

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

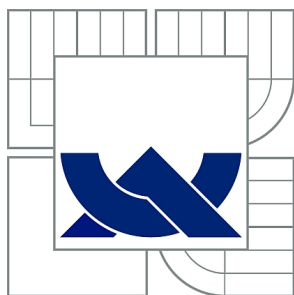
ANALÝZA UŽIVATELSKÉHO PROVOZU V MOBILNÍCH SÍTÍCH 4.
GENERACE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

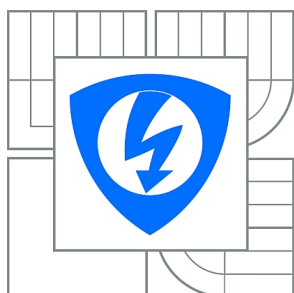
AUTOR PRÁCE
AUTHOR

MICHAL DUDA

BRNO 2014



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**

ANALÝZA UŽIVATELSKÉHO PROVOZU V MOBILNÍCH SÍTÍCH 4. GENERACE

USER PLANE ANALYSIS IN 4G MOBILE NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

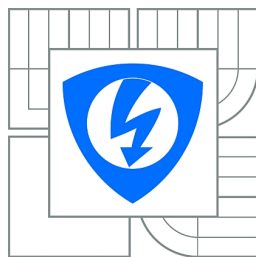
AUTOR PRÁCE
AUTHOR

MICHAL DUDA

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. VÍT NOVOTNÝ, Ph.D.

BRNO 2014



**VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ**

**Fakulta elektrotechniky
a komunikačních technologií**

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Michal Duda

ID: 146812

Ročník: 3

Akademický rok: 2013/2014

NÁZEV TÉMATU:

Analýza uživatelského provozu v mobilních sítích 4. generace

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou mobilních sítí LTE-EPC. Zaměřte se především na uživatelskou rovinu a její protokolovou výstavbu. Prostudujte základní procedury týkající se realizace běžných služeb realizovaných v současnosti uživateli v mobilní síti, jako jsou prohlížení webových stránek, stahování souborů, přístup k elektronické poště, sledování streamovaného videa či poslouchání audia. Prostudujte možné chybové situace, které mohou při realizaci služeb nastat a rozdělte je na příčiny způsobené vlastní mobilní sítí a příčiny mimo ni a posuďte, jak lze příčinu chyby lokalizovat z hlediska původu. Navrhněte sadu výkonnostních indikátorů hodnotících po kvalitativní stránce mobilní síť z hlediska realizovaných služeb, po konzultaci se školitelem vyberte některé z nich, sestavte vztahy pro jejich výpočet a navrhněte vhodné způsoby zjištění potřebných parametrů pro jejich výpočet, realizujte analýzu vzorku datového provozu a výsledky zhodnoťte.

DOPORUČENÁ LITERATURA:

- [1] GUNNAR H. SAE / EPC from A-Z. Inacon, ISBN 978-3-936273-59-5, Germany, 2011
- [2] LESCUYER, P., LUCIDARME, T. Evolved Packet System: The LTE and SAE Evolution of 3G UMTS. John Wiley & Sons, ISBN: 978-0-470-05976-0, GB, 2008

Termín zadání: 10.2.2014

Termín odevzdání: 4.6.2014

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.

Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Cieľom práce je problematika mobilných sietí LTE-EPC. Dočítať sa môžete predovšetkým o užívateľskej rovine a jej protokolovej výbave. Sú tu opísané základné procedúry týkajúce sa realizácie bežných služieb realizovaných v súčasnosti užívateľmi v mobilných sieťach, ako sú prehliadanie webových stránok, sťahovanie súborov, prístup k elektronickej pošte či sledovanie streamovaného videa. Ďalej sa môžete dočítať o navrhutej sade výkonnostných indikátorov hodnotiacich po kvalitatívnej stránke mobilnú sieť z hľadiska realizovaných služieb, o vzťahoch pre ich výpočet a vhodných spôsoboch zistenia potrebných parametrov pre ich výpočet. Nakoniec sa môžete dočítať o spôsobe, akým sa poskytnutá vzorka dát zo siete LTE analyzovala a následne vyhodnotila.

KĽÚČOVÉ SLOVÁ

LTE, E-UTRAN, EPC, bearer, QoS, MBMS, KPI

ABSTRACT

The aim of the work is the mobile network LTE-EPC. You can read all about user plane and its protocol feature. This work describes procedures relating to the implementation of current services performed in the present by users in mobile networks, such as web browsing, file downloading, accessing email or watching streaming video. Furthermore, you can read about the proposed set of performance indicators for evaluation after qualitatively mobile network in terms of implemented services on the relations of their calculation and the appropriate way to identify the necessary parameters for the calculation. Finally, you can read about the method in which have been given sample of data from the LTE network analyzed and evaluate.

KEYWORDS

LTE, E-UTRAN, EPC, bearer, QoS, MBMS, KPI

DUDA, Michal *Analýza užívateľského toku v mobilných sieťach 4. generácie*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačných technológií, Ústav telekomunikací, 2014. 69 s. Vedúci práce bol doc. Ing. Vít Novotný, Ph.D.

PREHLÁSENIE

Prehlasujem, že som svoju bakalársku prácu na tému „Analýza užívateľského toku v mobilných sieťach 4. generácie“ vypracoval samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/nebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o právu autorskom, o právach súvisejúcich s právom autorským a o zmene niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávných dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno

.....

(podpis autora)

POĎAKOVANIE

Rád bych poděkoval vedoucímu diplomové práce panu doc. Ing. Vít Novotný Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno

.....

(podpis autora)

POĎAKOVANIE

Výzkum popsáný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno

.....
(podpis autora)

OBSAH

Úvod	11
1 Systém LTE	12
1.1 Architektúra LTE	12
1.1.1 E-UTRAN architektúra	12
1.1.2 EPC architektúra	13
2 Užívateľská rovina	16
2.1 Architektúra užívateľskej roviny v E-UTRAN	16
2.2 Architektúra užívateľskej roviny v EPC	17
2.2.1 GTP tunelovanie dát	17
3 Realizácia mobilných služieb	20
3.1 Quality of Service	20
3.1.1 Typy bearerov a ich vlastnosti	20
3.2 Prehliadanie webových stránok	24
3.3 Prezeranie elektronickej pošty	27
3.4 Sťahovanie súboru	29
3.5 Sledovanie mobilnej televízie	31
3.5.1 Architektúra služby	31
3.5.2 Pribeh sledovania mobilnej televízie	33
4 Kvalita realizovaných služieb	37
4.1 Meranie kvality služieb	37
4.2 Kľúčové indikátory výkonnosti (KPI)	37
4.2.1 Úspešnosť vytvorenia E-RAB	38
4.3 FTP	38
4.3.1 Miera zlyhania prístupu k FTP službe	39
4.3.2 Čas vytvorenia IP služby FTP	39
4.3.3 Čas FTP relácie	40
4.3.4 Miera zlyhania FTP relácie	40
4.3.5 Miera prerušenia prenosu dát	41
4.3.6 Priemerná rýchlosť sťahovania/nahrávania dát	41
4.4 HTTP/HTTPS	41
4.4.1 Miera zlyhania prístupu k HTTP/HTTPS službe	42
4.4.2 Čas vytvorenia služby HTTP/HTTPS	42
4.4.3 Čas HTTP/HTTPS relácie	43
4.4.4 Miera zlyhania HTTP/HTTPS relácie	43

4.4.5	Miera prerušenia prenosu dát	44
4.4.6	Miera zlyhania vytvorenia TCP/IP spojenia so serverom . . .	44
5	Analýza dátovej komunikácie	45
5.1	Chybové stavy	46
6	Vyhodnotenie dátovej komunikácie	48
6.0.1	Úspešnosť vytvorenia E-RAB	48
6.1	HTTP	48
6.1.1	Čas vytvorenia IP služby HTTP	48
6.1.2	Čas HTTP relácie	50
6.1.3	Miera zlyhania prístupu k HTTP službe	50
6.1.4	Miera zlyhania HTTP relácie	52
6.1.5	Miera prerušenia prenosu dát	52
6.1.6	Množstvo vyslaných HTTP žiadostí a odpovedí	53
6.1.7	Množstvo opakovaných dát	54
6.2	Vyhodnotenie HTTP komunikácie	54
6.3	HTTPS	55
6.3.1	Čas vytvorenia IP služby HTTPS	55
6.3.2	Čas HTTPS relácie	57
6.3.3	Miera zlyhania prístupu k HTTPS službe	57
6.3.4	Miera zlyhania HTTPS relácie	59
6.3.5	Miera prerušenia prenosu dát	59
6.3.6	Množstvo opakovaných dát	60
6.4	Vyhodnotenie HTTPS komunikácie	60
7	Záver	62
	Literatúra	63
	Zoznam skratiek	65
	Zoznam príloh	68
A	Obsah CD	69

ZOZNAM OBRÁZKOV

1.1	Architektúra EPS	12
1.2	Vývoj architektúry UTRAN do E-UTRAN	13
1.3	Vývoj jadra EPS	13
1.4	Architektúra zariadení v EPC	14
1.5	Prepojenie EPC s inými 3GPP a nie-3GPP technológiami	15
2.1	Protokolová výbava užívateľskej roviny v E-UTRAN	16
2.2	Protokolová výbava užívateľskej roviny v EPS	17
2.3	Použitie GTP tunela v prípade pohybu používateľa	18
2.4	Efekt GTP tunelovania (s použitím IPv4 pre GTP transport)	19
3.1	EPS bearer a jeho časti	20
3.2	Typy bearerov a ich vlastnosti [8]	21
3.3	Defaultný bearer pre 2 služby	21
3.4	Defaultný bearer pre služby s garantovanou a negarantovanou prenosovou rýchlosťou	22
3.5	Diagram vytvorenia defaultného EPS bearera	25
3.6	Priebeh odoslania HTTP requestu a následné prijatie HTTP response	26
3.7	Priebeh odoslania POP3 Retrieve správy a následné prijatie e-mailu	28
3.8	Otvorenie TCP spojenia používateľom a prenos súboru od FTP serveru	30
3.9	Logická architektúra MBMS služby	32
3.10	Architektúra užívateľskej roviny MBMS služby	33
3.11	Paket smerujúci od BM-SC k MBMS GW a paket smerujúci od MBMS GW k eNodeB	35
3.12	Streamovanie televízneho kanálu	36
5.1	Port mirroring.	45
5.2	Filtrovanie HTTP komunikácie a protokolu slap.	45
5.3	Grafické rozhranie programu.	46
6.1	Histogram časových úsekov vytvorenia služby HTTP	49
6.2	Histogram časových úsekov HTTP relácie.	51
6.3	Graf HTTP žiadostí podľa typov.	53
6.4	Graf HTTP odpovedí podľa typov.	53
6.5	Graf pomeru opakovaných a všetkých HTTP dát.	54
6.6	Histogram časových úsekov vytvorenia služby HTTPS	56
6.7	Histogram časových úsekov HTTPS relácie.	58
6.8	Graf pomeru opakovaných a všetkých HTTPS dát.	60

ZOZNAM TABULIEK

3.1	Úrovne QCI a vlastnosti paketov	24
4.1	Body pre zachytenie dát na výpočet úspešnosti vytvorenia E-RAB. . .	38
4.2	Body pre zachytenie dát na výpočet miery zlyhania prístupu k FTP službe.	39
4.3	Body pre zachytenie dát na výpočet času vytvorenia služby FTP. . .	39
4.4	Body pre zachytenie dát na výpočet času FTP relácie.	40
4.5	Body pre zachytenie dát na výpočet miery zlyhania FTP relácie. . . .	40
4.6	Body pre zachytenie dát na výpočet miery prerušenia prenosu dát. . .	41
4.7	Body pre zachytenie dát na výpočet miery zlyhania prístupu k službe.	42
4.8	Body pre zachytenie dát na výpočet času vytvorenia služby.	42
4.9	Body pre zachytenie dát na výpočet času HTTP/HTTPS relácie. . .	43
4.10	Body pre zachytenie dát na výpočet miery zlyhania relácie.	43
4.11	Body pre zachytenie dát na výpočet miery prerušenia prenosu dát. . .	44
4.12	Body pre zachytenie dát na výpočet miery zlyhania vytvorenia spojenia.	44

ÚVOD

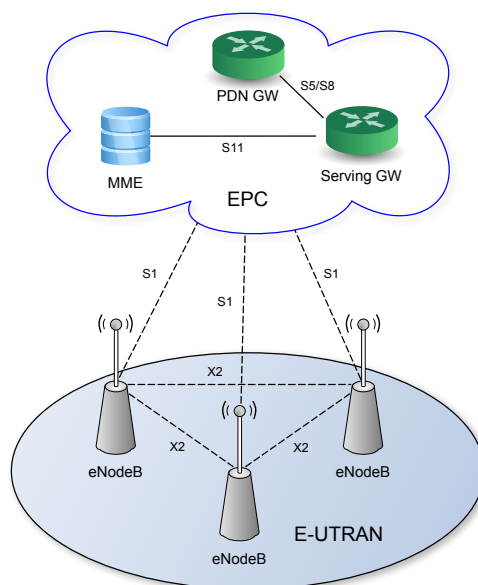
Táto práca sa venuje mobilnej sieti LTE (Long Term Evolution). Zameriava sa na užívateľskú rovinu a jej protokolovú výbavu. Sú tu popísané základné procedúry, týkajúce sa realizácie bežných služieb realizovaných používateľmi mobilných sietí LTE, ako sú prehliadanie webových stránok, prístup k elektronickej pošte, sťahovanie súborov či sledovanie streamovaného videa. Môžete sa dočítať o navrhnutej sade kľúčových indikátorov výkonnosti a vzťahoch pre ich výpočet, ktoré hodnotia sieť z hľadiska realizovaných služieb. Nakoniec sa dočítate o spôsobe, akým sa poskytnutá vzorka dát zo siete analyzovala a následne vyhodnotila.

1 SYSTÉM LTE

Long Term Evolution (LTE) je štandard pre vysokorýchlostnú bezdrôtovú komunikáciu mobilných zariadení a terminálov. Je založená na sieťových technológiach GSM/EDGE a UMTS/HSxPA, zvyšuje kapacitu a rýchlosť prenosu informácií používaním rozdielnych rádiových rozhraní súčasne spolu s vylepšeniami jadra siete. Tento štandard bol vytvorený spoločnosťou 3GPP.

1.1 Architektúra LTE

LTE (EPS) je vyvinutý paketový systém, ktorý sa delí na prístupovú časť E-UTRAN a riadiacu časť Evolved packet core (EPC). Architektúra Evolved Packet System (EPS) je zobrazená na obrázku 1.1.

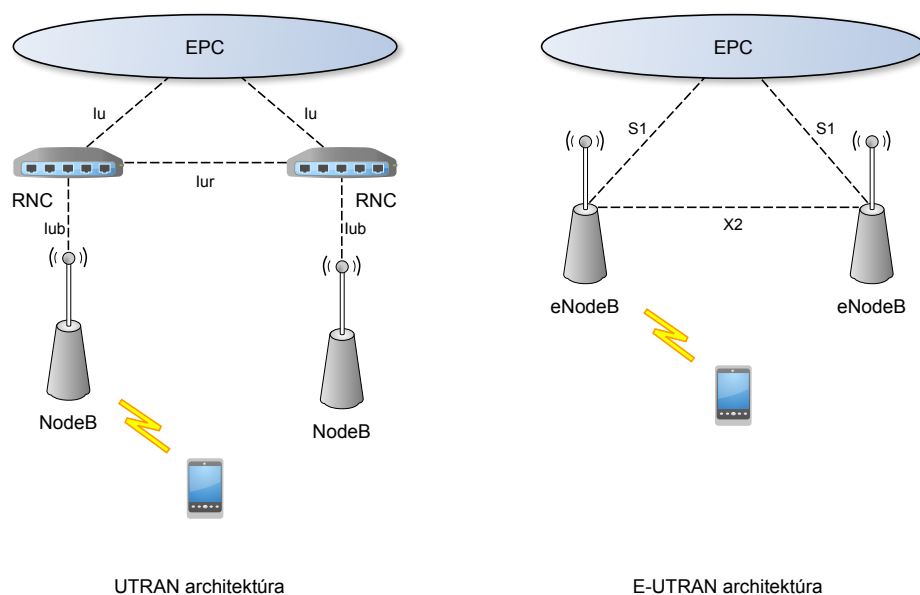


Obr. 1.1: Architektúra EPS

1.1.1 E-UTRAN architektúra

Architektúra E-UTRANu je oproti architektúre UTRANu pomerne jednoduchá. Tvorí ju iba jeden prvok eNodeB. Tento prvok je priamo pripojený cez rozhranie S1 do smerovačov v EPC. Nové rozhranie X2 bolo definované medzi jednotlivými eNodeB. Hlavným významom tohto rozhrania je minimalizovať stratu paketov, spôsobenú mobilitou používateľov. Pohybom používateľa sieťou sa teda môžu neposlané a nepotvrdené pakety uchovať v starom eNodeB, a cez rozhranie X2 môžu byť

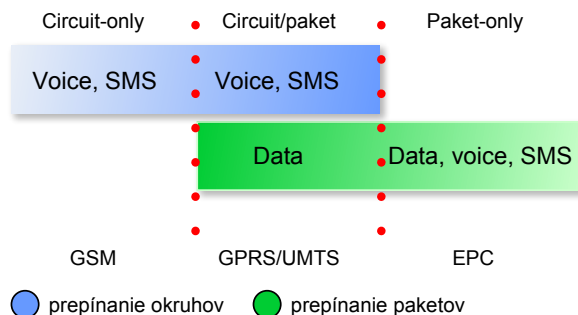
tieto pakety prenesené do nového eNodeB. Zjednodušená architektúra E-UTRANu a UTRANu je znázornená na obrázku 1.2.



Obr. 1.2: Vývoj architektúry UTRAN do E-UTRAN

1.1.2 EPC architektúra

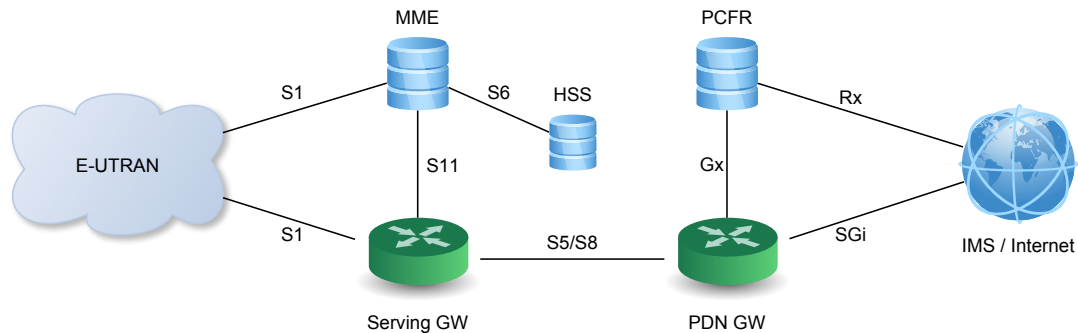
EPC je posledný vývojový stupeň jadra sieťovej architektúry 3GPP. Keďže internetový protokol (IP) sa stal hlavným protokolom pre transport všetkých služieb, EPC využíva iba technológiu prepínania paketov. Vývoj tejto architektúry je znázornený na obrázku 1.3.



