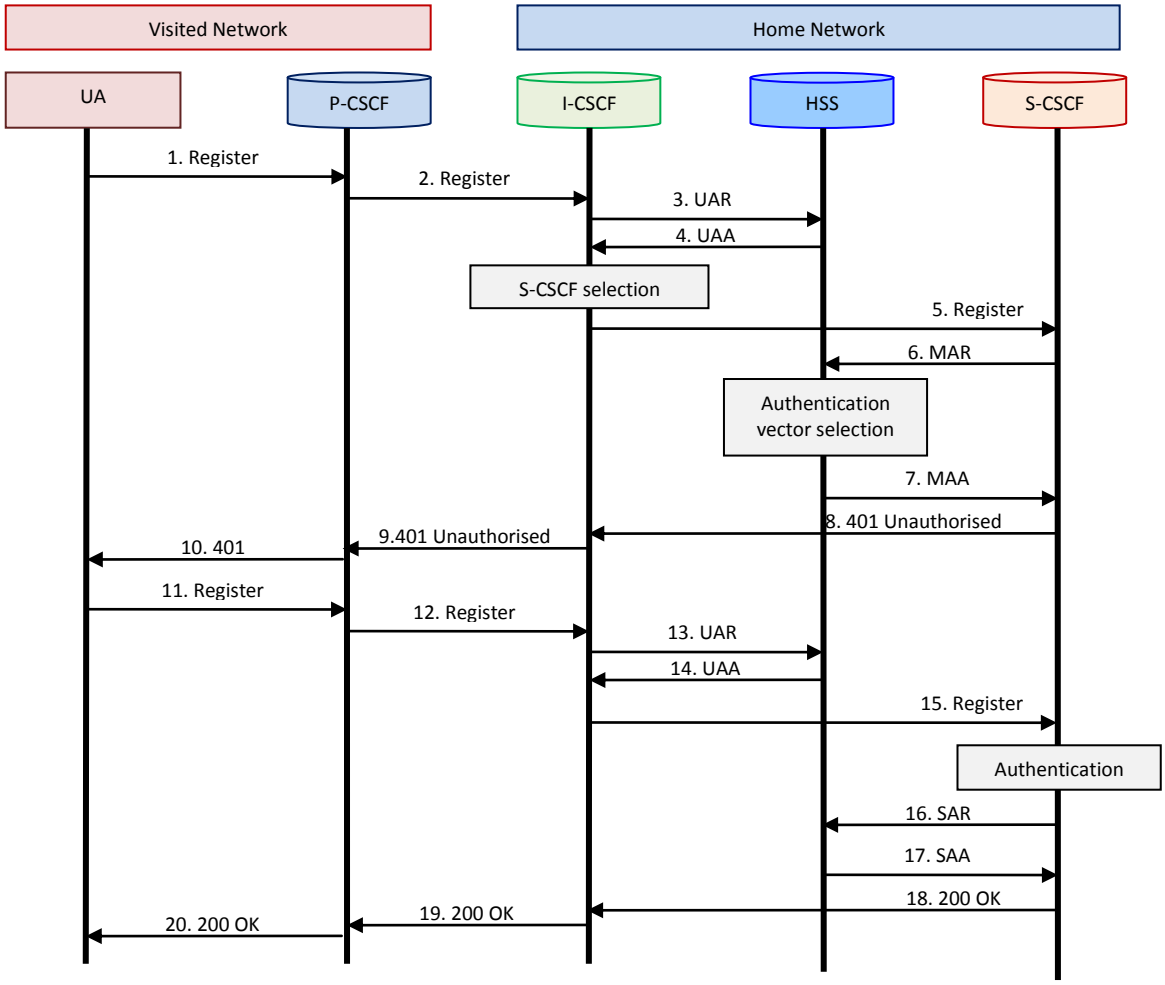
b) SIM-karta identifikace uživatele konkrétní sítě s konkrétními službami
   - MCC (Mobile Country Code) identifikace státu,
   - MNC (Mobile Network Code) identifikace sítě – poskytovatele
   - MSIN (Mobile Subscribe Identification Number) registrační číslo účastníka

c) MSISDN skutečné telefonní číslo účastníka

Obrázek 3-3. SIM, USIM a ISIM v UICC pro 3GPP IMS terminal

Tabulka 3-2. Přehled parametrů Cx AVP Diameteru

Cx parametr	AVP Name
Visited Network Identifier	Visited-Network-Identifier
Public Identity	Public-Identity
Private Identity	User-Name
S-CSCF Name	Server-Name
AS Name	
S-CSCF capabilities	Server-Capabilities
Result	Result-Code
	Experimental-Result-Code
User profile	User-Data
Server Assignment Type	Server-Assignment-Type
Authentication data	SIP-Auth-Data-Item
Item Number	SIP-Item-Number
Authentication Scheme	SIP-Authentication-Scheme
Authentication Information	SIP-Authenticate
Authorization Information	SIP-Authorization
Confidentiality Key	Confidentiality-Key
Integrity Key	Integrity-Key
Number Authentication Items	SIP-Number-Auth-Items
Reason for de-registration	Deregistration-Reason
Charging Information	Charging-Information
Routing Information	Destination-Host
Type of Authorization	Authorization-Type
Associated Private Identities	Associated-Identities
Digest Authenticate	SIP-Digest-Authenticate
Digest Realm	Digest-Realm
Digest Domain	Digest-Domain
Digest Algorithm	Digest-Algorithm
Digest QoP	Digest-QoP
Digest HA1	Digest-HA1
Line Identifier	Line-Identifier
Wildcarded PSI	Wildcarded-PSI
Wildcarded Public User Identity	Wildcarded-IMPU



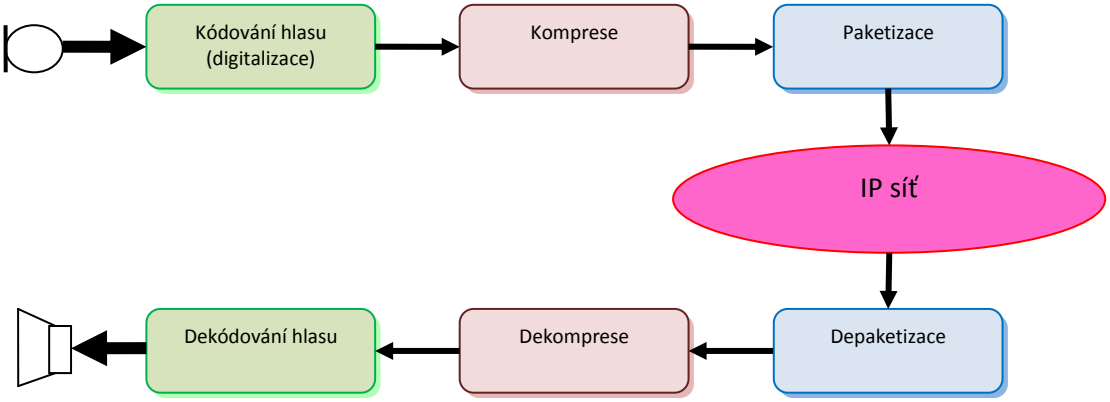
Obrázek 3-4. Prvotní registrace uživatele v síti IMS

Každá prvotní registrace (autentizace) uživatele spočívá (obrázek 3-4):

1. Účastnický přístroj odešle identifikační kód SIM karty, popř. kód zařízení (u mobilních telefonů) a žádost o autentizaci.
2. Lokalizační server tyto kódy srovná s databází. A odešle terminálu potvrzovací zprávu o autentizaci.
3. Následné každé přihlášení do sítě je jen otázkou autorizace

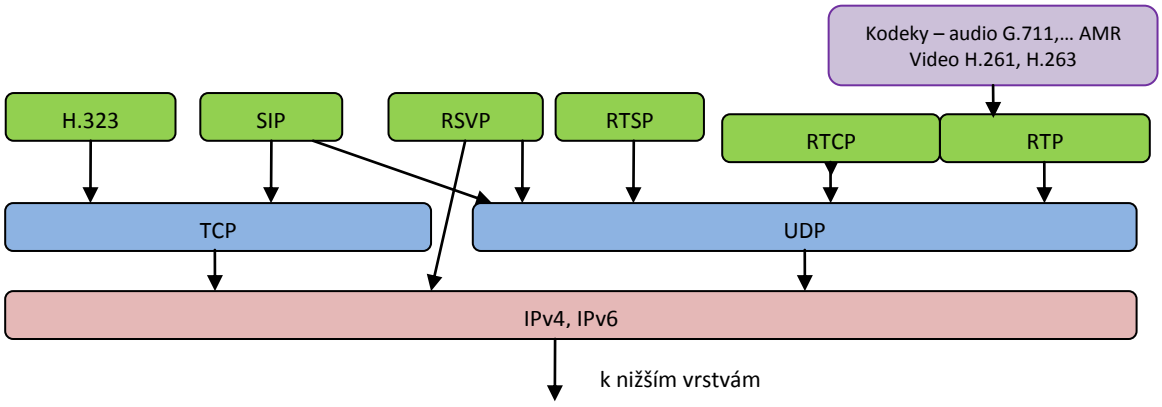
4 VoIP

VoIP (Voice over IP) je hlasová služba využívající pro přenos hlasu paketové sítě. Pro přenos hlasu po datových sítích je zapotřebí hlas nejprve digitalizovat poté zakódovat, zkomprimovat, zabalit do paketů a odeslat sítí k příjemci. Příjemce musí s daty naložit v opačném pořadí tj. přijmout pakety, dekomprimovat, dekódovat a převést je do sluchátka. Na následujícím obrázku vidíme základní princip přenosu hlasu po digitálních sítích.



Obrázek 4-1. Princip přenosu hlasu IP sítěmi

Pro komunikaci dvou zařízení v datové síti je zapotřebí použít dohodnuté standardy komunikace a těmi jsou právě protokoly. Pro přenos dat v IP sítích jsou zapotřebí tyto protokoly:



Obrázek 4-2. Zjednodušený model protokolové sady

- **Kodeky** audia a videa jsou nutné pro přenos hlasu a videa po datových sítích.
- **H.323** – řídicí protokol IP telefonie je v architektuře pro mobilní telefonii na bázi IMS nahrazen protokolem SIP.
- **SIP** – řídicí textově orientovaný signalizační protokol.
- **RSVP** – protokol pro reservaci prostředků na Internetu.
- **RTSP** – protokol aplikační vrstvy navazuje a řídí audio a video stream mezi klientem a serverem

- **RTP/RTCP** – protokol pro přenos dat v reálném čase.
- **TCP** – protokol transportní vrstvy. TCP je spojově orientovaný protokol pro přenos dat na transportní vrstvě se spolehlivým doručováním.
- **UDP** – protokol transportní vrstvy. UDP je nespojově orientovaný protokol bez potvrzování doručení. Z tohoto důvodu je ovšem oproti TCP rychlejší.
- **IP** – základní protokol pro přenos dat v paketových sítích označovaný se spolehlivostí best-effort.

