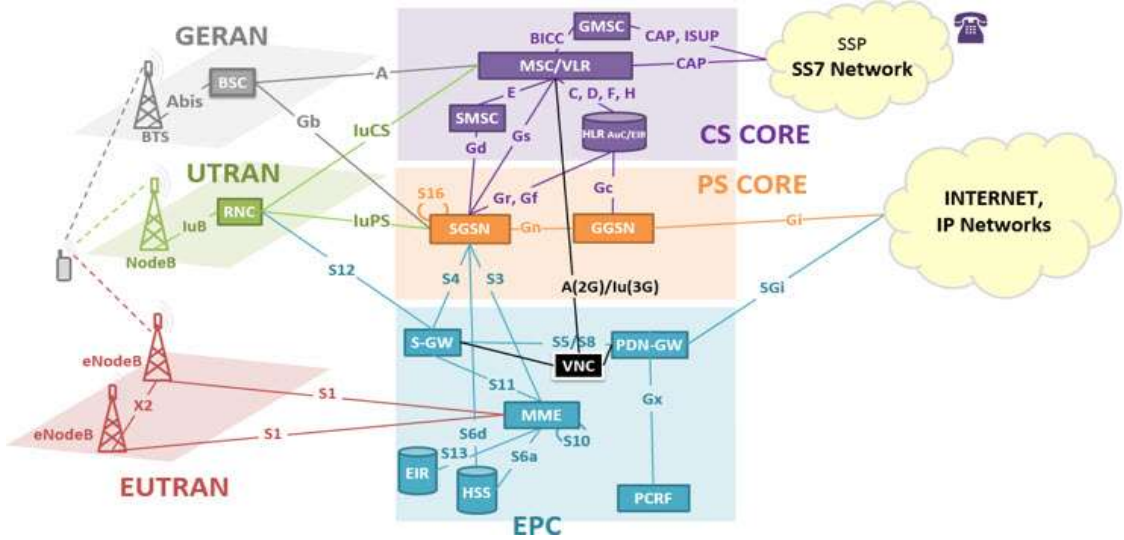




Komunikácia v mobilných sieťach 1

Vytvorenie 5G Core (5GC)

KIS FRI UNIZA



Vytvorené v rámci projektu KEGA 026TUKE-04/2021

Agenda

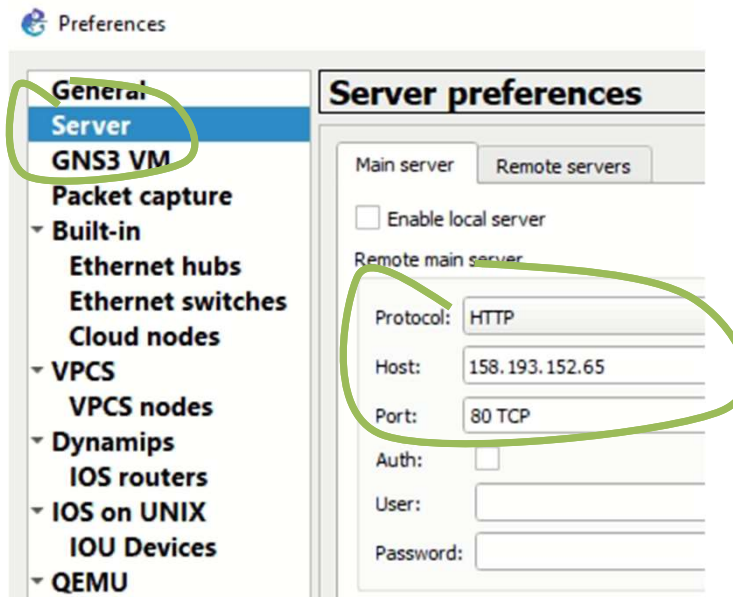
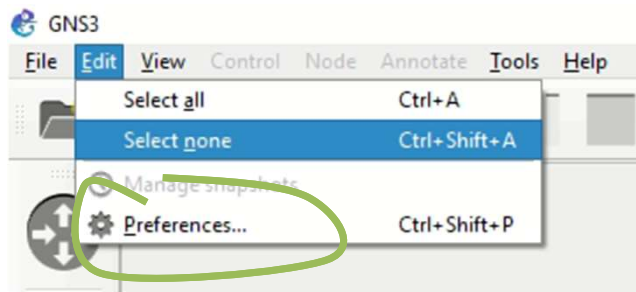
- Vytvorenie projektu s virtualizovanou 5G topológiou a kontrola nastavenia
- Konfigurácia uzlov virtuálnej mobilnej siete
- Aktivácia jednotlivých funkčných prvkov
- Konfigurácia UPF inštancie na zabezpečenie internetovej konektivity
- Úlohy



Vytvorenie projektu s virtualizovanou topológiou a kontrola nastavenia

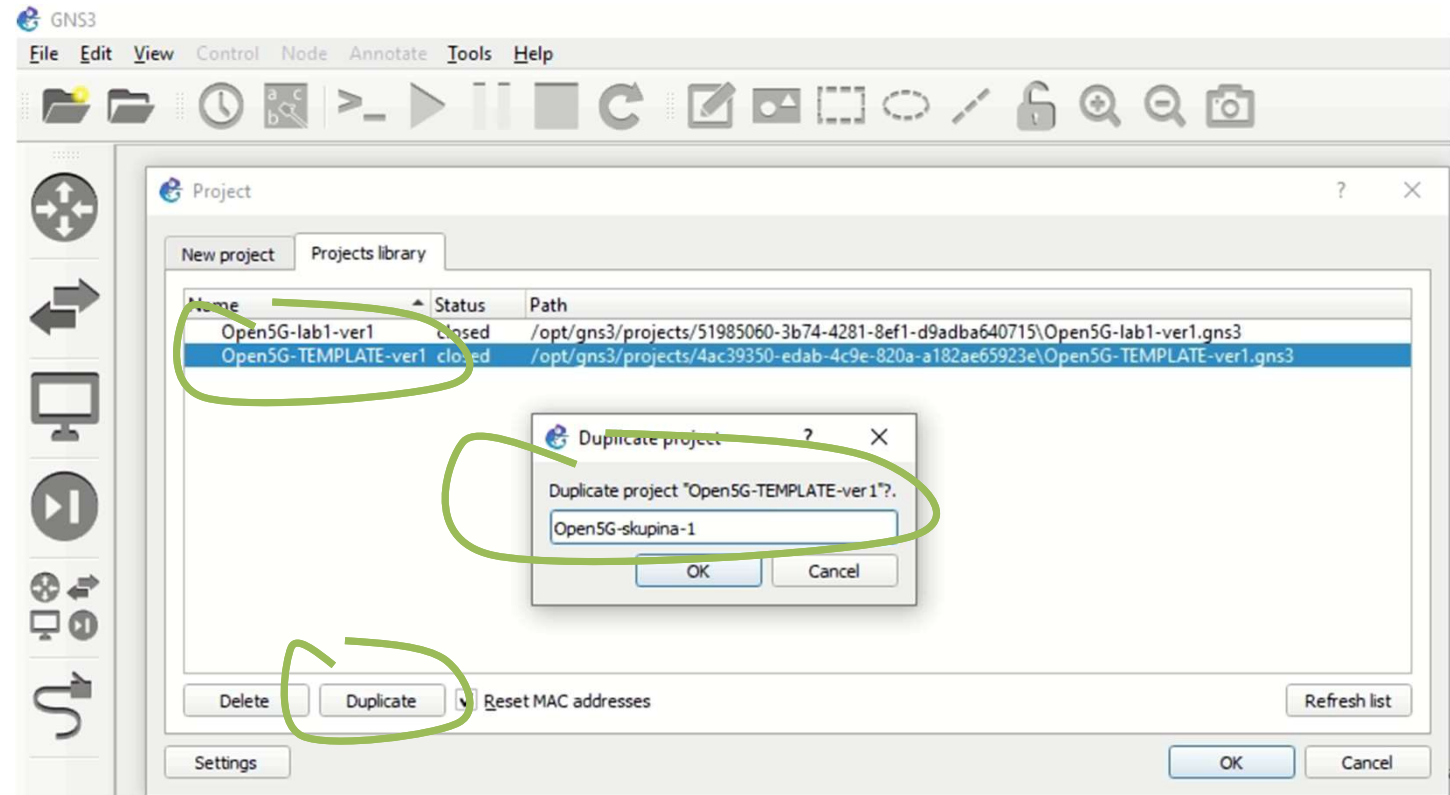
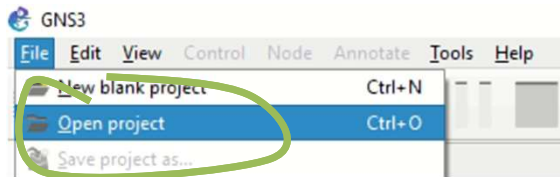
GNS3 - Graphical Network Simulator-3