Obr. 1.3: Vývoj jadra EPS

Architektúra EPC pozostáva z týchto prvkov:

- MME
- Home Subscriber Server
- Serving Gateway
- Policy Control and Charging Rules Function
- Packet Data Network Gateway



Obr. 1.4: Architektúra zariadení v EPC

Mobility Management Entity (MME)

MME sa zaoberá riadiacou rovinou. Stará sa o signalizáciu, vzťahujúcu sa k mobilite a bezpečnosti prístupu k E-UTRAN.

Home Subscriber Server (HSS)

V podstate je to databáza, ktorá uchováva informácie týkajúce sa používateľov a predplatiteľov. Poskytuje podporu mobilných funkcií ako napr. autentizácia používateľa a autorizácia prístupu.

Serving Gateway

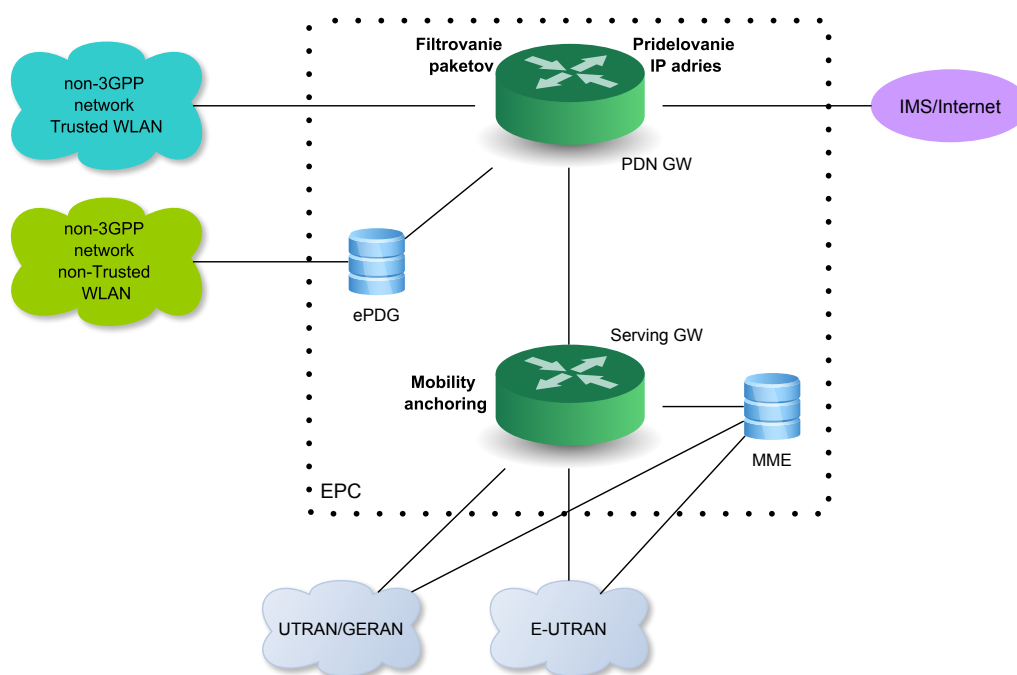
Serving GW prenáša IP dáta smerujúce od používateľa do externých sietí. Pôsobí ako vstupný bod pre používateľské dáta, smerujúce do internetu a zároveň plní úlohu spojujúceho bodu medzi LTE a ostatnými technológiami 3GPP ako GPRS a UMTS. Dočasne uchováva dáta, pokiaľ nie je žiadny rádiový bearer dostupný a používateľ je neaktívny. Tiež uchováva používateľské dáta, kvôli ich duplikácii pre prípad zákonného odpočúvania.

Policy Control and Charging Rules Function (PCRF)

PCRF je zodpovedný za politiku kontroly rozhodovania a za kontrolovanie funkcionality účtovania na základe toku dát v Policy Control Enforcement Function (PCEF). PCRF poskytuje QoS autorizáciu, ktorá rozhoduje, ako sa bude zaobchádzať s určitým dátovým tokom v PCEF a ubezpečuje sa, že je to v súlade s používateľským predplateným profilom.[10]

Packet Data Network Gateway (PDN GW)

PDN GW je zodpovedný za pridelenie IP adres pripojeným užívateľom a za presadzovanie QoS. PDN GW slúži ako koncový bod paketových dát, vedených do rozhrania externých paketových dátových sietí. Jeho úlohou je filtrácia používateľských IP paketov do rozdielnych QoS bearerov. Taktiež slúži ako vstupný bod pre spoluprácu s ostatnými technológiami, ako napr. WiMAX. Jeho súčasťou je PCEF, ktorého úlohou je kontrola používateľských dát, detekcia používanej služby a počítanie veľkosti prenesených a prijatých dát pre každého pripojeného používateľa. PCEF prepustí ďalej iba dátové služby, ktoré zodpovedajú aktívnym pravidlám prijatých od PCRF.[4]



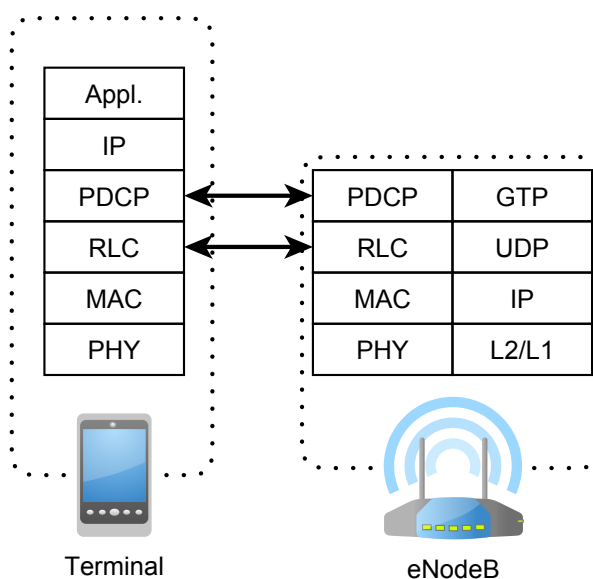
Obr. 1.5: Prepojenie EPC s inými 3GPP a nie-3GPP technológiami

2 UŽÍVATEĽSKÁ ROVINA

Táto kapitola popisuje celkovú end-to-end protokolovú štruktúru užívateľskej roviny EPS, ktorá je zodpovedná za prenos používateľských dát.

2.1 Architektúra užívateľskej roviny v E-UTRAN

Protokolová výbava užívateľskej roviny od terminálu k eNodeB je zobrazená na obrázku 2.1.



Obr. 2.1: Protokolová výbava užívateľskej roviny v E-UTRAN

- **PDCP vrstva (Packet Data Convergence Protocol)**

Hlavná úloha PDCP vrstvy pozostáva z kompresie hlavičky a implementácie bezpečnosti, ako sú šifrovanie a integrita dát. Túto vrstvu používajú rádiové bearery. Každý z týchto bearerov zodpovedá toku špecifických informácií používateľských dát.

- **RLC (Radio Link Control)**

RLC vrstva poskytuje vrstve PDCP základné služby ako sú segmentácia dát a mechanizmus opravy chýb ARQ (Automatic Repeat Request). RLC mapuje každý prichádzajúci tok do logického kanálu, ktorý putuje do vrstvy MAC.

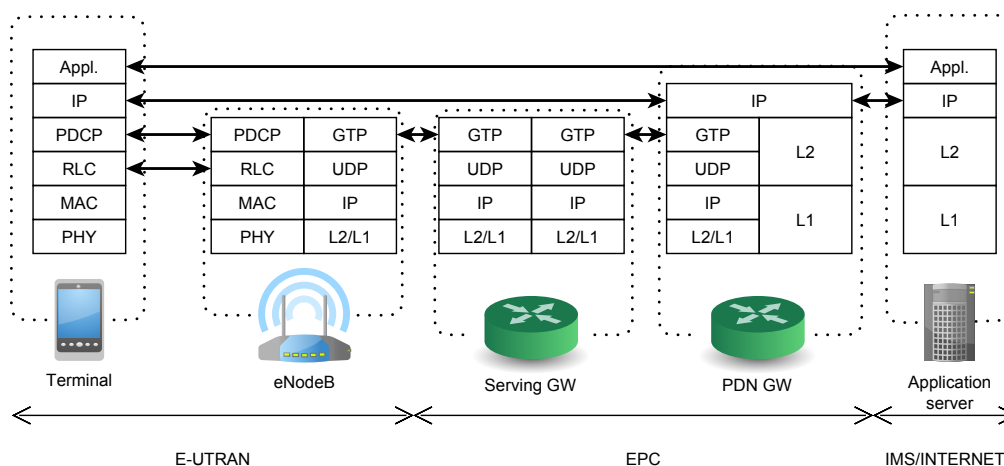
- **MAC (Media Access Control)**

Hlavnou úlohou vrstvy MAC je mapovanie a multiplexing logických kanálov do transportných kanálov. Logické kanály sú najskôr zoradené podľa priority. Vrstva tiež podporuje HARQ (Hybrid ARQ), čo je v podstate proces rýchleho opakovania. Následne je dátový tok doručený do fyzickej vrstvy, kde sú aplikované kódovanie a modulácia a dáta sú odoslané rádiovým rozhraním.

2.2 Architektúra užívateľskej roviny v EPC

Z pohľadu bezdrôtových sietí, vrátane prístupovej časti a jadra siete, užívateľská rovina nezahrňuje len dáta používateľov, ako hlasové pakety alebo webový obsah, ale zahŕňa tiež signalizáciu spojenú s aplikačnými službami ako sú SIP alebo RTCP.

End-to-end protokolová výbava užívateľskej roviny od terminálu k aplikačnému serveru je zobrazená na obrázku 2.2. Na obrázku je aplikačná vrstva (založená na prenose IP) prítomná iba na termináli a aplikačnom serveri. Pakety aplikačnej vrstvy sú smerované prostredníctvom brán paketových jadier PDN GW predtým, ako dosiahnu aplikačný server. V tomto prípade, aplikačná vrstva môže obsahovať veľké množstvo protokolov ako end-to-end transportné protokoly (napr. TCP alebo UDP) a RTP protokol na prenos používateľských dát, rovnako ako signalizácia protokolov na aplikačnej vrstve.



Obr. 2.2: Protokolová výbava užívateľskej roviny v EPS

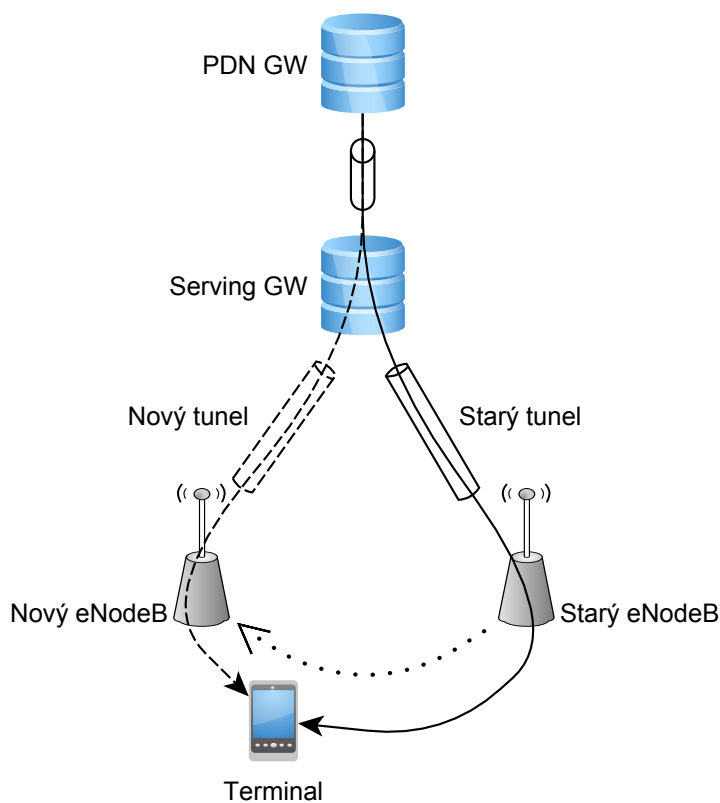
2.2.1 GTP tunelovanie dát

Tunel je vo svete telekomunikácií pojem, ktorý označuje obojsmernú point-to-point komunikáciu medzi dvoma subjektami. Hlavným dôvodom tunelovania dát v 3GPP

sieťach je riešenie problémov so smerovaním paketov vyplývajúcich z pohybu terminálov.

Vzhľadom na pakety, prichádzajúce od externých sietí do PDN GW, sa môže paket počas relácie zmeniť. Napríklad zmena aktuálneho eNodeB, alebo v menšej miere zmena aktuálneho Serving GW môže nastať behom streamovania alebo prezerania webu, z čoho vyplýva, že cesta paketu musí byť modifikovaná v záujme zachovania kontinuity služby. V jadre 3GPP siete je príslušný Serving GW alebo PDN GW aktualizovaný hneď, ako terminál zmení používaný eNodeB. V záujme zachovania kontinuity služby, je hneď na to vytvorený nový tunel do aktuálneho eNodeB.

Na obrázku 2.3 je zobrazené prispôbenie tunela v prípade zmeny používateľom používaného eNodeB. Tunel, ktorý vedie od PDN GW ku Serving GW sa nezmenil, ale musí byť nastavený nový tunel, vedúci od Serving GW k aktuálnemu eNodeB.



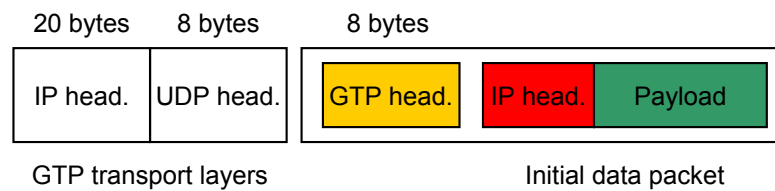
Obr. 2.3: Použitie GTP tunela v prípade pohybu používateľa

Podľa 3GPP definície je tunelovanie používateľských dát medzi sieťovými prvkami obstarávané vrstvou GTP, zdedenou od 2G/GPRS štandardu.

GTP protokol je zložený z dvoch častí:

- Užívateľská časť (GTP-U), ktorá zabezpečuje zapúzdrovanie a prenos používateľských dát.
- Kontrolná časť (GTP-C), ktorá je používaná v EPC a zabezpečuje všetky procedúry a správy pre správu tunela (napr. vytvorenie, zmenu alebo ukončenie tunela).

Obrázok 2.4 ilustruje proces zapúzdrovania. Dátový paket je zachovaný a bez zmeny. K paketu je pridaná hlavička GTP (obsahujúca hlavne konečný bod tunela a sekvenčné číslo GTP PDU) používaná prijímačom na identifikovanie tunela, s ktorým je paket spojený.[2]



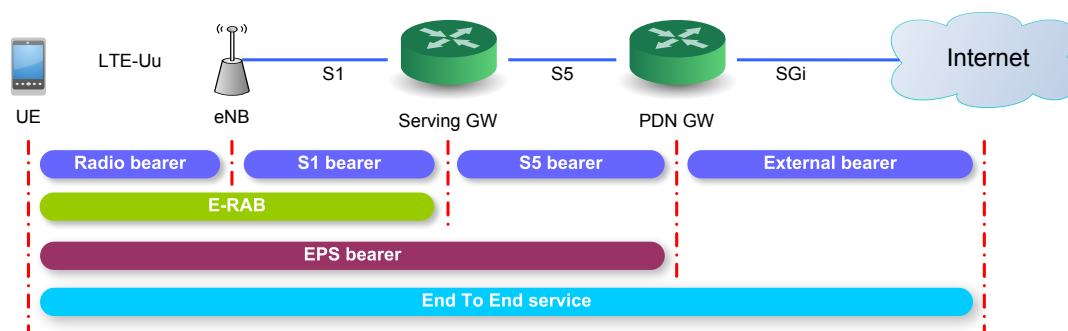
Obr. 2.4: Efekt GTP tunelovania (s použitím IPv4 pre GTP transport)

3 REALIZÁCIA MOBILNÝCH SLUŽIEB

V tejto sekcii popisujem najpoužívanějšíe mobilné služby, ako napr. prezeranie webových stránok či e-mailu. Užívatelia budú vždy chcieť mať čo najlepší zážitok z používania predplatených služieb a taktiež sa vždy nájdu užívatelia, ktorí sú ochotní priplatiť si za väčšiu šírku pásma a lepší prístup k sieti. Nie iba užívatelia, ale aj služby potrebujú lepšie prioritné zaobchádzanie v LTE sieti, ako napr. VoIP telefonovanie. O tieto aspekty sa stará QoS (Quality of Service).

3.1 Quality of Service

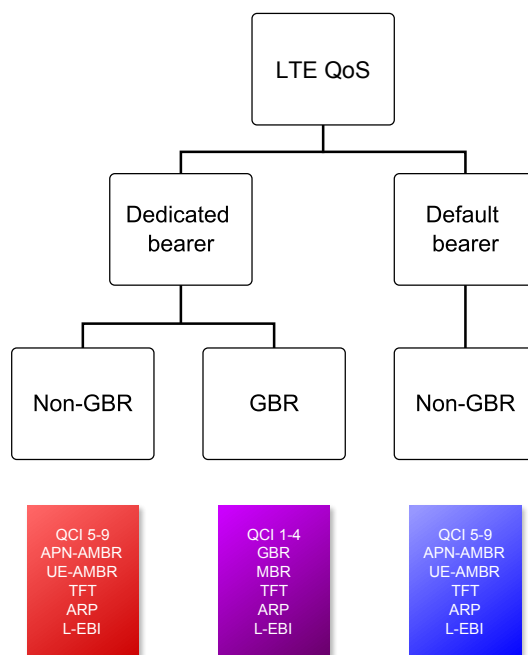
QoS definuje priority pre používateľov a služby v čase vysokého vyťaženia siete. V LTE sieti je QoS implementované medzi UE (User equipment) a PDN GW a je aplikovaný na súbor bearerov. Bearer je v podstate virtuálny koncept nastavenia siete, ktorý zabezpečuje špeciálne zaobchádzanie s určitým dátovým tokom, VoIP dáta budú prioritizované sieťou pred HTTP dátami. QoS je aplikovaná na rádiový bearer, S1 bearer a S5/S8 bearer sú spolu nazývané EPS bearer.



