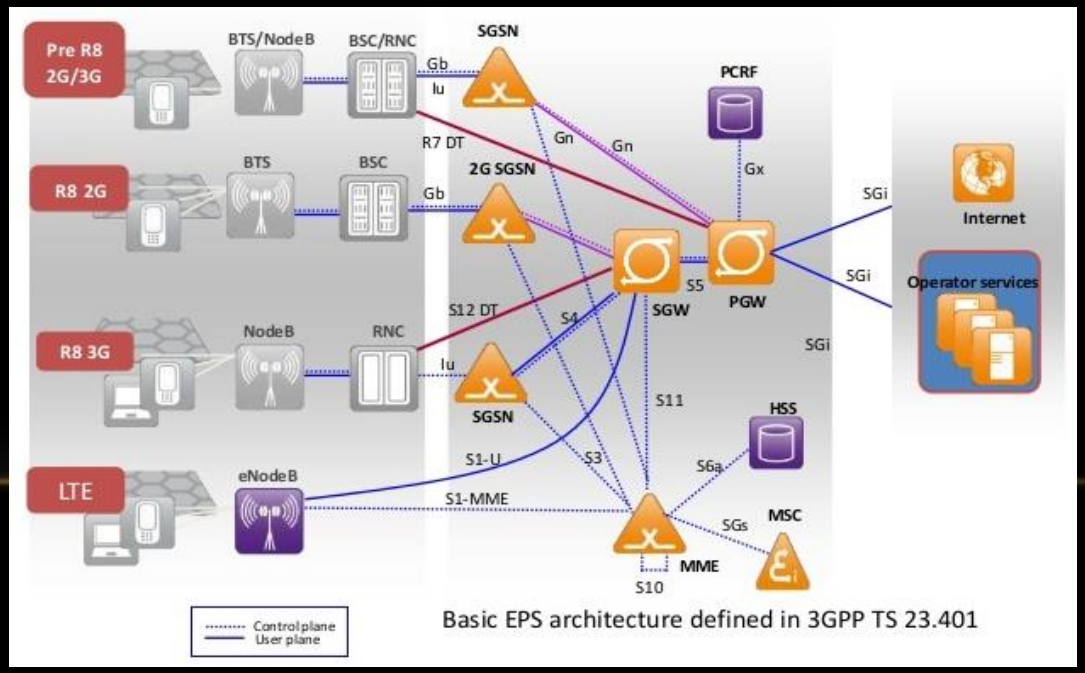
S4 TUKABEL

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

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

ZADANIE

- **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)~~
  - Doplnenie rozhrania S4 (signalizácia a používateľské dáta) do nwEPC (GTPC/GTP-U)