- SW simulátor sietí, vytvorený v roku 2008. Umožňuje kombinovať virtuálne sieťové prvky s reálnym SW sieťovým operačným systémom od rôznych výrobcov a rôznych typov. Rovnako aj poskytuje prostredie pre koncové zariadenia (s OS Windows, Linux a iné)
- Funguje v klient – server móde. SW klient sa pripája na lokálny alebo vzdialený server. Klient poskytuje grafické prostredie ku existujúcim projektom na serveri.
- Skontrolovať nastavenie:



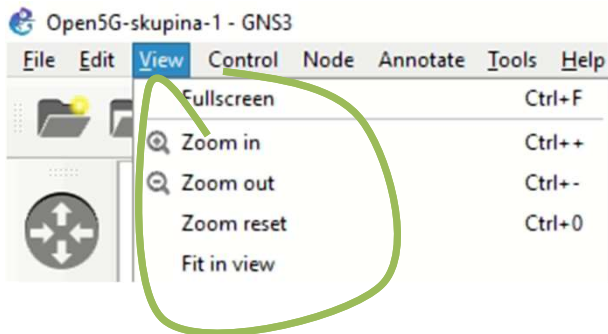
GNS3 – Nový projekt

- Vytvorenie si vlastného projektu, použite číslovanie vašej skupiny

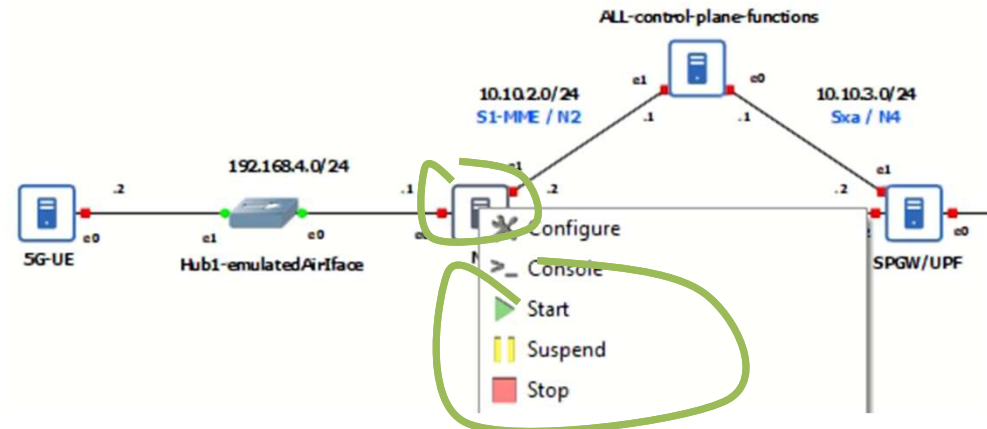
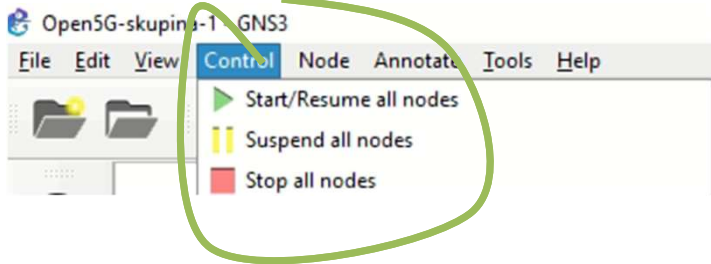


GNS3 – Zobrazenie a spustenie predkonfigurovaných uzlov v projekte

- Možnosť si prispôbiť grafické zobrazenie topológie

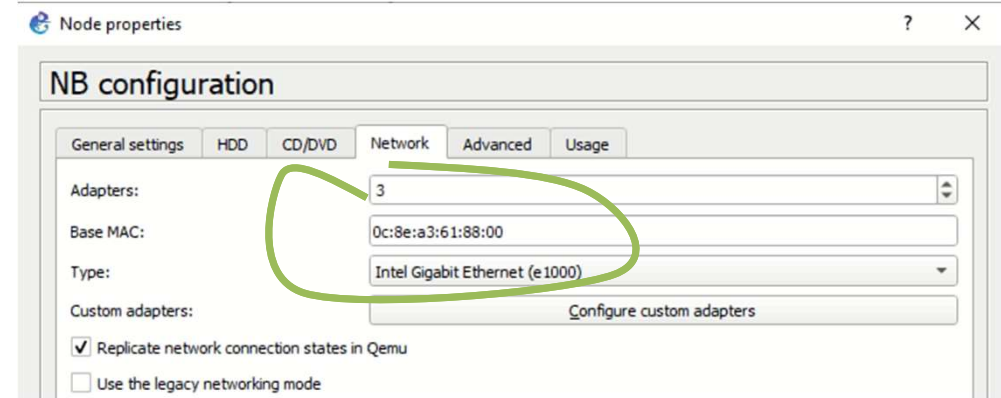
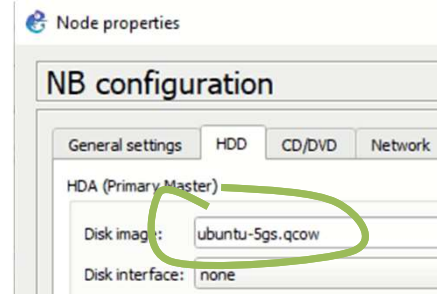
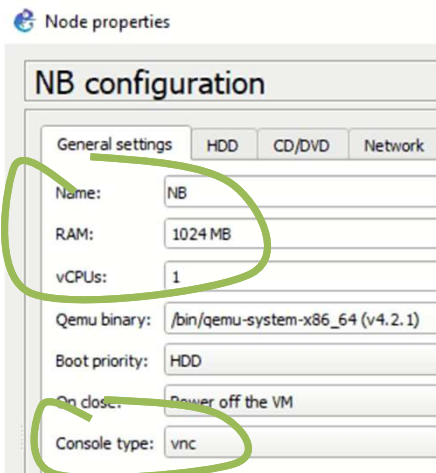
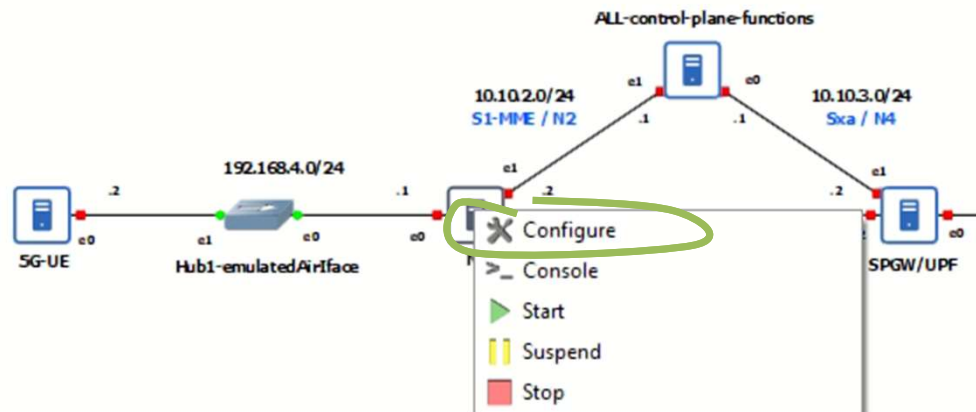


- Spustenie alebo zastavenie všetkých prvkov v topológii (jeden uzol je možné spustiť cez right-click)



