I want my own cellular network!

Having fun with LTE networks and Open5Gs

FOSDEM'24

~$ whoami

Alessandro Arcieri

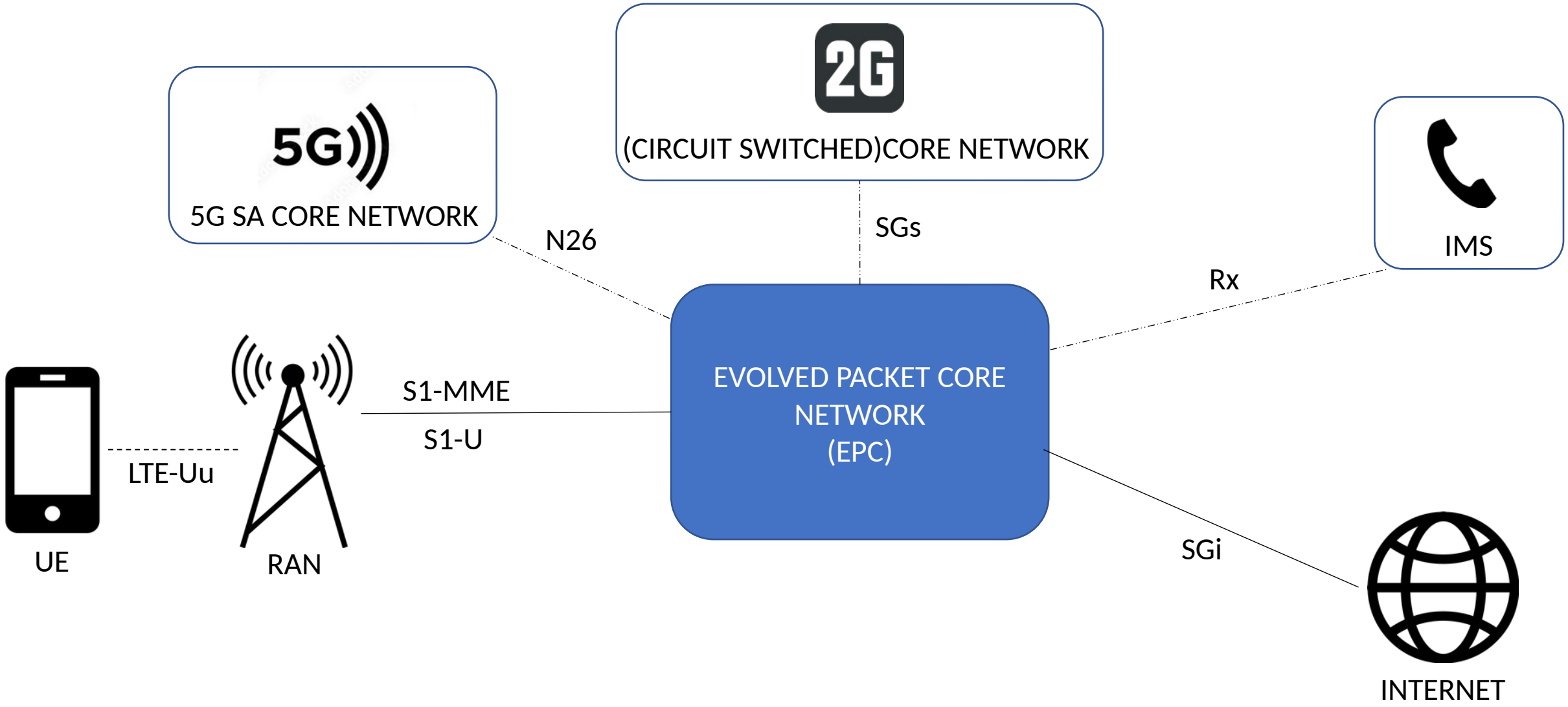
Mobile and IP Network Engineer @ TIM Italy

Linux&Networking Enthusiast by the age of 15 y.o.

