ifiyemi leigha

ISEP

PARIS, FRANCE

December 23, 2023

**Part-1: Deployment of a 5G mobile network LAB Report**

[Document subtitle]

**Part-1: Deployment of a 5G mobile network**

**Environment Setup (~30 minutes)**

**Install Docker Engine**

Use the official documentation to install docker engine: <https://docs.docker.com/engine/install/>

A screenshot of a computer

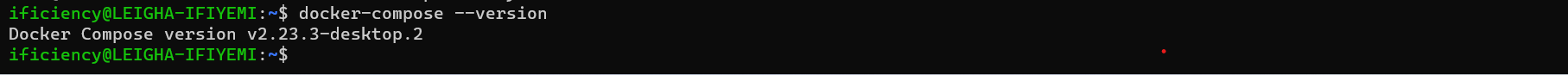
Description automatically generated

**Install Docker Compose**

Use the official documentation to install docker compose: <https://docs.docker.com/compose/install/>

A computer screen with white text

Description automatically generated



A screenshot of a computer

Description automatically generated

**Install free5gc/gtp5g kernel module**

Follow the installation instructions provided here: <https://github.com/free5gc/gtp5g>

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A black screen with a black background

Description automatically generated

**Configuration (~60 minutes)**

**Get free5gc-compose**

A screen shot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

**Explore the configuration**

1. What is the configured Public Land Mobile Network (PLMN) ID ?

A computer screen shot of a black screen

Description automatically generated

Based on the output above from the **nssfcfg.yaml** file, the configured Public Land Mobile Network (PLMN) ID in the Free5GC deployment is identified by the Mobile Country Code (MCC) and Mobile Network Code (MNC). From the configuration, the PLMN ID can be determined as follows:

* **MCC (Mobile Country Code):** **208**
* **MNC (Mobile Network Code):** **93**

Therefore, the PLMN ID for your setup is **20893**.

This PLMN ID is essential for various network functions and configurations in the 5G core network. It's used to uniquely identify the mobile network and is critical for routing and management of subscriber sessions and data.

The configuration file also details other important network settings, such as supported S-NSSAIs (Single Network Slice Selection Assistance Information) for the PLMN, indicating the network's capability to handle different types of 5G network slices and services. This includes various combinations of SST (Slice/Service Type) and SD (Slice Differentiator) for the specified PLMN.

1. What are the configured 5G slices?

In the provided configuration output from the **nssfcfg.yaml** file, the 5G slices are defined under the section **supportedNssaiInPlmnList**, particularly within the **supportedSnssaiList**. These slices are specified using a combination of SST (Slice/Service Type) and SD (Slice Differentiator).

Based on your output, here are the configured 5G slices:

1. **Slice 1:**
   * SST: **1**
   * SD: **010203** This slice represents a service type with SST=1 and a unique identifier (Slice Differentiator) of **010203**.
2. **Slice 2:**
   * SST: **1**
   * SD: **112233** This slice also has an SST=1 but with a different Slice Differentiator, **112233**.
3. **Slice 3:**
   * SST: **1**
   * SD: **000003** Similar to the first two, this slice has SST=1 but with SD=**000003**.
4. **Slice 4:**
   * SST: **2**
   * SD: **000001** This slice indicates a different service type (SST=2) with Slice Differentiator **000001**.
5. **Slice 5:**
   * SST: **2**
   * SD: **000002** Another slice with SST=2, but with a unique SD of **000002**.

Each combination of SST and SD defines a specific network slice. In 5G networks, network slicing is a fundamental feature that allows the creation of multiple virtual networks atop a shared physical infrastructure. Each slice can be optimized for specific types of services or customers, like enhanced mobile broadband (eMBB), ultra-reliable low latency communications (URLLC), or massive machine type communications (mMTC).

The configuration shows a setup that supports multiple slices, with two different service types (SST=1 and SST=2) and various slice differentiators, allowing for diverse service requirements and use cases.

1. What are the integrity algorithms used by the Access and Mobility management Function ?

OUTPUT

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

From the **amfcfg.yaml** file content you provided, we can identify the integrity algorithms configured for use by the Access and Mobility management Function (AMF) in your Free5GC deployment. The relevant section in your configuration is under the **security** subsection:

security: # NAS security parameters

integrityOrder: # the priority of integrity algorithms

- NIA2

# - NIA0

cipheringOrder: # the priority of ciphering algorithms

- NEA0

# - NEA2

The **integrityOrder** section lists the integrity algorithms in the order of their priority. Based on your configuration:

* **NIA2:** This is the primary integrity algorithm configured for use. NIA2 is a standard 5G integrity algorithm known for its robust security features.
* **NIA0:** This algorithm is commented out in your configuration (indicated by the **#** symbol), suggesting that it is not currently in use or is a secondary option. NIA0 typically refers to a null integrity algorithm, meaning no integrity protection.