4.1 Kódování hlasu

Aby mohl být hlas, který je analogový, přenesen pomocí digitální sítě, je nutné jej přepracovat na digitální. To se děje v analogově digitálním převodníku. Protože se tato bakalářská práce má zabývat mobilními sítěmi budu se tedy věnovat kódování vhodnému pro přenos mobilními sítěmi.

Analogově digitální převodník může být součástí kodéru zdroje signálu. Zdrojové kódování má za cíl snížit přenosovou rychlost signálu, tím se sníží požadavky na šířku pásma rádiového kanálu. Horní mezní kmitočet zdrojového kódování řečových signálů je 4kHz. Používají se tři základní skupiny kodérů:

- kodéry tvarového průběhu (Waveforms coders) – zdrojové kódování tvaru vlny
- vokodéry (Vocoders, Voice coders) – parametrické zdrojové kódování
- hybridní kodéry – hybridní zdrojové kódování, kombinace obou předchozích skupin

Hodnocení kvality kodérů se provádí dle stupnice MOS (Mean Option Score) kde:

1= nepřijatelná, 2=špatná, 3=přijatelná, 4=dobrá, 5=nepřijatelná. Za výchozí hodnotu zdrojového kódování se považuje PCM (Pulse Code Modulation) pulzně kódová modulace. Tato modulace převádí hovorový analogový signál v rozsahu 300 až 3400 Hz na digitální signál ve třech krocích a to vzorkováním, kvantováním a kódováním. Při vzorkovacím kmitočtu 8kHz se vytvoří digitální signál o přenosové rychlosti 64kbit/s. V následující tabulce jsou uvedeny používané kodeky s jejich přenosovými rychlostmi a hodnocením MOS.

Tabulka 4-1. Kodeky s přenosovými rychlostmi a hodnocením MOS

Kodek	Přenosová rychlost [kbit/s]	MOS [1 až 5]
G.711 (PCM)	64	4,1
G.726 (ADPCM)	32	3,85
RPE-LPC	14,77	3,54
MPE-LTP	13,20	3,27
SBC-APCM	13,00	3,14
SBC-ADPCM	15,00	2,92

Na prvním řádku je uveden kodek G.711, pro možnost srovnání.

Kodek G.726 se v mobilních sítích nepoužívá, ale najdeme ho v přenosných telefonech. Systém ADPCM (Adaptive Differential Pulse Code Modulation) je adaptivní diferenciální impulzová kódovaná modulace. S její pomocí lze dosáhnout redukci bitového toku a zlepšení rekonstruovaného signálu.

Na dalších čtyřech řádcích jsou kodeky používané v sítích GSM.

RPE-LPC (Regular Pulse Excitation – Linear Predictive Coding) je kombinace regulárního buzení, kde je přesně stanovena vzájemná poloha impulsů a určuje se tedy pouze poloha prvního impulsu s lineárním prediktivním kódováním, kde zpracování signálu je časové (vokodér).

MPE-LTP (Multi Impulse Excitation – Long Term Prediction) – multiimpulsní buzení, kde vzájemná poloha a velikost impulsů se určují samostatně s dlouhodobou predikcí, která zjemňuje hovorové spektrum.

Poslední dva řádky jsou varianty PCM. U obou těchto kódování je využito principu maskovacího jevu lidského sluchu. Člověk je schopen vnímat zvuky jen v určitém kmitočtovém pásmu od 16 Hz do 16 kHz a určité síly. Využije se zde tedy zdrojové subpásmové kódování SBC (SubBand Coding), kde se akustický signál rozdělí na kmitočtová pásma a podle nejsilnějších složek se vybere, kterým užitečným maskovacím signálem bude překryt. Tímto způsoben dosáhneme podstatné snížení přenosové rychlosti, bez toho aniž by se subjektivně snížila kvalita přijímaného signálu. Maskovacího jevu se využívá u zdrojového kódování těchto typů:

- MPEG1 (Audio Layer1) – nejjednodušší, ale poskytuje jen malou redukci
- MPEG1 (Audio Layer2) – oproti Layer1 snižuje přenosovou rychlost na nízkých kmitočtech
- MPEG1 (Audio Layer3) – snižuje bitovou rychlost, používá modifikovanou diskrétní kosinovu transfomaci MDCT

Systém IMS je určen pro širokopásmovou komunikaci různých komunikačních systémů. Pro mobilní systém 3G UMTS je použito kódování řečových signálů pomocí řečového kodeku AMR (Adaptive Multi-Rate Speech Coding). Výstupní přenosová rychlost se mění v závislosti na řečové aktivitě. Během telefonního hovoru nehovoří účastníci najednou, ale v hovoru se střídají. Proto jsou jednotlivé směry přenosu využity na polovinu. Detektor hlasové aktivity sleduje, kdy účastník nehovoří. V tom okamžiku se do signálu vkládá informace o komfortním šumu. Tento způsob kódování zajišťuje snížení přenosové rychlosti a tím zvýšení kapacity celého systému. Takto navržený kodek dosahuje přenosové rychlosti od 12,20 kbit/s do 1,80 kbit/s. Nejmenší hodnoty je dosaženo během hovorového klidu. Tabulka 4-2 ukazuje seznam kodeků pro mobilní sítě dle 3GPP TS26.103 V7.0.0 (VI. 2007).

Tabulka 4-2. Kodeky pro GSM a UMTS

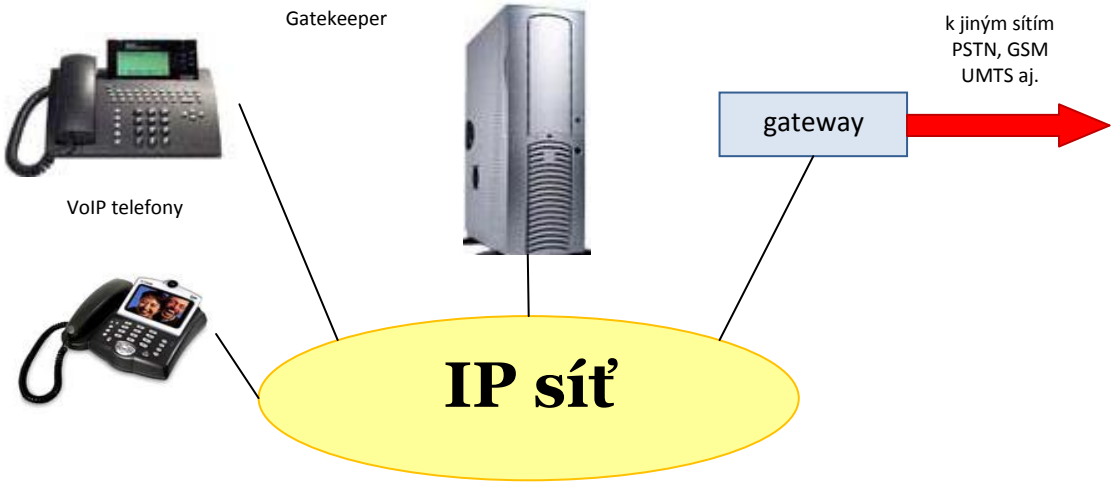
Typ kodeku - název	Zkratka	přen. rychlost [kbit/s]
GSM Full Rate	GSM FR	13,0
GSM Half Rate	GSM HR	5,6
GSM Enhanced Full Rate	GSM EFR	12,2
Full Rate Adaptive Multi-Rate	FR AMR	
Half Rate Adaptive Multi-Rate	HR AMR	
UMTS Adaptive Multi-Rate	UMTS AMR	
UMTS Adaptive Multi-Rate 2	UMTS AMR 2	
TDMA Enhanced Full Rate	TDMA EFR	7,4
PDC Enhanced Full Rate	PDC EFR	6,7
Full Rate Adaptive Multi-Rate WideBand	FR AMR-WB	
UMTS Adaptive Multi-Rate WideBand	UMTS AMR-WB	

4.2 Architektury VoIP

V současnosti vedle sebe existují dvě standardizované architektury, které jsou označovány podle stěžejních protokolů, a to protokolů H.323 a SIP. Protokolu SIP je podrobně popsán v kapitole 4.3.3. Protokol H.323 se pro komunikaci VoIP v mobilních sítích nepoužívá. Proto jej popíši velmi stručně.

4.2.1 Architektura H.323

Základními prvky jsou terminál, gatekeeper, gateway a MCU
Terminálem se rozumí koncové zařízení – telefon nebo PC
Gateway – je brána spojující architekturu H.323 s jinou architekturou pro hlasovou službu, nejčastěji s telefonní sítí či s architekturou SIP.
MCU – jednotka, která zajišťuje provoz při konferečních hovorech
Gatekeeper – je centrem celé architektury H.323. Probíhá zde autentizace, autorizace, účtování služeb, překlad telefonních čísel na IP adresy, směrování hovorů a další.



Obrázek 4-3. Architektura H.323

4.3 Protokoly VoIP

4.3.1 Protokol SDP

Pomocí protokolu SDP (Session Description Protocol) jsou přenášeny detaily potřebné zejména při přenosu multimediálních aplikacích. S jeho pomocí se přenáší informace o multimediálních tocích.

SDP protokol zahrnuje informace o:

- typ média - obrazový, zvukový aj
- transportní protokol – RTP/UDP/IP, H320 atd.
- formát média – H.261 video, MPEG video atd.
  při multicastovém vysílání ještě obsahuje zprávy o multicastové adresy pro média
- transportní port
- čase aktivní relace
- informace o doručení
- kontaktní informace o uživateli (uživatelích)
- název a účel relace

SDP je textově orientovaný protokol. Hlavní doporučenou znakovou sadou je UTF-8, ale povoluje též sadu ISO 8859-1. Každá SDP zpráva obsahuje několik řádků. Každý řádek je složen ve formátu *typ = hodnota*.