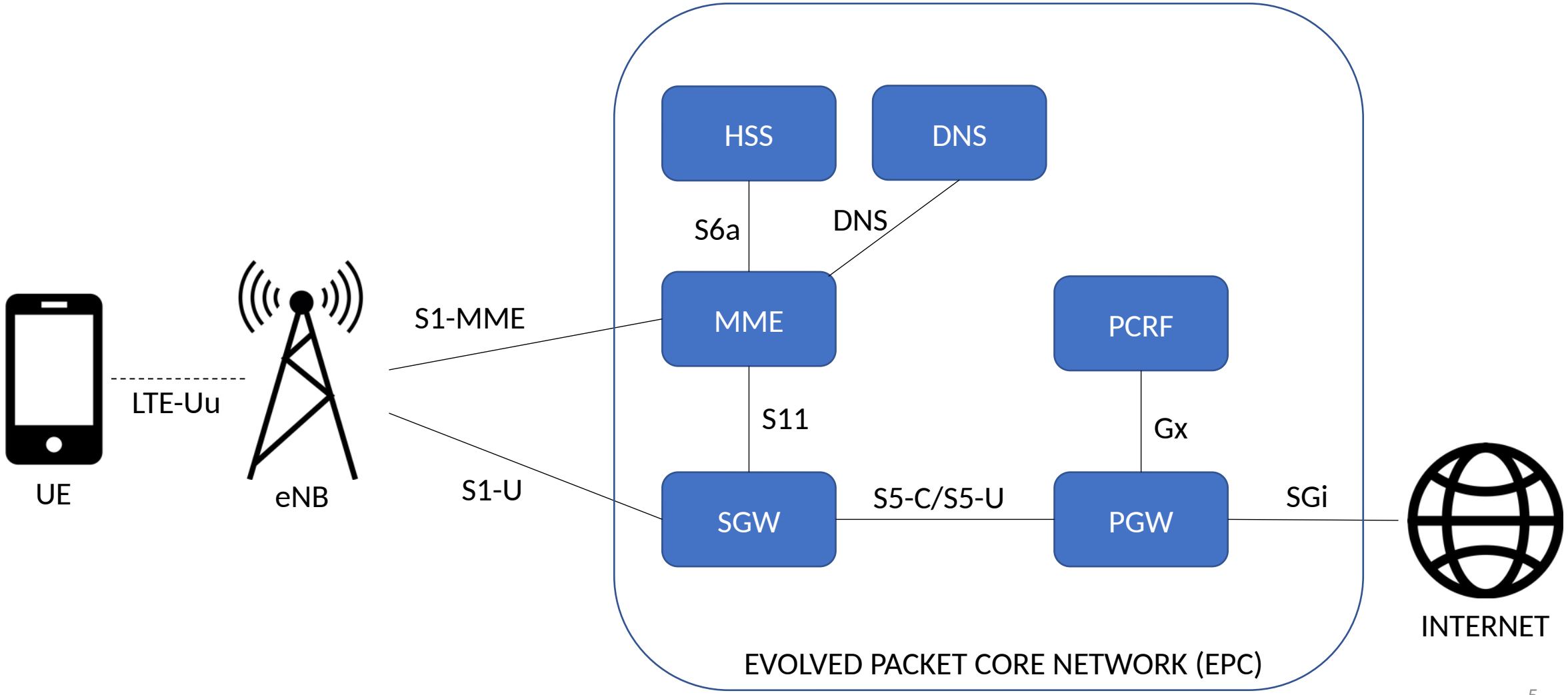
Index

1. LTE Network Overview
2. LTE Network Deep Dive
3. CS vs PS Network comparision
4. Attach Procedure
5. CUPS Paradigm
6. OSS LTE network implementations
7. Open5GS
8. Hardware requirements
9. Dockerized blueprint
10. DEMO
11. Further readings