GNS3 – Kontrola nastavenia virtuálnych inštancií

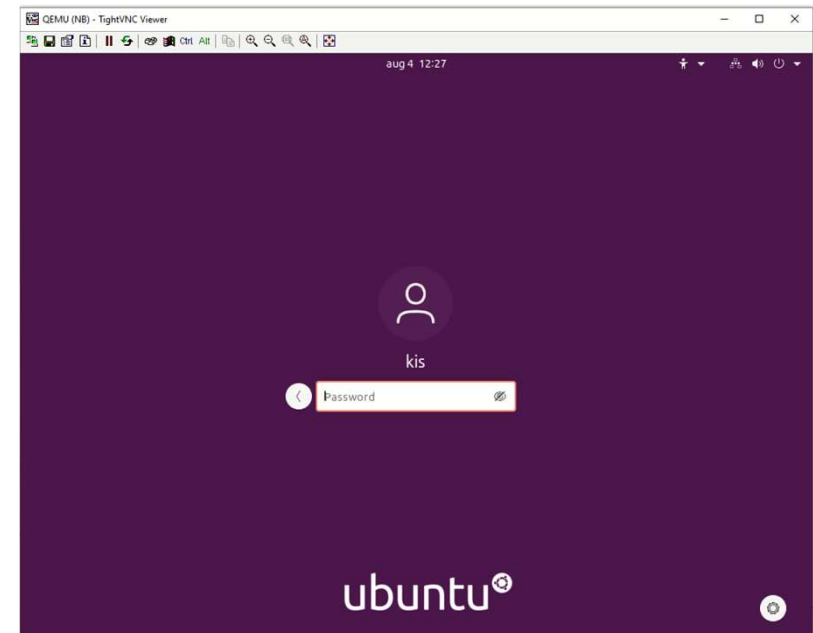
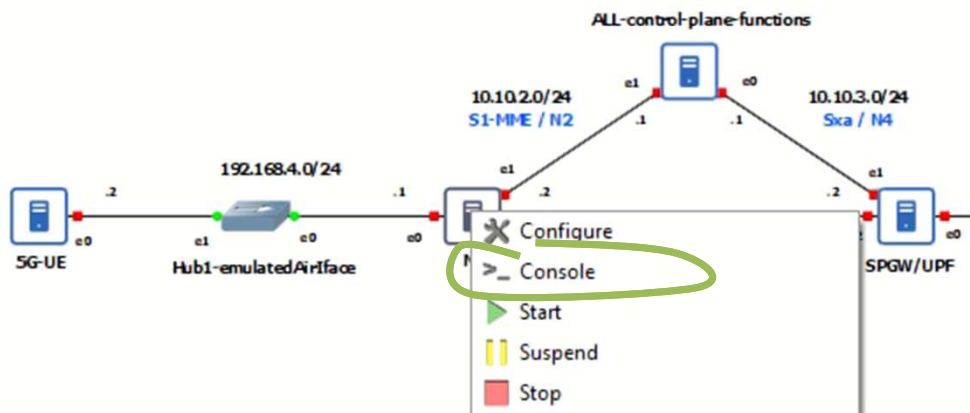
- Počet vCPU, pridelenej RAM, typ komunikácie s inštanciou (grafické rozhranie VNC), OS (Linux Ubuntu (R20 LTS 64bit) a sieťových rozhraní



Spustenie virtuálnych inštancií

- Spustenie, vid' predchádzajúce snímky
- Kontrola spustených inštancií
- Prihlásenie sa na konkrétnu inštanciu
 - Vytvorí sa nové okno s grafickým rozhraním
 - Login/Pass kis/kis123

Node	Console
5G-UE	vnc 158.193.152.65:5907
ALL-control-plane-functions	vnc 158.193.152.65:5905
Hub1-emulatedAirface	none
Internet	none
NB	vnc 158.193.152.65:5906
SPGW/UPF	vnc 158.193.152.65:5904