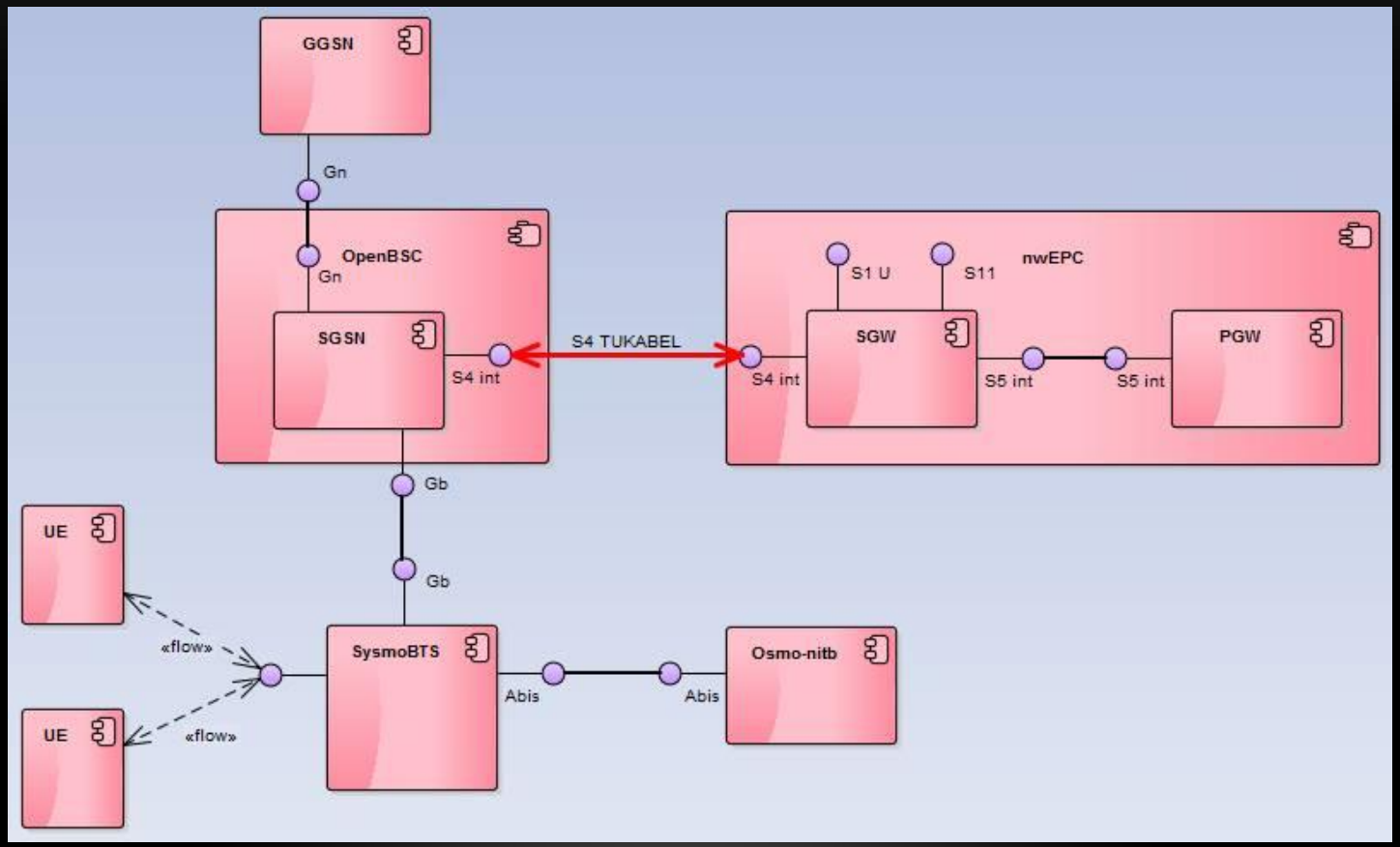
MOTIVÁCIA

- Zatiaľ neimplementované S4 rozhranie v riešeniach s voľne dostupným zdrojovým kódom openBSC a nwEPC
- Prechod z 2G/3G sietí do LTE siete (SGSN -> SGW)
- Urobiť poslednú skúšku ako sieťari ☺

ZÁKLADNÉ KOMPONENTY

- SGSN (Service GPRS Support Node)
  - Tunelovanie IP paketov, detunelovanie GTP paketov
  - Manažment mobility (attach/detach), účtovanie používateľských dát
- GGSN (Gateway GPRS Support Node)
  - Spolupráca medzi GPRS sieťou a vonkajšou sieťou s prepínaním paketov
- SGW (Serving Gateway)
  - Bod ukotvenia medzi LTE a inými 3GPP technológiami
  - Ukončenie S4 rozhrania a spracovanie premávky medzi 2G/3G systémami a PGW
- PGW (Packet Data Network Gateway)
  - Poskytuje konektivitu UE k externým PDN

NÁVRH S4 ROZHRANIA



AKO SGSN VIE ŽE MÁ MS PRIPOJIŤ DO LTE?