LTE Network - Overview



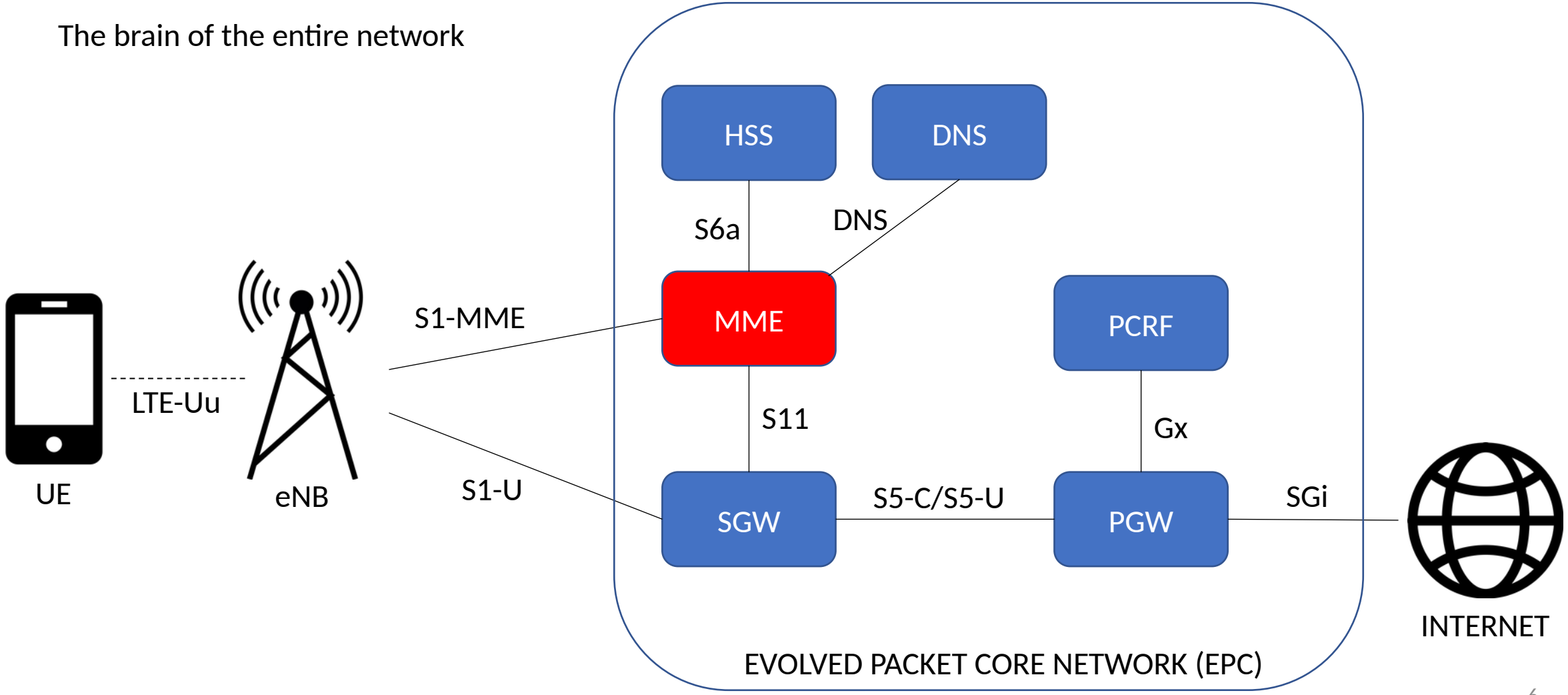
LTE Network – Deep Dive



LTE Network – Deep Dive

MME: Mobility Management Element

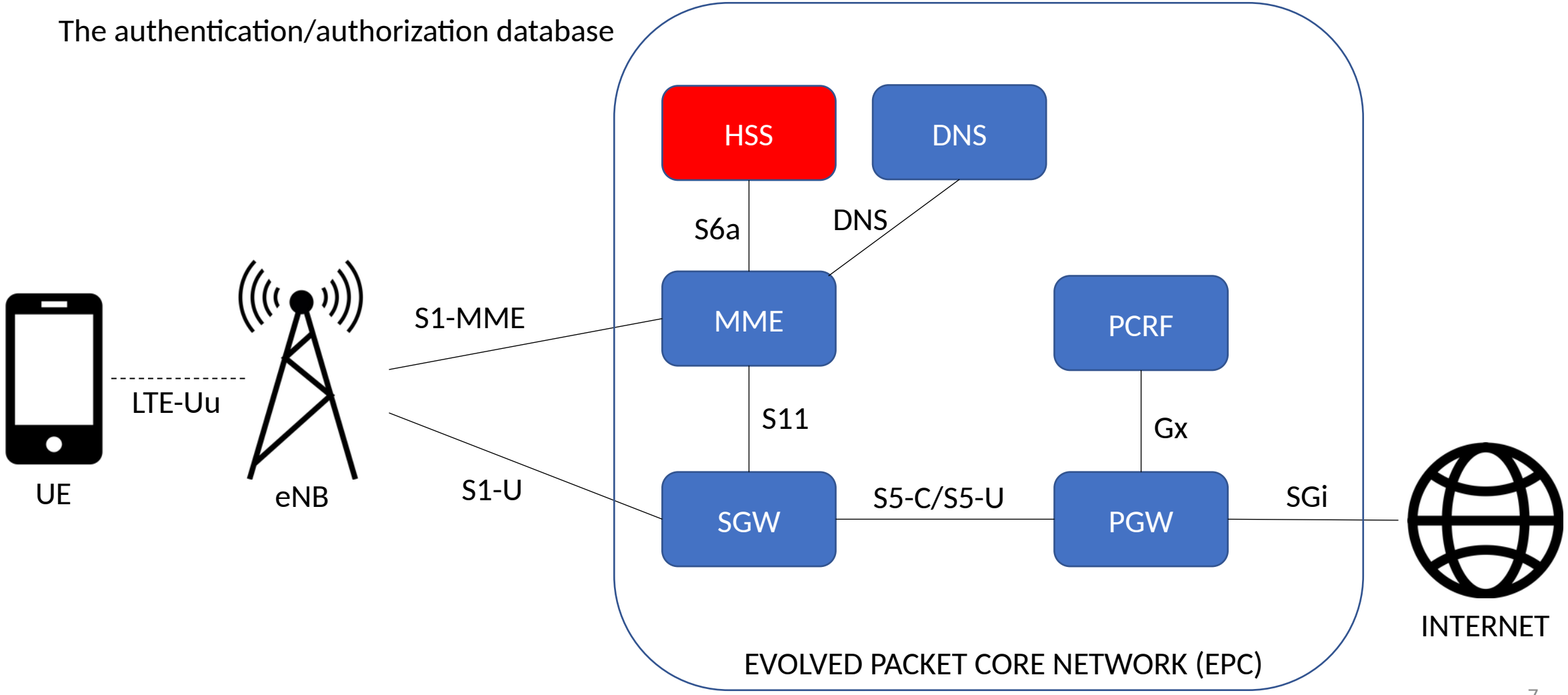
The brain of the entire network



LTE Network – Deep Dive

HSS: Home Subscriber server

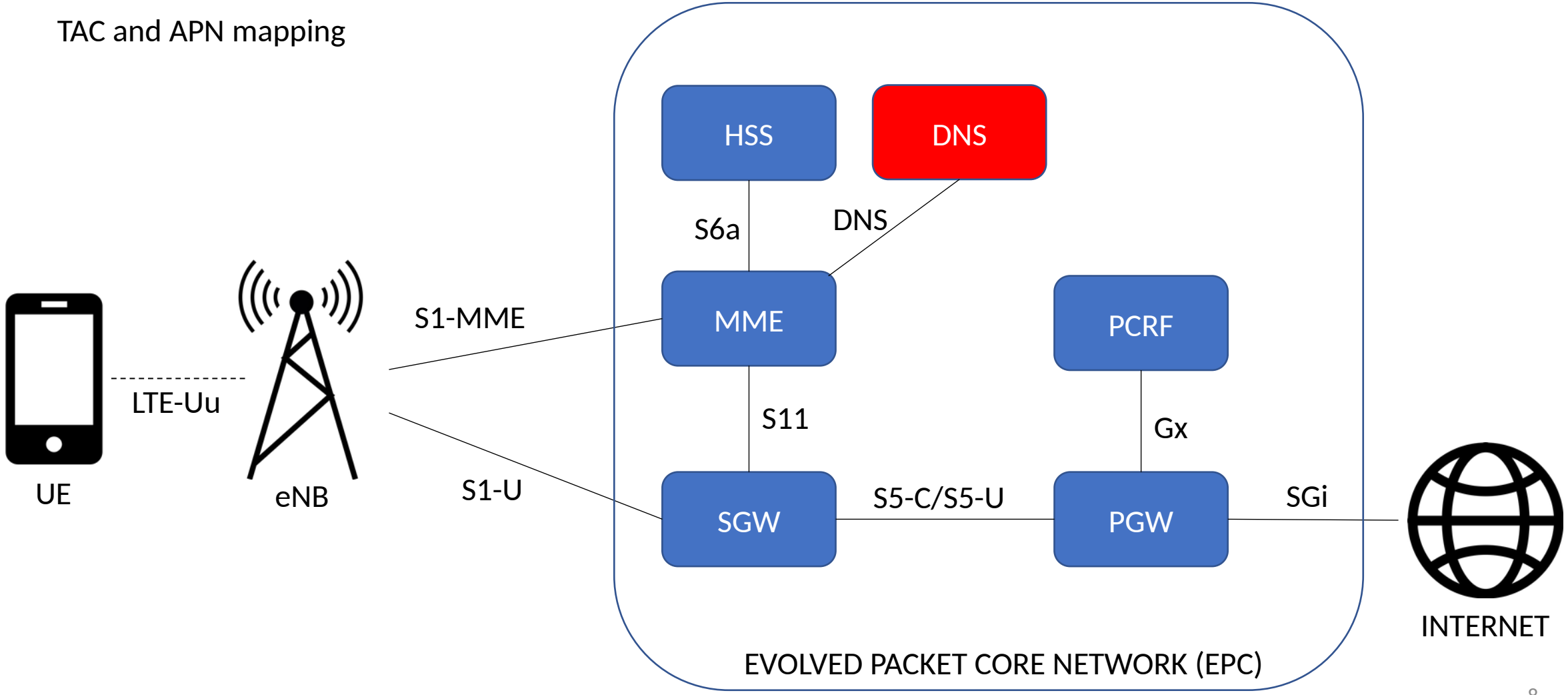
The authentication/authorization database