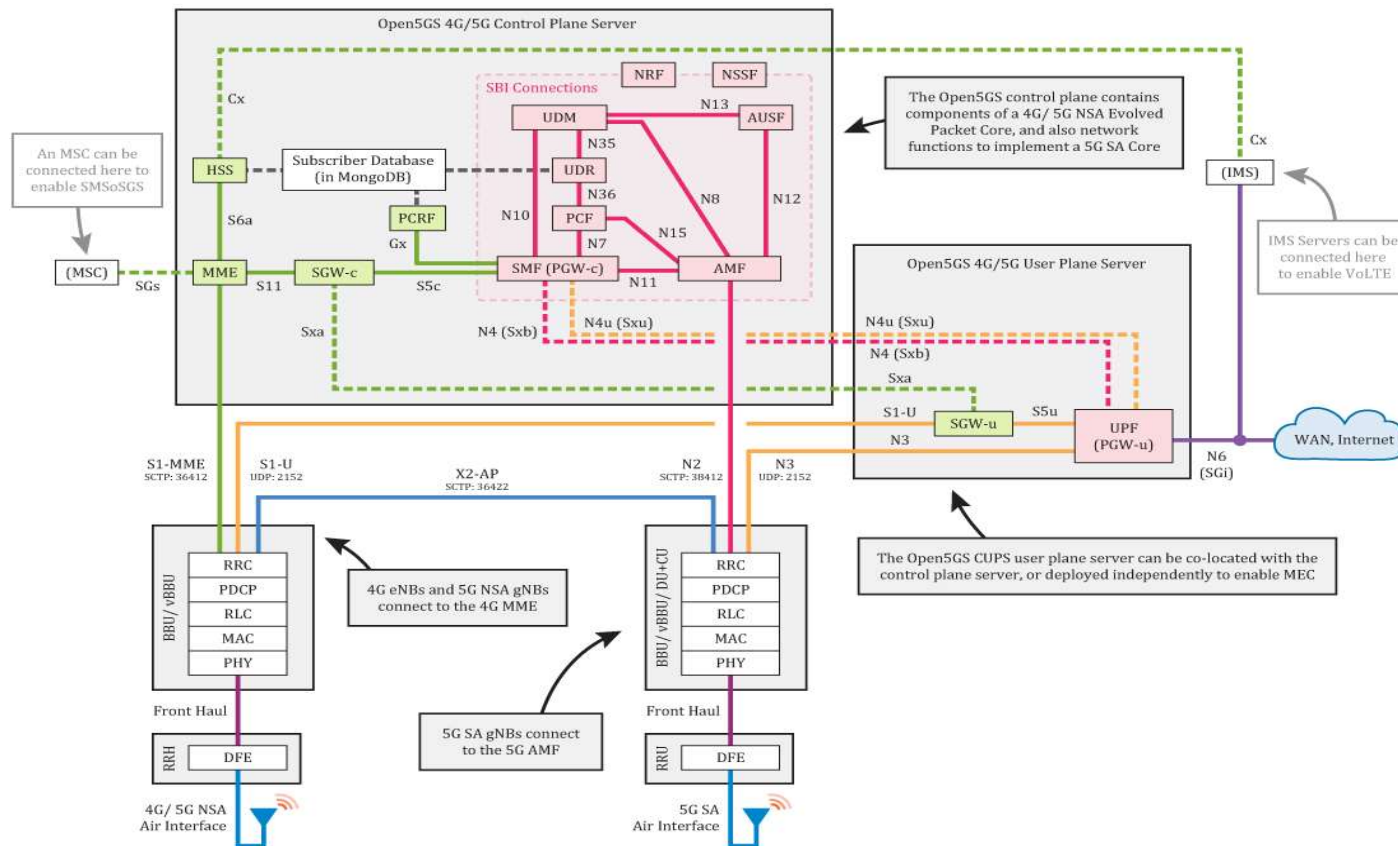




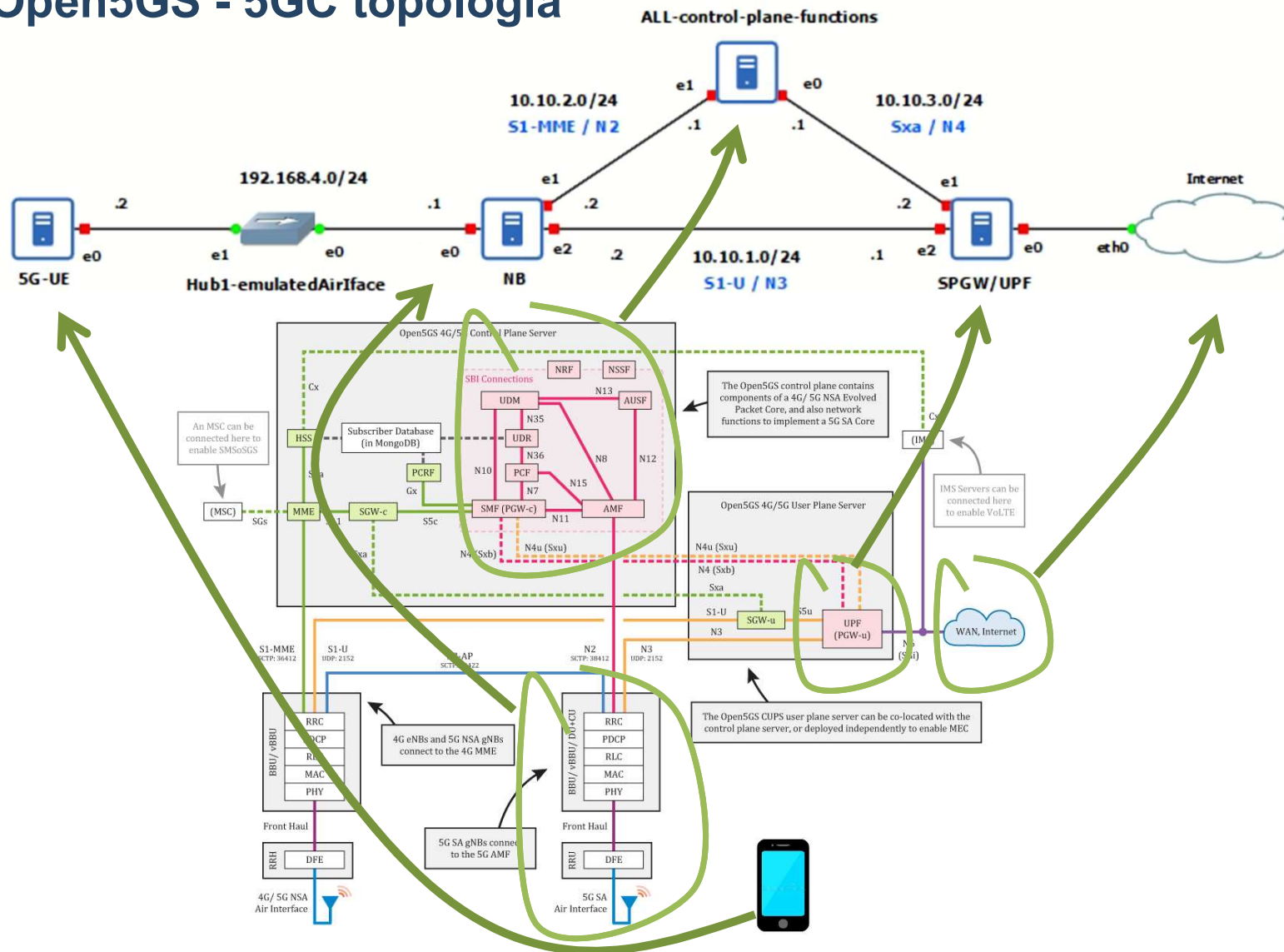
Konfigurácia uzlov virtuálnej mobilnej siete

Open source projekt Open5GS

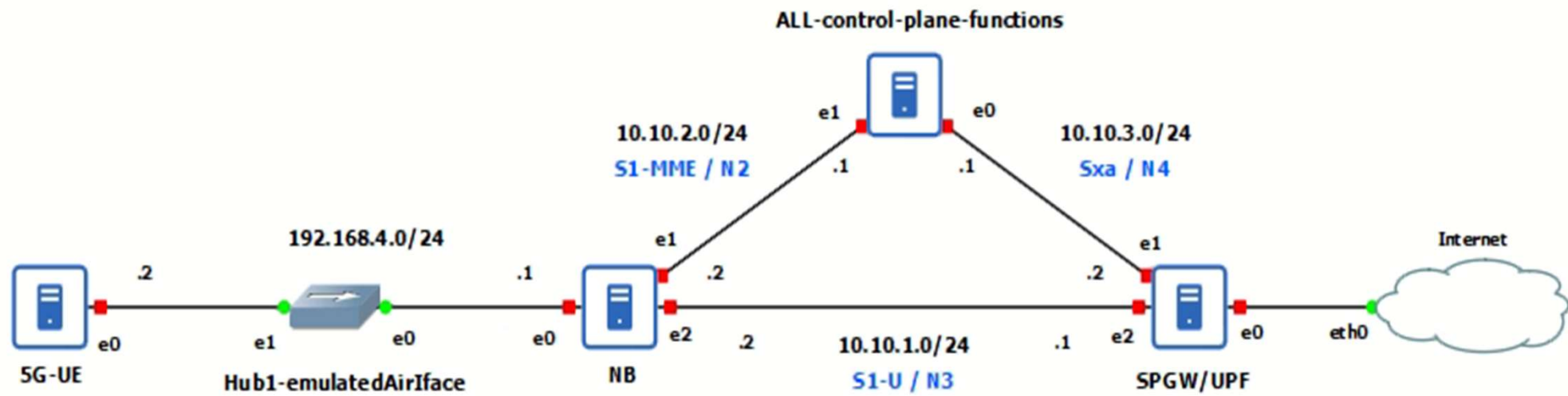
- Tento projekt umožňuje si vybudovať vlastnú virtualizovanú NR/LTE infraštruktúru <https://open5gs.org/>
- Implementované v jazyku C
- Jednotlivé uzly v GNS3 projekte už majú predinštalovaný Open5GS software a knižnice.



GNS3 - Open5GS - 5GC topológia



Topológia a adresácia



UE inštancia - konfigurácia

Nastaviť IP adresu na rozhranie ens3

použiť grafické rozhranie

192.168.4.2 netmask 255.255.255.0 gw 192.168.4.1

Overenie nastavenia rozhrania cez CLI

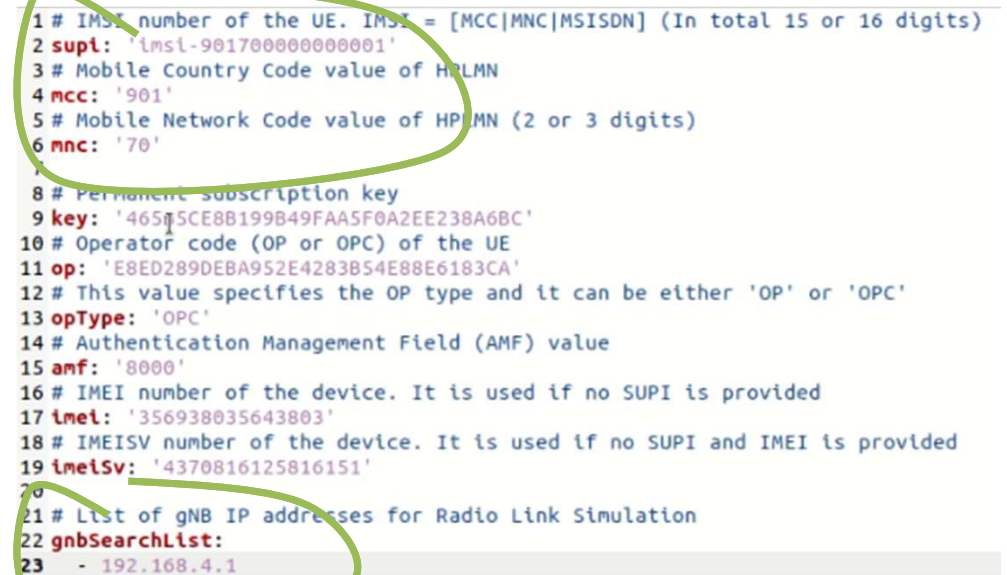
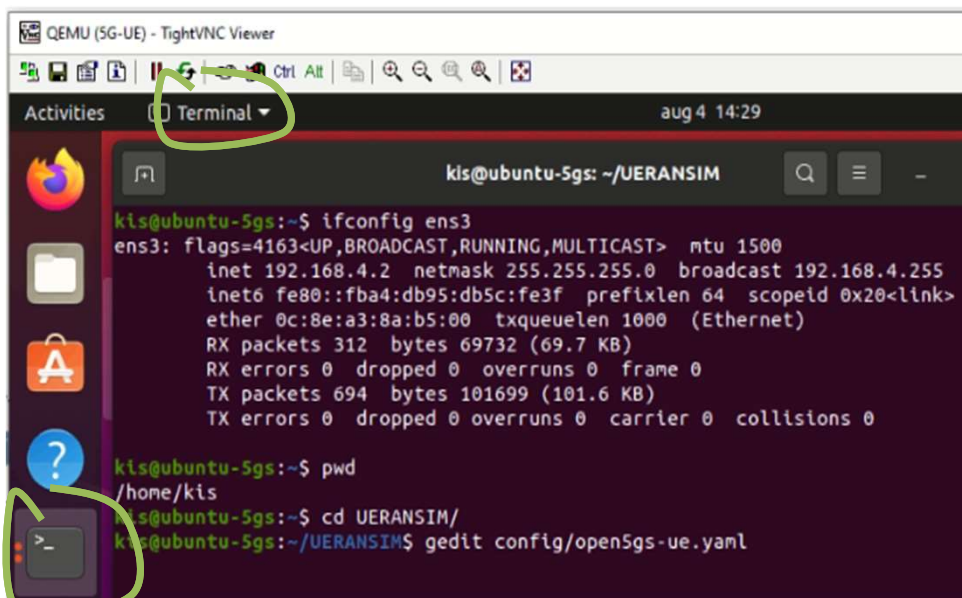
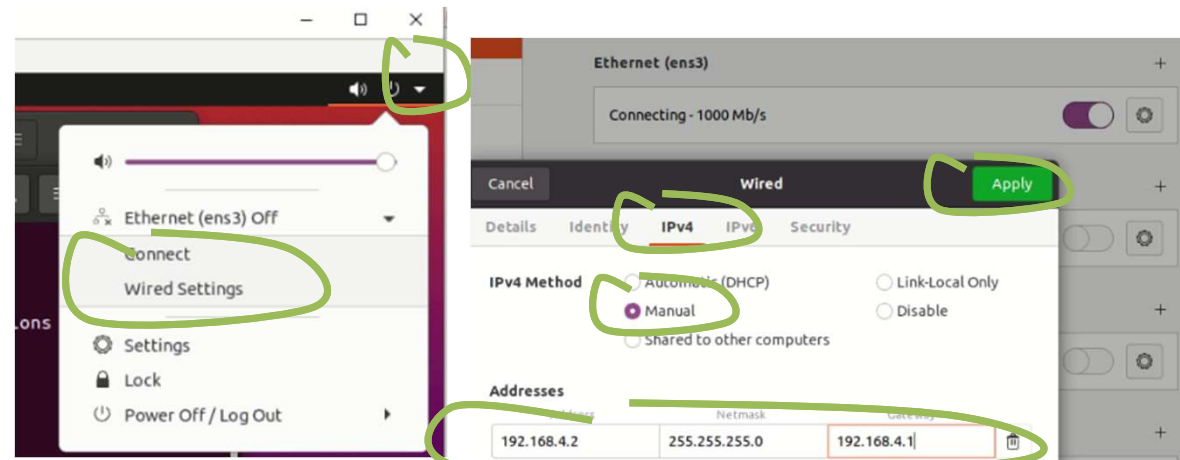
ifconfig ens3