- GPRS Mobility Management správa Attach Request
- MS odosiela do siete Attach Request z dôvodu vytvorenia spojenia
- Informačný element (IE) MS network capability
- V IE, v poli value, sa nachádza bit EPC capability -> indikuje podporu prístupu MS na EPC
  - 0 EPC nie je podporované
  - 1 EPC je podporované

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

EPC CAPABILITY

```
⊞ 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
```

S4 ROZHRANIE

- Na S4 rozhraní sa používajú protokoly GTP-U pre používateľskú rovinu a GTPv2-C pre riadiacu rovinu
- GTPv2-C: signalizácia, úprava QoS, vytvorenie, správa a vymazanie GTP tunelov
- GTP-U: prenos používateľských dát cez GTP tunely
- Pre vytvorenie a vymazanie tunela 4 základné typy správ (GTPv2-C –> Message Type):
  - Create Session Request/Response
  - Delete Session Request/Response

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							

GTP-U

- Všeobecný formát hlavičky
- Tu nás zaujíma iba TEID

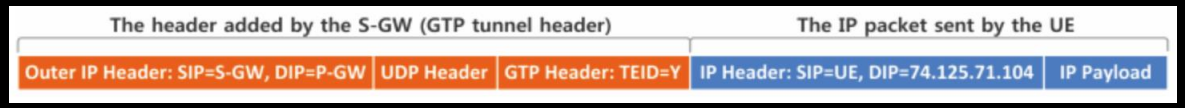
Octets	Bits 8	7	6	5	4	3	2	1
1	Version			PT	(*)	E	S	PN
2	Message Type							
3	Length (1st Octet)							
4	Length (2nd Octet)							
5	Tunnel Endpoint Identifier (1st Octet)							
6	Tunnel Endpoint Identifier (2nd Octet)							
7	Tunnel Endpoint Identifier (3rd Octet)							
8	Tunnel Endpoint Identifier (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)							

VYTVORENIE GTP TUNELA (V LTE)