The integrity algorithm ensures data integrity and authentication between the user equipment (UE) and the core network, particularly for NAS (Non-Access Stratum) signaling. The choice of these algorithms is crucial for maintaining the security and integrity of communications within the 5G network.

1. What are the ciphering algorithms used by the Access and Mobility management Function ?

The ciphering algorithms used by the Access and Mobility Management Function (AMF) in your Free5GC deployment are also specified in the **amfcfg.yaml** file, in the same **security** section where the integrity algorithms are defined. From the content you provided:

security: # NAS security parameters

integrityOrder: # the priority of integrity algorithms

- NIA2

# - NIA0

cipheringOrder: # the priority of ciphering algorithms

- NEA0

# - NEA2

Under the **cipheringOrder** section, the following ciphering algorithms are listed:

1. **NEA0:** This algorithm is currently the primary ciphering algorithm configured for use. NEA0 typically refers to a null encryption algorithm, meaning no encryption is applied. This is often used for testing purposes or in environments where encryption is not deemed necessary.
2. **NEA2:** Similar to NIA0, this algorithm is commented out (indicated by the **#** symbol), suggesting that it is not actively in use or is a secondary option. NEA2 is a standard 5G ciphering algorithm known for its strong security features.

Ciphering algorithms in 5G are used to ensure the confidentiality of user data and signaling between the user equipment (UE) and the network. The choice of these algorithms is important for protecting against eavesdropping and ensuring the privacy of communications within the 5G network.

Given that NEA0 (null encryption) is the primary ciphering algorithm in your configuration, it's important to consider whether this aligns with your security requirements, especially in a production or public-facing environment. For enhanced security, you would typically use an algorithm like NEA1 or NEA2, which provides actual data encryption.

1. What are the supported PLMN IDs by the AUthentication Server Function ?

A screenshot of a computer

Description automatically generated

The supported PLMN IDs by the Authentication Server Function (AUSF) in your Free5GC deployment are listed under the **plmnSupportList** section in the **ausfcfg.yaml** configuration file. Based on the content you provided, here are the supported PLMN IDs:

1. **First PLMN ID:**
   * **MCC (Mobile Country Code):** **208**
   * **MNC (Mobile Network Code):** **93** The complete PLMN ID for this entry is **20893**.
2. **Second PLMN ID:**
   * **MCC (Mobile Country Code):** **123**
   * **MNC (Mobile Network Code):** **45** The complete PLMN ID for this entry is **12345**.

These PLMN IDs define the mobile networks that the AUSF in your 5G setup is configured to support. The AUSF uses these identifiers to authenticate and authorize users of the specified mobile networks. Ensuring the correct configuration of these PLMN IDs is crucial for the proper operation and interoperability of network services within the 5G core network.

1. What is the configured Tracking Area Code for the gNodeB ?

A computer screen shot of a black screen

Description automatically generated

Based on the output you've provided from what appears to be the gNodeB configuration file, the configured Tracking Area Code (TAC) for the gNodeB in your Free5GC deployment is:

* **TAC:** **1**

The TAC is a key parameter used in the management of mobility and paging in cellular networks. It is used to define a specific geographic area within the network, allowing the network to efficiently manage and page devices based on their location.

Your gNodeB configuration also includes other important parameters like the Mobile Country Code (MCC), Mobile Network Code (MNC), NR Cell Identity (NCI), and details of the supported S-NSSAIs, which are critical for the network's operation and for defining the service characteristics of each network slice.

The TAC, along with the MCC and MNC, plays a crucial role in identifying the tracking areas for mobile devices connected to the network and is essential for the proper functioning of the mobility management processes in the network.

1. What are the 5G slices supported by the gNodeB ?  
     
   A computer screen shot of a black screen

   Description automatically generated

The 5G slices supported by the gNodeB in your Free5GC deployment are detailed under the **slices** section in the gNodeB configuration output you provided. Each slice is defined by a combination of SST (Slice/Service Type) and SD (Slice Differentiator).

