POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES

Безопасность мобильного интернета изнутри и снаружи

Сафронов Илья

Мобильный интернет снаружи

— APN : internet.operator.ru
— login: internet
— password: internet

APN(Access Point Name) – обозначение шлюза между мобильной сетью и другой сетью (например Интернет)

Процедура подключения

1. GPRS Attach
2. PDP Context Activation

GPRS Attach

- Начало общения абонентского терминала с пакетной сетью оператора начинается с процедуры GPRS Attach
- В процедуре GPRS Attach происходит аутентификация и авторизация по следующим параметрам:
  - Идентификация абонента(IMSI)
  - Аутентификация(Зашитый в SIM ключ)
  - Проверка IMEI (опционально)
  - Проверка доступных абоненту сервисов(Internet, MMS, WAP)
- После успешной процедуры GPRS Attach абонент может пользоваться услугами пакетной передачи данных (загорается значок).

3GPP TS 29.060

Словарик

SGSN

SGSN – Устройство обеспечивающее основные функции мобильной передачи пакетных данных

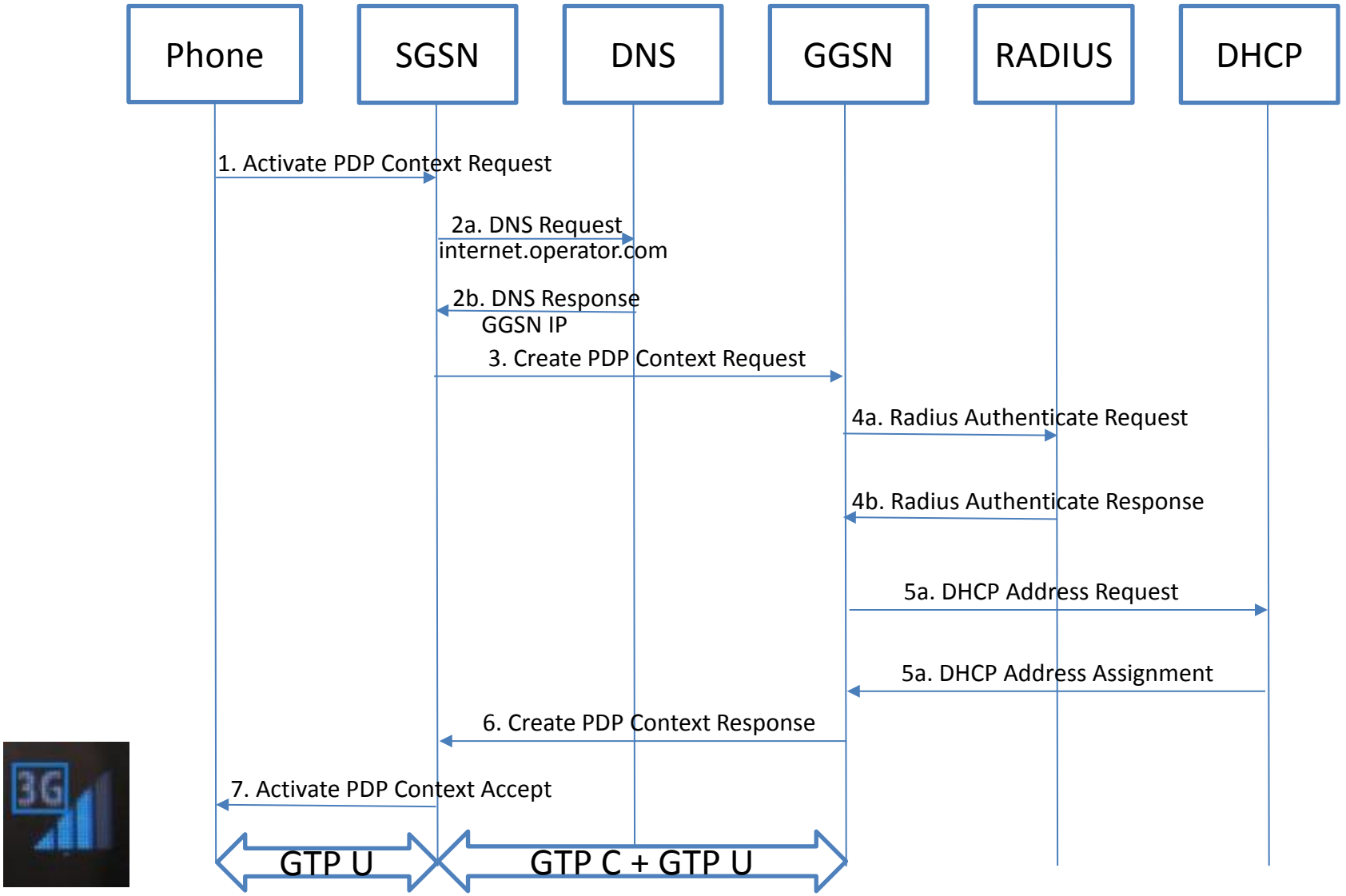
GGSN

GGSN – Маршрутизатор, обеспечивающий связь клиентов с внешними сетями (например Интернет) (APN)