- UE -> eNodeB

- eNodeB -> SGW

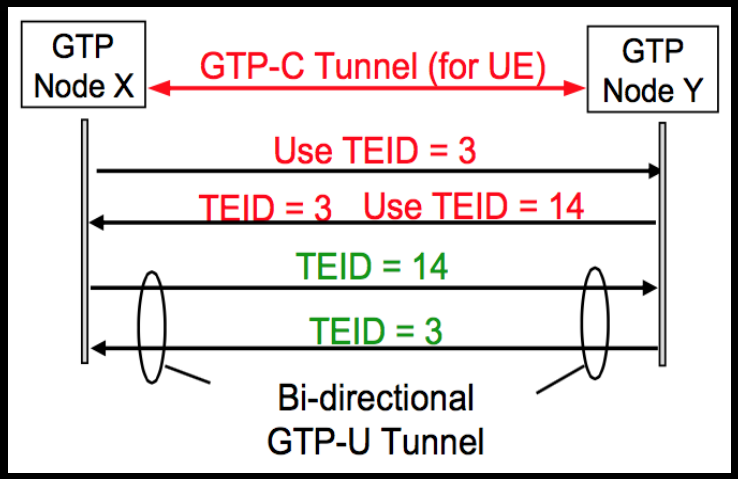
- SGW -> PGW



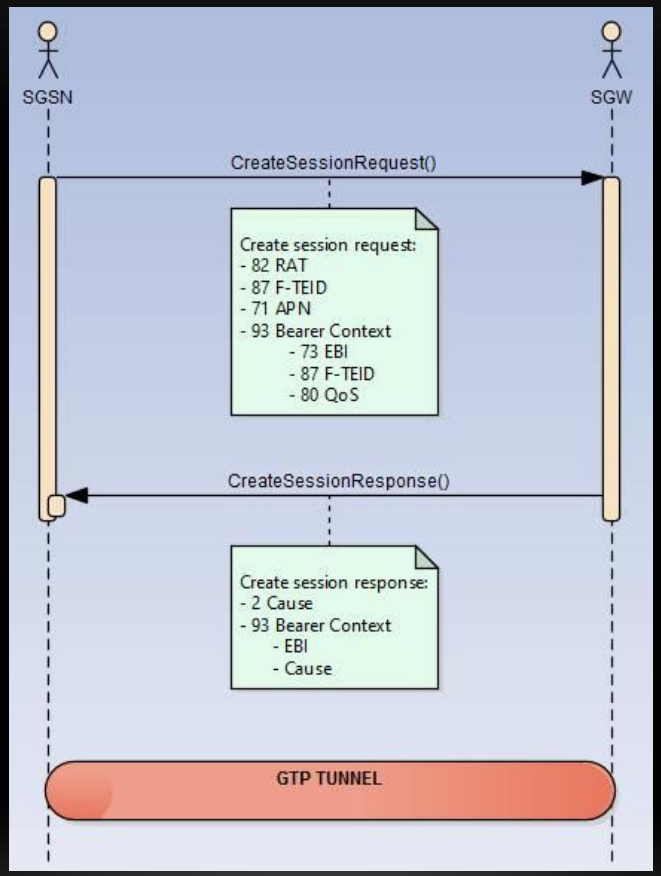
- PGW -> PDN

PROCES VÝMENY TEID

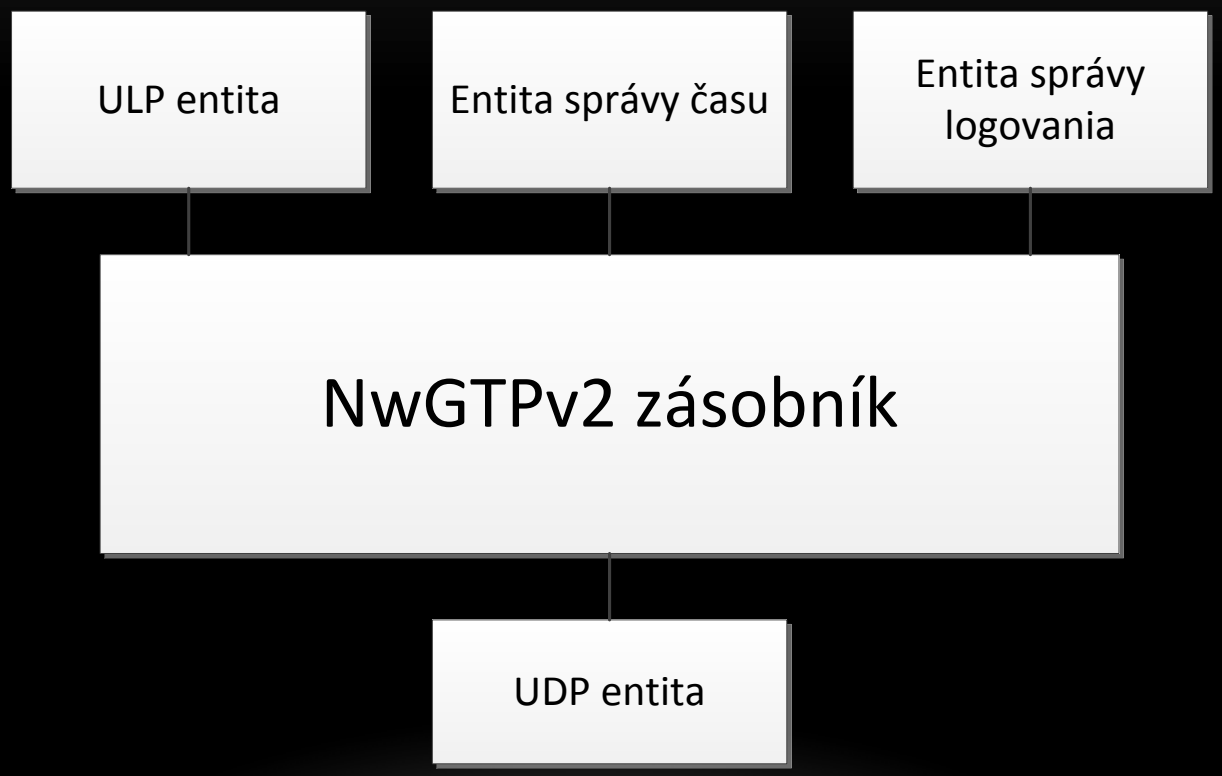
- Hodnoty TEID v Create Session Request
  - TEID v GTP hlavičke= 0
  - TEID v IE „Sender F-TEID for Control Plane“ = 3
  - TEID v IE „Bearer Context to be created“ = 3
- Hodnoty TEID v Create Session Response
  - TEID v GTP hlavičke= 3
  - TEID v IE „Sender F-TEID for Control Plane“ = 14
  - TEID v IE „Bearer Context to be created“ = 14



