

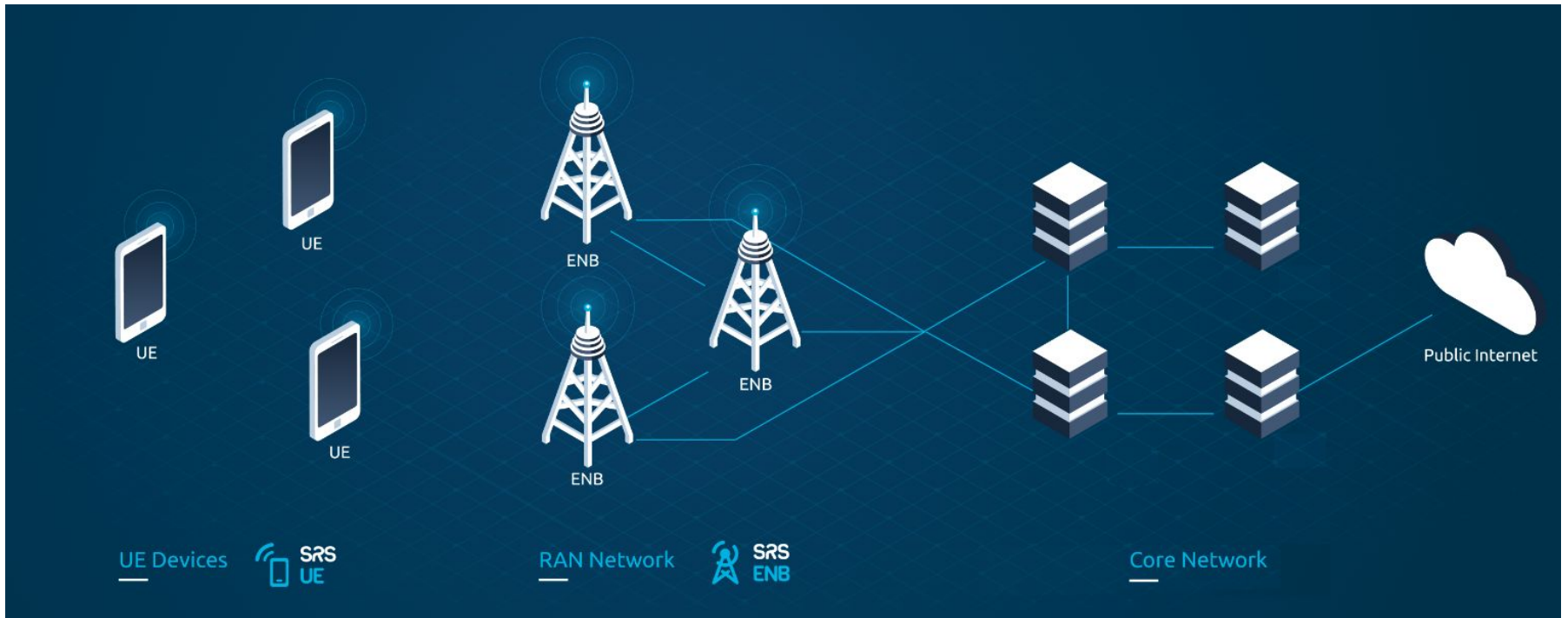
Open-source 5G RAN - srsRAN

Open 5G Forum - Fall 2021

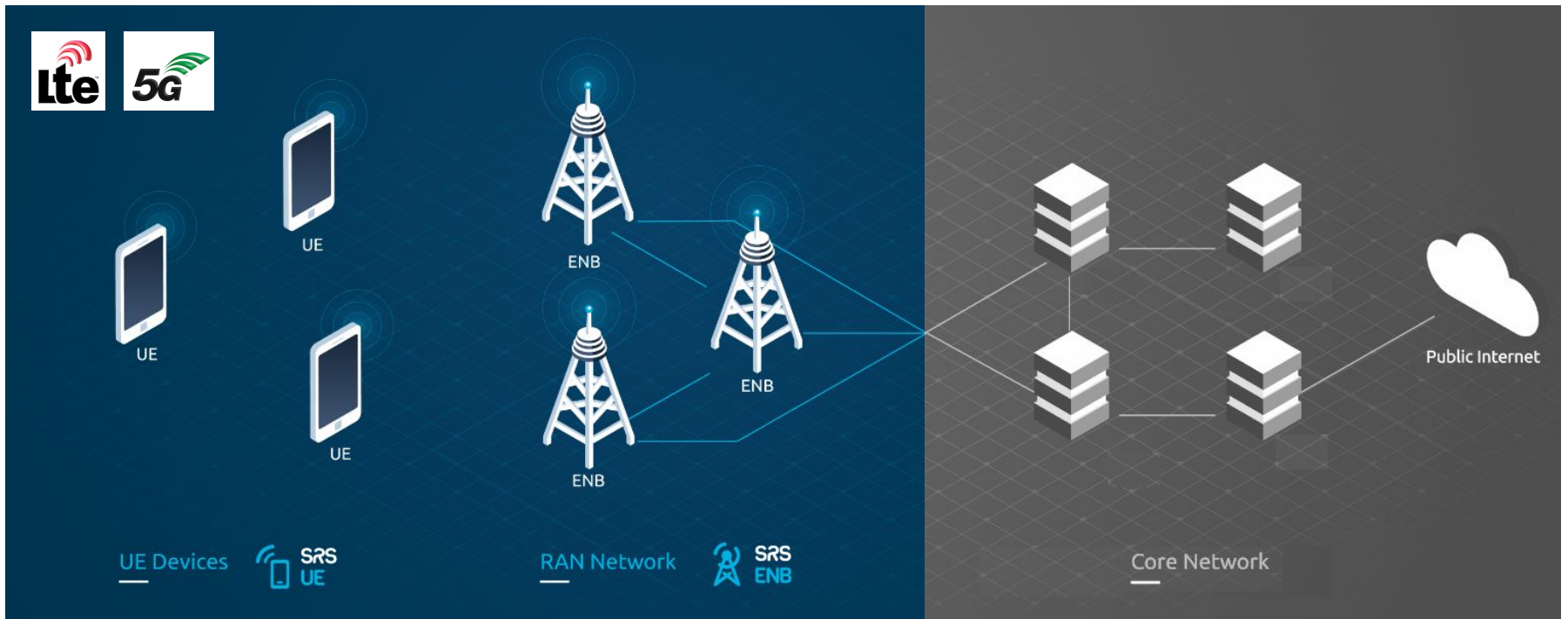
17 November 2021

Software Radio Systems, Ltd
www.srs.io

SRS LTE



SRS RAN



Objectives

Most trusted open-source software for mobile wireless networks

How to get it?



srsRAN

Open Source 4G/5G from Software Radio Systems (SRS)

<https://www.srsran.com> [@srsranproject](https://twitter.com/srsranproject) info@softwareradiosystems.com

[Overview](#) [Repositories 3](#) [Packages](#) [People 13](#) [Teams](#) [Projects](#) [Settings](#)

Pinned

srsRAN Public

Open source SDR 4G/5G software suite from Software Radio Systems (SRS)

C++ 2.3k 767

srsRAN_docs Public

Documentation for the srsRAN project

Makefile 27 24

Customize your pins

People



[Invite someone](#)

Repositories

Find a repository... Type Language Sort New

srsRAN_docs Public

Documentation for the srsRAN project

Makefile 27 AGPL-3.0 24 5 1 Updated 5 days ago

srsRAN Public

Open source SDR 4G/5G software suite from Software Radio Systems (SRS)

C++ 2,335 767 74 6 Updated 5 days ago

Top languages

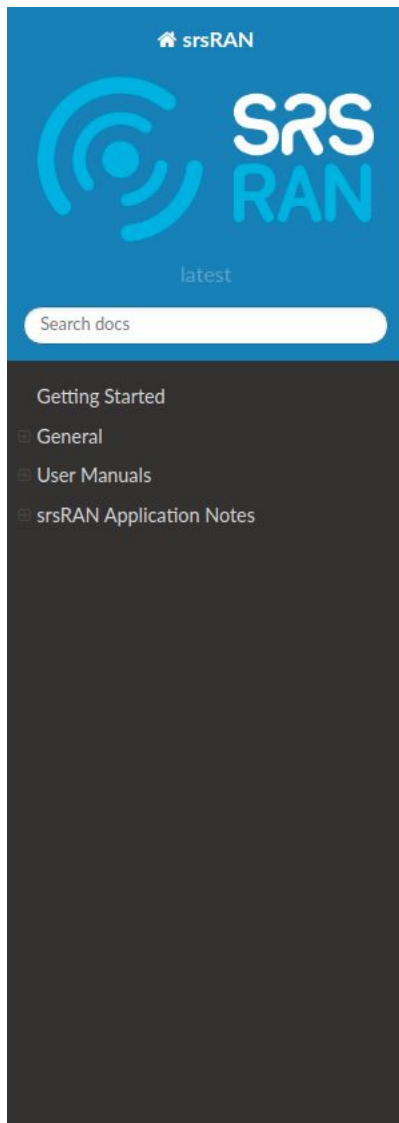
C++ Makefile

<https://github.com/srsran>

How to use it?