Obr. 3.1: EPS bearer a jeho časti

3.1.1 Typy bearerov a ich vlastnosti

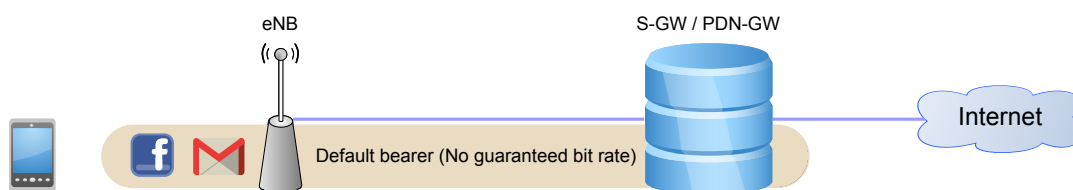
Poznáme 2 typy bearerov a to Defaultný a Dedikovaný bearer. Ak je používateľ pripojený k sieti, je tu vždy aspoň 1 defaultný bearer, zatiaľ čo Dedikovaný bearer je založený vždy vtedy, keď je treba poskytnúť QoS špecifickej službe. Na obrázku 3.2 je zobrazené hierarchické rozdelenie QoS bearerov.



Obr. 3.2: Typy bearerov a ich vlastnosti [8]

Defaultný bearer

Keď sa používateľ pripojí do siete, vytvorí sa defaultný bearer, ktorý existuje tak dlho, ako dlho je používateľ pripojený do siete. Tento bearer je služba best effort (QCI 5). Každý defaultný bearer má vlastnú IP adresu. Používateľ si môže naraz prezerať webové stránky, kontrolovať elektronickú poštu, či využívať službu Facebook. V tomto prípade budú 3 defaultné bearre. Každý má vlastnú IP adresu a majú pridelené QCI 5 až 9, čo zodpovedá službám Non-GBR, ktoré nemajú garantovanú prenosovú rýchlosť.

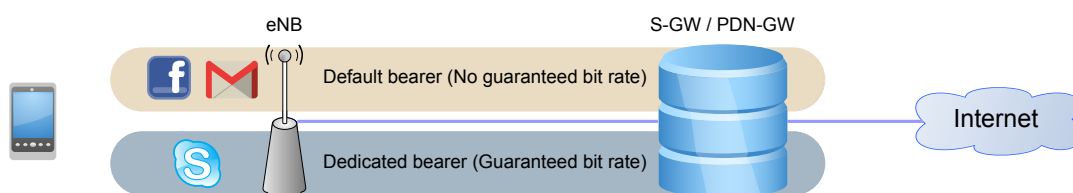


Obr. 3.3: Defaultný bearer pre 2 služby

Dedikovaný bearer

Dedikovaný bearer poskytuje určený tunel pre 1 alebo viac prioritizovaných služieb (VoIP, video atď). Správa sa ako dodatočný bearer pre defaultný bearer, takže nepotrebuje mať vlastnú IP adresu, keďže defaultný bearer ju má. S jedným defaultným bearerom môže byť spojených až 10 dedikovaných bearerov. Dedikovaný bearer môže využívať služby s garantovanou rýchlosťou pripojenia, ako aj služby bez garantovanej rýchlosti pripojenia. Používa traffic flow template (TFT), aby zabezpečil špeciálne zaobchádzanie pre služby. Zvyčajne LTE sieť s VoLTE (Voice over LTE) má:[6]

1. **Defaultný bearer 1:** Použitý pre signalizačné SIP správy, vzťahujúce sa k IMS sieti (QCI 5).
2. **Dedikovaný bearer :** Je spojený s defaultným bearerom a používa sa pre VoLTE a VoIP služby ako Skype alebo telefónny hovor (QCI 1).
3. **Defaultný bearer 2:** Používaný pre ostatné služby, ktoré môže používateľ používať, ako prezeranie webu, elektronickej pošty či sledovanie videa.



Obr. 3.4: Defaultný bearer pre služby s garantovanou a negarantovanou prenosovou rýchlosťou

Defaultný bearer môže byť iba typu Non-GBR, ale dedikovaný bearer môže byť typu GBR alebo Non-GBR. GBR poskytuje garantovanú prenosovú rýchlosť a je spojený s parametrami:

- **GBR (The Minimum Guaranteed Bit Rate)**
Minimálna garantovaná prenosová rýchlosť pre EPS bearer. Je špecifikovaná nezávisle pre downlink a uplink.
- **MBR (The Maximum Guaranteed Bit Rate)**
Maximálna garantovaná prenosová rýchlosť pre EPS bearer. Je špecifikovaná nezávisle pre downlink a uplink.

Non-GBR neposkytuje garantovanú prenosovú rýchlosť a je spojený s parametrami:

- **APN-AMBR (Access Point Name - Aggregate Maximum Bit Rate)**
Je to maximálna celková povolená priepustnosť služby s negarantovanou rýchlosťou pripojenia do Serving alebo PDN GW.
- **UE-AMBR (User Equipment - Aggregate Maximum Bit Rate)**
Je to maximálna celková povolená priepustnosť služby s negarantovanou rýchlosťou pripojenia medzi Serving GW, PDN GW a UE.

TFT (Traffic Flow Template)

TFT je vždy spojované s dedikovaným bearerom, zatiaľ čo defaultný bearer ho obsahovať môže, ale nemusí. TFT filter definuje pravidlá, podľa ktorých vedú sieťové prvky alebo používateľ, ktorý IP paket má byť odoslaný cez konkrétny dedikovaný bearer. Tieto TFT filtre vytvára PCRF a rozosiela ich pre UE ako **context setup message** pre posielanie dát v smere do internetu, v smere z internetu sa o TFT filtrovanie stará PDN GW. Väčšinou býva pravidlo definované na základe zdrojovej či cieľovej IP adresy alebo zdrojového či cieľového portu. TFT filtre sa aplikujú per direction, čiže na každý smer.

ARP (Allocation and Retention Priority)

Alokácia a zachovanie priority (ARP) sa používa na rozhodovanie o tom, či bude požiadavka na modifikáciu alebo vytvorenie bearera prijatá (vzhľadom na súčasnú situáciu zdrojov).

L-EBI (Linked EPS Bearer ID)

Ako bolo vysvetlené v sekcii ohľadne dedikovaného beareru, vieme že každý dedikovaný bearer je spojený s jedným z defaultných bearerov. L-EBI hovorí dedikovanému beareru, s ktorým defaultným bearerom je prepojený.

QCI (QoS Class Identifier)

Je spojovaný so všetkými bearermi a definuje vlastnosti IP paketov, ako je zobrazené v tabuľke 3.1.[5]

QCI	Typ Beareru	Priorita	Oneskorenie paketu	Služba
1	GBR	2	100 ms	VoIP hovor
2		4	150 ms	Video hovor
3		3	50 ms	Online hry (v reálnom čase)
4		5	300 ms	Video streaming
5	Non-GBR	1	100 ms	IMS signalizácia
6		6	300 ms	Video, TCP služby ako email, www, ftp
7		7	100 ms	Hudba, video, interaktívne hry
8		8	300 ms	Video, TCP služby ako email, www, ftp
9		9		

Tab. 3.1: Úrovně QCI a vlastnosti paketov

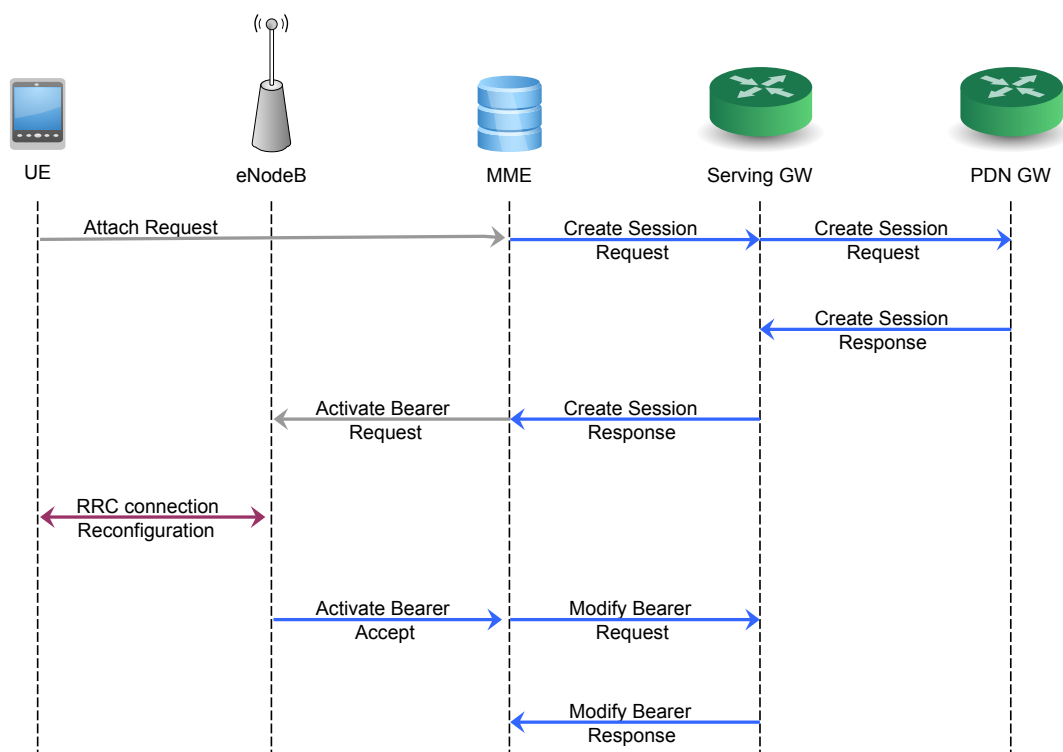
3.2 Prehliadanie webových stránok

Po prihlásení používateľa do siete, používateľ dostane TFT filter od PCRF cez `context setup message` správu. V TFT filtri má používateľ definované služby, ktoré môže využívať, a typ beareru, cez ktorý má konkrétna služba komunikovať. Aby mohol používateľ komunikovať s webovým serverom, musí byť najskôr vytvorený EPS bearer. Diagram EPS beareru je zobrazený na obrázku 3.5.

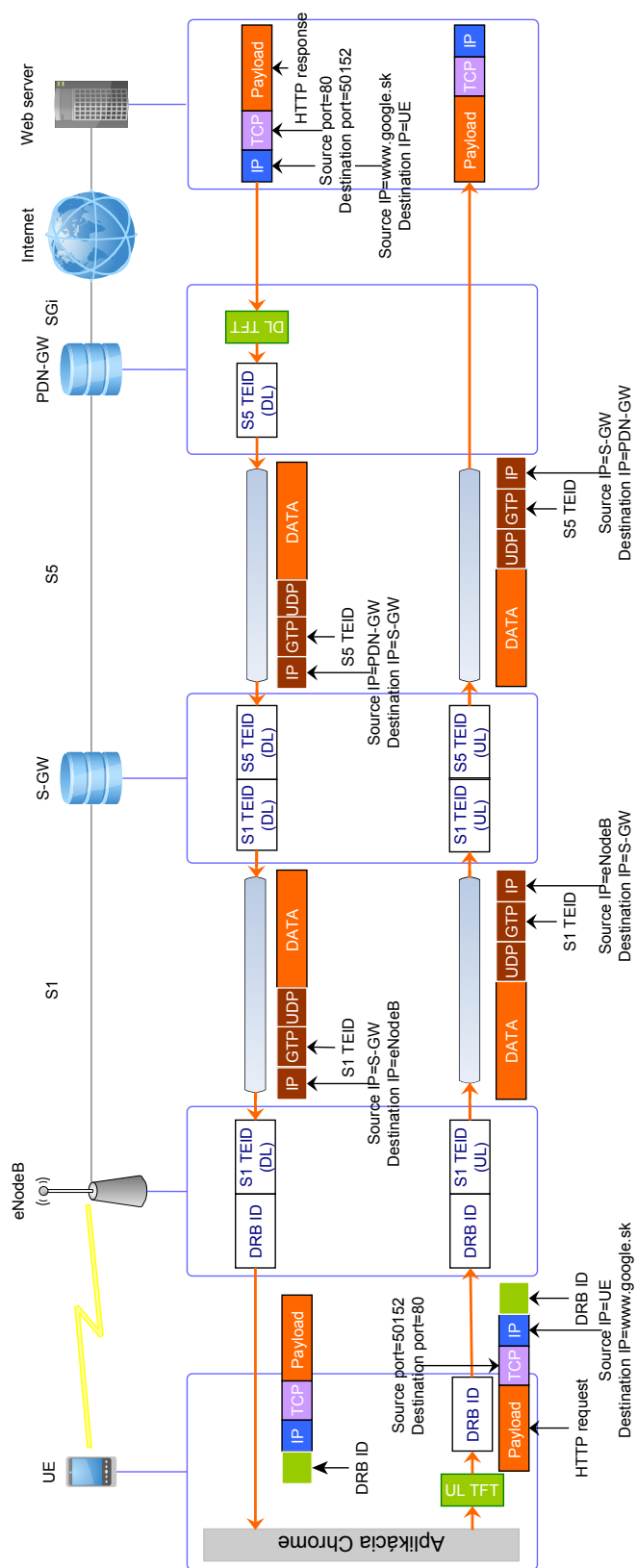
Na prehliadanie webových stránok slúži používateľovi webový prehliadač, ktorý využíva protokol aplikačnej vrstvy OSI modelu HTTP na prenos HTML súborov z webových serverov. Po zadaní adresy používateľom napr. `www.google.sk`, ktorú používateľ získal od DNS serveru, sa vyšle zapúzdrená požiadavka HTTP request na webový server. V prípade EPS siete, z terminálu používateľa putuje zapúzdrená požiadavka s DRB ID používateľa (Data Radio Bearer identifier) na webový server cez eNodeB defaultným rádiovým bearerom. Od eNodeB je cez defaultný S1 bearer požiadavka zapúzdrená GTP protokolom tak, že sa pridá hlavička UDP, GTP-U hlavička obsahujúca TEID (Tunnel Endpoint Identification) a IP hlavička obsahujúca zdrojovú IP adresu eNodeB a cieľovú IP adresu S GW, a následne je tunelovaná do Serving GW. Ďalej je požiadavka tunelovaná do PDN GW cez defaultný S5 bearer. Tu PCEF počíta veľkosť prenesených a prijatých dát pre každého používateľa. PDN GW už ďalej smeruje paket buď rovno cez internet na webový server, alebo smeruje paket do IMS (ak ho operátor používa) a následne cez internet na webový server.

Webový server odpovedá pomocou HTTP response a paket je smerovaný cez internet do PDN GW. Do PDN GW prichádza externý bearer a nastáva tu filtrácia paketov v smere downlink. PDN GW obsahuje TFT filtre od PCRF. Najčastejšie tieto filtre triedia pakety na základe zdrojovej a cieľovej IP adresy, zdrojového a cieľového portu alebo protokolu. V našom prípade by sa zhodoval zdrojový port 80,

alebo použitý protokol (HTTP). Tým pádom bude paket tunelovaný GTP protokolom cez S5 bearer do S-GW, čiže sa paket zapúzdri pridaním UDP hlavičky, GTP-U hlavičky, ktorá obsahuje tunel endpoint identifikátor a IP hlavičku obsahujúcu IP adresu Serving GW a PDN GW. Tým istým spôsobom je paket tunelovaný do eNodeB. Ďalej je paket smerovaný cez rádiový bearer priamo používateľovi pridaním DRB ID eNodeB. Celý postup je znázornený na obrázku 3.6.



Obr. 3.5: Diagram vytvorenia defaultného EPS bearera



Obr. 3.6: Pribeh odoslania HTTP requestu a následné prijatie HTTP response

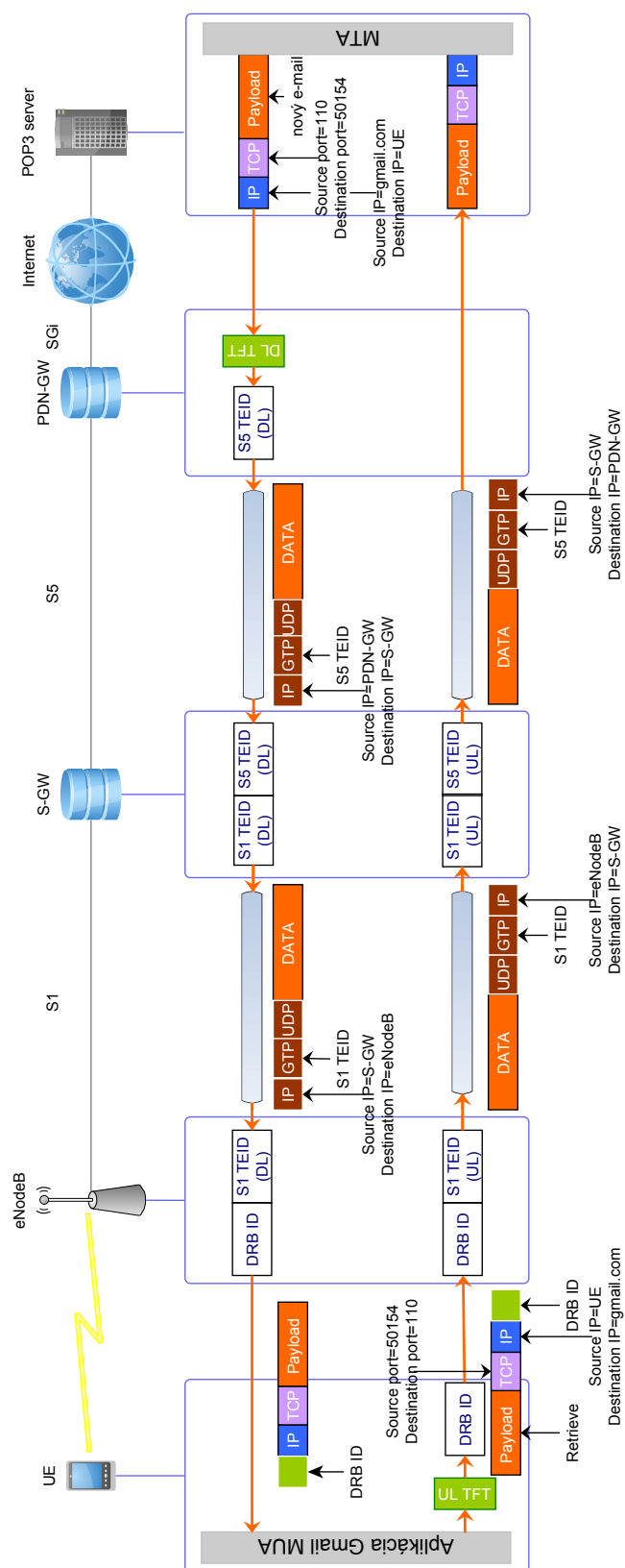
3.3 Prezeranie elektronickej pošty

Veľká časť tejto komunikácie je rovnaká ako pri HTTP komunikácii. Používateľ už obdržal TFT filter od PCRF cez `context setup message` správu. Vo TFT filtri má používateľ definované služby, ktoré môže využívať, ako aj typ bearera, cez ktorý má konkrétna služba komunikovať. Aby mohol používateľ komunikovať s e-mailovým serverom, musí byť najskôr vytvorený EPS bearer. Diagram vytvorenia EPS beareru je zobrazený na obrázku 3.5.

