5G Labs

Training Manual

Revision: 2.0
Published: Feb 2025

5G Labs Training Manual

Signaltron reserves all rights to this document and the information contained herein. Products, names, logos and designs described herein may in whole or in part be subjected to intellectual property rights. Reproduction, use, modification, or disclosure to third parties of this document or any part thereof without the express permission of Signaltron is strictly prohibited. The information contained herein is provided “as is” and Signaltron assumes no liability for the use of the information. No warranty, either expressed or implied, is given, including but not limited, with respect to the accuracy, correctness, reliability and fitness for a particular purpose of the information. Signaltron reserves the right, without prior notice or liability, to make changes in equipment design or specifications. This document may be revised by Signaltron at any time. For most recent documents, visit www.signaltron.com.

Information supplied by Signaltron Systems Pvt Ltd. is believed in good faith to be accurate and reliable, while every care has been taken in preparing these documents. However, Signaltron Systems Pvt Ltd. does not make any representations and gives no warranties of whatever nature in respect of these documents, including without limitation, the accuracy or completeness of any information, facts and/or opinions contained therein. No responsibility is assumed by Signaltron Systems Pvt Ltd. for the use of the documents or for the rights of third parties which may be affected in any way by the use thereof. The provision of these documents (and the documents themselves) does not constitute professional advice of any kind. Any representation(s) in these documents concerning performance of Signaltron Systems Pvt Ltd. product(s) are for informational purposes only and are not warranties of future performance, either expressed or implied. Signaltron Systems Pvt Ltd., its affiliates, directors, employees, and agents shall not be held liable for any damages or losses, of any nature whatsoever, arising from any use of and/or reliance on the documents. These documents may contain flaws, omissions, or typesetting errors; no warranty is granted, nor liability assumed in relation thereto. Information contained herein is periodically updated and changes will be incorporated into subsequent editions. If you have encountered an error, please notify Signaltron Systems Pvt Ltd. Product performance figures quoted within this document are indicative and for information purposes only.

Table of Contents

Document Information

This document details procedures for using 5G Network and related equipment provided as part of 5G Labs. This document is intended for qualified personnel with a working knowledge of 5G.

Revision History

Revision Details	Date	Summary of Changes
Rev 1.0	Feb-2025	Original Document

Glossary/Abbreviation

Abbreviation	Description
5G	5th Generation Mobile Communication Technology
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
BSF	BootStrap Function
CPE	Customer Premise Equipment
CPRI	Common Public Radio Interface
DPD	Digital Pre-distortion
DPDK	Data Plane Development Kit
EGW	Edge Gateway
eMBB	Enhanced Mobile Broadband
gNodeB	5g Basestation
GUI	Graphical User Interface
HDMI	High-Definition Multimedia Interface
IoT	Internet Of Things
LED	Light Emitting Diode
MIMO	Multiple-Input Multiple-Output
mMTC	Massive Machine-Type Communication
NF	Network Function
NMS	Network Monitoring System
NR	New Radio
NRF	Network Repository Function
NSSF	Network Slice Selection Function

PCF	Policy Control Function
PFCP	Packet Forwarding Control Protocol
QEC	Quantum Error Correction
QoS	Quality Of Service
RAN	Radio Access Network
RU	Radio Units
SCP	Service Communication Proxy
SMF	Session Management Function
TSP	Telecommunications Service Provider
UDM	Unified Data Management
UDR	User Data Repository
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communication
USB	Universal Serial Bus
VPP	Vector Packet Processor
VR	Virtual Reality

References

1. Ajna XR Head Set User Manual
2. COSGrid IoT Gateway User Manual
3. COSGrid Network Gateway Firewall User Manual
4. Kenstel CPE User Manual
5. Microtek UPS User Manual
6. Niral OS User Manual
7. Niral OS Core Edge Controller User Manual
8. Nivetti 24 Port Switch User Manual
9. Samsung M13 Mobile User Manual
10. Samsung Monitor User Manual
11. Sparsh CCTV Camera User Manual
12. STGNB2215-XX-ID User Manual
13. NMS for gNB user manual
14. 5G Drone User Guide
15. 3GPP Specification 37.324
16. 3GPP Specification 38.331
17. 3GPP Specification 38.323
18. 3GPP Specification 38.322
19. 3GPP specification 38.321
20. 3GPP Specification 29.281
21. 3GPP Specification 38.413
22. 3GPP specification 38.412
23. 3GPP Specification 23.501
24. 3GPP specification 24.501

1. Introduction to 5G Labs

The Department of Telecommunications (DoT) has awarded the establishment of 100 5G Use Case Labs to educational institutions across the country, with the primary objective of nurturing skills and promoting active engagement with 5G technologies among students and start-up communities. These labs will facilitate the development, experimentation of 5G applications in various socioeconomic verticals.

