Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

Mobile network equipment vendor

(Core network)

Semestrálny projekt

Tím 1: Erik Matejov, Tomáš Morvay, Peter Protuš, Matúš Križan

Tím 2: Patrik Dikant, Boris Žalman, Jaroslav Cút, Albert Prágai

Študijný program: Počítačové a komunikačné systémy a siete

Študijný odbor: Počítačové inžinierstvo

Miesto vypracovania: Ústav počítačových systémov a sietí, FIIT STU Bratislava

Máj 2015

Zadanie projektu

Ako výrobca infraštruktúry pre mobilné siete sa zúčastňujete výberového konania na dodanie sieťového uzla pre nového operátora. Spolu s partnerskou firmou (partnerský tím) vyvíjate dvojicu spolupracujúcich sieťových uzlov (zdieľajúcich jedno rozhranie). Vytvorte dvojice tímov a vyberte si jeden pár spolupracujúcich sieťových uzlov. Zvoľte si vhodnú sadu správ a procedúr, ktoré bude vaše riešenie podporovať. Svoj výber zdôvodnite. Implementujte zvolené funkcionality a otestujte ich. Implementáciu je dovolené (a odporúčané) postaviť na už existujúcich projektoch (napr. osmo-sgsn, openGGSN, freediameter, nwEPC, ...).

Tip: Je vhodné aby tímy pri finálnej fáze projektu spolupracovali a otestovali kompatibilitu svojich sieťových uzlov.

Tip2: Na otestovanie uzlov budete pravdepodobne potrebovať vygenerovať sieťovú prevádzku na iných rozhraniach vašich uzlov, odporúčame použiť tcpreplay/text2pcap a dodané vzorky sieťovej prevádzky.

Tip3: Odporúčaný filter v programe Wireshark pre vzorky sieťovej prevádzky je „ranap || gsm_a_dtap || udp.port == 4568 || gsm_map || gtp || s1ap || diameter || gtpv2“. Správy na rozhraní medzi SGSN a BSC (Gb) nie sú správne dekódované programom Wireshark, preto treba UDP segmenty s portom 4568 dekódovať ako protokol GPRS-NS.

Tip4: Wireshark v predvolenom nastavení nedefragmentuje DIAMETER správy prenášané SCTP protokolom, preto to treba manuálne nastaviť (preferences-> protocols-> SCTP -> zaškrtnúť “reassemble fragmented SCTP user messages“).

S4 based SGSN/SGW

Doplnenie rozhrania S4 (signalizácia a používateľské dáta) do osmo-sgsn (GTPC/GTP-U)

Doplnenie rozhrania S4 (signalizácia a používateľské dáta) do openGGSN (GTPC/GTP-U)

Obsah

1 Úvod 1

2 Analýza 2

2.1 SGSN 2

2.2 GGSN 3

2.3 EPC 3

2.3.1 Serving Gateway 3

2.3.2 Packet Data Network Gateway 4

2.4 GPRS Mobility Management správy 5

2.4.1 Attach Request 5

2.4.2 MS network capability 5

2.5 Rozhranie S4 6

2.6 GTP (GPRS Tunelling Protocol) 6

2.6.1 Control plane 7

2.6.2 User plane 10

2.7 Vytvorenie GTP tunela v LTE 13

2.8 Procedúry 14

2.8.1 Vybrané GTP-C procedúry 15

2.8.2 GTP-U procedúry 16

2.8.3 Výmena identifikátorov TEID 16

3 Špecifikácia požiadaviek 18

4 Návrh 19

4.1 Testovacia architektúra 19

4.2 Vytvorenie GTP tunela 19

4.3 Doplnenie do openBSC 20

4.4 Doplnenie do nwEPC 20

5 Implementácia 22

5.1 Použité existujúce riešenia 22

5.2 openBSC 22

5.2.1 Pridanie podpory GTPv2 22
5.2.2 EPC Capability Flag 23
5.2.3 Konverzia IMSI, MSISDN a IMEI 23
5.2.4 Posielanie Create Session Request 24
5.3 nwEPC 25
5.4 Kódové označenie projektu: S4Tukabel 25
6 Testovanie 26
6.1 Odoslanie prázdnej GTPv2 správy z SGSN 26
6.2 Odoslanie správy Create session request 26
6.3 Odpoveď Create session response 28
7 Zhodnotenie 29
8 Bibliography 30

1 Úvod

Mobilná sieť je najznámejším príkladom bunkovej siete. Mobilný telefón prijíma alebo nadväzuje spojenie pomocou základňovej stanice alebo vysielacej veže. Na komunikáciu s mobilným telefónom sa používajú rádiové vlny. Mobilné siete používajú bunkovú architektúru, pretože rádiové frekvencie sú obmedzený zdieľaný prostriedok.

Telekomunikační operátori nasadili hlasové a dátové bunkové siete vo väčšine oblastí sveta. To mobilným telefónom umožňuje pripojenie k verejnej telefónnej sieti a Internetu. V Slovenskej republiky sa v súčasnosti prevádzkujú siete 2G, 3G a 4G. Z toho vyplýva aj potreba zabezpečenia prechodu medzi danými sieťami.

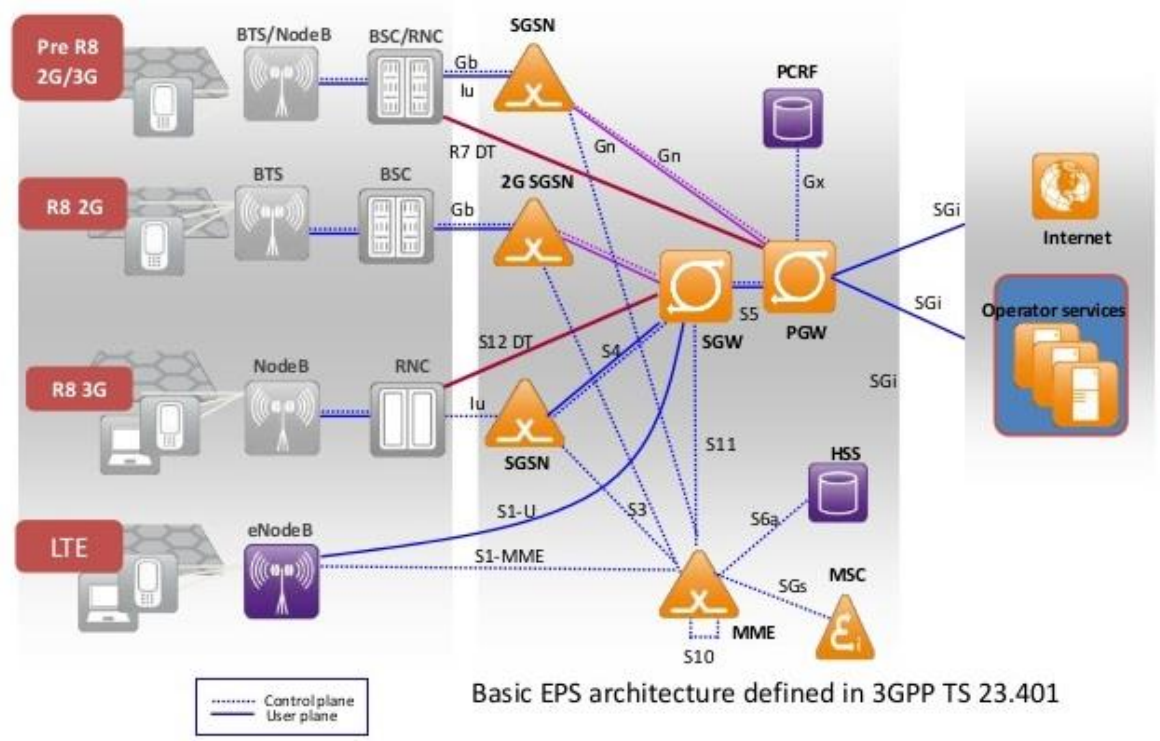
Jednou z možností ako prejsť z 2G a 3G siete do 4G siete, v prípade že nie je vytvorený priamy tunel, je použiť rozhranie S4 nachádzajúce sa medzi SGSN a SGW. Cieľom tejto práce je navrhnúť a doplniť práve S4 rozhranie do riešení s voľne dostupným zdrojovým kódom.

Tento dokument vznikol v rámci predmetu Architektúra mobilných sietí na FIIT STU. Predstavuje dokumentáciu k projektu Mobile network equipment vendor (Core network). Obsahuje analýzu, špecifikáciu požiadaviek, návrh riešenia, implementáciu a testovanie implementovaného riešenia.

2 Analýza

V tejto kapitole sa nachádza popis základných prvkov mobilnej architektúry spolu s rozhraniami, ktoré sa medzi nimi nachádzajú. Popísané sú iba komponenty ktoré museli byť bližšie analyzované pri riešení projektu.

Na obrázku 1 sa nachádza všeobecná architektúra LTE mobilnej siete, ktorej komponenty sú popísané nižšie. Keďže sa jedná o LTE sieť chýba v danej architektúre komponent GGSN, ktorý sa ešte bežne v mobilných sieťach vyskytuje. Avšak po analýze projektov s otvoreným zdrojovým kódom OsmoSGSN a nwEPC sa zistilo, že v oboch projektoch absentuje implementácia S4 rozhrania. To má za následok malú úpravu zadania tohto projektu, keďže bude navrhnuté a implementované S4 rozhranie na pôvodné miesto v sieti kam patrí, teda medzi SGSN a SGW.



Obrázok 1: Architektúra mobilnej siete [1]

2.1 SGSN

SGSN je skratkou anglického Service GPRS Support Node a je hlavným komponentom siete GPRS, v ktorej zabezpečuje prepínanie paketov. SGSN je pripojené na BTS cez Gb-rozhranie a slúži ako prístupový bod do siete GPRS pre mobilných používateľov. Na druhej strane SGSN prenáša dáta medzi SGSN a GGSN (a opačne), pričom na GGSN sa pripája pomocou GTP protokolu. SGSN robí aj konverziu z IP používanej v backbone sieti do SNDCP a LLC protokolov používaných medzi SGSN a mobilnými používateľmi. Tieto protokoly robia konverziu a šifrovanie. SGSN má za úlohu aj autentizáciu GPRS mobilných telefónov. Pokiaľ prebehne autentifikácia úspešne, SGSN zaregistruje telefón pre GPRS sieť a stará sa o riadenie mobility.

OsmoSGSN je bezplatná softvérová implementácia SGSN, ktorá implementuje GPRS manažment mobility (GMM) a manažment relácie (SM). V súčasnosti je táto implementácia v experimentálnom štádiu.

2.2 GGSN

GGSN je skratkou anglického Gateway GPRS Support Node a je druhým hlavným komponentom GPRS siete. GGSN je zodpovedné za spoluprácu medzi GPRS sieťou a externými sieťami s prepínaním paketov akými sú napr. Internet a X.25 siete. Z pohľadu externých sietí na GGSN je GGSN smerovač do podsiete, pretože pred nimi „skrýva“ GPRS infraštruktúru. Keď prijme GGSN dáta adresované špecifickému používateľovi, skontroluje, či je daný používateľ aktívny. Pokiaľ áno, GGSN prepošle dáta na SGSN, aby sa postaralo o doručenie používateľovi. Pokiaľ používateľ nie je aktívny, dáta budú vymazané. Na druhej strane, pakety vytvorené telefónom budú smerované do správnej siete pomocou GGSN. Preto si GGSN musí udržiavať záznamy aktívnych a SGSN záznamy pripojených používateľov. Taktiež je GGSN zodpovedné za prideľovanie IP adries používateľom mobilnej siete a za vyúčtovanie využitých služieb.

OpenGGSN je softvérová implementácia GGSN, ktorá sa používa mobilnými operátormi ako rozhranie medzi internetom a zvyškom mobilnej sieťovej infraštruktúry.

2.3 EPC

EPC je skratkou anglického Evolved Packet Core a je to základná sieť pre LTE založená na IP. Je špecifikovaná v 3GPP Release 8 štandarde, ktorý bol dokončený v prvom štvrťroku 2009.