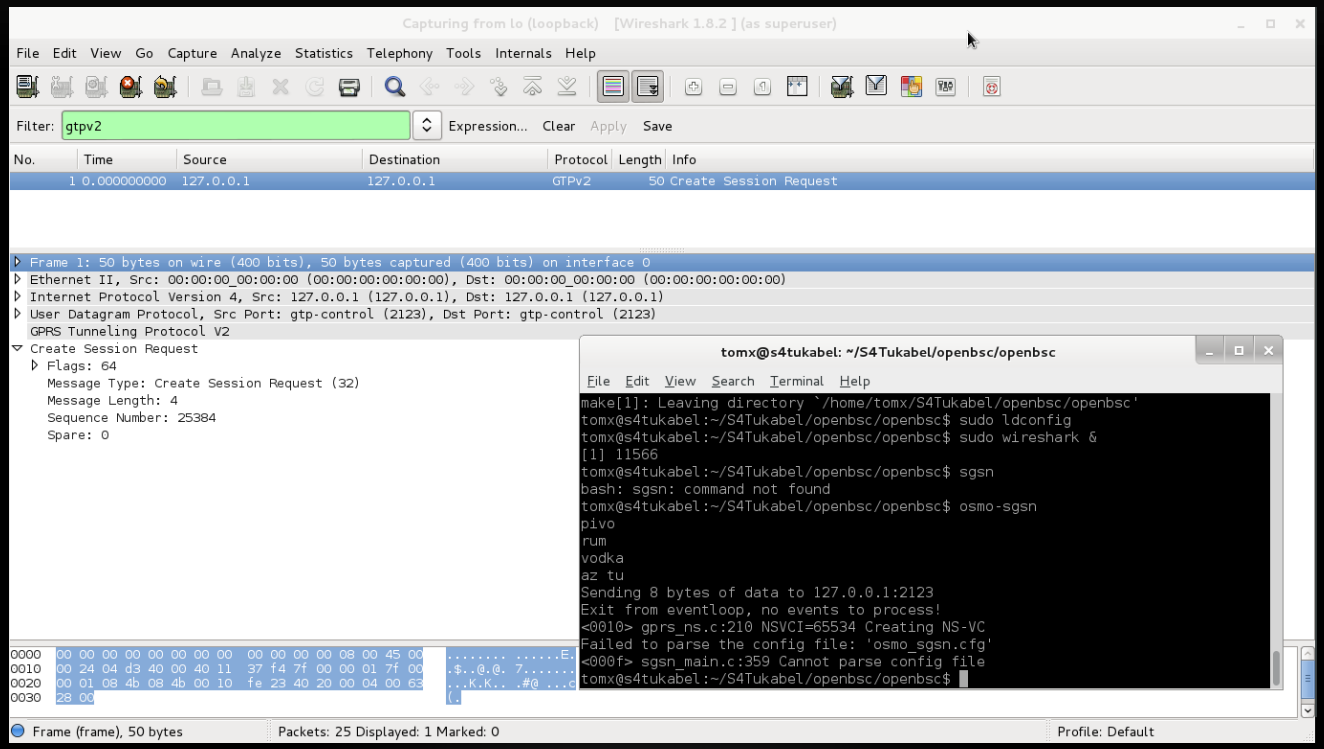
NAVRHNUTÉ VYTVORENIE GTP TUNELA



KNIŽNICA NwGTPv2



ODOSLANIE PRÁZDNEJ GTPV2-C SPRÁVY



ODOSLANIE CREATE SESSION REQUEST

```
<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)
```