This initiative marks a significant step towards democratizing access to 5G technology by empowering educational institutions and startups to explore its transformative potential. By facilitating hands-on learning and innovation, the program seeks to drive technological advancements and foster a new wave of applications that leverage the capabilities of 5G.

5G use case labs inspire to develop applications which can make meaningful difference in the lives of the people around the globe and develop applications which are specific to India's requirements. This takes us a step closer to aatmanirbharta. The use cases could span across a variety of verticals including education, agriculture, health, power, urban management, mining, logistics, resource management, tourism, sports, security, e-governance etc.

Signaltron is providing the 5G lab infrastructure for some of these labs. gNodeB provided in 5G lab Infrastructure is the Signaltron's Sahyadri series of Radio Access Network Equipment featuring highly integrated, compact and versatile NR Base Stations delivering high capacity to enable ubiquitous connectivity to all. A key part of Sahyadri RAN, the STGNB2215 Base Station is easy to install and gives the flexibility to run all functions of NR (5G) gNodeB in a single enclosure. gNodeB in 5G lab is envisaged and designed to cater for specific requirements of 5G use case lab and provide required infrastructure for providing a fast-learning curve of the cutting-edge technology for the students. Experimenting with the setup will generate interest in areas like embedded system, telecom technology, machine learning, AI applications and robotics.

Signaltron System's STGNB2215 is an indigenously developed 5G base station. On the backhaul side, the gNodeB interfaces directly with the IP network through ethernet and on the air interface side, it connects directly to antenna. The base station showcases Signalchip's SCRF4502, Agumbe chipset, which features high fidelity mixed-signal analog RF and integrated advanced signal processing functions such as DPD, CFR and QEC. SCRF4502 can transmit and receive 5G signals in a wide range of frequencies.

The base station is also integrated with indigenously developed 5G core, IMS, MEC server. This makes the entire 5G network fully indigenous and demonstrates end to end technology capability. 5G gNodeB (base station) is the crucial component of the 5G ecosystem which is responsible for transmitting and receiving wireless signals from various user equipment.

2. 5G Lab Network Setup

a. 5G Lab Overview

Key components of 5G Lab are 5G gNodeB, 5G Core, Firewall, Switch, Edge computing on x86 server, Network Management System, CPE, 5G Camera, IoT Gateway, evaluation board with sensors, Firewall, CPE, 5G phones, 5G Sim Cards.

