MobSys Lab 1: **LTE and 5G-SA Advanced**

Navid Nikaein, Alireza Mohammadi, Chieh-Chun Chen, and Zaineb Benamar

2023-2024

Important Note

While copying text from the PDF, please make sure you respect the spacings. The spaces are not copyable from the PDF, so you should type them manually. For ease of use, a copy of all the code snippets is provided separately in the `code.sh` file.

After one week, a sample file for Wireshark PCAPs would be uploaded to Moodle. Students who cannot finish the lab on time, could use this PCAP to answer the questions at the end of the lab to at least get the grades for the questions.

1 Prerequisites

First, login again to your user account by running the following command:

```
$ gcloud auth login
```

This command will open a browser window and ask you to login to your Google account. If the browser did not open automatically, you can copy the URL from the terminal and paste it in your browser. After logging in, you will be asked to grant access to the Google Cloud SDK.

Now you need to retrieve the credentials for the GKE cluster of your group. To do so, run the following command:

```
$ gcloud container clusters get-credentials ors-cluster{group-id} \
    --region europe-west6 --project comsyslab
```

You should replace the `{group-id}` with your group number.

Now you should be able to use the CLI to interact with the platform. To test it out run the following command:

```
$ cli extract infra
```

In the result you should see a brief description of the infrastructure of the whole cluster, including the different nodes, their properties, and the associated radio components. This time you should see only two nodes.

2 Background

For doing this lab you need to be familiar with the following three concepts:

1. Absolute Radio Frequency Channel Number (ARFCN)
2. TDD Pattern
3. Radio Bearers and Logical Channels

2.1 Absolute Radio Frequency Channel Number (ARFCN)

ARFCN is a term commonly used in mobile communication systems to uniquely identify a specific carrier frequency or within a frequency band. It is important for frequency planning, channel allocation, and communication between mobile devices and base stations. Term ARFCN started from the GSM and evolved with the new technologies like UARFCN for UMTS/WCDMA, named EARFCN for E-UTRA/LTE and now renamed as NR-ARFCN for 5G/NR.

ARFCNs are like numbered parking spots. The center frequency of a carrier is like the parking lot, and the frequency grid spacing is the distance between spots. In the context of Frequency Division Duplexing (FDD), distinct ARFCN values are allocated for the downlink and uplink directions due to their differing frequencies. Equivalently, the offset with respect to the downlink ARFCN could be used to identify the uplink ARFCN. By default, the UL ARFCN is exactly lower than the DL ARFCN by the value of the bandwidth. However, in the Time Division Duplexing (TDD) system, a singular ARFCN value is sufficient as the downlink and uplink frequencies coincide.

To convert the ARFCN and frequency values in MHz to each other, the equations 1 and 2 are used, where N is the ARFCN value, f is the frequency in MHz, f_{off} is the frequency offset in MHz, N_{off} is the ARFCN offset, and Δ is the frequency grid spacing in kHz. The values of f_{off}, N_{off}, and Δ depend on the frequency range as given in the table 1.

$$f = f_{\text{off}} + \Delta(N - N_{\text{off}}) \tag{1}$$

$$N = N_{\text{off}} + \frac{f - f_{\text{off}}}{\Delta} \tag{2}$$

Frequency range	Δ	f_{off}	N_{off}	Range of N
0 – 3000 MHz	5 kHz	0 MHz	0	0 – 599999
3000 – 24250 MHz	15 kHz	3000 MHz	600000	600000 – 2016666
24250 – 100000 MHz	60 kHz	24250 MHz	2016667	2016667 – 3279167

Table 1: ARFCN offsets and constants for different frequency ranges.

Important Note

While choosing the frequencies for the next lab exercises, you have to make sure that the chosen frequencies are divisible by the frequency grid spacing Δ and the subcarrier spacing used.