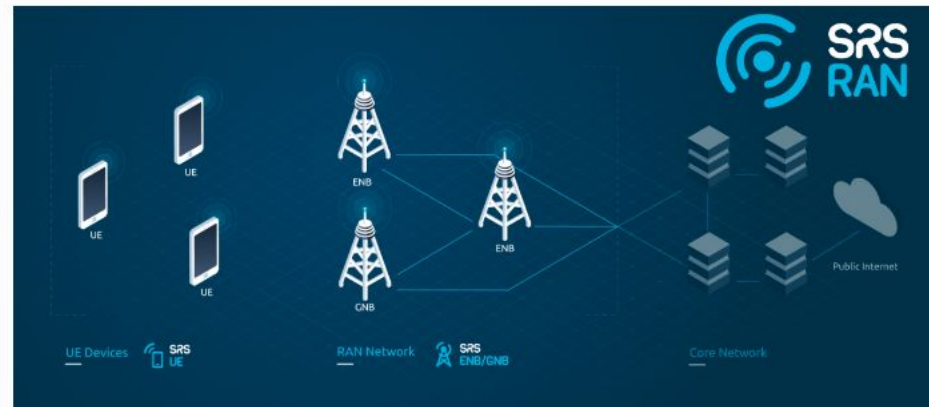
How to use it?



» srsRAN 21.04 Documentation

[Edit on GitHub](#)

srsRAN 21.04 Documentation



srsRAN is a free and open-source 4G and 5G software radio suite.

Featuring both UE and eNodeB/gNodeB applications, srsRAN can be used with third-party core network solutions to build complete end-to-end mobile wireless networks. For more information, see www.srsran.com.

The srsRAN suite currently includes:

- srsUE: a full-stack 4G and 5G NSA UE application (**5G SA coming 2022**)
- srsENB: a full-stack 4G eNodeB and 5G NSA gNodeB application
- srsGNB: a full-stack 5G SA gNodeB application (**coming 2022**)
- srsEPC: a light-weight 4G EPC implementation with MME, HSS and S/P-GW

All srsRAN software runs in linux with off-the-shelf compute and radio hardware.

Is it any good?



Is it any good?



Is it any good?

The screenshot shows the srsRAN website's Research page. At the top, there is a navigation bar with links for Download, Community, Research (highlighted), and Commercial. The main header area features the srsRAN logo and the text "srsRAN for Research" with a sub-header "Published research using srsRAN". A callout box on the right provides instructions for installing the latest release on Ubuntu, including terminal commands: `sudo add-apt-repository ppa:softwareradiosystems/srsran`, `sudo apt-get update`, and `sudo apt-get install srsran -y`.

The main content area displays a grid of 12 research paper cards, each with a title, author information, and a "2021" date tag. Each card also features a circular icon with a right-pointing arrow. The cards are as follows:

- A Context-aware Radio Resource Management in Heterogeneous Virtual RANs** (Politecnico di Torino)
- QCell: Self-optimization of Softwarized 5G Networks through Deep Q-learning** (Politecnico de Milano, Northeastern University, WIoT)
- Democratizing Cellular Access with CellBricks (Extended Version)** (UC Berkeley, Virginia Tech, Facebook, ICSI)
- FedRAN: Federated Mobile Edge Computing with Differential Privacy** (University of Utah)
- Design, Implementation and Experimental Evaluation of a Network-Slicing aware Mobile Protocol Stack** (UC3M)
- ProChecker: An Automated Security and Privacy Analysis Framework for 4G LTE Protocol Implementations** (Pennsylvania State University)
- BERSERKER: ASN-1 Based Fuzzing of Radio Resource Control Protocol for 4G and 5G** (KTH, Ericsson)
- Experimental Evaluation of Power Consumption in Virtualized Base Stations** (TCD, TU Delft, i2CAT, ICREA, NEC)
- Demonstrating a Bayesian Online Learning for Energy-Aware Resource Orchestration in vRANs** (TCD, TU Delft, i2CAT, ICREA, NEC)
- Virtualized Cellular Networks with Native Cloud Functions** (University of Vigo)
- Rise of the Machines: On the Security of Cellular IoT Devices** (KU Leuven)
- Mobile and Wireless Research on the POWDER Platform** (University of Utah)

At the bottom of the grid, there is a pagination bar with numbers 1 through 19, where 1 is highlighted.

Is it any good?

A reflection on the history of cellular security research and the security outlook of 5G

Published on June 26, 2019



Roger Piqueras Jover
Senior Security Architect at Bloomberg LP

3 articles [Following](#)

About 10 years ago, I started working on mobile and cellular security research. While most of my work in the early days leveraged costly [network testing equipment and a neat lab set-up](#), I also experimented with a number of open-source implementations of the LTE (Long Term Evolution) PHY layer, which were critical for the work on protocol-aware jamming back in 2011. Everything changed in 2012, though. On December 31st 2011 the first commit for [openLTE](#) had been uploaded and for the very first time, there was an open-source implementation of the LTE stack aiming to go beyond the PHY layer. Just a couple of years later, by 2013/2014, after outstanding progress in the development of openLTE, I was in the lab able to test LTE IMSI-catching, taking advantage of unprotected *AttachReject* messages and tracking devices via mapping MSISDN (i.e. phone numbers) to TMSI to C-RNTI.

“Currently srsLTE is by far the best and most widely used – both in academia and industry – tool for LTE security research”

Is it any good?



GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Mobile Security Hall of Fame

CVD-2017	0007	Altaf Shaik	Technical University of Berlin and Kaitiaki Labs https://www.isti.tu-berlin.de/security_in_telecommunications
CVD-2017	0007	Revishankar Borgeonkar	SINTEF Digital and Kaitiaki Labs https://www.sintef.no/en/cyber-security/#/
CVD-2018	0008	David Rupprecht Katharina Kohls Christina Pöpper Thorsten Holz	Ruhr University Bochum and New York University Abu Dhabi https://www.alter-attack.net
CVD-2018	00011	Loïc Ferreira	Orange Labs / IRISA http://crypto.rd.francetelecom.com/people/Ferreira
CVD-2018	00011	Gildas Avoine	INSA Rennes / IRISA http://avoine.net
CVD-2018	0012	David Basin Jennik Dreier Lucca Hirschi Sasa Radomirovic Ralf Sasse Vincent Stettler	ETH Zurich, Université de Lorraine CNRS, Inria, University of Dundee https://arxiv.org/abs/1806.10360
CVD-2018	0013	Merlin Chlosta David Rupprecht Thorsten Holz	Ruhr University Bochum, Germany Paper, Talk
CVD-2018	0013	Christina Pöpper	NYU Abu Dhabi, United Arab Emirates Paper, Talk
CVD-2018	0014	Elisa Bertino	Purdue University https://www.cs.purdue.edu/homes/bertino/
CVD-2018	0014	Omer Chowdhury	University of Iowa http://homepage.dvms.uiowa.edu/~comarhaider/
CVD-2018	0014	Mitziu Echeverria	University of Iowa
CVD-2018	0014	Syed Rafiul Hussain	Purdue University https://relentless-warrior.github.io/
CVD-2018	0014	Ninghui Li	Purdue University https://www.cs.purdue.edu/homes/ninghui/
CVD-2019	0018	Altaf Shaik	Technical University of Berlin https://www.isti.tu-berlin.de/security_in_telecommunications
CVD-2019	0018	Revishankar Borgeonkar	SINTEF Digital https://www.sintef.no/en/all-employees/employee/?empid=7610
CVD-2019	0024	David Rupprecht Christina Pöpper Thorsten Holz	Ruhr University Bochum, Germany and New York University Abu Dhabi
CVD-2019	0026	Cathal Mc Daid	AdaptiveMobile Security https://www.adaptivemobile.com
CVD-2019	0029	Syed Rafiul Hussain Mitziu Echeverria Imtiaz Karim Omer Chowdhury Elisa Bertino	Purdue University University of Iowa Purdue University University of Iowa Purdue University
CVD-2019	0030	David Rupprecht Katharina Kohls Thorsten Holz	Ruhr University Bochum
CVD-2019	0030	Christina Pöpper	NYU Abu Dhabi

Is it any good?



GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Mobile Security Hall of Fame

CVD-2017	0007	Altaf Shaik	Technical University of Berlin and Kaitiaki Labs https://www.isti.tu-berlin.de/security_in_telecommunications
CVD-2017	0007	Revishankar Borgeonkar	SINTEF Digital and Kaitiaki Labs https://www.sintef.no/en/cyber-security/#/
CVD-2018	0008	David Rupprecht Katharina Kohls Christina Pöpper Thorsten Holz	Ruhr University Bochum and New York University Abu Dhabi https://www.alter-attack.net
CVD-2018	00011	Loïc Ferreira	Orange Labs / IRISA http://crypto.rd.francetelecom.com/people/Ferreira
CVD-2018	00011	Gildas Avoine	INSA Rennes / IRISA http://avoine.net
CVD-2018	0012	David Basin Jennik Dreier Lucca Hirschi Sasa Radomirovic Ralf Sasse Vincent Stettler	ETH Zurich, Université de Lorraine CNRS, Inria, University of Dundee https://arxiv.org/abs/1806.10360
CVD-2018	0013	Merlin Chlosta David Rupprecht Thorsten Holz	Ruhr University Bochum, Germany Paper, Talk
CVD-2018	0013	Christina Pöpper	NYU Abu Dhabi, United Arab Emirates Paper, Talk
CVD-2018	0014	Elisa Bertino	Purdue University https://www.cs.purdue.edu/homes/bertino/
CVD-2018	0014	Omer Chowdhury	University of Iowa http://homepage.dvms.uiowa.edu/~comarhalder/
CVD-2018	0014	Mitziu Echeverria	University of Iowa
CVD-2018	0014	Syed Rafiul Hussain	Purdue University https://relentless-warrior.github.io/
CVD-2018	0014	Ninghui Li	Purdue University https://www.cs.purdue.edu/homes/ninghui/
CVD-2019	0018	Altaf Shaik	Technical University of Berlin https://www.isti.tu-berlin.de/security_in_telecommunications
CVD-2019	0018	Revishankar Borgeonkar	SINTEF Digital https://www.sintef.no/en/all-employees/employee/?empid=7610
CVD-2019	0024	David Rupprecht Christina Pöpper Thorsten Holz	Ruhr University Bochum, Germany and New York University Abu Dhabi
CVD-2019	0026	Cathal Mc Daid	AdaptiveMobile Security https://www.adaptivemobile.com
CVD-2019	0029	Syed Rafiul Hussain Mitziu Echeverria Imtiaz Karim Omer Chowdhury Elisa Bertino	Purdue University University of Iowa Purdue University University of Iowa Purdue University
CVD-2019	0030	David Rupprecht Katharina Kohls Thorsten Holz	Ruhr University Bochum
CVD-2019	0030	Christina Pöpper	NYU Abu Dhabi

Who maintains it?

- Private company founded in 2012
- Office locations in Ireland and Spain
- Global customer base
- 22 Full-Time Employees
- 100% SDR Engineering
- 100% Organic growth



How is it funded?



- Open-source under AGPL

OR

- Commercial source-code license



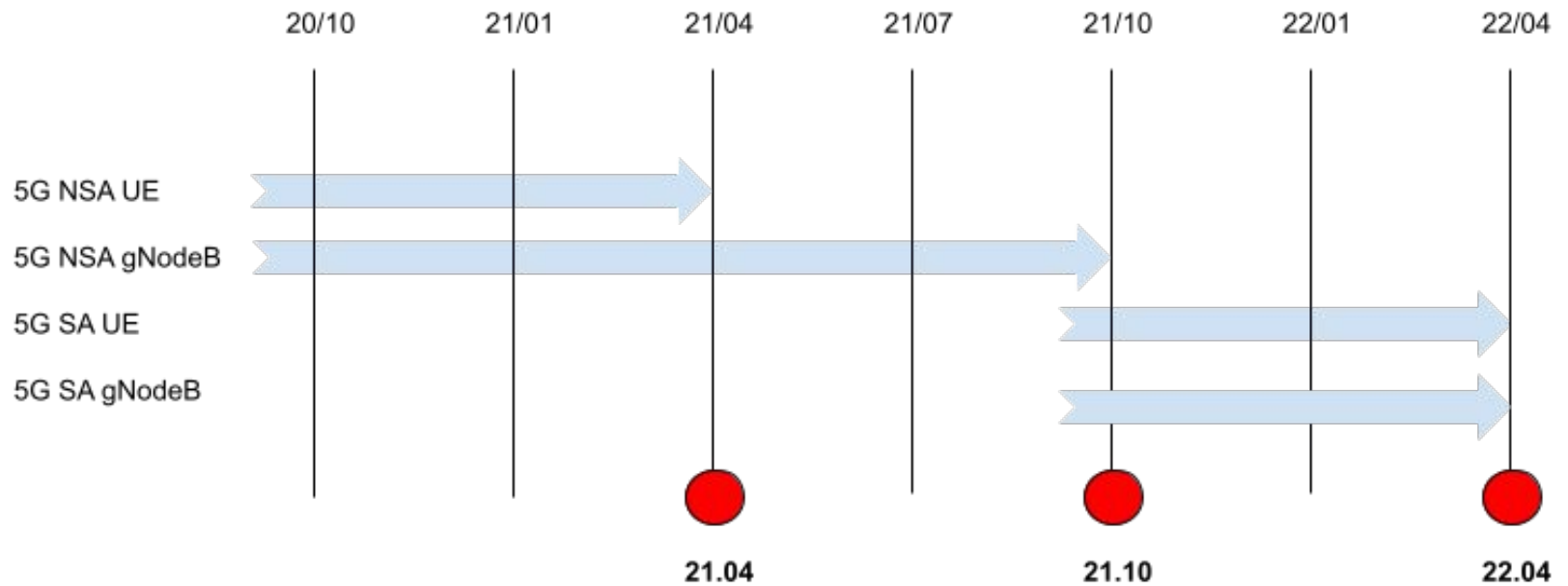
How is it funded?



European Space Agency

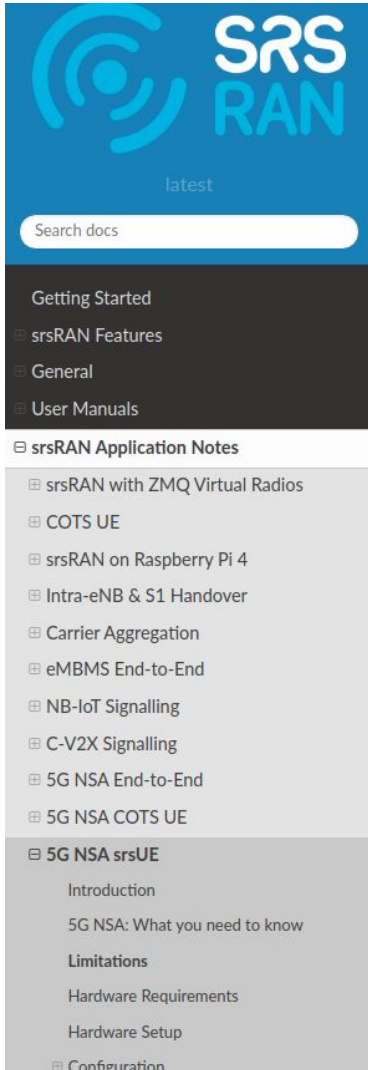


Roadmap?



21.04 - 5G NSA UE

21.04 - 5G NSA UE



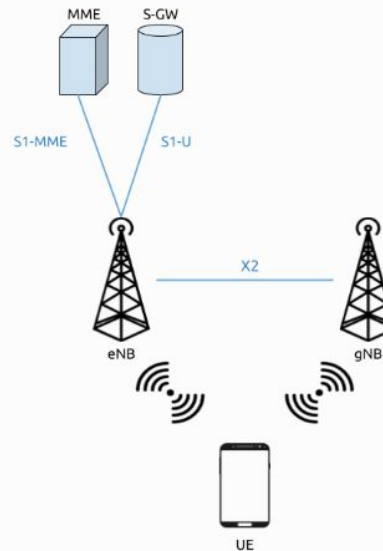
The screenshot shows the srsRAN documentation website. At the top left is the srsRAN logo. Below it is a search bar labeled "Search docs". The main navigation menu is on the left, with categories: Getting Started, srsRAN Features, General, User Manuals, srsRAN Application Notes, and 5G NSA srsUE. The 5G NSA srsUE section is expanded, showing sub-items: Introduction, 5G NSA: What you need to know, Limitations, Hardware Requirements, Hardware Setup, and Configuration.

5G NSA srsUE

Introduction

The 21.04 release of srsRAN brought 5G NSA (Non-Standalone) support to srsUE. This application note shows how the UE can be used with a third-party 5G NSA network. In this example, we use the Amari Callbox Classic from Amarisoft to provide the network.