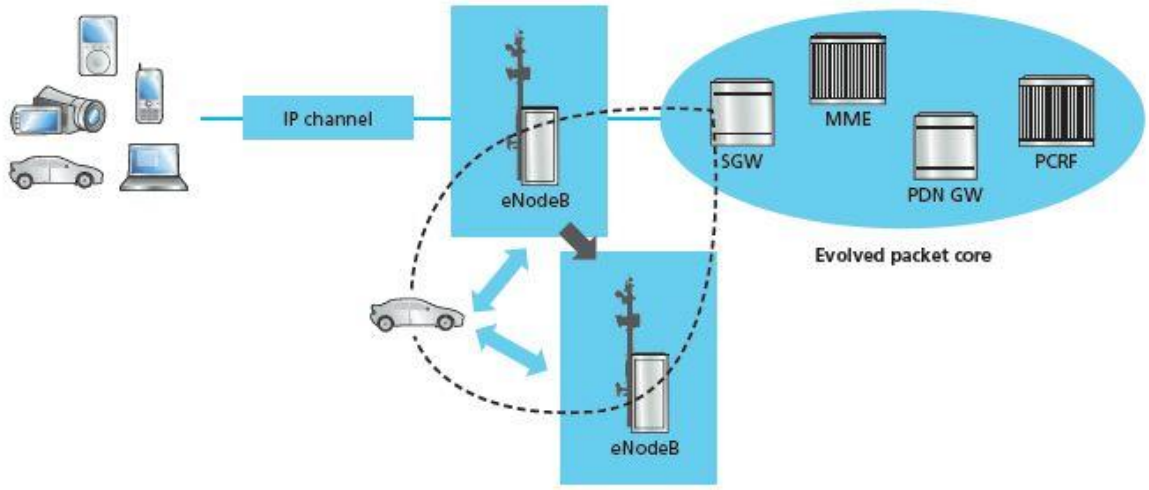
EPC poskytuje základnú funkcionalitu, ktorá bola v predošlých mobilných generáciách (2G, 3G) realizovaná pomocou dvoch samostatných subdomén: prepínanie okruhov pre hlas a prepínanie paketov pre dáta. V LTE sú tieto dve základné subdomény, používané na samostatné spracovanie a prepínanie hlasu a dát, spojené do jednej IP domény. LTE je od začiatku do konca založená na IP: od mobilných telefónov a ďalších zariadení s IP podporou, cez eNodeB (LTE základňové stanice), EPC až po celú aplikačnú doménu (IMS a non-IMS).

EPC je realizované pomocou 4 komponentov:

- Serving Gateway (SGW)
- Packet Data Network (PDN) Gateway (PGW)
- Mobility Management Entity (MME)
- Policy and Charging Rules Function (PCRF)

2.3.1 Serving Gateway

SGW je prvok, ktorého hlavnou funkciou je riadiť user-plane mobilitu a tváriť sa ako demarkačný bod medzi RAN a základnou sieťou. SGW udržiava dátové cesty medzi eNodeB a PGW. Z funkcionálneho hľadiska je SGW koncový bod smerom od PDN rozhrania k E-UTRAN. Keď sa zariadenia pohybujú medzi oblasťami obsluhovanými eNodeB elementami v E-UTRAN, SGW slúži ako miestne ukotvenie mobility. To znamená, že pakety sú smerované cez tento bod kvôli vnútornej E-UTRAN mobilite a mobilite s inými 3GPP technológiami, ako 2G/GSM a 3G/UMTS. Na obrázku 2 je ilustrovaný Serving Gateway.



Obrázok 2: Serving Gateway [2]

2.3.2 Packet Data Network Gateway

Podobne ako SGW, aj PGW je konečný bod paketového dátového rozhrania smerom k PDN. Ako miesto ukotvenia pre relácie smerom k externým PDN musí PGW podporovať:

- Funkcie presadzovanie politiky (aplikuje operátorom zadefinované pravidlá pre alokáciu a použitie zdrojov)
- Filtrovanie paketov (napríklad hlboká inšpekcia paketov pre detekciu typu aplikácie)
- Podpora účtovania (napríklad účtovanie za URL)

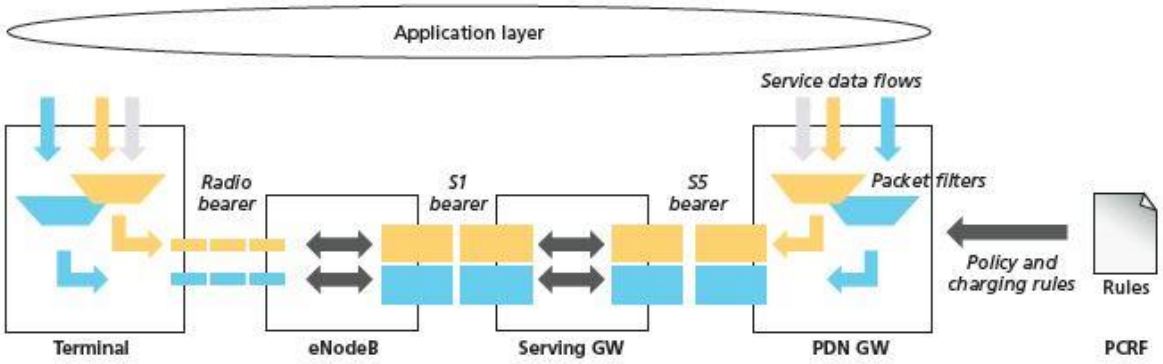
V LTE prebieha dátová premávka cez virtuálne spojenia nazývané dátové toky služieb (SDF). SDF sú podľa poradia prenášané cez bearery – virtuálne kontajnery s jedinečnými QoS vlastnosťami. Obrázok 3 ilustruje scenár, kde je jeden alebo viac SDF agregovaných a prenášaných cez jeden bearer.

Obrázok 3 SDF a bearery [2]

Jeden bearer, dátová cesta medzi UE a PDN, má tri segmenty:

- Rádio bearer medzi UE a eNodeB
- Dátový bearer medzi eNodeB a SGW (S1 bearer)
- Dátový bearer medzi SGW a PGW (S5 bearer)

Obrázok 4 ilustruje tri segmenty, ktoré predstavujú end-to-end bearer. Hlavnou úlohou PGW je presadenie QoS pre každá z týchto SDF, zatiaľ čo sa SGW zameriava na dynamické rieadenie bearerov.



Obrázok 4: End-to-end dátová cesta v LTE [2]

nwEPC je voľne dostupná softvérová implementácia SAE/EPC Serving Gateway alebo SGW a Packet Data Network Gateway alebo PGW, ktorý sa často označuje aj ako SAE-Gateway.

2.4 GPRS Mobility Management správy

Tieto správy bolo nutné analyzovať kvôli potrebe zistiť, či má mobilná stanica podporu prístupu k EPC a z SGSN môže byť následne nadviazané spojenie pomocou S4 rozhrania smerom na SGW do LTE siete. Po prvotnej analýze bolo zistené, že potrebná informácia sa nachádza v správe Attach Request, ktorá je popísaná v nasledujúcej kapitole.

2.4.1 Attach Request

Táto správa sa odosiela od UE do siete z dôvodu vytvorenia GPRS alebo kombinovaného GPRS spojenia. Povinné informačné elementy v Attach Request správe sú nasledujúce:

- Protocol discriminator
- Skip indicator
- Attach request message identity
- MS network capability
- Attach type
- GPRS ciphering key sequence number
- DRX parameter
- Mobile identity
- Old routing area identification
- MS Radio Access capability

Z povinných informačných elementov je ďalej analyzovaný len MS network capability, keďže ostatné nie sú pre project dôležité.

2.4.2 MS network capability

Účelom informačného elementu MS network capability je poskytnúť sieti informácie o aspektoch mobilnej stanice súviasiacich s GPRS. Obsah IE môže mať vplyv na spôsob akým sieť spracováva operácie mobilnej stanice. MS network capability informácia indikuje všeobecné charakteristiky mobilnej stanice a a preto musí byť nezávislá od frekvenčného pásma kanálu na ktorý je odoslaná. Maximálna dĺžka je 10 oktetov. Obsah MS network capability je znázornený na obrázku 5.

8	7	6	5	4	3	2	1	
MS network capability IEI								octet 1
Length of MS network capability contents								octet 2
MS network capability value								octet 3-10

Obrázok 5: Formát informačného elementu MS network capability [3]

V MS network capability value sa v druhom bajte nachádza bit EPC capability, ktorý je kľúčový pri zisťovaní podpory prístupu UE k EPC. V rámci druhého bajtu je to šiesty bit, t.j. tretí najmenej významný bit v bajte alebo tretí bit zľava. Indikuje, či mobilná stanica podporuje prístup k EPC cez prístupové siete iné ako GERAN a UTRAN. Sieť môže použiť túto informáciu na rozhodnutie či použije PGW alebo GGSN [**3**].

- 0 EPC nie je podporované
- 1 EPC je podporované

Na obrázku 6 je v Attach Request správe zvýraznený EPC capability bit pomocou programu Wireshark.

```
⊞ Frame 9: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
⊞ Ethernet II, Src: Vmware_fd:81:0b (00:0c:29:fd:81:0b), Dst: Vmware_00:0a:02 (00:50:56:00:0a:02)
⊞ Internet Protocol Version 4, Src: 172.16.48.41 (172.16.48.41), Dst: 172.16.47.51 (172.16.47.51)
⊞ User Datagram Protocol, Src Port: 4568 (4568), Dst Port: 30000 (30000)
⊞ GPRS Network Service, PDU type: NS_UNITDATA, BVCI 2
⊞ Base Station Subsystem GPRS Protocol
⊞ MS-SGSN LLC (Mobile Station - Serving GPRS Support Node Logical Link Control)  SAPI: GPRS Mobility Management
⊟ GSM A-I/F DTAP - Attach Request
  ⊞ Protocol Discriminator: GPRS mobility management messages (8)
    DTAP GPRS Mobility Management Message Type: Attach Request (0x01)
  ⊟ MS Network Capability
      Length: 3
      0... .... = GEA/1: Encryption algorithm not available
      .0.. .... = SM capabilities via dedicated channels: Mobile station does not support mobile terminated point to point SMS via dedicated signalling channels
      ..1. .... = SM capabilities via GPRS channels: Mobile station supports mobile terminated point to point SMS via GPRS packet data channels
      ...0 .... = UCS2 support: The ME has a preference for the default alphabet (defined in 3GPP TS 23.038 [8b]) over UCS2
      .... 00.. = SS Screening Indicator: Default value of phase 1 (0x00)
      .... ..0. = SoLSA Capability: The ME does not support SoLSA
      .... ...0 = Revision level indicator: Used by a mobile station not supporting R99 or later versions of the protocol
      0... .... = PFC feature mode: Mobile station does not support BSS packet flow procedures
    ⊞ .000 000. = Extended GEA bits: 0x00
      .... ...1 = LCS VA capability: LCS value added location request notification capability supported
      0... .... = PS inter-RAT HO from GERAN to UTRAN Iu mode capability: PS inter-RAT HO to UTRAN Iu mode not supported
      .0.. .... = PS inter-RAT HO from GERAN to E-UTRAN S1 mode capability: PS inter-RAT HO to E-UTRAN S1 mode not supported
      ..0. .... = EMM Combined procedures capability: Mobile station does not support EMM combined procedures
      ...0 .... = ISR support: The mobile station does not support ISR
      .... 1... = SRVCC to GERAN/UTRAN capability: SRVCC from UTRAN HSPA or E-UTRAN to GERAN/UTRAN supported
      .... .1.. = EPC capability: EPC supported
```

Obrázok 6: EPC capability bit

2.5 Rozhranie S4

Toto rozhranie spája SGSN a SGW. Poskytuje podporu riadenia a mobility medzi GPRS základnou sieťou a funkciou ukotvenia. Taktiež poskytuje user-plane tunelovanie ak nie je vytvorený priamy tunel. S4 rozhranie nemá ekvivalentné rozhranie v 3G mobilnej sieti, pretože poskytuje interoperabilitu medzi 3G a 4G sieťami. Poskytuje GPRS tunelovací protokol, riadiaci (GTP-C) verziu 2 a používateľký (GTP-U), vo vnútri UDP datagramov [**4**].