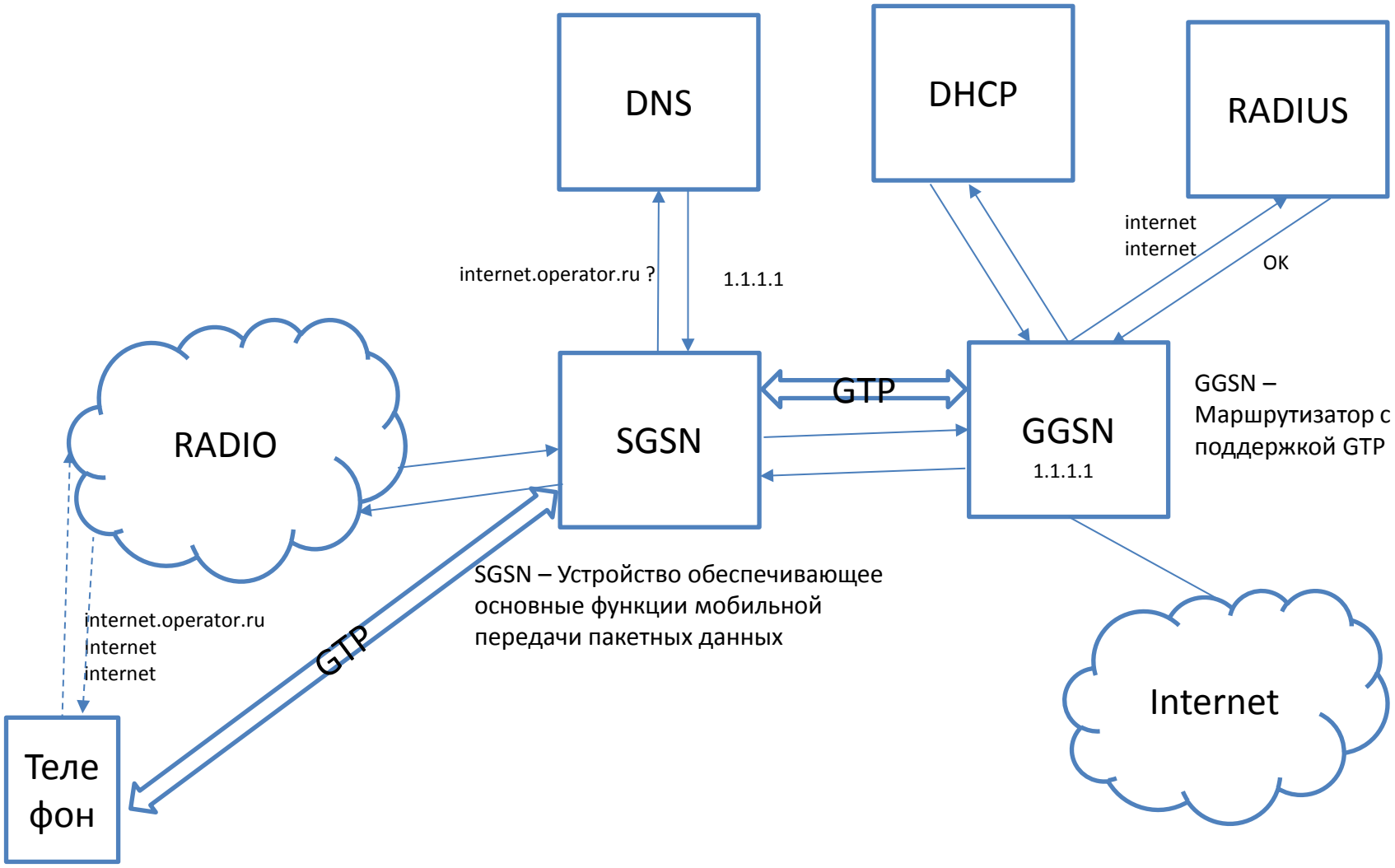
Группа протоколов туннелирования и управления пакетным трафиком в мобильных сетях