Příklad popisu [převzato z RFC 2327]:

```
v=0
o=mhandley 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP seminar
i=A Seminar on the session description protokol
u=http://www.cs.ucl.ac.uk/staff/M.Handley/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait
```

Jednotlivé řádky popisují:

značka	popis	povinný údaj
Session description – popis relace		
v=	protocol version - verze protokolu	ano
o=	origin - identifikátor tvůrce relace – uživatelské jméno, číslo relace (časová značka NTP), typ sítě, typ adresy (IPv4), adresa	ano
s=	session name - název relace – formát ISO 10646	ano

značka	popis	povinný údaj
i=	session information popis relace – jednoduchý popis relace (může obsahovat vlastnosti aj.)	ne
u=	URI of description odkaz na další informace o relaci	ne
e=	email adress – emailová adresa	ne
p=	phone number – telefonní číslo	ne
c=	connection information informace o spojení – typ sítě, typ dresy (IPv4), adresa	ne
b=	bandwith information šířka pásma	ne
z=	time zone adjustments časová zóna	ne
k=	encryption key šifrovací klíč	ne
a=	atributy vlastnosti relace – mohou být typu : kategorie, klíčové slovo, packet time – čas v milisekundách pro data v paketu, recvonly – pouze přijmout, type, orient – povolené hodnoty portrait, landscape a seascape (orientace), dále zde mohou být popsány speciální porty (rtp, rtcp) atd.	ne
time description - časový popis		
t=	time the session is aktive časování (začátek a konec relace) – doba startu, doba běhu dáme-li druhý údaj roven nule pak je relace ohraničena pouze jako jedno vysílání	ano
r=	repeat times počet opakování relace	ne
media description – popis média		
m=	název média a transportní adresa typ média, port, transportní protokol (RTP),	ano
dále zde mohou být atributy „i, c, b, k, a. se stejným významem jako výše		ne

Tabulka 4-3. SDP popis

4.3.2 Protokoly pro přenos dat v reálném čase

4.3.2.1 Protokoly RTP/RTCP

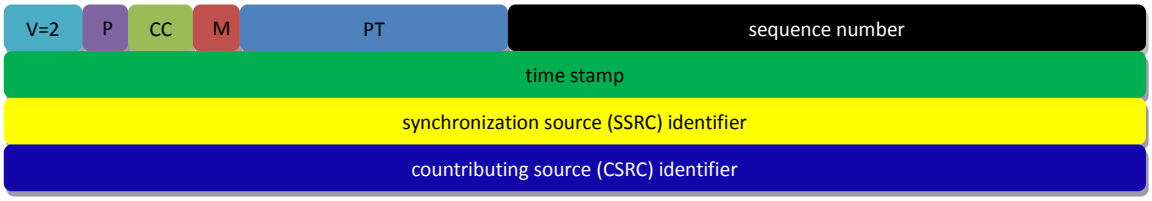
RTP (Real-time Transport Protocol) je určený pro distribuce audia a videa na Internetu. Samotný protokol RTP se řadí mezi nespolehlivé služby. Jeho spolehlivost je proto kontrolována protokolem RTCP (RTP Control Protokol). Protokol RTP/RTCP má zabudována většina audio a video přehrávačů.

RTP payload – data posílaná v RTP paketu. Mohou to být zvukové sekvence nebo komprimovaná obrazová data.

RTP paket – sestává s fixní hlavičky, obsahuje informace o pořadí paketu, o čase vzniku, a o konkrétním streamu. RTP paket nemusí obsahovat pouze jeden RTP paket, ale může obsahovat i několik RTP paketů. Celý RTP „maxi“ paket se pak vloží do UDP paketu.

RTCP paket – má podobnou strukturu jako RTP paket. Sestává s fixní hlavičky a následných elementů, které se mění v závislosti na typu RTCP paketu. Více RTCP paketů je sloučeno do jednoho většího RTCP paketu a odesláno jako jeden RTCP paket.

RTP media type – je seznam jaké mediální typy mohou být přenášeny během jednoho RTP přenosu.



Obrázek 4-4. Formát RTP hlavičky

V (version) 2 bity - informace identifikuje verzi RTP v současné době verze 2

P (padding) 1 bit – informace o přítomnosti doplňujícího oktetu na konci paketu, určuje počet přidaných oktetů

X (extension) 1 bit - je-li na konci doplňující 8-bitové pole pak je stálá hlavička následována rozšiřovací hlavičkou. Rozšiřovací mechanizmus je určen pouze k omezenému využití

CC (CSRC coount) 4 bity – CSRC obsahuje počet CSRC identifikátorů (zdrojů), které obsahuje rozšířená hlavička

M (marker) 1 bit – závisí na typu přenášených dat (PT)

PT (payload type) 7 bitů – typ přenášeného média (užitečné zatížení), aplikace na straně příjemce prozkoumá typ dat a dle toho je zpracuje. Pro video či audio konference jsou zpracovány tabulky s čísly určující kodeky pro jednotlivé typy dat (audio či video).

sequence number 16 bitů – identifikační pořadové číslo paketu, přijímací strana dle tohoto identifikátoru zjistí stav přijatých paketů, např. jejich ztrátu, pakety mimo pořadí aj. Protože důsledkem malého počtu bitů dochází k tzv. přetečení (vynulování), dochází u real-time aplikací jako např. u VoIP k nulování každých 20 min. Z důvodu bezpečnosti není počáteční hodnota tohoto čísla nulová, ale je vybrána náhodně.

timestamp 32 bitů – časová značka sloužící k synchronizaci, toto číslo neustále narůstá, v okamžiku, kdy dosáhne maximální hodnotu, je jeho hodnota vynulována

SSRC 32 bitů – identifikuje zdroj, číslo, které je náhodné a pro každého účastníka relace jedinečné. Pro všechny pakety od jednoho účastníka jsou SSRC stejná, tak tato pakety tvoří jeden tok.

CSRC 32 bitů – seznam zdrojů, rozeznává jednotlivé přispěvatele RTP toků, nručí ovšem za jejich správnou synchronizaci

HeaderExtension – rozšířená hlavička, je uložena před vlastním payload data a je signalizována bitem X

Payload Header – povinná hlavička zátěže, obecná informace o každém typu zátěže

Payload Data – poslední část RTP paketu

RTCP (RTP Control Protocol) – kontroluje data přenášená pomocí RTP. Zajišťuje čtyři hlavní funkce:

- Poskytuje odezvu na kvalitu přenesených dat
- Garantuje transportní úroveň
- Při on-line spojení každý účastník spojení (např. videokonference) může vidět celkový

počet účastníků spojení
- Zprostředkovává minimální řízení

Druhy RTCP paketů:
SR – (Sender report) zpráva vysílače
RR – (Receiver report) zpráva přijímače
SDES – (Source Description) popisovače zdrojů
BYE – signalizuje ukončení spojení
APP – (Application specific) specifické aplikační funkce

Každý RTCP paket začíná fixní částí jako RTP paket, následují prvky ve struktuře, která může být proměnná. Každý paket má velikost 32 bitového slova. Pomocí tohoto je dosažena možnost stohovatelnosti těchto paketů. Takto sloučené RTCP pakety do jednoho paketu se pak vkládají do paketů nižších vrstev jako např. UDP. Přitom každý jednotlivý RTCP paket nese svoji informaci. Slučování RTCP paketů se řídí určitými pravidly:

- statistika o sloučených paketech, v SR nebo RR, by měla být přijata či odeslána s každým sloučeným RTCP paketem
- každý nový přijímač musí přijmout CNAME (canonical name) kanonické jméno, je to jedinečné jméno v rámci jedné RTP relace
- počet a typ paketů musí být uvedeno v prvním paketu

Jeden sloučený paket musí obsahovat alespoň dva dílčí RTCP pakety s tímto formátem:

- encryption prefix (šifrovací předpona) je-li paket šifrován, musí to být uvedeno pro každý sloučený paket zvlášť
- SR nebo RR v prvním paketu sloučeného RTCP paketu slouží k ověření hlavičky paketu
- Additional RR je-li počet zdrojů větší než 31, pak by měl v dodatečné RR následovat prvotní paket
- SDES pakety obsahující CNAME položku jsou v každém sloučeném RTCP paketu
- BYE nebo APP další druhy RTCP paketů. Pouze BYE paket je vždy jako poslední.

RTP/RTCP je navržen tak, aby docházelo k automatickému přiřazování spojení. Přidělí se přenosová šířka pásma, která je rozdělena mezi účastníky. Například při audio konferenci se předpokládá, že bude hovořit vždy jen jeden účastník konference i když celkově může být účastníků konference několik. Provoz na tomto kanále podléhá přiřazovacímu pořádku. Šířka kanálu je omezena propustností sítě. Kanál je přidělován automaticky dispečerem. Kontakt s dispečerem je omezen jen na malou část přenosového kanálu, tak aby nebyl zhoršen transportní přenos (kontrolní kanál). Interval mezi jednotlivými RTCP pakety se lineárně váže k počtu účastníků spojení. U spojení s malým počtem účastníků jsou RTCP pakety zasílány s velmi malou dobou periody přibližně každých 5s. RTCP pakety by neměly zatížit linku více jak 5%. Nově připojení účastnící konference jsou přidáni k již připojeným účastníkům a dle toho se vypočte nový interval RTCP paketu.

SR (Sender Report) RTCP paket

Zpráva vysílače sestává ze tří sekcí. Může být následována ještě čtvrtou profilovou rozšiřovací částí.

V (version) 2 bity - informace identifikuje verzi RTP

P (padding) 1 bit – informace o přítomnosti doplňujícího oktetu na konci paketu

RC 5bitů – celkový počet RTCP paketů v tomto jednom sloučeném RTCP paketu (UDP datagram)

PT 8 bitů – typ paketu pro SR=200

length 16 bitů – délka paketu

SSRC 32 bitů – informace o zdroji pro synchronizaci

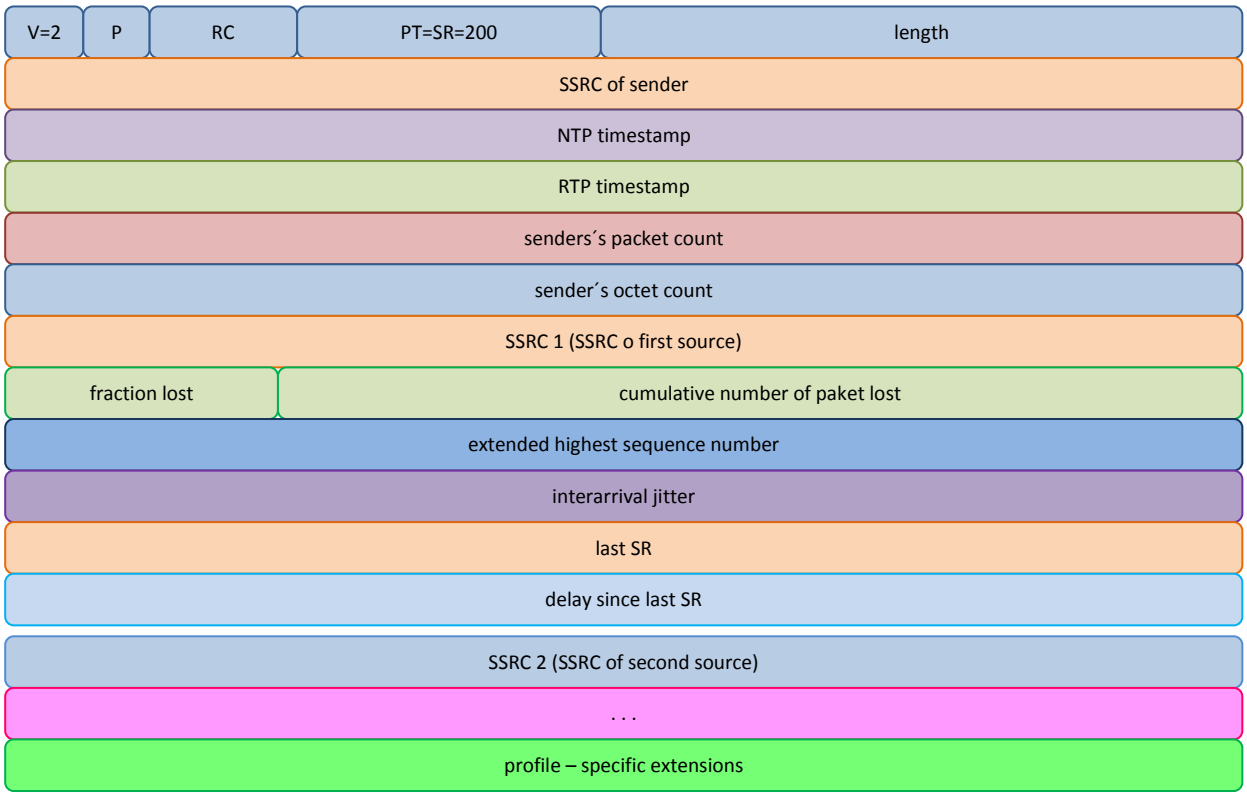
NTP 64 bitů – čas vytvoření zprávy

RTP timestamp 32 bitů – stejný čas jako NTP

sender´s octet count – celkový počet přenesených oktetů, mimo hlavičku a přidané pakety v RTP paketech

SSRC n 32 bitů – zdrojový identifikátor

Dále jsou zde uvedeny informace o ztrátách paketů od posledního generování SR, průměrné zpoždění, kolísání zpoždění a další. Všechny tyto informace jsou potřebné pro zjištění kvality spojení.