cd ~/UERANSIM

gedit config/open5gs-ue.yaml # config file for UE

gnbSearchList: # IP of gNB

- 192.168.4.1



gNB inštancia - konfigurácia

Nastaviť IP adresu na rozhranie ens3, ens4 a ens5
použiť grafické rozhranie

ens3: 192.168.4.1 netmask 255.255.255.0 #smer UE

ens4: 10.10.2.2 netmask 255.255.255.0 #smer all CTRL plane functions

ens5: 10.10.1.2 netmask 255.255.255.0 #smer UPF

Overenie nastavenia rozhraní cez CLI a konektivity na UE

ifconfig

ping 192.168.4.2

cd ~/UERANSIM

gedit config/open5gs-gnb.yaml # config file for gNB

linkIp: 192.168.4.1 # local IP to UE over air

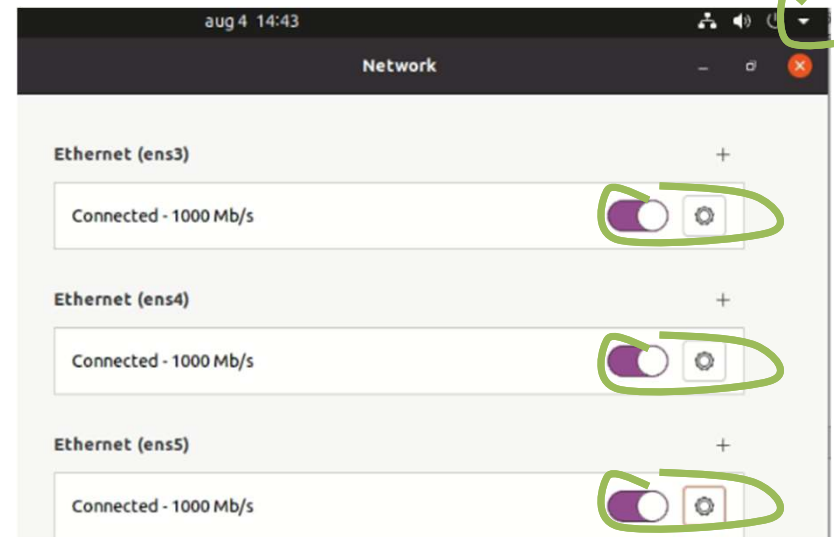
ngapIp: 10.10.2.2 # local IP to all ctrl functions

gtpIp: 10.10.1.2 # local IP to UPF

amfConfigs:

- address: 10.10.2.1 # IP of AMF

```
kis@ubuntu-5gs:~$ ping 192.168.4.2
PING 192.168.4.2 (192.168.4.2) 56(84) bytes of data:
64 bytes from 192.168.4.2: icmp_seq=1 ttl=64 time=0.777 ms
64 bytes from 192.168.4.2: icmp_seq=2 ttl=64 time=0.791 ms
^C
--- 192.168.4.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1023ms
rtt min/avg/max/mdev = 0.777/0.784/0.791/0.007 ms
kis@ubuntu-5gs:~$
```



```
1 mcc: '901' # Mobile Country Code value
2 mnc: '70' # Mobile Network Code value (2 or 3 digits)
3
4 nci: '0x000000010' # NR Cell Identity (36-bit)
5 idLength: 32 # NR gNB ID length in bits [22...32]
6 tac: 1 # Tracking Area Code
7
8 linkIp: 192.168.4.1 # gNB's local IP address for Radio Link
9 ngapIp: 10.10.2.2 # gNB's local IP address for N2 Interface
10 gtpIp: 10.10.1.2 # gNB's local IP address for N3 Interface
11
12 # List of AMF address information
13 amfConfigs:
14 - address: 10.10.2.1
15 port: 38412
```

All control plane functions – AMF, SMF, PCF, UDR, UDM, AUSF, NRF, NSSF inštancia – konfiguracia

Nastaviť IP adresu na rozhranie ens3, ens4

použiť grafické rozhranie

ens3: 10.10.3.1 netmask 255.255.255.0 #smer UPF

ens4: 10.10.2.1 netmask 255.255.255.0 #smer gNB

Overenie nastavenia rozhraní cez CLI a konektivity na gNB

ifconfig ens3

ifconfig ens4

ping 10.10.2.2

Meniť len tie rozhrania, ktoré sú mimo virtuálnu inštanciu:

sudo gedit /etc/open5gs/smf.yaml # config file for SMF

```
smf:  
  pfcf:  
    10.10.3.1
```

```
upf:  
  pfcf:  
    10.10.3.2
```

sudo gedit /etc/open5gs/amf.yaml # config file for AMF

```
amf:  
  ngap:  
    10.10.2.1
```

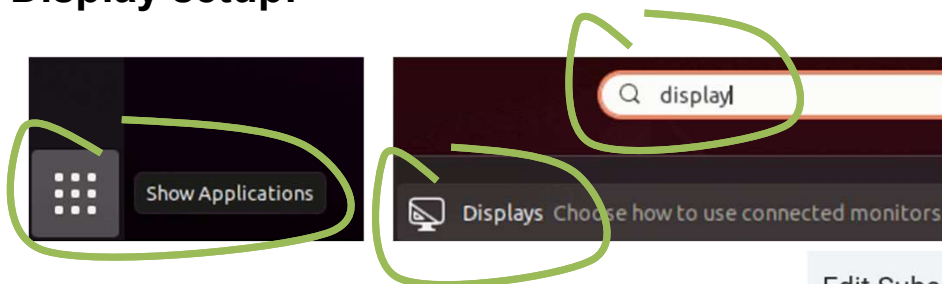
```
319 smf:  
320   sbi:  
321     - addr: 127.0.0.4  
322       port: 7777  
323   pfcf:  
324     - addr: 10.10.3.1
```

```
428 upf:  
429   pfcf:  
430     - addr: 10.10.3.2
```

```
178 amf:  
179   sbi:  
180     - addr: 127.0.0.5  
181       port: 7777  
182   ngap:  
183     - addr: 10.10.2.1
```

All control plane functions - vytvorenie 5G používateľa v UDR (MongoDB databáza)

Display setup:



Web UI pre UDR:

<http://localhost:3000>

Login/Pass: admin/1423

Novy subscriber:

Nakopírovať hodnoty

IMSI

K key

OP key (alebo OPc)

Poznámka:

