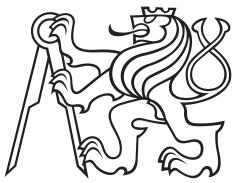
Diplomová práce



České
vysoké
učení technické
v Praze

F3

Fakulta elektrotechnická
Katedra telekomunikační techniky

Simulace Diameter rozhraní IMS sítě na open-source platformě

Bc. Tomáš Krbec
Komunikační systémy

Květen 2018
Vedoucí práce: Ing. Ivan Pravda, Ph.D., Ing. et Ing. Radim Kalfus, Ph.D.

Poděkování / Prohlášení

Rád bych poděkoval panu Ing. et Ing. Radimu Kalfusovi, Ph.D. a panu Ing. Ivanu Pravdovi, Ph.D. za poskytnuté rady a děkuji i oponentovi za přečtení a ohodnocení práce. Dále děkuji své manželce Bc. Barbaře Krbcové za podporu.

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne 24.05.2018

.....

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Krbec** Jméno: **Tomáš** Osobní číslo: **406110**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Komunikace, multimédia a elektronika**

Studijní obor: **Komunikační systémy**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Simulace Diameter rozhraní IMS sítě na open-source platformě

Název diplomové práce anglicky:

Diameter interface simulation on open-source platform in IMS network

Pokyny pro vypracování:

Nastudujte možnosti open-source platforem a API dostupných pro použití v mobilních sítích a tyto vzájemně porovnejte. Pro zvolenou platformu vypracujte simulační scénáře na úrovni jednotlivých Diameter zpráv simulující rozhraní 3GPP Gx a Rx dle Release 10 sítě IMS. Takto navržené scénáře na zvolené platformě dále zrealizujte.

Seznam doporučené literatury:

[1] OLSSON, M.: EPC and 4G Packet Networks: Driving the Mobile Broadband Revolution [online].2nd;2;. GB: Academic Press, 2013;2012;. ISBN: 9780123945952
[2] NAKHJIRI, Madjid; NAKHJIRI, Mahsa: AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility [online].1. Aufl.;1;. GB: Wiley, 2005. ISBN: 9780470011942
[3] GAENGER, K., KREHER, R. a Inc.: BOOKS24X7. LTE Signaling : Troubleshooting and Optimization [online].1. Somerset: John Wiley & Sons, Incorporated, 2010;2011;. ISBN: 9780470977729
[4] JEPSEN, T. C.: Java in telecommunications: solutions for next generation networks. Chichester: Wiley-Academy, 2001. ISBN 9780471498261

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Ivan Pravda, Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Ing. et Ing. Radim Kalfus, T-Mobile Czech Republic a.s.

Datum zadání diplomové práce: **07.09.2017** Termín odevzdání diplomové práce: **25.05.2018**

Platnost zadání diplomové práce: **30.09.2018**

Ing. Ivan Pravda, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

23. 9. 2018 Datum převzetí zadání	Podpis studenta

Abstrakt / Abstract

Nastudujte možnosti open-source platforem a API dostupných pro použití v mobilních sítích a tyto vzájemně porovnejte. Pro zvolenou platformu vypracujte simulační scénáře na úrovni jednotlivých Diameter zpráv simulující rozhraní 3GPP Gx a Rx dle Release 10 sítě IMS. Takto navržené scénáře na zvolené platformě dále zrealizujte.

Klíčová slova: Diameter, Gx rozhraní, Rx rozhraní, PCRF

Diameter interface simulation on an open-source platform in an IMS network. Familiarize with capabilities of open-source platforms and APIs applicable to mobile network industry. Create a simulation model including documentation of 3GPP Gx and Rx interface.

Keywords: Diameter, Gx interface, Rx interface, PCRF.

Title translation: Diameter interface simulation on open-source platform in IMS network

Obsah /

Tabulky / Obrázky

Kapitola 1
Úvod

Často skloňované téma ve veřejnoprávních médiích, v souvislosti s mobilními operátory, je vysoká cena za nabízené služby. Náklady související s nákupem frekvenčních licencí a provozem sítě jsou přitom buď opomíjeny, nebo bagatelizovány. V rámci této práce jsem se blíže zaměřil právě na možnost snížení provozních nákladů snížením nákladů na pořízení, úpravy a provoz telekomunikační sítě.

Tuzemští operátoři při změně z okruhově přepínaných sítí na sítě paketově přepínané již z velké části přešli z drahých proprietárních obvodů na levnější procesory s instrukční sadou x86. Místy ztráta rychlosti je kompenzována vhodnou architekturou a především rychlejší dobou uvedení nových změn na trh. To dalo systémovým architektům větší volnost při vyjednávání podmínek s dodavateli, samotná údržba a poskytování náhradních dílů se tím také značně zjednodušuje.

Přechodem na x86 nastala doba doba optimalizace nákladů na hardware. Aplikační sofware, stále proprietární a uzavřený, mohl být provozován na takzvaném COTS[1] hardwaru, tedy standardním hardware, poskytovaném za řádově nižší ceny. Nyní přichází doba otevření i samotného aplikačního softwaru, alespoň v takové míře, kde je kód aplikační logiky možné na žádost upravit buď programátory dodavatele, nebo v některých případech dokonce i vývojáři daného mobilního operátora. To přináší nejen vyšší transparentnost do skutečných nákladů spojených s úpravou, ale i rychlejší rekonfiguraci. Nabízí se tedy možnost, že veškeré know-how zůstane u operátora.

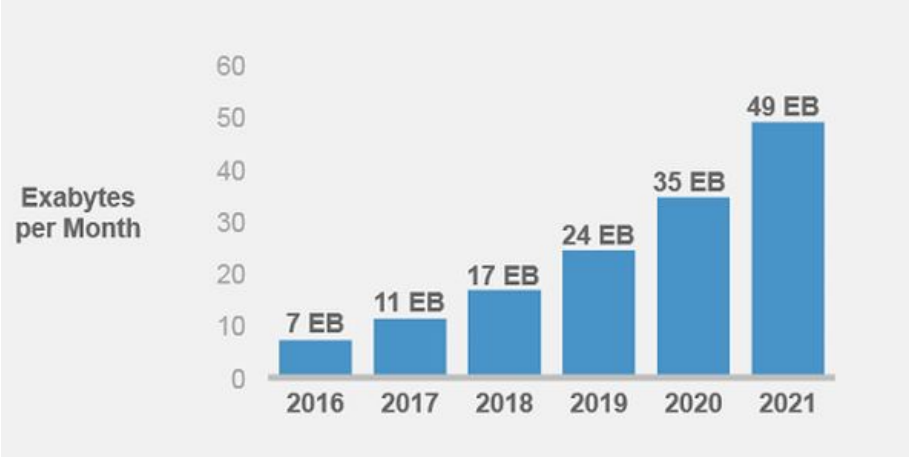
Velké společnosti jako například Google či Amazon již používají ve svých komerčních projektech řešení s otevřeným kódem, příkladem může být Apache Hadoop, Kubernetes nebo například Openstack[18]. Dokonce je to prospěšné pro obě strany, společnosti snáze získají zaměstnance se znalostmi řešení, protože kdokoliv má právo zkoušet, testovat a opravovat otevřený kód. Společnost naopak přispívá částí svých zisků nebo času svých zaměstnanců na údržbu a inovaci řešení.

Proč jsem si vybral téma zaměřené na opensource u mobilních signalizačních protokolů? Mobilní síť byla díky standardizačním snahám rozdělena na jednotlivé základní funkcionality s jasně definovanými rozhraními a protokoly specifikované v příslušných doporučeních standardizačních institucí. To spolu se zájmem velkých telekomunikačních dodavatelů umožnilo rozvoj opensource platforem, které dosahují výkonnosti a vysoké stability tak potřebné pro budoucí reálné nasazení v sítích mobilních operátorů. Opensource telekomunikační frameworky jsou nyní již dostatečně kvalitní a konkurenceschopné na vytvoření signalizační aplikace pro použití u operátorů.

Pokud vynechám protežování vlastních služeb, tak stále lze najít příklady rozdělení zákazníků a jejich služeb do prioritních skupin. Kvalita služby ze signalizační části nevymizela a nejspíše dlouho nevymizí. S rostoucím významem mobilních datových přenosů, exponenciálně stoupají i přenosové rychlosti[16]. Kvalita služby spolu s řízením priorit datových toků se tak stává důležitým tématem.

Paketové sítě s sebou přinesly i problémy, je nutné vyhradit dostatečnou přenosovou kapacitu a stále je třeba zaručit prioritu službám jako například Voice over LTE oproti

[1] Commercial off-the-shelf



Obrázek 1.1. Trend spotřeby mobilních dat, citováno z [16].

datovým tokům. Kvalita služby si proto našla v signalizační části sítě funkci nazývanou PCRF server a její funkcionalita pro IMS část postavená na opensource základech bude demonstrována v této diplomové práci. Nutno podotknout, že pojem kvalita služby se netýká pouze jednoho bajtu v IP hlavičce, ale prioritě zasílané do rádiové přístupové sítě.

Kapitola 2
Mobilní sítě

2.1 3GPP

Dle[26] projekt 3GPP zaštiťuje 7 standardizačních institucí z celého světa a pokrývá svět telekomunikací od přístupových sítí, bezpečnosti a kvality služby, až po jednotlivá rozhraní například v IMS a interakci mezi nimi. Pokud pomineme nadnárodní operátory, důvod vzniku 3GPP je již patrný při vycestování do zahraničí, kde máme možnost volat přes partnerského operátora a tím odpadá nutnost kupovat si SIM kartu v dané lokalitě. Interakce mezi operátory, rozhraní a protokoly, které pro komunikaci používají jsou standardizované a v tomto případě značně ulehčuje integraci dvou neznámých systémů – protistran. 3GPP se rozděluje na 3 specifikační skupiny:

- **TSG RAN**[1]– skupina definuje nároky a požadavky od fyzické vrstvy po L3 ISO/OSI modelu pro FDD a TDD. Příklad rozhraní: Iu, Iub, Iur, S1 a X2,
- **TSG SA**[2]– tato skupina se zabývá architekturou a procesně řídí ostatní skupiny,
- **TSG CT**[3]– skupina má na starost hlavní funkcionalitu, například, že se účastník A dovolá účastníkovi B s rozdílným typem telefonu a nezatíží tím celou síť, ale bude mu pouze přidělena poměrná část sítě. Aby si účastník mohl zavolat, existuje v telefonní síti plno prvků s danou funkcí a rozhraními pro komunikaci s ostatními prvky. Prvky, propojení a používané protokoly specifikuje právě tato skupina.

Každá skupina se dále rozděluje na tzv. pracovní podskupiny, které řeší detailní problémy spjaté například s architekturou či bezpečností. 3GPP využívá metodu, kde každá práce se stává ze třech kroků:

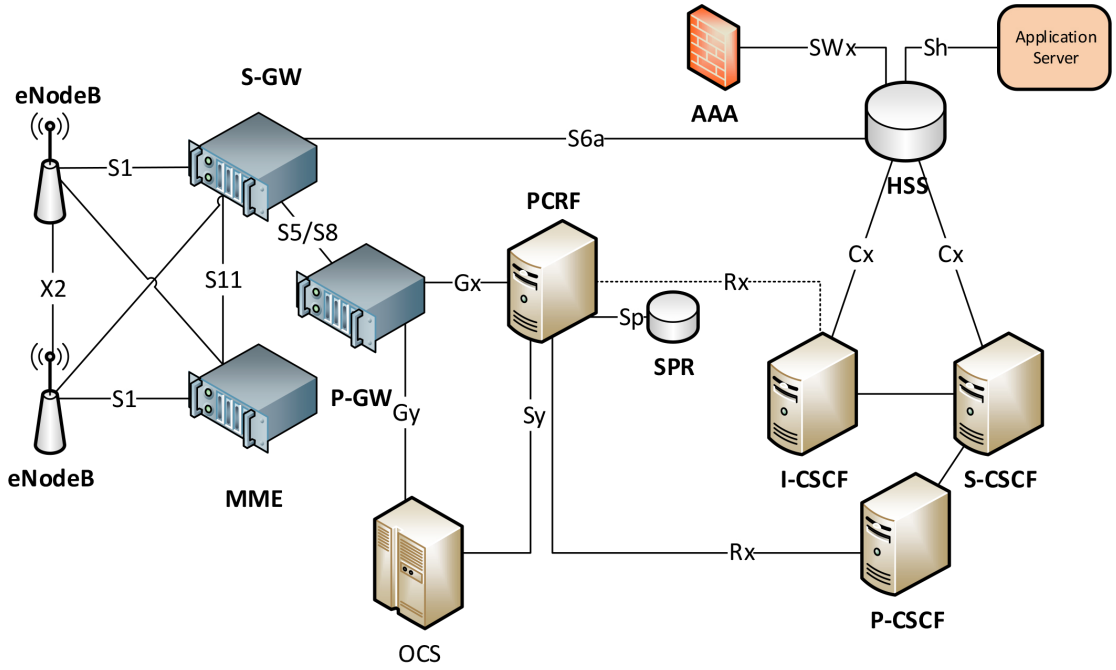
1. Evaluace požadavků a popisu z pohledu uživatele služby a operátora.
2. Problémy jsou rozpadnuty do menších funkčních celků a jsou zjišťovány vztahy mezi celky.
3. V tomto kroku se zaručuje, že všechny protokoly a procesy jsou popsány detailně a v souladu s požadavky.

Všechny potřebné dokumenty 3GPP včetně technických specifikací jsou dostupné online. Tato práce se bude především zabývat entitou PCRF a její interakcí s entitou P-GW na jedné straně a P-CSCF na straně druhé.

2.2 Architektura

Na obrázku 2.1 je vidět část možné architektury mobilní sítě operátora. V další části této kapitoly bude popis zařízení a funkcí v ní naznačených.

[1] Radio Access Network – rádiová přístupová síť
[2] Service and Systems Aspects – služby a systémová hlediska
[3] Core Network and Terminals – jádro sítě a terminály



Obrázek 2.1. Část architektury mobilní sítě pro IMS a EPC.

eNodeB, jedná se o základnovou stanici ve 4G, kde každá stanice je většinou propojena se sousední eNodeB pomocí X2 rozhraní a s MME/S-GW pomocí S1 rozhraní. Princip X2 rozhraní spočívá především v usnadnění přepojení účastníka mezi dvěmi eNodeB. Základnová stanice je zodpovědná za přenos informací pomocí radiového rozhraní – modulaci, kódování a multiplexing (v případě příjmu informací se jedná o inverzní funkce). ENodeB zároveň funguje i jako IP směrovač a přepínač, funkce základnové stanice v LTE se přímo dotýká prvních třech vrstev ISO/OSI modelu.

MME zprostředkovává NAS signalizaci (Non-access stratum) směrem k terminálu. NAS signalizace je popsána v sekci 3.4. MME je klíčovým prvkem v komunikaci s terminálem a propagaci změn z a do terminálu. Dále sestavuje základní a vyhrazené EPS kanály, ověřuje terminál vůči HSS a a spravuje výměnu klíčů. MME podporuje mobilitu mezi 3G a 4G přístupovými sítěmi.

S-GW směruje a přesílá pakety, terminál je připojen pouze k jedné S-GW. V případě přechodu z jedné eNodeB na druhou zároveň funguje jako kotevní bod, spojení do S-GW zůstává a pokud dojde k úspěšnému přechodu na RAN, stávající S-GW zašle ukončující pakety a dochází k přepnutí mezi S-GW. Na síťové vrstvě se prvek chová jako směrovač a směruje pakety ke správnému terminálu a naopak. Paketům nastavuje QoS parametry na základě přidružených EPS kanálů. Pokud je terminál v nečinném stavu, S-GW šetří přenosovou kapacitu sítě a terminuje downlink terminálu. Pokud dorazí nové pakety, je znovu zahájen paging terminálu.