Obrázek 4-5. Příklad zprávy vysílače

Pro výpočet průměrného zpoždění v přijímačích RTP streamu jsou potřeba následující informace:

- časové razítko RTP paketu *I*.

- čas příchodu RTP paketu *I* .
- rozdíl časů dvou po sobě jdoucích paketů přijatých přijímačem a odeslaných vysílačem.
- průměrné kolísání zpoždění příchozích RTP paketů *I*.

4.3.2.2 Protokol RTSP

RTSP (Real Time Streaming Protocol) tento protokol se používá pro streamování médií na Internetu a je založen na základu RTP. Umožňuje vzájemnou domluvu klienta a serveru s tím, že uživatel má plnou kontrolu nad poskytovaným médiem. Zejména se tento protokol využije při službě video-on-deman a audio-on-deman (video nebo audio na vyžádání). Uživatel může přehrávání pozastavit následně ze stejného místa pustit dál, může přetáčet atd. RTSP je takové dálkové ovládání po síti.

RTSP request mohou být přeneseny různými cestami. Mohou mít trvalá spojení nebo jedno spojení na žádost a druhé jako odpověď nebo tzv. „malé spojení“ (connectionless mód).

Jednotlivé příkazy protokolu RTSP:

OPTIONS - získání dostupných metod
SETUP - přidělí zdroj streamů, je na začátku relace
ANNOUNCE - změna popisu mediálního objektu
DESCRIBE - získá popis mediálního objektu
PLAY - spuštění přehrávání
RECORD - start záznamu přenosu na přiděleném streamu přes SETUP
PAUSE - dočasně pozastaví přenos streamů
REDIRECT - přesměrování klienta na nová server
SET_PARAMETR - ovládání zařízení nebo kódování
TEARDOWN - přeruší přenos dat a ukončí spojení se serverem

Příklad komunikace klient server:

Získání dostupných metod:

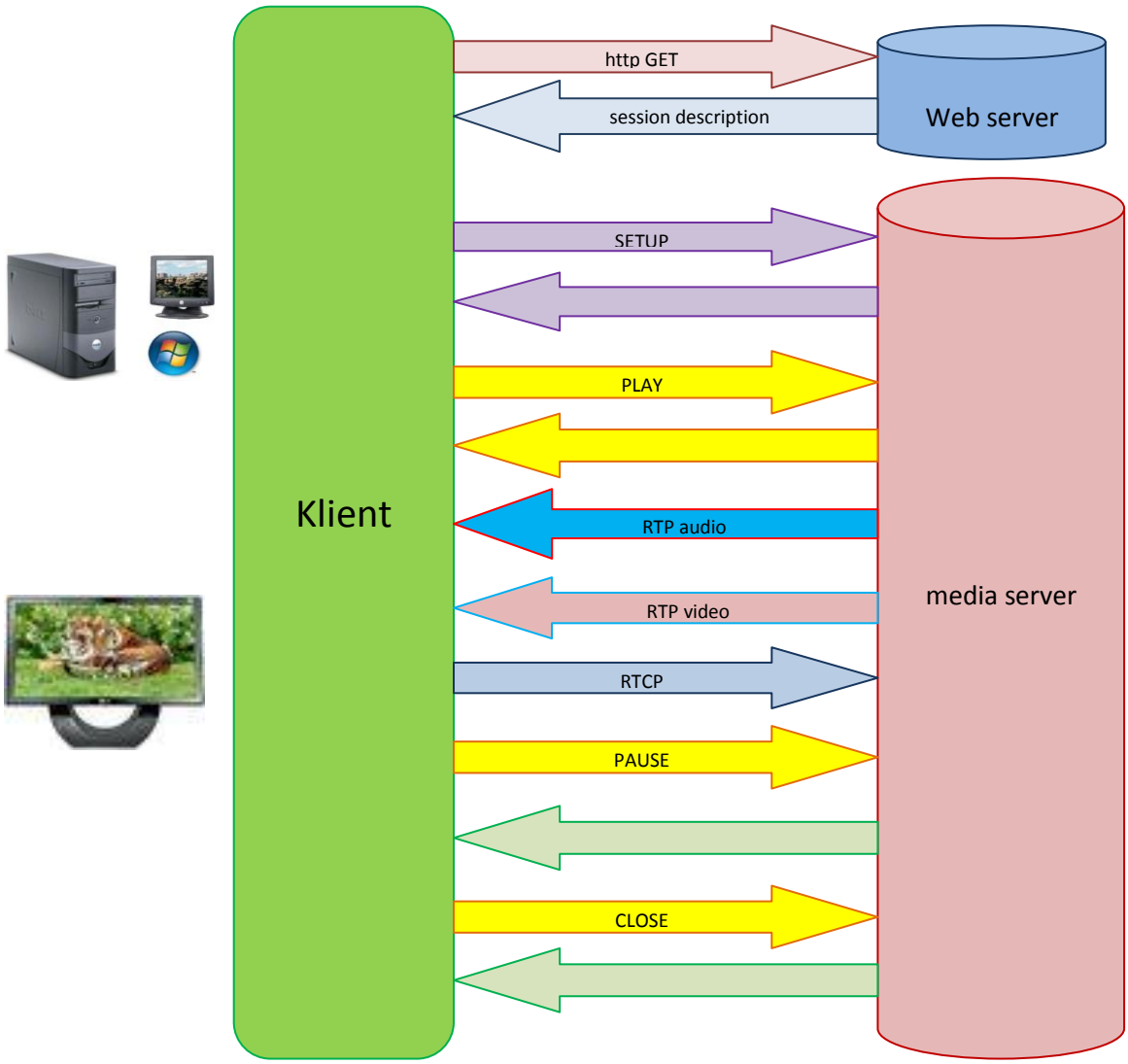
```
C->S:  OPTIONS *RTSP/1.0
       CSeq: 1
       Require: implicite-play
       Proxy-Require: gzipped-messages
S->C:  RTSP/1.0 200 OK
       CSeq: 1
       Public: DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE
```

Získání popisu streamu:

```
C->S:  DESCRIBE rtsp://server.example.com/fizzle/foo RTSP/1.0
       CSeq: 312
       Accept: application/sdp, application/rtsl, application/mheg
S->C:  RTSP/1.0 200 OK
```

CSeq: 312
Date: 30 Jun 2008 23:59:59 GMT
Content-Type: application/sdp
Content-Length: 376

v=0
o=vhladik 2890844526 2890842807 IN IP4 126.16.64.4
s=IMS Seminar
i=A Seminar on the IP Multimedia Subsystem
u=http://www.cs.mujwebicek.cz/haryk/xhladi00/ims.03.ps
e=hladv@webik.cz (Vladka Hladik)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 3456 RTP/AVP 0
m=video 2232 RTP/AVP 31
m=whiteboard 32416 UDP WB
a=orient:portrait



Obrázek 4-6. Příklad výměny RTSP zpráv

Otevření streamu a sestavení cesty:

```
C->S:  SETUP rtsp://example.com/foo/bar/baz.rm RTSP/1.0
       CSeq: 302
       Transport: RTP/AVP;unicast;klient_port=4588-4589
S->C:  RTSP/1.0 200 OK
       CSeq: 302
       Date: 31 May 2008 10:06:54 GMT
       Session: 47112344
       Transport: RTP/AVP;unicast;
         client_port=4588-4589;server_port=6256-6257
```

Pozastavení přehrávání – pause:

```
C->S:  PAUSE rtsp://example.com/fizzle/foo RTSP/1.0
       CSeq:834
       Session: 12345678
S->C:  RTSP/1.0 200 OK
       CSeq:834
       Date: 31 May 2008 10:06:54 GMT
```

Ukončení přehrávání:

```
C->S:  TEADOWN rtsp://example.com/fizzle/foo RTSP/1.0
       CSeq: 892
       Session 12345678
S->C: RTSP/1.0 200 OK
       CSeq: 892
```

4.3.3 Architektura protokolu SIP

Na vývoj IP (Internet Protocol) Multimedia Subsystem byl zejména kladen základní požadavek a to nezávislost přístupu k síti. V praxi to znamená možnost přístupu k jakékoliv službě jakoukoliv přístupovou IP sítí. Důležité je též zajištění kvality služeb QoS. Jak již bylo výše zmíněno je systém IMS postaven na protokolu Session Initiation Protocol (SIP) [2]. Protokol SIP se vyvíjí již od roku 1996. A prvním navrhovaným standardem pro protokol SIP byl v roce 1999 standard pod označením RFC 2543. V roce 2002 byl vydán nový standard pod označením RFC 3261. V tomto dokumentu je vyspecifikováno pouze jádro. Dále byl tento protokol rozšířen o další doplňky a doporučení a to pod označeními:

- RFC 3261 – SIP: Session Initiation Protocol
- RFC 3262 – Reliability of Provisional Responses in Session Initiation Protocol (SIP)
- RFC 3263 – Session Initiation Protocol (SIP), Locating SIP Servers
- RFC 3264 – An Offer/Answer Model with Session Description Protocol (SDP)
- RFC 3265 – Session Initiation Protocol (SIP) – Specific Event Notification

Jedná se o textově orientovaný protokol, sloužící k iniciaci, ukončení a dohledem nad spojením mezi dvěma či více účastníky. Během relace mohou uživatelé zasílat textové zprávy,

soubory aj. SIP je součástí sady protokolů TCP/IP a proto využívá další protokoly z této sady. Tento protokol ovšem nedokáže zajistit potřebnou kvalitu spojení Quality of Service (QoS). Pro zajištění potřebné kvality jsou uvnitř SIP zprávy obsaženy zprávy jiného protokolu, který zajistí potřebnou rezervaci síťových prostředků, vyspecifikuje typ přenášených dat, použité kódování pro multimediální data, dále jejich parametry, čísla portů. Pro popis přenášených dat se většinou využívá protokol SDP (Session Description Protocol), pro reservaci síťových prostředků se jedná o protokol RSVP (Resource reSerVation Protocol). Pro přenos multimediálních dat je použit protokol RTP/RTCP (Real Time Protocol/RTP Control Protocol) popř. RTSP (Real Time Streaming Protocol).