Predpokladám, že používateľ využíva na kontrolu e-mailov mobilnú e-mailovú aplikáciu Gmail. Po otvorení aplikácie prebieha prihlasovanie sa k používateľovmu e-mailu. Najskôr prebieha vytvorenie TCP spojenia cez three way handshake. Potom používateľ posíla svoju e-mailovú adresu cez príkaz USER. Server túto adresu potvrdí a žiada od používateľa heslo. Následne používateľ posíla svoje heslo, a server posíla potvrdenie. Celá táto komunikácia prebieha v pozadí aplikácie Gmail. Potom sa používateľovi zobrazí aplikácia, ktorá obsahuje staré uložené e-maily.

Používateľ chce vedieť, či má nové e-maily, preto vyšle príkaz STAT na server. POP3 server indikuje používateľovi, že má 1 e-mail v schránke. Používateľ teda žiada server o zaslanie novej správy cez požiadavku RETRIEVE. Táto zapúzdrená požiadavka s DRB ID používateľa, ako aj všetky ostatné požiadavky, je vyslaná cez defaultný rádiový bearer na e-mailový POP3 server. Telefón používateľa vie, že má posílať požiadavky, týkajúce sa e-mailu, cez defaultný rádiový bearer na základe TFT filtra. Od eNodeB je už požiadavka ďalej zapúzdrená UDP, GTP-U hlavičkou, ktorá obsahuje TEDI eNodeB (Tunnel Endpoint Identification) a IP hlavičkou obsahujúcou zdrojovú IP adresu eNodeB a cieľovú IP adresu S GW. Následne je tunelovaná do Serving GW cez S1 defaultný bearer. Potom je požiadavka tunelovaná s TEDI S GW do PDN GW cez S5 defaultný bearer. Súčasťou PDN GW je PCEF, ktoré má za úlohu počítat prenesené dáta pre každého používateľa. PDN GW potom ďalej smeruje tento paket cez internet na e-mailový POP3 server.

E-mailový server odpovedá a zasiela používateľovi vyžiadaný e-mail. Paket dorazí do PDN GW cez externý bearer. Tu nastáva filtrácia paketov v smere downlink na základe napr. zdrojového portu, (v tomto prípade 110), alebo na základe použitého protokolu POP3. Paket je tunelovaný do Serving-GW a následne do eNodeB. Od eNodeB je paket smerovaný k používateľovi cez rádiový bearer. Celý postup je znázornený na obrázku 3.7.



Obr. 3.7: Priebeh odoslania POP3 Retrieve správy a následné prijatie e-mailu

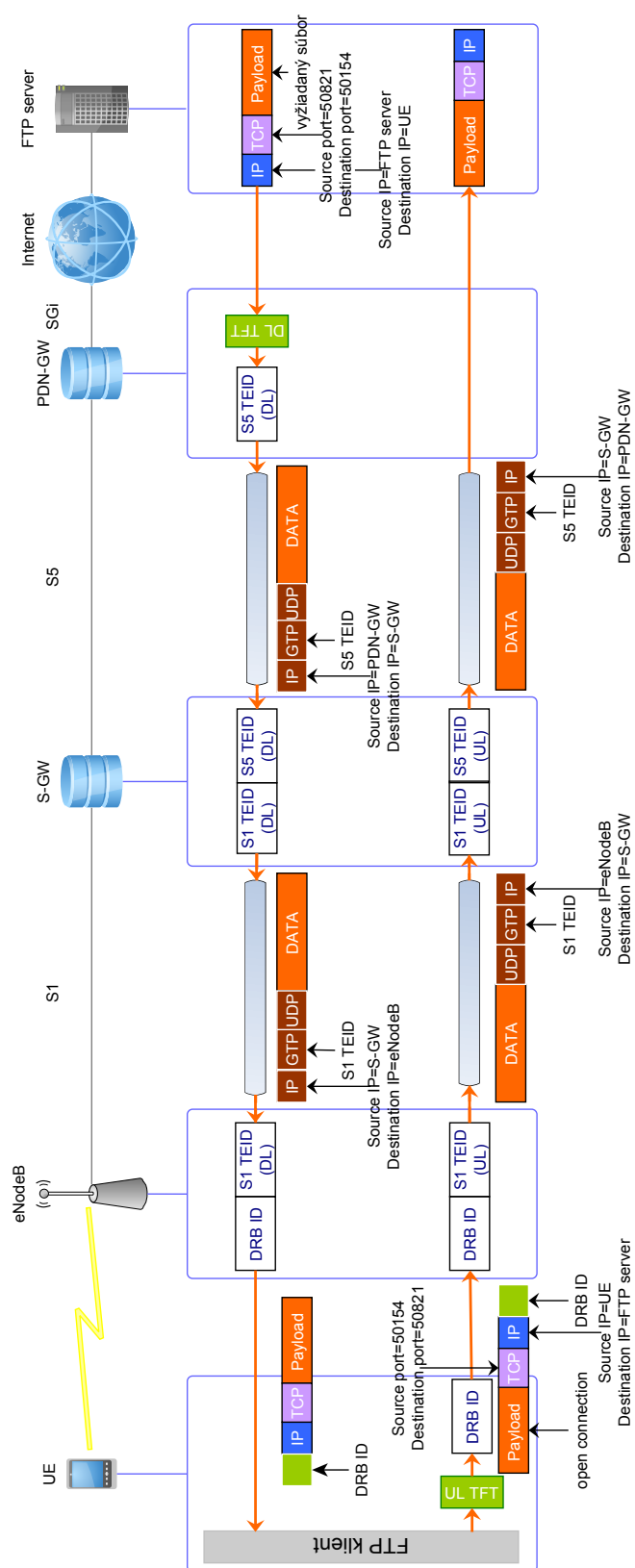
3.4 Sťahovanie súboru

V tejto sekcii je opísaný spôsob, akým používateľ sťahuje súbor napr. zo svojho domáceho FTP serveru. FTP je protokol, ktorý sa využíva na prenos hlavne väčších súborov. V dnešnej dobe FTP servery bežia v aktívnom alebo v pasívnom móde. Väčšina z nich beží v móde pasívnom, a to hlavne preto, že v dnešnej dobe je spojenie, vytvárané zo vzdialeného serveru k používateľovi v sieti, zakázané firewallom.

Používateľ si chce zo svojho FTP serveru stiahnuť film. Nachádza sa v zamestnaní, kde je ich sieť chránená firewallom, čiže FTP server používateľa musí pracovať v pasívnom móde. Používateľ využíva svoj prehliadač, aby sa pripojil k svojmu serveru. Po zadaní adresy, musí používateľ zadať prihlasovacie údaje a následne uvidí koreňový list súborov na stiahnutie. Keď si používateľ vyberie súbor, ktorý chce stiahnuť a klikne naň, v tej chvíli UE vyšle príkaz PASV na server, ktorý odpovie svojou IP adresou a dynamicky zvoleným portom. UE následne otvorí TCP spojenie, pričom využije údaje prijaté zo serveru a následne nastáva prenos súboru.

Každá požiadavka UE je vedená LTE sieťou. Keď UE posiela príkaz PASV na server, pridá k paketu DRB ID používateľa a vyšle tento príkaz cez defaultný rádiový bearer do eNodeB. Následne eNodeB použije vytvorený tunel, pridá TEDI a GTP hlavičku a paket je tunelovaný cez S1 defaultný bearer do Serving-GW, kde sa tento proces opakuje, a paket sa tuneluje cez S5 defaultný bearer do PDN GW, ktorý následne smeruje paket na FTP server.

FTP server odpovedá poslaním príkazu PASV s IP adresou klienta a zvoleným dynamickým portom. Tento paket je smerovaný do PDN GW. Tu následne nastáva filtrácia paketov a ich počítanie. FTP protokol je povolený a teda PDN GW tuneluje paket pridaním GTP hlavičky do Serving GW, ktorý paket tuneluje do eNodeB. ENodeB pridá DRB ID a posiela paket cez rádiový bearer do UE. Na obrázku 3.8 je zobrazené otvorenie spojenia na prenos používateľom a následný prenos súboru od FTP serveru.



Obr. 3.8: Otvorenie TCP spojenia používateľom a prenos súboru od FTP serveru

3.5 Sledovanie mobilnej televízie

V tomto prípade môže byť služba realizovaná dvoma spôsobmi. Operátor môže službu ponúkať pomocou Multimedia Broadcast Multicast Services (MBMS). V opačnom prípade musí používateľ sledovať mobilnú televíziu cez internet. Ďalej sa zameriame na spôsob, keď operátor ponúka službu cez MBMS.

MBMS by sa nemalo mýliť s IP Multicastom. IP multicast môže byť podporovaný bezdrôtovými sieťami, ale v tomto prípade IP multicast nepovoľuje zdieľanie spoločného rádiového zdroja pre používateľov, pripojených do jednej rádiostanice.[2]

MBMS služba je tvorená dvomi službami: broadcast a multicast. Hlavné rozdiely medzi službami sú:

- Broadcastová služba môže byť prijímaná hociktorým používateľom, ktorý sa nachádza v oblasti, kde je služba ponúkaná.
- Multicastová služba môže byť prijímaná iba používateľmi, ktorí si službu predplatili, a sú pripojení do multicastovej skupiny spojennej so službou.

Broadcastové a multicastové služby sú jednosmerné point-to-multipoint prenosy multimediálnych dát. Tieto služby sú používané pre prenos napr. textu, hudby, videa od zdroja Broadcast Multicast Service Centre (BM-SC) ku:

- Hociktorému používateľovi, ktorý sa nachádza v oblasti služby (teda v prípade Broadcastovej služby).
- Členom multicastovej skupiny (teda v prípade Multicastovej služby).

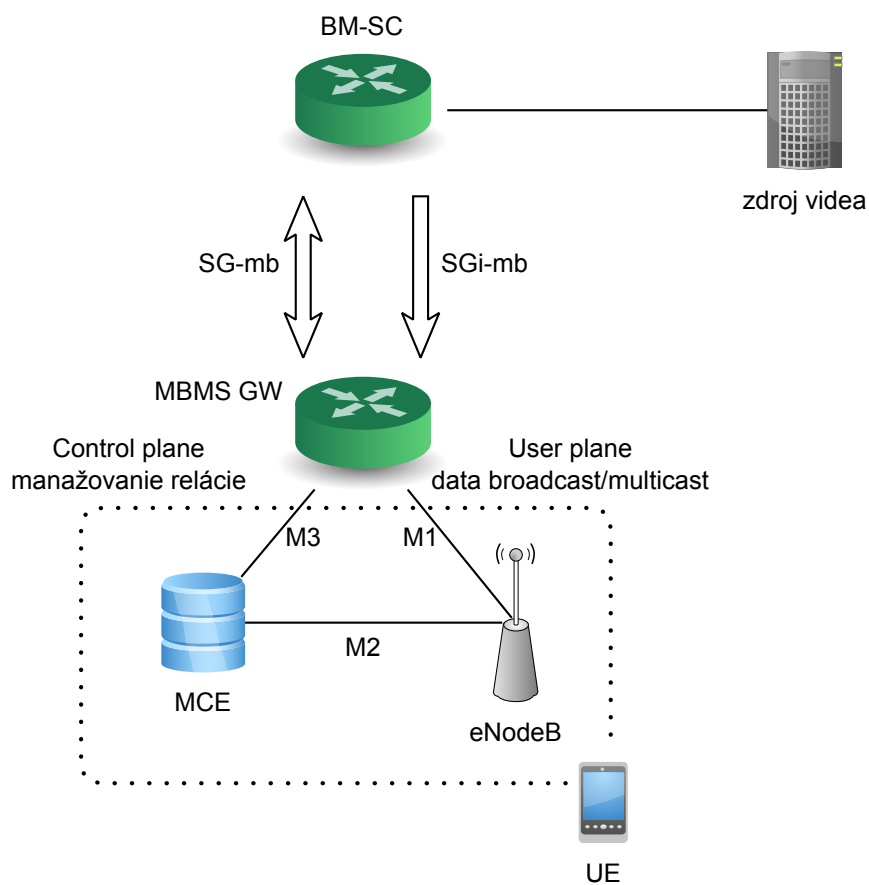
Pokiaľ chce používateľ prijímať broadcastovú službu, stačí, aby mal túto službu povolenú na svojom termináli. Operátor preto nemôže vedieť, kto túto službu prijíma a teda by ju nevedel účtovať.

V prípade multicasu je potrebné, aby sa používateľ pridal do konkrétnej skupiny a mohol službu prijímať. V tomto prípade multicastová služba povoľuje operátorovi, aby nastavil účtovacie pravidlá pre túto službu.[1]

3.5.1 Architektúra služby

Z hľadiska EPS sietí, kvôli tejto službe bolo treba zaviesť dva nové logické sieťové prvky: MCE a MBMS GW.

MCE (Multi-cell/multicast Coordination Entity) je prvok, zodpovedný za alokáciu časových a frekvenčných zdrojov pre multi-stanicový MBMS prenos. MCE je logický člen, najčastejšie integrovaný do eNodeB.



Obr. 3.9: Logická architektúra MBMS služby

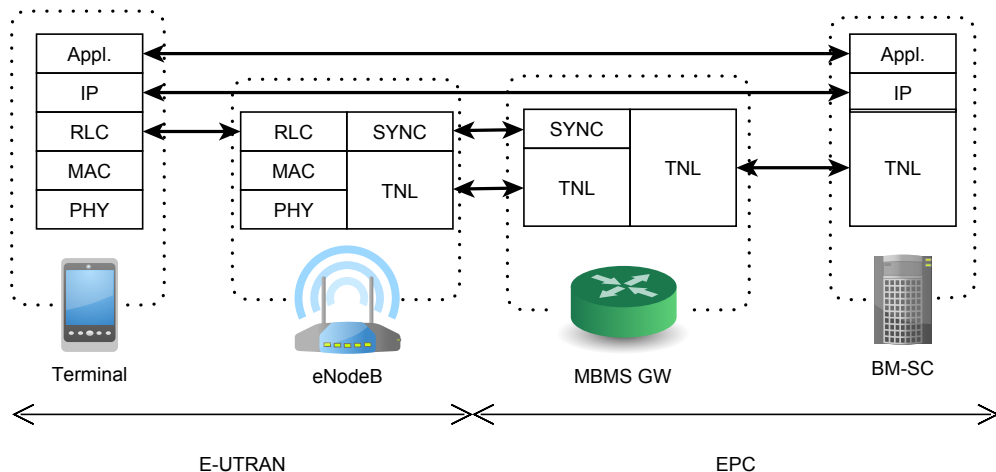
MBMS GW (MBMS Gateway) je vstupný bod pre broadcastový a multicastový tok dát. Jeho úlohou je posielanie dát do všetkých eNodeB patriacich do oblasti služby, a taktiež sa stará o riadenie relácie (ako štart a ukončenie relácie). Jeho úlohou je tiež účtovanie služby pre používateľov, ktorí majú aktívnu MBMS reláciu.

BM-SC poskytuje službu koncovému používateľovi. Služí ako vstupný bod pre broadcastové a multicastové externé zdroje operátora.

Jeho hlavné funkcie sú:

- Autorizácia používateľských požiadaviek na aktivovanie MBMS služby.
- Plánovanie broadcastových a multicastových relácií.
- Oznámenie služby, ktorá môže byť uskutočnená cez SMS (Short Message Service).
- Zabezpečuje integritu a ochranu dôvernosti dát MBMS.

Na obrázku 3.10 je zobrazená architektúra EPS užívateľskej roviny pre MBMS služby.



Obr. 3.10: Architektúra užívateľskej roviny MBMS služby

TNL (Transport Network Layer) reprezentuje protokoly založené na IP prenose. TNL na M1 interface je založený na IP multicaste, takže povoľuje point to multipoint prenos.

SYNC protokol používaný cez M1 interface povoľuje synchronizáciu obsahu. SYNC nesie prídavné informácie, podľa ktorých môže eNodeB identifikovať časovanie prenosových rádiových rámcov a zistiť stratovosť paketov.

Pre streamované služby je prenos dát založený na RTP/RTCP (Real Time Protocol/Real Time Control Protocol). Tento typ protokolu povoľuje používateľovi obnoviť časové informácie dát, ktoré môžu byť zmenené prenosovým oneskorením. FEC hlavička je pridaná na každý RTP paket, aby umožnila detekciu chýb a ich prípadnú korekciu používateľom. Umožní používateľovi zrekonštruovať chýbajúcu časť prijatých dát.