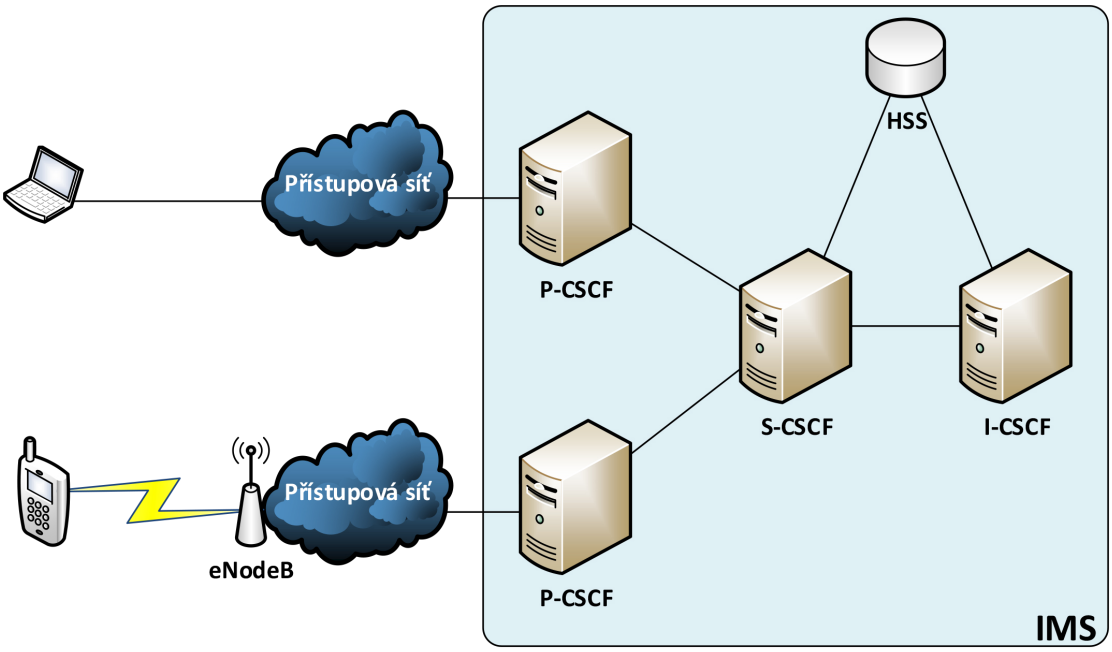
P-GW Packet Gateway, v některých literaturách nazývaná jako Packet Data Network Gateway (PDN-Gateway)[8]. Primární funkcí je řízení GTP tunelů do S-GW, překlad QCI[1] na Diffserv Code Point (transportní vrstva ISO/OSI modelu), dále přiřazuje terminálu IP adresu nebo adresy a směruje uživatelské pakety. Méně chtěnou funkcí z pohledu uživatele je filtrace a inspekce paketů. V případě připojení do více sítí, do více APN, terminál může mít připojení k více P-GW. P-GW bývá připojena s

[1] QoS Class Identifier

OCS[1] pomocí Gy rozhraní, kde dochází k informování o velikosti spotřebovaných dat a s PCRF[2] pomocí Gx rozhraní.

IMS je řídící část sítě pro zřizování multimediálních služeb, která je nezávislá na přístupu a používá internetové protokoly[3]. Základem je, že komunikace probíhá po IP protokolu. Terminál může získat IP připojení v roamingu a připojit se do IMS i ze zahraničí, zároveň to klade nároky na kvalitu služby. Nezávislost na přístupu znamená, že lze využít jakékoliv sítě poskytující IP konektivitu (WLAN, xDSL, optické připojení,..). Obecně kladené požadavky na IMS se dají formulovat následovně:

- podpora IP relací,
- podpora kvality služby (QoS),
- podpora propojení s internetem a s okruhově přepínanými sítěmi,
- podpora roamingu.



Obrázek 2.2. Zjednodušený diagram IMS.

Ve veřejném internetu mohou pakety dorazit i s vysokou odezvou a ve špatném pořadí, některé pakety také nemusí být doručeny. Takové chování by znatelně ovlivnilo uživatelský dojem, proto součástí IMS jsou podpůrné protokoly a mechanismy k zajištění kvality služby od počátečního bodu do koncového. Terminál například síti podává informace o podporovaných protokolech a kodecích a žádá síť o přidělení prostředků. Síť podle své podpory a obsazenosti přiděluje prostředky.

Bezpečnost je dalším klíčovým požadavkem pro telekomunikační systémy a IMS využívá přinejmenším stejnou úroveň jako okruhově přepínané sítě. Uživatelé jsou ověřeni a až poté zaregistrováni do sítě.

Nezbytnou součástí IMS sítě také je účtování zákazníků a více možností jak účtovat zákazníka, například:

1. pouze strana A je účtována,

[1] Online Charging System
[2] Policy and Charging Rule Function
[3] Především protokoly definované IETF

2. pouze strana B je účtována,
3. kombinace výše uvedeného.

Dále se nabízí možnost účtování na základě obsahu, v IMS lze rozdělit účtování mezi videohovory a běžné hlasové hovory. Podporované je, jak offline, tak i online účtování.

3GPP rozhodlo použít pro architekturu IMS rozdělení mezi vrstvy. Snaha byla oddělit transportní vrstvu, řízení relace od signalizace. Rozdělení je následující:

- aplikační vrstva,
- kontrolní vrstva,
- transportní vrstva.

CSCF je označení pro skupinu SIP[1] serverů nebo SIP proxy serverů. Jedná se o kontrolní vrstvu IMS jádra. Rozděluje se podle funkce na tři signalizační servery:

- Proxy-CSCF – Proxy CSCF je bod prvního kontaktu terminálu s IMS, jedná se o příchozí a odchozí SIP server. P-CSCF registruje uživatele do IMS a generuje data pro účtování zákazníka. Jak již je z názvu patrné, P-CSCF se chová jako proxy definované v RFC3261, směruje SIP REGISTER do I-CSCF na základě doménového jména vyplněného v požadavku, směruje SIP požadavky od terminálu do S-CSCF a kontroluje a zabezpečuje obsah zpráv.
- Interrogating-CSCF – Interrogating CSCF je server na okraji sítě operátora a veřejně dostupný pro ostatní operátory. Samotnou funkcí je zakrytí topologie sítě, získání S-CSCF, která obsluhuje terminál a přeposílání zpráv do S-CSCF.
- Serving-CSCF – Serving CSCF je mozek IMS, i pro roamingové scénáře se nachází v operátorově síti a není vystavena veřejně pro ostatní operátory. Provádí registrace a řízení relace. S-CSCF má znalost IP terminálu a která P-CSCF byla využita pro vstup do jádra IMS.

HSS bylo přejato z anglického `Home Subscriber Server`. Jedná se o databázové úložiště uživatelských dat a relací samotných uživatelů. V případě, že uživatel není v HSS vytvořen, tak se u většiny operátorů ani nezaregistruje do IMS. HSS podporuje i okruhově přepínané sítě. Od 5. vydání 3GPP byl HLR a AuC zařazen pod HSS. HSS je dostupné pro MME přes rozhraní S6a, další rozhraní mířící do HSS jsou S6d, Gr, SWx, dále Cx a Sh rozhraní do IMS. V HSS musí existovat podpora pro různé protokoly, rozhraní používají MAP a Diameter. Mezi klíčové funkce HSS patří podpora uživatelské bezpečnosti, identifikace terminálu, podpora mobility (ukládání SGSN/MME) a autorizační data pro VLR/AAA a pro sestavení/ukončení hovorů.

SPR, Subscriber Profile Repository, je databáze definovaná pro držení dynamických uživatelských dat oproti více statickým datům držených v HSS. SPR je přes rozhraní Sp propojeno s PCRF. Často bývá i součástí PCRF nežli samostatná databáze. V porovnání s HSS rozhraní nebylo příliš zdokumentováno a 3GPP poskytuje pouze obecná doporučení a důvodem nejspíše je, že S6a a S6d rozhraní v HSS mohou sloužit pro komunikaci i mezi operátory, ale Sp rozhraní je pouze interní a jen mezi PCRF a SPR[8].

2.3 QoS

Dnešní pestrá nabídka služeb od operátorů šitých na míru zákazníkům přináší zvýšené nároky kladené na jejich sítě. Šířka přenosového pásma je ve všech lokalitách pravidelně navyšována, ale v určitých případech může nastat situace, že bude plně vyčerpána a je

[1] Session Initiation Protocol

potřeba určit, které služby jsou prioritnější a které ne. Každý si určitě dokáže představit, že placený videohovor přes operátorovu síť musí být bezvýpadkový a s dostatečnou kvalitou videa, aby to negativně neovlivnilo uživatelskou zkušenost.

Nejen datové toky, ale i skupiny uživatelů se od sebe budou lišit[8]. Síť se bude jinak chovat k příchozím roamingovým uživatelům než k domácím. Přeznačkování je známé, že probíhá na úrovni paketů, ale zde se objevuje koncept zvaný EPS kanál. Začíná u terminálu a končí v P-GW, nejedná se pouze o zaručení kvality na IP vstvě, ale součástí je i rádiová část. Kanál je definovaný jako IP přenosová cesta s určitou kapacitou, zpožděním a chybovostí. Prioritních tříd je 9 a kombinují předchozí požadavky. Vždy pro relaci existuje alespoň jeden základní EPS kanál, další kanály se nazývají vyhrazené a sestavují a deaktivují se na základě požadavků služeb a sítě.

Největší změna pro vytváření kanálů je viditelná při přechodu z GERAN[1] rádiové přístupové sítě do EUTRAN[2]. QoS na GERAN síti byl při zakládání spravován telefonem, na EUTRAN síti je už rozhodovací kompetence přesunuta do samotné sítě. Od 8. vydání 3GPP specifikace pro Gx rozhraní patří do EPS kanálu dva důležité atributy QCI a ARP[3][34]. QCI je numerický ukazatel na parametry kvality služby. ARP značí prioritu mezi kanály, např. při tísňových službách[9].

[1] GSM EDGE Radio Access Network
[2] Evolved Universal Terrestrial Radio Access Network
[3] Allocation and Retention Priority

Kapitola 3
Signalizace a protokoly

V jádru sítě se využívá mnoho protokolů, IMS a NGN jsou sítě založené na protokolech IP, SIP, Diameter nebo například H.248/Megaco[6]. Následující kapitoly se budou zabývat nejznámějšími protokoly v telekomunikačním světě.

3.1 Internet Protocol (IPv4/IPv6)

Je to nejpoužívanější protokol v počítačových sítích, je spojen se sítí Internet a jejím rozšířením po celém světě. Zasílaná zpráva se jmenuje datagram a obsahuje data a hlavičku IP protokolu o velikosti 20 až 64 bajtů (IPv4). IP datagram vzhledem k své proměnné velikosti podporuje fragmentaci u zdroje a znovusložení v cílové destinaci. V případě signalizace se jedná o nežádoucí jev [4]. Výhoda IPv6 je především v multihomingu, kde terminál může být připojen k více zdrojům konektivity zároveň a v případě výpadku jedné konektivity je využita konektivita druhá. V otázce bezpečnosti vyniká IPv6 více než IPv4, přináší lepší podporu IPsec tunelů. Zákazník při používání IPv6 může mít stejnou IP adresu v zahraničí i v domácí síti.

3.2 SCTP

Motivace použití jiného protokolu než TCP byla podporována nedostatky pro současné aplikace. TCP například nabízí spolehlivý přenos dat a přesné uspořádání dat při doručení. Některé aplikace přesné uspořádání nevyužijí a zbytečně tato operace prodlužuje dobu dodání. Další limitací byla například absence multihomingu. Na SCTP je nahlíženo jako na vrstvu mezi SCTP aplikací a IP vrstvou. Základní nabízenou službou SCTP je spolehlivé doručení zpráv mezi SCTP aplikacemi, které pro odeslání a doručení mohou využít více IP adres, tedy výše zmíněný multihoming. SCTP udržuje a kontroluje stav spojení pomocí kontrolních zpráv, které mají pouze jeden účel - zjistit stav spojení[4].

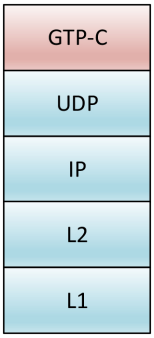
3.3 GTP

Jedná se o starší protokol jež je zkratkou z GPRS Tunneling Protocol a je využit při mnohačetném propojení prvků, ať už v síti domácí či mezi zahraničním partnerem a domácím prvkem. Tento protokol jen výsledkem z GSM standardů a specifických požadavků, jako je mobilita, řízení kanálů a tunelování uživatelských dat pro GPRS. Původní myšlenka byla využít GTP pouze pro 2G, ale je využit i v dalších generacích sítě (ve vyšší verzi pro řídící vrstvu - GTPv2-C). Rozděluje se na dvě části, na řídící část GTP-C a uživatelskou část GTP-U. Funkce jsou:

1. **řízení pohybu** – zprávy spadající do této funkce spravují identifikaci terminálu, stav terminálu napříč síťovými prvky a řídí přenos dat během handoveru,

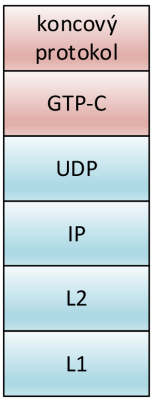
2. **řízení tunelů** – vytváření a mazání uživatelských relací, mazání kanálů. Informace pro zahájení pagingu a správa GTP tunelů pro terminály také patří do této funkcionality,
3. **funkce pro specifické služby** – do této kategorie patří například přidání podpory pro CS Fallback/SRVCC od GTPv2,
4. **funkce pro údržbu systému** – podpora celkové stability a obnovení z chybového stavu.

Na obrázku 3.1 je vidět, že GTP protokol je vystaven nad UDP/IP protokolem, IP protokol může být verze 4 nebo 6. GTP tunely jsou používány mezi dvěma prvky s GTP rozhraními. Unikátními identifikátory jsou TEID[1], IP adresa a UDP port. Pro řídící část GTP protokolu, GTP-C, je pro jeden terminál použit pouze jeden pár TEID[4].



Obrázek 3.1. GTP-C stack,

Uživatelská část GTP protokolu je vidět na obrázku 3.2. GTP-U tunely jsou používány pro přenos uživatelských dat. TEID je použito pro odlišení, ke kterým datům tunel patří. GTP-U tunely jsou zakládány MME po rozhraní S1.



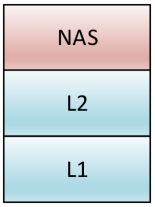
Obrázek 3.2. GTP-U stack

3.4 NAS

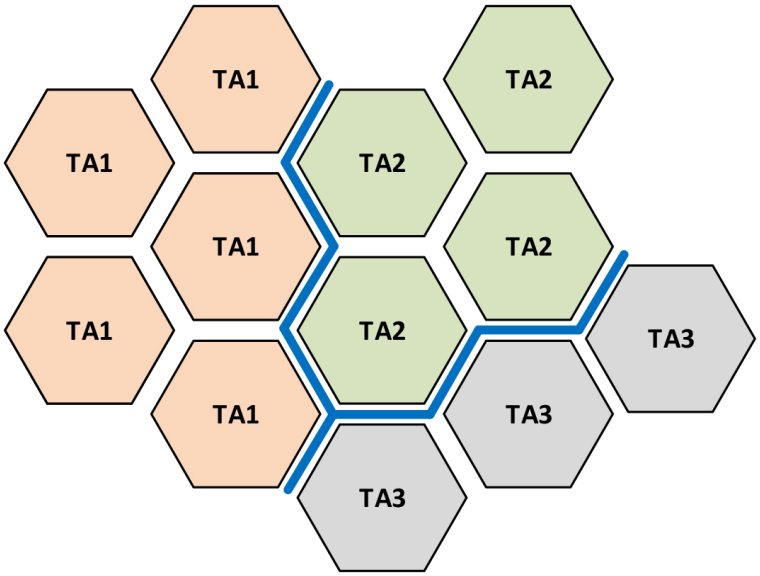
Zprostředkovává nerádiovou signalizaci směrem k terminálu. Z pohledu protokolové vrstvy je nejvyšší vrstvou z kontrolní úrovně.

Rozděluje se na dvě kategorie: řízení pohybu a řízení relace. Řízení pohybu popisuje procesy k zajištění mobility, přístupu, ověření a bezpečnosti. Po přihlášení do sítě je účastníkova lokalita sledována pomocí TAU identifikátoru.

[1] Tunnel Endpoint Identifier - stanoví přijímací strana.



Obrázek 3.3. NAS protokol



Obrázek 3.4. Tracking Area Update, citováno z [8].