2.2 TDD and TDD Pattern

In modern wireless communication systems like 5G, the efficient utilization of available resources is essential to ensure reliable and high-speed data transmission. One key aspect of achieving this efficiency is the concept of Time Division Duplexing (TDD). TDD is a fundamental technique that enables simultaneous uplink (UL) and downlink (DL) communication on the same frequency band, albeit at different time intervals. This method plays a crucial role in optimizing the capacity and performance of 5G networks.

TDD offers several advantages in 5G networks:

- **Full-Duplex Potential**: While it's challenging for a single radio to simultaneously transmit and receive on the same frequency, TDD overcomes this challenge by allocating separate time slots for transmission and reception.
- **Flexibility**: TDD's dynamic adaptation allows network operators to optimize resource allocation based on varying demands This flexibility is crucial for meeting diverse application requirements.
- **Efficiency**: By efficiently utilizing the same frequency band for both UL and DL communication, TDD optimizes the overall network capacity and data rates.

LTE uses a set of fixed TDD patterns, defined by the 3GPP standard, while NR provides a flexible way of configuring the DL and UL resources. The parameters used to define a custom TDD configuration are:

1. DL-UL transmission periodicity in milliseconds (ms).
2. Reference subcarrier spacing to calculate the number of slots in the DL-UL pattern.
3. Number of consecutive full DL slots at the beginning of each DL-UL pattern.
4. Number of consecutive DL symbols in the beginning of the slot following the last full DL slot.
5. Number of consecutive full UL slots at the end of each DL-UL pattern.
6. Number of consecutive UL symbols in the end of the slot preceding the first full UL slot.
7. Number of guard period (GP) symbols.

GP is the time between Downlink and Uplink transmission. Its purpose is to avoid interference within a cell and ensure coexistence among cells by compensating for propagation delays. GP is not required between Uplink and Downlink, as there is less chance of collision because of the base station timing advance feature. Figure 1 is an example of the resulting TDD DL-UL pattern based on these parameters. This DL-UL pattern repeats itself in the timeline.

Let us do the calculations for the example in figure 1. First of all, the periodicity of the TDD pattern is noticeable as 5 ms. The values that could be used for the periodicity according to the standard are 0.5, 0.625, 1, 1.25, 2.5, 5, and 10 ms. This means each pattern is defined within a frame (10ms) and the number of times the pattern is repeated within a frame is given in the table 2.

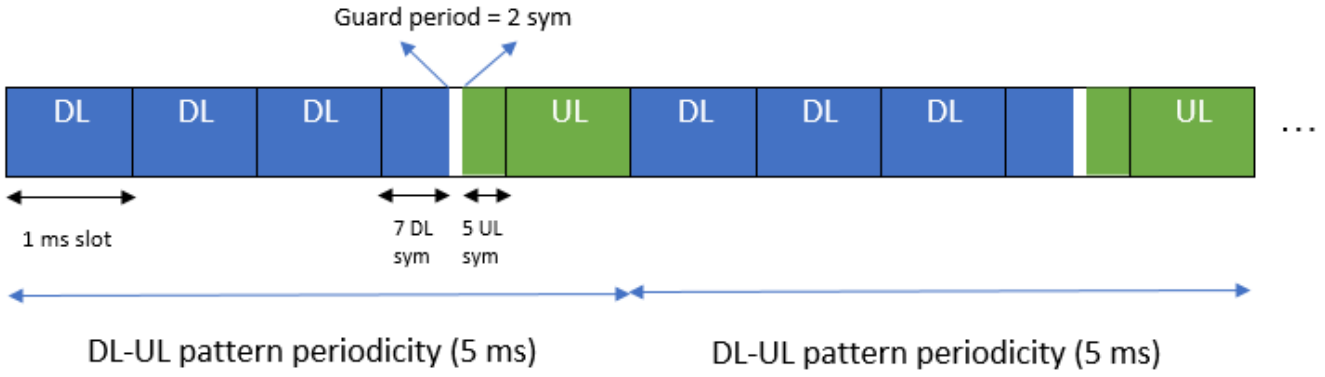

Figure 1: Example of a TDD DL-UL pattern.