2.6 GTP (GPRS Tunelling Protocol)

GTP je značne používaný na niektorých rozhraniach v EPC, napríklad na S11 medzi MME a SGW alebo S5/S8 medzi SGW a PGW. GTP sa taktiež používa na S1-U medzi eNodeB a SGW. GTP môžeme považovať za kombináciu dvoch protokolov: GTP-C (pre control plane) a GTP-U (pre user plane). GTP-U sa používa na tunelovanie používateľských dát, zatiaľ čo GTP-C sa používa napríklad na nastavenie a uvoľnenie týchto tunelov.

Pre EPC je špecifické použitie druhej verzie GTP protokolu pre control plane (GTPv2-C). Hlavnou úlohou GTP-U protokolu je zapuzdrenie a tunelovanie používateľských dátových paketov medzi

uzlami v sieti. V E-UTRAN je použitý na S1 rozhraní (a X2 rozhraní medzi eNodeB). V EPC je použitý napríklad na S5/S8 (SGW-PGW) a na S4 medzi SGW a SGSN.

Každý používateľský dátový IP paket je zapuzdrený a je pridaná GTP hlavička. Hlavička okrem iných vecí obsahuje Tunnel Endpoint Identifier (TEID). TEID je lokálne pridelené referenčné číslo, ktoré jednoznačne identifikuje GTP tunel v uzli, ktorý ho pridelil. Preto má GTP tunel dve TEID, jedno na každom konci.

GTP-C protokol používa niekoľko rôznych EPC rozhraní. Presný súbor používaných procedúr v GTP-C preto závisí od rozhrania.

GTPv2-C špecifikácia nerozdeľuje GTP funkcie ani tak veľmi do procedúr ako do scenárov. Napríklad špecifická GTP-C správa (a teda i procedúra) používaná na uvoľnenie EPS bearera v SGW bude odlišná v závislosti od toho, či uvoľnenie inicializuje UE alebo eNodeB/MME. Dôsledkom toho je, že existujú viaceré GTP-C správy/procedúry ktoré viac-menej dosiahnu ten istý cieľ [**5**].

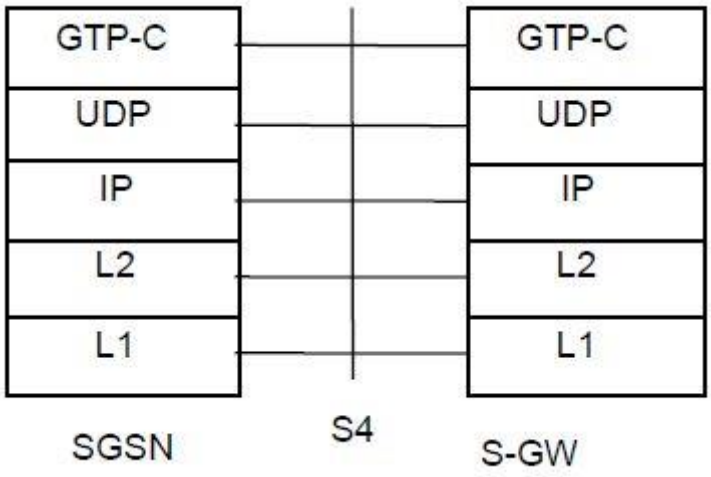
Funkcionalita spomínaných GTP protokolov [**6**]:

- GTP-U – Je to relatívne jednoduchý protokol na prenos používateľových dát v oddelených tuneloch pre každý PDP kontext (Packet Data Protocol – je to dátová štruktúra ktorá nesie informácie o účastníkovej relácii > účastníkova IP adresa, účastníkove IMSI (identifikátor účastníka), účastníkov Tunnel Endpoint ID (TEID) pre PGW a Tunnel Endpoint (TEID) pre SGW). GTPv1-U protokol je používaný na výmenu používateľských dát cez GTP tunely prostredníctvom Sx rozhraní.
- GTP-C – Vykonáva signalizáciu medzi SGW a PGW v základnej GPRS sieti na aktiváciu a deaktiváciu účastníckych relácií, upravuje parameter kvality služieb alebo aktualizuje relácie pre účastníkov používajúcich roaming, ktoré prichádzajú z iného SGW. eGTP-C (alebo GTPv2-C) protokol je zodpovedný za vytvorenie, údržbu a vymazanie tunelov na viacerých Sx rozhraniach.
- GTP‘ – prenos účtovacích dát

2.6.1 Control plane

Control plane pozostáva z protokolov pre riadenie a podporu user plane funkcií:

- Riadenie prístupových spojení E-UTRA siete, ako pripojenie a odpojenie z E-UTRAN
- Riadenie atribútov zavedeného sieťového prístupového spojenia, ako aktivácia IP adresy
- Riadenie smerovacej cesty zavedeného sieťového spojenia s cieľom podpory mobility používateľa
- Riadenie prideľovania sieťových zdrojov na splnenie požiadaviek používateľa



Obrázok 7: Protokolový zásobník S4 rozhrania

GTP-C: Tento protokol tuneluje signalizačné správy medzi SGSN a SGW (S4).

UDP: Tento protokol prenáša signalizačné správy [**7**].

2.6.1.1 Všeobecný formát GTPv2-C hlavičky

Control plane GTP používa variabilnú dĺžku hlavičky, ktorá musí byť násobkom 4 oktetov. Obrázok 8 ilustruje formát GTPv2-C hlavičky.

Octets	Bits 8	7	6	5	4	3	2	1
1	Version			P	T	Spare	Spare	Spare
2	Message Type							
3	Message Length (1st Octet)							
4	Message Length (2nd Octet)							
m to k(m+3)	If T flag is set to 1, then TEID shall be placed into octets 5-8. Otherwise, TEID field is not present at all.							
n to (n+2)	Sequence Number							
(n+3)	Spare							

Obrázok 8: Hlavička GTPv2-C protokolu.

Prvých 8 bitov správy vyzerá nasledovne:

- Bity 8-6 reprezentujú pole verzie, pre GPTv2-C je to decimálna 2, teda Version = „010“.
- Bit 5 reprezentuje Piggybacking flag (P).
- Bit 4 reprezentuje TEID flag (T). Vysvetlený je na obrázku 6.
- Bity 3-1 sú rezervné, odosielateľ ich musí nastaviť na „0“ a prijímajúca entita ich ignoruje.

Druhý oktet Message Type určuje typ správy. Existuje ich veľmi veľa preto boli vybrané 4 najdôležitejšie potrebné pri vytváraní a rušení tunela a sú znázornené v tabuľke 1.

Message Type hodnota (decimálna)	Správa
32	Create Session Request
33	Create Session Response

36	Delete Session Request
37	Delete Session Response

Tabuľka 1: Typy správ v hlavičke protokolu GTPv2-C

Oktety 3 a 4 indikujú dĺžku správy v oktetoch okrem povinnej časti GTP-C hlavičky (prvé 4 oktety). TEID (ak je prítomné) a Sequence Number sú taktiež zahrnuté do dĺžky správy.

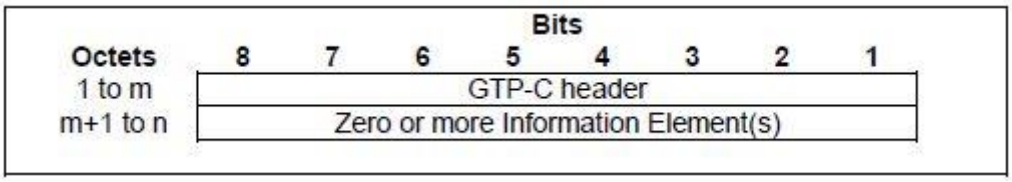
2.6.1.2 Podmienky pre odoslanie TEID=0 v GTPv2-C hlavičke

Ak peer nemá dostupné TEID, toto pole musí byť aj tak dostupné v hlavičke a jeho hodnota musí byť nastavená na „0“v nasledujúcej správe (je ich viac, ale vybraná bola iba tá, ktorá súvisí s riešeným projektom):

- Create Session Request správa na S4/S11, ak pre dané UE ešte SGSN/MME nezískali TEID z SGW.

2.6.1.3 Formát GTPv2-C správy

Za GTP-C hlavičkou môžu nasledovať informačné elementy podľa typu riadiacej správy, tak ako je vidno na obrázku 9.



Obrázok 9: Formát GTPv2-C správy

2.6.1.4 Create Session Request správa

Smer tejto správy musí byť z MME/SGSN na SGW, z SGW na PGW a z ePDG na PGW.

Správa musí byť odoslaná na S4 rozhranie od SGSN na SGW ako súčasť procedúry PDP Context Activation. Týchto procedúr je oveľa viac, no nebudú pre tento projekt potrebné. Ak je správa Create Session Request prijatá na SGW s TEID = 0 v hlavičke pre existujúce aktívne PDN spojenie, tak táto správa musí byť považovaná za požiadavku na novú reláciu. Existujúce PDN spojenie by malo byť lokálne vymazané ešte pred tým ako je vytvorená nová relácia.

V tabuľke 2 sa nachádzajú povinné informačné elementy (IE) v Create Session Request správe.

Informačné elementy	Podmienka/Komentár	Typ IE
RAT Type	Tento IE musí byť nastavený na 3GPP prístupový typ alebo na hodnotu spĺňajúcu charakteristiku non-3GPP prístupu, ktorý UE používa na pripojenie k EPS. ePDG môže použiť typ prístupovej technológie z nedôveryhodnej non-3GPP prístupovej sieti, ak je schopný ho získať, inak uvedie Virtual ako RAT Type.	RAT Type
Odosielateľove F-TEID pre control plane		F-TEID
Access Point Name		APN
Bearer Contexty na vytvorenie	Niekoľko IE s rovnakým typom a hodnotou inštancie musí byť obsiahnutých v S4 rozhraní ako potreba reprezentácie zoznamu bearerov.	Bearer Context

	Jeden bearer musí byť zahrnutý vpre E-UTRAN Initial Attach, PDP Context Activation atď.	

Tabuľka 2: Povinné IE v Create Session Request správe

V tabuľke 3 sa nachádzajú povinné IE v Bearer Context na vytvorenie

Oktet 1	Bearer Context IE Type = 93 (decimálne)	
Oktet 2 a 3	Length = n	
Oktet 4	Rezervné polia	
Informačné elementy	Podmienka/Komentár	Typ IE
EPS Bearer ID		EBI
Bearer Level QoS		Bearer QoS

Tabuľka 3: Povinné IE v Bearer Context elemente

2.6.1.5 Create Session Response správa

Správa musí byť odoslaná na S4 rozhranie od SGW na SGSN ako súčasť procedúry PDP Context Activation. Týchto procedúr je oveľa viac, no nebudú pre tento projekt potrebné.

V tabuľke 4 sa nachádzajú povinné informačné elementy (IE) v Create Session Response správe.

Informačné elementy	Podmienka/Komentár	Typ IE
Cause		Cause
Bearer Contexty vytvorené		Bearer Context

Tabuľka 4: Povinné IE v Create Session Response správe

V tabuľke 5 sa nachádzajú povinné IE v Bearer Context vytvorené.