Poloha je aktualizována během přechodu hranic, vyobrazených na obrázku 3.4. Pomocí TAU zprávy[1] lze v rušných oblastech terminálu zaslat list TAL s TAU identifikátory, pro které pak terminál nebude zasílat aktualizace v daných lokalitách[8].

Zamezí se signalizačnímu přehlcení sítě. Dále do řízení pohybu patří například paging. Při řízení relace dochází k sestavení IP spojení do PDN (Packet Data Network). Po sestavení spojení je otvírán základní EPS kanál[2] pro signalizaci a v případě potřeby vyhrazené kanály[3] pro VoLTE či VoWifi, v případě videa i ViLTE, které ale nebylo komerčně spuštěno. Obecně platí že dodatečné kanály jsou otevírány s menší prioritou než je samotná signalizace. Pro jedno spojení do PDN sdílí základní kanály stejnou IP a APN. Terminál ale může mít spojení do PDN více, například do internetu a IMS.

3.5 SIP

SIP je protokol na aplikační úrovni, který je používán pro sestavení, správu a ukončování multimediálních relací v IMS síti operátorů (a i obecně v IP sítích). SIP pochází od skupiny IETF a jeho podobnost s protokolem HTTP či SMTP není náhoda. Klíčové prvky SIP protokolu:

1. nezávislost na transportní vrstvě,
2. směrovatelnost požadavků,

[1] Tracking Area Update
[2] Default EPS bearer
[3] Dedicated EPS bearer

3. oddělení signalizace od aplikačních popisů,
4. rozšiřitelnost,
5. mobilita.

Popularita SIP protokolu vděčí také nezávislosti na technologii přístupové sítě. Při vydávání nových verzí je zaručena zpětná funkčnost na systémech, které nové funkce nepodporují, nebo nechtějí, ale mají požadavek na aktualizované základní bloky[7].

3.6 Diameter

Diameter protokol je nástupce protokolu Radius, jehož nedostatky má kompenzovat. Vylepšeno bylo například spolehlivé dodání zprávy, větší velikost pro informace u jednotlivých atributů a myšleno bylo také na bezpečnost. Z Radiusu zůstal Diameteru obsah zpráv skládající se z atributů AVP[1]. Diameter je definován ve standardu IETF RFC 3588 a 6733. Aplikace komunikující po Diameter rozhraní se může chovat jako:

- klient – navazuje spojení s agentem nebo se serverem,
- server – čeká na příchozí spojení a povoluje komunikaci klientů mající ve své konfiguraci,
- agent – na okrajích operátorovy sítě a zaručuje směrování zpráv podle obsahu a funguje i jako firewall před roamingovými partnery. Agent má různé způsoby použití, zprávy může pouze přesílat, což je časově nejrychlejší na zpracování, protože aplikace zpracovává pouze úvodní bajty zpráv. Funkce proxy poskytuje i možnost změny atributů z důvodu například skrytí topologie sítě. Další schopností je funkce prostředníka, s každým prvkem má vytvořené vlastní Diameter spojení.

Diameter podporuje zabezpečení dat pomocí TLS[2] nebo pomocí IPsec. RFC3588 přikazuje, že každá aplikace v roli agenta nebo serveru s Diameter rozhraním musí podporovat zabezpečení pomocí IPsec. Pro klienty není požadavek nutností.

[1] Attribute Value Pair
[2] Transport Layer Security

Kapitola 4
Gx rozhraní

4.1 Úvod

Diameter rozhraní Gx se nachází mezi PCRF[1] a PCEF[2], kde je používáno na přidávání, aktualizaci a odebírání PCC pravidel a informaci o stavových změnách na rozhraní k terminálu[32]. PCC pravidlo je nastavováno v PCEF pro pakety určitého datového toku a skládá se z:

- **názvu** – pojmenování pravidla, pokud se jedná o statické pravidlo, pak pravidla musí být synchronizovány mezi PCRF a PCEF. Dynamické pravidlo je nastavováno samotným PCRF a dodatečná synchronizace není potřeba,
- **identifikátoru služby**,
- **filtru služby** – k přesnému zacílení datového toku, parametry typu downlink, uplink a nebo například IP adresa terminálu,
- **precedensu,**
- **chování** – PCC pravidlo má podobný koncept jako IP tables, chování udává, zda-li se má tok povolit nebo zahodit,
- **QoS parametrů** – propustnost pro sestupný a vzestupný kanál a tzv. QCI,
- **parametrů pro účtování** – odlišující například toky v roamingu a v domácí síti.

Na základě PCC pravidla může dojít k:

- odlišení toků,
- jejich správnému účtování,
- kontroly toku (např. blokace dat v zahraničí)

Schéma Gx rozhraní vnímaného standardem je viditelné na obrázku 4.1.

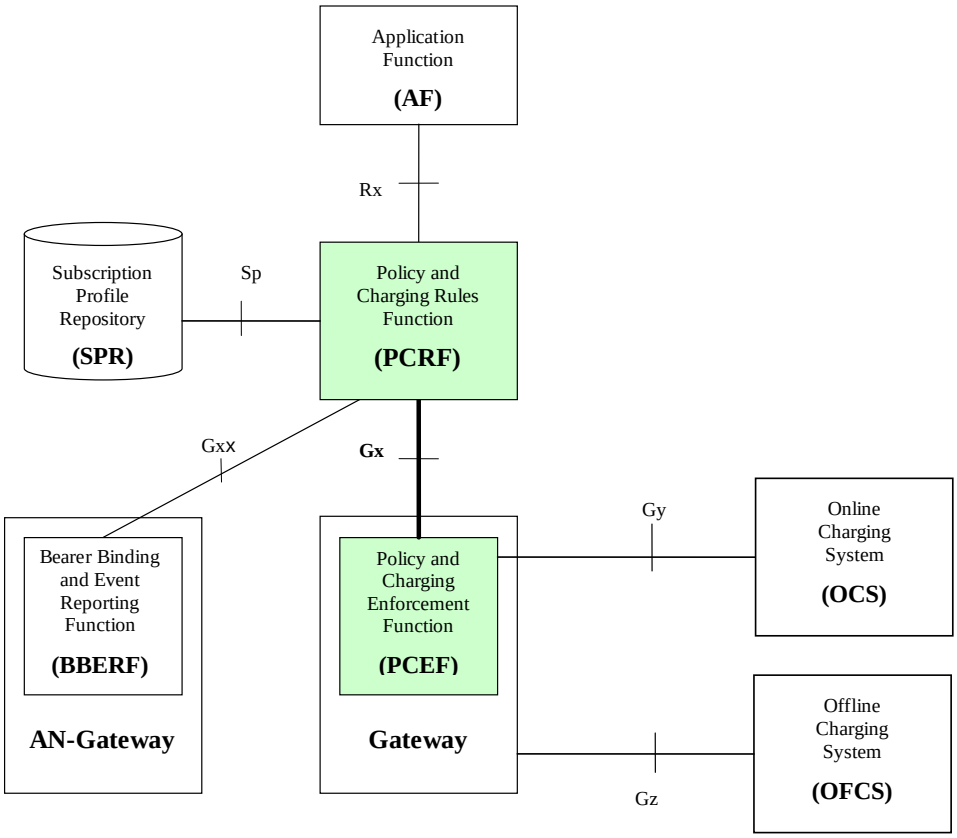
4.2 Změny na Gx rozhraní

Referenční vydání pro porovnání změn ve specifikacích Gx rozhraní je v této práci použito 7. vydání 3GPP specifikace[35]. V navazujících podkapitolách budou popsány nejdůležitější změny. Detailní vypracované změny atributů zpráv rozhraní pro jednotlivá vydání jsou popsány v příloze B

4.2.1 8. vydání

Přináší nově funkci BBERF[3], která využívá rozhraní Gxx pro komunikaci s PCRF. Funkci lze nalézt v S-GW (popř. v HSGW nebo ePDG) a dohlíží na správné párování QoS informací IP toků v S5/S8 rozhraní s kanály na S1 rozhraní[2]. PCRF má možnost si vyžádat informování o změnách v BBERF pro dané toky.

[1] Policy and Charging Rules Function
[2] Policy and Charging Enforcement Function
[3] Bearer Binding and Event Reporting Function



Obrázek 4.1. Gx schéma, citováno z [32]

Dále 8. vydání specifikace nově představuje ARP[1]. Pokud nastane síťová zácpa, kanál s vyšším ARP může nahradit kanál s nižším číslem[34].

4.2.2 9. vydání

Dává možnost využití IMS pro tísňové služby, standard přikazuje, že PCRF drží seznam tísňových APN ve své konfiguraci a zaručuje jim adekvátní prioritu v síti.

Mezi další přínosy patří rozšíření počtu relací pro jedno APN[33].

4.2.3 10. vydání

Specifikuje možnost sponzorovaného spojení v PCC pravidlech a související logice. Dále v PCC pravidlech přidává pole pro verzi IP protokolu. Z pohledu aplikační funkce na Rx rozhraní novinkou je i MPS[2] podpora, rozšiřuje tedy možnosti kombinace QCI a ARP[32].

4.2.4 11. vydání

Novinkou je Sd rozhraní do TDF[3]. PCRF zasílá po Sd rozhraní novou skupinu pravidel nazvanou ADC[4]. ADC na základě vstupů řídí vzestupný a sestupný datový tok terminálu[31].

[1] Allocation and Retention Priority
[2] Multimedia Priority Services
[3] Traffic Detection Function
[4] Application Detection and Control rules

4.2.5 12. vydání

Aktualizace Gyn a Gzn rozhraní související s TDF funkcí. V tomto vydání byly také doporučeny mechanismy předcházející zahlcení na Diameter rozhraních[30].

4.2.6 13. vydání

Nově aktualizace pro poskytování pozice přes Netloc funkcionalitu. Vhodné to je především v kontextu s tísňovými službami. Další aktualizace proběhla v přístupových sítích, bylo přidáno NB-IoT mezi Diameter informace na Gx rozhraní. Přidáno bylo i nové rozhraní St, které spojuje PCRF a TSSF[1], která nově dává možnost aplikovat ADC pravidla i na (S)Gi-LAN rozhraní. Další novinou jsou NBIFOM pravidla[2] umožňující přesměrovat zvolený typ datového toku do různých přístupových sítí[29].

4.2.7 14. vydání

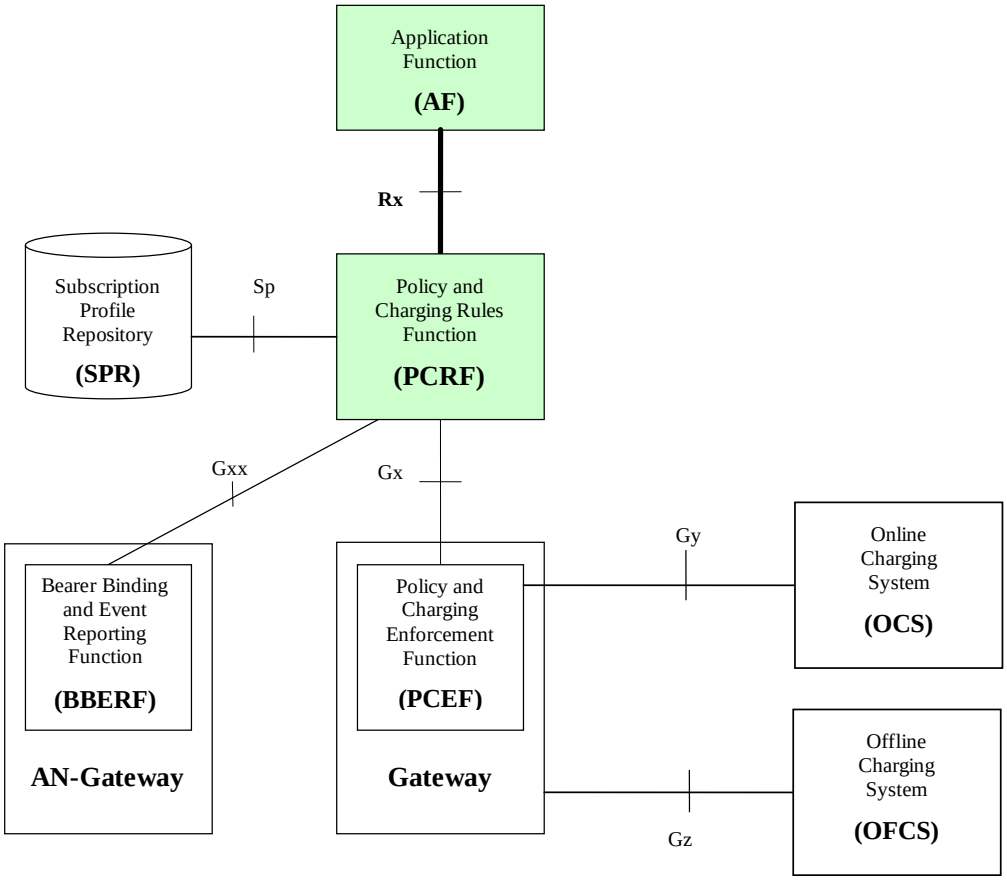
Ve 14. dochází k přidání nových odebíraných informací po Gx, jako je třeba změna eNodeB. Došlo i k aktualizaci a upřesnění NBIFOM a sponzorovaných dat pro TDF[28].

[1] Traffic Steering Support Function
[2] Network-Based IP Flow Mobility

Kapitola 5
Rx rozhraní

Rx rozhraní je mezi PCRF a AF[1], jelikož aplikační funkce je jen standardizační pojetí funkcionality, tak v praxi se setkáváme s rozhraním mezi PCRF a P-CSCF. AF má možnost si objednat informování o změnách na účastníkovi - jeho relaci, například, že došlo k ukončení relace nebo zákazník přešel na jiný druh rádiové přístupové sítě[8]. Protokol na Rx rozhraní je Diameter, P-CSCF využívá rozhraní při sestavování, změnách a terminaci hovoru přes IMS. PCRF potvrzuje, že zvolené kodeky a hodnoty pro hovor splňují parametry PCC pravidel v PCRF.

Schéma Rx rozhraní vnímaného standardem je viditelné na obrázku 5.1.



Obrázek 5.1. Rx schéma, citováno z [36]

[1] Application Function

Kapitola 6
Open-source platformy a API

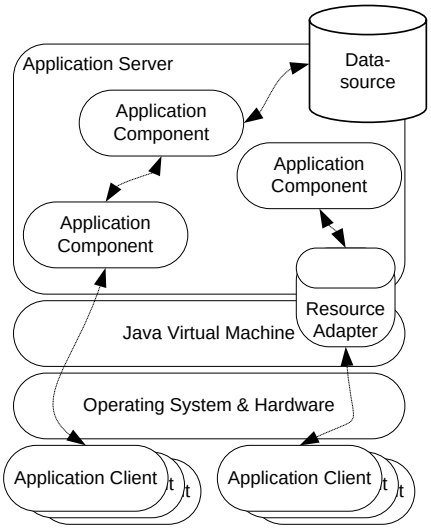
6.1 JAIN SLEE

V roce 1998 SUN Microsystems začaly s projektem JAIN, jehož zkratka znamená Java API pro integrované sítě. Za cíl si kladl vytvořit platformu pro novou generaci aplikací pro telekomunikační odvětví a nahradit staré, masivní a zastaralé aplikace. Vyústěním projektu JAIN byl vznik standardu JAIN SLEE (JSR-22, novější JSR-240), který definuje API a sémantiku aplikačního serveru pro telekomunikace[23].

Samotná specifikace vydaná pod záštitou Java Community Procesu definuje, že JAIN SLEE architektura využívá model skládající se z objektově orientovaných komponent[22], které lze skládat do bloků a dosáhnout komplexní, ale přehledné aplikace. Princip komunikace a skládání je ve standardu popsán také.

Výše zmíněný komponentový model SLEE[1] lze připodobnit podobným modelů jako EJB, Servlet nebo JSP. Nejedná se o Java EE, ačkoliv sdílí stejný přístup, kde aplikace běží v samostatném kontejneru. JAIN SLEE je více orientováno na příchozí a odchozí události s asynchronním přístupem, kde požadavkem je, co nejmenší odezva systému. Integrace JAIN SLEE a Java EE je podporována. Nejedná se ani o konkurenci Java EE, cílem je nahradit proprietární telekomunikační řešení řešením standardizovaným.