Klient navazuje se serverem spojení pomocí zpráv protokolu. Jedno zařízení může pracovat jako klient a druhé jako server i klient. Pro názorný příklad telefon se chová při odchozím hovoru jako klient, ovšem při příchozím hovoru jako server. Zprávy SIP protokolu jsou dva typy a to žádosti a odpovědi (Request a Response). Tyto zprávy si mezi sebou vyměňují klient a server kde:

- User Agent (UA) je koncové zařízení SIP sítě obvykle se jedná o SIP telefony nebo aplikace běžící na PC. Starají se o navazování spojení s jinými UA. Rozlišujeme User Agent Client (UAC) je to ta část, která se stará o navazování spojení s jinými UA a druhá část je User Agent Server (UAS) tato část zpracovává příchozí volání a odpovídá na ně. V takovémto telefonu je obsažen jak UAC tak UAS.
- Úkolem serverů je zprostředkovat spojení dvou či více UA, kontakt mezi volajícím a volaným.V SIP architektuře rozlišujeme tři typy serverů:

  - *Proxy server* – přijímá žádosti o spojení od jednotlivých UA. Tyto žádosti předá buď dalšímu proxy serveru a to v tom případě není-li volaný účastník v jeho okruhu, nebo je předá přímo volanému účastníkovi.
  - *Redirect server* – tento server stejně jako proxy přijímá žádosti o spojení, ale nespojuje je. Volajícímu (ať se jedná o server nebo přímo o UA) pošle odpověď kam má svoje volání směrovat. Volající si musí pak volání na získanou adresu odeslat.
  - *Registrar server* – přijímá žádosti UA k registraci a tím aktualizuje databázi koncových zařízení, jež jsou v jeho lokalizaci. Tuto informaci zašle lokalizační službě a UA zašle potvrzení
  - *Lokalizační server* – je databáze informací o účastnících (adresa, popř. číslo) informace mezi lokalizačním serverem a ostatními servery se vyměňuje pomocí protokolu Lightweight Directory Access Protocol (LDAP)

V praxi jsou tyto servery obvykle součástí jedné aplikace. Tato aplikace přijímá žádosti od koncových zřízení k registraci a podle toho jak je nakonfigurována se chová jako proxy nebo jako redirect server. K identifikaci UA se v protokolu SIP používá URI (Uniform Ressource Identifier). Jsou takto identifikování koncoví účastníci a mohou to být i brány, hlasové záznamníky aj.

Příklady identifikátoru:

- sip: xhladi00@seznam.cz
- sip: 12345678@seznam.cz
- sip: vlada@1.2.3.4
- tel: +420567891234

4.3.3.1 Zprávy a metody protokolu SIP

Mezi jednotlivými UA nebo UA a serverem dochází k výměně zpráv. K základním metodám patří [14], [15]:

- INVITE žádost o sestavení spojení
- ACK potvrzení INVITE konečným příjemcem
- BYE ukončení spojení
- CANCEL zrušení spojení
- REGISTER žádost o registraci User Agenta URI
- OPTIONS jaké schopnosti a možnosti má server
- INFO přenáší Mid-Call signalizace
- NOTIFY přenos
- PRACK vezme na vědomí dočasnou odpověď
- PUBLISH uvolnění zprávy serveru
- REFFER přenos uživatelského URI
- SUBSCRIBE jednotlivé události oznamují své žádosti
- UPDATE upravuje vlastnosti spojení
- MESSAGE naléhavá zpráva

Z protokolu HTTP byl do protokolu SIP převzat systém číselného kódu a je využíván pro odpovědi na metody. Tento kód se dělí na šest základních skupin nebo-li tříd (s příklady kódů odpovědí):

- 100-199 informační zprávy – posílá proxy nebo redirect server v případě trvá-li zpracovávání delší dobu nebo-li požadavek byl přijat, ale výsledek ještě není znám
  100 Trying – vysílá obvykle proxy server
  180 Ringing – vysílá UA , vyzvánění volaného
- 200-299 kladné vyřízení požadavku
  200 OK – úspěšné vyřízení
- 300-399 dotaz směrovat jinam, přesměrování – redirect serveru
  300 Multiple choices – několikanásobný výběr
  302 Moved temporarily – dotaz je třeba směrovat jinam
  305 Use Proxy

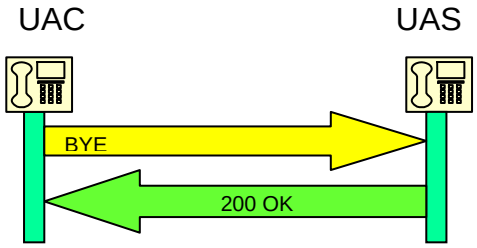
- 400-499 chyba klienta, špatná formulace dotazu
  400 Bad regest – špatný požadavek
  403 Forbidden – zakázáno
  480 Temporarily unavailable – dočasně nedostupný
  481 Call/Transaction does not exist – hovor/spojení neexistuje
- 500-599 chyba serveru
  500 Server Internal Error – interní chyba serveru
  501 Not Implemented - neimplementováno
- 600-699 všeobecná chyba
  600 Busy everywhere – obsazen všude
  604 Does not exist anywhere – dotazovaný nikde neexistuje
  606 Not Acceptable – nepřijatelný požadavek

Nyní si uvedeme příklad zprávy se SIP žádostmi

1 *INVITE sip: hlada@seznam.cz SIP/2.0*
2 *Via: SIP/2.0/UDP 192.168.1.10:5060;branch=fg6Gjue7Zde*
3 *To: Hlada<sip:hlada@seznam.cz>*
4 *From: Vlada<sip:xhladi00@seznam.cz>;tag=hjut8r07k*
5 *Call-ID: dgt6jfkrGF78923uo*
6 *Max-Forwards: 65*
7 *CSeq: 1 INVITE*
8 *Contact: sip:xhladi00@192.168.1.10*
9 *Content-Length: 256*

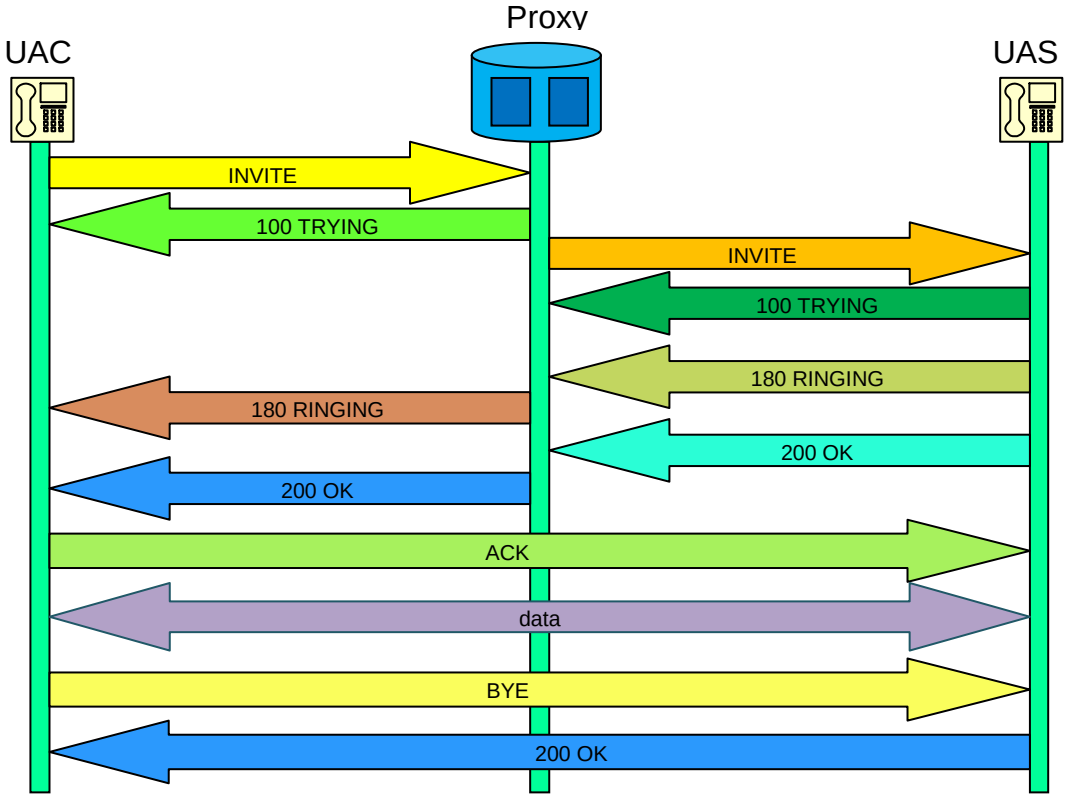
1. řádek je název metody, URI volaného účastníka a verze protokolu SIP.
2. řádek tag *Via* obsahuje verzi protokolu SIP, transportní protokol, host name (jméno volajícího) nebo IP adresu a číslo portu. Každý server, kterým zpráva prochází, přidává další Via tag. Odpověď prochází stejnou cestou, kterou přišla žádost. Branch je identifikátor relace.
3. řádek obsahuje jméno volaného účastníka a jeho URI
4. řádek obsahuje jméno volajícího účastníka a jeho URI, tag je náhodný řetězec generovaný pro každý dialog
5. řádek obsahuje jedinečný identifikátor pro dané spojení
6. řádek určuje maximální počet přeskoků dané zprávy, Dosáhne-li hodnoty nula je vyslána odpověď 483 To Many Hops
7. řádek definuje sekvenční číslo žádosti, další žádost toto číslo inkrementuje o 1
8. řádek definuje jednu nebo více SIP URI volajícího, je to informace pro ostatní uživatele
9. řádek určuje velikost přenášené zprávy v bitech