Pre sťahované služby, (ako prenos obrázku, 3GPP audio/video súbor alebo prenos binárnych súborov), služba MBMS používa FLUTE protokol (File Delivery over Unidirectional Transport). FLUTE je jednosmerný prenosový protokol špeciálne

navrhnutý pre multicastový prenos, a preto nepotrebuje spojenie od odosielateľa k prijímateľovi. Poskytuje formát, ktorý špecifikuje meno, veľkosť a typ súboru, ktorý bude prenesený. Prenosová spoľahlivosť je zabezpečená použitím Forward Error Correction (FEC) integrovaného do FLUTE.[2]

3.5.2 Priebeh sledovania mobilnej televízie

V prvom rade musí mať používateľ túto službu predplatenú. Celá komunikácia prebieha cez prvky UE, eNodeB, MBMS GW a BM-SC a používajú sa MBMS

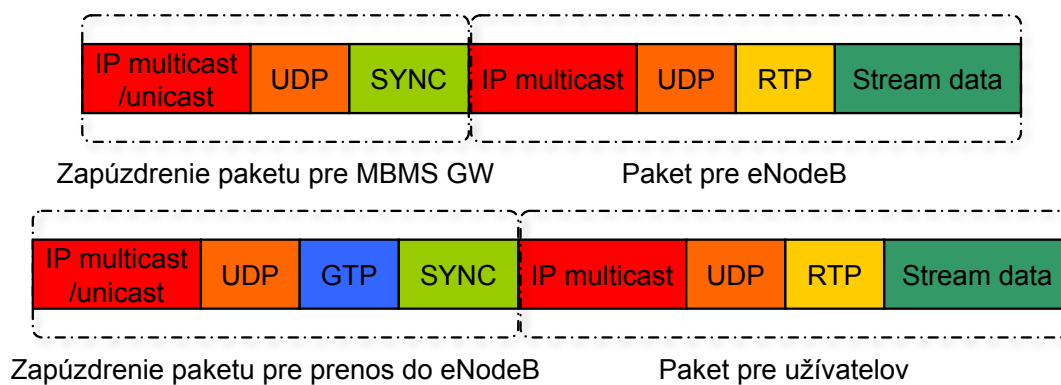
(dedikované) bearre. Ako prvé používateľ otvorí aplikáciu, cez ktorú bude službu sledovať. Vtedy používateľ prijme všetky potrebné informácie [multicastové adresy, čísla portov, TMGI (používa sa na rozlíšenie MBMS služieb ako napríklad rozlíšenie rôznych TV kanálov, používaných kodekov)] cez MBMS bearer pomocou SDP. Následne používateľ oznamuje prijímanie MBMS služby, a vstúpi do multicastovej skupiny pomocou IGMP. Služba môže využívať jeden alebo viac MBMS bearerov. Používateľ požiada MBMS GW o vytvorenie dátového MBMS beareru. Po vytvorení beareru, je používateľ informovaný o prebiehajúcich a nasledujúcich MBMS prenosoch. Používateľ si vyberie, ktorý prenos chce sledovať a začne prijímať dáta.

Tieto dáta BM-SC prijíma cez RTP. BM-SC vytvorí dáta pre používateľov, čiže ku streamu pridá SRTP hlavičku, UDP hlavičku obsahujúcu číslo portu, IP hlavičku, kde je cieľová multicastová adresa. BM-SC posieľa tento stream používateľom v multicastovej skupine cez MBMS GW v MBMS beareri, a preto je potrebné pridať hlavičku UDP a hlavičku IP, kde je cieľová unicastová adresa MBMS GW, alebo multicastová adresa viacerých MBMS GW.[9]

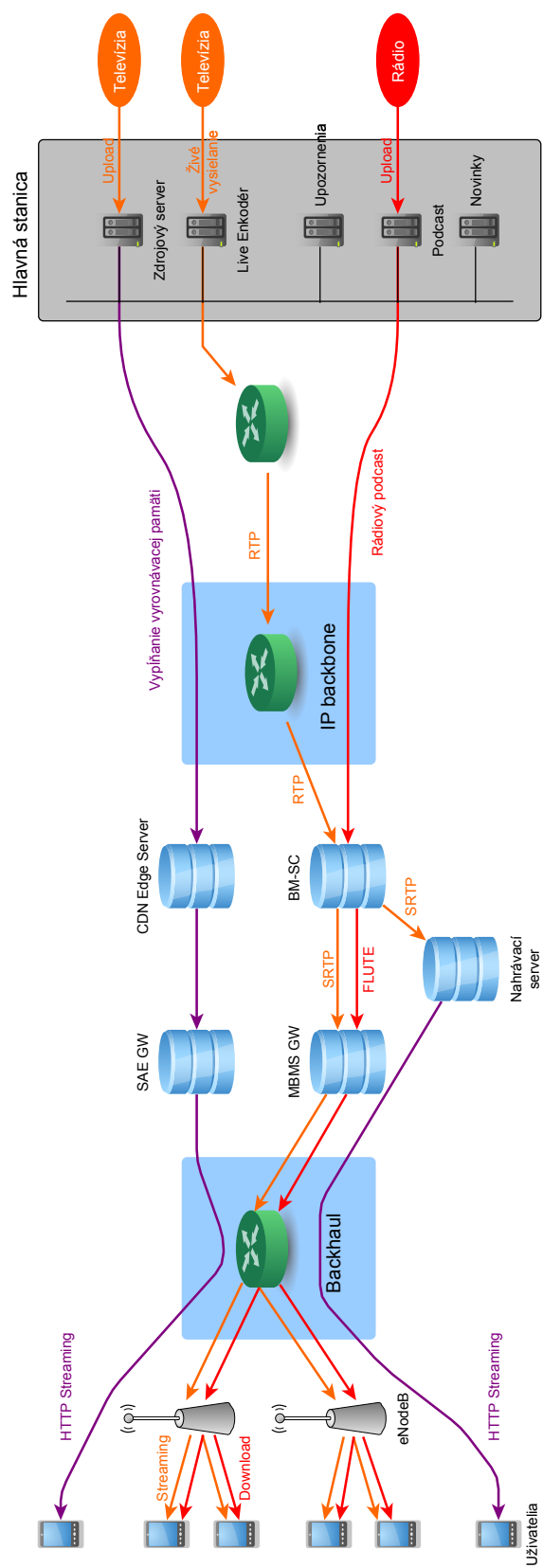
MBMS GW paket prijme, pridá hlavičku SYNC, v ktorej BM-SC nastaví pole TS (Time Stamp) podľa času prijatia paketu plus jeho oneskorenie, a znova ho zapúzdri pomocou GTP protokolu pridaním hlavičky UDP a hlavičky IP, v ktorej sa nachádza cieľová multicastová adresa viacerých eNodeB.[7]

eNodeB broadcastuje RTP stream s cieľovou IP multicastovou adresou používateľovi cez rádiový bearer a používateľ môže prijať RTP stream akonáhle porovná prijaté TMGI s TMGI rádiového bearera. Ak sa TMGI zhodujú (tzn. že sa jedná o používateľom vybraný TV kanál), UE prijíma RTP stream. Na obrázku 3.12 je znázornené streamovanie videa spolu s HTTP streamovaním.

HTTP živé streamovanie funguje na princípe rozdelenia streamu na malé HTTP súbory, ktoré sú zaslané používateľovi. Používa sa požiadavka HTTP request a odpoveď HTTP response. Na základe zdrojového portu 80 prejde tento stream cez ktorýkoľvek firewall alebo proxy server. Používateľ používa URL súbor playlistu .m3u8. Tento playlist obsahuje iba list súborov na prehratie a metadáta popisujúce obsah. Pokiaľ tento playlist nemá koncový tag, jedná sa o živý stream. Celá táto komunikácia funguje cez EPS bearer, na rozdiel od MBMS streamovania, ktoré funguje cez MBMS bearer, nezávisle na EPC.[3]



Obr. 3.11: Paket smerujúci od BM-SC k MBMS GW a paket smerujúci od MBMS GW k eNodeB



Obr. 3.12: Streamovanie televízneho kanálu

4 KVALITA REALIZOVANÝCH SLUŽIEB

Pre používateľa ako predplatiteľa služieb je dôležité, aby jeho služby pracovali bezchybne, a aby bol so službami spokojný. V tejto sekcii sú opísané spôsoby, akými môžeme zmerať kvalitu služieb komunikujúcich cez LTE sieť ako aj možné príčiny zlyhania služieb a následná lokalizácia týchto chýb.

4.1 Meranie kvality služieb

Po tom ako operátor zavedie novú sieť (v našom prípade LTE sieť), je potrebné overiť sieťovými prvkami poskytovanú kvalitu služieb a ich QoS funkciu. Overenie kvality služieb LTE siete vyžaduje zaťaženie siete paketami, zodpovedajúcimi najpoužívanejším službám v mobilnej komunikácii ako HTTP a FTP, a následné meranie ich kľúčových indikátorov (KPI).[11]

4.2 Kľúčové indikátory výkonnosti (KPI)

KPI sú indikátory, ktoré nám pomáhajú zmerať výkonnosť a kvalitu služieb. Operátori využívajú KPI pre zistenie poruchovosti služieb, kedy simulujú plné vyťaženie siete. Pre zaručenie funkčnosti služby pre milióny používateľov sa merajú rôzne kľúčové indikátory v čase.

Dátové aplikácie sú typické služby, využívajúce TCP spojenia, ktoré sú charakterizované variabilnou prenosovou rýchlosťou a toleranciou k nejakej strate a oneskoreniu paketov predtým, ako používateľ spozoruje zníženie kvality služby.

Na to, aby používateľ mohol začať používať niektorú službu, musí byť vytvorený rádiový prístupový bearer (E-RAB). Preto je potrebné zmerať úspešnosť vytvorenia E-RAB. Je potrebné zachytiť pakety uvedené v tabuľke 4.2.1, ktoré budú použité na výpočet úspešnosti vytvorenia rádiového prístupového beareru pomocou KPI.

4.2.1 Úspešnosť vytvorenia E-RAB

Úspešnosť vytvorenia E-RAB vyjadruje pravdepodobnosť, že klient je schopný začať používať službu HTTP.

Všeobecná rovnica:

$$\text{Úspešnosť vytvorenia [\%]} = \frac{\text{počet úspešne vytvorených bearerov}}{\text{počet prijatých pokusov o vytvorenie beareru}} * 100. \quad (4.1)$$

Zachytávané body:

Tab. 4.1: Body pre zachytenie dát na výpočet úspešnosti vytvorenia E-RAB.

Vytvorenie E-RAB	Typ paketu na zachytenie
Pokusy o vytvorenie	Štart: paket obsahujúci žiadosť o vytvorenie
Úspešne vytvorenie	Stop: paket obsahujúci odpoveď na vytvorenie
Neúspešné vytvorenie	Bod stop nebol prijatý

4.3 FTP

Aby boli užívatelia spokojní s FTP, musia byť naplnené určité kritéria. Najskôr musí byť používateľ schopný nadviazať spojenie s FTP serverom v rozumnom čase. Keď sa používateľ pripojí na server, musí byť schopný vytvoriť dátové spojenie v pasívnom či aktívnom režime. Keď je kontrolné a dátové spojenie vytvorené, spoľahlivosť dátového spojenia je veľmi dôležitá. Sťahovanie súboru pri ktorom zlyhá polovica paketov je veľmi otravné pre používateľa, a značne sa tým zvyšuje čas preberania súboru. Toto nás vedie k priepustnosti siete. Všetky oneskorenia a chyby spojenia vedú k zníženiu priepustnosti siete, a taktiež aj aktuálna rýchlosť sťahovania súboru bude znižovať priepustnosť siete. Na meranie kvality prenosu súboru sa používajú KPI.

4.3.1 Miera zlyhania prístupu k FTP službe

Miera zlyhania prístupu k IP službe vyjadruje pravdepodobnosť, že klient nie je schopný nadviazať úspešné TCP/IP spojenie so serverom, a vyžiadať si z neho dáta.

Všeobecná rovnica:

$$\text{Miera zlyhania } [\%] = \frac{\text{neúspešné pokusy o vytvorenie IP spojenia so serverom}}{\text{všetky pokusy o vytvorenie IP spojenia so serverom}} * 100. \quad (4.2)$$

Zachytávané body:

Tab. 4.2: Body pre zachytenie dát na výpočet miery zlyhania prístupu k FTP službe.

Prístup k službe	Typ paketu na zachytenie
Pokusy o prístup k službe	Štart: odoslanie paketu SYN
Úspešne pokusy	Stop: prijatie prvého paketu obsahujúceho žiadaný obsah
Neúspešné pokusy	Bod stop nebol prijatý

4.3.2 Čas vytvorenia IP služby FTP

Čas vytvorenia služby FTP je čas, potrebný na vytvorenie TCP/IP spojenia so serverom, od vyslania počiatočného dotazu na server do vyslania alebo prijatia prvých dát.

Všeobecná rovnica:

$$\text{Čas vytvorenia } [s] = (t_{\text{úspešné vytvorenie služby}} - t_{\text{začiatok vytvárania služby}}). \quad (4.3)$$

Zachytávané body:

Tab. 4.3: Body pre zachytenie dát na výpočet času vytvorenia služby FTP.

Čas vytvorenia služby	Typ paketu na zachytenie
Čas pokusu o vytvorenie služby	Štart: odoslanie prvého paketu SYN
Čas úspešného vytvorenia služby	Stop: prijatie prvého paketu obsahujúceho obsah

4.3.3 Čas FTP relácie

Čas relácie je čas, potrebný na úspešné dokončenie FTP relácie od jej začiatku.

Všeobecná rovnica:

$$\text{Čas relácie [s]} = (t_{\text{koniec relácie}} - t_{\text{začiatok relácie}}). \quad (4.4)$$

Zachytávané body:

Tab. 4.4: Body pre zachytenie dát na výpočet času FTP relácie.

Čas relácie	Typ paketu na zachytenie
Čas úspešného začatia relácie	Štart: odoslanie prvého paketu SYN
Čas dokončenia relácie	Stop: prijatie posledného paketu obsahujúceho dáta

4.3.4 Miera zlyhania FTP relácie

Miera zlyhania relácie vyjadruje pomer nedokončených relácií a úspešne začatých relácií.

Všeobecná rovnica:

$$\text{Miera zlyhania relácie [\%]} = \frac{\text{nedokončené relácie}}{\text{úspešne začaté relácie}} * 100. \quad (4.5)$$

Zachytávané body:

Tab. 4.5: Body pre zachytenie dát na výpočet miery zlyhania FTP relácie.

Zlyhanie relácie	Typ paketu na zachytenie
Úspešne začaté relácie	Štart: odoslanie paketu SYN
Dokončené relácie	Stop: prijatie posledného paketu obsahujúceho žiadaný obsah
Nedokončené relácie	Bod stop nebol prijatý

4.3.5 Miera prerušenia prenosu dát

Miera prerušenia prenosu dát vyjadruje pomer nedokončených dátových prenosov a prenosov, ktoré začali úspešne.

Všeobecná rovnica:

$$\text{Miera prerušenia prenosu } [\%] = \frac{\text{nekompletné prenosy dát}}{\text{úspešne začaté prenosy dát}} * 100. \quad (4.6)$$

Zachytávané body:

Tab. 4.6: Body pre zachytenie dát na výpočet miery prerušenia prenosu dát.

Prerušenie prenosu	Typ paketu na zachytenie
Úspešne začaté relácie	Štart: prijatie prvého súboru s dátami
Kompletné prenosy	Stop: prijatie posledného súboru s dátami
Nekompletné prenosy	Bod stop nebol prijatý

4.3.6 Priemerná rýchlosť sťahovania/nahrávania dát

Tento parameter opisuje priemernú rýchlosť prenosu dát meranú po celú dobu pripojenia k službe. Tento parameter vieme veľmi ľahko zmerať pomocou nástroja Iperf, ktorý dokáže vytvoriť TCP a UDP dátové toky a zmerať priepustnosť siete ktorá dátové toky prenáša.

4.4 HTTP/HTTPS

Niektoré KPI použité pri službe FTP sú použité aj pri tejto službe. V konečnom dôsledku, obe tieto služby zaujíma prenos súborov. Z pohľadu používateľa sú tu určité veci, ktoré vo väčšine prípadov spôsobia zlepšenie zážitku z užívania služby. Niektoré dáta sa načítavajú dlhšiu dobu ako iné. Ak by používateľ mal čakať, pokým sa načítajú všetky dáta stránky (text + obrázky + aplety), a až potom by bola stránka zobrazená, používateľ by určite nebol spokojný so službou. Ak by používateľ uvidel text skôr, a postupne by sa zobrazovali ostatné aspekty stránky, používateľ by bol oveľa spokojnejší.

4.4.1 Miera zlyhania prístupu k HTTP/HTTPS službe

Miera zlyhania prístupu k IP službe vyjadruje pravdepodobnosť, že klient nieje schopný nadviazať úspešné TCP/IP spojenie so serverom, a vyžiadať si z neho dáta.

Všeobecná rovnica:

$$\text{Miera zlyhania } [\%] = \frac{\text{neúspešné pokusy o vytvorenie IP spojenia so serverom}}{\text{všetky pokusy o vytvorenie IP spojenia so serverom}} * 100. \quad (4.7)$$

Zachytávané body:

Tab. 4.7: Body pre zachytenie dát na výpočet miery zlyhania prístupu k službe.

Prístup k službe	Typ paketu na zachytenie
Pokusy o prístup k službe	Štart: odoslanie paketu SYN
Úspešne pokusy	Stop: prijatie prvého paketu obsahujúceho žiadaný obsah
Neúspešné pokusy	Bod stop nebol prijatý

4.4.2 Čas vytvorenia služby HTTP/HTTPS

Čas vytvorenia služby je čas, potrebný na vytvorenie TCP/IP spojenia so serverom, od vyslania počiatočného dotazu na server, do vyslania alebo prijatia prvých dát.

Všeobecná rovnica:

$$\text{Čas vytvorenia } [s] = (t_{\text{úspešné vytvorenie služby}} - t_{\text{začiatok vytvárania služby}}). \quad (4.8)$$

Zachytávané body:

Tab. 4.8: Body pre zachytenie dát na výpočet času vytvorenia služby.

Čas vytvorenia služby	Typ paketu na zachytenie
Čas pokusu o vytvorenie služby	Štart: odoslanie prvého paketu SYN
Čas úspešného vytvorenia služby	Stop: prijatie prvého paketu obsahujúceho obsah

4.4.3 Čas HTTP/HTTPS relácie

Čas relácie je čas, potrebný na úspešné dokončenie HTTP/HTTPS relácie od jej začiatku.

Všeobecná rovnica:

$$\text{Čas relácie [s]} = (t_{\text{koniec relácie}} - t_{\text{začiatok relácie}}). \quad (4.9)$$

Zachytávané body:

Tab. 4.9: Body pre zachytenie dát na výpočet času HTTP/HTTPS relácie.

Čas relácie	Typ paketu na zachytenie
Čas úspešného začatia relácie	Štart: odoslanie prvého paketu SYN
Čas dokončenia relácie	Stop: prijatie posledného paketu obsahujúceho dáta

4.4.4 Miera zlyhania HTTP/HTTPS relácie

Miera zlyhania relácie vyjadruje pomer neúspešne dokončených relácií a úspešne začatých relácií.

Všeobecná rovnica:

$$\text{Miera zlyhania relácie [\%]} = \frac{\text{neúspešné dokončené relácie}}{\text{úspešne začaté relácie}} * 100. \quad (4.10)$$

Zachytávané body:

Tab. 4.10: Body pre zachytenie dát na výpočet miery zlyhania relácie.