Na následujícím obrázku 6.1 je možné vidět sdílený kontejnerový model pro JAIN SLEE a Javu EE.



Obrázek 6.1. Java EE a JAIN SLEE model, citováno z [1].

JAIN SLEE standard podporuje 3 klíčová tvrzení při návrhu komunikace s externím rozhraním:

[1] Service Logic Execution Environment

- podpora standardů,
- podpora potřeb druhé strany aplikace na rozhraní,
- vrstvení rozhraní.

Aplikační server poskytuje možnosti ukládání logů, monitoringu a připojení. Na příkladu monitoringu lze vidět, že princip se při tvorbě aplikací opakuje, proto koncept přepoužití již hotových částí je v JAIN SLEE standardu také začleněn.

V JAIN SLEE se vyskytuje následující anglická terminologie:

1. **Events** – události, jedná se o stěžejní funkcionalitu JAIN SLEE. Funguje na principu vystavení a odběru událostí. Interní směrování událostí je prováděno samotným aplikačním serverem.
2. **Activity Context** – komponenta, která spravuje spojení mezi logicky propojenými SBB a přicházející událost směruje správnému elementu. V případě, že se jedná o událost označenou jako úvodní, tak je Activity Context komponenta instanciována. SBB může přijmout pouze události z asociovaných komponent Activity Context.
3. **Service Building Block** – komponenta, která tvoří samotnou funkcionalitu aplikace. Po splnění své funkce předává výsledek dalšímu SBB nebo pomocí rozhraní externímu elementu.
4. **Resource Adaptors** – pomocí vztahů a definicí zpráv utváří rozhraní a funguje jako zdroj událostí pro SBB a zároveň slouží i jako brána pro komunikaci externím světem.

Jediný dostupný opensource projekt je vedený společností Restcomm pod licencí AGPL3[14].

6.2 SIP Servlet

Pod pojmem servlet si většina lidí představí HTTP Servlet, který obsluhuje protokol HTTP. Java Servlet se nazývá každý program, který implementuje rozhraní Servlet. Rozhraní Sip Servlet tvrzení potvrzuje, rozšiřuje dané Servlet rozhraní.

Zde, jak je již z názvu patrné, se jedná o SIP aplikační server postavený na základech Java EE. Stejně jako JAIN SLEE, SIP Servlet je definován v Java specifikaci JSR-116 a novější JSR-289. Obsahuje několik tříd, které reagují na příchozí události pomocí metod s předdefinovanou syntaxí[7], uvedenou na následujícím příkladu metody `doInvite`,

```
protected void doInvite(SipServletRequest request)
        throws ServletException, IOException {

if (request.isInitial()) {
Proxy proxy = request.getProxy();
proxy.setRecordRoute(true);
proxy.setSupervised(true);
proxy.proxyTo(request.getRequestURI());
}
System.out.println("SimpleProxyServlet: Got request:\n" + request);
} .
```

Obrázek 6.2. Příklad doInvite metody[21].

Oproti HTTP, kdy přichází požadavek a odchází odpověď, je SIP protokol náročnější. Příchozí zprávy mohou přicházet nezávisle na jejich odchozím pořadí a zpracovávány jsou asynchronně.

6.3 Rhino

Rhino SLEE je aplikační server pro vývoj telekomunikačních aplikací. Je postaven na Java platformě a JAIN SLEE specifikaci 1.1 (JSR 240). Podporuje protokoly jako jsou například DIAMETER, SS7 (INAP,CAP), SIP a ISC.

Přidanou hodnotou je architektura vhodná pro nasazení na produkční systémy a vývoj a úprava vlastních Resource Adaptorů[15].

6.4 Parlay

Jednalo se o framework a API započaté v roce 1998 pěti spolupracujícími společnostmi. Skupina společností `The Parlay Group` úzce spolupracovala s 3GPP projektem a ETSI institutem a rok po začátku spolupráce se dočkali prvního vydání. Skupina dále byla a aktivní a dokonce spolupracovala i s JAIN projektem. Parlay aplikace mohou být spuštěny na aplikačních serverech, kde SCS je nazývána serverová část a aplikace klientská část. Pro komunikaci mezi nimi je použita infrastruktura CORBA. SCS je brána, jejíž vstupy a výstupy vedou do klíčových systémů operátorovy sítě[5].

Na obrázku 6.3 se architektura dělí na 3 úrovně:

- aplikaci,
- bránu,
- externí rozhraní.

Externí rozhraní implementují specifické protokoly (H.323, INAP, ...). Stejně jako v případě výše zmíněných API nabízejí volnost, komponenty nižších vstev lze použít jako stavební kámen i u dalších aplikací. Výběr a specifikace externího rozhraní je ale mimo rozsah Parlay specifikace, pokryto je pouze rozhraní mezi aplikací a bránou[11].

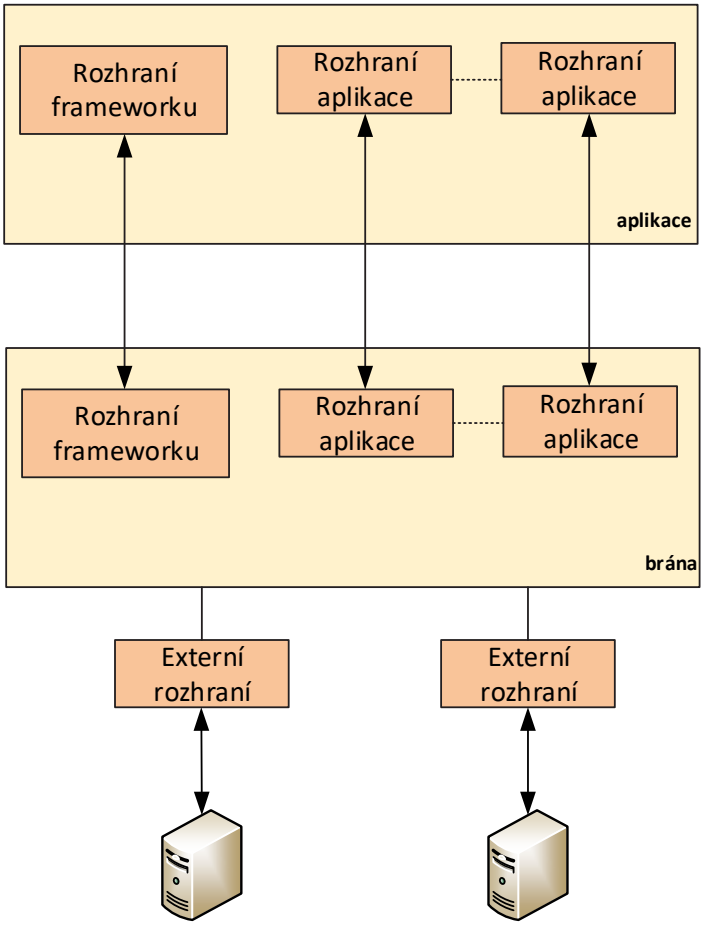
6.5 Elixir/OTP

Elixir je funkcionální programovací jazyk, který staví na pilířích, jako jsou tolerance vůči chybám, distribuovanost a nízká odezva. Elixir vychází z jazyka Erlang(využívá Erlang VM) hojně využívaným v telekomunikačním odvětví. Erlang nabízí soubor knihoven a pravidel ulehčující vývoj aplikací běžících v reálném čase nazvaný OTP[1]. Napsaný kód je strukturován následovně:

- **funkce** – jsou shlukovány v souborech zvané moduly, funkce použité v ostatních modulech jsou exportovány a moduly je musí importovat,
- **moduly** – společně tvoří aplikaci, mají dodatečný popisný soubor, který popisuje souborovou strukturu, moduly a parametry,
- **finální verze** – nejvyšší vrstva obsahující všechny v definičním souboru popsané aplikace.

Hlavní elementem je zpráva, vytvářející izolovaný proces, který může komunikovat s ostatními procesy pouze pomocí předávání zpráv ve formátu `Pid!Msg`[12]. Erlang oproti Elixiru postrádá moderní nástroje pro vytváření a správu balíčků[19] a v určitých případech i syntaxi napomáhající k porozumění kódu, jak zmiňuje sám zakladatel Erlangu v [20].

[1] Open Telecom Platform



Obrázek 6.3. Parlay architektura, citováno z [11].

6.6 Zhodnocení platforem

V Kapitolách 6.1 až 6.5 byly rozebrány základní vlastnosti a architektury nejrozšířenějších opensource platforem. Z analýzy vyplývá, že platformy se vzájemně liší nejen zaměřením na odlišné protokoly, ale i složitostí implementace. Mezi výše zmíněnými platformami, jsou i takové, které jsou pro vývoj aplikace s Diameter rozhraními nevhodné nebo například příliš složité.

Mezi nevyhovující patří Parlay a SIP Servlet. Parlay nabízí plný přístup ke všem schopnostem společným pro všechny protokoly, ale mnoho jich společných není a není podporováno ani v Parlay API. Další nevýhodou je, že Parlay brány nenabízí aplikační prostředí, kde by aplikace běžela. Aplikace musí bohužel použít externí aplikační server[27]. Dle dostupných pramenů a jejich dat vydání lze soudit, že už se jedná o pomalu vymírající projekt.

SIP Servlet je nevyhovující z pohledu podpory protokolů. Zaměřuje se pouze na SIP protokol.

Rhino se vyskytuje někde na pomezí použitelnosti, protože funguje částečně komerčně, omezená licence je dostupná na [17]. Produkční nasazení by si vyžádalo další investici. Ale v ceně je nabízena přehledná dokumentace a podpora při nasazení.

Elixir a Erlang jsou dobrou volbou, pokud je člověk dostatečně seznámen se stylem programování v nich. Nevýhodou je náročnost syntaxe jazyka a nutné seznámení s vlastnostmi Beam (Erlang) VM. Další nedostatek je zmíněn v [12] a jedná se o pomalý start, na který je potřeba myslet při návrhu architektury.

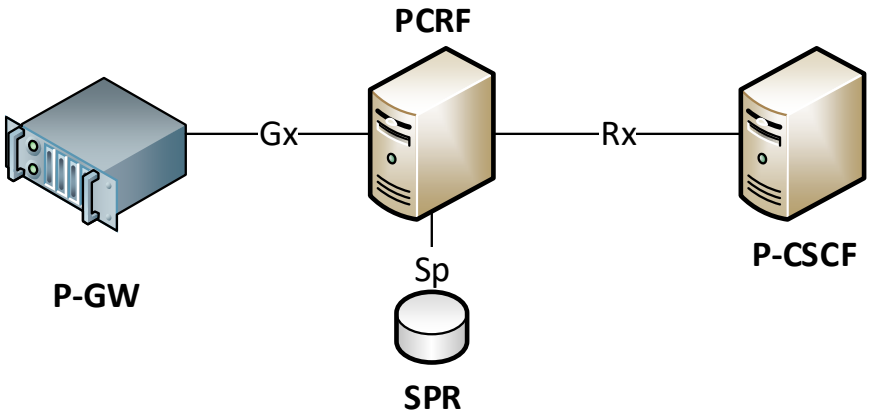
Volně nabízená implementace standardu JAIN SLEE nabízí vhodnou architekturu pro vývoj telekomunikačních aplikací závislých na dostupnosti. Už ve svých počátcích dosahoval lepších hodnot z hlediska výkonnosti než Parlay[10]. JAIN SLEE využívá nadstavby nad využívaným aplikačním serverem JBoss, aktuálně ve verzi Wildfly. Aplikační server již řeší otázky monitoringu a logování. Dohromady s programovacím jazykem Java nabízí obrovský potenciál, jazyk je v praxi používaný a dosahuje v TIOBE indexu prvních míst[13], proto dostupnost knihoven k použití je více než dostatečná. V [3] zmiňuje, že už v době vydání knihy Java Community Process specifikuje použití Javy pro spracování požadavků v reálném čase. Resource Adaptor pro Diameter je taktéž k dispozici. Z analýzy tedy vyplývá, že pro vývoj aplikace implementující PCRF funkcionalitu je tedy nejvhodnější varianta JAN SLEE s otevřeným zdrojovým kódem spravovanou společností Restcomm.

Kapitola 7
Aplikace obsluhující rozhraní Gx a Rx

7.1 Obecný návrh

Účelem PCRF je v aktuálním čase rozhodovat o přidělování kvality služby (QoS) a nastavení příslušného PCC pravidla[1] na Gx rozhraní. PCRF spojuje vstupní informace na signalizační vstvě sítě, podpůrných systémů a ostatních zdrojů jako jsou portály a operátorské aplikace pro mobilní telefony. Výše zmíněné PCC pravidlo je tvořeno automaticky na základě vstupů mířících do PCRF, jmenovitě:

- informace ze CRM uložené v SPR,
- informace získané synchronně, v reálném čase z Diameter rozhraní (např. signalizace hovoru),
- informace z nestandardních/interních vstupů operátorů po REST/Webservice rozhraních. Následující obrázek 7.1 ukazuje možnou integraci s ePC(P-GW) s IMS (P-CSCF).



Obrázek 7.1. Obecná architektura modelu.

7.1.1 QoS

Proč je potřeba řídit kvalitu služby? Existují skupiny uživatelů, kteří potřebují být obslouženi přednostně. Nebo například služby jako Voice over LTE musí být obslouženy přednostně, protože jinak by docházelo k negativní uživatelské zkušenost a nevýhody paketově přepínaných sítí by převážily jejich výhody. Pokud sítě starších okruhově přepínaných spojují hovor v průměru okolo 7 sekund, nelze aby novější generace operátorské sítě spojovala hovor stejně dlouho. PCRF na základě signalizačního toku od P-CSCF rozpozná službu citlivou na latenci a jitter a přiřadí správné QoS parametry (na Diameteru nazvané QCI) a nastaví požadavky i na radiové přístupové síti.

[1] Charging Rule

Aplikace byla vybrána na základě skutečného použití v sítích operátorů. Zvolena byla 3GPP funkcionalita PCRF. Navrhované řešení se přibližuje technice vývoje softwaru, kde se aplikace rozdělí na menší funkční celky - tzv. microservices. Tento koncept se využívá i v sítích páté generace. Řešení navrhuje rozdělit PCRF definované v 3GPP na dva menší funkční celky:

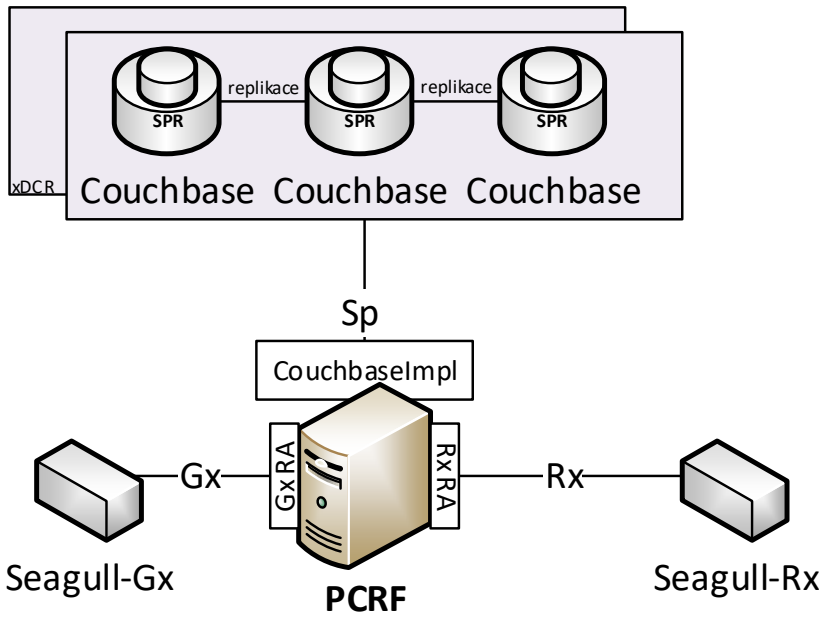
1. datové – napojené pouze na rozhraní Gx, mající za úkol řešit téma datových propozice, měřit spotřebovaná data zákazníka a pružně reagovat na absenci nebo aktivaci datových balíčků,
2. IMS – využívající rozhraní Gx a Rx, začleněné do IMS signalizace při řízení hovorů přes paketově přepínané jádro sítě.