LTE Network – Deep Dive

DNS: Domain Name Server

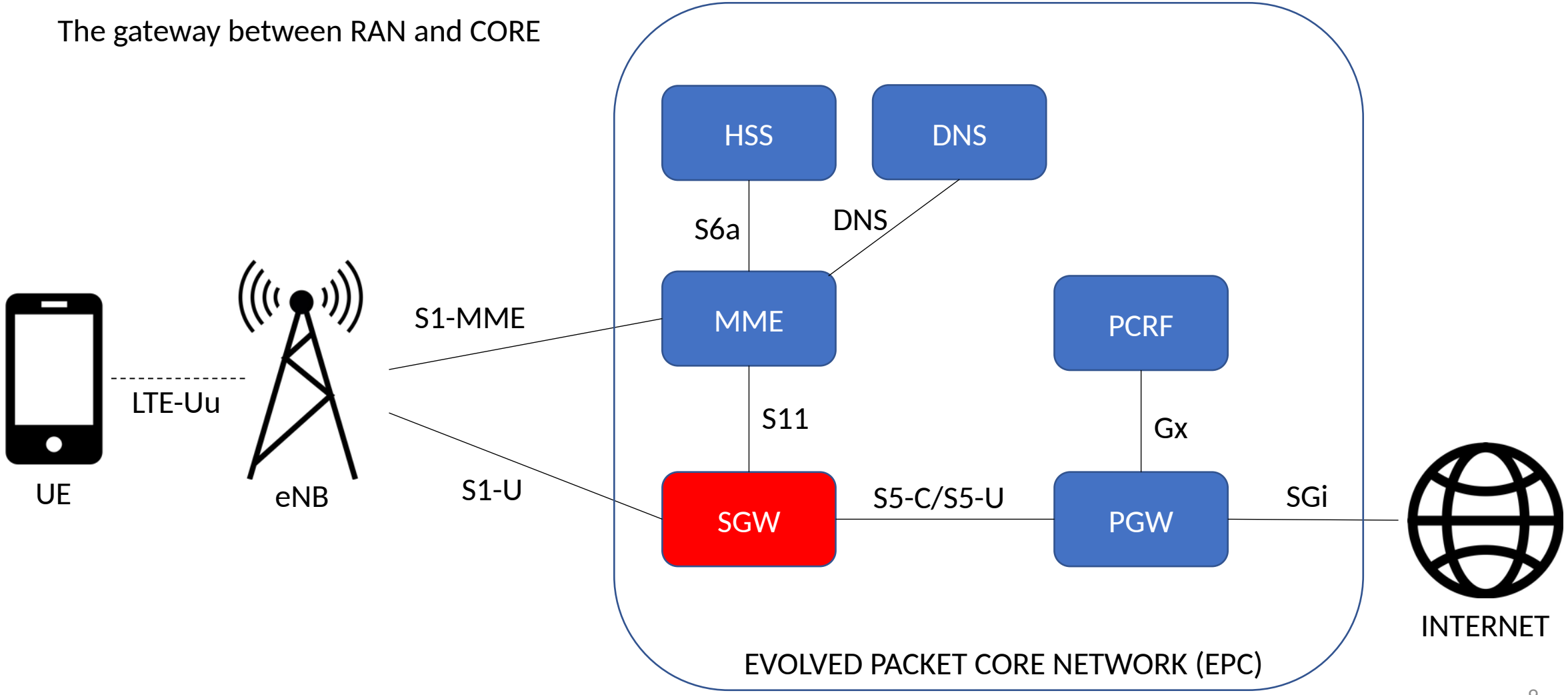
TAC and APN mapping



LTE Network – Deep Dive

SGW: Serving Gateway

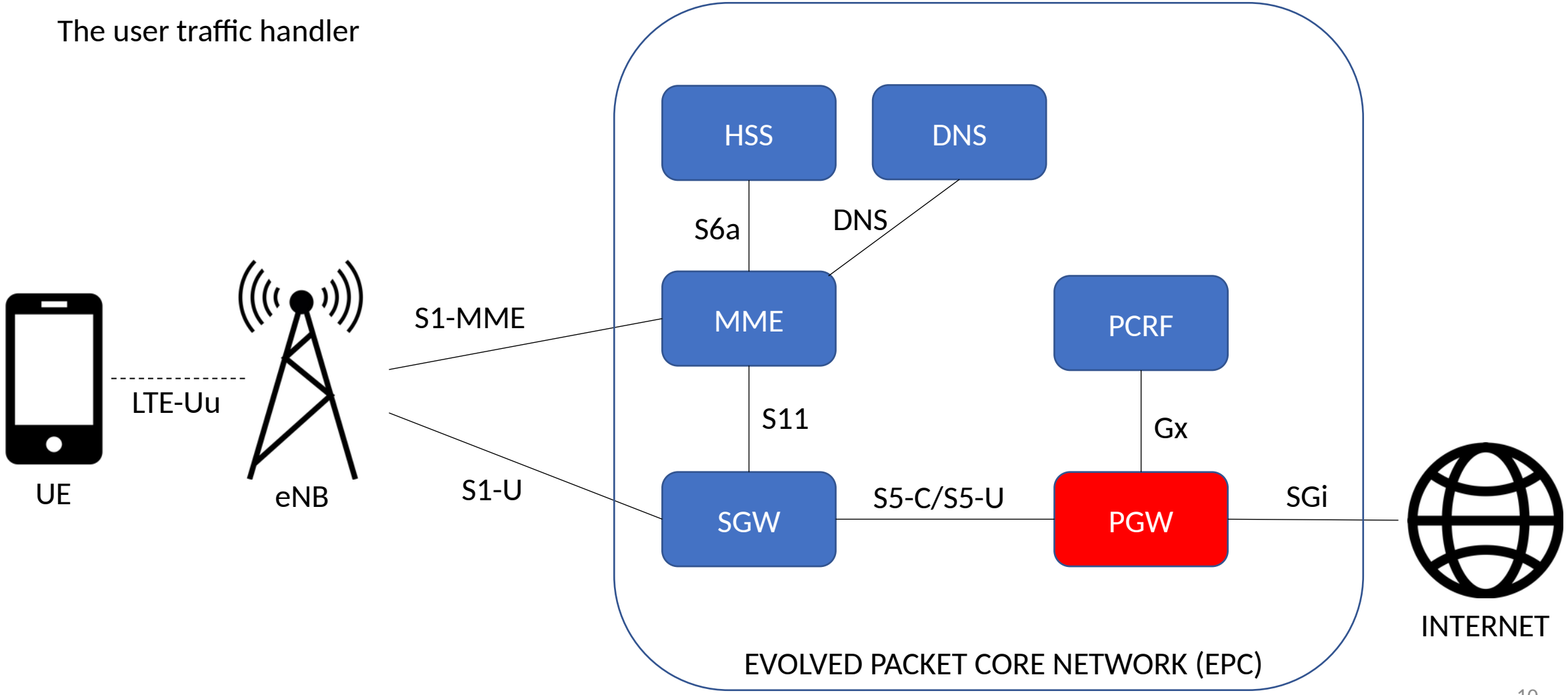
The gateway between RAN and CORE



LTE Network – Deep Dive