Oktet 1	Bearer Context IE Type = 93 (decimálne)	
Oktet 2 a 3	Length = n	
Oktet 4	Rezervné polia	
Informačné elementy	Podmienka/Komentár	Typ IE
EPS Bearer ID		EBI
Cause	Tento IE musí indikovať, či bolo zavedenie bearera úspešné a ak nie, tak dáva informáciu s dôvodom.	Cause

Tabuľka 5: Povinné IE v Bearer Context elemente

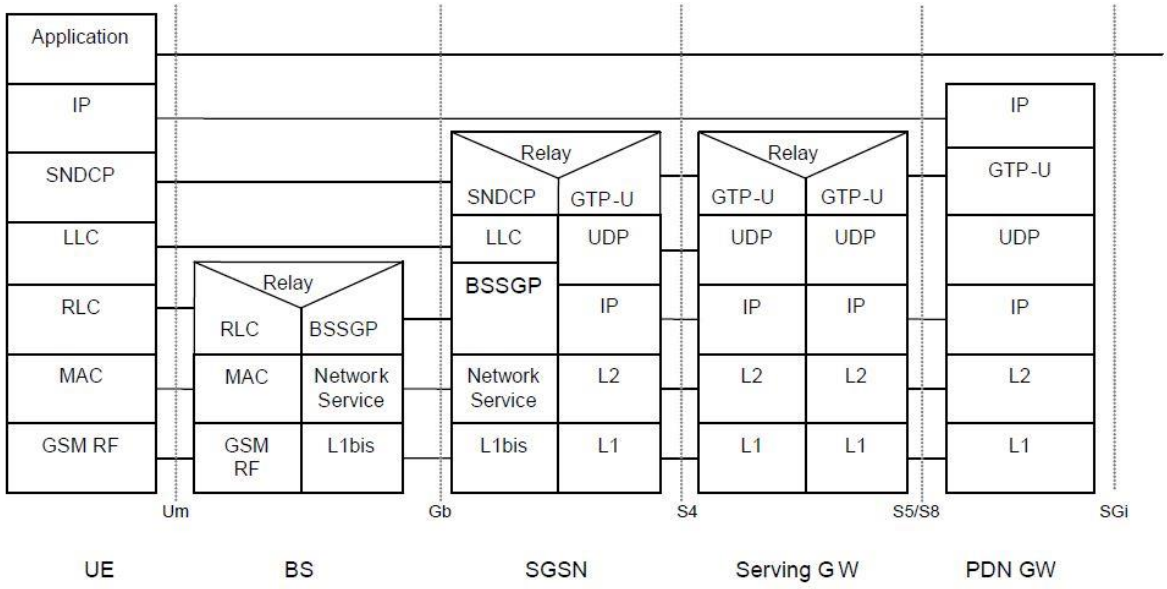
Niektoré možné hodnoty Cause:

- Request accepted
- Missing or unknow APN
- Denied in RAT
- All dynamic addresses are occupied
- GRE key not found

Všetky informácie pochádzajú z [**5**].

2.6.2 User plane

Na obrázku 10 je znázornený UE – PGW user plane s 2G prístupom cez S4 rozhranie.

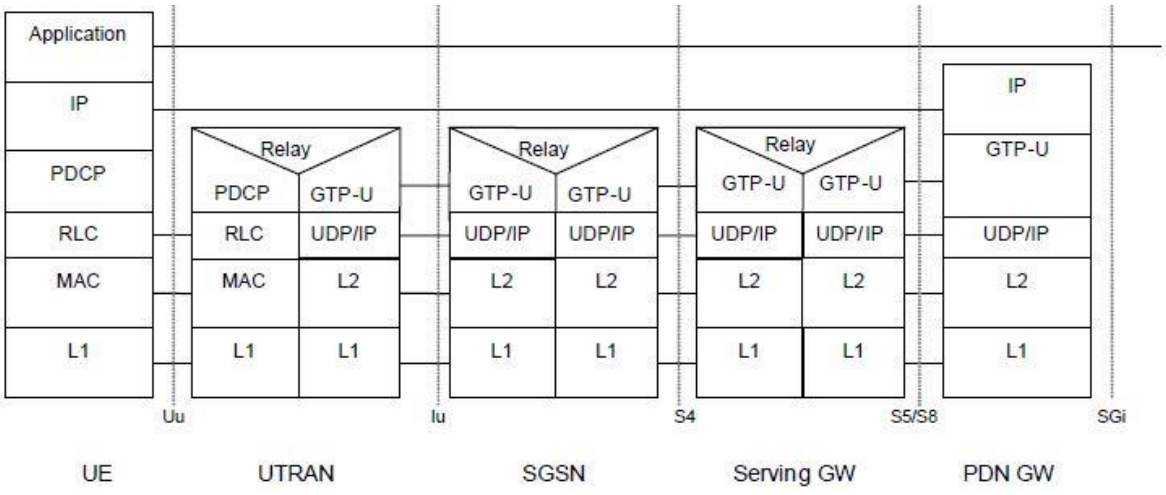


Obrázok 10: Protokolový zásobník end-to-end spojenia z 2G siete cez S4 rozhranie [7]

GTP-U: Tento protokol tuneluje používateľské dáta medzi SGSN a SGW rovnako ako medzi SGW a PGW v chrbticovej sieti. GTP musí zapuzdrovať všetky IP pakety koncových používateľov.

UDP/IP: Sú to protokoly chrbticovej siete použité na smerovanie používateľských dát a riadiacej signalizácie.

Na obrázku 11 je znázornený UE – PGW user plane s 3G prístupom cez S4 rozhranie.



Obrázok 11: Protokolový zásobník end-to-end spojenia z 3G siete cez S4 rozhranie [7]

GTP-U: Tento protokol tuneluje používateľské dáta medzi UTRAN a SGSN, medzi SGSN a SGW a medzi SGW a PGW v chrbticovej sieti. GTP musí zapuzdrovať všetky IP pakety koncových používateľov.

UDP/IP: Sú to protokoly chrbticovej siete použité na smerovanie používateľských dát a riadiacej signalizácie.

SGSN riadi zriadenie user plane tunela a zriaďuje tunel medzi SGSN a SGW, samozrejme ak nie je zriadený priamy tunel.

Všetky informácie pochádzajú z [**7**].

2.6.2.1 Všeobecný formát GTP-U hlavičky

GTP-U hlavička môže mať variabilnú dĺžku, ktorej minimum je 8 bajtov. Obrázok 12 ilustruje formát GTP-U hlavičky.

Octets	Bits 8	7	6	5	4	3	2	1
1	Version			PT	(*)	E	S	PN
2	Message Type							
3	Length (1st Octet)							
4	Length (2nd Octet)							
5	Tunnel Endpoint Identifier (1st Octet)							
6	Tunnel Endpoint Identifier (2nd Octet)							
7	Tunnel Endpoint Identifier (3rd Octet)							
8	Tunnel Endpoint Identifier (4th Octet)							
9	Sequence Number (1st Octet) 1) 4)							
10	Sequence Number (2nd Octet) 1) 4)							
11	N-PDU Number 2) 4)							
12	Next Extension Header Type 3) 4)							

Obrázok 12: Formát GTP-U hlavičky [8]

1) Toto pole je prítomné iba ak S=1.
2) Toto pole je prítomné iba ak PN=1.
3) Toto pole je prítomné iba ak E=1.
4) Toto pole je prítomné ak a iba ak akýkoľvek jeden alebo viac z S, PN a E flagov je nastavený.

Povinné polia:

- Version: Toto pole určuje verziu GTP-U protokolu. Musí byť nastavené na 1.
- Protocol Type (PT): Tento bit sa používa na odlíšenie medzi GTP (PT=1) a GTP‘ (PT=0).
- (*)
- Extension Header flag (E): Indikuje prítomnosť Extension Header ak E=1.
- Sequence Number flag (S): Indikuje prítomnosť Sequence Number ak S=1.
- N-PDU Number flag (PN): Indikuje prítomnosť N-PDU Number ak PN=1.
- Message Type: Indikuje typ GTP-U správy.
- Length: Dĺžka paketu v oktetoch, okrem prvých 8 povinných oktetov.
- TEID: Toto pole jednoznačne identifikuje koncový bod tunela v prijímajúcej entite. Prijímajúca koncová strana GTP tunela lokálne priraďuje TEID hodnotu, ktorú má vysielajúca strana použiť.

Typy správ v GTP-U sa nachádzajú v tabuľke 6.

Message Type Hodnota (decimálna)	Správa	GTP-U	GTP‘
1	Echo Request	X	X
2	Echo Response	X	X

3-25	Rezervované		
26	Error Indication	X	
27-30	Rezervované		
31	Supported Extension Header Notification	X	
32-253	Rezervované		
254	End Marker	X	
255	G-PDU	X	

Tabuľka 6: Typy správ v GTP-U

Všetky informácie pochádzajú z [**8**].

2.7 Vytvorenie GTP tunela v LTE

V tejto kapitole je opísané vytovrenie GTP tunela v LTE sieti, keďže sa nám nepodarilo nájsť konkrétny príklad na tunel vytovrený cez rozhranie S4. Avšak tento tunel by sa nemal líšiť od toho, ktorý potrebujeme v našom projekte a preto budeme vychádzať z tejto špecifikácie.

IP pakety odosielané LTE zariadením (UE) sú doručované z eNodeB na PGW prostredníctvom GTP tunelov. To znamená, že všetky IP pakety, ktoré UE posiela sú vždy doručované cez eNodeB na PGW bez ohľadu na to aká je ich cieľová IP adresa.

UE -> eNodeB

UE posiela IP paketa s cieľovou IP adresou napríklad 74.125.71.104 (IP adresa www.google.com) na eNodeB prostredníctvom rádiovej linky. Pôvodný paket odosielaný z UE vyzerá približne takto:

eNodeB -> SGW

Po prijatí IP paketu od UE pridáva eNodeB GTP hlavičku tunela skadajúcu sa z troch samostatných hlavičiek (GTP hlavička, UDP hlavička a IP hlavička pre GTP tunelovanie) pred IP paket. Potom odosielaný paket z eNodeB na SGW vyzerá nasledovne:

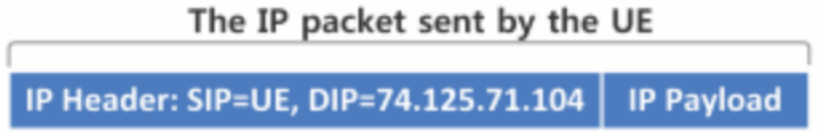
Takže ak medzi eNodeB a SGE existuje iba IP smerovacia sieť, smerovanie je založené na cieľovej IP adrese paketu (napríklad IP adresa SGW, cieľová adresa vo vonkajšej IP hlavičke) a potom je podľa toho IP paket doručený na SGW.

SGW -> PGW

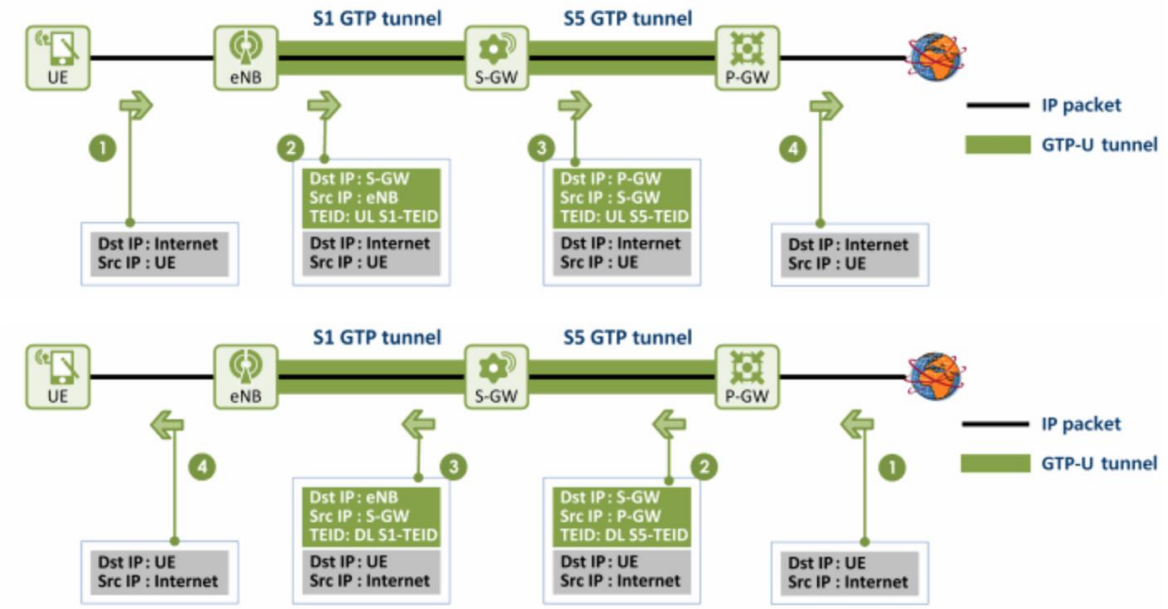
Po tom čo SGW príjme paket z eNodeB, upraví jeho GTP hlavičku a IP hlavičku (vonkajšiu) nasledovne:

PGW -> PDN (www.google.com)

PGW odstráni z paketu všetky tri hlavičky (vonkajšiu IP hlavičku, UDP hlavičku, GTP hlavičku) a doručí pôvodný paket odoslaný UE na Internet.