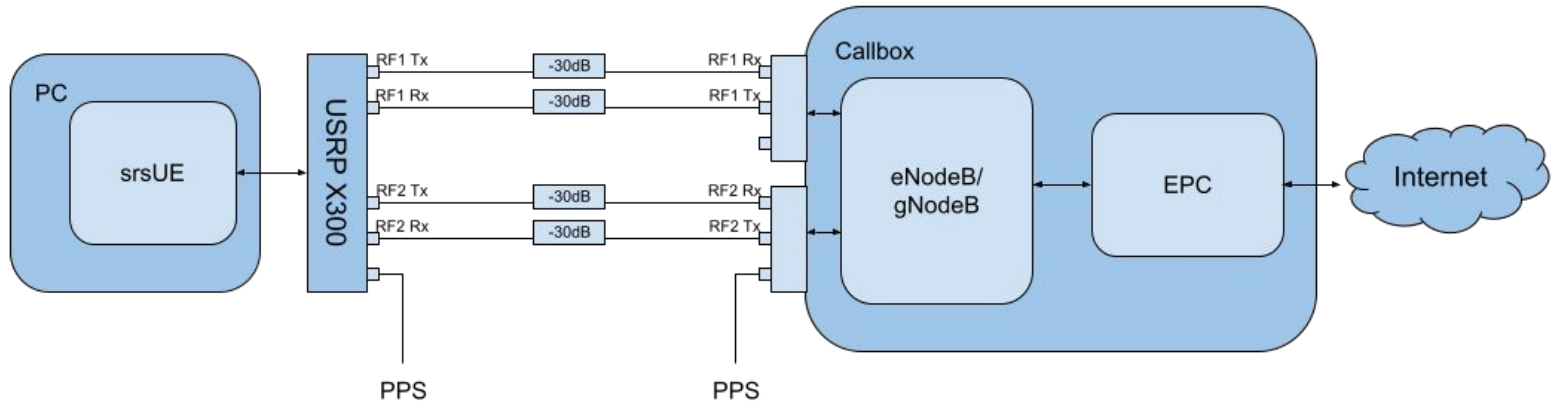
5G NSA: What you need to know



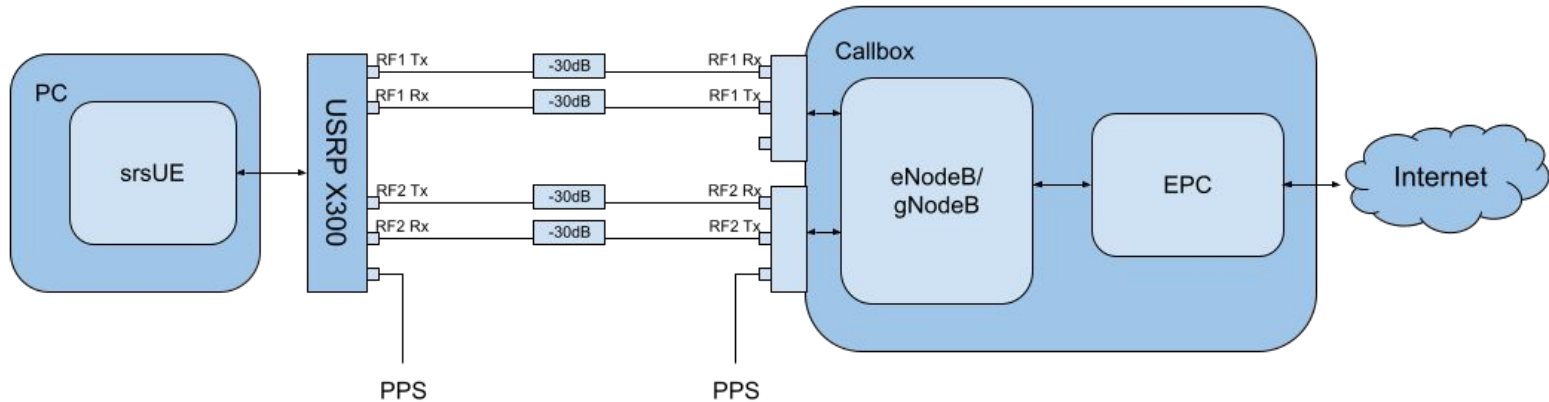
5G NSA Mode 3

https://docs.srsran.com/en/latest/app_notes/source/5g_nsa_amari/source/index.html

21.04 - 5G NSA UE



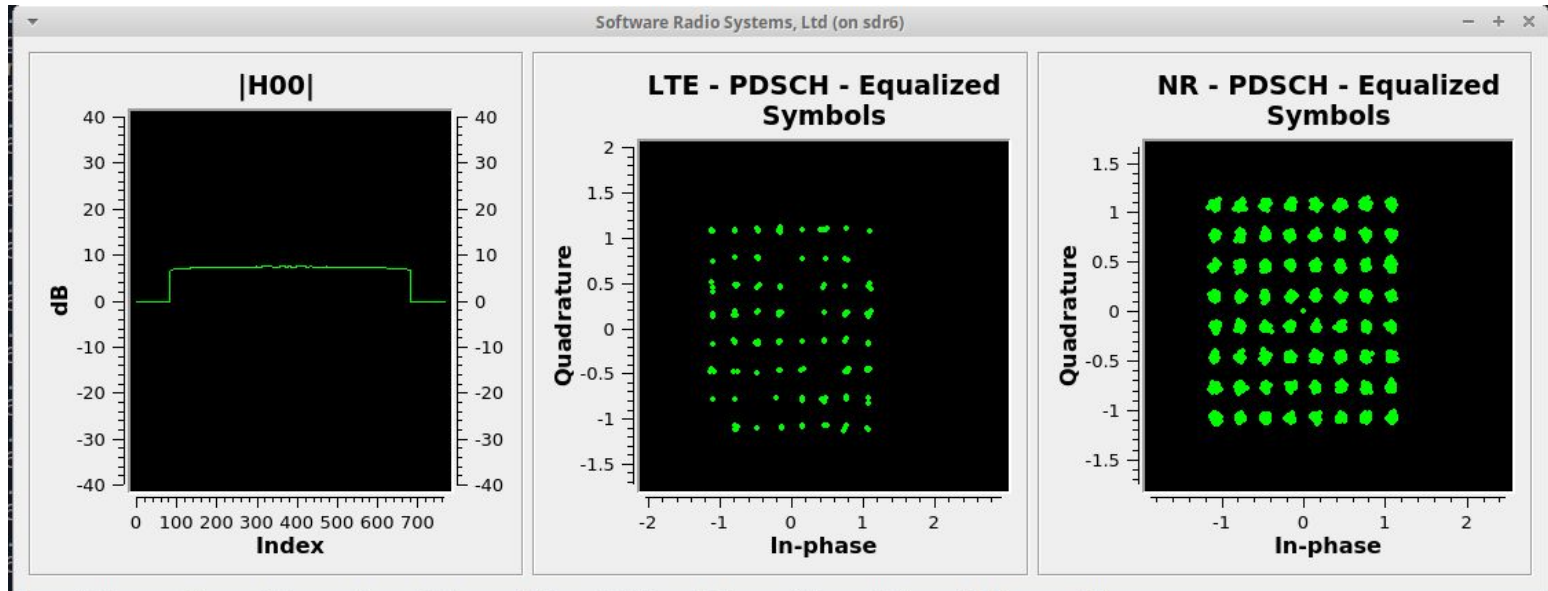
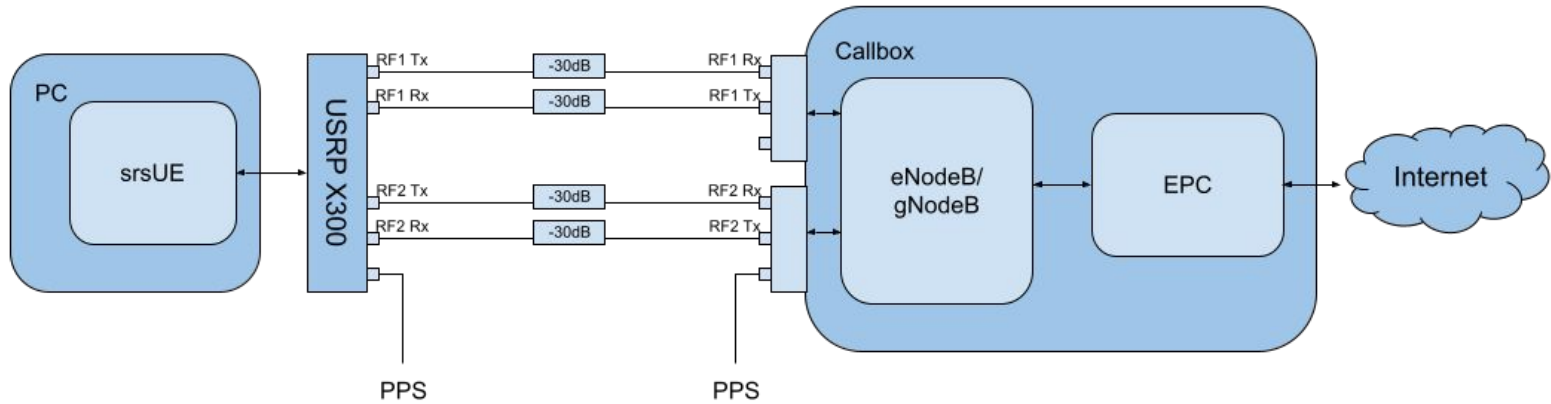
21.04 - 5G NSA UE



```

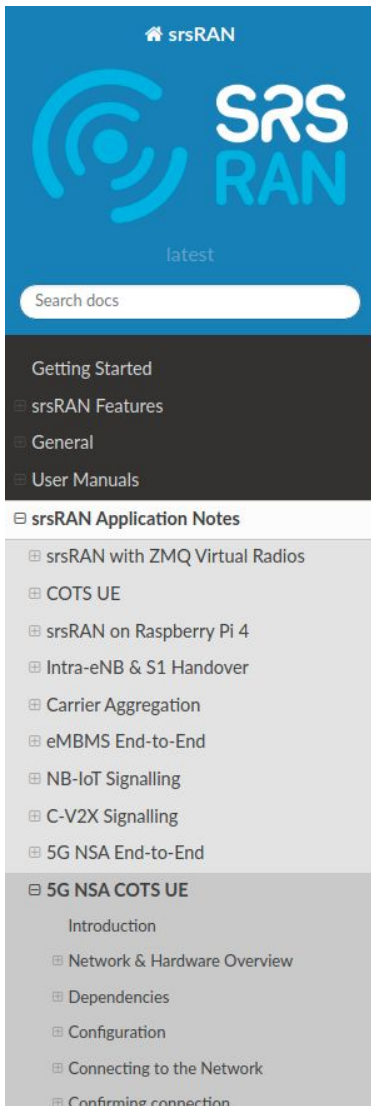
Found Cell: Mode=FDD, PCI=1, PRB=50, Ports=1, CF0=0.1 KHz
Found PLMN: Id=00101, TAC=7
Random Access Transmission: seq=17, tti=8494, ra-rnti=0x5
RRC Connected
Random Access Complete.      c-rnti=0x3d, ta=3
Network attach successful. IP: 192.168.4.2
Amarisoft Network (Amarisoft) 20/4/2021 23:32:40 TZ:105
RRC NR reconfiguration successful.
Random Access Transmission: prach_occasion=0, preamble_index=0, ra-rnti=0x7f, tti=8979
Random Access Complete.      c-rnti=0x4601, ta=23
-----Signal-----|-----DL-----|-----UL-----
rat  pci  rsrp  pl  cfo  | mcs  snr  iter  brate  bler  ta_us  | mcs  buff  brate  bler
lte   1   -52  13   12  | 19   40   0.5   15k    0%   7.3   | 16   0.0   10k    4%
nr    500   4   0  881m | 2    31   1.0    0.0    0%   0.0   | 17   0.0   6.0k   0%
lte   1   -49   7  -4.8 | 28   40   0.5   1.4k   0%   7.3   | 0    0.0   0.0    0%
nr    500   3   0  -5.9 | 27   35   1.0   1.3k   0%   0.0   | 28   0.0  148k   0%
lte   1   -58  16  -3.7 | 28   40   0.5   1.4k   0%   7.3   | 0    0.0   0.0    0%
nr    500   3   0  -7.7 | 27   35   1.0   1.3k   0%   0.0   | 28   0.0  148k   0%
lte   1   -61  19  428m | 28   40   0.5   1.4k   0%   7.3   | 0    0.0   0.0    0%
nr    500   4   0   2.2 | 27   30   1.4   67k    0%   0.0   | 28   28   143k   0%
lte   1   -61  19 -507m | 28   40   0.5   1.4k   0%   7.3   | 0    0.0   0.0    0%
nr    500   4   0  924m | 27   24   1.9   18M    0%   0.0   | 28   0.0   3.7k   0%
lte   1   -61  19   3.8 | 28   40   0.5   1.4k   0%   7.3   | 0    0.0   0.0    0%
nr    500   4   0   3.5 | 27   24   1.9   18M    0%   0.0   | 0    0.0   0.0    0%
lte   1   -61  19   3.8 | 28   40   0.5   1.4k   0%   7.3   | 0    0.0   0.0    0%
nr    500   4   0   3.1 | 27   24   1.9   18M    0%   0.0   | 0    0.0   0.0    0%
    
```