PGW: Packet Gateway

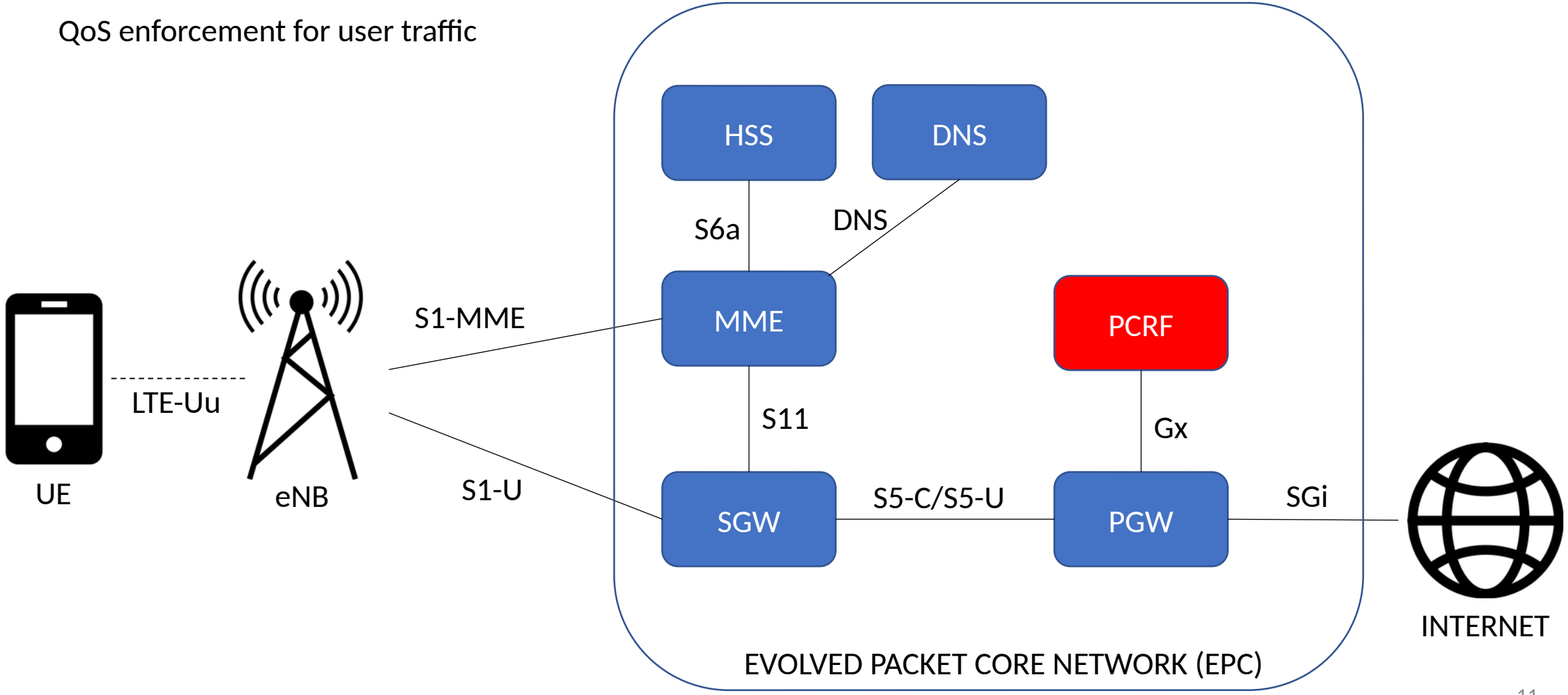
The user traffic handler



LTE Network – Deep Dive

PCRF: Policy and Charging Rules Function

QoS enforcement for user traffic



CS vs PS networks

Circuit Switched Core (2G/3G)