3GPP TS 29.060

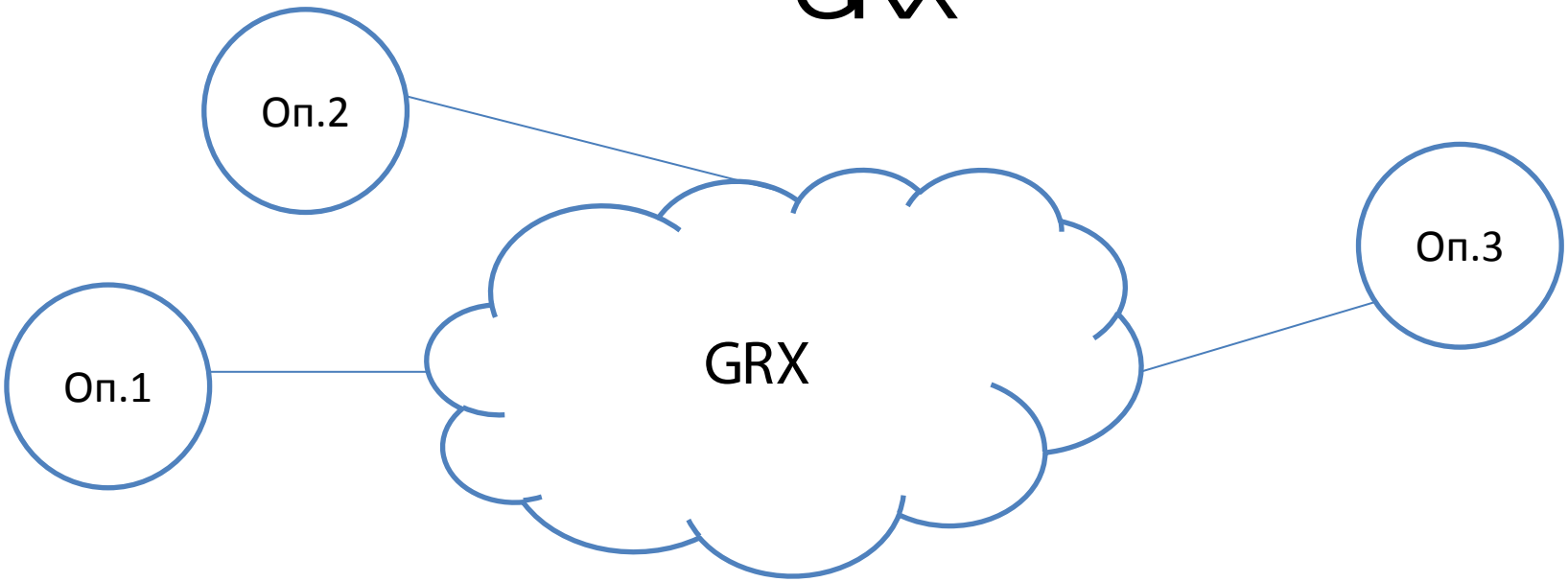
PDP Context Activation



Логическая схема подключения

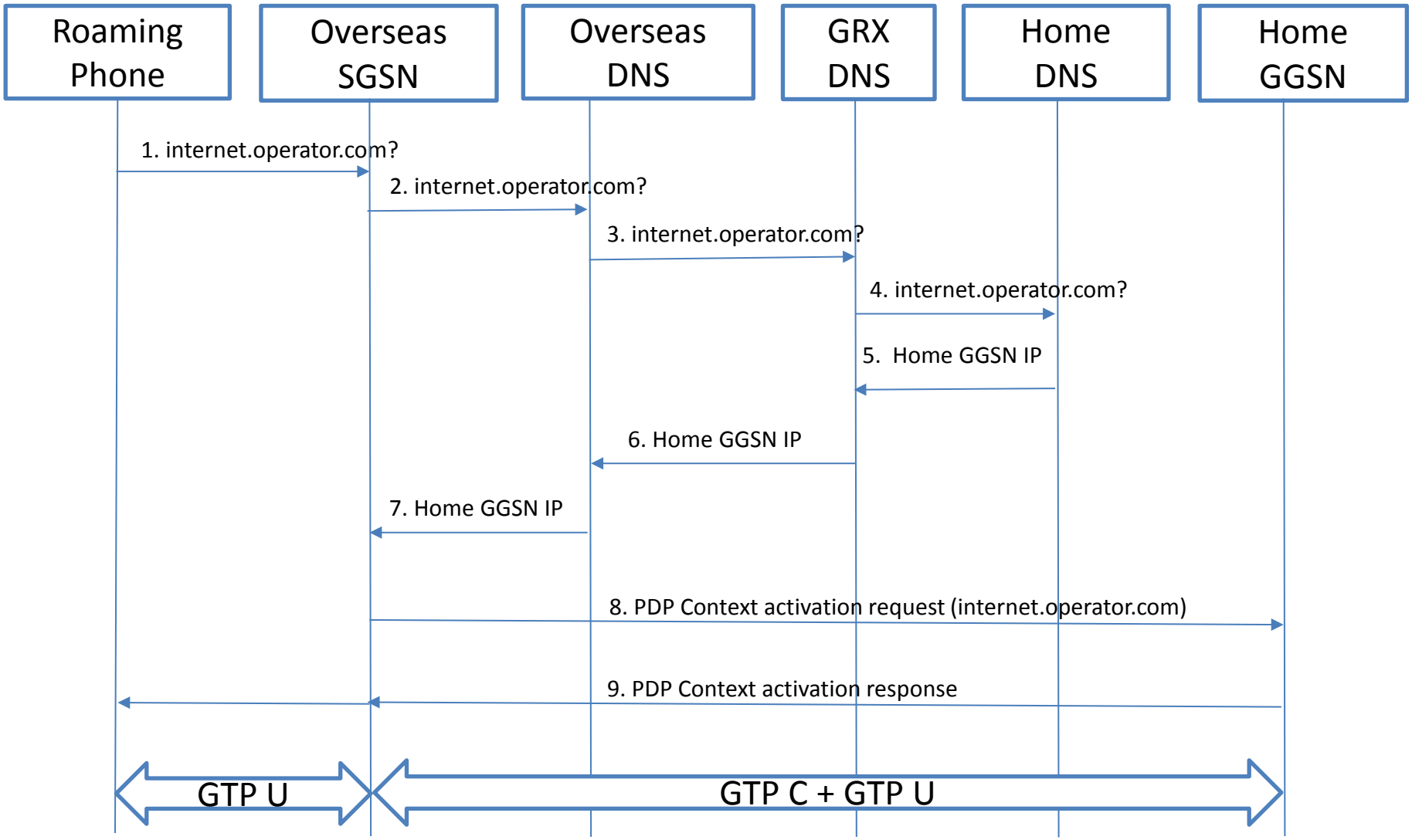


GRX



GRX (Global Roaming Exchange)– сеть для обмена пакетных данных роуминговых абонентов мобильных сетей

Internet Roaming



Интернет в роуминге for dummies

Домашний Оп.