From your output, here are the configured 5G slices supported by the gNodeB:

1. **Slice Configuration:**
   * **SST (Slice/Service Type):** **0x1** (in hexadecimal format)
   * **SD (Slice Differentiator):** **0x010203** (in hexadecimal format)

This configuration indicates that the gNodeB supports a single 5G slice with an SST of **1** and an SD of **010203**. The SST value specifies the general characteristics of the slice, such as eMBB (enhanced Mobile BroadBand), URLLC (Ultra-Reliable Low Latency Communications), or mMTC (massive Machine Type Communications). The SD value provides a more specific differentiation within the SST, allowing for fine-grained control and customization of the slice.

The concept of network slicing is a key feature of 5G networks, enabling the network to provide tailored connectivity services that meet specific requirements of different applications, services, or user groups. Each slice can be optimized for particular types of traffic or service levels, providing a more efficient and flexible use of network resources.

1. What is the N2 service port of the AMF ?

A computer screen shot of a black screen

Description automatically generated

Based on the content you provided from the **amfcfg.yaml** file, the N2 service port of the AMF (Access and Mobility Management Function) in your Free5GC deployment is identified in the **ngapPort** field. The configuration shows:

* **N2 Service Port (NGAP Port) of the AMF:** **38412**

This port number, **38412**, is used for the NGAP (Next Generation Application Protocol) communications over the N2 interface between the AMF and the gNodeBs in your 5G network. The NGAP protocol is essential for a range of control plane functions, including initial UE (User Equipment) access, mobility management, paging, and more.

It's important to ensure that this port is correctly configured and accessible for the proper functioning of the AMF and its communication with other network elements, particularly the gNodeBs.

1. What is the service port of the Network Repository Function ?  
     
   A computer screen shot of a black screen

   Description automatically generated  
     
     
     
   Based on the content from your **nrfcfg.yaml** file, the service port of the Network Repository Function (NRF) in your Free5GC deployment is specified in the **sbi** section. The configuration shows:

**NRF Service Port:** **8000**

This port (**8000**) is used for the Service-Based Interface (SBI) communications of the NRF. The NRF in a 5G core network plays a crucial role in maintaining information about all network functions, handling their discovery and registration. It allows different network functions to find and communicate with each other, making the correct configuration of this service port essential for the overall functionality and interoperability of the network components.

1. What is the service port of the Policy and Control Function ?  
     
   A computer screen shot of a black screen

   Description automatically generated

Based on the content from your **pcfcfg.yaml** file, the service port of the Policy and Control Function (PCF) in your Free5GC deployment is specified in the **sbi** section. The configuration indicates:

* **PCF Service Port:** **8000**

This port (**8000**) is utilized for the Service-Based Interface (SBI) communications of the PCF. The PCF in a 5G core network is responsible for policy control decision-making, which includes managing policy rules for network behavior, Quality of Service (QoS) control, and controlling the flow of data. The correct configuration of this service port is crucial for the PCF's communication with other network functions and its overall functionality within the network.

1. What are the available Data Network Names ?  
     
   A screenshot of a computer

   Description automatically generated  
     
   Based on the contents of the **smfcfg.yaml** file from your Free5GC deployment, the available Data Network Names (DNNs) are defined under the **snssaiInfos** section, within the **dnnInfos** subsection. Here are the DNNs configured in your setup:

**DNN:** **internet**

This DNN is associated with two different S-NSSAIs (Single Network Slice Selection Assistance Information), both having an SST of **1** but with different Slice Differentiators (**010203** and **112233**). The DNN "internet" is a common identifier used in mobile networks to denote the general-purpose internet service.

Each S-NSSAI paired with a DNN represents a specific type of network slice that can offer different services. In your case, it appears that the same DNN (**internet**) is being used for multiple network slices, which allows users connected to these slices to access internet services.

The DNN is a critical element in the 5G network as it determines the type of data services available to the users and how the user plane data is handled and routed within the network.

1. What are the IP pools for each Data network in each slice ?  
     
   A screenshot of a computer

   Description automatically generated

The **upfcfg.yaml** file you provided contains the IP pool configuration for the Data Network Name (DNN) supported by the UPF (User Plane Function) in your Free5GC deployment. Here are the details:

1. **DNN:** **internet**
   * **CIDR (Classless Inter-Domain Routing) for Assigned IPv4 Pool:** **10.60.0.0/24**

This configuration indicates that for the DNN **internet**, the UPF has an IP pool set with the range **10.60.0.0/24**. This range will be used to assign IPv4 addresses to User Equipment (UEs) connected to this particular data network.