V nasledujúcich riadkoch je bližšie vysvetlené TEID, ktoré sa nachádza v GTP hlavičke a nebolo zatiaľ spomenuté. Povedzme, že existuje 100 UE ktoré sú pripojené na SGW a PGW. Vzhľadom k tomu, že na jedno UE sa vytvára jeden GTP tunel (môže byť vytvorených aj viac ako jeden), tak sa vytvorí 100 GTP tunelov. Teraz musí byť LTE sieť schopná rozlíšiť ktorý GTP tunel patrí ktorému UE. Na tento účel sa kukaždému UE priraďuje TEID. Napríklad je priradené TEID = UL S1-TEID (napr. 0x12345678) pre linku z eNodeB na SGW a TEID = UL S5-TEID (napr. 0xabcdef12) pre linku z SGW na PGW. Viď obrázok 13.



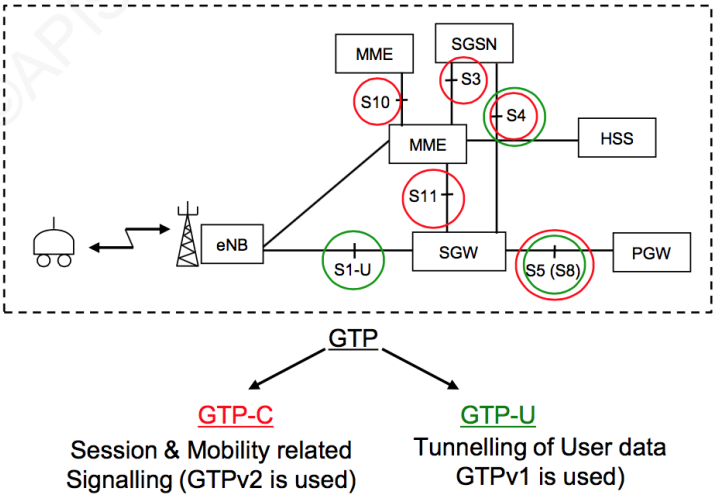
Obrázok 13: Formát paketov a hodnoty v hlavičke GTP tunela [9]

Teraz keď sú použité špecifické TEID pre každé UE, LTE sieť vie rozlíšit jej účastníkov (UE) kontrolovaním ich TEID namiesto IP adries. PGW však kontroluje aj TEID aj IP adresu, zatiaľ čo eNodeB a SGW kontroluje iba TEID.

Dôležité je pri TEID vedieť, že sú jednosmerné. To znamená, že môžu slúžiť iba na jeden smer a to buď uplink alebo downlink. Takže pre premávku z Internetu na UE sú priradené a použité nové TEID pre linky z PGW na SGW a z SGW na eNodeB [**9**].

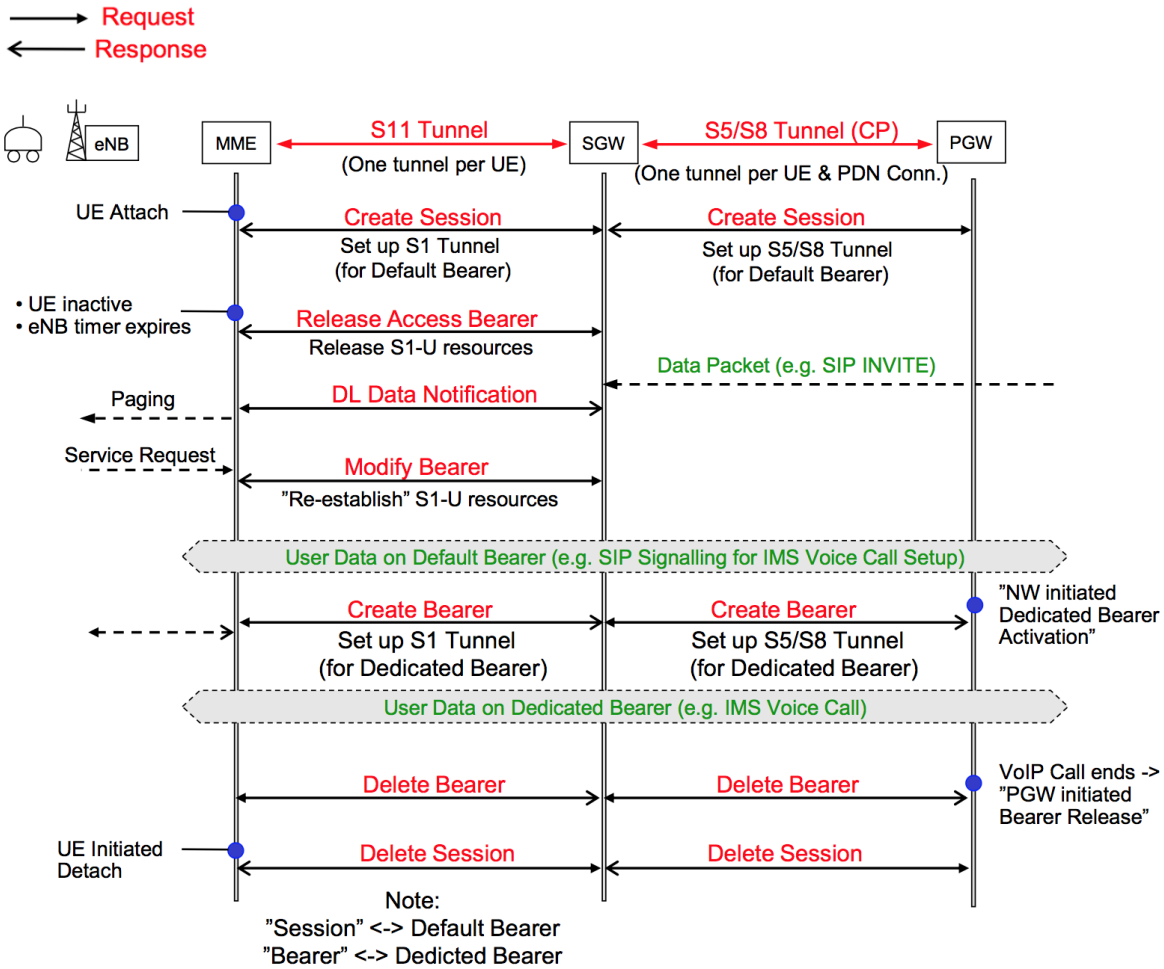
2.8 Procedúry

V tejto kapitole sa nachádzajú procedúry potrebné pre vytvorenie GTP tunela. Nikde sa nám nepodarilo nájsť konkrétny príklad pre rozhranie S4, preto sa riadime procedúrami na S5/S8 rozhraní, ktoré rovanko ako S4 používajú GTPv2-C a GTP-U, ako je možné vidieť aj na obrázku nižšie.



Obrázok 14: Prítomnosť GTP-C a GTP-U protokolov na rozhraniach v LTE architektúre [10]

2.8.1 Vybrané GTP-C procedúry



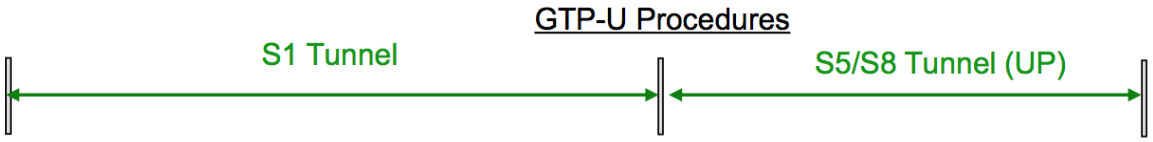
Obrázok 15: Najhlavnejšie GTP-C procedúry [10]

Ako už bolo spomenuté, pri riešení nášho projektu sa budeme inšpirovať procedúrami na rozhraní S5/S8. Ako je vidno na obrázku, na rozhraní sa vykonáva osem základných procedúr, z toho sú štyri dôležité pre vytvorenie a zrušenie tunela:

- Create Session Request
- Create Session Response
- Delete Session Request
- Delete Session Response

Tieto procedúry budú ďalej zohľadnené pri návrhu a implementácii S4 rozhrania do existujúcich projektov.

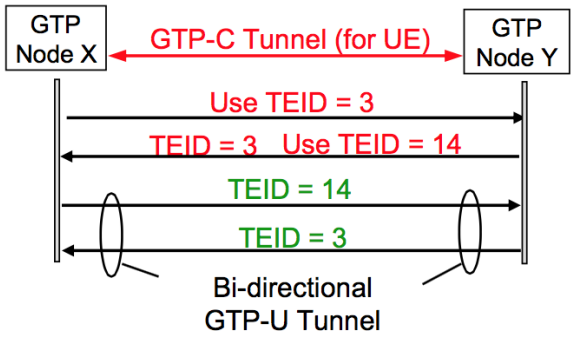
2.8.2 GTP-U procedúry



Obrázok 16: GTP-U tunely [10]

GTP-C pripraví všetky veci na to, aby sa pomocou GTP-U mohli v tuneloch prenášať používateľské data.

2.8.3 Výmena identifikátorov TEID



Obrázok 17: Proces výmeny TEID [10]

Pri vytváraní GTP tunela sa ako prvá odosiela správa Create Session Request z GTP Node X na GTP Node Y. Súčasťou tejto správy sú aj tri hodnoty TEID. TEID v GTP hlavičke, ktoré identifikuje druhý koniec tunela, musí byť pri inicializovaní nastavené na hodnotu 0, keďže TEID druhého konca ešte nie je známe a uzly si hodnoty TEID pridelujú lokálne. TEID, ktoré je súčasťou informačného elementu „Sender F-TEID for Control Plane“ je hodnota, ktorá identifikuje koncovú stranu tunela vygenerovanú na uzle GTP Node X pre control plane. Posledné TEID je súčasťou informačného elementu „Bearer Context to be created“ a jeho hodnota identifikuje koncovú stranu tunela vygenerovanú na GTP Node X, avšak pre user plane. Pri Create Session Request sa vytvára Default Bearer a preto sú TEID pre user plane a control plane na S4 rozhraní rovnaké. Podľa obrázka sa teda v Create Session Request odošlú hodnoty TEID nasledovne:

- TEID v GTP hlavičke= 0
- TEID v IE „Sender F-TEID for Control Plane“ = 3
- TEID v IE „Bearer Context to be created“ = 3

GTP Node Y po prijatí Create Session Request odpovedá pomocou správy Create Session Response. TEID v GTP hlavičke, ktoré identifikuje druhý koniec tunela na GTP Node X, je podľa informácie v správe Create Session Request nastavené na hodnotu 3. TEID, ktoré je súčasťou informačného elementu „Sender F-TEID for Control Plane“ je hodnota, ktorá identifikuje koncovú stranu tunela

vygenerovanú na uzle GTP Node Y pre control plane. Posledné TEID je súčasťou informačného elementu „Bearer Context to be created“ a jeho hodnota identifikuje koncovú stranu tunela vygenerovanú na GTP Node Y, avšak pre user plane. Pri Create Session Request sa vytvára Default Bearer a preto sú TEID pre user plane a control plane na S4 rozhraní rovnaké. Podľa obrázka sa teda v Create Session Response odošlú hodnoty TEID nasledovne:

- TEID v GTP hlavičke= 3
- TEID v IE „Sender F-TEID for Control Plane“ = 14
- TEID v IE „Bearer Context to be created“ = 14

Týmto pádom bol zriadený tunel ktorý má na oboch koncoch identifikátori a môžu sa ním začať prenášať používateľské dáta. Používateľské dáta smerujúce z SGSN na SGW budú mať V GTP hlavičke TEID = 14 a dáta smerujúce z SGW na SGSN budú mať v GTP hlavičke TEID = 3.

3 Špecifikácia požiadaviek

Cieľom tohto projektu je navrhnúť a implementovať základnú podporu rozhrania S4 (vytvorenie a zrušenia tunela) do riešení s otvoreným zdrojovým kódom. V architektúre mobilných sietí sa rozhranie S4 používa na komunikáciu medzi uzlom Serving GPRS Support Node (SGSN) a uzlom Serving GateWay(S-GW). V úlohe uzla SGSN bude použitá voľne dostupná implementácia OsmoSGSN [1] a v úlohe uzla S-GW voľne dostupná implementácia nwEPC. V obchoch týchto riešeniach rozhranie S4 zatiaľ nie je implementované.