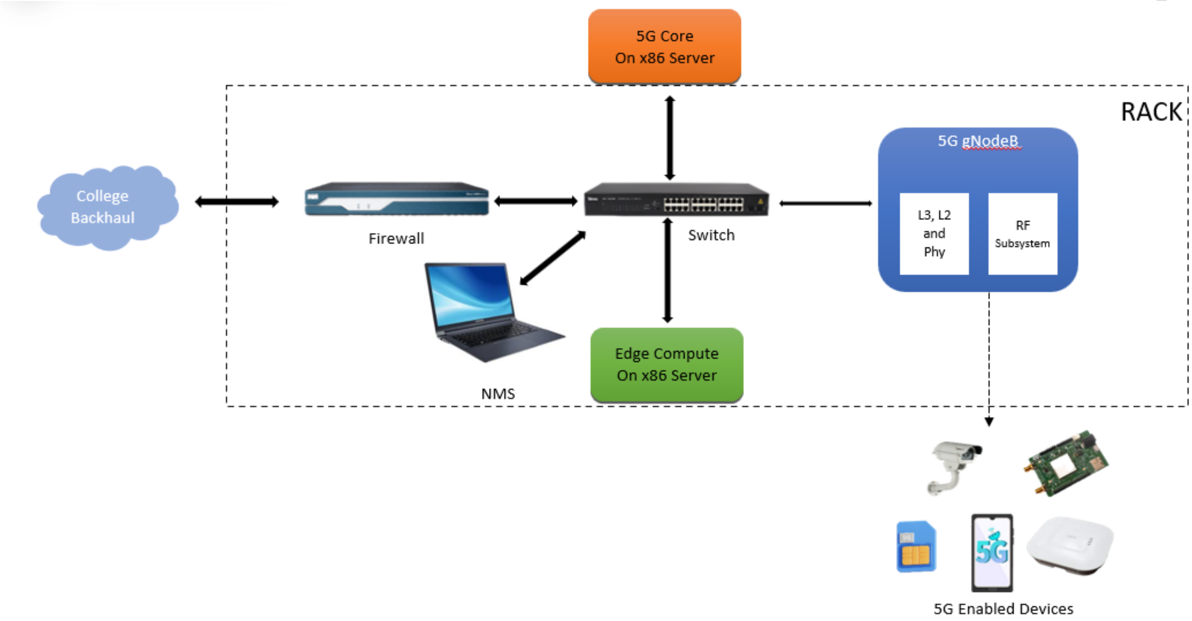


Figure 1 5G Lab Network Diagram

b. Architecture of 5G Lab

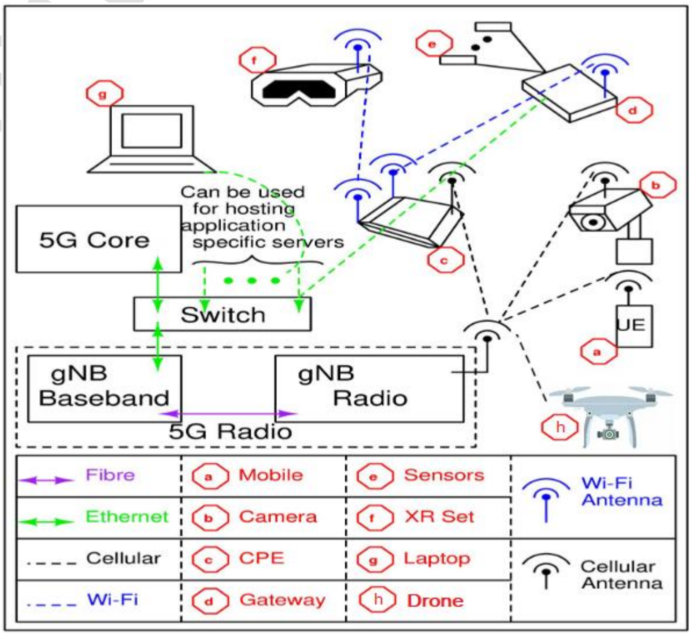


Figure 2 5G Lab architecture

c. Systems in 5G Lab

1. 5G use case labs also contain other equipment that seamlessly integrates with the base station.
2. 5G Radio: 5G radio, also known as 5G New Radio (NR), is a wireless technology that allows devices to connect to the internet at high speeds. It's the global standard for 5G networks.
3. 5G Core, 5G sims, 5G handsets and other network infrastructure: It enables data transfer and internet access services.

4. IoT gateway: With the rise in IoT technology, a lot of applications pertaining to remote farming, rural healthcare and many more can be developed using IoT sensors and can be integrated with 5G network using IoT gateway. Few relevant applications are described below-

   Smart Home Automation/Smart Building/Smart Cities: Solutions can be done to better the traffic monitoring and control, energy-efficient street/building lighting, and connected appliances (smart refrigerators, ovens etc).

   Healthcare and Wearable Technology: Remote health monitoring with wearable technology and smart medical devices like insulin implants help remote doctors check and treat patients.

   Agriculture: IoT systems can enable precision farming, crop monitoring, livestock monitoring, automated irrigation etc. This solution along with data analysis will help farmers to get better yields.