Periodicity (ms)	Number of patterns per frame
0.5	20
0.625	16
1	10
1.25	8
2.5	4
5	2
10	1

Table 2: Number of patterns per frame for different periodicities.

Now we need to calculate the slot duration to figure out how many slots could fit in the time period defined by the pattern. The slot duration depends on the reference subcarrier spacing which has a value of 15 kHz in the example of the figure 1. To properly calculate the slot duration, we first define an intermediate variable called the numerology μ. The numerology μ of the system is defined by the logarithm of the ratio of subcarrier spacing in kHz as over 15kHz. Table 3 shows the numerology values for different subcarrier spacings. LTE only supports the numerology value of zero.

So in our example of the figure 1, the slot duration is 1ms and hence the number of slots in the pattern of 5ms is 5. From this 5 slots, 3 are used for DL, 1 for UL, and 1 for the flexible DL/UL. In the flexible DL/UL slot, the number of DL symbols is 7 and the number of UL symbols is 5 with 2 guard symbols. The total number of symbols in each slot is 14, unless you use the extended Cyclic Prefix (CP), only applicable for the SCS of 60kHz, which has 12 symbols per slot.

The guard symbols are needed because of the signal propagation. The DL signal takes some time to reach (propagate to) UE, hence we need some additional time from the end of DL signal. Otherwise, the UE may transmit UL signal before it completes the reception of DL signals and as a result there would be interference between DL and UL signal. The guard period is not needed for UL to DL because DL and UL are always properly aligned thanks to timing advance where the gNB sends timing advance to make UL signal perfectly aligned in time domain. The suggested GPs for the different cell

Subcarrier spacing (kHz)	SCS divided by 15kHz	Numerology (μ)	Slot duration	Slots per frame
15	1	0	1 ms	10
30	2	1	0.5 ms	20
60	4	2	0.25 ms	40
120	8	3	125 μs	80
240	16	4	62.5 μs	160
480	32	5	31.25 μs	320
960	64	6	15.625 μs	640

Table 3: Numerology values for different subcarrier spacings.

sizes (propagation delays) are as the table 4:

Cell size (km)	Guard Period (GP)
< 10.7	2 symbols
10.7 - 21.4	4 symbols
21.4 - 32.1	6 symbols

Table 4: Guard Period (GP) for different cell sizes.

For other examples of the TDD pattern, checkout this link:
https://www.sharetechnote.com/html/5G/5G_FrameStructure.html

2.3 Radio Bearers and Logical Channels

In the protocol stack of the RAN, at each layer, we use different terms to indicate how the data is treated. Table 5 shows the terms.

Layer	Term
PDCP	Radio Bearer (RB)
RLC	Logical Channel (LC)
MAC	Transport Channel
PHY	Physical Channel

Table 5: Terms used at different layers of the RAN protocol stack.

We have two types of radio bearers:

- **Signaling Radio Bearer (SRB)**: SRBs are used for the transmission of RRC messages.
- **Data Radio Bearer (DRB)**: DRBs are used for the transmission of user data.

There are four types of SRBs in 5G-NR:

- SRB0: Maps to CCCH LC and is used for the transmission of RRC messages.
- SRB1: Maps to DCCH LC (ID 1) and is used for the transmission of RRC messages with NAS piggybacked data perhaps.
- SRB2: Maps to DCCH LC (ID 2) and is used for the transmission NAS messages, it has lower priority than SRB1 and maybe configured after the AS security is established.
- SRB3: Maps to DCCH LC (ID 3) and is used when the UE is in NSA mode.

The table 6 shows the mapping of the signaling messages to the SRBs.