4.3.3.2 Základní principy komunikace SIP klientů



Obrázek 4-7. SIP přímá komunikace

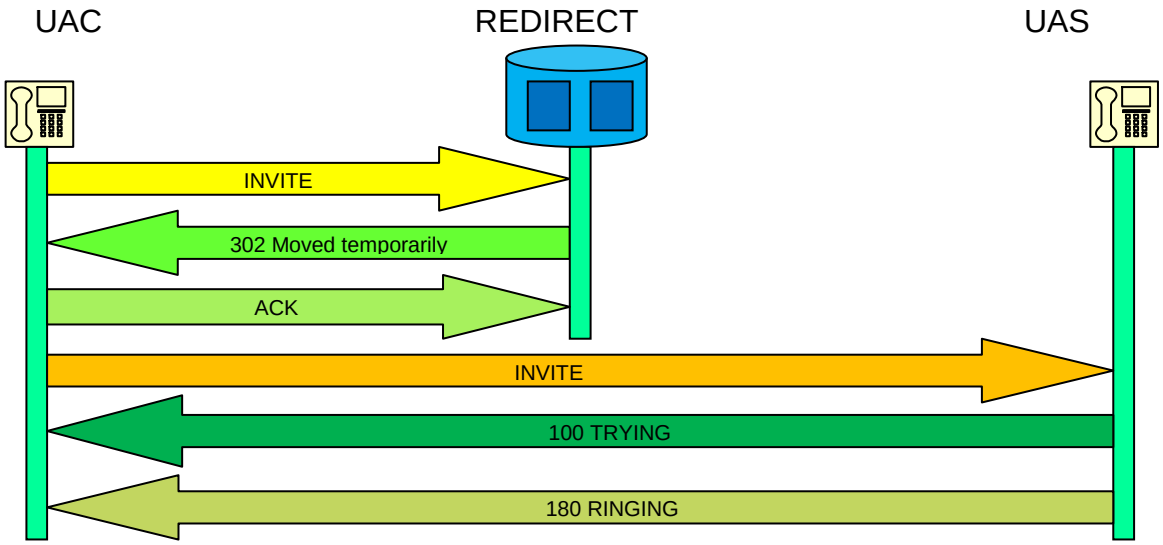
Komunikace a signalizace mezi dvěma klienty v případě, že volaný účastník zná adresu volaného účastníka, probíhá na úrovni účastník – účastník. Na obrázku 4-7. je uveden příklad jednoduché komunikace dvou UA. User Agent Client (UAC) vyšle zprávu – žádost o ukončení spojení BYE směrem k User Agent Server (UAS). UAS odešle zprávu 200-OK směrem k UAC.



Obrázek 4-8. SIP komunikace dvou účastníků se serverem proxy

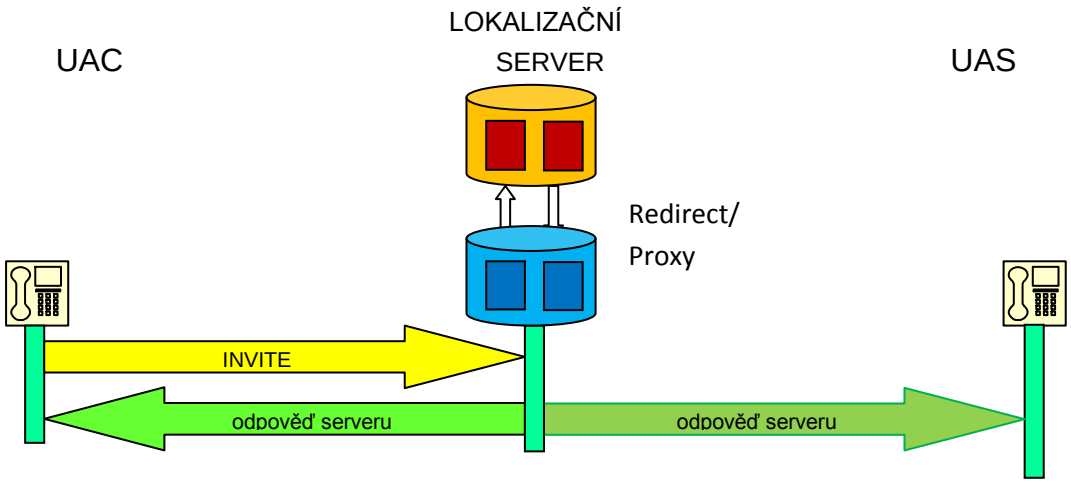
Obrázek 4-8. zobrazuje komunikaci dvou účastníků prostřednictvím Proxy serveru. UAC vyšle žádost na sestavení spojení INVITE s druhým účastníkem proxy serveru. Proxy server žádost přijme a odešle prvnímu účastníku 100 TRYING (zpráva se vyřizuje), a odešle druhému účastníku UAS žádost INVITE. UAS odešle zpět zprávu 180 RINGING „vyzváněcí tón“. Proxy server tuto zprávu přepošle UAC. Druhý účastník UAS přijal hovor a tím odeslal zprávu 200 OK. První účastník odešle přes proxy server signál ACK. Oba účastníci si

„vyměňují data“ – hovoří spolu. Rozhodne-li se první účastník pro ukončení spojení odešle zprávu BYE a druhý účastník odešle 200 OK. Tím je spojení ukončeno.



Obrázek 4-9. SIP komunikace se serverem Redirect

Na obrázku 9. je další způsob navazování komunikace. První účastník vyšle žádost INVITE serveru redirect. Ten vrátí zpět informaci kam správně směrovat požadavek. První účastník odešle ACK. Vyšle znovu INVITE, ale tentokrát již přímo volanému účastníku. Dál již komunikace probíhá jak v předešlém případě.



Obrázek 4-10. SIP dotaz

Obrázek 10. znázorňuje komunikaci (dotaz) Proxy nebo Redirect serveru na adresu neznámého účastníka. Komunikace mezi Proxy a lokalizačním serverem probíhá pomocí protokolu LDAP. Po provedeném dotazu spojení probíhá jak v předešlém případě.

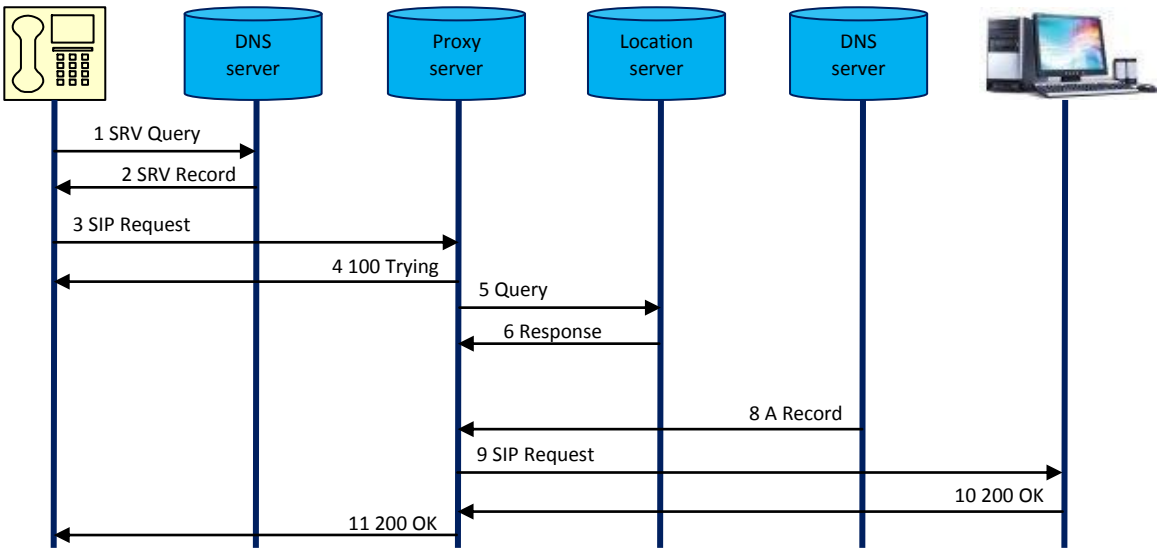
Jednou z hlavních funkcí SIP protokolu je rozlišování adres. Rozlišování začíná na informaci URI a končí uživatelským jménem a IP adresou. Rozlišení může provést jak user agent tak server. Procedura rozlišení adres projde následujícími základními kroky:

- DNS NAPTR – kontrola DNS záznamu a stanovení přenosových protokolů
- DNS SRV – určení doménového jména serveru a čísla portu
- DNS A – určení IP adresy hosta
- ENUM- je-li telefonní číslo, pak jeho stanovení

Ve skutečnosti se procedura při rozlišování adres skládá z více kroků. Nejprve proxy server určuje směrovací tabulky nebo DNS a posléze zasílá žádosti. Tyto žádosti jsou směrovány k cíli a mohou tedy projít, přes více proxy serverů, než se k cíli dostanou. Odpovědi se vracejí tou stejnou cestou, jakou šli žádosti, ale v opačném směru. To je umožněno pomocí tagu Via, kde je tato cesta uložena.

Obrázek 4-11. Rozlišování adresnázorňuje příklad rozlišování adres.
UA A (na obrázku značka telefonu vlevo) žádá o spojení s UA B (na obrázku vpravo obrázek PC), který je identifikovaným SIP URI (sip: kokes@hrusice.eu).

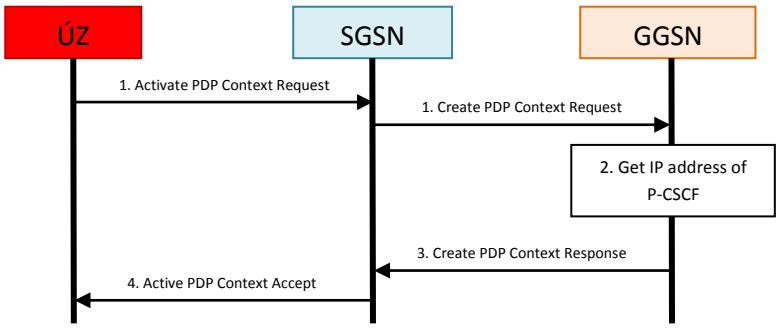
1. UA A provede nejdříve DNS NAPTR (Name Autority Pointer)
2. dotaz SRV (Service Record). To je potřebné pro stanovení transportního protokolu (TCP, UDP) a k určení proxy serveru pro doménu UA B.
3. následně je vyslána žádost k proxy serveru
4. proxy server vyřizuje žádost
5. proxy server vyšle žádost k lokalizační službě
6. LS odpovídá aktuální pozici URI UA B
7. proxy server vysílá žádost DNS serveru pro vyhledání URI adresy
8. odpověď A záznam
9. následuje žádost k UA B
10. UA B vrací potvrzení OK
11. Proxy přeposílá OK UA A



Obrázek 4-11. Rozlišování adres

5 Podpora IMS v současných mobilních sítích

Pro nasazení IMS v dnešních mobilních sítích je nutná podpora tohoto systému v těchto sítích. S tímto nasazením souvisí tzv. PDP (Packet Data Protocol) context. Je to vazba mezi mobilním terminálem (ÚZ) a bránou GGSN na úrovni PDP protokolu. PDP je obecný název protokolu pro přenos dat v mobilních sítích. Tímto protokolem je IP protokol.



Obrázek 5-1. Procedura PDP kontextu v síti GPRS.