Info z `UERANSIM/config/open5gs-ue.yaml`

UE inštancia; SIM informácie

Edit Subscriber

Subscriber Configuration

IMSI*

901700000000001

Subscriber Key (K)*

465B5CE8B199B49FAA5F0A2EE238A6BC

Authentication Management Field (AMF)*

8000

USIM Type

OP

Operator Key (OPc/OP)*

E8ED289DEBA952E4283B54E88E6183CA

UE-AMBR Downlink*

1

Unit

Gbps

UE-AMBR Uplink*

1

Unit

Gbps

Slice Configurations

SST*

1 2 3 4

SD

Default S-NSSAI

CANCEL

SAVE

UPF inštancia - konfigurácia

Nastaviť IP adresu na rozhranie ens3, ens4

použiť grafické rozhranie

```
ens3: DHCP (default)           #smer Internet
ens4: 10.10.3.2 netmask 255.255.255.0 #smer ctrl_plane
ens5: 10.10.1.1 netmask 255.255.255.0 #smer gNB
```

Overenie nastavenia rozhraní cez CLI a konektivity na gNB a ctrl plane

ifconfig ens4

ifconfig ens5

ping 8.8.8.8

ping 10.10.3.1

ping 10.10.1.2

Meniť len tie rozhrania, ktoré sú mimo virtuálnu inštanciu:

sudo gedit /etc/open5gs/upf.yaml # config file for UPF

```
upf:
  pfcps:
    - addr: 10.10.3.2
  gtpu:
    pfcps:
      - addr: 10.10.1.1
```

```
139 upf:
140   pfcps:
141     - addr: 10.10.3.2
142   gtpu:
143     - addr: 10.10.1.1
144   subnet:
145     - addr: 10.45.0.1/16
146     - addr: 2001:230:cafe::1/48
```



Aktivácia jednotlivých funkčných prvkov

UPF inštancia

sudo -s

```
systemctl list-units --no-legend | grep open5gs | awk '{print$1}' | xargs -l % sh -c 'echo "%: $(systemctl disable --now %)"'  
# zakázanie všetkých Open5GS procesov
```

```
systemctl restart --now open5gs-upfd # restart/spustenie relevantných procesov a načítanie konfiguračných súborov
```

```
ps -ef | grep open5gs* # overenie spustených procesov
```

exit

Poznámka: vhodné vytvoriť si súbor v domovskom adresári, kde sa uloží vyššie uvedený zoznam príkazov. Neskôr použiť copy&paste funkciu

All control plane functions

sudo -s

```
systemctl list-units --no-legend | grep open5gs | awk '{print$1}' | xargs -l % sh -c 'echo "%: $(systemctl disable --now %)"' # zakázanie všetkých Open5GS procesov
```

```
systemctl restart --now open5gs-smfd open5gs-amfd open5gs-udmd open5gs-udrd open5gs-ausfd open5gs-pcfd open5gs-nrfd open5gs-nssfd # restart/spustenie relevantných procesov a načítanie konfiguračných súborov
```

```
ps -ef | grep open5gs* # overenie spustených procesov
```

exit

Poznámka: vhodné vytvoriť si súbor v domovskom adresári, kde sa uloží vyššie uvedený zoznam príkazov. Neskôr použiť copy&paste funkciu.

gNB inštancia

cd UERANSIM/

sudo build/nr-gnb -c config/open5gs-gnb.yaml

```
kis@ubuntu-5gs: ~/UERANSIM
kis@ubuntu-5gs:~$ cd UERANSIM/
kis@ubuntu-5gs:~/UERANSIM$ sudo build/nr-gnb -c config/open5gs-gnb.yaml
[sudo] password for kis:
UERANSIM v3.1.5
[2021-08-06 13:56:39.021] [sctp] [info] Trying to establish SCTP connection (
10.10.2.1:38412)
[2021-08-06 13:56:39.026] [sctp] [info] Sctp connection established (10.10.2.1:3
8412)
[2021-08-06 13:56:39.028] [sctp] [debug] Sctp association setup ascId[239]
[2021-08-06 13:56:39.028] [ngap] [debug] Sending NG Setup Request
[2021-08-06 13:56:39.063] [ngap] [debug] NG Setup Response received
[2021-08-06 13:56:39.064] [ngap] [info] NG Setup procedure is successful
```

UE inštancia – registrácia UE zariadenia a vytvorenie priamej konektivity (GTP tunel) na UPF; pridelenie IP adresy pre koncové zariadenie

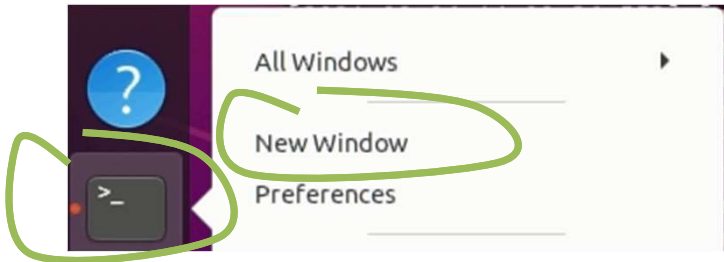
cd UERANSIM/

sudo build/nr-ue -c config/open5gs-ue.yaml

```
kis@ubuntu-5gs: ~ - UERANSIM
kis@ubuntu-5gs:~$ cd UERANSIM/
kis@ubuntu-5gs:~/UERANSIM$ sudo build/nr-ue -c config/open5gs-ue.yaml
[sudo] password for kis:
UERANSIM v3.1.5
[2021-08-06 14:00:36.549] [nas] [debug] NAS layer started
[2021-08-06 14:00:36.550] [rrc] [debug] RRC layer started
[2021-08-06 14:00:36.550] [nas] [info] UE switches to state [MM-DEREGISTERED/PLMN-SEARCH]
[2021-08-06 14:00:36.552] [nas] [info] UE connected to gNB
[2021-08-06 14:00:36.553] [nas] [info] UE switches to state [MM-DEREGISTERED/NORMAL-SERVICE]
[2021-08-06 14:00:36.553] [nas] [debug] Sending Initial Registration
[2021-08-06 14:00:36.554] [nas] [info] UE switches to state [MM-REGISTER-INITIATED/NA]
[2021-08-06 14:00:36.555] [rrc] [debug] Sending RRC Setup Request
[2021-08-06 14:00:36.558] [rrc] [info] RRC connection established
[2021-08-06 14:00:36.558] [nas] [info] UE switches to state [CM-CONNECTED]
[2021-08-06 14:00:36.709] [nas] [debug] Security Mode Command received
[2021-08-06 14:00:36.709] [nas] [debug] Derived NAS keys integrity[5443F857F23C49D37B23E9899F1E46FD]
ciphering[52B3E71EF3A412972B70779A71A0E91C]
[2021-08-06 14:00:36.709] [nas] [debug] Selected integrity[2] ciphering[0]
[2021-08-06 14:00:36.760] [nas] [debug] Registration accept received
[2021-08-06 14:00:36.760] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2021-08-06 14:00:36.760] [nas] [info] Initial Registration is successful
[2021-08-06 14:00:36.760] [nas] [info] Initial PDU sessions are establishing [1#]
[2021-08-06 14:00:36.760] [nas] [debug] Sending PDU session establishment request
[2021-08-06 14:00:37.206] [nas] [debug] PDU Session Establishment Accept received
[2021-08-06 14:00:37.253] [nas] [info] PDU Session establishment is successful PSI[1]
[2021-08-06 14:00:37.572] [app] [info] Connection setup for PDU session[1] is successful, TUN in
terface[uesimtun0, 10.45.0.2] is up.
```

UE inštancia – kontrola tunelového rozhrania a konektivity na UPF

1. Otvoriť nové terminálové okno (right-click)



2. Overenie nového tunelového rozhrania smerom na UPF inštanciu; CLI príkaz
ifconfig [uesimtun0] # optional iface argument

```
uesimtun0: flags=369<UP,POINTOPOINT,NOTRAILERS,RUNNING,PROMISC> mtu 1400  
inet 10.45.0.2 netmask 255.255.255.255 destination 10.45.0.2  
inet6 fe80::b03c:94ab:841d:2836 prefixlen 64 scopeid 0x20<link>  
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500
```

3. Overenie používateľovej konektivity na UPF inštanciu cez vytvorený tunel
ping 10.45.0.1 -I uesimtun0

```
kis@ubuntu-5gs:~$ ping 10.45.0.1 -I uesimtun0  
PING 10.45.0.1 (10.45.0.1) from 10.45.0.2 uesimtun0: 56(84) bytes of data.  
64 bytes from 10.45.0.1: icmp_seq=1 ttl=64 time=3.55 ms  
64 bytes from 10.45.0.1: icmp_seq=2 ttl=64 time=2.76 ms
```