Message	**Direction**	**Logical Channel**	**RLC**	**SRB**
MasterInformationBlock	UE <– BS	BCCH	TM	N/A
MeasurementReport	UE –> BS	DCCH	AM	SRB1,SRB3
RRCReestablishment	UE <– BS	DCCH	AM	SRB1
RRCReestablishmentComplete	UE –> BS	DCCH	AM	SRB1
RRCReestablishmentRequest	UE –> BS	CCCH	TM	SRB0
RRCReconfiguration	UE <– BS	DCCH	AM	SRB1, SRB3
RRCReconfigurationComplete	UE –> BS	DCCH	AM	SRB1, SRB3
RRCSetup	UE <– BS	CCCH	TM	SRB0
RRCSetupComplete	UE –> BS	DCCH	AM	SRB1
RRCSetupRequest	UE –> BS	CCCH	TM	SRB0
SecurityModeCommand	UE <– BS	DCCH	AM	SRB1
SecurityModeComplete	UE –> BS	DCCH	AM	SRB1
SIB1	UE <– BS	BCCH	TM	N/A
SystemInformation	UE <– BS	BCCH	TM	N/A
UEAssistanceInformation	UE –> BS	DCCH	AM	SRB1
UECapabilityEnquiry	UE <– BS	DCCH	AM	SRB1
UECapabilityInformation	UE –> BS	DCCH	AM	SRB1
ULInformationTransfer	UE –> BS	DCCH	AM	SRB1, SRB2

Table 6: Mapping of the signaling messages to the SRBs.

At the RRC layer, we have the following logical channels:

- Common Control Channel (CCCH) and Dedicated Control Channel (DCCH) are used to transfer RRC signaling messages, used both in uplink and downlink.
- Dedicated Traffic Channel (DTCH) is used to transfer application data, used both in uplink and downlink.

- Broadcast Control Channel (BCCH) is used to transfer both the Master Information Block (MIB) and System Information Blocks (SIB). MIB is mapped to BCH and PBCH; SIBs are mapped to DL-SCH and PDSCH (downlink only).
- Paging Control Channel (PCCH) is used to transfer paging messages from the network to the UE (downlink only).

Figures 2 and 3 from https://www.nrexplained.com/chmap show these channels and how they are mapped to the transport channels and physical channels in the uplink and downlink directions.

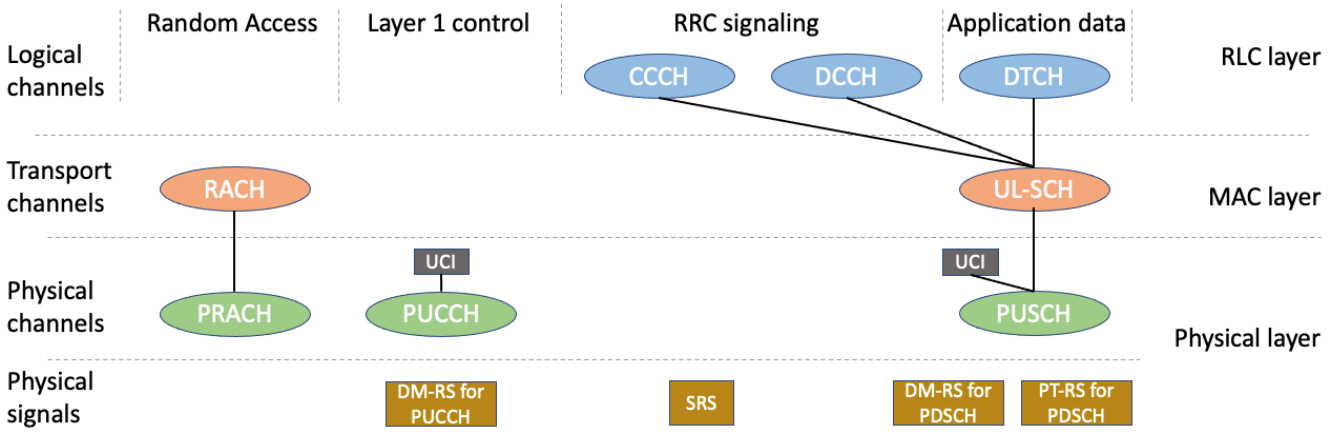

Figure 2: Logical channels in the uplink direction.