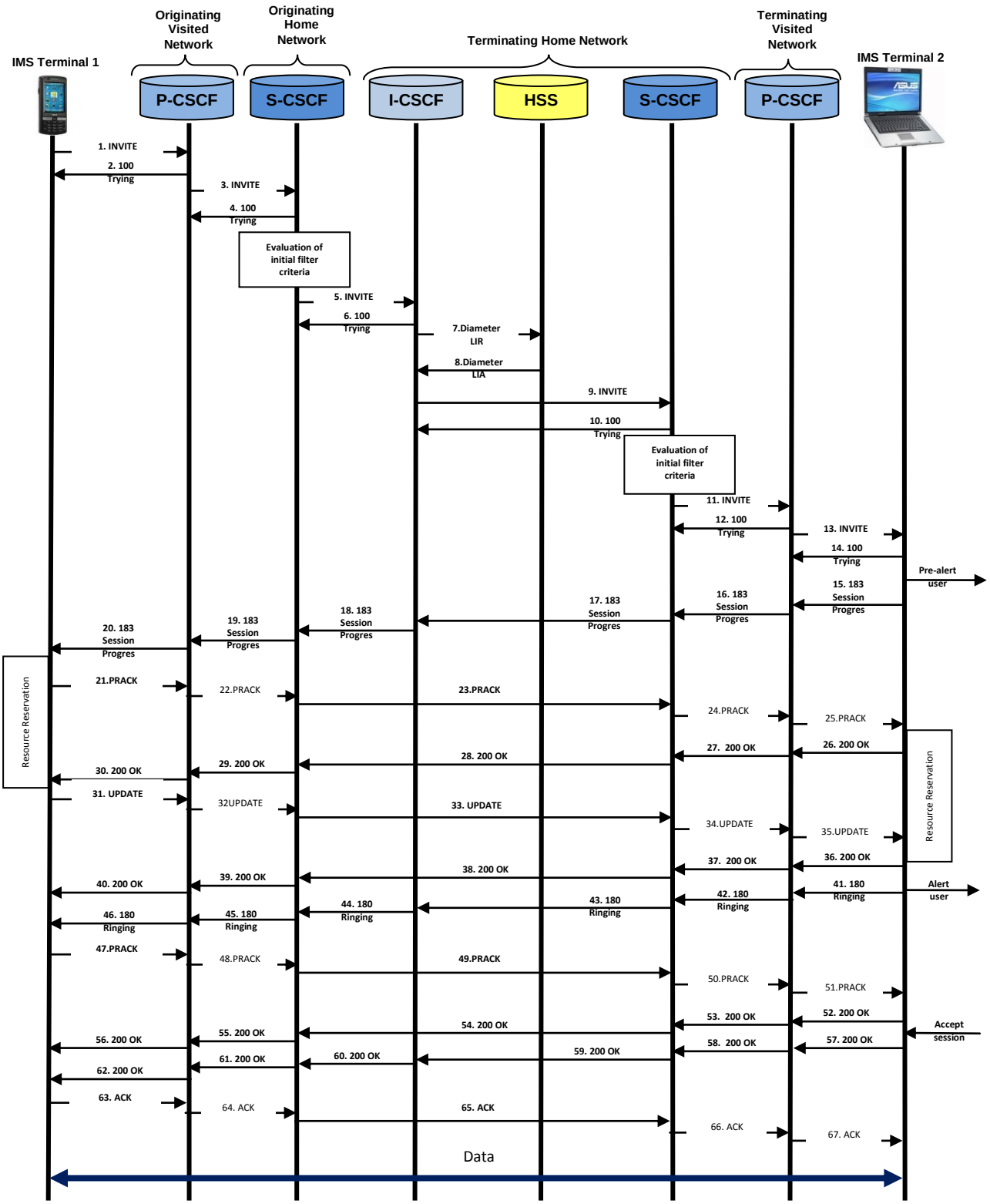
Proces zajištění PDP kontextu v mobilních sítích GPRS/UMTS [27], [29] je zobrazen na obrázku 5-1.:

1. ÚZ vyšle dotaz pro získání IP adresy P-CSCF. Tento požadavek SGSN předá GGSN
2. GGSN získá adresu P-CSCF. GGSN v tomto procesu, na základě požadavků ÚZ, také rozhodne, jaké síťové zdroje bude garantovat a provede jejich reservaci.
3. GGSN na základě mapování požadovaných parametrů QoS odešle ve zprávě *Create PDP Context Response* definované parametry SGSN.
4. SGSN ověří možnosti zajištění reservace síťových prostředků a dle stanovených parametrů sestaví nosnou službu přes přístupovou rádiovou síť a odešle ÚZ zprávu o sestavení této služby.

ÚZ může, po přijetí zprávy *Active PDP Context Accept* a získání IP adresy P-CSCF, již komunikovat se sítí IM CN subsystem. Sestavení PDP kontextu a získání IP adresy P-CSCF je pouze pro volajícího účastníka sítě GPRS, toto neplatí pro příchozí hovor. Nyní může proběhnout registrace na přiděleném P-CSCF.

Dále již ÚZ pracuje jako IMS terminál.

Typickým příkladem spojení v síti s implementací IMS je spojení uvedené na Obrázek 5-2. Spojení dvou IMS terminálů [2]. Oba terminály jsou účastníky sítě s podporou IMS, ale každý má jinou domovskou síť. Terminál 1 vyšle žádost o spojení k P-CSCF. P-CSCF odešle potvrzení o tom, že žádost zpracovává. Žádost se postupně vyřizuje v jednotlivých blocích. Mezi I-CSCF a HSS proběhne ověřovací proces (autentizace a autorizace) zprávami protokolu Diameter. Postupně je sestavováno spojení (15 - 20). Pro přenos datového toku jsou zarezervovány prostředky (21 - 35). Pak dojde k vyzvánění, k potvrzení přijetí spojení a k samotnému spojení. Pak se již přenášejí uživatelská data.



Obrázek 5-2. Spojení dvou IMS terminálů

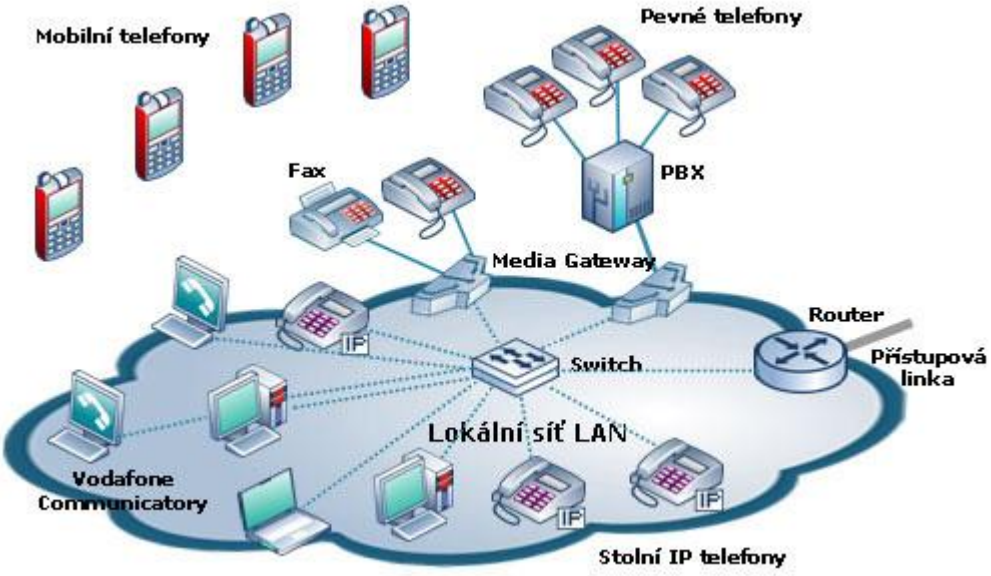
5.1 Možnosti stávajících mobilních sítí

Sítě s implementací IMS nabízí uživatelům velké množství služeb, od klasické telefonie po služby s real-time aplikacemi např. IPTV. Pro poskytování těchto služeb je příprava sítí a tudíž připravenost operátorů na tyto služby nejdůležitější částí.

V současné době je u nás na trhu operátor, který je nejlépe vybaven a nabízí kompletní služby IMS, s možností připojení prakticky všemi možnými způsoby. Tímto operátorem je O2. Nabízí připojení pevnou sítí ADSL2+, připojení rádiovými technologiemi ať už mobilními GPRS/EDGE, CDMA, HSDPA/UMTS nebo WiFi hot-spoty. Nabízí služby základní, doplňkové i speciální. Do základních služeb se např. zahrnuje hovorová služba, do doplňkových služeb – zobrazení čísla volajícího, záznam v nepřítomnosti volaného, přesměrování aj. a do speciálních služeb video na vyžádání, audio na vyžádání aj. Tyto služby jsou s implementací technologie IMS, kterou dodala firma *Telefónica.*

Další operátor T-mobile nezůstává, co se technologií připojení týče, za O2 příliš pozadu. Ovšem jeho nabídka služeb není tak široká jako v předchozím případě.

Třetím nejstarším operátorem na našem trhu je Vodafone. V jeho případě se nabídka služeb, s implementací IMS od firmy Ericsson, týká zatím bohužel jen firemních zákazníků.



Obrázek 5-3. Obrázek realizace řešení v zákaznické lokalitě [6]

Čtvrtým a zatím nejmladším operátorem na trhu je Ufon. Poskytuje rádiové připojení na bázi technologie CDMA 2000 [8]. Zatím ovšem tímto signálem není pokryto celé území. A jeho nabídka služeb se omezuje na „pevný mobilní telefon“ nebo připojení pomocí rádiového modemu.

Pro přehlednost uvádím v tabulce 5-1 možnosti připojení od jednotlivých operátorů a nutné technické vybavení s uvedenými náklady na pořízení.

V tabulce jsou uvedeny jen vybrané tarify od jednotlivých poskytovatelů, aby bylo možno srovnat poměr rychlost/cena. Tyto dvě hodnoty jsou totiž pro většinu zákazníků rozhodující. Z hodnot uvedených v tabulce je vidět finanční náročnost koncových zařízení. Omezující např. u firmy O2 je povinnost mít zřízen aktivní mobilní tarif. Tatáž firma sice nabízí rychlejší mobilní připojení ovšem také za podstatně vyšší cenu. Bohužel se tak ukazuje, že stálé mobilní připojení není pro běžného uživatele přitažlivé.

Tabulka 5-1. Srovnání možností připojení operátorů.