Práca na tomto projekte sa skladá z dvoch hlavných častí:

1. Pridanie rozhrania S4 do OsmoSGSN
2. Pridanie rozhrania S4 do nwEPC

Na tomto riešení pracujú dva tímy študentov, kde každý tím má za úlohu pripraviť rozhranie S4 na vybranom uzle. Obe časti riešenia musia byť navzájom kompatibilné, a preto je dôležitá vzájomná komunikácia tímov.

Po prvotnej analýze sme zistili, že doplnenie rozhrania S4 vyžaduje podporu protokolu GTP na oboch uzloch. Podľa štandardu má rozhranie S4 implementovať nasledovné verzie protokolu:

- GTPv1 pre používateľské dáta (user plane) - označuje sa aj GTP-U, GTPv1-U
- GTPv2 pre riadiace dáta (control plane) - označenia aj GTPv2-C, eGTP

V osmoSGSN je implementovaný protokol GTP-U pomocou knižnice libgtp. V nwEPC je implementovaný protoko GTP-U pomocou knižnice nw-gtpv1u a protokol GTPv2-C pomocou knižnice nw-gtpv2c. Tieto protokoly sa používaju na rozhraní S4 medzi uzlami SGSN a SGW. Preto jedným z hlavných cieľov bude doplnenie podpory protokolu GTPv2-C do osmoSGSN.

Ďalším hlavným cieľom projektu bude základné vytvorenie GTP tunela cez rozhranie S4 (PDP Context Activation). Tieto operácie vyžadujú implementáciu nasledujúcich dvoch GTP-C správ [5]:

- Create Session Request
- Create Session Response

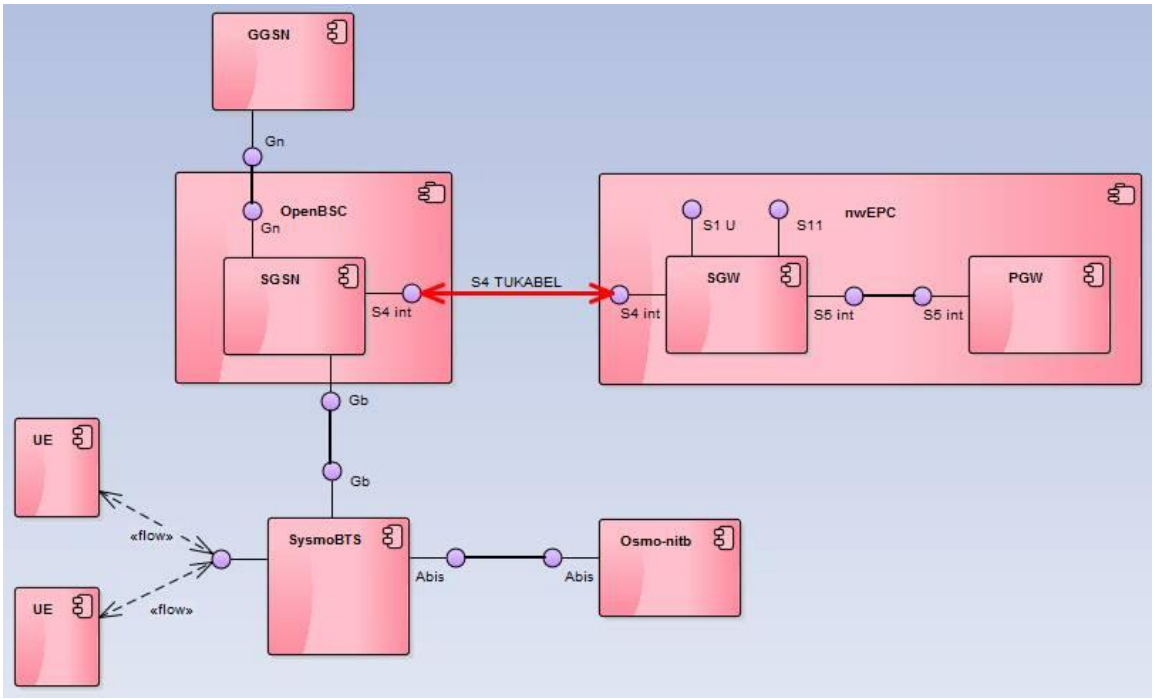
Hlavným prínosom tohto projektu bude pridanie podpory rozhrania S4 a protokolu GTPv2-C do existujúcich riešení s otvoreným zdrojovým kódom. V ideálnom prípade bude riešenie commitnuté do oficiálnych repozitárov oboch použitých riešení a môže tak slúžiť ďalším vývojárom.

4 Návrh

V tejto kapitole sa nachádza základný návrh riešenia tohto projektu.

4.1 Testovacia architektúra

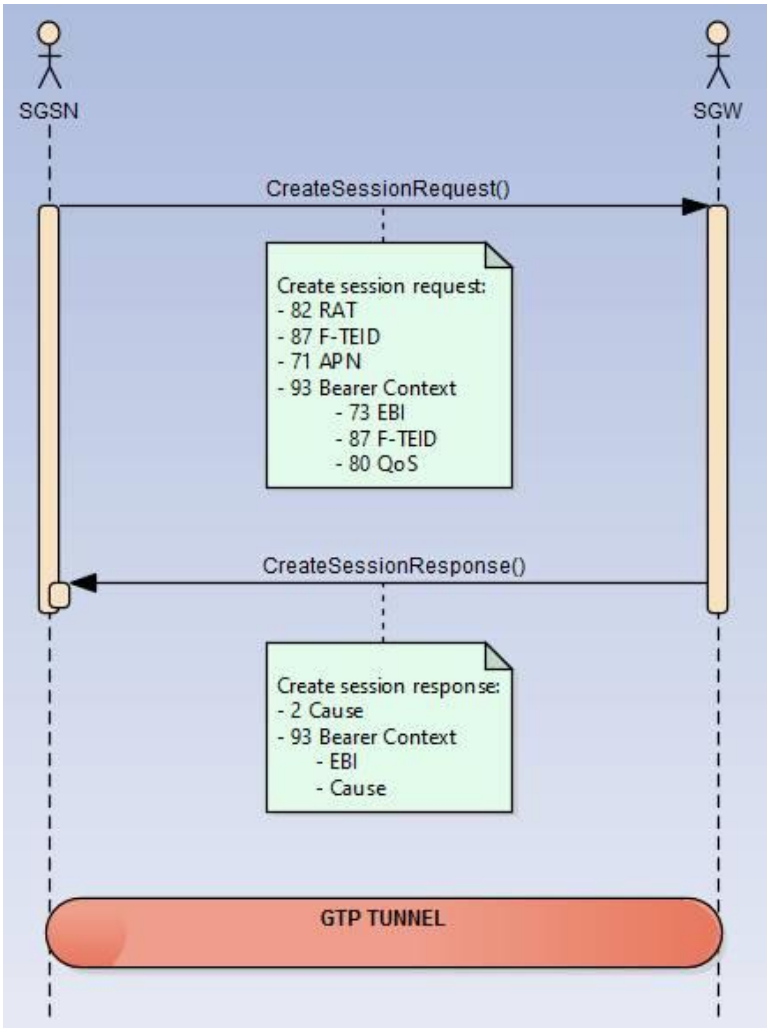
Na obrázku 18 sa nachádza testovacia architektúra pomocou ktorej sa bude dať overiť riešenie. Červenou je znázornený návrh rozhrania S4, ktoré bude pridané medzi SGSN a SGW.



Obrázok 18 – Testovacai architektúra

4.2 Vytvorenie GTP tunela

Na obrázku 19 je znázornená výmena správ Create Session Request a Create Session Response, ktoré vytvoria GTP tunel. Po analýze týchto správ sa podarilo z 3GPP štandardov zistiť povinné informačné elementy, ktoré sa musia v týchto správach nachádzať. Nie je vylúčené, že pri implementácii bude potrebné doimplementovať aj ďalšie, ktoré boli uvádzané ako podmienené. Pre návrh však stačí spomenúť povinné.



Obrázok 19: Proces vytvorenia GTP tunela

4.3 Doplnenie do openBSC

V prvom rade je na strane SGSN pri Attach Request správe potrebné zistiť, či je mobilná stanica schopná pripojenia k LTE sieti. Ak áno, treba vytvoriť GTP tunel na S4 rozhraní smerom k SGW. V analýze je detailnejšie uvedené, ktorý bit deteguje podporu mobilnej stanice k EPC. Jedná sa o EPC capability bit, ktorého kontrolu je potrebné do osmoSGSN doimplementovať.

Do openBSC, konktrétne do osmoSGSN, je taktiež potrebné doplniť podporu pre protokol GTPv2-C. Tento problém sme sa rozhodli vyriešiť použitím knižnice nw-gtpv2c, ktorá sa používa v projekte nwEPC.

Vytvorenie správy Create Session Request potrebnej pri vytváraní tunela je znázornené na obrázku vyššie a takisto toto vytvorenie správa treba doimplementovať. Formát použitej hlavičky aj povinné informačné elementy sú bližšie znázornené v analýze. Pri návrhu rozšírenia openBSC boli dodržané všetky postupy podľa 3GPP štandardov.

4.4 Doplnenie do nwEPC

Na strane nwEPC je takisto potrebné doplniť S4 rozhranie. Treba doimplementovať prijatie a spracovanie správy Create Session Request odosielanej z SGSN. Na túto správu je potom potrebné

vytvoriť odpoved Create Session Response, aby bol úspešne vytvorený GTP tunel. Samozrejme, odpoveď môže byť aj taká, že sa tunel vytvoriť nepodarilo. Formát použitej hlavičky aj povinné informačné elementy sú bližšie znázornené v analýze.

V prípade prichádzajúcich správ z PDN siete je takisto potrebné podľa vytvoreného bearera k UE rozhodnúť, či bude správa odosielaná S1 rozhraním, alebo S4 rozhraním. Táto funkcionalitu bude taktiež doimplementovaná. Pri návrhu rozšírenia nwEPC boli dodržané všetky postupy podľa 3GPP štandardov.

5 Implementácia

5.1 Použité existujúce riešenia

Pri implementácii (a testovaní) boli použité nasledujúce existujúce projekty:

- **openBSC**
- **nwEPC**
- libosmocore
- libosmo-netif
- libosmo-abis
- libosmo-sccp
- openggsn

Všetky tieto projekty majú otvorený zdrojový kód. Zmeny sme spravili len v projektoch openBSC a nwEPC. Repozitáre s použitými verzia jednotlivých projektov a našimi zmenami sú dostupné na adrese: https://github.com/S4Tukabel

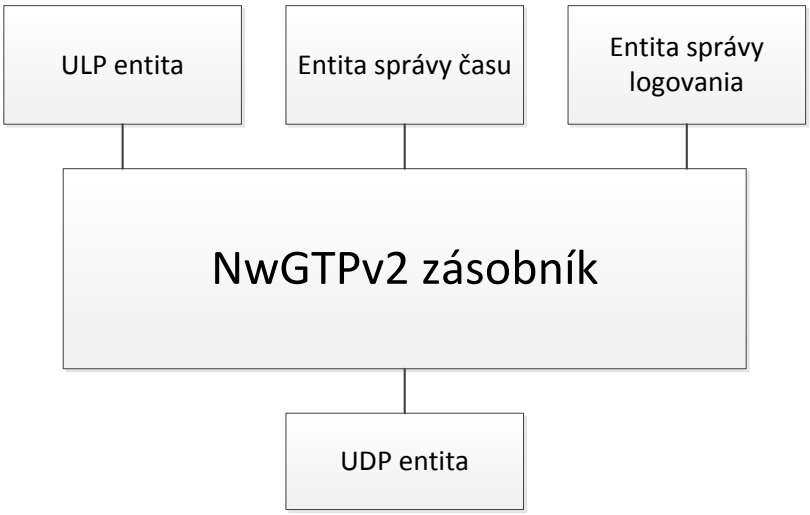
5.2 openBSC

5.2.1 Pridanie podpory GTPv2

Na pridanie podpory GTPv2 bola použitá voľne dostupná knižnica nwGTPv2, ktorá implementuje protokol GTPv2 známy aj ako eGTP-C podľa štandardu 3GPP TS 29.274. Knižnica je súčasťou projektu nwEPC. Podporuje správu transakcií, vytváranie a parsovanie správ, overenie správy, echo reakciu a správu opakovaného prenosu.