- CCCH, DCCCH, DTCH all map to UL-SCH and PUSCH.
- Physical Uplink Control Channel (PUCCH) transfers Uplink Control Information (UCI), including Scheduling Requests, HARQ Acknowledgements and Channel State Information (CSI). It is not used to transfer higher layer information.
- Random Access Channel (RACH) is used to transfer the index of the preamble sequence.
- Demodulation Reference Signals (DM-RS) are sequences which are known to the base station. They are needed for base station to estimate the channel properties for PUCCH and PUSCH.
- Sounding Reference Signal (SRS) is used by the base station for channel-aware packet scheduling and link adaptation.
- Phase Tracking Reference Signal (PT-RS) is used to compensate for phase noise generated by the local oscillators at both the transmitter and receiver.
- CCCH, DCCCH, DTCH all map to DL-SCH and PDSCH.
- Physical Downlink Control Channel (PDCCH) transfers Downlink Control Information (DCI), which is used by the base station to allocate uplink and downlink resources. DCI can also be used to provide uplink power control commands, config slot format, and indicate that pre-emption has occured. It is not used to transfer higher layer information.

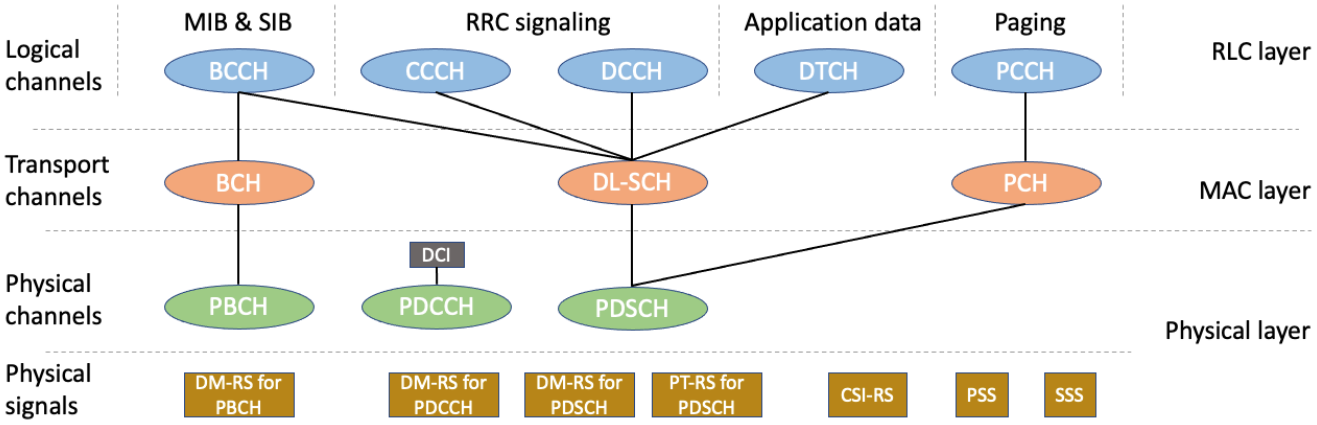

Figure 3: Logical channels in the downlink direction.

- Demodulation Reference Signals (DM-RS) are sequences which are known to the UE. They are needed for UE to estimate the channel properties for PBCH, PDCCH, and PDSCH.
- Phase Tracking Reference Signal (PT-RS) is used to compensate for phase noise generated by the local oscillators at both the transmitter and receiver.
- Channel State Information Reference Signal (CSI-RS) is used by the UE to measure and report channel quality. This information can be used by the link adaptation algorithm at the Base Station. It can also be used for beam management and connected mode mobility procedures.
- Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS) are used during the cell search procedure and beam management procedure. SSS is used for Reference Signal Received Power (RSRP) and Reference Signal Received Quality (RSRQ) measurements.