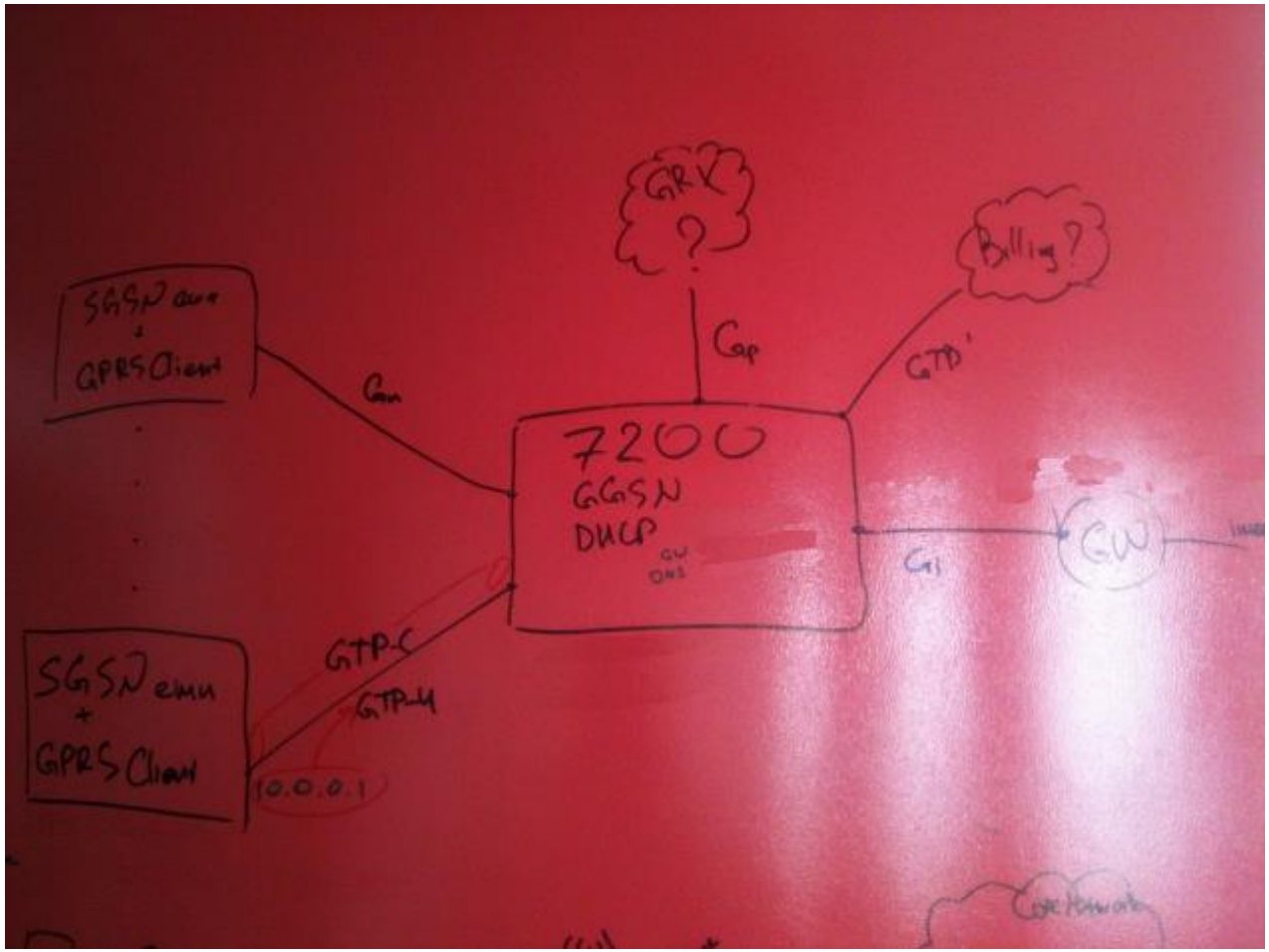
GRX

Интернет

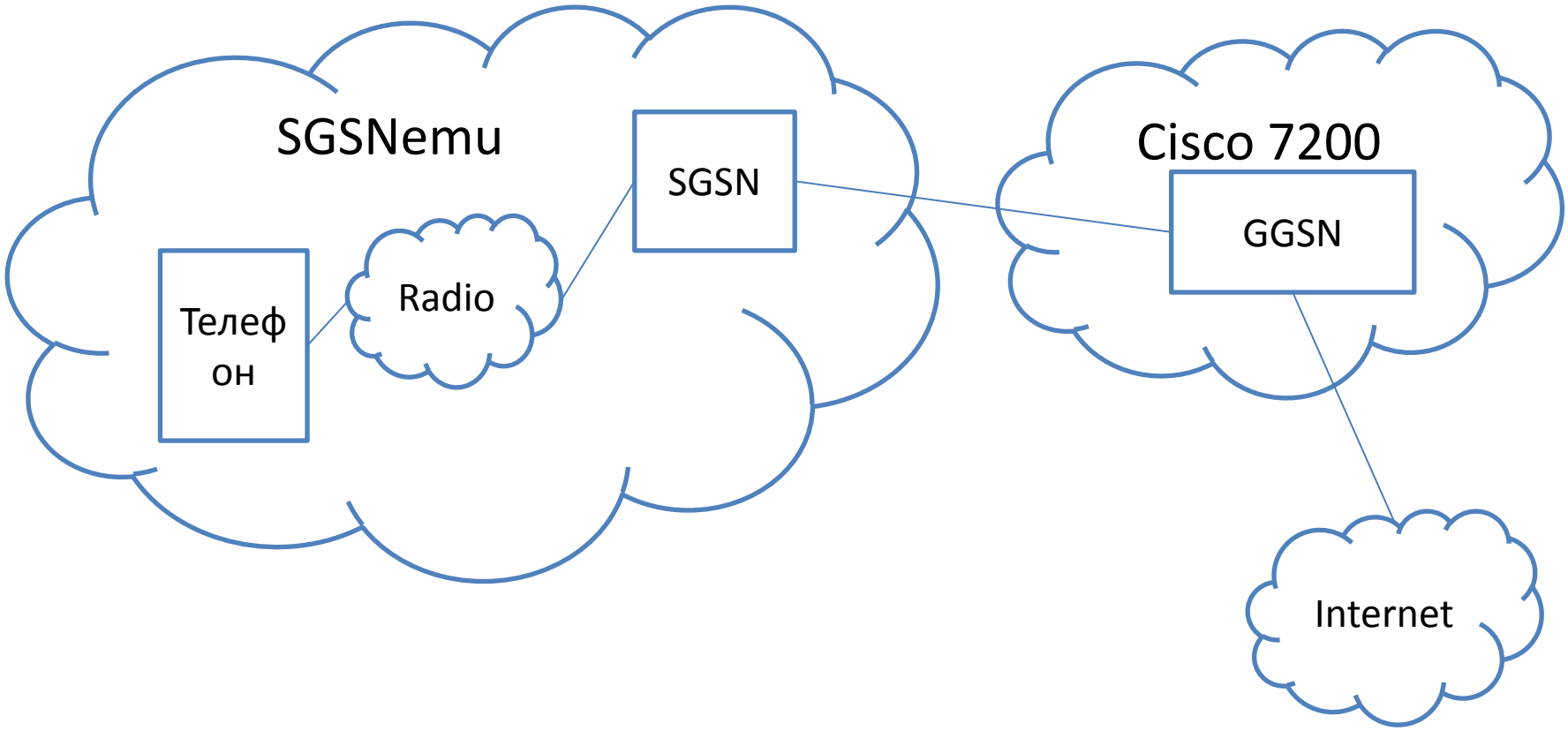
Зарубежный Оп.

Абонент в отпуске

SGSN+GGSN на коленке



Схема

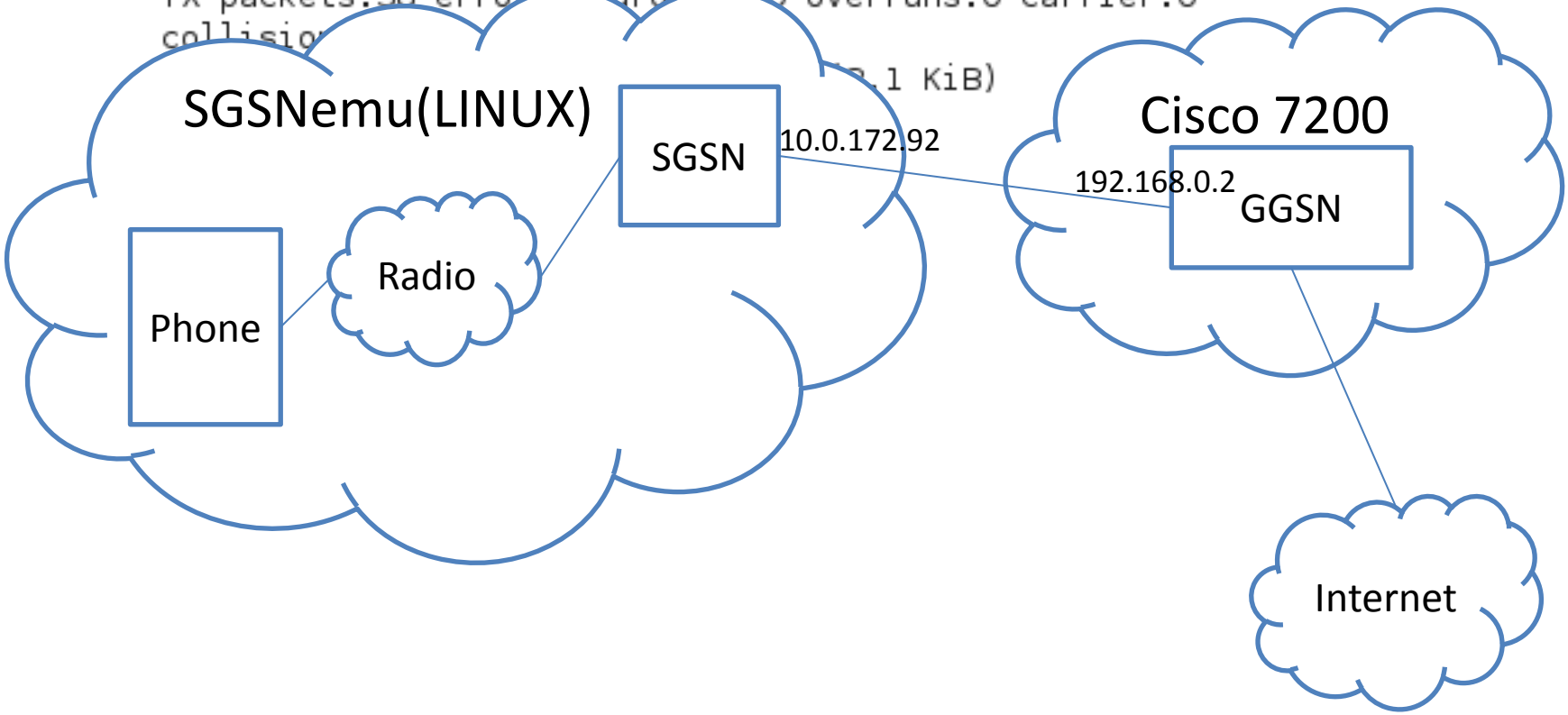


How it works

```
sgsnemu -l 10.0.172.92 -r 192.168.0.2 --createif --defaultroute
```