Operátor						
použitá technologie		CDMA 2000 UMTS		GPRS/EDGE, UMTS	GPRS/EDGE	CDMA 2000
rychlost připojení		512kbit / s		512kbit / s	236kbit / s 75% pokrytí ostatní 85kbit / s	400 – 700 kbit / s
název služby		O2 Internet mobil 512 plus		Internet standart	připojení na stálo	ufonův fofr Internet
měsíční platba bez DPH/ s DPH		699,- / 831,81		699,- / 831,81	546,20 / 650,.	594,- vč. DPH
FUP		2,8 GB / týden		5 GB / měsíc	neomezeně	2 GB / týden
použité přípojné (koncové) zařízení	**typ**	datová karta CDMA 2000	telefon s podporou UMTS např. Nokia 6120 classic	4G modem UMTS	datová karta nebo USB modem Vodafone Mobile Connect	USB modem AnyData ADU-510L
	cena s DPH	5095,-	6 295,- 1,- (*	3599,-	3977,-	4999,-
Poznámka:		pro zřízení této služby je nutné mít aktivní mobilní tarif (* týká se pouze zákazníků s uzavřenou smlouvou				zatím nenabízí vlastní mobilní telefony

Možnosti kombinací, zejména u O2 a T-mobile, jsou různé [5], [6] . Je možné využít též připojení pomocí hot-spotů. Ty jsou rozmístěny v místech s velkým počtem uživatelů např. velká města, dálnice apod. Připojení WiFi je však omezeno „předplatným“. Můžete si vybrat mezi měsíčním paušálem na 10 hodin za 178,5 Kč vč. DPH nebo na neomezené připojení za 1069,81 Kč vč. DPH. I zde jsou k dispozici předplacené kupóny od 200,- do 950,- Kč, kde se za 1 hodinu připojení účtuje 40,-Kč. Prakticky stejnou službu nabízí i T-mobile s cenou 15Kč/10 min. Zbývající dva operátoři tuto službu nenabízí.

Tabulka 5-2. Pevné připojení vs. mobilní připojení pro operátora O2.

	Rychlost	Cena s DPH
Pevné připojení	2048 kb / s	474,80 Kč
	6144 kb / s	950,00 Kč
Mobilní připojení	1024 kb / s	1069,81 Kč

Tabulka 5-2. uvádí srovnání pevné připojení versus mobilní připojení. „Nejpomalejší“ připojení přes pevnou síť s rychlostí 2Mb/s poskytuje T-mobile a O2 za 474,81 Kč vč. DPH. O2 nabízí ještě při stejné rychlosti připojení za 950,- Kč vč. DPH službu O2 Trio. Mezi těmito dvěma službami, jak je vidět na první pohled, je rozdíl nejen v ceně, ale také v poskytnutých službách. O2 v tomto balíku nabízí např. službu IPTV. Při stejné ceně 950,- s pevným připojením můžeme získat rychlost připojení 6144kb/s což je šestkrát více než za cenu 1069,81 s mobilní připojením. -Při srovnání mobilní rádiové připojení versus pevné připojení ADSL, pevné připojení zatím vyhrává.

Závěr

Ve své bakalářské práci jsem se zaměřila na možnosti poskytování služeb v datových sítích. Možnosti poskytování služeb v sítích s implementací IMS jsou široké. Mohu tak s jedním přístrojem telefonovat, poslouchat rádio, sledovat TV vysílání, díky navigaci bezpečně dojet do vytčeného cíle cesty, brouzdat po Internetu a mít tak nejnovější novinky neustále v dosahu, číst a psát e-mail, posílat SMS, MMS a mnoho dalších možností. Bohužel toto je ovšem možné pokud máme v jednom přístroji všechny možnosti připojení. U mobilních přístrojů je to připojení pomocí GPRS, EDGE, UMTS a dále je vybaven Wifi a dalšími technologiemi bezdrátového přístupu jako je Bluetooth aj. Kompletní služby IMS u nás zatím nabízí jen O2. Poskytovatelé se v dnešní době snaží převést veškerou komunikaci (ať už jde o klasickou hlasovou službu) na spojení pomocí datových sítí. U sítí třetí generace (3G) UMTS, CDMA2000 spojení na principu přepojování paketů není problémem. Jedinou nevýhodou těchto systémů je jejich malé pokrytí. Veškerá hlasová komunikace spěje k tomu, aby byla provozována na principu VoIP. I když toto nebude operátory přesně takto deklarováno. Pod pojmem VoIP si širší veřejnost (běžný uživatel PC s připojením k Internetu) představí „telefonování po Internetu zdarma“. I když toto telefonování zdarma není úplně pravdivé, protože každé připojení k Internetu něco stojí. Mobilní připojení k Internetu pomocí technologie GPRS a EDGE (u nás zatím nejdostupnější signál) je prozatím poměrně drahé. Jako další možnost mobilního připojení se jeví možnost připojení Wifi tzv. hot-spotů. Ovšem toto není mobilní v pravém smyslu slova mobilní. Toto posledně jmenované připojení nabízí dva z našich mobilních operátorů. Ale tyto terminály též nepokrývají celé území, pro svůj výkon (možný dosah) by musely být rozesety velmi hustě a také neumožňují realizovat služby za pohybu rychlostí větší než jednotky km/h. Jako další se jeví možnost využít poměrně rozsáhlou síť regionálních WiFi sítí. Ale to je spíše otázkou jednání mezi poskytovateli jednotlivých připojení a mobilními operátory. Prozatím širší rozšíření „IP telefonie zdarma“ nebo-li VoIP v sítích 3G není realizovatelná. Za prvé není v ekonomickém zájmu samotných operátorů nabízet VoIP a za druhé dostupnost mobilních (telefonů) terminálů s různými možnostmi připojení je z ekonomického hlediska pro většinu obyvatelstva s průměrným platem téměř nedostupná. Proto používání technologie VoIP, tak jak ji známe, bude ještě po nějaký čas typické pro většinu obyvatel s pevným připojením k Internetu. Ovšem když přihlédnu k dokumentu „Broadband strategie ČR“, kde je specifikováno „do roku 2010 má mít cca 50% populace možnost využívat vysokorychlostní přístup k Internetu“, je tato podmínka splněna. Sítě s implementací IM CN subsystem (Internet protocol Multimedia Core Network subsystem) budou do budoucna provozovány různými technologiemi, proto uživatelé mohou zvolit jedno mnohopřístupové zařízení nebo několik zařízení a každé pro jinou službu, nebo zvolit za vyšší finanční částku jedno připojení, kde budou mít od jednoho poskytovatele všechny služby.

Použitá literatura:

[1] CAMARILLO,G., GARCÍA-MARTÍN,M.-A. The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds, Second Edition. Wiley, ISBN-13: 978-0470018187, 2006

[2] Miikka Poikselka, Aki Niemi, Hisham Khartabil, Georg Mayer The IMS: IP Multimedia Concepts and Services. Wiley, ISBN-13: 978-04700119061, 2006

[3] Český telekomunikační úřad, Sokolovská 219, Praha 9, V Praze dne 3. října 2001 Č.j. 26485/2001-610 Číslovací plán signalizačních bodů signalizačních sítí signalizačního systému č.7

[4] Vysokorychlostní přístup ke službám elektronických komunikací Identifikační kód projektu YA632004003, Etapa č. 2, Návrh postupu státu při podpoře telekomunikačního trhu tak, aby se na základě perspektiv konvergence sítí a služeb stimulovalo liberalizované telekomunikační prostředí. TESTCOM, Technický a zkušební ústav telekomunikací a pošt Praha, 148 01 Praha 4, Hvožďanská 3, leden 2007

[5] www.cs.o2.cz

[6] www.vodafone.cz/corporate/why/index.htm

[7] www.t-mobile.cz

[8] www.ufon.cz

[9] www.micr.cz/files/2060/NBBS.pdf

[10] www.ericsson.com/technology/whitepapers/index.shtml

[11] www.earchiv.cz – e-archiv Jiřího Peterky

[12] www.techabulary.com

[13] Řízení kvality služeb v bezdrátových sítích
www.utko.feec.vutbr.cz/~molnar/mmos/wifi_umts.pdf
Zdroje dostupné z http://tools.ietf.org/html/

[14] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. SIP: Session Initiation Protocol. RFC 3261, June 2002

[15] J. Rosenberg, H. Schulzrinne. Reliability of Provisional Responses in Session Initiation Protocol (SIP). RFC 3262, June 2002

[16] J. Rosenberg, H. Schulzrinne Columbia U. Session Initiation Protocol (SIP), Locating SIP Servers, RFC 3263, June 2002

[17] J. Rosenberg, H. Schulzrinne Columbia U. An Offer/Answer Model with Session Description Protocol (SDP). RFC 3264, June 2002

[18] A.B. Roach. Session Initiation Protocol (SIP) – Specific Event Notification, RFC 3265, June 2002

[19] M. Handley, V. Jacobson, C. Perkins University of Glasgow. SDP: Session Description Protocol, RFC 4566, July 2006

[20] H. Schulzrinne Columbia University, S. Casner, R. Frederick Blue Coat Systems Inc. V. Jacobson. RTP: A Transport Protocol for Real-Time Applications, RFC 3550, July 2003

[21] H. Schulzrinne Columbia University, S. Casner. RTP Profile for Audio and Video Conferences with Minimal Control, RFC 3551, July 2003

[22] D. Hoffman, G. Fernando Sun Microsystems, Inc. V. Goyal, Inc. M. Civanlar. RTP Payload Format for MPEG1/MPEG2 Video, RFC 2250,January 1998

[23] H. Schulzrinne Columbia U., A. Rao Netscape, R. Lanphier RealNetworks. Real Time Streaming Protocol (RTSP), RFC 2326, April 1998

[24] P. Calhoun, Inc. J. Loughney Nokia, E. Guttman Sun Microsystems, Inc. G. Zorn Cisco Systems, Inc. J. Arkko Ericsson. Diameter Base Protokol. RFC 3588, September 2003

[25] R. Braden, L. Zhang UCLA, S. Berson ISI, S. Herzog IBM Research, S. Jamin Univ. of Michigan. Resource ReSerVation Protocol (RSVP). RFC 2205, September 1997
Zdroje dostupné z http://www.3gpp.org/specs/numbering.htm

[26] 3GPP TR 21.978 V3.0.0 (2000-06) (Release 1999) Feasibility Technical Report – CAMEL Control of VoIP Services

[27] 3GPP TS 22.173 V8.2.0 (2008-03) (Release 8) Technical Specification Group services and System Aspect; IP Multimedia Core Network Subsystem (IMS); Multimedia Telephony Service and supplementary services; Stage 1

[28] 3GPP TS 22.228 V8.4.0 (2008-03) (Release 8) Technical Specification Group services and System Aspect; Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1

[29] 3GPP TS 22.340 V8.1.0 (2008-3) (Release 8) Technical Specification Group services and System Aspect; IP Multimedia Systém (IMS) messaging; Stage 1
[30] 3GPP TS 23.228 V8.4.0 (2008-03) (Release 8) Technical Specification Group services and System Aspect; IP Multimedia Subsystem (IMS); Stage 2
[31] 3GPP TS 26.141 V7.1.0 (2006-03) (Release 7) Technical Specification Group services and System Aspect; IP Multimedia Systém (IMS) Messaging and Presence; Media formats and codecs
[32] 3GPP TS 23.107 V7.1.0 (2007-09) (Release 7) Technical Specification Group services and System Aspect; Quality of Service (QoS) koncept and architecture