CREATE SESSION REQUEST / RESPONSE

create_session_req5.pcap [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

No.	Time	Source	Destination	Protocol	Length	Info
497	78.7456910	127.0.4.4	127.0.0.41	GTPv2	199	Create Sess

```
⊞ Frame 497: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on in
⊞ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:0
⊞ Internet Protocol Version 4, Src: 127.0.4.4 (127.0.4.4), Dst: 127.0.0.41 (127.
⊞ User Datagram Protocol, Src Port: 2123 (2123), Dst Port: 2123 (2123)
  GPRS Tunneling Protocol V2
⊟ Create Session Request
  ⊞ Flags: 0x48
    Message Type: Create Session Request (32)
    Message Length: 153
    Tunnel Endpoint Identifier: 0
    Sequence Number: 1082152
    Spare: 0
  ⊞ International Mobile Subscriber Identity (IMSI) : 231020108352794
  ⊞ MSISDN : ?
  ⊞ Mobile Equipment Identity (MEI) : 352019066269310
  ⊞ RAT Type : GERAN (2)
  ⊞ Serving Network : MCC 231 Slovak Republic, MNC 02
  ⊞ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S4 SGSN GTP-C interfac
  ⊞ Selection Mode : Network provided APN, subscription not verified
  ⊞ PDN Type : IPv4
  ⊟ PDN Address Allocation (PAA) :
      IE Type: PDN Address Allocation (PAA) (79)
      IE Length: 5
      0000 .... = CR flag: 0
      .... 0000 = Instance: 0
      .... .001 = PDN Type: IPv4 (1)
      PDN Address and Prefix(IPv4): 0.0.0.0 (0.0.0.0)
  ⊞ Access Point Name (APN) : internet
  ⊞ APN Restriction : value 0
  ⊟ Bearer Context : [Grouped IE]
      IE Type: Bearer Context (93)
      IE Length: 44
      0000 .... = CR flag: 0
      .... 0000 = Instance: 0
    ⊞ EPS Bearer ID (EBI) : 5
    ⊞ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S4 SGSN GTP-U interf
```

Frame (frame), 199 bytes | Packets: 602 · Displayed: 16 (... | Profile: Default

create_session_req5.pcap [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

No.	Time	Source	Destination	Protocol	Length	Info
505	78.7462460	127.0.0.41	127.0.4.4	GTPv2	117	Create Sess

```
⊞ Frame 505: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interfa
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 127.0.0.41 (127.0.0.41), Dst: 127.0.4.4 (127.0.
⊞ User Datagram Protocol, Src Port: 2123 (2123), Dst Port: 2123 (2123)
  GPRS Tunneling Protocol V2
⊟ Create Session Response
  ⊞ Flags: 0x48
    Message Type: Create Session Response (33)
    Message Length: 69
    Tunnel Endpoint Identifier: 143392800
    Sequence Number: 1082152
    Spare: 0
  ⊞ Cause : Request accepted (16)
  ⊟ PDN Address Allocation (PAA) :
      IE Type: PDN Address Allocation (PAA) (79)
      IE Length: 5
      0000 .... = CR flag: 0
      .... 0000 = Instance: 0
      .... .001 = PDN Type: IPv4 (1)
      PDN Address and Prefix(IPv4): 10.66.10.253 (10.66.10.253)
  ⊞ APN Restriction : value 0
  ⊞ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S5/S8 PGW GTP-C interface
  ⊟ Bearer Context : [Grouped IE]
      IE Type: Bearer Context (93)
      IE Length: 24
      0000 .... = CR flag: 0
      .... 0000 = Instance: 0
    ⊞ EPS Bearer ID (EBI) : 5
    ⊞ Cause : Request accepted (16)
    ⊞ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S5/S8 PGW GTP-U interfa
```

Text item (text), 28 bytes | Packets: 602 · Displayed: 16 (... | Profile: Default

DEMO

ĎAKUJEME