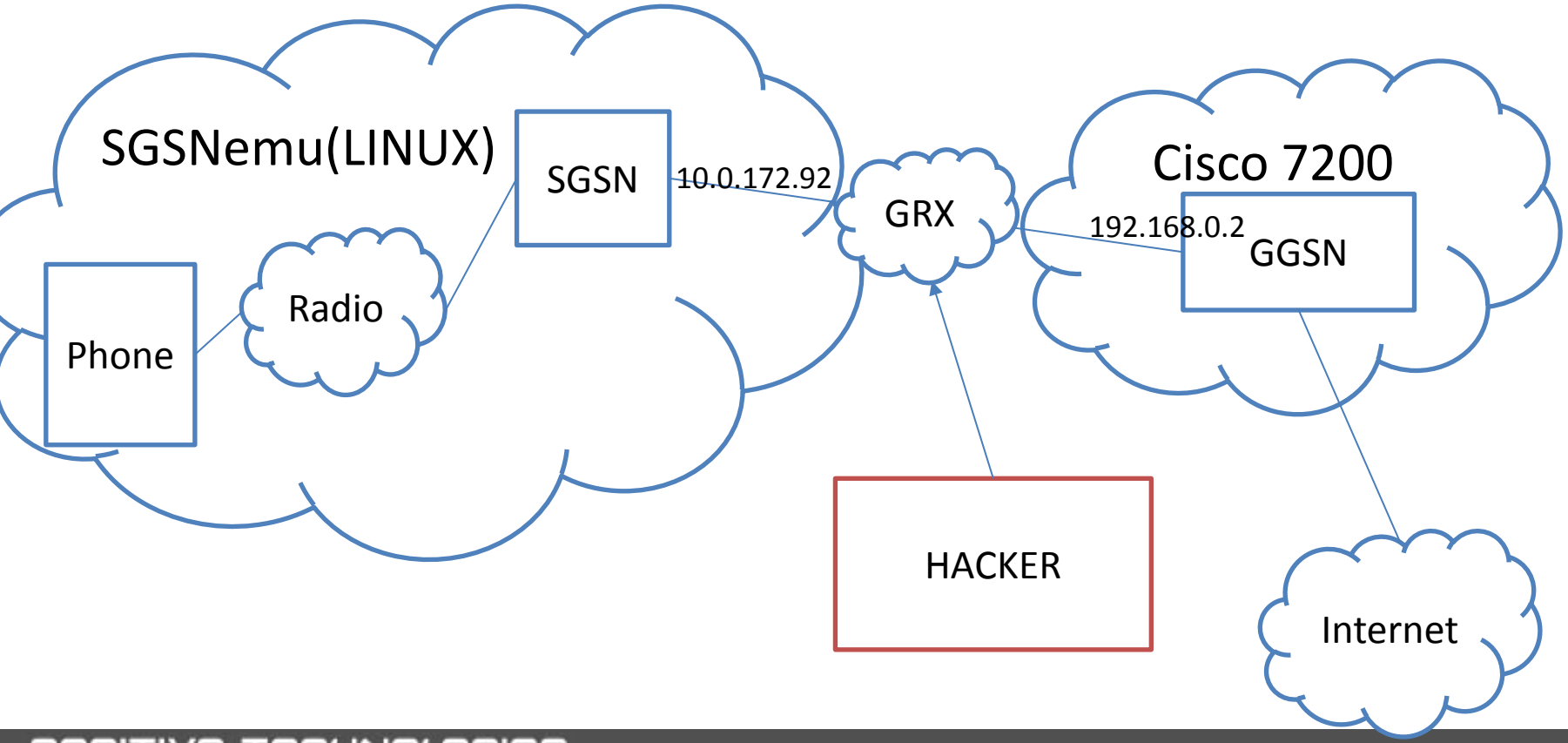
```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00

          inet addr:10.0.0.159  P-t-P:10.0.0.159  Mask:255.255.255.255
          UP POINTOPOINT RUNNING  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
                                                    (2.1 KiB)
```



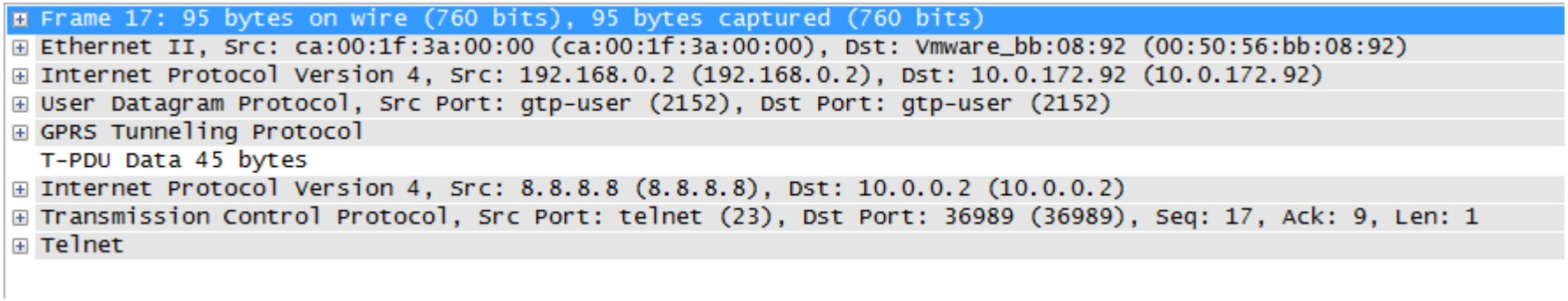
Dumps

3	0.015816	10.0.172.92	192.168.0.2	56 GTP	Echo request
4	0.015940	10.0.172.92	192.168.0.2	155 GTP	Create PDP context request
5	0.019215	192.168.0.2	10.0.172.92	62 GTP	Echo response
6	0.021507	192.168.0.2	10.0.172.92	62 GTP	Create PDP context response
7	261.517217	vmware_bb:08:92		44 ARP	who has 192.168.0.2? Tell 10.0.172.92
8	261.536747	ca:00:1f:3a:00:00		62 ARP	192.168.0.2 is at ca:00:1f:3a:00:00
9	261.536759	10.0.172.92	192.168.0.2	56 GTP	Echo request
10	261.536868	10.0.172.92	192.168.0.2	155 GTP	Create PDP context request
11	261.544207	192.168.0.2	10.0.172.92	62 GTP	Echo response
12	261.560458	192.168.0.2	10.0.172.92	62 GTP	Create PDP context response



GTP (безопасность)