User is «connected» to the network
when is able to make voice calls

SS7 and legacy signaling protocols
Payload on TDM links

Very specialized and customized HW/SW solutions
(often vendor-specific)

User needs to authenticate to the Network
Network is always «trusted»

Packet Switched Core (4G EPC)

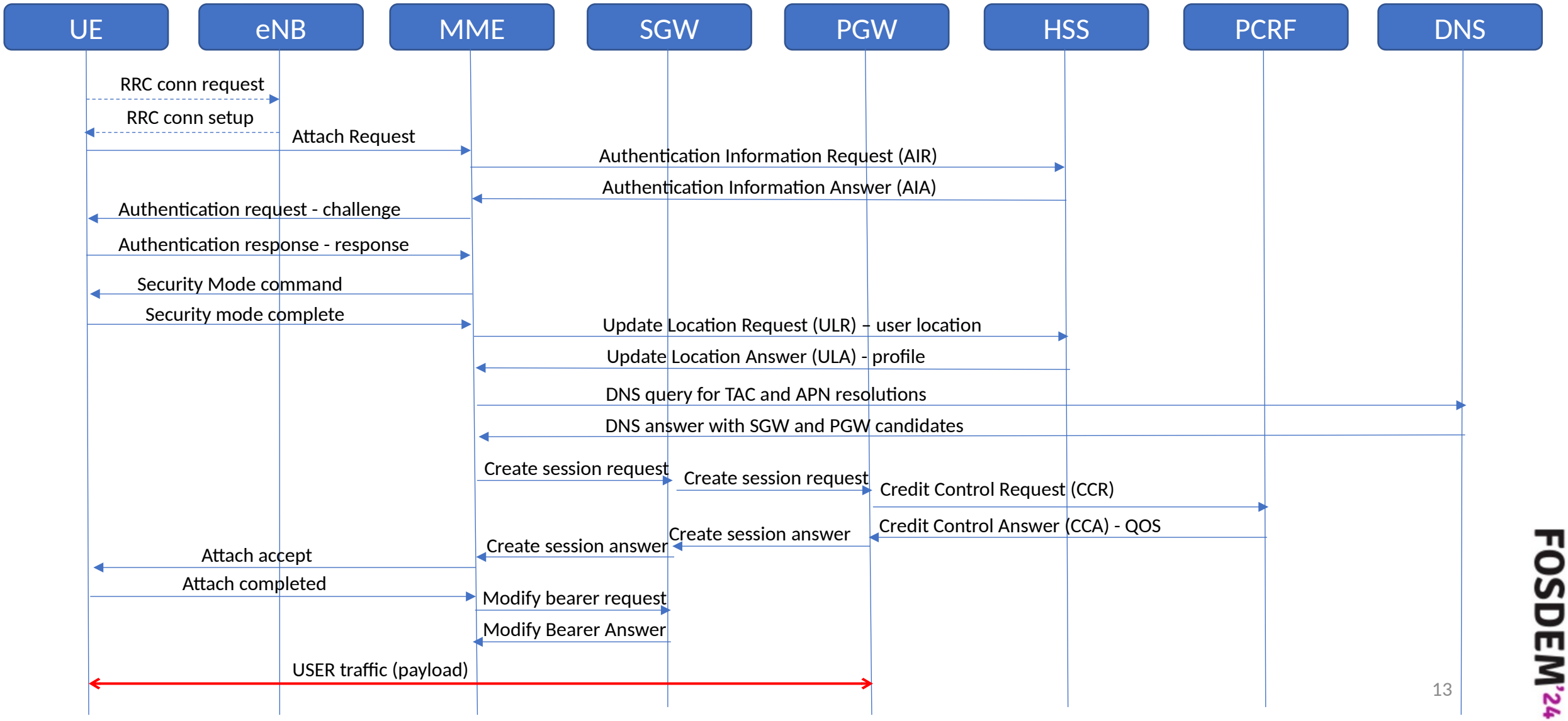
User is «connected» to the network
when is able to exchange IP packets