Zlyhanie relácie	Typ paketu na zachytenie
Úspešne začaté relácie	Štart: odoslanie paketu SYN
Dokončené relácie	Stop: prijatie paketu FIN
Nedokončené relácie	Bod stop nebol prijatý

4.4.5 Miera prerušenia prenosu dát

Miera prerušenia prenosu dát vyjadruje pomer nedokončených dátových prenosov a prenosov, ktoré začali úspešne.

Všeobecná rovnica:

$$\text{Miera prerušenia prenosu } [\%] = \frac{\text{nekompletné prenosy dát}}{\text{úspešne začaté prenosy dát}} * 100. \quad (4.11)$$

Zachytávané body:

Tab. 4.11: Body pre zachytenie dát na výpočet miery prerušenia prenosu dát.

Prerušenie prenosu	Typ paketu na zachytenie
Úspešne začaté relácie	Štart: prijatie prvého súboru s dátami
Kompletné prenosy	Stop: prijatie paketu FIN
Nekompletné prenosy	Bod stop nebol prijatý

4.4.6 Miera zlyhania vytvorenia TCP/IP spojenia so serverom

Miera zlyhania vytvorenia TCP/IP spojenia vyjadruje pravdepodobnosť, že klient nie je schopný nadviazať úspešné spojenie so serverom.[14]

Všeobecná rovnica:

$$\text{Miera zlyhania } [\%] = \frac{\text{neúspešné pokusy o vytvorenie spojenia so serverom}}{\text{všetky pokusy o vytvorenie TCP/IP spojenia so serverom}} * 100. \quad (4.12)$$

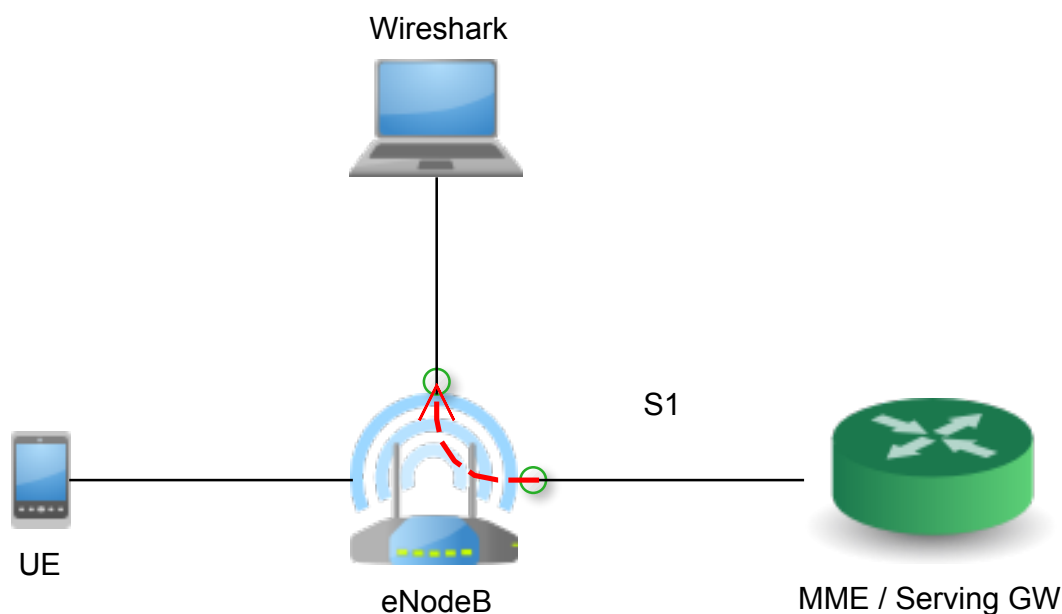
Zachytávané body:

Tab. 4.12: Body pre zachytenie dát na výpočet miery zlyhania vytvorenia spojenia.

Vytvorenie spojenia	Typ paketu na zachytenie
Pokusy o vytvorenie	Štart: odoslanie paketu SYN
Úspešne pokusy	Stop: prijatie potvrdzujúceho paketu ACK
Neúspešné pokusy	Bod stop nebol prijatý

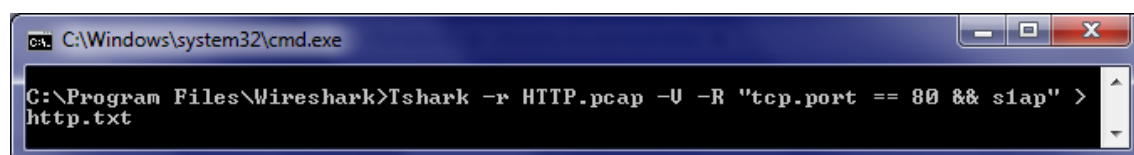
5 ANALÝZA DÁTOVEJ KOMUNIKÁCIE

Analýza bola uskutočnená na poskytnutých dátach zo siete LTE, kedy rozhranie S1 bolo mirorované a dáta boli odchytené pomocou programu Wireshark, ako môžete vidieť na obrázku 5.1.



Obr. 5.1: Port mirroring.

Z takto odchytených dát sa vyfiltrovala len HTTP/HTTPS komunikácia spolu so s1 aplikačným protokolom (slap) pomocou programu Tshark, čo je terminálová verzia Wiresharku. Na vyfiltrovanie žiadanej komunikácie bol použitý príkaz, ktorý je zobrazený na obrázku 5.2. Výstupom tohto filtra je textový súbor, v ktorom sú jednotlivé rámce oddelené prázdny riadkom.



Obr. 5.2: Filtrovanie HTTP komunikácie a protokolu slap.

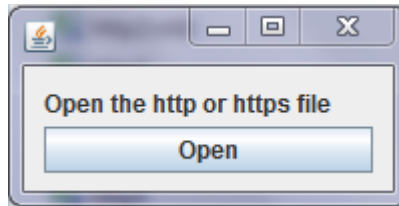
Textový súbor sa následne vložil do vytvoreného programu, ktorý spočítal a vypísal potrebné parametre pre výpočet KPI. Program bol napísaný v programovacom jazyku Java. Vstupný textový súbor musí obsahovať vo svojom názve text **http** alebo **https**, aby naň program vedel aplikovať určené pravidlá.

```

if (fileName.contains("https"))
    gethttpsstats(br);
else
    getHttpstats(br);

```

Výstupom tohto programu je súborový formát (.csv), ktorý sa uloží do zložky, z ktorej bol vybraný vstupný textový súbor. Výstupný súbor sa následne otvoril v tabuľkovom editore MS Excel za účelom dopočítania KPI a vyhodnotenia dát.



Obr. 5.3: Grafické rozhranie programu.

5.1 Chybové stavy

Najväčším nepriateľom kvality služieb sú chybové stavy. So zväčšujúcim sa vytážením siete narastá počet chybových stavov a tým sa zväčšuje oneskorenie siete a samozrejme klesá kvalita ponúkaných služieb.

Chybové situácie môžeme rozdeliť na situácie spôsobené vlastnou mobilnou sieťou a situácie mimo vlastnej mobilnej siete.

1. Chybové situácie spôsobené vlastnou mobilnou sieťou

Z pohľadu používateľa sa chyby spôsobené vlastnou mobilnou sieťou prejavia znemožnením prístupu používateľa k jeho službám. Chyba môže nastať pri vytváraní E-RAB. Pokiaľ nebude EPS bearer vytvorený, používateľ nebude môcť vytvoriť spojenie s webovým serverom. Na zistenie tejto chyby môžeme použiť nástroj Traceroute, ktorý nám zobrazí odozvy všetkých smerovačov, ktoré dáta smerovali. V prípade nevytvorenia E-RAB, nám Traceroute nezobrazí odozvu ani z jedného zariadenia, cez ktoré bol paket smerovaný. Pokiaľ poznáme sieťovú konfiguráciu prvkov v sieti, vieme bližšie špecifikovať, na ktorom zariadení nastala chyba a ďalej ju bližšie identifikovať. V prípade, že EPS bearer je vytvorený, z zachádza sa s ním podľa pravidiel prijatých od PCFR.

2. Chybové situácie spôsobené mimo vlastnej mobilnej siete

V prípade, že EPS bearer bol vytvorený, nemala by v používateľovej sieti nastať chyba. Za predpokladu, že po vytvorení EPS beareru dáta úspešne opustia sieť LTE, budú smerované cez internet na webový server. Počas smerovania dát môže dôjsť k výpadku určitej trasy alebo k jej preťaženiu. To môže spôsobiť, že dáta sú buď zahodené alebo doručené s oneskorením, pretože protokol IP negarantuje správne doručenie dát. V prípade straty dát sú dáta znova preposielané. Lokalizovať chybový stav mimo vlastnej mobilnej siete je veľmi obtiažne, pretože dáta môžu byť smerované mnohými smermi. Používateľ môže použiť nástroj Traceroute, ktorý nám zobrazí odozvy všetkých smerovačov, ktoré smerovali dáta.

6 VYHODNOTENIE DÁTOVEJ KOMUNIKÁCIE

Na vyhodnotenie služby HTTP využijem KPI popísané v kapitole 4.2.

6.0.1 Úspešnosť vytvorenia E-RAB

Úspešnosť vytvorenia E-RAB vyjadruje pravdepodobnosť, že klient je schopný začať používať službu HTTP.

Rovnice výpočtu:

$$\text{Úspešnosť vytvorenia } [\%] = \frac{\text{počet úspešne vytvorených bearerov}}{\text{počet všetkých pokusov o vytvorenie beareru}} * 100, \quad (6.1)$$

$$\text{Úspešnosť vytvorenia} = \frac{24}{24} * 100 = 100\%. \quad (6.2)$$

Ako **pokus o vytvorenie beareru** bol počítaný paket, ktorý obsahoval text **Initial Context Setup Request**, teda paket so žiadosťou o vytvorenie E-RAB.

Za **úspešne vytvorený bearer** sa považoval prijatý paket, ktorý obsahoval text **Initial Context Setup Response**, teda paket potvrdzujúci vytvorenie E-RAB.

Úspešnosť vytvorenia beareru je 100%. Z toho vyplýva, že v sieti prevádzkovateľa nenastala chyba pri vytváraní beareru.

6.1 HTTP

6.1.1 Čas vytvorenia IP služby HTTP

Čas vytvorenia služby HTTP je čas (medián), potrebný na vytvorenie TCP/IP spojenia so serverom, od vyslania počiatočného dotazu na server do vyslania alebo prijatia prvých dát.

Dátová komunikácia bola zachytávaná približne 30 minút. Predpokladá sa, že prevádzkovateľ siete bude monitorovať a vyhodnocovať sieť po celý deň, a preto je vhodné rozdeliť komunikáciu na časové úseky. V tomto prípade sa kvôli krátkemu zachytávanému úseku komunikácia rozdelila na 2 časové úseky po 15 minútach.

Pri výpočtoch sa vychádzalo z rovnice 4.8.

Výpočet pre interval 0 až 15 minút:

$$\text{Čas vytvorenia služby} = 38,08 \text{ ms.} \quad (6.3)$$

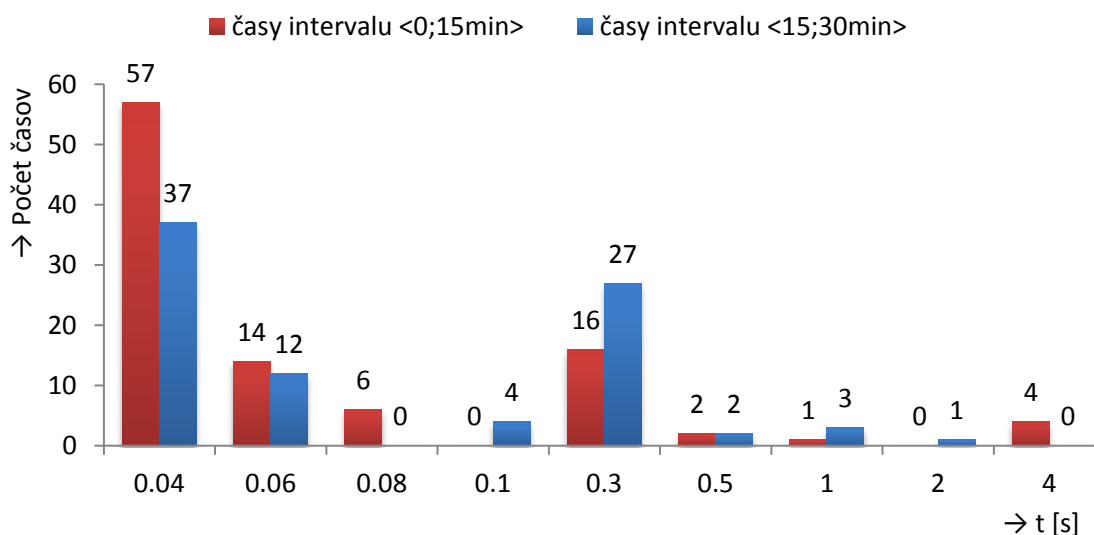
Výpočet pre interval 15 až 30 minút:

$$\text{Čas vytvorenia služby} = 43,15 \text{ ms.} \quad (6.4)$$

Ako bod Štart sa vyhladal paket, ktorý obsahoval text **Flags: 0x002 (SYN)** a zároveň text **Destination port: http (80)** teda paket, ktorý žiada o vytvorenie TCP/IP spojenia so serverom. V tomto pakete sa našla položka **Arrival Time**, ktorá sa následne vypísala spolu s číslom zdrojového portu.

Ako bod Stop sa vyhladal paket, ktorý obsahoval text **Request Method: GET**, takže aj všetky ostatné typy HTTP žiadostí. Tento paket žiada zaslanie konkrétneho webového obsahu zo serveru. Následne sa našla položka **Arrival Time**, ktorá sa vypísala spolu s cieľovým portom. V prípade, že takýto paket nebol zachytený, použije sa na výpočet čas prvého paketu, ktorý obsahuje text **Status Code.u**

Na obrázku 6.1 je vidieť histogram časových úsekov vytvorenia služby HTTP. Z týchto dát môže prevádzkovateľ alebo používateľ siete zhodnotiť, aký časový okamžik musí užívateľ najčastejšie čakať do vyslania prvých dát na webový server.



Obr. 6.1: Histogram časových úsekov vytvorenia služby HTTP

6.1.2 Čas HTTP relácie

Čas (medián) relácie je čas, potrebný na úspešné dokončenie HTTP relácie od jej začiatku.

Tak isto ako v sekcii 6.1.1, bola komunikácia rozdelená na dva časové úseky, ktoré reprezentujú rôzne časové úseky, ktoré si prevádzkovateľ môže žiadať analyzovať.

Pri výpočtoch sa vychádzalo z rovnice 4.9.

Výpočet pre interval 0 až 15 minút:

$$\text{Čas relácie} = 0,274 \text{ s.} \quad (6.5)$$

Výpočet pre interval 15 až 30 minút:

$$\text{Čas relácie} = 0,153 \text{ s.} \quad (6.6)$$

Ako bod Štart sa vyhladal paket, ktorý obsahoval text **Flags: 0x002 (SYN)** a zároveň text **Destination port: http (80)** teda paket, ktorý žiada o vytvorenie TCP/IP spojenia so serverom. V tomto pakete sa našla položka **Arrival Time**, ktorá sa následne vypísala spolu s číslom zdrojového portu.

Ako bod Stop sa vyhladal posledný paket, ktorý obsahoval text **Status Code**. Je to paket, ktorý obsahuje odpoveď od HTTP serveru a žiadané dáta. Následne sa v ňom našla položka **Arrival Time**, ktorá sa vypísala spolu s číslom cieľového portu.

Na obrázku 6.2 je zobrazený histogram časových úsekov potrebných na úspešné načítanie stránky. Z týchto údajov môžeme vyčítať, za aký čas sa používateľovi najčastejšie zobrazí žiadaný webový obsah, nehladiac na veľkosť načítaného obsahu.

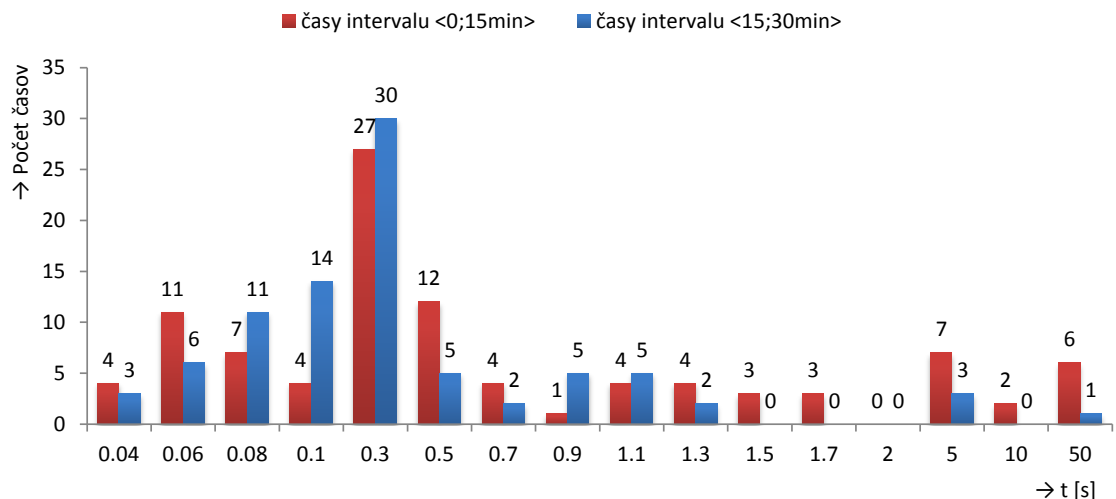
6.1.3 Miera zlyhania prístupu k HTTP službe

Miera zlyhania prístupu k IP službe vyjadruje pravdepodobnosť, že klient nie je schopný nadviazať úspešné TCP/IP spojenie so serverom a vyžiadať si z neho dáta.

Rovnice výpočtu:

$$\text{Miera zlyhania [\%]} = \frac{\text{neúspešné pokusy o vytvorenie IP spojenia so serverom}}{\text{všetky pokusy o vytvorenie IP spojenia so serverom}} * 100, \quad (6.7)$$

$$\text{Miera zlyhania prístupu k službe} = \frac{205-188}{224} * 100 = \frac{17}{224} * 100 = 7,59\%. \quad (6.8)$$



Obr. 6.2: Histogram časových úsekov HTTP relácie.

Ako **všetky pokusy o vytvorenie IP spojenia so serverom** sa počítali pakety, ktoré obsahovali text **Flags: 0x002 (SYN)** a zároveň text **Destination port: http (80)**. Sú to pakety, ktoré žiadajú o vytvorenie TCP/IP spojenia so serverom. Všetky nájdené pakety tohto typu sa sčítali.