Aplikace demonstruje požadavky kladené na PCRF používané při sestavování, udržování a ukončování VoLTE, VoWifi a ViLTE hovorů. Rozdělení provozu mezi dvě PCRF není obsahem této práce, ale je technicky realizovatelné například pomocí dvou rozdílných APN.

7.2 Detailní návrh

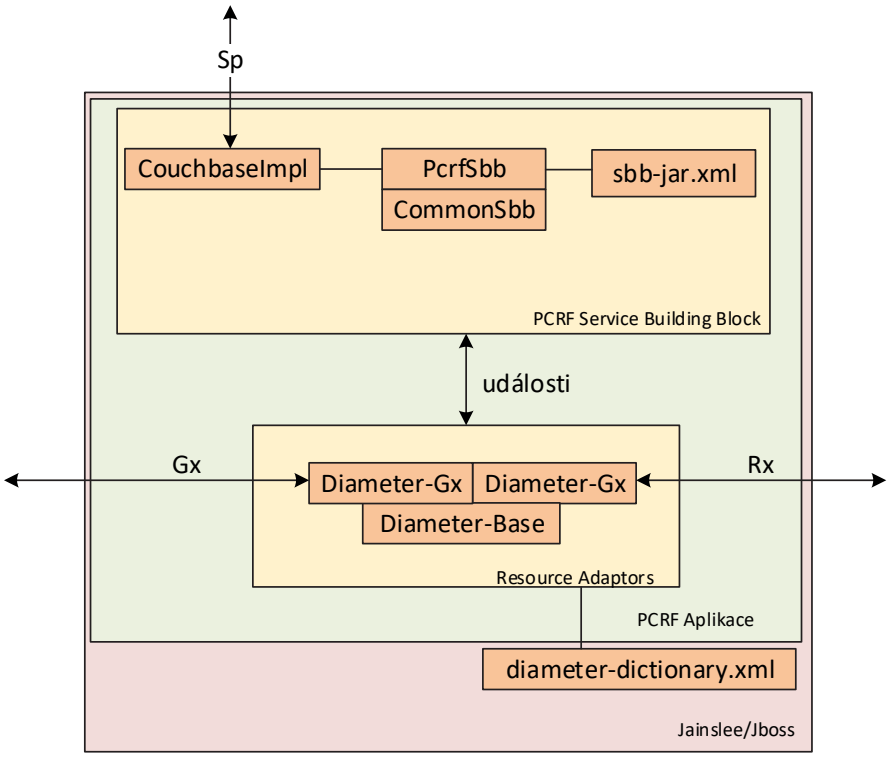
Na obrázku 7.2 je nastíněn návrh integrace aplikace. Při dodávce aplikace do operátorovi sítě by mohl zaznít požadavek na dodání i SPR databáze, proto součástí aplikace je i databáze Couchbase 7.2.2. Na obrázku jsou už naznačeny aplikační moduly rozhraní Gx a Rx, jejich detailní popis následuje v Kapitole 7.2.4.

Simulaci na otestování funkčnosti obstarávají dvě rozhraní do simulátoru Seagull.



Obrázek 7.2. Interní struktura rozhraní

Obrázek 7.3 zobrazuje navrženou vnitřní architekturu aplikace. Samotná aplikace se rozděluje na dva bloky, blok poskytující Diameter protokol a blok související s logikou aplikaci. V souborech ve formátu XML jsou uložené konfigurační parametry pro aplikaci.



Obrázek 7.3. Interní struktura aplikace

7.2.1 Couchbase

Couchbase je NoSQL databáze dostupná na `https://www.couchbase.com/`. V PCRF aplikaci je použit pouze jeden server databáze. Couchbase vyniká jednoduchostí, obsahuje webové rozhraní pro konfiguraci clusteru, nastavení replikací a replikace mezi datovými centry xDCR[1], proto demonstrace škálování u více datacenter je jen otázka konfigurace a dostupného hardware.

7.2.2 Seagull simulátor

Seagull je simulátor mnoha protokolů napsaný v C++, dostupný na `http://gull.sourceforge.net/`. Poskytuje vše potřebné pro podporu simulace aplikace po Diameter rozhraní. Seagull je použit v mé verzi s dodatečně opraveným chováním pro Diameter keep-alive zprávy. Verze je veřejně dostupná na `https://github.com/tom130/seagull`.

Simulační scénáře se v simulátoru tvoří v XML souborech, navázání Diameter spojení pomocí zpráv CER a CEA je vidět na následujícím příkladu:

```
  <send channel="channel-Gx">
      <action>
          <set-value name="HbH-id" format="$(HbH-counter)"></set-value>
          <set-value name="EtE-id" format="$(EtE-counter)"></set-value>
          <set-value name="Origin-Realm" format="diameter\_realm"></set-
value>
```

[1] `https://developer.couchbase.com`

```
            <set-value name="Origin-Host" format="seagull-Gx"></set-value>
        </action>
        <command name="CER">
            <avp name="Origin-Host" value="______"></avp>
            <avp name="Origin-Realm" value="_____"></avp>
            <avp name="Host-IP-Address" value="0x0001C0A83850"></avp>
            <!-- IPV4 10.3.252.94-->
            <avp name="Vendor-Id" value="8164"></avp>
            <avp name="Product-Name" value="ASR5000"></avp>
            <avp name="Origin-State-Id" value="1094807040"></avp>
            <avp name="Supported-Vendor-Id" value="5535"></avp>
            <avp name="Supported-Vendor-Id" value="10415"></avp>
            <avp name="Auth-Application-Id" value="16777238"></avp>
            <avp name="Inband-Security-Id" value="0"></avp>
            <avp name="Vendor-Specific-Application-Id">
                <avp name="Vendor-Id" value="10415"></avp>
                <avp name="Auth-Application-Id" value="16777238"></avp>
            </avp>
            <avp name="Firmware-Revision" value="60354"></avp>
        </command>
        <action></action>
    </send>
    <receive channel="channel-Gx">
        <action>
            <check-value name="Result-Code" behaviour="error"></check-value>
        </action>
        <command name="CEA">
            <avp name="Result-Code" value="2001"></avp>
        </command>
    </receive>
    <wait-ms value="100"></wait-ms>
```

Obrázek 7.4. Úsek simulační scénáře pro navázání spojení.

7.2.3 Resource Adaptors

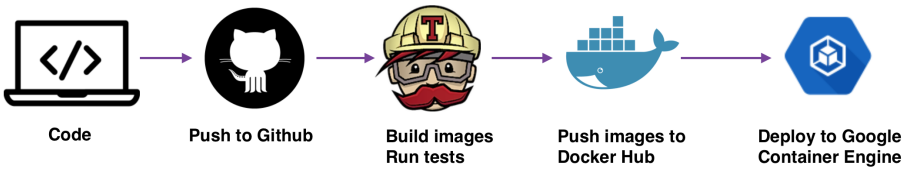
Resource Adaptor je komponenta v JAIN SLEE, která poskytuje aplikaci prostředky pro komunikaci. Protokol je vždy závislý na konkrétní implementaci, v diplomové práci jsou používány pouze pro komunikaci po Diameter rozhraních.

7.2.4 Metodika vývoje a nasazení

Na obrázku 7.5 je vidět způsob vývoje diplomové práce. Na začátku je vývoj aplikace v jazyce Java a ve vývojovém prostředí IntelliJ Idea[1], po zpracování úkolů na denní bázi je využit verzovací systém Git a studentům dostupná webová nadstavba Github[2]. Dále došlo k integraci průběžné integrace pomocí Travis CI[3], která využije popis projektu v Mavenu k sestavení artefaktu - JAR souboru. V tomto kroku jsou již zaintegrované dílčí testy[4] na ověření základní funkcionality frameworku.

Dalším krokem je vytvoření Docker obrazu pomocí v repozitáři přiloženého Dockerfile předpisu. Docker[5] je způsob virtualizace na bázi LXC kontejnerizace přidané do

[1] https://www.jetbrains.com/idea/
[2] https://github.com/
[3] https://travis-ci.com/
[4] v angličtině Unit testy
[5] https://github.com/docker/docker-ce



Obrázek 7.5. Životní cyklus Dockeru, citováno z[25]

Linuxového jádra v roce 2008 [24]. Vytváří izolované prostředí na hostitelském systému (ale může to být i v rámci clusteru). Docker zajistí aplikaci konzistenci prostředí od verze operačního systému až po dodatečné knihovny. Travis CI po sestavení artefaktu zabalí aplikaci do Docker obrazu. Obraz je použitelný i pro produkční nasazení.

```
env:
  global:
    - secure: "DOCKER_USER"
    - secure: "DOCKER_PASS"
    - COMMIT=${TRAVIS_COMMIT::8}
    - JBOSS_HOME=$TRAVIS_BUILD_DIR/wildfly/jslee/
language: java
install: true
script: mvn clean install
after_success:
  - cd $TRAVIS_BUILD_DIR/enablers/pcrf-server/du/target && ant deploy
  - cd $TRAVIS_BUILD_DIR/resources/diameter-base/du/target && ant deploy
  - cd $TRAVIS_BUILD_DIR/resources/diameter-gx/du/target && ant deploy
  - cd $TRAVIS_BUILD_DIR/resources/diameter-rx/du/target && ant deploy
  - docker login -u $DOCKER_USER -p $DOCKER_PASS
  - export REPO=githubrepo/pcrf
  - export TAG=`if [ "$TRAVIS_BRANCH" == "master" ]; then echo "latest"
    else echo $TRAVIS_BRANCH ; fi`
  - docker build -f $TRAVIS_BUILD_DIR/wildfly/Dockerfile -t $REPO:$COMMIT
    $TRAVIS_BUILD_DIR/wildfly/
  - docker tag $REPO:$COMMIT $REPO:$TAG
  - docker tag $REPO:$COMMIT $REPO:travis-$TRAVIS_BUILD_NUMBER
  - docker push $REPO
```

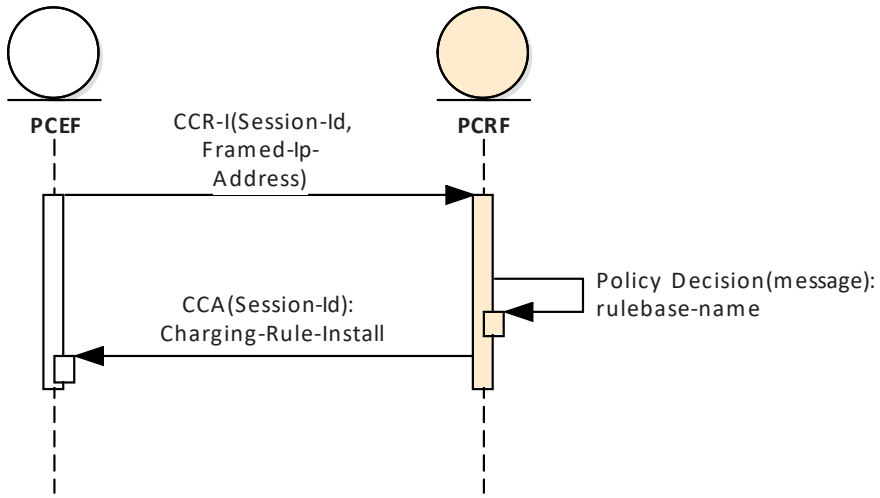
Obrázek 7.6. Konfigurační soubor pro Travis CI.

7.3 Scénáře

Následující scénáře popisují možnosti příchozí zpráv. Součástí aplikace jsou i následující scénáře pro ověření funkcionality ve výše zmíněném simulačním programu Seagull. V některých případech musí dokonce dojít ke stejné posloupnosti skupiny zpráv, aby dané chování bylo pozorovatelné. Navázání spojení je pro přehlednost v následujících materiálech vynecháno.

7.3.1 Připojení terminálu do sítě

Navázání spojení terminálu s ePC a získání IP adresy vygeneruje zprávu Credit Control Request Diameter protokolu, která je zasílána po rozhraní Gx z P-GW do PCRF. Důvodem je žádost o sestavení základního EPS kanálu.



Obrázek 7.7. Připojení terminálu.

Obsah příchozí zprávy Credit-Control-Request Initial je vidět na 7.1. V případě, že by primární APN bylo nastavené na IMS i pro datovou část, tak by IMS PCRF obsluhovalo i žádosti o přípojení od všech účastníků v 4G RAN. Obsah zpráv přišlých po Gx rozhraní by se nelišil, směrem od PCRF, narozdíl od datových propozic, dává smysl využít pouze jednoho pravidla.

Attribute-Value Pair	**Hodnota**
Auth-Application-Id(258)	16777238
Origin-Host(264)	seagull-Gx
Origin-Realm(296)	diameter_realm
Destination-Realm(283)	diameter_realm
CC-Request-Type(416)	INITIAL_REQUEST
CC-Request-Number(415)	0
Destination-Host(293)	jslee
Origin-State-Id(278)	1370427633
Subscription-Id(443)	-
*Subscription-Id-Type(450)	END_USER_E164
*Subscription-Id-Data(444)	420000000001
Subscription-Id(443)	-
*Subscription-Id-Type(450)	END_USER_IMSI
*Subscription-Id-Data(444)	230010000000001
Supported-Features(628)	-
*Vendor-Id(266)	10415
*Feature-List-ID(629)	1
*Feature-List(630)	2
Network-Request-Support(1024)	NETWORK_REQUEST

Framed-IP-Address(8)	192.168.1.3
IP-CAN-Type(1027)	3GPP-EPS
RAT-Type(1032)	EUTRAN
User-Equipment-Info(458)	-
*User-Equipment-Info-Type(459)	IMEISV
*User-Equipment-Info-Value(460)	-
**User-Equipment-Info-Value	490154203237518
QoS-Information(1016)	-
*APN-Aggregate-Max-Bitrate-UL(1041)	64000
*APN-Aggregate-Max-Bitrate-DL(1040)	64000
Default-EPS-Bearer-QoS(1049)	-
*QoS-Class-Identifier(1028)	QCI_5
*Allocation-Retention-Priority(1034)	-
**Priority-Level(1046)	-
***Pre-emption-Capability(1047)	PRE-EMPTION_CAPABILITY_DISABLED
***Pre-emption-Vulnerability(1048)	PRE-EMPTION_VULNERABILITY_DISABLED
AN-GW-Address(1050)	10.1.80.140
3GPP-User-Location-Info(22)	38323332663031303237...
3GPP-MS-TimeZone(23)	GMT+ 10hours 45minutes
Called-Station-Id(30)	ims
Bearer-Usage(1000)	GENERAL
Online(1009)	DISABLE_ONLINE
Offline(1008)	DISABLE_OFFLINE
Access-Network-Charging-Address(501)	10.255.80.123
Access-Network-Charging-Identifier-Gx	-
*Access-Network-Charging-Identifier-Gx	000001f7c0000014000028af3365326633313130

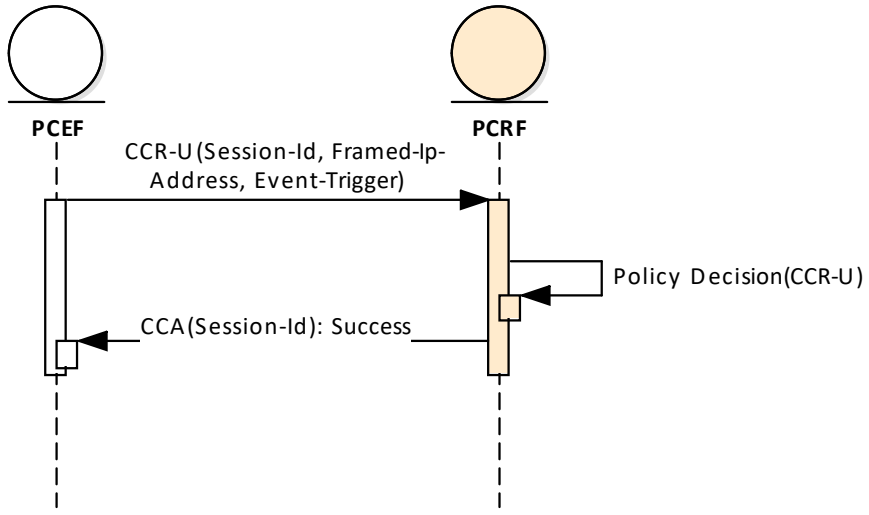
Tabulka 7.1. Obsah příchozí Credit-Control-Request Initial

Attribute-Value Pair	Hodnota
Session-Id(263)	gx-session;145020081;11038;0
Auth-Application-Id(258)	16777238
Origin-Host(264)	jslee
Origin-Realm(296)	diameter_realm
Route-Record(282)	seagull-Gx
CC-Request-Type(416)	INITIAL_REQUEST
CC-Request-Number(415)	0
Origin-State-Id(278)	1024
Charging-Rule-Install(1001)	-
*Charging-Rule-Base-Name(1001)	ims
Result-Code(268)	DIAMETER_SUCCESS

Tabulka 7.2. Obsah odchozí odpovědi na Credit-Control-Request Initial

7.3.2 Aktualizace relace po rozhraní Gx

Aktualizace je zasílána při změnách na zákazníkovi, například pokud terminál přechází mezi přístupovými sítěmi. V tomto případě je očekáváno od PCRF potvrzení, že má zákazník záznam v SPR a databází relací (oboje je integrované do Couchbase).