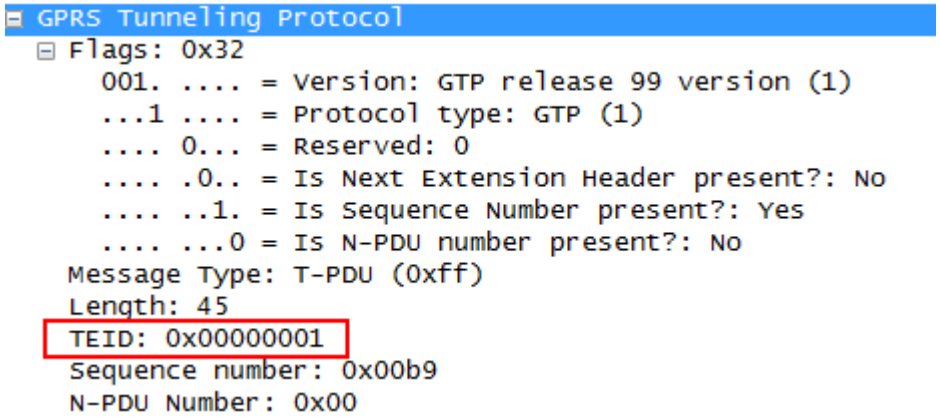
— Протокол туннелирования



3GPP TS 29.060

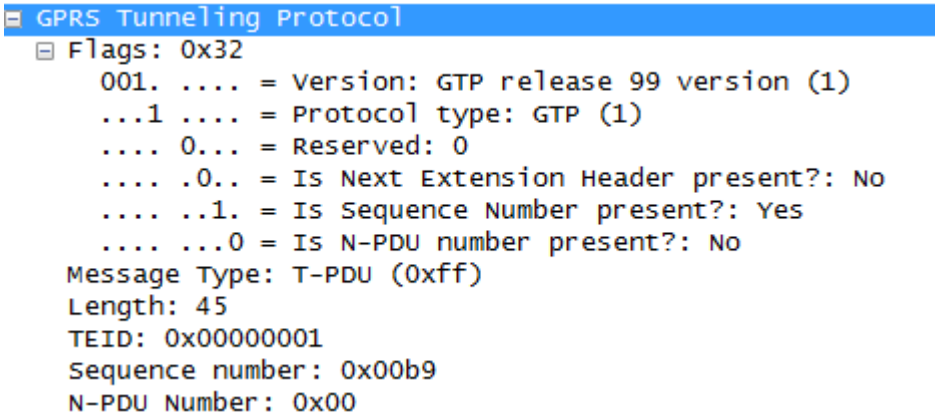
GTP (безопасность)

— Туннели отделяет только id



GTP (безопасность)

— Отсутствует аутентификация/шифрование



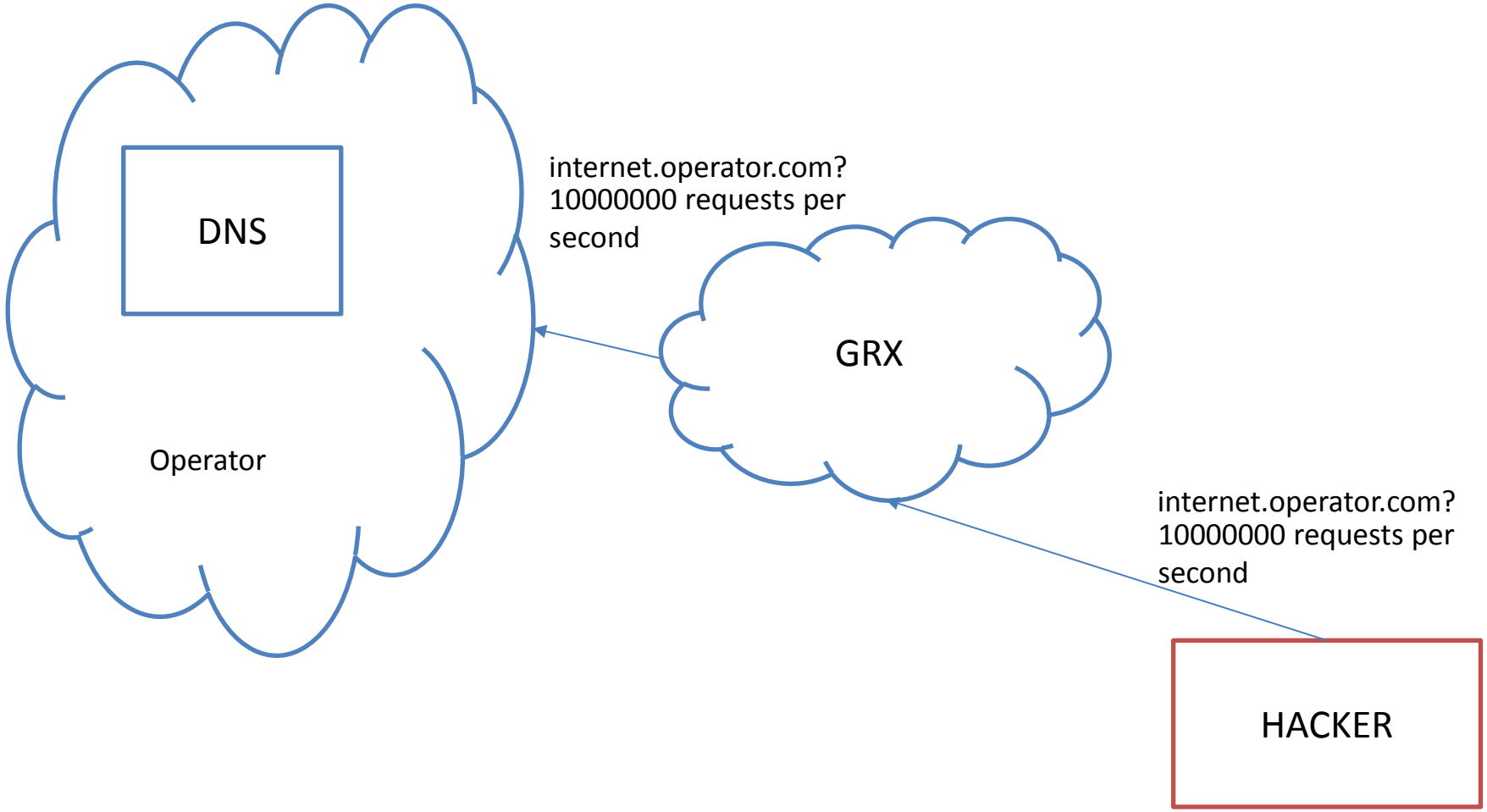
3GPP TS 29.060

GTP (безопасность)