21.04 - 5G NSA UE



21.10 - 5G NSA eNodeB

21.10 - 5G NSA eNodeB



The screenshot shows the srsRAN documentation website. At the top, there is a search bar labeled "Search docs" and a "latest" indicator. Below the search bar is a navigation menu with the following items: "Getting Started", "srsRAN Features", "General", "User Manuals", and "srsRAN Application Notes". Under "srsRAN Application Notes", there is a list of application notes, with "5G NSA COTS UE" selected and expanded to show its sub-sections: "Introduction", "Network & Hardware Overview", "Dependencies", "Configuration", "Connecting to the Network", and "Confirming connection".

5G NSA COTS UE

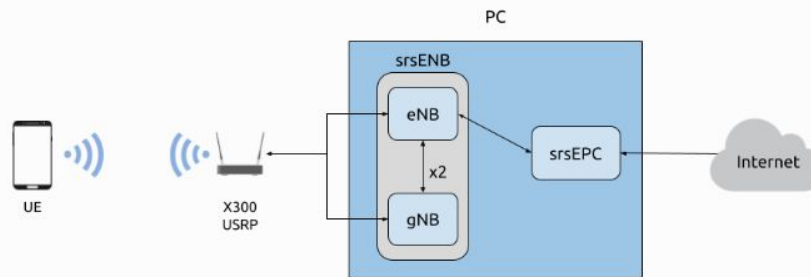
Tip

Operating a private 5G NSA network on cellular frequency bands may be tightly regulated in your jurisdiction. Seek the approval of your telecommunications regulator before doing so.

Introduction

This application note shows how to create your own 5G NSA network using srsENB, srsEPC and a 5G capable COTS UE. There are two options for network setup when connecting a COTS UE: The network can be left as is, and the UE can communicate locally within the network, or the EPC can be connected to the internet through the P-GW, allowing the UE to access the internet for web-browsing, email etc.

Network & Hardware Overview



Simplified network architecture

Setting up a 5G NSA network and connecting a 5G COTS UE requires the following:

- PC with a Linux based OS, with srsRAN installed and built
- A dual channel RF-frontend with independent RF chains
- A 5G NSA-capable UE
- USIM/ SIM card (This must be a test card or a programmable card, with known keys)

21.10 - 5G NSA eNodeB

srsENB

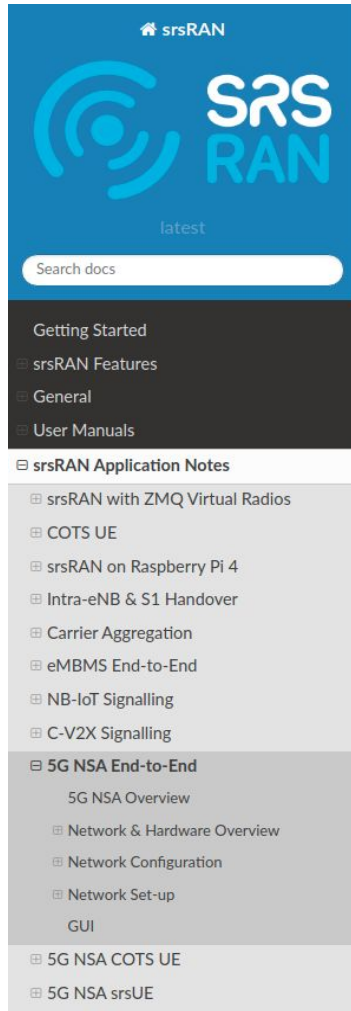
If a successful connection is made, a `RACH` message should be seen followed by a `USER <ID> connected` message where "`<ID>`" is the RNTI assigned to the UE:

```
==== eNodeB started ====
Type <t> to view trace
Setting frequency: DL=806.0 Mhz, UL=847.0 MHz for cc_idx=0 nof_prb=50
Setting frequency: DL=1842.5 Mhz, UL=1747.5 MHz for cc_idx=1 nof_prb=52
User 0x46 connected
RACH: slot=7691, cc=0, preamble=41, offset=1, temp_crnti=0x4602
```

-----DL-----									-----UL-----							
lte	46	12	0	5	2.5k	4	0	0%	25.7	9.4	23	23	17k	4	0	0%
nr	4601	n/a	0	0	0	0	0	0%	n/a	n/a	0	0	38k	4	0	0%
lte	46	13	0	0	0	0	0	0%	n/a	6.2	0	0	0	0	0	0%
nr	4601	n/a	0	0	0	0	0	0%	n/a	n/a	0	0	0	0	0	0%
lte	46	13	0	0	0	0	0	0%	n/a	6.2	0	0	0	0	0	0%

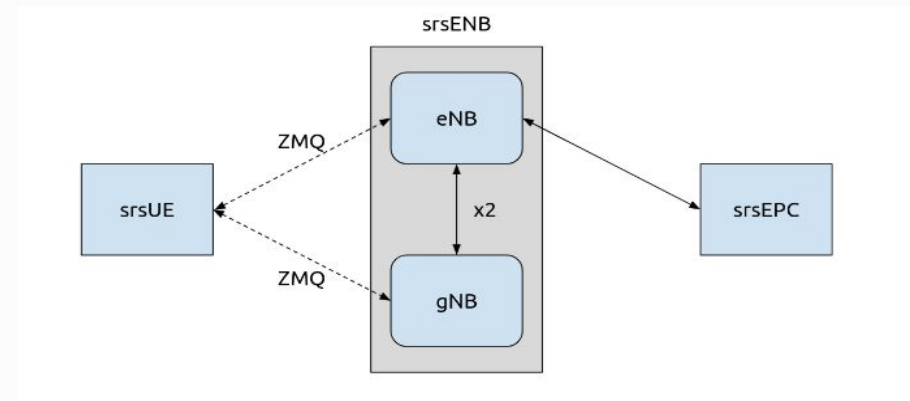
21.10 - End-to-end with virtual radio

21.10 - End-to-end with virtual radio



Network & Hardware Overview

For this application note we will be using [ZeroMQ](#) in place of physical RF hardware. A detailed outline of how to install and use ZMQ with srsRAN can be found [here](#). This app note will assume prior knowledge of use of ZMQ with srsRAN.



Simplified overview of the network architecture

This set up requires the following:

- srsUE running in a separate network namespace
- srsENB configured so that both an LTE eNB, and an NSA gNB cell are created at run time
- srsEPC with the UE included in the list of subscribers

21.10 - CoreScope

21.10 - CoreScope

srsran / corescope Public

<> Code Issues Pull requests Actions Projects **Wiki** Security Insights Settings

Home

Brendan edited this page 27 days ago · 7 revisions



CoreScope Wiki

Welcome to the CoreScope wiki!

CoreScope combines gNodeB and UE components without any radio transmission. It behaves like a UE and exposes an IP interface, but to the core network side, connecting directly to the AMF and UPF via the gNodeB.