Obrázek 7.8. Aktualizace relace.

Důležitým atributem ve zprávách je IP adresa terminálu – `Framed-IP-Address`. Je nastavená jako primární klíč pro Gx relace.

Attribute-Value Pair	Hodnota
Session-Id(263)	gx-session;145020081;11038;0
Auth-Application-Id(258)	16777238
Origin-Host(264)	seagull-Gx
Origin-Realm(296)	diameter_realm
Destination-Realm(283)	diameter_realm

CC-Request-Type(416)	UPDATE_REQUEST
CC-Request-Number(415)	1
Destination-Host(293)	jslee
Origin-State-Id(278)	1370427633
Subscription-Id(443)	-
*Subscription-Id-Type(450)	END_USER_E164
*Subscription-Id-Data(444)	420000000001
Subscription-Id(443)	-
*Subscription-Id-Type(450)	END_USER_IMSI
*Subscription-Id-Data(444)	230010000000001
Network-Request-Support(1024)	NETWORK_REQUEST
Framed-IP-Address(8)	192.168.1.3
IP-CAN-Type(1027)	3GPP-EPS
RAT-Type(1032)	EUTRAN
User-Equipment-Info(458)	-
*User-Equipment-Info-Type(459)	IMEISV
*User-Equipment-Info-Value(460)	-
**User-Equipment-Info-Value	490154203237518
QoS-Information(1016)	-
*APN-Aggregate-Max-Bitrate-UL(1041)	64000
*APN-Aggregate-Max-Bitrate-DL(1040)	64000
AN-GW-Address(1050)	10.1.80.140
3GPP-User-Location-Info(22)	38323332663031303237...
3GPP-MS-TimeZone(23)	GMT+ 10hours 45minutes
Called-Station-Id(30)	ims
Access-Network-Charging-Address(501)	10.255.80.123
Event-Trigger(1006)	QOS_CHANGE
Event-Trigger(1006)	RAT_CHANGE
Event-Trigger(1006)	USER_LOCATION_CHANGE

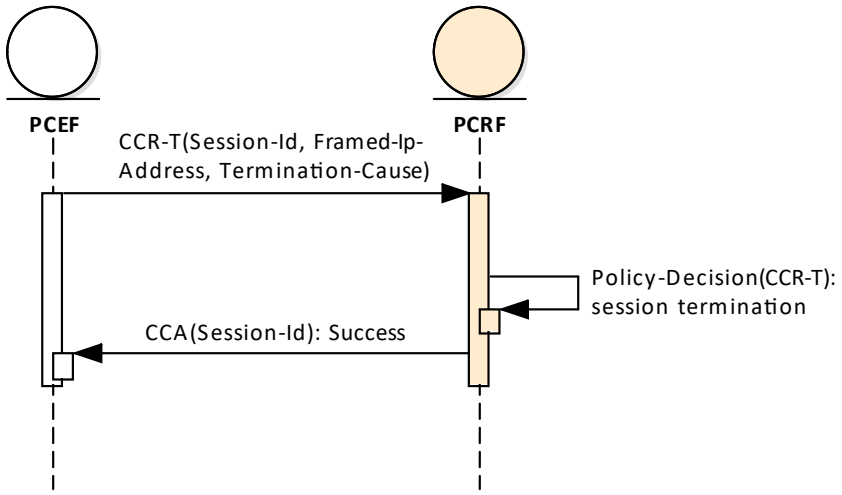
Tabulka 7.3. Obsah příchozí Credit-Control-Request Update

Attribute-Value Pair	Hodnota
Session-Id(263)	gx-session;145020081;11038;0
Auth-Application-Id(258)	16777238
Origin-Host(264)	jslee
Origin-Realm(296)	diameter_realm
Route-Record(282)	seagull-Gx
CC-Request-Type(416)	UPDATE_REQUEST
CC-Request-Number(415)	1
Origin-State-Id(278)	1024
QoS-Information(1016)	-
*APN-Aggregate-Max-Bitrate-UL(1041)	64000
*APN-Aggregate-Max-Bitrate-DL(1040)	64000
Result-Code(268)	DIAMETER_SUCCESS
Event-Trigger(1006)	RAT_CHANGE
Event-Trigger(1006)	USER_LOCATION_CHANGE

Tabulka 7.4. Obsah odchozí odpovědi na Credit-Control-Request Update

7.3.3 Ukončení relace

U tohoto scénáře se nevyžaduje pouze potvrzení, ale i akce aplikace vedoucí na smazání záznamů pro ukončovanou relaci.



Obrázek 7.9. Ukončení relace.

Attribute-Value Pair	Hodnota
Session-Id(263)	gx-session;145020081;11038;0
Auth-Application-Id(258)	16777238
Origin-Host(264)	seagull-Gx
Origin-Realm(296)	diameter_realm
Destination-Realm(283)	diameter_realm
CC-Request-Type(416)	TERMINATION_REQUEST

CC-Request-Number(415)	2
Destination-Host(293)	jslee
Origin-State-Id(278)	1370427633
Subscription-Id(443)	-
*Subscription-Id-Type(450)	END_USER_E164
*Subscription-Id-Data(444)	420000000001
Subscription-Id(443)	-
*Subscription-Id-Type(450)	END_USER_IMSI
*Subscription-Id-Data(444)	230010000000001
Framed-IP-Address(8)	192.168.1.3
Termination-Cause(295)	DIAMETER_LOGOUT
User-Equipment-Info(458)	-
*User-Equipment-Info-Type(459)	IMEISV
*User-Equipment-Info-Value(460)	-
**User-Equipment-Info-Value	490154203237518
Called-Station-Id(30)	ims
Access-Network-Charging-Address(501)	10.255.80.123

Tabulka 7.5. Obsah příchozí Credit-Control-Request Terminate

Attribute-Value Pair	Hodnota
Session-Id(263)	gx-session;145020081;11038;0
Auth-Application-Id(258)	16777238
Origin-Host(264)	jslee
Origin-Realm(296)	diameter_realm
Route-Record(282)	seagull-Gx
CC-Request-Type(416)	TERMINATE_REQUEST
CC-Request-Number(415)	2
Origin-State-Id(278)	1024
Result-Code(268)	DIAMETER_SUCCESS

Tabulka 7.6. Obsah odchozí odpovědi na Credit-Control-Request Terminate

7.3.4 Zpráva Re-Authorization Request

Pokud PCRF potřebuje vynutit pravidlo na síti, použije tuto zprávu. Nastavované dynamické PCC pravidlo je viditelné u atributu `Charging-Rule-Name`. Po tomto kroku PCRF očekává potvrzení o provedených změnách.

Attribute-Value Pair	Hodnota
Session-Id(263)	gx-session;145020081;11038;0
Auth-Application-Id(258)	16777238
Origin-Host(264)	seagull-Gx
Origin-Realm(296)	diameter_realm

Destination-Realm(283)	diameter_realm
Destination-Host(293)	jslee
Re-Auth-Request-Type(285)	AUTHORIZE_ONLY
Event-Trigger(1006)	QOS_CHANGE
Event-Trigger(1006)	RAT_CHANGE
Event-Trigger(1006)	USER_LOCATION_CHANGE
Charging-Rule-Install(1001)	-
*Charging-Rule-Definition(1003)	-
**Charging-Rule-Name(1005)	rx.realm;151016280;0:704656758:1409313516
**Rating-Group(432)	9000
**Flow-Information(1058)	-
***Flow-Description(507)	permit in ip from 10.60.90.161 49120 to 10.207.22.210 10062
***Flow-Direction(1080)	UPLINK
**Flow-Information(1058)	-
***Flow-Description(507)	permit in out from 10.207.22.210 10062 to 10.60.90.161 49120
***Flow-Direction(1080)	DOWNLINK
**Flow-Status(1058)	ENABLED
**QoS-Information(1016)	-
***Qos-Class-Identifier(1028)	QCI_1
***Max-Requested-Bandwidth-UL(516)	128000
***Max-Requested-Bandwidth-DL(515)	128000
***Guaranteed-Bitrate-UL(1026)	128000
***Guaranteed-Bitrate-DL(1025)	128000
***Allocation-Retention-Priority(1034)	-
****Priority-Level(1046)	-
****Pre-emption-Capability(1047)	PRE-EMPTION_CAPABILITY_DISABLED
****Pre-emption-Vulnerability(1048)	PRE-EMPTION_VULNERABILITY_DISABLED
**Online(1009)	DISABLE_ONLINE
**Offline(1008)	ENABLE_OFFLINE
**Precendence(1010)	1
**Access-Network-Charging-Identifier-Gx	000001f7c0000014000028af3365326633313130
**Flows(510)	-
***Media-Component-Number(518)	16780285
***Flow-Number(518)	33560570
*Charging-Rule-Definition(1003)	-
**Charging-Rule-Name(1005)	rx.realm;151016280;0:704656758:1409313516

**Rating-Group(432)	9000
**Flow-Information(1058)	-
***Flow-Description(507)	permit in ip from 10.60.90.161 49121 to 10.207.22.210 10063
***Flow-Direction(1080)	UPLINK
**Flow-Information(1058)	-
***Flow-Description(507)	permit out from 10.207.22.210 10063 to 10.60.90.161 49121
***Flow-Direction(1080)	DOWNLINK
**Flow-Status(1058)	ENABLED
**QoS-Information(1016)	-
***Qos-Class-Identifier(1028)	QCI_1
***Max-Requested-Bandwidth-UL(516)	128000
***Max-Requested-Bandwidth-DL(515)	128000
***Guaranteed-Bitrate-UL(1026)	128000
***Guaranteed-Bitrate-DL(1025)	128000
***Allocation-Retention-Priority(1034)	-
****Priority-Level(1046)	-
****Pre-emption-Capability(1047)	PRE-EMPTION_CAPABILITY_DISABLED
****Pre-emption-Vulnerability(1048)	PRE-EMPTION_VULNERABILITY_DISABLED
**Online(1009)	DISABLE_ONLINE
**Offline(1008)	ENABLE_OFFLINE
**Precendence(1010)	1
**Access-Network-Charging-Identifier-Gx	000001f7c0000014000028af3365326633313130
**Flows(510)	-
***Media-Component-Number(518)	16780285
***Flow-Number(518)	33560570

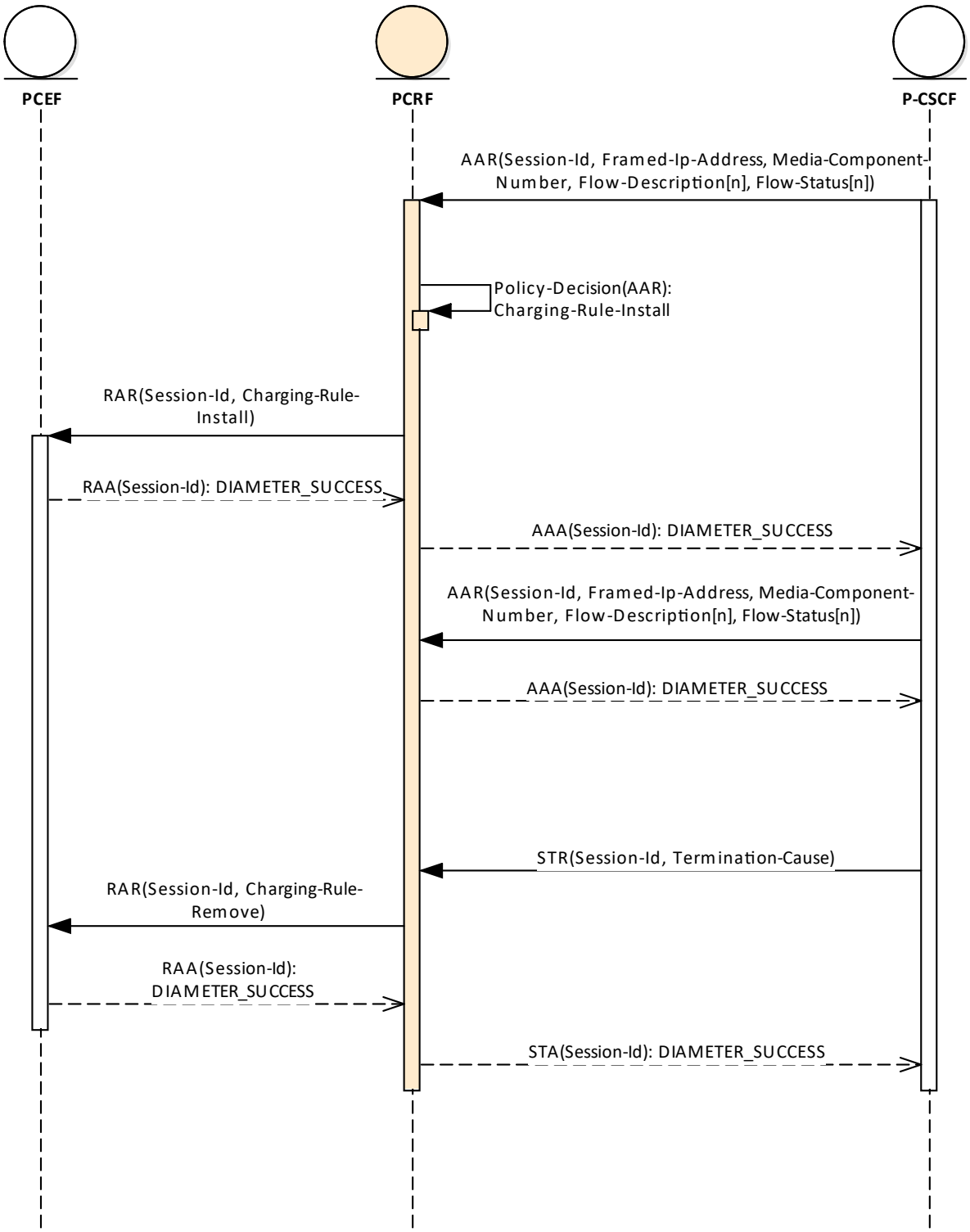
Tabulka 7.7. Obsah odchozí Re-Authorization Request

Attribute-Value Pair	**Hodnota**
Session-Id(263)	gx-session;145020081;11038;0
Auth-Application-Id(258)	16777238
Origin-Host(264)	seagull-Gx
Origin-Realm(296)	diameter_realm
Route-Record(282)	jslee
Origin-State-Id(278)	1024
Result-Code(268)	DIAMETER_SUCCESS
RAT-Type(1032)	EUTRAN
3GPP-User-Location-Info(22)	38323332663031303237...
Access-Network-Charging-Address(501)	10.255.80.123

Tabulka 7.8. Obsah příchozí Re-Authorization Answer

7.3.5 VoLTE hovor

VoLTE hovor je kombinací výše uvedených scénářů a `Authorization-Authentication Request` zprávy od AF(P-CSCF)7.9



Obrázek 7.10. VoLTE hovor.