Neúspešné pokusy o vytvorenie IP spojenia so serverom sa vypočítali rozdielom počtu ukončených spojení a počtu úspešne dokončených spojení, čo znamená, že sme dostali počet chýb, ktoré vznikli v dôsledku neprijatia odpovede od HTTP serveru (OK).

V komunikácii ako prvý ukončuje spojenie klient, no môže nastať situácia, kedy klient hneď po prijatí všetkých dát od webového serveru neukončí spojenie, ale nechá toto spojenie otvorené pre ďalšie prípadné žiadosti. Preto sú na webových serveroch často nastavené časové intervaly, počas ktorých ak klient nevyšle žiadosť o webový obsah, tak server toto spojenie automaticky ukončí, a preto sa za ukončenie spojenia považoval paket, ktorý obsahoval text **Flags: 0x011 (FIN, ACK)** a zároveň text **Source port: http (80)**.

Úspešne dokončené spojenie je spojenie, ktoré obsahuje celú úspešnú komunikáciu – teda žiadosť o vytvorenie TCP/IP spojenia (SYN), žiadosť o zaslanie webového obsahu (GET) alebo prvá odpoveď od HTTP serveru (OK), posledná odpoveď od HTTP serveru (OK) a žiadosť o ukončenie spojenia (FIN).

6.1.4 Miera zlyhania HTTP relácie

Miera zlyhania relácie vyjadruje pomer neúspešne dokončených relácií a relácií, ktoré začali úspešne.

Rovnice výpočtu:

$$\text{Miera zlyhania relácie [\%]} = \frac{\text{neúspešne dokončené relácie}}{\text{úspešne začaté relácie}} * 100, \quad (6.9)$$

$$\text{Miera zlyhania relácie} = \frac{224-188-17}{224} = \frac{19}{224} * 100 = 8,48\%. \quad (6.10)$$

Ako **úspešne začatá relácia** sa počítala komunikácia, keď klient vyslal žiadosť o vytvorenie TCP/IP spojenia a server vyslal potvrdenie vytvorenia spojenia. Pre žiadosť o vytvorenie spojenia paket obsahoval text **Flags: 0x002 (SYN)** a zároveň text **Destination port: http (80)**. Pre potvrdenie vytvorenia spojenia paket obsahoval text **Flags: 0x012 (SYN, ACK)** a zároveň text **Source port: http (80)** s predpokladom, že posledné potvrdenie (ACK) klient poslal.

Neúspešné dokončené relácie boli počítané rozdielom počtu úspešne začatých relácií, počtu úspešne dokončených spojení a počtu neúspešných pokusov o vytvorenie IP spojenia so serverom. To znamená, že od počtu úspešne nadviazaných TCP spojení sa odpočítali všetky úspešne dokončené spojenia a počet chýb, ktoré vznikli v dôsledkom neprijatia odpovede od HTTP serveru (OK). Výsledkom je počet chýb, ktoré vznikli v dôsledku neukončenia spojenia.

6.1.5 Miera prerušenia prenosu dát

Miera prerušenia prenosu dát vyjadruje pomer nedokončených dátových prenosov a prenosov, ktoré začali úspešne.

Rovnice výpočtu:

$$\text{Miera prerušenia prenosu [\%]} = \frac{\text{nekompletné prenosy dát}}{\text{úspešne začaté prenosy dát}} * 100, \quad (6.11)$$

$$\text{Miera prerušenia prenosu [\%]} = \frac{224-188-17}{224-17} * 100 = 9,18\%. \quad (6.12)$$

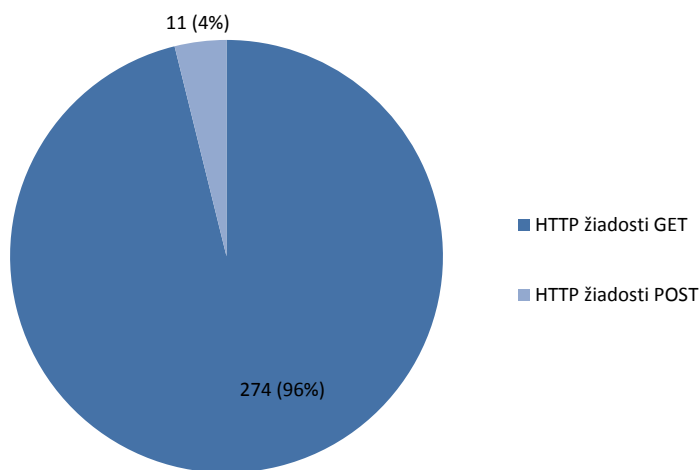
Úspešne začaté prenosy sa vypočítali rozdielom úspešne začatých spojení a neúspešných pokusov o vytvorenie IP spojenia so serverom, čím sme dostali počet

úspešných prijatí odpovedí zo serveru.

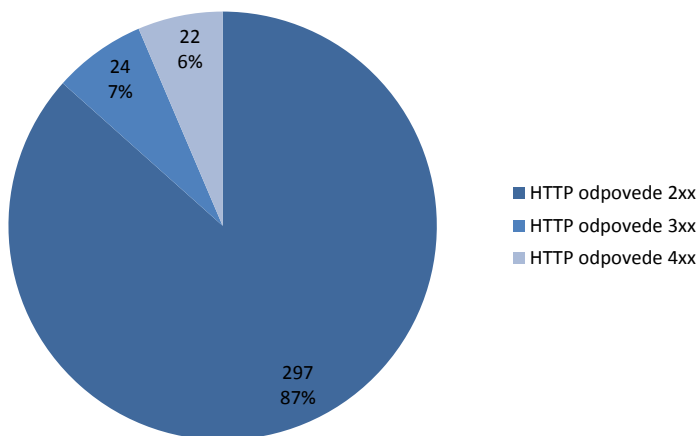
Nekompletné prenosy dát sa vypočítali rozdielom počtu úspešne začatých relácií a počtu ukončených relácií s predpokladom, že relácia ešte nebola ukončená z dôvodu neúplného načítania webovej stránky.

6.1.6 Množstvo vyslaných HTTP žiadostí a odpovedí

V grafoch 6.3 a 6.4 vidieť rôznorodosť všetkých vyslaných typov HTTP žiadostí na webový server a všetkých vyslaných typov HTTP odpovedí používateľovi.



Obr. 6.3: Graf HTTP žiadostí podľa typov.

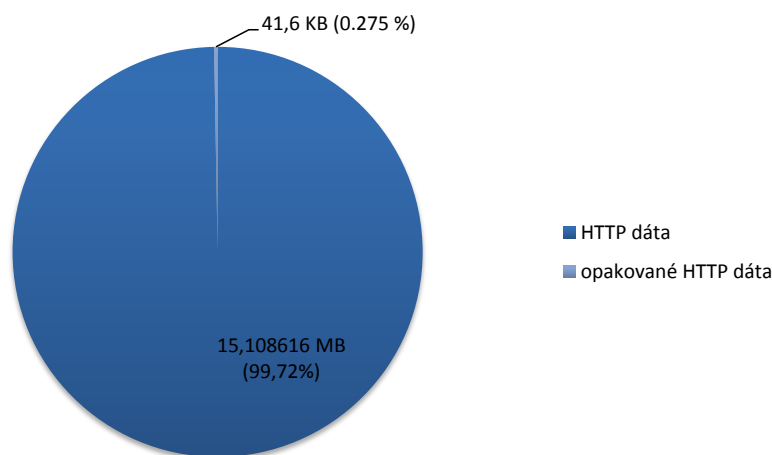


Obr. 6.4: Graf HTTP odpovedí podľa typov.

6.1.7 Množstvo opakovaných dát

Množstvo opakovaných dát udáva počet dát, ktoré bolo treba znovu či už na webový server alebo používateľovi preposlať.

Počas HTTP komunikácie sa prenieslo celkovo 15,1 MB dát, pričom 41,6 kB tvorilo opakovane preposielané HTTP dáta. Na obrázku 6.5 vidieť percentuálne vyjadrenie počtu opakovane preposielaných dát.



Obr. 6.5: Graf pomeru opakovaných a všetkých HTTP dát.

6.2 Vyhodnotenie HTTP komunikácie

Na začiatku komunikácie je potrebné vytvoriť E-RAB. V nami testovanej sieti bola úspešnosť vytvorenia 100% a teda nenastala žiadna chyba pri jeho vytváraní. Následne používateľ zadá žiadanú webovú stránku do webového prehliadača. Nastane vytvorenie TCP/IP spojenia s webovým serverom a používateľ vyšle HTTP žiadosť (GET) na webový server. Pokiaľ všetko prebehne v poriadku, klient začne prijímať žiadaný webový obsah zo serveru. Po vypočítaní príslušného KPI som zistil, že v 7,59% prípadov si klient nebol schopný vyžiadať webový obsah zo serveru. Tieto chybné situácie majú negatívny dopad na používateľa, pretože predlžujú čas potrebný na zobrazenie potrebnej informácie. V 8,48% prípadov klient úspešne nadviazať TCP/IP spojenie so serverom, no neúspešne dokončil preberanie webového obsahu a v 9,13% prípadov klient úspešne začal preberať webový obsah no preberanie nedokončil. Tieto chybové situácie nepôsobia na používateľa negatívne, pretože si ich používateľ pravdepodobne spôsobil sám. Keď sa používateľovi zobrazili potrebné informácie, nečakal na celkové načítanie obsahu a hneď webový prehliadač zatvoril alebo si vyžiadala inú webovú stránku. To znamená, že relácia nebola úspešne

ukončená, no používateľ dostal hľadanú informáciu. Celková veľkosť HTTP dát bola 15,15 MB, z toho 41,6 kB dát bolo opakovane prenesených. Dáta boli zachytené na nevyťaženej sieti, tzn. že na celej sieti komunikovalo len jedno používateľské zariadenie.

V dôsledku toho usudzujem, že vzniknuté chybové stavy boli spôsobené mimo testovanú LTE sieť.

Z histogramu 6.1 je vidieť, že používateľ mohol najčastejšie žiadať o webový obsah za 40 ms od začatia komunikácie. Tiež môžeme vyčítať, že v niektorých ojedinelých prípadoch, mohol používateľ začať žiadať o webový obsah v rozmedzí 1 až 4 s. Tieto chyby sú spôsobené vplyvom vyťaženia webového serveru.

Následne z histogramu 6.2 je vidieť, že kompletný webový obsah bol najčastejšie načítaný za 60 ms až 0,5 s v závislosti od veľkosti žiadanej stránky. Taktiež tu môžeme vyčítať, že v niektorých prípadoch bol kompletný webový obsah načítaný v rozmedzí 10 až 50 s. Tieto hodnoty sú spôsobené tým, že používateľ si vyžiadal určitý webový obsah, napr. stránku s IT novinkami, no po jeho prijatí neukončil spojenie. Používateľ si prečítal potrebné informácie a následne klikol na ďalšiu záložku na stránke, čím si vyžiadal ďalší webový obsah na rovnakom spojení. V dôsledku tohto bol posledný paket s webovým obsahom zaslaný v neskorom čase. Preto tieto údaje nepovažujem za chybu spôsobenú vplyvom chybnej situácie na sieti. Prevádzkovateľa siete zaujímajú najviac údaje v čase najväčšieho zataženia jeho siete, teda v čase najväčšieho počtu pripojených používateľov do siete. Preto som časové údaje rozdelil v tabuľkovom editore na intervaly, ktoré simulujú vyťaženie siete v rôznych časoch.

6.3 HTTPS

Protokol HTTPS využíva na prenos údajov protokol HTTP, no prenášané dáta sú zabezpečené protokolom SSL alebo TLS. Preto nebolo možné vyčítať zo zachytených údajov, či sa jedná o HTTP žiadosť alebo odpoveď, preto sa všetky KPI vypočítali s predpokladom, že paket obsahujúci text `Content Type: Application Data` a text `Destination port: https (443)` je paket s HTTP žiadosťou, a paket obsahujúci text `Content Type: Application Data` a text `Source port: https (443)` je paket s HTTP odpoveďou.

6.3.1 Čas vytvorenia IP služby HTTPS

Čas vytvorenia služby je čas (medián) potrebný na vytvorenie TCP/IP spojenia so serverom, od vyslania počiatočného dotazu na server do vyslania alebo prijatia prvých dát.

Podobne ako v sekcii 6.1.1 bola komunikácia rozdelená na časové úseky. Pri výpočtoch sa vychádzalo z rovnice 4.8

Výpočet pre interval 0 až 15 minút:

$$\text{Čas vytvorenia služby} = 193,3 \text{ ms.} \quad (6.13)$$

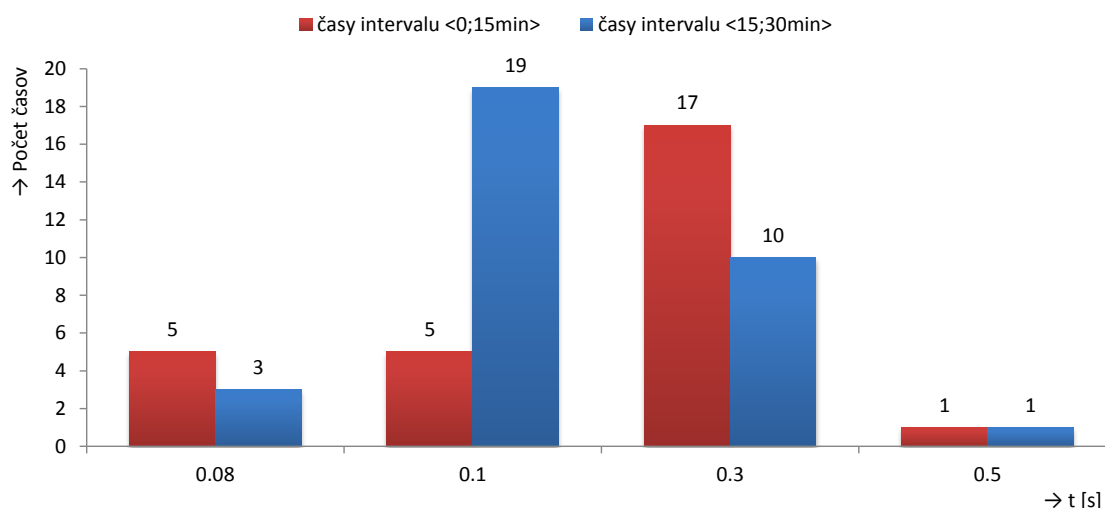
Výpočet pre interval 15 až 30 minút:

$$\text{Čas vytvorenia služby} = 90,2 \text{ ms.} \quad (6.14)$$

Ako bod Štart sa vyhladal paket, ktorý obsahoval text **Flags: 0x002 (SYN)** a zároveň text **Destination port: http (80)** teda paket, ktorý žiada o vytvorenie TCP/IP spojenia so serverom. V tomto pakete sa našla položka **Arrival Time**, ktorá sa následne vypísala spolu s číslom zdrojového portu.

Ako bod Stop sa vyhladal paket, ktorý obsahoval text **Content Type: Application Data** a text **Destination port: http (443)**. Tento paket žiada zaslanie konkrétneho webového obsahu zo serveru. Následne sa našla položka **Arrival Time**, ktorá sa vypísala spolu s cieľovým portom. V prípade, že takýto paket nebol zachytený, použije sa na výpočet čas prvého paketu, ktorý obsahuje text **Content Type: Application Data** a text **Source port: https (443)**.

Na obrázku 6.6 vidieť histogram časových úsekov vytvorenia služby HTTPS. Z týchto dát môže prevádzkovateľ alebo používateľ siete zhodnotiť, aký časový okamžik musí užívateľ najčastejšie čakať do vyslania prvých dát na webový server.



Obr. 6.6: Histogram časových úsekov vytvorenia služby HTTPS

6.3.2 Čas HTTPS relácie

Čas relácie je čas (medián) potrebný na úspešné dokončenie HTTPS relácie od jej začiatku.

Tak isto ako v sekcii 6.3.1, bola komunikácia rozdelená na dva časové úseky, ktoré reprezentujú rôzne časové úseky.

Pri výpočtoch sa vychádzalo z rovnice 4.9

Výpočet pre interval 0 až 15 minút:

$$\text{Čas relácie} = 0,305 \text{ s.} \quad (6.15)$$

Výpočet pre interval 15 až 30 minút:

$$\text{Čas relácie} = 0,238 \text{ s.} \quad (6.16)$$

Ako bod Štart sa vyhladal paket, ktorý obsahoval text **Flags: 0x002 (SYN)** a zároveň text **Destination port: http (80)** teda paket, ktorý žiada o vytvorenie TCP/IP spojenia so serverom. V tomto pakete sa našla položka **Arrival Time**, ktorá sa následne vypísala spolu s číslom zdrojového portu.

Ako bod Stop sa vyhladal posledný paket, ktorý obsahoval text **Content Type: Application Data** a text **Source port: https (443)**. Je to paket, ktorý obsahuje odpoveď od HTTP serveru a žiadané dáta. Následne sa v ňom našla položka **Arrival Time**, ktorá sa vypísala spolu s číslom cieľového portu.

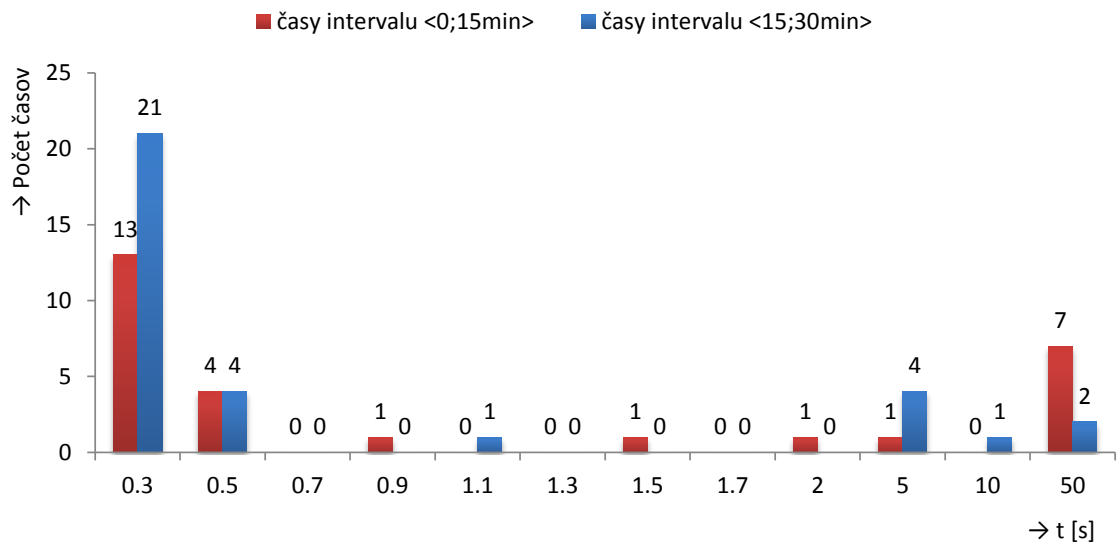
Na obrázku 6.7 je zobrazený histogram časových úsekov potrebných na úspešné načítanie stránky. Z týchto údaj môžeme vyčítať, za aký čas sa používateľovi najčastejšie zobrazí žiadaný webový obsah, nehladiac na veľkosť načítaného obsahu.