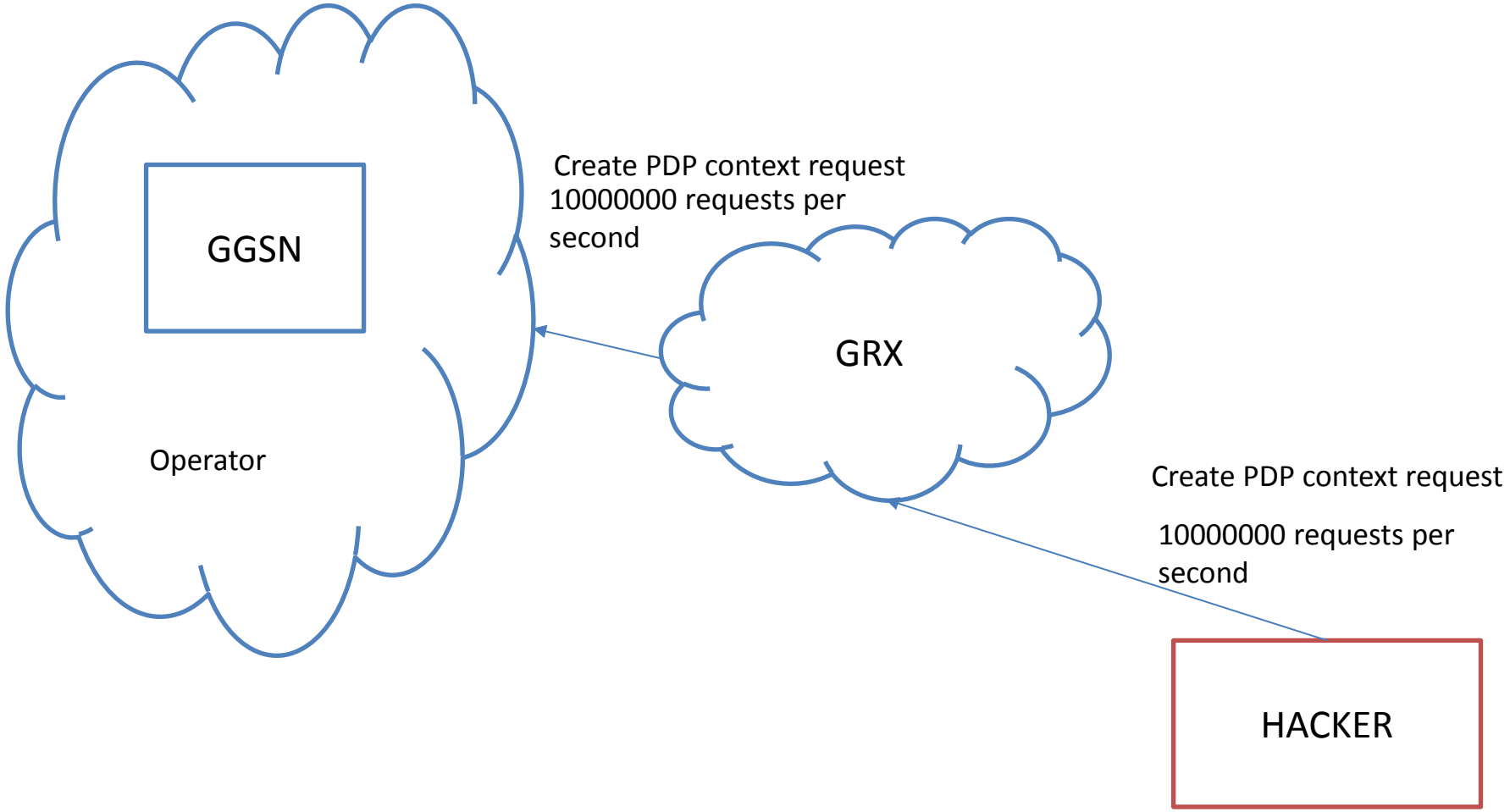
- Может использоваться для передачи биллинговой информации (GTP’)

+	Bits 0-2	3	4	5	6	7	8-15	16-31	32-47
0	Version	PT [0]	Reserved			Hdr len	Type	Length	Sequence Number