Zásobník (stack) knižnice nwGTPv2 je navrhnutý s ohľadom na vysokú prenositeľnosť. Pre niektoré utility infraštruktúry ako vstup/výstup, logovanie, časovanie alebo viacvláknovosť sa knižnica spolieha na používateľskú aplikáciu. Na toto sa používa mechanizmus spätného volania (callback). Na obrázku 20 sú znázornené externé entity, na ktorých je knižnica postavená [**11**].

- **User Layer Protocol (ULP) entita** - Táto entita určuje správanie používateľskej GTP aplikácie. V tejto vrstve je implementovaná inteligentná logika pre GTP aplikácie, ktoré stavajú na GTP zásobníku.
- **UDP entita** - Vrstva pod GTP zásobníkom zodpovedná za UDP vstup/výstup medzi zásobníkom a sieťou.
- **Entita správy času**
- **Entita správy logovania**



Obrázok 20: Externé entity knižnice nwGTPv2

Tieto entity sú vytvárané vo funkcii `S4Initialize()`, ktorej definícia sa nachádza v súbore `sgsn_s4.c`. Ak základ poslúžia inicializácia vo vzorových aplikáciách `nw-egtping` a `nw-helloworld`. Vytvorené entity sú z pamäte uvoľnené volaním funkcie `S4Finalize()` pri ukončení SGSN.

5.2.2 EPC Capability Flag

Pri pripájaní telefónu do siete vytvára openBSC každému účastníkovi štruktúru s názvom `sgsn_mm_ctx`. Tá obsahuje všetky informácie, ktoré telefón posiela pri Attach Request. Táto štruktúra obsahuje štruktúru `ms_network_capa`, kde je uložený celý MS Network Capability. Podľa špecifikácie sme preto vytvorili funkciu, ktorá nám vráti potrebný EPC Capability Flag:

```
/* Determines whether the EPC capability flag is present and set in */
/* MS Network Capability IE  (TS 24.008 v10.15.0 section 10.5.5.12)*/
int sgsn_mm_ctx_is_epc_capable(struct sgsn_mm_ctx *mmctx)
{
	return (mmctx->ms_network_capa.len >= 3
		&& (mmctx->ms_network_capa.buf[2] & 0b100));

}
```

5.2.3 Konverzia IMSI, MSISDN a IMEI

Keďže openBSC si ukladá informácie o IMSI, MSISDN a IMEI v textovom formáte a knižnica nwgtpv2c požaduje tieto údaje ako array s big endian číslami. Vytvorená funkcia prerába tento string na požadované pole:

```
static void imsi_str2arr(char *str, NwU8T *imsi)
{
	unsigned int n;
	unsigned int imsi_len = strlen(str);

	for (n = 0; n < 16; n += 2) {
		NwU8T val;
		if (n < imsi_len)
			val = (str[n]-'0') & 0xf;
		else
			val = 0xf;
		   if (n + 1 < imsi_len)
		       val = val | (((str[n + 1]-'0') & 0xf) << 4);
		   else
		       val = val | (0xf << 4);

		   imsi[n / 2] = val;
	}
}
```

5.2.4 Posielanie Create Session Request

Ak príde na SGSN Activate PDP Request a telefón má nastavený EPC Capability Flag, posiela sa Create Session Request na nwEPC. Pre zachovanie funkčnosti siete sa pošle aj štandardný Activate PDP Request. Create Session Request vytvorí paket s nasledujúcimi hodnotami, ktorý odošle na adresu nwEPC. Obsah odoslaných polí sme vyplnili podľa 3GPP TS 24.008 v10.15.0:

- Hlavička: CREATE SESSION REQ, TEID 0
- IMSI
- MSISDN
- IMEI
- RAT Type –GERAN (2)
- Serving Network (MCC, MCN)
- FTEID
  - Instance 0
  - Type S4_SGSN_GTPC (17)
  - Teid – náhodne generované pre každý pripojený telefón
  - IPv4: SGSN adresa
- Selection Mode – 2
- PDN type – IPv4
- PAA – IPv4: 0.0.0.0
- APN – „internet“
- APN Restriction – No restriction (0)
- Bearer Context
  - EBI – 5 (first usable)
  - FTEID
    - Instance 2
    - Type S4_SGSN_GTPU (15)
    - Teid – 3 (chyba – nevytvorilo viac ako jeden bearer)
    - IPv4: SGSN adresa
  - QOS

- Qci – 1
- maximumBitRateUplink: 0
- maximumBitRateDownlink: 0
- guaranteedBitRateUplink: 0
- guaranteedBitRateDownlink: 0

5.3 nwEPC

Kvôli rozsiahlej analýze, potrebnej na vypracovanie tohto projektu a neskoršiemu nedostatku času na implementáciu sa nerobili žiadne zmeny na nwEPC. Create Session Request sa posiela priamo na S5 rozhranie PGW, ktorý na neho odpovie:

- Hlavička: CREATE SESSION RESPONSE, TEID vygenerované
- CAUSE: REQUEST ACCEPTED
- PAA – IPv4: pridelená IP
- APN Restriction (z požiadavky)
- FTEID
    - Instance 1
    - Type S5/S8_PGW_GTPC (7)
    - Teid – pridelené
    - IPv4: PGW adresa
- Bearer Context
    - EBI – (z požiadavky)
    - CAUSE: REQUEST ACCEPTED
    - FTEID
        - Instance 2
        - Type S5/S8_PGW_GTPU (5)
        - Teid – pridelené
        - IPv4: PGW adresa

5.4 Kódové označenie projektu: S4Tukabel

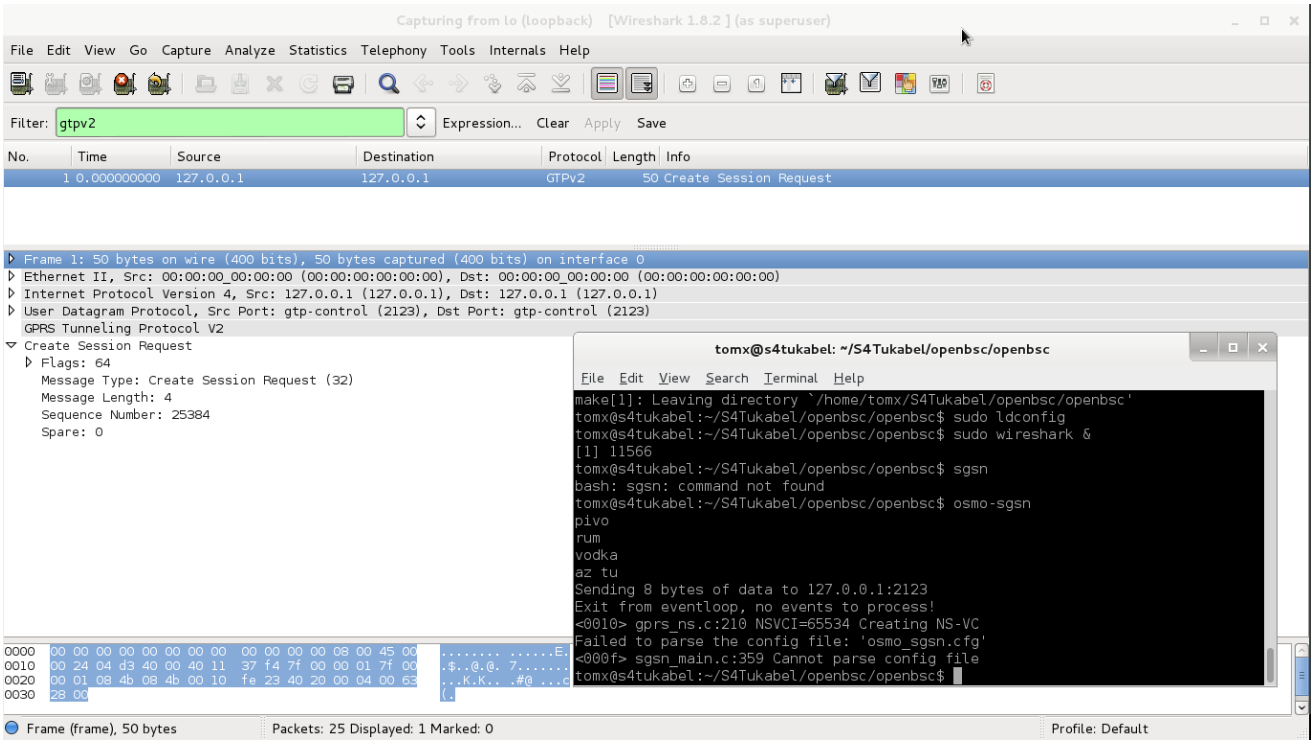
Pre projekt bolo zvolené kódové označenie S4Tukabel a taktiež bolo vytvorené logo, ktoré je zobrazené na obrázku 21.

Obrázok 21: Logo projektu S4Tukabel

6 Testovanie

6.1 Odoslanie prázdnej GTPv2 správy z SGSN

Na obrázku 22 je zobrazené testovanie odoslania prázdnej správy. Správu sme odosielali na S5 rozhranie PGW, keďže vytváranie tunela prebieha obdobne ako na rozhraní S4.



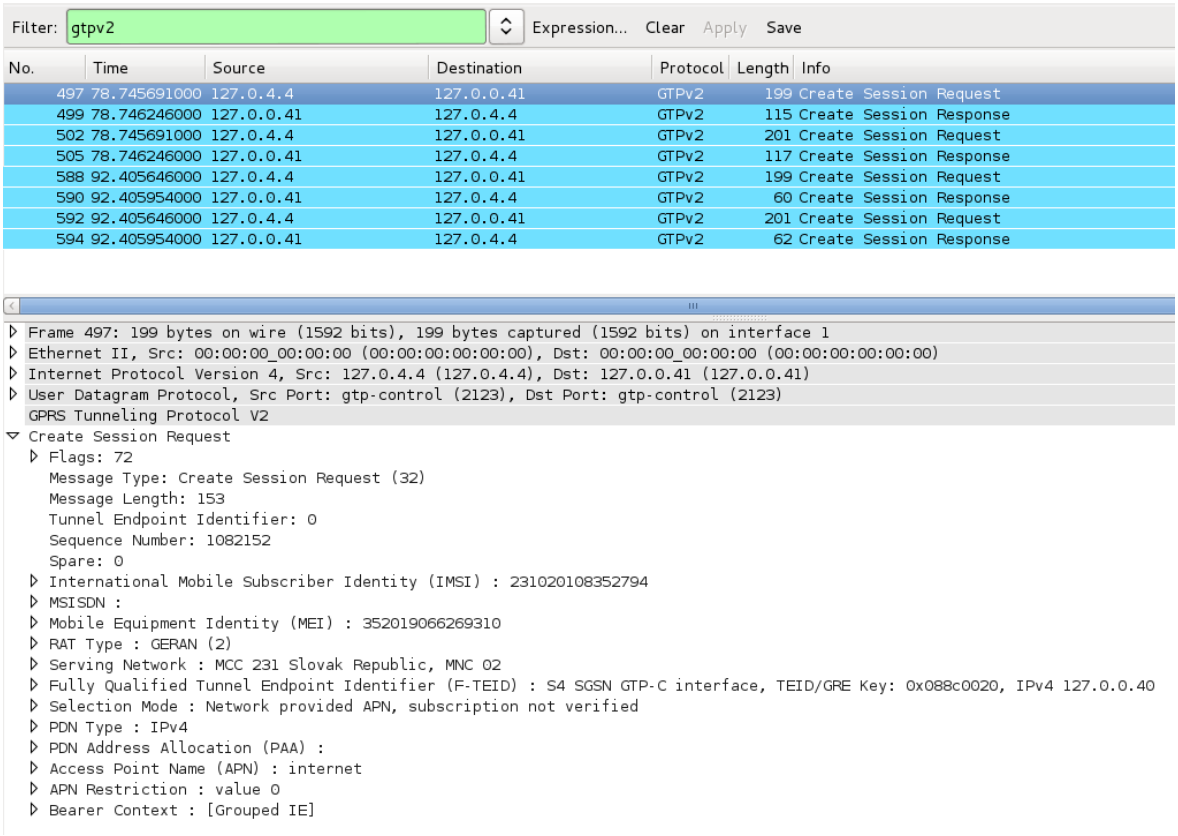
Obrázok 22: Odoslanie prázdnej GTPv2 správy z SGSN