All-IP network for signaling and user plane

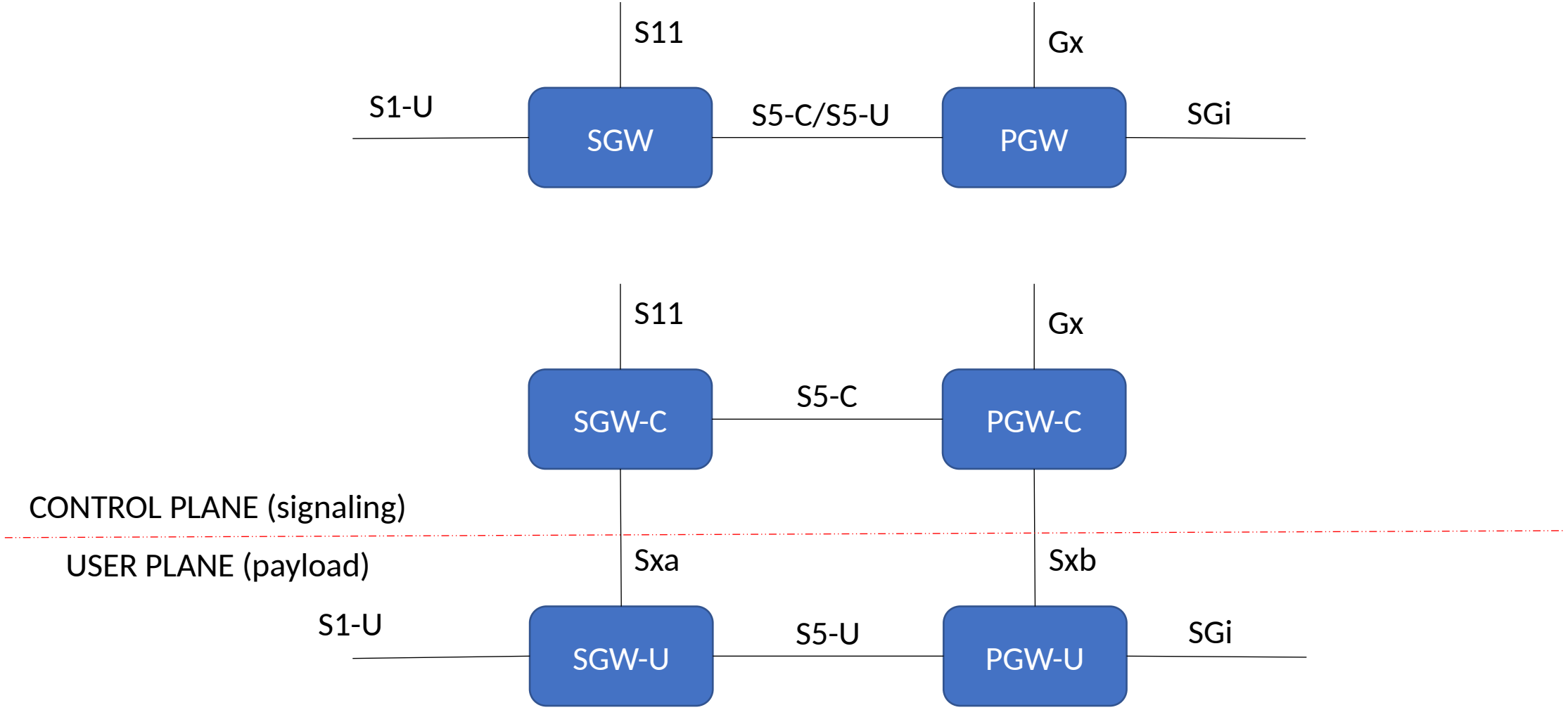
COTS HW and SW
(many commercial solutions are based on Linux and x86)

User and Network mutually authenticate each other

Attach procedure



CUPS paradigm



Now, what about my network?

There are many OSS projects that focuses on implementing 2-3-4-5G Core Network and RAN functions

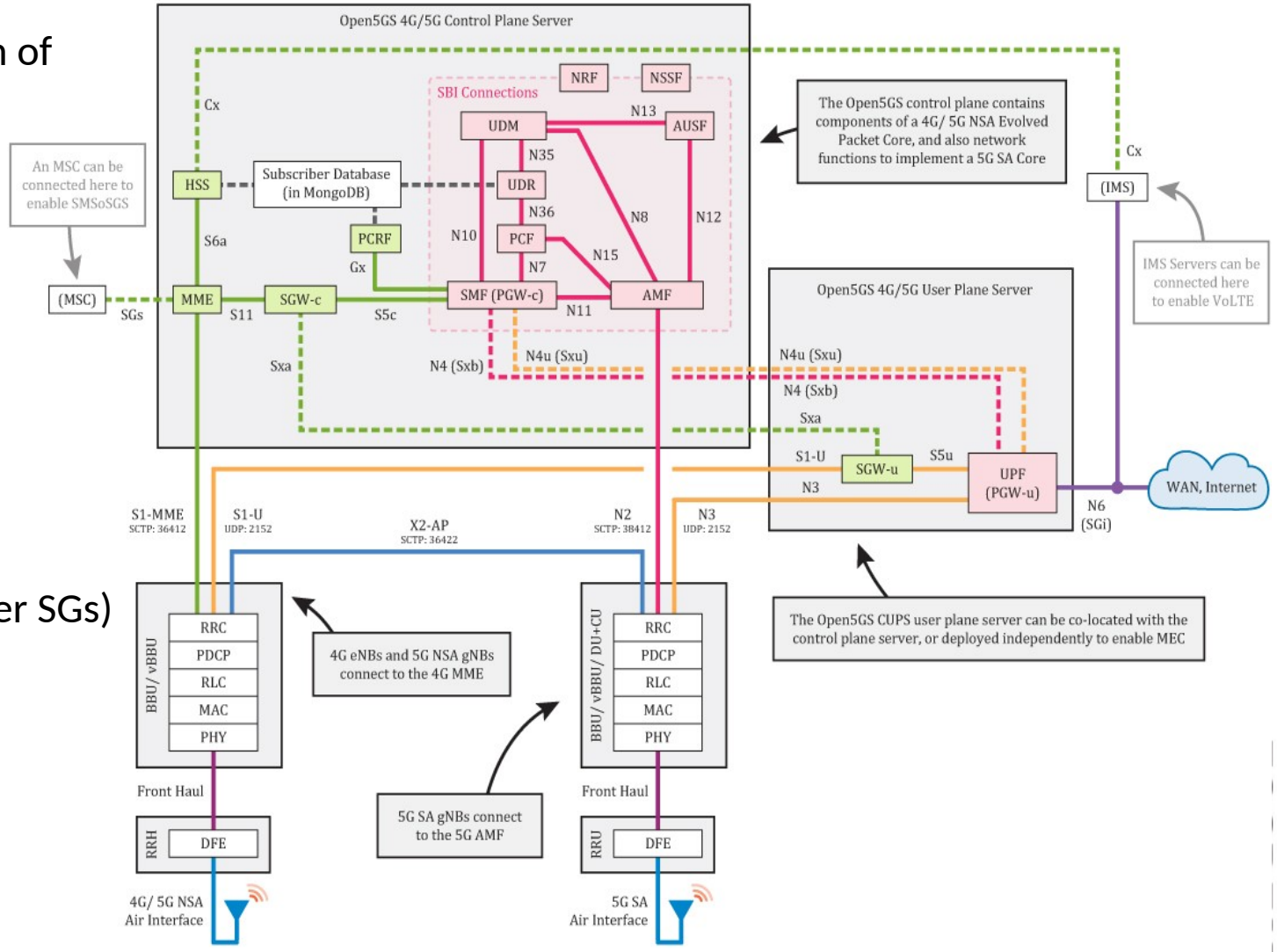
- Open5GS
- NextEPC
- srsRAN & srsEPC
- Osmocom

Open5GS

Open5GS is a C-language Open Source implementation of 5GC and EPC, i.e. the core network of NR/LTE network.