U zprávy AAR nás především zajímají atributy `Flow-Description`, které se promítnou do zprávy `Re-Authorization Request` a atributů `Flow-Description`, avšak struktura zanoření se na Gx rozhraní liší. Na obrázku 7.10 si lze povšimnout, že v pořadí druhý příchozí `Authorization-Authentication Request` není PCRF vytvořen `Re-Authorization Request` na Gx rozhraním. Důvodem je, že nedochází ke změně PCC pravidla, pouze se mění kodeky.

Attribute-Value Pair	**Hodnota**
Session-Id(263)	rx-session;145020081;11038;0
Auth-Application-Id(258)	16777236
Origin-Host(264)	seagull-Rx
Origin-Realm(296)	diameter_realm
Destination-Realm(283)	diameter_realm
Destination-Host(293)	jslee
Framed-IP-Address(8)	192.168.1.3
AF-Charging-Identifier	000001f7c0000014000028af3365326633313130
Media-Component-Description(517)	-
*Media-Component-Number(518)	704656758
*Media-Sub-Component(519)	-
**Flow-Number(518)	33560570
**Flow-Description(507)	permit in ip from 10.60.90.161 49120 to 10.207.22.210 10062
**Flow-Description(507)	permit in out from 10.207.22.210 10062 to 10.60.90.161 49120
**Flow-Status(511)	ENABLED
*Media-Sub-Component(519)	-
**Flow-Number(518)	33560571
**Flow-Description(507)	permit in ip from 10.60.90.161 49121 to 10.207.22.210 10063
**Flow-Description(507)	permit out from 10.207.22.210 10063 to 10.60.90.161 49121
**Flow-Usage(512)	RTCP
**Flow-Status(511)	ENABLED
*Media-Type(520)	AUDIO
*Max-Requested-Bandwidth-UL(516)	128000
*Max-Requested-Bandwidth-DL(515)	128000
*AF-Application-Identifier(504)	sbc
*Flow-Status(511)	ENABLED
*Codec-Data(524)	downlink\noffer\nm=audio ...
*Codec-Data(524)	uplink\noanswer\nm=audio ...
Specific-Action(513)	INDICATION_OF_LOSS_OF_BEARER

Tabulka 7.9. Obsah příchozí Authorization-Authentication Request

Attribute-Value Pair	Hodnota
Session-Id(263)	rx-session;145020081;11038;0
Auth-Application-Id(258)	16777236
Origin-Host(264)	jslee
Origin-Realm(296)	diameter_realm
Destination-Realm(283)	diameter_realm
Destination-Host(293)	seagull-Rx
Result-Code(268)	DIAMETER_SUCCESS
RAT-Type(1032)	EUTRAN
3GPP-User-Location-Info(22)	38323332663031303237...
Access-Network-Charging-Identifier(502)	000001f7c0000014000028af3365326633313130
Access-Network-Charging-Address(501)	10.255.80.123
IP-CAN-Type(1027)	3GPP-EPS
RAT-Type(1032)	EUTRAN

Tabulka 7.10. Obsah odchozí Authorization-Authentication Answer

Kapitola 8
Závěr

Diplomová práce se zabývá problematikou telekomunikačních aplikací, jejich otevřeným kódem a možným použití v praxi. V úvodu práce vysvětluje motivaci pro zvolení daného tématu. Téma se jeví jako vysoce aktuální díky použití otevřeného kódu v nových souvislostech, totiž v telekomunikacích. V Kapitole 2 je čtenářům přiblížena standardizace, struktura mobilní sítě a signalizace. V signalizaci je kladen detail na Gx rozhraní, kde vznikl přehled verzí a jejich změn, které v dosavadní literatuře chybělo. V Příloze B je obdobně zpracován seznam tzv. AVP atributů nacházejících se ve zprávách Diameter protokolu.

V Kapitole 6 přináší analýzu volně dostupných platforem a specifikací pro vytvoření aplikace, konkrétně byly porovnávány programovací jazyky jako Elixir nebo Erlang, starší specifikace Parlay s JAIN SLEE specifikací a její volně dostupnou implementací v programovacím jazyku Java. Zadáním této práce bylo vytvořit aplikaci zasazenou mezi dvě rozhraní protokolu Diameter – Gx a Rx. Ve standardech je tato aplikace zmiňována jako PCRF[32]. Jako nejvhodnější platforma pro splnění tohoto zadání byl zvolen projekt JAIN SLEE.

Kapitola 7 se soustředí na praktickou implementaci aplikace. Zde se dokonce nabízí uchopit PCRF jako logickou funkci, která jde rozdělit na dva funkční celky. Jeden zaměřený více na PCC pravidla a datové balíčky, a druhý zaměřený na IMS signalizaci pro VoLTE/VoWifi hovory, která je i demonstrována v praktické části. Přínos pro čtenáře může mít samotný návrh a architektura aplikace, kde Diameter rozhraní Sp je napojené na NoSQL databázi Couchbase a žádná jiná práce toto propojení zatím neuvažovala. Dalším zajímavým bodem je novodobé pojetí průběžného testování (angl. Continuous Integration) v diplomové práci, kde je popsáno automatické otestování po nahrání nové verze kódu i automatický způsob vytváření Docker obrazů. Tento princip zaručuje stálé prostředí, které může být nasazeno do živé sítě.

Součástí aplikace je i samostatně vytvořený scénář pro funkční otestování. Scénář je spouštěn aplikací Seagull s opravenou chybou ve stavovém automatu Diameter aplikace. Simulace, databáze a aplikace mají každá separátní Docker obraz, dokonce je jde přizpůsobit i reálným podmínkám, v Dockeru lze vytvořit stejnou síť se stejným testovaným rozsahem IP adres.

Funkční aplikace je demonstrací, že JAIN SLEE je použitelné pro vytváření aplikací pro telekomunikační odvětví. Tento koncept může mobilním operátorům ušetřit náklady, nabízí možnost interního vývoje minimálně všech Diameter aplikací, přitom vědomosti zůstanou uvnitř firmy, nikoliv u dodavatele řešení. Dalším výhodou je, že operátor může pružně reagovat na požadavky ke změnám na aplikaci, čas uvedení nové funkcionality na trh se rapidně snižuje.

JAIN SLEE poskytuje vše potřebné pro vývoj, nasazení a monitoring aplikace. Poslední bod nebyl v této práci obsažen. Nadstavbou této práce může být nastavení a rozšíření monitoringu a vytvoření tzv. Resource Adaptoru pro Couchbase, aktuálně je volán přímo z třídy aplikace.

Hlavním cílem práce bylo vytvořit Diameter aplikaci pro Gx a Rx rozhraní a vedlejším cílem zanalyzovat dostupné platformy, což bylo splněno. Byla zvolena a odůvodněna platforma, navrhnuta architektura, interakce přes rozhraní, testovací scénáře i zrealizována samotná aplikace.

Literatura

[1] Bossche, Van Den, Bruno, De Vleeschauwer, Tom Verdickt, Filip De Turck, Bart Dhoedt a Piet Demeester. *On the use of Java Server Side Technologies for the Design of Dynamically Redeployable MMOGs.* [online]. 1.vyd. Las Vegas, Nevada, USA: CSREA Press, 2006 [cit. 2018-05-14].

[2] Holma, Harri a Antti. Toskala. *LTE for UMTS*. Second Edition vyd. Chichester, West Sussex, United Kingdom: Wiley, 2011. ISBN 978-0-470-66000-3.

[3] Jepsen, Thomas C. a Farooq. Anjum. *Java in telecommunications*. 2nd ed. vyd. New York: Wiley, 2001. ISBN 9780471498261.

[4] Kreher, Ralf a Karsten Gaenger. *LTE signaling, troubleshooting, and optimization*. 3rd ed. vyd. Chichester, West Sussex, UK: Wiley, 2011. ISBN 9780470977729.

[5] Moerdijk, A.-J. a L. Klostermann. Opening the networks with Parlay/OSA standards and aspects behind the APIs. *IEEE Network* [online]. 2003, ročník 17, č. 3, s. 58-64 [cit. 2018-05-19]. ISSN 0890-8044. DOI 10.1109/MNET.2003.1201478. Dostupné z:
`http://ieeexplore.ieee.org/document/1201478/`.

[6] Nakhjiri, Madjid. a Mahsa. Nakhjiri. *AAA and network security for mobile access*. 3rd ed vyd. Hoboken, NJ: John Wiley & Sons, 2005. ISBN 9780470011942.

[7] Noldus, Rogier. *IMS application developer's handbook*. 1.vyd vyd. Amsterdam: Academic Press, 2011. ISBN 978-0-12-382192-8.

[8] Olsson, Magnus, Catherine Mulligan, Shabnam Sultana, Stefan Rommer a Lars Frid. *EPC and 4G packet networks*. Second edition. vyd. Boston: Elsevier/AP, Academic Press is an imprint of Elsevier, 2013. ISBN 9780123945952.

[9] Perez, Andre. *VoLTE and ViLTE*. Hoboken, NJ: Wiley, 2016. ISBN 978-1-84821-923-6.

[10] Tselikas, Nikolaos D., Nikolaos L. Dellas, Eleftherios A. Koutsoloukas, Sofia H. Kapellaki, George N. Prezerakos a Iakovos S. Venieris. Distributed service provision using open APIs-based middleware. *Journal of Systems and Software* [online]. 2007, ročník 80, č. 5, s. 765-777 [cit. 2018-05-19]. ISSN 01641212. DOI 10.1016/j.jss.2006.06.035. Dostupné z:
`http://linkinghub.elsevier.com/retrieve/pii/S0164121206001786`.

[11] Yates, M. J. a I. Boyd. The Parlay network API specification. In: *BT Technology Journal* [online]. 2007 [cit. 2018-05-19]. s. 205-211. ISSN 1358-3948. DOI 10.1007/s10550-007-0076-7. Dostupné z:
`http://link.springer.com/10.1007/s10550-007-0076-7`.

[12] Burcsi, P., A. Kovács a A. Tátrai. Start-phase control of distributed systems written in Erlang/OTP. In: *Acta Univ. Sapientiae, Informatica* [online]. Cluj-Napoca, Romania: Univ. Sapientiae, 2010 [cit. 2018-05-19]. s. 10-27. ISSN 2066-7760.

[13] *TIOBE Index for May 2018.* [online]. Eindhoven, The Netherlands: TIOBE software, 2018 [cit. 2018-05-20]. Dostupné z:
https://www.tiobe.com/tiobe-index/.

[14] *Restcomm Jain-Slee. Github*[online]. Austin, USA: Restcomm, 2018 [cit. 2018-05-20]. Dostupné z:
https://github.com/RestComm/jain-slee.

[15] *OpenCloud Rhino Platform. Rhino Developer Portal*[online]. Enfield, UK: Metaswitch, 2011 [cit. 2018-05-20]. Dostupné z:
https://developer.opencloud.com.

[16] *Mobile data traffic will increase 7-fold from 2016 to 2021, Cisco says. ZDNet*[online]. San Francisco, USA: CBS Interactive, 2017 [cit. 2018-05-22]. Dostupné z:
https://www.zdnet.com/article/mobile-data-traffic-will-increase-7-fold-from-2016-to-2021-cisco-says/.

[17] *Educational Community License. Rhino Developer Portal*[online]. Enfield, UK: Metaswitch, 2011 [cit. 2018-05-20]. Dostupné z:
https://developer.opencloud.com.

[18] *Kubernetes community contribution.. Stackalytics*[online]. OpenStack Foundation, 2018 [cit. 2018-05-22]. Dostupné z:
http://stackalytics.com/?project_type=kubernetes-group&metric=commits.

[19] Loder, Wolfgang. *Erlang and Elixir for imperative programmers*. 1.vyd. vyd. New York, NY: Springer Science Business Media, 2016. ISBN 978-1-4842-2393-2.

[20] *A week with Elixir. Joe Armstrong - Erlang and other stuff* [online]. London: Joe Armstrong, 2013 [cit. 2018-05-20]. Dostupné z:
https://joearms.github.io/published/2013-05-31-a-week-with-elixir.html.

[21] *The SIP Servlet Tutorial.* [online]. Redwood City, California, USA: Oracle Corporation and/or its affiliates, 2010 [cit. 2018-05-17]. Dostupné z:
https://docs.oracle.com/cd/E19355-01/820-3007/gfmqz/index.html.

[22] *JAIN SLEE (JSLEE) 1.1 Specification.* 1.1. Santa Clara, USA: Sun Microsystems„ 2008.

[23] *Developing Portable Applications With JAINSLEE.* Enfield, Spojené království: 2008. Dostupné z:
https://developer.opencloud.com/devportal/download/attachments/13927711/DevelopingPortableApplicationsWithJAINSLEE.pdf.

[24] *LXC Github Projekt.* [online]. San Francisco, Kalifornie, USA: GitHub, Inc., 2008 [cit. 2018-04-09]. Dostupné z:
https://github.com/lxc/lxc.

[25] *Životní cyklus Dockeru. Random Musings*[online]. Random Musings: Random Musings, 2016 [cit. 2018-05-08]. Dostupné z:
https://chengl.com/docker-workflow/.

[26] *About 3GPP. 3GPP Global Iniciative: The Mobile Broadband Standard*[online]. Sophia Antipolis: 3GPP Mobile Competence Centre, 2017 [cit. 2017-10-16]. Dostupné z:
http://www.3gpp.org/about-3gpp/about-3gpp.

[27] *OSA Parlay and Parlay-X. Rhino Developer Portal*[online]. Enfield, UK: Metaswitch, 2011 [cit. 2018-05-20]. Dostupné z:
https://developer.opencloud.com.

[28] *3GPP TS 29.212 V14.6.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC); Reference points (Release 14).* V14.6.0. Valbonne, France: 3GPP, 2017.

[29] *3GPP TS 29.212 V13.11.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC); Reference points (Release 13).* V13.11.0. Valbonne, France: 3GPP, 2017.

[30] *3GPP TS 29.212 V12.13.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC); Reference points (Release 12).* V12.13.0. Valbonne, France: 3GPP, 2016.

[31] *3GPP TS 29.212 V11.18.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC); Reference points (Release 11).* V11.18.0. Valbonne, France: 3GPP, 2016.

[32] *3GPP TS 29.212 V10.17.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC) over Gx reference point (Release 10).* V10.17.0. Valbonne, France: 3GPP, 2016.

[33] *3GPP TS 29.212 V9.19.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC) over Gx reference point (Release 9).* V9.19.0. Valbonne, France: 3GPP, 2014.

[34] *3GPP TS 29.212 V8.24.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC) over Gx reference point (Release 8).* V8.24.0. Valbonne, France: 3GPP, 2014.

[35] *3GPP TS 29.212 V7.16.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7).* V7.16.0. Valbonne, France: 3GPP, 2013.

[36] *3GPP TS 29.214 V10.14.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC) over Rx reference point (Release 10).* V10.14.0. Valbonne, France: 3GPP, 2015.