The IP pool's CIDR notation **10.60.0.0/24** specifies that UEs can be assigned any IP address in the range from **10.60.0.1** to **10.60.0.254**, with **10.60.0.0** being the network address and **10.60.0.255** reserved as the broadcast address in this subnet.

Such configurations are crucial for managing user plane data traffic within the network, as they define the specific IP address ranges that can be allocated to UEs accessing the network's services. The UPF, being a key component of the 5G core network's user plane, handles the routing and forwarding of user data based on these IP allocations.

1. What is the Subscription Permanent Identifier of the UE default configuration ?  
     
   A computer screen shot of a black screen

   Description automatically generated

Based on the output you provided from the UE (User Equipment) configuration file, the Subscription Permanent Identifier (SUPI) of the UE in your Free5GC deployment is:

* **SUPI:** **imsi-208930000000001**

This SUPI is composed of the following parts:

* **IMSI:** International Mobile Subscriber Identity
* **MCC:** Mobile Country Code - **208**
* **MNC:** Mobile Network Code - **93**
* **MSIN:** Mobile Subscriber Identification Number - **30000000001**

The SUPI, specifically the IMSI part (**208930000000001**), is a critical identifier used in the 5G network to uniquely identify a subscriber. It is used for various purposes, including authentication, billing, and establishing network sessions.

The configuration also includes other key parameters for the UE, such as the permanent subscription key (**key**), operator code (**op** and **opType**), and Authentication Management Field (**amf**). These parameters are essential for the UE's authentication and secure communication within the 5G network.

1. What are the integrity algorithms supported by the UE ?

A screenshot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

The output from the **uecfg.yaml** configuration file of UERANSIM provides detailed information about the UE (User Equipment) configuration, including the supported integrity and encryption algorithms. Here's a summary and interpretation of the relevant parts:

**Supported Integrity Algorithms**

Under the **integrity** section, the configuration specifies the following algorithms:

* **IA1**: This is set to **true**, indicating support for this integrity algorithm.
* **IA2**: Also set to **true**, showing support.
* **IA3**: Set to **true**, meaning this algorithm is supported as well.

**Supported Encryption Algorithms**

Under the **ciphering** section, the following encryption algorithms are supported:

* **EA1**: Supported (**true**).
* **EA2**: Supported (**true**).
* **EA3**: Supported (**true**).

**Other Relevant Configuration Details**

* **Supi**: The IMSI number of the UE.
* **Key**, **op**, **opType**: These are related to the authentication parameters.
* **Amf**, **imei**, **imeiSv**: Other device-specific identifiers.
* **gnbSearchList**: List of gNB (gNodeB) IP addresses.
* **Sessions**: Initial PDU sessions configuration.
* **Configured NSSAI**: Network Slice Selection Assistance Information.
* **integrityMaxRate**: Maximum data rate for integrity protection in the user plane.

1. What are the ciphering algorithms supported by the UE ?

A screenshot of a computer

Description automatically generated

The ciphering algorithms supported by the UE (User Equipment) in the UERANSIM configuration are detailed in the **ciphering** section of the **uecfg.yaml** file provided. Here's a summary of the supported ciphering algorithms:

1. **EA1**: This is set to **true** in the configuration file, indicating that this encryption algorithm is supported by the UE. EA1 is generally associated with the SNOW 3G stream cipher.
2. **EA2**: Also set to **true**, showing support for this algorithm. EA2 typically refers to AES (Advanced Encryption Standard) in GCM (Galois/Counter Mode).
3. **EA3**: This is also supported (**true**). EA3 usually refers to the ZUC stream cipher.

These algorithms are used for encrypting the user data and signaling data between the UE and the network to ensure data privacy and security.

**Deployment of 5G mobile network (~30 minutes)**

**NFs**

Use the provided docker-compose file to deploy the following components:

* gNB
* NRF
* AMF
* SMF
* PCF
* NSSF
* AUSF
* UDM
* UDR
* UPF

**WebUI**

Connect to the WebUI and verify that your 5GC is up and running.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Attach a UE, capture traffic, and analyze (~60 minutes)**

**UE provisionning**

Provision a UE in the 5G core network using the WebUI.

A screenshot of a computer

Description automatically generated

**Attachment procedure**

Start an attachment procedure of the UE to the gNB and core network.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Analysis**

Capture the application logs and the registration procedure, and analyse the protocols in use