The aim of the project is to connect the existing components of the UE and gNodeB, to provide a convenient tool for testing 5G Core setups without the hassle of setting up a RAN infrastructure.

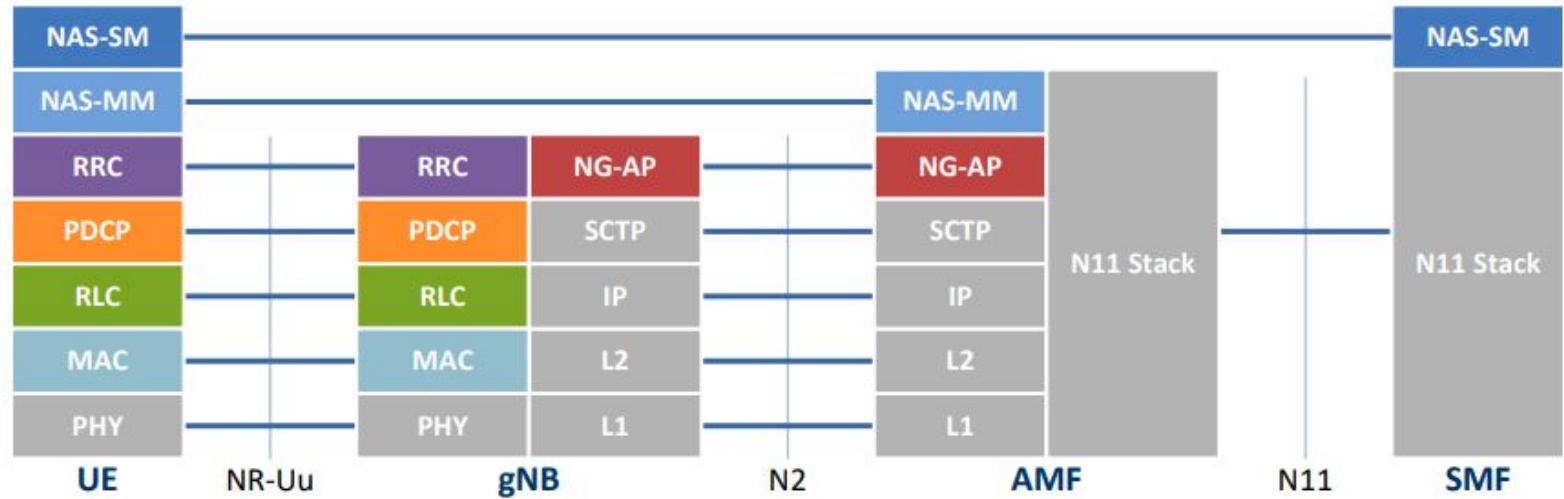
Checkout the following documentation sections to get started with CoreScope:

- Read about how to install CoreScope [here](#)
- See examples of how to configure CoreScope [here](#)
- Supported features can be found [here](#)
- Learn about using CoreScope and its APIs [here](#)