3 LTE Guided Lab

In this experiment, we deploy a simple 4G LTE network using Software Radio Systems (SRS) [1] LTE Zero-MQ (ZMQ) simulator.

Note

In this lab, we do not have a T-Tracer to pause the RAN execution, hence to capture all the packets, you need to open the Wireshark immediately after the core network (EPC) is ready.

To prepare Wireshark environment, before the installation of the network, in a separate terminal, run the following commands. Like before the ports 5687 and 5847 are temporary ports used by the SRS LTE for dumping the MAC layer packets.

[1] https://docs.srsran.com/projects/4g/en/latest/

```
$ udp_ports="2123 or 2152 or 5687 or 5847"
$ sctp_ports="38412 or 38472 or 36421 or 36412"
$ filter="(sctp port $sctp_ports) or (udp port $udp_ports)"
```

Note

Use the file called `simple-lte.yaml` for this lab. The lab assistants would guide you through the file and the deployment steps.

You need to open the file and replace the PLMN for both the network and the UE to have MCC `001` and MNC of your group number with leading zeros if needed (two digits). Remember to perform the same operation for both the `Network` and the `Terminal` sections (IMSI).

Note

If at any point the deployment fails, refer to the subsection 3.2, for removing the deployment, before trying from the beginning.

3.1 Deployment and PCAP

Use the command `cli install network simple-lte.yaml` to deploy the network. It should finish without errors and printout the two Kubernetes resource names that were created. Check for the status of the deployment using the command `cli observe`.

Right after the EPC is ready, open the Wireshark and start capturing the packets. To do so, run the following command:

```
$ cli extract pcap srs-enb.srs-lte.eurecom -- "$filter" | wireshark -k -i -
```

Then wait until all the **Elements** including the UE are in the `STATUS` set to `1/1 Y` state.

Questions

1. Explain the role of each of the **Elements** in the deployment.
2. Record the output of the observe by taking a screenshot and add it to your report.

Note

The deployment should reach the mentioned state in less than 3 minutes. If it is taking longer, please ask for help.

To verify the E2E connection, let us check the EPC and eNB logs. To do so, run the following command:

```
$ cli extract logs {element}
```

You could use the `Tab` key to complete the name of the element.

Questions

1. Explain what is each of the ports used for in 4G/5G interfaces and show the protocol stack.
2. Investigate if there is any user traffic in the PCAP already and if any the type of the traffic (after the UE readiness).
3. Generate some TCP DL traffic and measure the throughput via the `--plot` option.
4. Explain the differences between the cell configuration of this lab and the previous lab.

3.2 Uninstall

To uninstall the network, use the following command:

```
$ cli remove network simple-lte.yaml
```

Checking via the `cli observe` command, you should see that all the elements are removed.

3.3 Questions

For the questions below, when applicable, verify the results both from the PCAP. If one piece of information is present in multiple messages, please specify all of them and explain the differences.

1. What are the IP addresses of eNB and MME? What is the port number of S1-MME?
2. What PLMN does the cell broadcast?
3. How many UEs are connected to the network?
4. What are the RNTIs of the connected UEs? What are their IMSIs and PLMNs? How do they signal their selected PLMN Identity?
5. Which logical channels are used during the RACH and RRC connection setup?
6. Map the RRC connection messages to the logical channels and RLC mode.
7. At what message number is the UE connected to the eNB and can start transmitting data?
8. At what message number does the UE have a data connection to the core network and internet?
9. Draw the message sequence chart and show the messages and their associated network entity (i.e. UE, eNB, MME)?

4 5G Data Plane

The second experiment is to deploy a simple 5G Standalone (SA) network using OpenAirInterface (OAI) [2] RF Simulator gNB and OAI minimal 5GC, but this time we modify some of the configurations and see the effect on the throughput.

Note

Use the file called `sa-data-plane.yaml` for this lab and modify it accordingly.