Features

- Release-17 compliant
- AES, Snow3G, ZUC algorithms for encryption
- Support of USIM cards using Milenage
- IPv6 support
- Multiple PDU session
- Handover(5GC Xn/N2 and EPC S1/X2)
- CSFB(Circuit Switched Fall Back) and SMSoS(SMS Over SGs)
- Support ePDG Interface(SWx, S6b, S2b)
- VoLTE(Voice over LTE) with HSS-Cx interface
- VoNR(Voice over NR)
- 5G Roaming



Hardware requirements

- Some form of computing HW (bare metal, vm, container)
- Basic knowledge of core network components and protocols
- One or more SDR for RAN
- RF shielded box or connectorized UE

  In almost all countries a specific authorization is required in order to transmit in air on LTE frequencies!

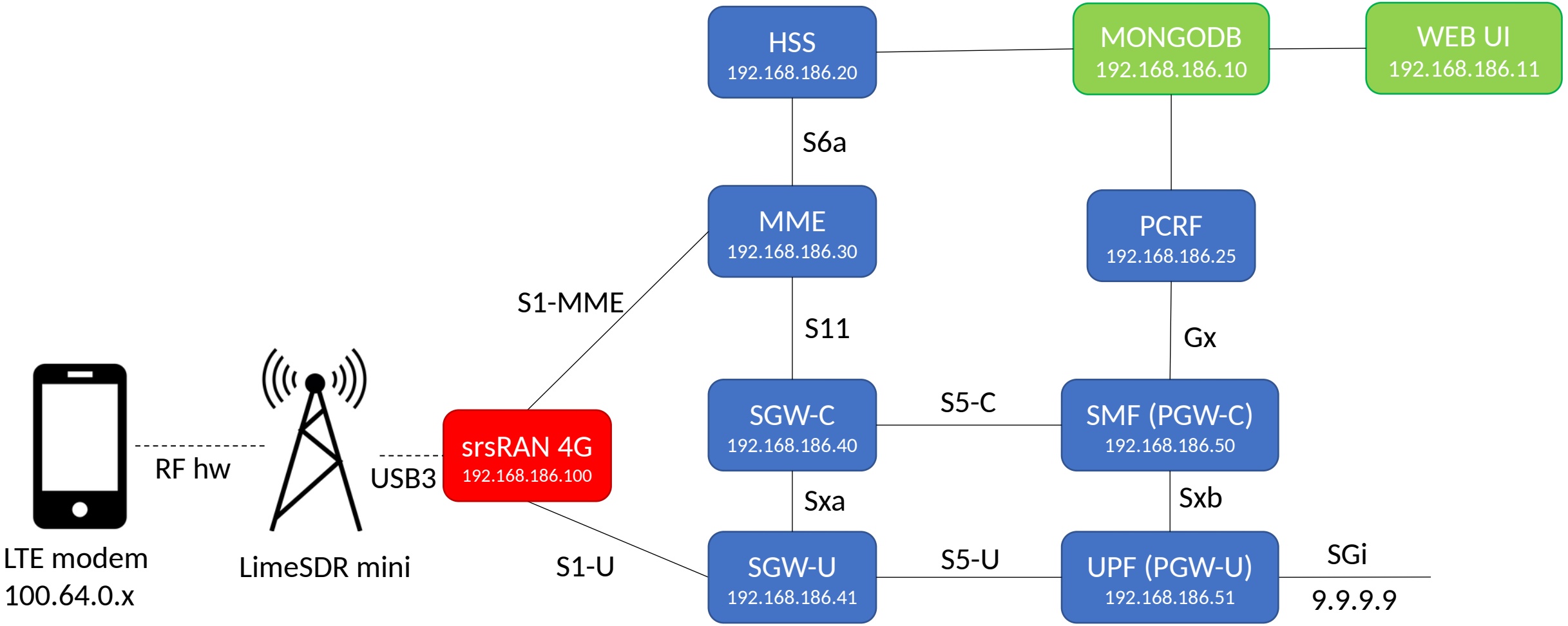
- RF spectrum analyzer (it will make your life easier)
- Programmable SIM card + programming software

  (sysmocom or random «whitelabel» cards can be found on amazon/aliexpress)

- Patience and time – trial and error is a common paradigm also in commercial networks

Dockerized blueprint

https://github.com/m4w0lf/MyOwnLTE/tree/FOSDEM-demo/open5gs/deployment



DEMO

What’s the point?

Historically speaking TELCO network are considered like black magic: just few people know how they work in detail.

It’s a very complex and large eco-system and our lives have been deeply changed by this tecnology

Q&A

Thank you!

Further resources

- 3GPP and ETSI documentation
  https://www.3gpp.org
- Open5GS official site
  https://open5gs.org
- srsRAN-4G project
  https://docs.srsran.com/projects/4g/en/latest/
- Osmocom project
  https://osmocom.org/projects/cellular-infrastructure
- @nickvsnetworking's blog
  https://nickvsnetworking.com
- Phil Greenland's blog
  https://www.quantulum.co.uk/blog/tag/srsran/