Příloha A
Zkratky

A.1 Zkratky

3GPP	3rd Generation Partnership Project
4G	Fourth Generation
AF	Application Function
API	Application Programming Interface
APN	Access Point Name
ARP	Allocation And Retention Priority
AuC	Autentication Center
AVP	Attribute Value Pair
BBERF	Bearer Binding and Event Reporting Function
CI	Continuos Intergration
COTS	Commercial Off-The-Shelf
CRM	Customer Relationship Management
CSCF	Call Session Control Function
CT	Core Network and Terminals
eNodeB	Evolved Node B
ePC	Evolved Packet Core
EPS	Evolved Packet System
EUTRAN	Evolved Universal Mobile Telecommunications System
FDD	Frequency-division duplex,
GERAN	GSM EDGE Radio Access Network
GPRS	General Packet Radio Service
GTP	GPRS Tunelling Protocol
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
JAIN	Java API For Integrated Services
MME	Mobility Management Entity
MPS	Multimedia Priority Services
NAS	Non-access Stratum
NBIFOM	Network-Based IP Flow Mobility
NB-IoT	Narrow Band Internet of Things
NGN	Next-generation Network
OCS	Online Charging Systém
OTP	Open Telecom Platform
PCEF	Policy and Charging Enforcement Function

PCRF	Policy and Charging Rules Enforcement Function
PDN	Packet Data Network
P-GW	PDN Gateway
QCI	QoS Class Identifier
QoS	Quality of Service
RA	Resource Adaptor
RAN	Radio Access Network
SA	Service and Systems Aspects
SBB	Service Building Block
SCTP	Stream Control Transmission Protocol
S-GW	Serving Gateway
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SPR	Subscriber Profile Repository
TAU	Tracking Area Update
TCP	Transmission Control Protocol
TDD	Time-division duplex
TDF	Traffic Detection Function
TEID	Tunnel Endpoint Identifier
TSSF	Traffic Steering Support Function
ViLTE	Video Over LTE
VoLTE	Voice Over LTE
VoWifi	Voice Over Wifi
WLAN	Wireless Local Area Network
xDCR	Cross Datacenter Replication
xDSL	Digital Subscriber Line
XML	Extensible Markup Language

Příloha B
Přílohy

B.1 Attribute-Value-Pair pro Gx rozhraní (7-14. vydání specifikace)

Attribute Name	AVP Code	Clause defined	Value Type (NOTE 2)	AVP Flag rules (NOTE 1)					Acc. Type	Release
				Must	May	Should not	Must not	May Encr.		
3GPP-PS-Data-Off-Status	2847	5.3.133	Enumerated	V	P		M	Y	3GPP-EPS	Rel.14
Access-Availability-Change-Reason	2833	5.3.121	Unsigned32	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS (NOTE 11)	Rel.13
Access-Network-Charging-Identifier-Gx	1022	5.3.22	Grouped	M,V	P			Y	All	Rel.7
Allocation-Retention-Priority	1034	5.3.32	Grouped	V	P		M	Y	All	Rel.8
AN-GW-Address	1050	5.3.49	Address	V	P		M	Y	All	Rel.8
AN-GW-Status	2811	5.3.100	Enumerated	V	P		M	Y	3GPP-EPS	Rel.11
APN-Aggregate-Max-Bitrate-DL	1040	5.3.39	Unsigned32	V	P		M	Y	All	Rel.8
APN-Aggregate-Max-Bitrate-UL	1041	5.3.40	Unsigned32	V	P		M	Y	All	Rel.8
Application-Detection-Information	1098	5.3.91	Grouped	V	P		M	Y	All	Rel.11
Bearer-Control-Mode	1023	5.3.23	Enumerated	M,V	P			Y	3GPP-GPRS 3GPP-EPS 3GPP2 Non-3GPP-EPS (NOTE 6)	Rel.7
Bearer-Identifier	1020	5.3.20	OctetString	M,V	P			Y	3GPP-GPRS	Rel.7
Bearer-Operation	1021	5.3.21	Enumerated	M,V	P			Y	3GPP-GPRS	Rel.7
Bearer-Usage	1000	5.3.1	Enumerated	M,V	P			Y	3GPP-GPRS 3GPP-EPS	Rel.7
Charging-Correlation-Indicator	1073	5.3.67	Enumerated	V	P		M	Y	All	
Charging-Rule-Base-Name	1004	5.3.5	UTF8String	M,V	P			Y	All	Rel.7
Charging-Rule-Definition	1003	5.3.4	Grouped	M,V	P			Y	All	Rel.7
Charging-Rule-Install	1001	5.3.2	Grouped	M,V	P			Y	All	Rel.7
Charging-Rule-Name	1005	5.3.6	OctetString	M,V	P			Y	All	Rel.7
Charging-Rule-Remove	1002	5.3.3	Grouped	M,V	P			Y	All	Rel.7
Charging-Rule-Report	1018	5.3.18	Grouped	M,V	P			Y	All	Rel.7
CoA-Information	1039	5.3.37	Grouped	V	P		M	Y	All (NOTE 8)	Rel.8
CoA-IP-Address	1035	5.3.33	Address	V	P		M	Y	All (NOTE 8)	Rel.8
Conditional-APN-Aggregate-Max-Bitrate	2818	5.3.105	Grouped	V	P		M	Y	All (NOTE 5)	Rel.12
Conditional-Policy-Information	2840	5.3.128	Grouped	V	P		M	Y	All	Rel.13
Credit-Management-Status	1082	5.3.102	Unsigned32	V	P		M	Y	All	Rel.12
CSG-Information-Reporting	1071	5.3.64	Enumerated	V	P		M	Y	3GPP-GPRS 3GPP-EPS	Rel.9
Default-Access	2829	5.3.120	Enumerated	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS (NOTE 11)	Rel.13
Default-Bearer-Indication	2844	5.3.132	Enumerated	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS	Rel.14
Default-EPS-Bearer-QoS	1049	5.3.48	Grouped	V	P		M	Y	All (NOTE 5)	Rel.8
Default-QoS-Information	2816	5.3.103	Grouped	V	P		M	Y	FBA	Rel.12

Default-QoS-Name	2817	5.3.104	UTF8String	V	P		M	Y	FBA	Rel.12
Event-Report-Indication	1033	5.3.30	Grouped	V	P		M	Y	All	Rel.8
Event-Trigger	1006	5.3.7	Enumerated	M,V	P			Y	All	Rel.7
Execution-Time	2839	5.3.127	Time	V	P		M	Y	All	Rel.13
Flow-Direction	1080	5.3.65	Enumerated	V	P		M	Y	All	Rel.7
Flow-Information	1058	5.3.53	Grouped	V	P		M	Y	All	Rel.7
Flow-Label	1057	5.3.52	OctetString	V	P		M	Y	All	Rel.7
Fixed-User-Location-Info	2825	5.3.112	Grouped	V	P		M	Y	FBA	
Guaranteed-Bitrate-DL	1025	5.3.25	Unsigned32	M,V	P			Y	All	Rel.7
Guaranteed-Bitrate-UL	1026	5.3.26	Unsigned32	M,V	P			Y	All	Rel.7
HeNB-Local-IP-Address	2804	5.3.95	Address	V	P		M	Y	3GPP-EPS	Rel.11
IP-CAN-Session-Charging-Scope	2827	5.3.114	Enumerated	V	P		M	Y	All	Rel.12
IP-CAN-Type	1027	5.3.27	Enumerated	M,V	P			Y	All	Rel.7
Metering-Method	1007	5.3.8	Enumerated	M,V	P			Y	All	Rel.7
Monitoring-Flags	2828	5.3.115	Unsigned32	V			M	Y	All	Rel.13
Monitoring-Key	1066	5.3.59	OctetString	V	P		M	Y	All	Rel.9
Mute-Notification	2809	5.3.98	Enumerated	V	P		M	Y	All	Rel.11
Monitoring-Time	2810	5.3.99	Time	V	P		M	Y	All	Rel.11
NBIFOM-Mode	2830	5.3.117	Enumerated	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS (NOTE 11)	Rel.13
NBIFOM-Support	2831	5.3.116	Enumerated	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS (NOTE 11)	Rel.13
NetLoc-Access-Support	2824	5.3.111	Unsigned32	V	P		M	Y	All	Rel.11
Network-Request-Support	1024	5.3.24	Enumerated	M,V	P			Y	3GPP-GPRS 3GPP-EPS 3GPP2 Non-3GPP-EPS (NOTE 6)	Rel.7
Offline	1008	5.3.9	Enumerated	M,V	P			Y	All	Rel.7
Online	1009	5.3.10	Enumerated	M,V	P			Y	All	Rel.7
Packet-Filter-Content	1059	5.3.54	IPFilterRule	V	P		M	Y	All (NOTE 5)	Rel.8
Packet-Filter-Identifier	1060	5.3.55	OctetString	V	P		M	Y	All (NOTE 5)	Rel.8
Packet-Filter-Information	1061	5.3.56	Grouped	V	P		M	Y	All (NOTE 5)	Rel.8
Packet-Filter-Operation	1062	5.3.57	Enumerated	V	P		M	Y	All (NOTE 5)	Rel.8
Packet-Filter-Usage	1072	5.3.66	Enumerated	V	P		M	Y	All	Rel.9
PCC-Rule-Status	1019	5.3.19	Enumerated	M,V	P			Y	All	Rel.7
PDN-Connection-ID	1065	5.3.58	OctetString	V	P			Y	All (NOTE 7)	Rel.9
PRA-Install	2845	5.3.130	Grouped	V	P		M		3GPP-EPS	Rel.14
PRA-Remove	2846	5.3.131	Grouped	V	P		M		3GPP-EPS	Rel.14
Precedence	1010	5.3.11	Unsigned32	M,V	P			Y	All	Rel.7

Pre-emption-Capability	1047	5.3.46	Enumerated	V	P		M	Y	3GPP- EPS, 3GPP-GPRS	Rel.8
Pre-emption-Vulnerability	1048	5.3.47	Enumerated	V	P		M	Y	3GPP- EPS, 3GPP-GPRS	Rel.8
Presence-Reporting-Area-Elements-List	2820	5.3.107	OctetString	V	P		M	Y	3GPP-EPS	Rel.12
Presence-Reporting-Area-Identifier	2821	5.3.108	OctetString	V	P		M	Y	3GPP-EPS	Rel.12
Presence-Reporting-Area-Information	2822	5.3.109	Grouped	V	P		M	Y	3GPP-EPS	Rel.12
Presence-Reporting-Area-Status	2823	5.3.110	Unsigned32	V	P		M	Y	3GPP-EPS	Rel.12
Priority-Level	1046	5.3.45	Unsigned32	V	P		M	Y	All	Rel.8
PS-to-CS-Session-Continuity	1099	5.3.84	Enumerated	V	P			Y	3GPP-EPS	Rel.12
QoS-Class-Identifier	1028	5.3.17	Enumerated	M,V	P			Y	All (Note 10)	Rel.7
QoS-Information	1016	5.3.16	Grouped	M.V	P			Y	All	Rel.7
QoS-Negotiation	1029	5.3.28	Enumerated	M,V	P			Y	3GPP-GPRS	Rel.7
QoS-Upgrade	1030	5.3.29	Enumerated	M.V	P			Y	3GPP-GPRS	Rel.7
RAN-NAS-Release-Cause	2819	5.3.106	OctetString	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS	Rel.12
RAN-Rule-Support	2832	5.3.122	Unsigned32	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS (NOTE 11)	Rel.13
RAT-Type	1032	5.3.31	Enumerated	V	P		M	Y	All (NOTE 4)	Rel.8
Redirect-Information	1085	5.3.82	Grouped	V	P		M	Y	All	Rel.11
Redirect-Support	1086	5.3.83	Enumerated	V	P		M	Y	All	Rel.11
Removal-Of-Access	2842	5.3.126	Enumerated	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS (NOTE 11)	Rel.13
Reporting-Level	1011	5.3.12	Enumerated	M,V	P			Y	All	Rel.7
Resource-Allocation-Notification	1063	5.3.50	Enumerated	V	P		M	Y	All	Rel.8
Resource-Release-Notification	2841	5.3.125	Enumerated	V	P		M	Y	All	Rel.13
Revalidation-Time	1042	5.3.41	Time	M,V	P			Y	All	Rel.7
Routing-Filter	1078	5.3.72	Grouped	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS	Rel.10
Routing-IP-Address	1079	5.3.73	Address	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS	Rel.10
Routing-Rule-Definition	1076	5.3.70	Grouped	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS	Rel.10
Routing-Rule-Identifier	1077	5.3.71	OctetString	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS	Rel.10
Routing-Rule-Install	1081	5.3.68	Grouped	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS	Rel.10
Routing-Rule-Remove	1075	5.3.69	Grouped	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS	Rel.10

Routing-Rule-Failure-Code	2834	5.3.119	Unsigned32	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS (NOTE 11)	Rel.13
Routing-Rule-Report	2835	5.3.118	Grouped	V	P		M	Y	3GPP-EPS, Non-3GPP-EPS (NOTE 11)	Rel.13
Rule-Activation-Time	1043	5.3.42	Time	M,V	P			Y	All	Rel.7
Rule-Deactivation-Time	1044	5.3.43	Time	M,V	P			Y	All	Rel.7
Rule-Failure-Code	1031	5.3.38	Enumerated	M.V	P			Y	All	Rel.7
Security-Parameter-Index	1056	5.3.51	OctetString	V	P		M	Y	All	Rel.7
Session-Release-Cause	1045	5.3.44	Enumerated	M,V	P			Y	All	Rel.7
TCP-Source-Port	2843	5.3.129	Unsigned32	V	P		M	Y	Non-3GPP-EPS	Rel.13
TDF-Information	1087	5.3.78	Grouped	V	P		M	Y	All	Rel.11
TDF-Application-Identifier	1088	5.3.77	OctetString	V	P		M	Y	All	Rel.11
TDF-Application-Instance-Identifier	2802	5.3.92	OctetString	V	P		M	Y	All	Rel.11
TDF-Destination-Host	1089	5.3.80	DiameterIdentity	V	P		M	Y	All	Rel.11
TDF-Destination-Realm	1090	5.3.79	DiameterIdentity	V	P		M	Y	All	Rel.11
TDF-IP-Address	1091	5.3.81	Address	V	P		M	Y	All	Rel.11
TFT-Filter	1012	5.3.13	IPFilterRule	M,V	P			Y	3GPP-GPRS	Rel.7
TFT-Packet-Filter-Information	1013	5.3.14	Grouped	M,V	P			Y	3GPP-GPRS	Rel.7
Traffic-Steering-Policy-Identifier-DL	2836	5.3.123	OctetString	V	P		M	Y	All	Rel.13
Traffic-Steering-Policy-Identifier-UL	2837	5.3.124	OctetString	V	P		M	Y	All	Rel.13
ToS-Traffic-Class	1014	5.3.15	OctetString	M,V	P			Y	All	Rel.7
Tunnel-Header-Filter	1036	5.3.34	IPFilterRule	V	P		M	Y	All (NOTE 8)	Rel.8
Tunnel-Header-Length	1037	5.3.35	Unsigned32	V	P		M	Y	All (NOTE 8)	Rel.8
Tunnel-Information	1038	5.3.36	Grouped	V	P		M	Y	All (NOTE 8)	Rel.8
UDP-Source-Port	2806	5.3.97	Unsigned32	V	P		M	Y	3GPP-EPS Non-3GPP-EPS	Rel.11
UE-Local-IP-Address	2805	5.3.96	Address	V	P		M	Y	Non-3GPP-EPS	Rel.11
Usage-Monitoring-Information	1067	5.3.60	Grouped	V	P		M	Y	All	Rel.9
Usage-Monitoring-Level	1068	5.3.61	Enumarated	V	P		M	Y	All	Rel.9
Usage-Monitoring-Report	1069	5.3.62	Enumerated	V	P		M	Y	All	Rel.9
Usage-Monitoring-Support	1070	5.3.63	Enumerated	V	P		M	Y	All	Rel.9
User-Location-Info-Time	2812	5.3.101	Time	V	P		M	Y	3GPP-GPRS. 3GPP-EPS	Rel.11
PCSCF-Restoration-Indication	2826	5.3.113	Unsigned32	V	P		M	Y	All	Rel.12

NOTE 1:	The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 6733 [61].
NOTE 2:	The value types are defined in IETF RFC 6733 [61].
NOTE 3:	AVPs marked with "CC" are applicable to charging control, AVPs marked with "PC" are applicable to policy control and AVPs marked with "Both" are applicable to both charging control and policy control. AVPs marked with "ADC" are applicable to application detection and control. AVPs marked with "ABC" are applicable to application based charging.
NOTE 4:	RAT-Type AVP applies to 3GPP, Non-3GPP-EPS, and 3GPP2 access types.
NOTE 5:	This AVP does not apply to 3GPP-GPRS access type.
NOTE 6:	The 3GPP2 usage is defined in 3GPP2 X.S0062 [30]. Non-3GPP-EPS usage applies to GTP based S2b,
NOTE 7:	This AVP only applies to case 2b as defined in 3GPP TS 29.213 [8].
NOTE 8:	This AVP only applies to case 2a as defined in 3GPP TS 29.213 [8].
NOTE 9:	AVPs marked with a supported feature (e.g. "Rel8", "Rel9", "IFOM" or "EPC-routed") are applicable as described in subclause 5.4.1.
NOTE 10:	The MissionCriticalQCIs supported feature indicates support for the Mission Critical QCI values 65, 69 and 70, and the Non Mission Critical QCI value 66 within the QoS-Class-Identifier AVP defined in subclause 5.3.17.
NOTE 11:	RAT type of Non-3GPP-EPS only applies to WLAN & VIRTUAL.

Obrázek B.1. Porovnání Diameter atributů v jednotlivých specifikacích, zdroj [28]