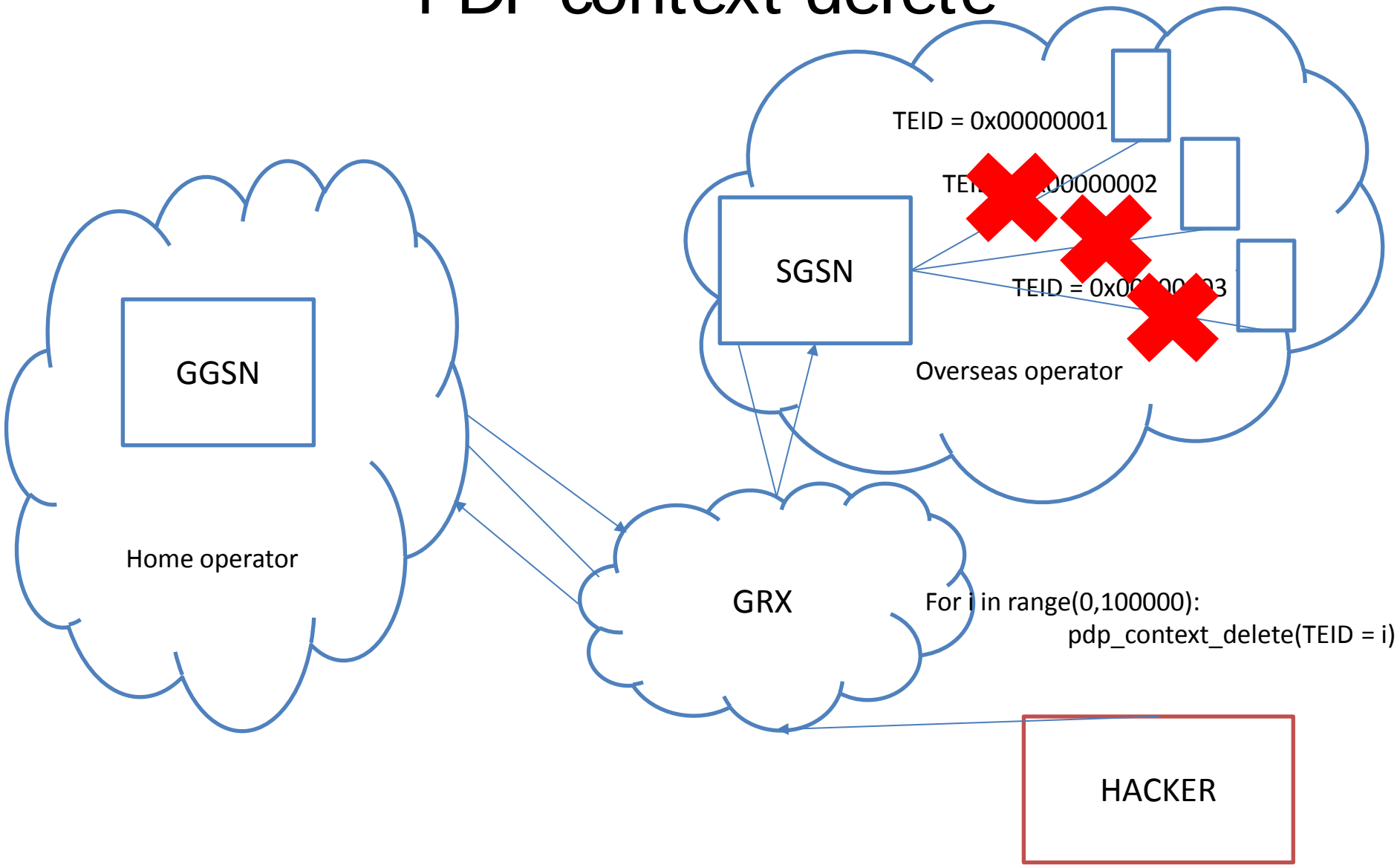
DNS Flood Attack



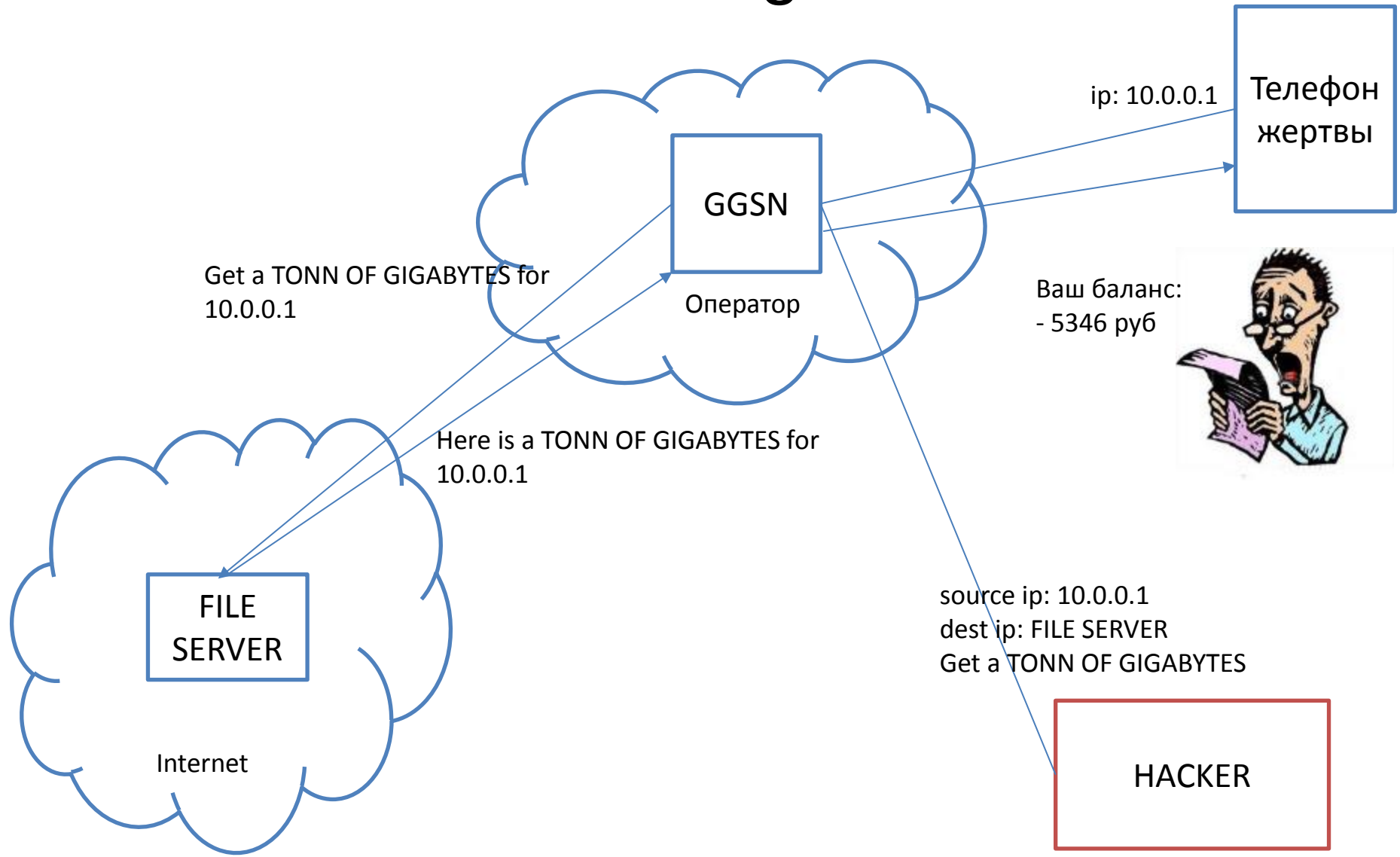
GTP Flood attack



PDP context delete



Overbilling attack



Что имеем

58.243.253.14
Anhui NOC 3G NET IPPOOL
Added on 26.05.2013
Hefei
Details

ZXR10 xGW-16, ZTE ZXR10 Software Version: ZXUN xGW(GGSN)V4.10.10.P7(1.0.0)

58.243.253.42
Anhui NOC 3G NET IPPOOL
Added on 25.05.2013
Hefei
Details

ZXR10 xGW-16, ZTE ZXR10 Software Version: ZXUN xGW(GGSN)V4.10.10.P7(1.0.0)

190.102.206.118
Colombia M@vil
Added on 24.05.2013
Bogotá
Details

Versatile Routing Platform Software
GGSN9811 (R) software, Version 5.50 (NE40E&80E V300R003C02B608)
Copyright (C) 2008-2010 HUAWEI Technologies Co., Ltd.
Quidway NetEngine 40E

58.243.253.10
Anhui NOC 3G NET IPPOOL
Added on 24.05.2013
Hefei
Details

ZXR10 xGW-16, ZTE ZXR10 Software Version: ZXUN xGW(GGSN)V4.10.10.P7(1.0.0)

Что имеем

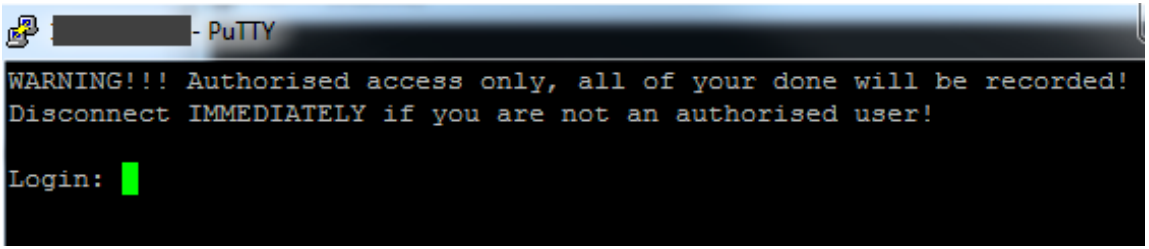
```
[redacted]# sgsnemu -l [redacted] -r [redacted] --createif

Using default DNS server
Local IP address is:    [redacted]
Remote IP address is:   [redacted]
IMSI is:                240010123456789 (0xf987654321010042)
Using NSAPI:            0
Using GTP version:      1
Using APN:              internet
Using selection mode:   1
Using MSISDN:           46702123456

Initialising GTP library
openggsn[4153]: GTP: gtp_newgsn() started
openggsn[4153]: gtp.c: 693: State information file (./gsn_restart) not found. Creating new file.
Setting up interface
Done initialising GTP library

Sending off echo request
Setting up PDP context #0
Waiting for response from ggsn........

Echo Request timed out
Retrying with version 0
Create PDP Context Request timed out
Retrying with version 0
Received echo response
Create PDP Context Request timed out
```



Что дальше?

— Исследование реальных сетей операторов

— Анализ видимых в Интернет gtp хостов

— Изучение LTE 

Конец рассказа
Спасибо за внимание

Сафронов Илья

isafronov@ ptsecurity.com