6.2 Odoslanie správy Create session request

Odoslanie správy Crete session request bolo testované pripojením mobilného telefónu so zapnutou podporou EPC (4G). Výstup modifikovanej SGSN na konzolu je zobrazený na obrázku 23. Správu zachytenú nás wireshark je možné vidieť na obrázku 24. Hodnoty v informačných elementoch bola overená manuálne a pokial to bolo môžné boli porovnané aj prislúchajúcimi informačnými elementami v správe Create PDP context Request odosielanej na GGSN.

```
<0011> gprs_bssgp.c:377 BSSGP TLLI=0x9dbf7f23 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=1 C   FCS=0xbeea02CMD=UI DATA
<0002> gprs_gmm.c:797 MM(/c3743a89) -> GMM IDENTITY RESPONSE: mi_type=0x02 MI(352019066269310)
<0002> gprs_gmm.c:424 MM(/c3743a89) <- GPRS IDENTITY REQUEST: mi_type=01
<0010> gprs_ns.c:547 NSEI=101 Timer expired in mode tns-test (30 seconds)
<0010> gprs_ns.c:490 NSEI=101 Tx NS ALIVE (NSVCI=101)
<0010> gprs_ns.c:529 NSEI=101 Starting timer in mode tns-alive (3 seconds)
<0010> gprs_ns.c:529 NSEI=101 Starting timer in mode tns-test (30 seconds)
<0010> gprs_ns.c:503 NSEI=101 Tx NS ALIVE_ACK (NSVCI=101)
<0011> gprs_bssgp.c:795 BSSGP BVCI=2 Rx Flow Control BVC
<0011> gprs_bssgp.c:377 BSSGP TLLI=0x9dbf7f23 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=1 C   FCS=0x793b16CMD=UI DATA
<0002> gprs_gmm.c:797 MM(/c3743a89) -> GMM IDENTITY RESPONSE: mi_type=0x01 MI(231020108352794)
<0002> sgsn_auth.c:157 MM(231020108352794/c3743a89) Requesting authorization
<0002> sgsn_auth.c:216 MM(231020108352794/c3743a89) Updating authorization (unknown -> accepted)
<0002> sgsn_auth.c:245 MM(231020108352794/c3743a89) Got authorization update: state unknown -> accepted
<0002> gprs_gmm.c:721 Authorized, continuing procedure, IMSI=231020108352794
<0002> gprs_gmm.c:311 MM(231020108352794/c3743a89) <- GPRS ATTACH ACCEPT (new P-TMSI=0xc3743a89)
<0011> gprs_bssgp.c:377 BSSGP TLLI=0xc3743a89 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=1 C   FCS=0xea1c55CMD=UI DATA
<0002> gprs_gmm.c:1357 MM(231020108352794/c3743a89) -> ATTACH COMPLETE
<0011> gprs_bssgp.c:377 BSSGP TLLI=0xc3743a89 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=1 C   FCS=0x57316aCMD=UI DATA
<0002> gprs_gmm.c:1856 MM(231020108352794/c3743a89) EPC capable message msg_type= 65
Sending 157 bytes of data to 127.0.0.41:2123
<0002> sgsn_s4.c:217 MM(231020108352794/c3743a89) -> CREATE SESSION REQ: IMSI=231020108352794 <TUKABEL>
<0002> gprs_gmm.c:1656 MM(231020108352794/c3743a89) -> ACTIVATE PDP CONTEXT REQ: SAPI=3 NSAPI=5 IETF IPv4
<0002> gprs_sgsn.c:723 MM(231020108352794/c3743a89) Found GGSN 0 for APN 'internet' (requested 'internet')
<0002> gprs_gmm.c:1748 MM(231020108352794/c3743a89) Using GGSN 0
<000f> sgsn_libgtp.c:131 Create PDP Context
<001c> pdp.c:214 Begin pdp_tidset tid = 5497253801020132
<001c> pdp.c:223 End pdp_tidset
<000f> sgsn_libgtp.c:451 libgtp cb_conf(type=16, cause=128, pdp=0xb7302840, cbp=0x88c1db0)
<000f> sgsn_libgtp.c:315 PDP(231020108352794/0) Received CREATE PDP CTX CONF, cause=128(Request accepted)
```

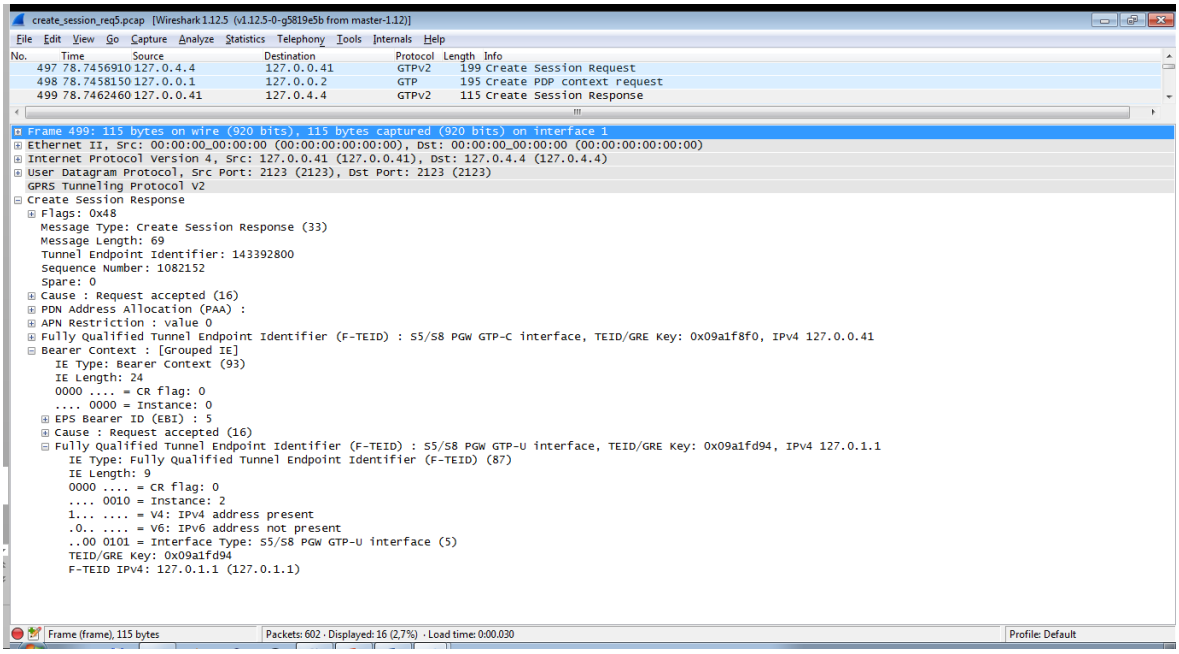
Obrázok 23: Výstup modifikovanej SGSN pri testovaní Create session request



Obrázok 24: GTP správy zachytené pri testovaní Create session request

6.3 Odpoveď Create session response

Ako bolo spomenuté v implementácii, správa Create session request bola odoslaná na PGW, ktorý odpovedal správou Create session response. Tým, že nwEPC odpovedalo úspešným vytvorením tunela sa podarilo dokázať, že nami vytvorená správa Create session request obsahuje všetky potrebné informácie.



Obrázok 25: Create session response odoslaná z PGW

7 Zhodnotenie

Na začiatku riešenia tohto projektu sa podarilo veľmi podrobne analyzovať všetky dôležité oblasti problematiky potrebné k ďalšiemu vývoju. Začali sme analýzou architektúry mobilnej siete (2G, 3G a 4G) a analýzou správ, ktoré sa v nej vymieňajú pri komunikácii medzi UE a ostatnými uzlami siete. Podarilo sa získať všetky teoretické informácie potrebné k tomu, aby bolo možné navrhnúť a implementovať S4 rozhranie medzi SGSN a GGSN umožňujúce prístup UE k PDN.

Práve pridanie S4 rozhrania medzi SGSN a GGSN bolo predmetom zadanie projektu, avšak narazili sme na niektoré informácie, ktoré trošku pozmenili znenie pôvodného zadania. Po navrhnutí S4 rozhrania prišla fáza implementovania do riešení s otvoreným zdrojovým kódom openBSC a openggsn. Pri vytváraní GTP tunela medzi SGSN a GGSN sme sa chceli inšpirovať v projekte nwEPC. Tu sa nám však podarilo zistiť, že nwEPC nemá implementovanú podporu pre S4 rozhranie, ktoré sa original v sieti nachádza medzi SGSN a SGW. Preto sme sa nakoniec rozhodli doiplmenetovať toto rozhranie medzi SGSN a SGW do projektov openBSC a nwEPC. Pri vytváraní tunela sme sa nakoniec aj tak inšpirovali v projekte nwEPC na rozhraní S5/S8 medzi SGW a PGW.

Do projektu osmoBSC bola pridaná podpora odosielania správy Create Session Request. Táto správa bola v rámci testovania odoslaná na S5 rozhranie PGW (v úlohe S4 rozhrania na SGW), ktorý odpovedal správou Create Session Response, v ktorej akceptoval vytvorenie tunela. Obe správy mali všetky povinné (mandatory) polia vyplnené podľa 3GPP štandardov. Toto riešenie môže byť použité ako základ pre kompletnú implementáciu rozhrania S4 podľa štandardu 3GPP.

8 Bibliography

[1] yusufd. (2013, Marec) Introduction into Mobile Core Network. [Online]. http://www.slideshare.net/yusufd/introduction-to-mobile-core-network-17667704

[2] Alcatel-Lucent. (2009) Introduction to Evolved Packet Core. [Online]. http://www.google.sk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCkQFjAB&url=http%3A%2F%2Fwww3.alcatel-lucent.com%2Fwps%2FDocumentStreamerServlet%3FLMSG_CABINET%3DDocs_and_Resource_Ctr%26LMSG_CONTENT_FILE%3DWhite_Papers%2FIntro_EPC_wp_0309.pdf&ei=UyBoV

[3] 3GPP. (2014, Október) ETSI TS 124.008 V 10.15.0. [Online]. http://www.etsi.org/deliver/etsi_ts/124000_124099/124008/10.15.00_60/ts_124008v101500p.pdf

[4] Juniper Networks. (2013, Február) Configuring GTP Services on the S4 Interface. [Online]. http://www.juniper.net/techpubs/en_US/junos-mobility12.1/topics/task/configuration/sgw-mobility-s4-configuring.html

[5] 3GPP. (2013, Január) ETSI TS 129.274 V 10.9.0. [Online]. http://www.etsi.org/deliver/etsi_ts/129200_129299/129274/

[6] Juniper Networks. (2013, Február) GPRS Tunneling Protocol (GTP) for GGSN/PDN. [Online]. http://www.juniper.net/techpubs/en_US/junos-mobility12.1/information-products/pathway-pages/gtp-pwp.pdf

[7] 3GPP. (2013, Apríl) ETSI TS 123.401 V 8.18.0. [Online]. http://www.etsi.org/deliver/etsi_ts/123400_123499/123401/08.18.00_60/ts_123401v081800p.pdf

[8] 3GPP. (2011, Október) ETSI TS 129.281 V 10.3.0. [Online]. http://www.etsi.org/deliver/etsi_ts/129200_129299/129281/10.03.00_60/ts_129281v100300p.pdf

[9] Netmanias. (2013, September) LTE GTP Tunnel. [Online]. http://www.netmanias.com/ko/post/blog/5836/lte-gtp-eps-bearer/lte-gtp-tunnel-i

[10] Apis. (2014) GPRS Tunneling Protocol - GTP.

[11] amitchawre. nwGTPv2 - eGTP Stack Library. [Online]. http://sourceforge.net/projects/nwgtpv2/files/