6.3.3 Miera zlyhania prístupu k HTTPS službe

Miera zlyhania prístupu k IP službe vyjadruje pravdepodobnosť, že klient nie je schopný nadviazať úspešné TCP/IP spojenie so serverom a vyžiadať si z neho dáta.

Rovnice výpočtu:

$$\text{Miera zlyhania } [\%] = \frac{\text{neúspešné pokusy o vytvorenie IP spojenia so serverom}}{\text{všetky pokusy o vytvorenie IP spojenia so serverom}} * 100, \quad (6.17)$$



Obr. 6.7: Histogram časových úsekov HTTPS relácie.

$$\text{Miera zlyhania} = \frac{69-63}{79} * 100 = \frac{6}{79} * 100 = 7,59\%. \quad (6.18)$$

Ako **všetky pokusy o vytvorenie IP spojenia so serverom** sa počítali pakety, ktoré obsahovali text **Flags: 0x002 (SYN)** a zároveň text **Destination port: http (80)**. Sú to pakety, ktoré žiadajú o vytvorenie TCP/IP spojenia so serverom. Všetky nájdené pakety tohto typu sa sčítali.

Neúspešné pokusy o vytvorenie IP spojenia so serverom sa vypočítali rozdielom počtu ukončených spojení a počtu úspešne dokončených spojení, čo znamená, že sme dostali počet chýb, ktoré vznikli v dôsledku neprijatia odpovede od HTTPS serveru (OK).

V komunikácii ako prvý ukončuje spojenie klient, no môže nastať situácia, kedy klient hneď po prijatí všetkých dát od webového serveru neukončí spojenie, ale nechá toto spojenie otvorené pre ďalšie prípadné žiadosti. Preto sú na webových serveroch často nastavené časové intervaly, počas ktorých ak klient nevyšle žiadosť o webový obsah, tak server toto spojenie automaticky ukončí. Preto sa za ukončenie spojenia považoval paket, ktorý obsahoval text **Flags: 0x011 (FIN, ACK)** a zároveň text **Source port: http (80)**.

Úspešne dokončené spojenie je spojenie, ktoré obsahuje celú úspešnú komunikáciu – žiadosť o vytvorenie TCP/IP spojenia (SYN), žiadosť o zaslanie webového obsahu (GET) alebo prvá odpoveď od HTTPS serveru (OK), posledná odpoveď od HTTPS serveru (OK) a žiadosť o ukončenie spojenia (FIN).

6.3.4 Miera zlyhania HTTPS relácie

Miera zlyhania relácie vyjadruje pomer neúspešne dokončených relácií a relácií, ktoré začali úspešne.

Rovnice výpočtu:

$$\text{Miera zlyhania relácie [\%]} = \frac{\text{neúspešne dokončené relácie}}{\text{úspešne začaté relácie}} * 100, \quad (6.19)$$

$$\text{Miera zlyhania relácie} = \frac{79-63-6}{79} = \frac{10}{79} * 100 = 12,66\%. \quad (6.20)$$

Ako **úspešne začatá relácia** sa počítala komunikácia, kedy klient vyslal žiadosť o vytvorenie TCP/IP spojenia a server vyslal potvrdenie vytvorenia spojenia. Pre žiadosť o vytvorenie spojenia paket obsahoval text **Flags: 0x002 (SYN)**, ako aj text **Destination port: http (80)**. Pre potvrdenie vytvorenia spojenia paket obsahoval text **Flags: 0x012 (SYN, ACK)** a zároveň text **Source port: http (80)** s predpokladom, že posledné potvrdenie klient poslal.

Neúspešné dokončené relácie sa vypočítali rozdielom počtu úspešne začatých relácií, počtu úspešne dokončených spojení a počtu neúspešných pokusov o vytvorenie IP spojenia so serverom. To znamená, že sme od počtu úspešne nadviazaných TCP spojení odpočítali všetky úspešne dokončené spojenia a počet chýb, ktoré vznikli v dôsledku neprijatia odpovede od HTTPS serveru (OK). Výsledkom je počet chýb, ktoré vznikli v dôsledku neukončenia spojenia.

6.3.5 Miera prerušenia prenosu dát

Miera prerušenia prenosu dát vyjadruje pomer nedokončených dátových prenosov a prenosov, ktoré začali úspešne.

Rovnice výpočtu:

$$\text{Miera prerušenia prenosu [\%]} = \frac{\text{nekompletné prenosy dát}}{\text{úspešne začaté prenosy dát}} * 100, \quad (6.21)$$

$$\text{Miera prerušenia prenosu [\%]} = \frac{79-63-6}{79-6} * 100 = 13,7\%. \quad (6.22)$$

Úspešne začaté prenosy sa vypočítali rozdielom úspešne začatých spojení a neúspešných pokusov o vytvorenie IP spojenia so serverom, čím sme dostali počet úspešne prijatých odpovedí zo serveru.

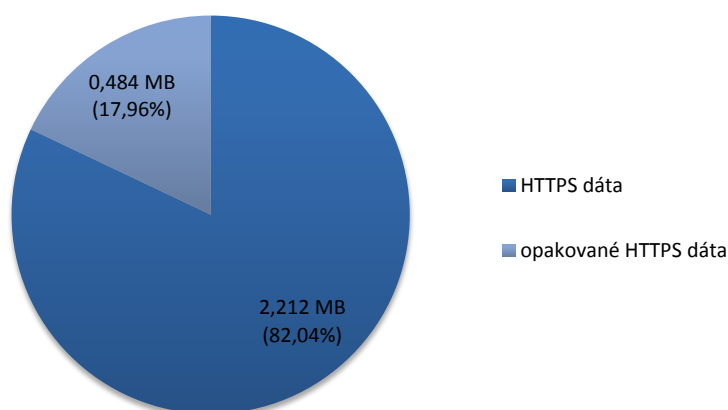
Nekompletné prenosy dát sa vypočítali rozdielom počtu úspešne začatých relácií a počtu ukončených relácií s predpokladom, že relácia ešte nebola ukončená z dôvodu neúplného načítania webovej stránky.

6.3.6 Množstvo opakovaných dát

Množstvo opakovaných dát udáva počet dát, ktoré bolo treba znovu preposlať na webový server alebo používateľovi.

Počas HTTPS komunikácie sa prenieslo celkovo 2,697 MB dát, pričom 0,484 MB tvorilo opakovane preposielané HTTPS dáta.

Na obrázku 6.8 je vidieť percentuálne vyjadrenie počtu opakovane preposielaných dát.



Obr. 6.8: Graf pomeru opakovaných a všetkých HTTPS dát.

6.4 Vyhodnotenie HTTPS komunikácie

Pri počítaní KPI pre službu HTTPS sa použili rovnaké vzorce ako pri službe HTTP. Kvôli šifrovaniu HTTP dát pomocou protokolu SSL/TSL som nedokázal určiť, či sa jedná o HTTP žiadosť alebo odpoveď. Pracoval som len s predpokladom, že pokiaľ paket obsahuje text `Content Type: Application Data` a text `Destination port: https (443)`, jedná sa HTTP žiadosť a v prípade `Source port: https (443)` sa jedná o HTTP odpoveď. Z vypočítaných KPI som zistil, že v 7,59% prípadov si klient nebol schopný vyžiadať webový obsah zo serveru. Ako už bolo spomínané v sekcii 6.2, tieto chyby negatívne vplývajú na používateľa, pretože predlžujú čas potrebný na zobrazenie potrebnej informácie. V 12,66% prípadov klient úspešne nadviazal TCP/IP spojenie so serverom, no neúspešne dokončil preberanie webového obsahu,

a v 13,7% prípadov klient úspešne začal preberať webový obsah, ale preberanie nedokončil. Tieto chybové situácie nepôsobia na používateľa negatívne, pretože si ich používateľ pravdepodobne spôsobil sám. V tomto prípade viem, že dodané odchytané dáta obsahovali aj Youtube komunikáciu. Youtube už v dnešnej dobe používa na prenos údajov službu HTTPS, preto usudzujem, že väčšina týchto chybových situácií bola spôsobená tým, že používateľ nedopozeral video do konca a tým pádom relácia nebola úspešne dokončená. Celková veľkosť HTTPS dát bola 2,7 MB, z toho 0,48 MB dát bolo opakovane prenesených. V porovnaní so službou HTTP, kde opakovane prenesené dáta tvoria len 0,275% z celkových HTTP dát, pri službe HTTPS opakovane prenesené dáta tvoria až 18% z celkových HTTPS dát. Z dôvodu zašifrovania HTTPS dát nebolo možné zistiť, aké dáta boli opakovane prenášané. Dáta boli zachytené na nevyťaženej sieti, tzn. že na celej sieti komunikovalo len jedno používateľské zariadenie. V dôsledku toho usudzujem, že vzniknuté chybové stavy boli spôsobené mimo testovanú LTE sieť.

Z histogramu 6.6 je vidieť, že najčastejšie mohol používateľ žiadať o webový obsah za 100 ms až 300 ms od začatia komunikácie. Porovnaním s dobou 40 ms pri službe HTTP, táto dlhšia doba je spôsobená tým, že pred zahájením komunikácie prebieha nastavenie šifrovania, autentizácia a výmena kľúčov medzi klientom a serverom. Následne z histogramu 6.7 je vidieť, že kompletný webový obsah bol najčastejšie načítaný za 300 ms až 500 ms v závislosti od veľkosti žiadanej stránky. Taktiež tu môžeme vyčítať, že v niektorých prípadoch bol kompletný webový obsah načítaný v rozmedzí 10s až 50 s. Tieto hodnoty sú spôsobené rovnakou situáciou ako pri službe HTTP, kedy používateľ nechá spojenie aj po prijatí všetkých dát otvorené kvôli ďalšej žiadosti o webový obsah. Takto vznikajú relácie, ktoré obsahujú aj časové údaje nečinnosti používateľa. Preto tieto údaje nepovažujem za chybu spôsobenú vplyvom chybnej situácie na sieti. Prevádzkovateľa siete zaujímajú najviac údaje v čase najväčšieho zaťaženia jeho siete, teda v čase najväčšieho počtu pripojených používateľov do siete, a preto som časové údaje rozdelil v tabuľkovom editore na intervaly, ktoré simulujú vyťaženie siete v rôznych časoch.

7 ZÁVER

V tomto dokumente som opísal problematiku sietí LTE. LTE siete sú čoraz viac ponúkaným spôsobom pripojenia do internetu pre mobilné zariadenia. Definoval som všetky potrebné zariadenia a ich funkcie pre realizáciu mobilných služieb. Zameriaval som sa na užívateľskú rovinu v častiach E-UTRAN a EPC a ich protokolovú výbavu. Detailne som popísal realizáciu bežných služieb v sieti LTE, ako je prehliadanie webových stránok, sťahovanie súborov, prístup k elektronickej pošte či sledovanie streamovaného videa. Navrhol som kľúčové indikátory výkonnosti (KPI), ktoré hodnotia sieť z hľadiska realizovaných služieb. Vytvoril som program, ktorý vypíše a spočíta všetky potrebné údaje na výpočet KPI pre službu HTTP a HTTPS. Program som aplikoval na poskytnutú vzorku dátovej komunikácie. Vypočítal som všetky navrhnuté KPI a následne som sieť zhodnotil po kvalitatívnej stránke.

LITERATÚRA

- [1] SESIA, S., TOUFIK, I., BAKER, M. *LTE – The UMTS Long Term Evolution: From Theory to Practice*. Velká Británie: John Wiley & Sons, Ltd., 2009. ISBN: 978-0-470-69716-0.
- [2] LESCUYER, P., LUCIDARME, T. *Evolved Packet System: The LTE and SAE Evolution of 3G UMTS*. Velká Británie: John Wiley & Sons, Ltd., 2008. ISBN: 978-0-470-05976-0.
- [3] SIGLIN, T. *HTTP Streaming: What You Need to Know*. Citované 15.5.2014. Online: <http://www.streamingmedia.com/Articles/Editorial/Featured-Articles/HTTP-Streaming-What-You-Need-to-Know-65749.aspx>.
- [4] FIRMIN, F. *The Evolved Packet Core*. Citované 19.11.2013. Online: <http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core>.
- [5] Basir, A. *Quality of Service (QoS) in LTE*. Uverejnené 31.1.2013, citované 3.11.2013. Online: <http://4g-lte-world.blogspot.cz/2013/01/quality-of-service-qos-in-lte.html>.
- [6] Basir, A. *Default Bearer, Dedicated Bearer... What exactly is bearer ?*. Uverejnené 20.5.2012, citované 3.11.2013. Online: <http://4g-lte-world.blogspot.cz/2012/05/default-bearer-dedicated-bearer-what.html>.
- [7] Thorsten, L., Ibanez, A., Zanin, A., Blockstrand, M. *Simultaneous delivery of multimedia content: Scalable push file delivery with MBMS*. Uverejnené 1. 2009, citované 9.12.2013. Online: http://www.ericsson.com/ericsson/corpinfo/publications/review/2009_01/files/MBMS.pdf.
- [8] Bouras, CH. *Multicast broadcast single frequency network*. Citované 10.12.2013. Online: <http://4g-lte-world.blogspot.cz/2013/03/gprs-tunneling-protocol-gtp-in-lte.html>.
- [9] 3GPP TS 23.246 version 11.1.0 Release 11. *Universal Mobile Telecommunications System (UMTS); LTE; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description*. Uverejnené 11.2012, citované 11.12.2013. Online: http://www.etsi.org/deliver/etsi_ts/123200_123299/123246/11.01.00_60/ts_123246v110100p.pdf.

- [10] Daniel, A. *Policy and charging control over Rx reference point*. Uverejnené 4.2008, citované 20.5.2014. Online: http://www.etsi.org/deliver/etsi_ts/129200_129299/129214/07.04.00_60/ts_129214v070400p.pdf.
- [11] IXIA. Knižnica. *Quality of Service (QoS) and Policy Management in Mobile Data Networks: Validating Service Quality to Ensure Subscriber Quality of Experience (QoE)*. Uverejnené 7.2011, citované 13.12.2013. Online: http://www.ixiacom.com/pdfs/library/white_papers/policy_management.pdf.
- [12] *Long Term Evolution (LTE): A Technical Overview*. Citované 14.12.2013. Online: http://www.motorolasolutions.com/web/Business/Solutions/Industry%20Solutions/Service%20Providers/Wireless%20operators/LTE/_Document/Static%20Files/6834_MotDoc_New.pdf.
- [13] Nohrborg, M. *LTE*. Citované 14.12.2013. Online: <http://www.3gpp.org/technologies/keywords-acronyms/98-lte>.
- [14] *Definition of Quality of Service parameters and their computation, ETSI TS 102 250-2 V1.6.2*. Citované 14.5.2014. Online: http://www.etsi.org/deliver/etsi_ts/102200_102299/10225002/01.06.02_60/ts_10225002v010602p.pdf.

ZOZNAM SKRATIEK

3GPP The 3rd Generation Partnership Project

APN-AMBR Access Point Name - Aggregate Maximum Bit Rate – celková maximálna povolená priepustnosť služby

ARP Address Resolution Protocol

BM-SC Broadcast Multicast Service Centre – centrum broadcastovej a multicastovej služby

eNodeB evolved Base transceiver station – vyvinutá vysielacia stanica

EPC Evolved Packet Core – vyvinuté paketové jadro

EPS Evolved Packet System – vyvinutý paketový systém

E-UTRAN Evolved Universal Terrestrial Radio Access Network – vyvinutý univerzálny pozemný rádiový prístup k sieti

E-RAB Evolved Radio Access Bearer – rádiový prístupový bearer

FEC Forward Error Correction – vopred stanovená detekcia chýb

FLUTE File Delivery over Unidirectional Transport – doručenie súboru cez jednosmerný prenos

GPRS General Packet Radio Service – paketová rádio služba

GTP GPRS Tunneling Protocol – tunelovací protokol

HSS Home Subscriber Server – odberateľský server

HTML HyperText Markup Language

HTTP HyperText Transfer Protocol

IGMP Internet Group Management Protocol – internetový skupinový manažovací protokol

IMS IP Multimedia Subsystem – IP multimediálny podsystém

IP Internet Protocol

KPI Key Performance Indicators – kľúčový indikátor výkonnosti

LTE Long Term Evolution

L-EBI Linked EPS Bearer ID – identifikátor prideleného EPS beareru

MBMS Multimedia Broadcast Multicast Service

MBMS GW Multimedia Broadcast Multicast Service Gateway

MME Mobility Management Entity – prvok mobilného manažmentu

PCEF Policy and Charging Enforcement Function

PCRF Policy and Charging Rule Function

PDN GW Packet Data Network Gateway

PDU Packet Data Unit

POP3 Post Office Protocol

QCI QoS Class Identifier

QoS Quality of Service – odberateľský server

RTCP RTP Control Protocol

RTP Realtime Transport Protocol

SDP Session Description Protocol

SIP Session Initiation Protocol

SMS Short Message Service

SRTP Secure RTP

STAT Status – stav

SYNC Synchronization protocol

Serving GW Serving Gateway

TFT Traffic Flow Template - filter

TMGI Temporary Mobile Group Identifier

TNL Transport Network Layer

TS Time Stamp – časová značka

UE User Equipment

UE-AMBR User Equipment - Aggregate Maximum Bit Rate

UMTS Universal Mobile Telecommunications System

URL Uniform Resource Locator

UTRAN Universal Terrestrial Radio Access Network

VoLTE Voice over LTE

WiMAX World Interoprability For Microwave Access

ZOZNAM PRÍLOH

A Obsah CD

69

A OBSAH CD

Priložený disk obsahuje nasledujúce položky:

- Elektronická verzia bakalárskej práce
- Vyexportovaný projekt so zdrojovým kódom
- Spustiteľný jar súbor
- Upravený výstupný excelovský súbor z programu