<https://github.com/srsran/corescope/wiki>

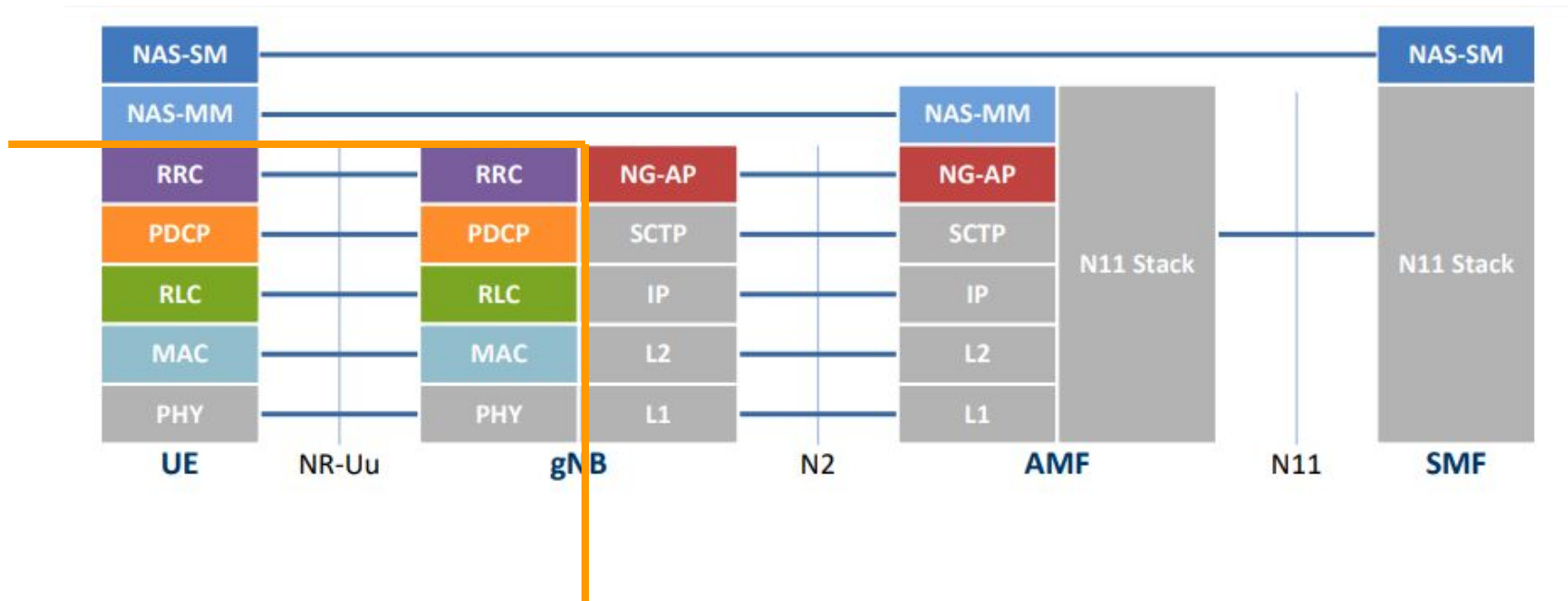
21.10 - CoreScope

Control Plane



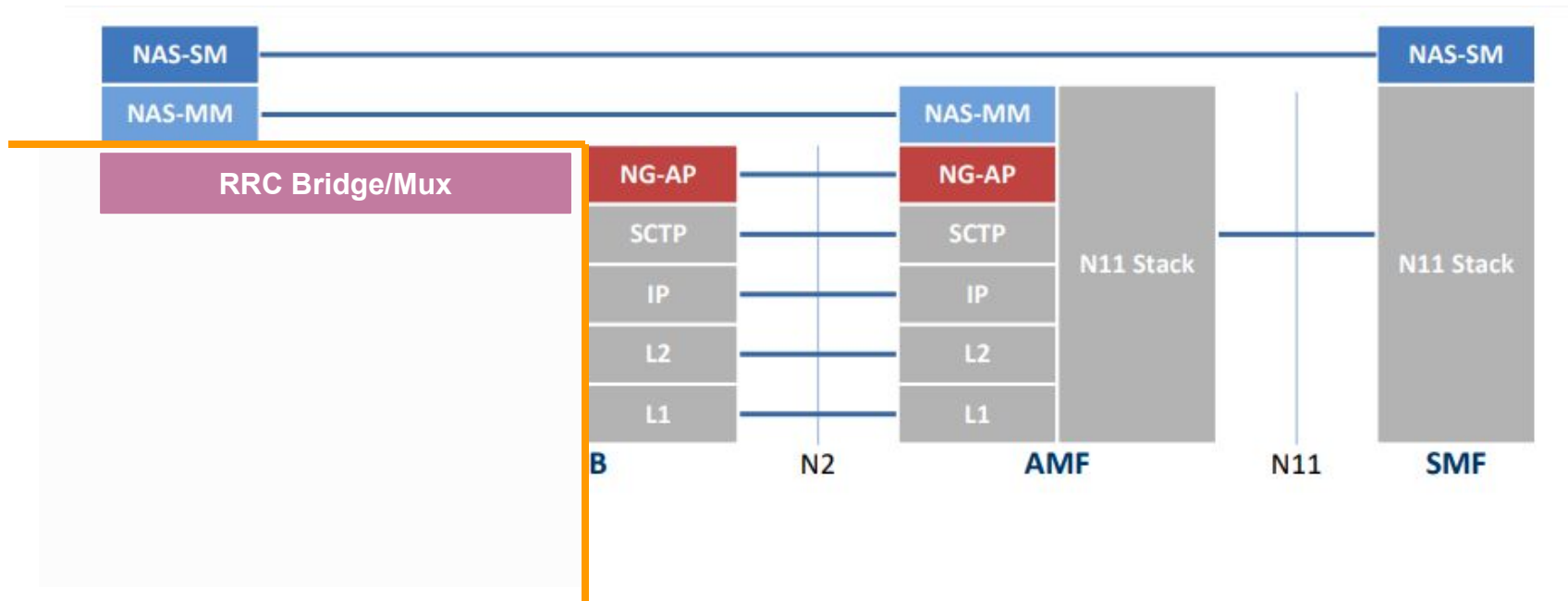
21.10 - CoreScope

Control Plane



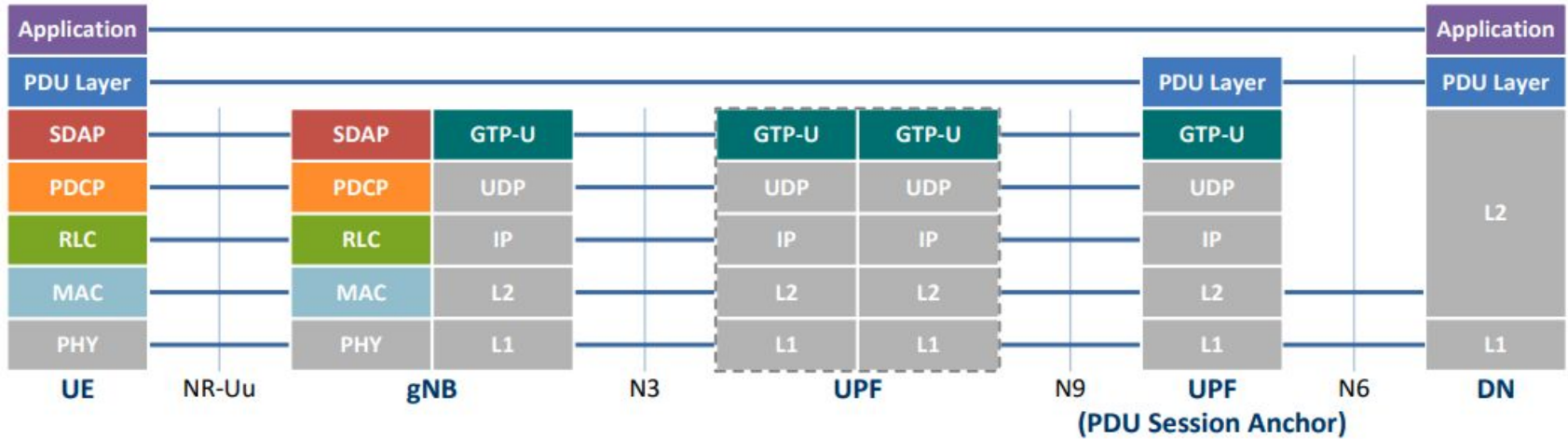
21.10 - CoreScope

Control Plane



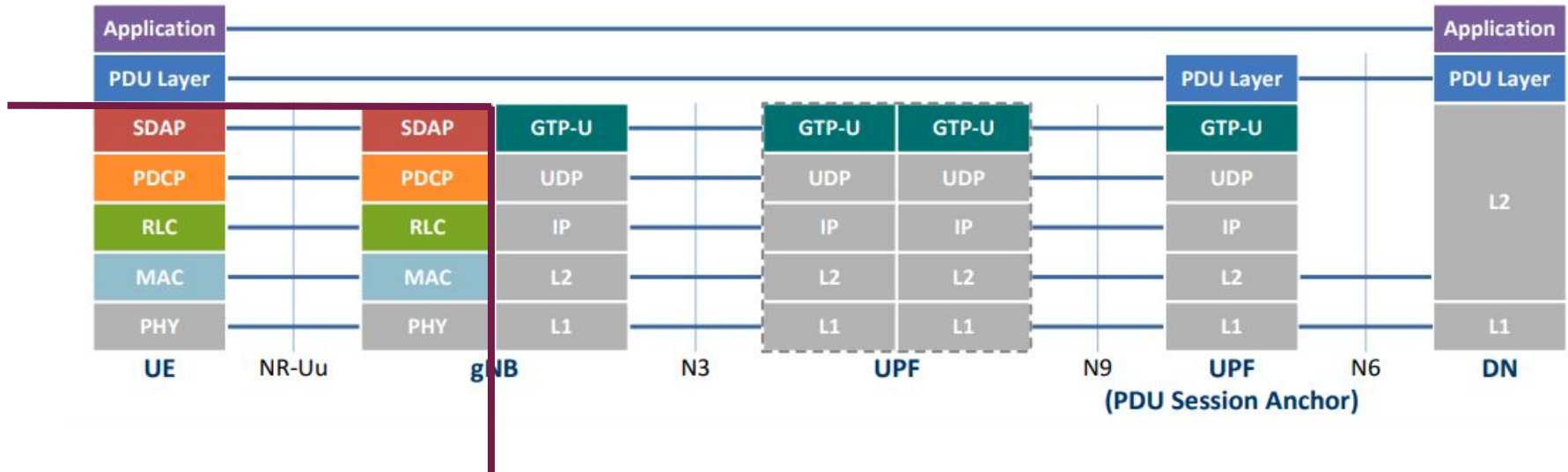
21.10 - CoreScope

User Plane



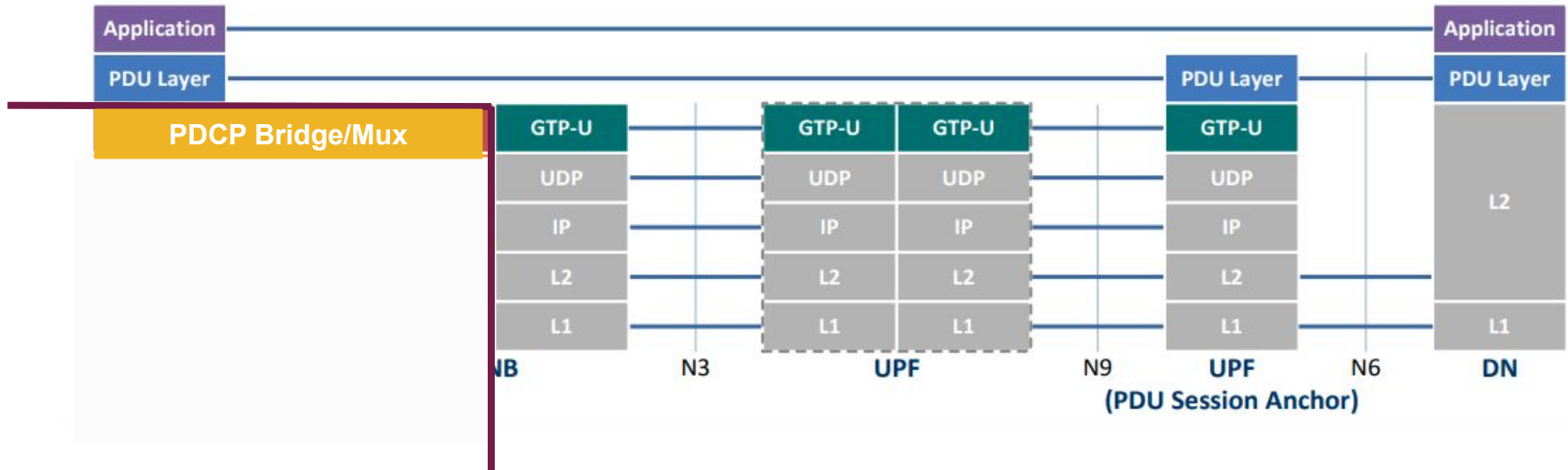
21.10 - CoreScope

User Plane



21.10 - CoreScope

User Plane



21.10 - CoreScope

Swagger Supported by SMARTBEAR /api-docs/oas-3.0.0.json Explore

CoreScope API 0.1 OAS3

/api-docs/oas-3.0.0.json

CoreScope API for Mobile Core Network Testing

CoreScope Team (corescope@srs.io) - Website

AGPLv3

Servers

http://localhost:8000 - Server on localhost

default

GET /corescope/api/gnb/{gnbId}/status Get gNodeB status by gnbID

GET /corescope/api/gnb/{gnbId}/config Get gNodeB current configuration by gnbID

POST /corescope/api/gnb/{gnbId}/ue Create a UE at a gNodeB.

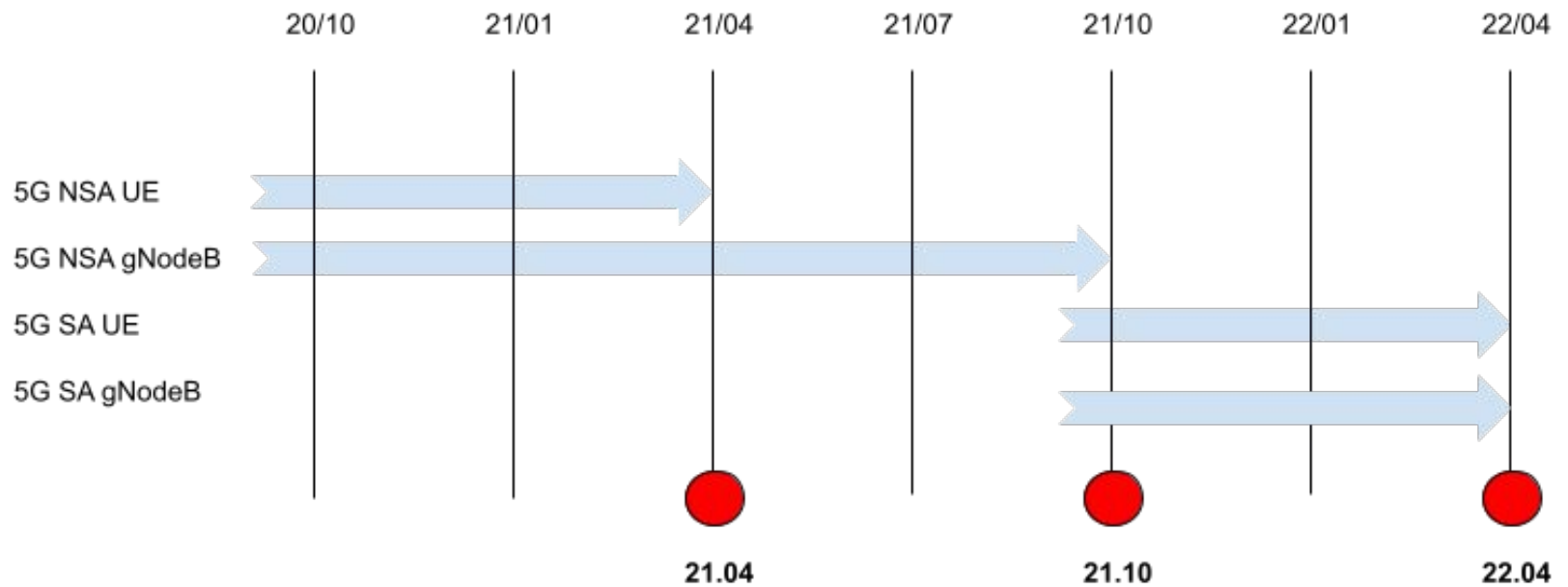
GET /corescope/api/gnb/{gnbId}/ue/{ueId} Gets the current UE configuration