4.1 TDD Pattern

Modify the YAML file to run the following two TDD pattern setups given in Table 7. For each of them, calculate the average DL TCP throughput for the duration of 60 seconds.

#	Period	DL Slots	UL Slots	DL Symbols	UL Symbols	Min Rx-Tx Slots
1	5ms	7	2	6	4	6
2	2.5ms	2	2	6	4	4

Table 7: TDD pattern configurations for the lab

Questions

1. Draw a figure to show each of the patterns for the duration of one frame.
2. On your figure, specify how the value of the min Rx-Tx slots is calculated.
3. Calculate the total number of symbols in DL and UL per second for each of the patterns.
4. Calculate the ratio of the DL symbols to the UL symbols for each of the patterns.
5. Calculate the DL throughput as megabits per symbol for each of the patterns and justify why the values should be close to each other.

4.2 ARFCN

Consider the following two cells with the following configuration given in the table 8. The first cell is an *imaginary* neighboring cell to the second cell that we are designing.

Deploy a modified version of the `simple-sa.yaml` file that contains the configuration as cell 2 ONLY (no need to create the first cell). Then measure the DL TCP throughput for the duration of 60 seconds for one of the UEs.

[2] https://openairinterface.org/

#	Band	ARFCN	Bandwidth
1	n78	640000	40MHz
2	n48	642000	40MHz

Table 8: ARFCN configurations for the lab

Questions

1. Draw these two cells on a frequency axis. Mark the frequencies in MHz on the axis and show each cell with an interval.
2. Calculate the center frequency of each cell in MHz.
3. How much of the bandwidth in percentage is overlapping between these two cells, causing interference?

To solve the interference problem, we could take two approaches:

1. Decrease the bandwidth of the second cell to avoid the overlapping.
2. Change the center frequency of the second cell to avoid the overlapping.

First go with the first approach and use a 20MHz bandwidth for the second cell. Then measure the DL TCP throughput again for the duration of 60 seconds for one of the UEs.

Questions

1. Draw these two cells on a frequency axis like before.
2. Compare the throughput with the previous one and explain the difference.
3. Considering both cells, would you consider the total throughput has been increased or decreased?

For the second option, consider the following three ARFCN numbers:

- 646000
- 642667
- 643000

From these three numbers, only one of them is a valid configuration. Try all the three numbers and extract the gNB logs to see if the gNB is able to start or not. If you managed to connect the UE, measure the DL TCP throughput for the duration of 60 seconds for one of the UEs.

Questions

1. Calculate the center frequency of each option in MHz.
2. Draw these two cells on a frequency axis like before for each of the options.
3. Compare the throughput with the previous ones and explain the differences.

4.3 Multiple UEs

Note

In this exercise, you would modify a network configuration. For this we suggest you to keep two separate files, `stage-1.yaml` and `stage-2.yaml`.

Create the `stage-1.yaml` file from the `simple-sa.yaml` file by removing the second UE and disabling the t-tracer. Move the second UE configuration to the `stage-2.yaml` file for later use. Deploy the simple 5G-SA network from the `stage-1.yaml` file. Wait for the UE to be ready and then start a TCP DL throughput test for the duration of 180 seconds by running the following command in a separate terminal window.

```
$ cli test throughput ue1 dl --plot -- gateway --time 180
```

Open a separate terminal window and roughly after 30 seconds, install the `stage-2.yaml` file WITHOUT uninstalling the network or stopping the first test. After another 30 seconds, in the second terminal, run a TCP DL throughput test for the second UE for the duration of 30 seconds.

Finally, after another 30 seconds, uninstall the `stage-2.yaml` file first WITHOUT stopping the first test. Let the first test to finish as well and then take a screenshot of the two plots. Uninstall the `stage-1.yaml` file too.

Questions

1. Explain the pattern seen in the plot for the first UE.
2. Why adding the second UE has caused the throughput of the first UE to drop, even without any traffic for the second UE?