UPF inštancia – kontrola tunelového rozhrania a konektivity na UPF

1. Overiť v logovacom súbore aktivitu ohľadne vytvorenia dátového spojenia s UE:
sudo tail /var/log/open5gs/upf.log

```
08/06 12:44:20.426: [upf] INFO: [Added] Number of UPF-Sessions is now 1 (../src/upf/context.c:157)
08/06 12:44:20.449: [gtp] INFO: gtp_connect() [127.0.0.4]:2152 (../lib/gtp/path.c:58)
08/06 12:44:20.449: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[internet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.c:334)
08/06 12:44:20.484: [gtp] INFO: gtp_connect() [10.10.1.2]:2152 (../lib/gtp/path.c:58)
```

2. Overenie nového tunelového rozhrania smerom na UPF inštanciu; CLI príkaz
ifconfig [ogstun] # optional iface argument

```
ogstun: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.45.0.1 netmask 255.255.0.0 destination 10.45.0.1
inet6 2001:230:cafe::1 prefixlen 48 scopeid 0x0<global>
inet6 fe80::5e3e:ae3b:d5ac:e79f prefixlen 64 scopeid 0x20<link>
```

3. Overenie konektivity na UP cez vytvorený tunel
ping 10.45.0.2 -I uesimtun0

```
kis@ubuntu-5gs:~$ ping 10.45.0.2 -I ogstun
PING 10.45.0.2 (10.45.0.2) from 10.45.0.1 ogstun: 56(84) bytes of data.
64 bytes from 10.45.0.2: icmp_seq=1 ttl=64 time=2.79 ms
64 bytes from 10.45.0.2: icmp_seq=2 ttl=64 time=2.11 ms
```




Konfigurácia UPF inštancie na zabezpečenie internetovej konektivity

UPF inštancia - Internet konektivita pre UE GTP tunely pre koncových zákazníkov

NAT konfigurácia smerom do Internetu:

```
sudo sysctl -w net.ipv4.ip_forward=1  
sudo iptables -t nat -A POSTROUTING -s 10.45.0.0/16 ! -o ogstun -j MASQUERADE
```

```
kis@ubuntu-5gs:~$ sudo sysctl -w net.ipv4.ip_forward=1  
net.ipv4.ip_forward = 1  
kis@ubuntu-5gs:~$ sudo iptables -t nat -A POSTROUTING -s 10.45.0.0/16 ! -o ogstun -j MASQUERADE
```

Notes:

Enable IP forwarding in Linux: net.ipv4.ip_forward=1

iptables - administration tool for IPv4 packet filtering and NAT.

- -t [table] This option specifies the packet matching table which the command should operate on
- POSTROUTING rule for packets which are about to go out
- ! -o [outgoing interface] name of an interface via which a packet is going to be sent; "!" argument before the interface name inverts the sense
- Masquerading is equivalent to specifying a mapping to the IP address of the interface the packet is going out

UE inštancia - Internet konektivita pre UE GTP tunely pre koncových zákazníkov

nastavenie default GW:

```
sudo route add default dev uesimtun0
```

```
netstat -rn
```

```
ping 8.8.8.8
```

```
kis@ubuntu-5gs:~$ sudo route add default dev uesimtun0
kis@ubuntu-5gs:~$ sudo netstat -rn
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
0.0.0.0          0.0.0.0         0.0.0.0         U        0 0          0 uesimtun0
0.0.0.0          192.168.4.1    0.0.0.0         UG        0 0          0 ens3
169.254.0.0     0.0.0.0         255.255.0.0     U        0 0          0 ens3
192.168.4.0     0.0.0.0         255.255.255.0   U        0 0          0 ens3
kis@ubuntu-5gs:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=12.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=11.8 ms
```

UE DNS resolving

Možnosť A)

Dočasné nastavenie po najbližší reštart VM inštancie

sudo gedit /etc/resolv.conf

```
14 # See man:systemd-resolved.service(8) for details about the supported modes of
15 # operation for /etc/resolv.conf.
16
17 nameserver 8.8.8.8|
18 nameserver 127.0.0.53
19 options edns0 trust-ad
```

```
kis@ubuntu-5gs:~$ ping www.six.sk
PING pmc.cvt.stuba.sk (147.175.1.70) 56(84) bytes of data.
64 bytes from pmc.cvt.stuba.sk (147.175.1.70): icmp_seq=1 ttl=58 time=
64 bytes from pmc.cvt.stuba.sk (147.175.1.70): icmp_seq=2 ttl=58 time=
64 bytes from pmc.cvt.stuba.sk (147.175.1.70): icmp_seq=3 ttl=58 time=
```

Možnosť B)

- Prostredníctvom GUI NetworkManager

The screenshot shows the NetworkManager GUI for a 'Wired' connection. The 'IPv4' tab is selected. Under 'IPv4 Method', the 'Manual' option is chosen. The 'Addresses' table shows one address: 192.168.4.2 with netmask 255.255.255.0 and gateway 192.168.4.1. The 'DNS' field is highlighted with a green circle and contains the value '8.8.8.8'. The 'Automatic' toggle is also visible.

Address	Netmask	Gateway	
192.168.4.2	255.255.255.0	192.168.4.1	

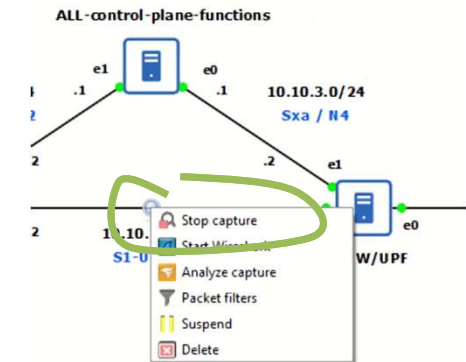
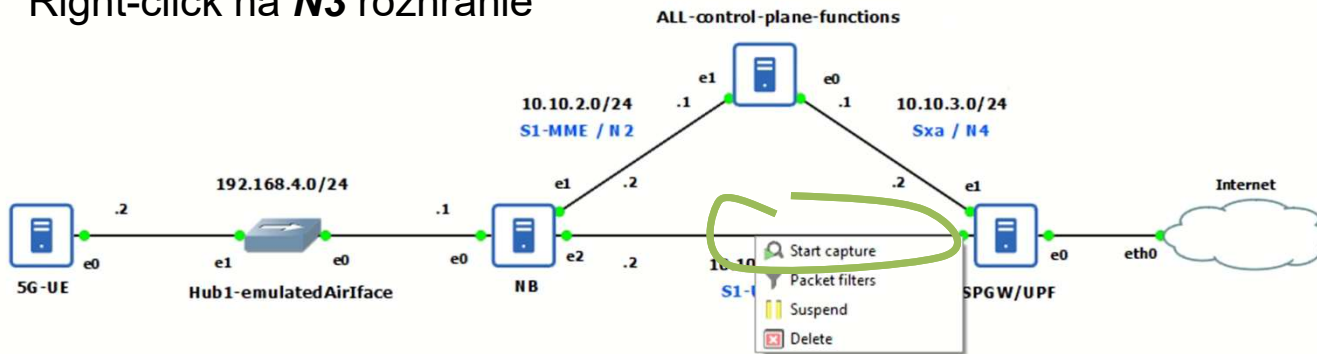
DNS Automatic

8.8.8.8

Separate IP addresses with commas

Záchyt dátových paketov prostredníctvom programu Wireshark na N3 rozhraní

- Right-click na **N3** rozhranie



Capturing from - [NB Ethernet2 to SPGW/UPF Ethernet2]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
11	73.280461	10.45.0.8	8.8.8.8	GTP <I..	142	Echo (ping) request id=0x0005, seq=1/256, ttl=64 (reply in 12)
12	73.290080	8.8.8.8	10.45.0.8	GTP <I..	142	Echo (ping) reply id=0x0005, seq=1/256, ttl=55 (request in 11)
13	74.282165	10.45.0.8	8.8.8.8	GTP <I..	142	Echo (ping) request id=0x0005, seq=2/512, ttl=64 (reply in 14)
14	74.292177	8.8.8.8	10.45.0.8	GTP <I..	142	Echo (ping) reply id=0x0005, seq=2/512, ttl=55 (request in 13)

> Frame 11: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface -, id 0

> Ethernet II, Src: 0c:8e:a3:61:88:02 (0c:8e:a3:61:88:02), Dst: 0c:8e:a3:73:7f:02 (0c:8e:a3:73:7f:02)

> Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.1

> User Datagram Protocol, Src Port: 2152, Dst Port: 2152

> GPRS Tunneling Protocol

> Flags: 0x34

> Message Type: T-PDU (0xff)

> Length: 92

> TEID: 0x0000001a (26)

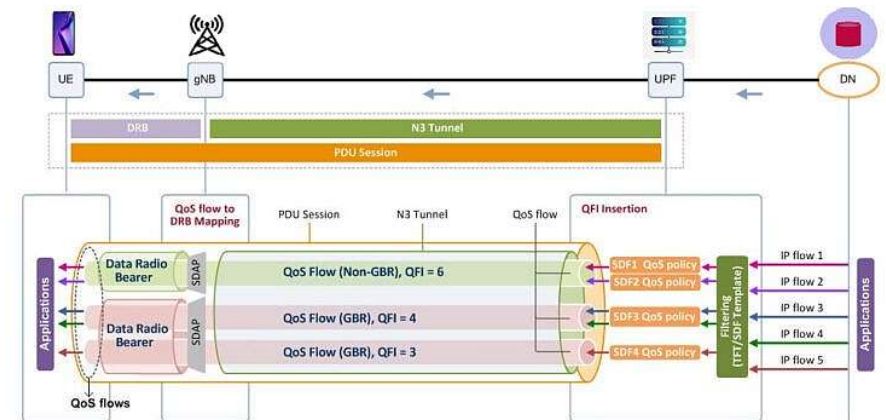
> Next extension header: PDU Session container (0x85)

> Extension header

> Internet Protocol Version 4, Src: 10.45.0.8, Dst: 8.8.8.8

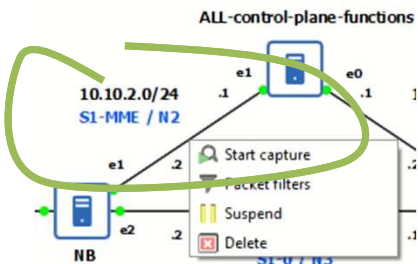
> Internet Control Message Protocol

```
kis@ubuntu-5gs:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=12.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=11.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=55 time=11.2 ms
```



Záchyt signalizácie na N2 rozhraní

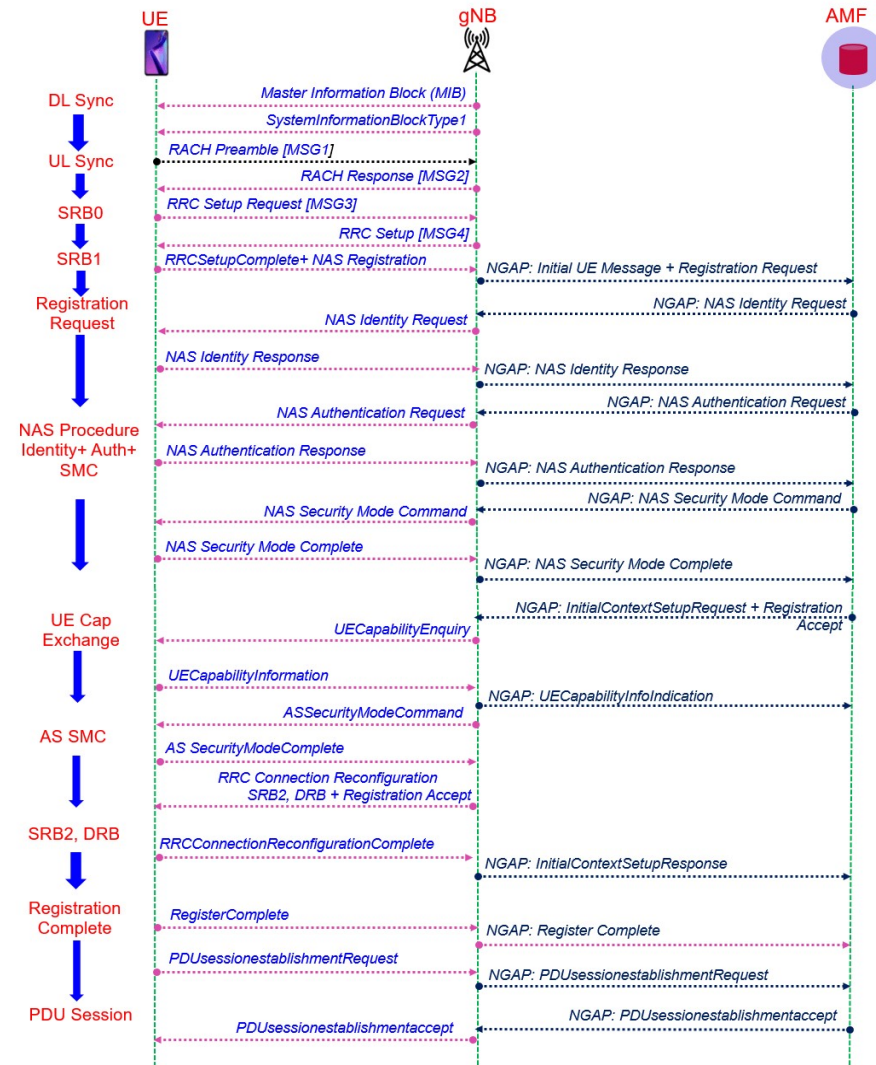
- Right-click na **N2** rozhranie
- The Non-Access Stratum (NAS) is a **set of protocols in LTE and 5G**. The NAS is used to convey non-radio signalling between the User Equipment (UE) and the MME or AMF
- NAS messages are transported using NGAP and SCTP protocols
- Some data in NAS message could be encrypted therefore Wireshark needs to be properly setup to decode it



Wireshark packet capture showing a Non-Access Stratum 5G (NAS) PDU. The packet is expanded to show the Security protected NAS 5GS message. The message is encrypted, and the 'Encrypted data' field is highlighted. A context menu is open over the encrypted data, with 'Protocol Preferences' selected. The 'Protocol Preferences' dialog is open, showing the 'Open Non-Access Stratum 5G (NAS) PDU preferences...' option, which is checked. The 'Try to detect and decode 5G-EA0 ciphered messages' option is also checked.

N2 signalizačné rozhranie – vytvorenie 5G UE PDU spojenia

- Registration request
 - The gNB sends the Initial UE Message to the selected AMF. The message carries the "Registration Request" message that was received from the UE in the RRC Setup Complete message.
- Authentication request, response and security mode and capabilities exchange
 - The AMF requests UE authentication vectors and algorithm information from the AUSF - Authentication Server Function. The response returns the master key which is used by AMF to derive NAS security keys. Initiate the authentication procedure with the UE. AMF sends the key selector, RAND and AUTN to the UE. The AMF signals the selected NAS security algorithm to the UE.
- Registration request and Registration accept
- Access and Mobility Subscription data exchange
- Setup the User Plane Function (UPF)
 - Initial Context setup Request and Response
 - PDU Session Resource Setup Request and Response
 - The AMF initiates a session setup with the gNB. The gNB signals the successful setup of PDU sessions. Messages include uplink and downlink TEID





Úlohy

Úloha č. 1

1. Prostredníctvom programu Wireshark odchytiť DNS request a response na doménu www.six.sk a príslušný ping na www.six.sk
 - a) Zachytiť ping komunikáciu na N3 rozhraní medzi gNB a UPF (screenshot a stručný popis)
 - b) Aká bola pridelená IPv4 adresa UE zariadeniu
 - c) Aký typ tunelového protokolu je použitý pre enkapsuláciu IP paketov koncového používateľa
 - d) Aká je hodnota uplink a downlink TEID identifikátoru tunelov (“adresy” GTP tunelu)

Úloha č. 2

Prostredníctvom programu Wireshark odchytiť signalizáciu na N2 rozhraní

1. Aktivovať Wireshark a spustiť registráciu UE v príslušnej virtuálnej inštancii
2. Zistiť a spraviť screenshot nasledujúcich parametrov:
 - a) Registration Request message
 - MCC a MNC a MSIN (IMSI)
 - čas registrácie a Tracking Area ID
 - b) Authentication response
 - Hodnota RES tokenu, ktorý bol vypočítaný UE zariadením a preposlaný na porovnanie do AMF
 - c) PDU Session Setup Request a Response
 - Pridelená IP adresa UE zariadeniu
 - Pridelená IP adresa gNB pre GTP tunel
 - Uplink a Downlink TEID



Ďakujem za pozornosť.



■ Vytvorené v rámci projektu KEGA 026TUKE-4/2021