GET /corescope/api/gnb/{gnbId}/ue/{ueId}/status Gets the current UE status

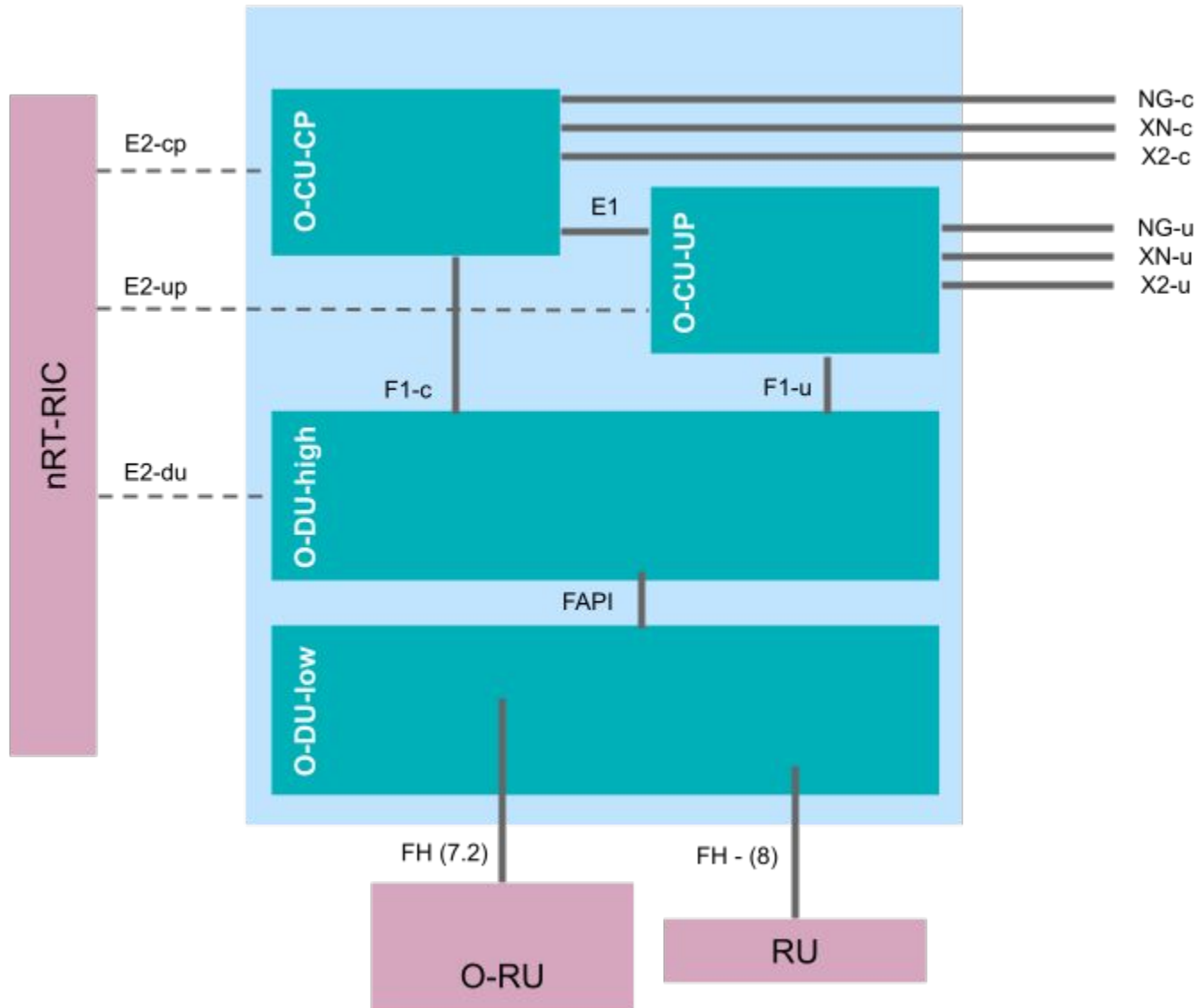
PUT /corescope/api/gnb/{gnbId}/ue/{ueId}/status Update UE Status

The Road Ahead

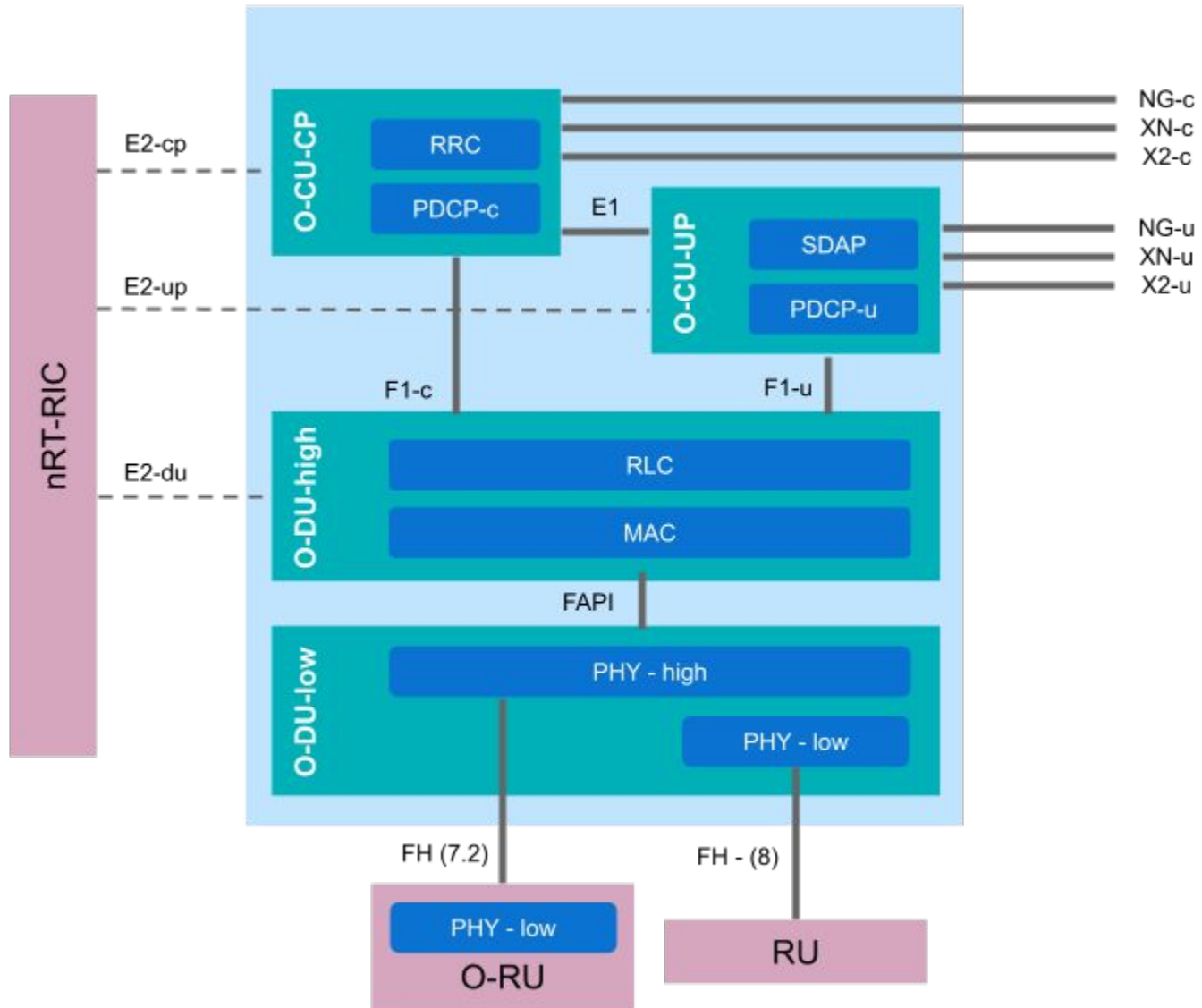
The Road Ahead



The Road Ahead



The Road Ahead



Thank you

info@srs.io