   Along with the above use cases, IoT technology will also make huge differences in automated and connected vehicles, energy management, environmental monitoring etc.
5. **Firewall**: is a Network Security appliance that processes network traffic and is capable of detecting and blocking sophisticated attacks by enforcing security policies. Moving beyond the conventional port/protocol inspection and blocking, COSGrid NGFW employs deep-packet inspection to bolster security measures and offer application-level inspection, intrusion prevention, thereby enhancing overall firewall capabilities.

6. **Switch**: Nivetti's 24 Port GE Base-T + 4 X 1G/10G SFP+ 1 RU Rack Mountable L2+ access Switch is a fully managed enterprise grade switch designed to provide versatile connectivity to spectrum of devices in an enterprise and branch office networks

7. **5G Drone:** Drone technology is revolutionizing the fields of agriculture, delivery systems, surveillance etc. It is also enabling creation of accurate digital twin in massive scales.

8. **5G Indoor CPE:** It acts as a bridge between the 5G network and the user's devices, providing a local Wi-Fi network or wired connections for various devices within the premises. With this, non 5G based applications running on Wi-Fi/ Ethernet can also be integrated and developed.

9. **5G Camera:** With 5G camera and URLLC applications like remote surgery and diagnosis can be developed. This will be a crucial factor in improving rural healthcare.

10. **5G Smart phones**: The smartphones connect to 5G Network and provides users with access to internet.

3. Protocol Summary

Below is the brief description of 3GPP protocol layers/modules present in various parts the of the 5G system.

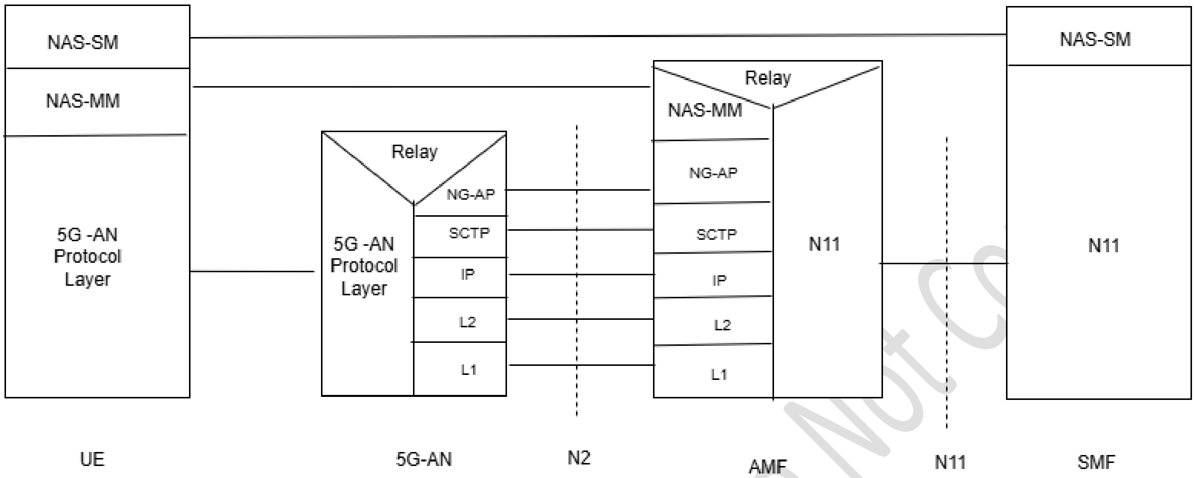


Figure 3 Protocol Stack showing NAS Layer on UE and AMF

a. Protocol Deployment on Server/UE/Chipset

The 5G Core Network is built on a diverse set of protocols that enable seamless communication and advanced capabilities. Let's break it down into structured categories:

Control Plane Protocols

NGAP (Next Generation Application Protocol): NGAP stands for Next Generation Application Protocol on the N2 interface between the gNB and the AMF (Access and Mobility management function). NGAP is transferred over SCTP (Stream Control Transmission Protocol). NGAP protocol provides transport function between UE and AMF by offering NAS signalling transport. Following are some of the procedures supported on NGAP interface in 5G Network deployed by 5G Labs.

- procedures to establish, maintain and release NG-RAN part of PDU sessions;
- the separation of each UE on the protocol level for user specific signalling management;
- the transfer of NAS signalling messages between UE and AMF;
- mechanisms for resource reservation for packet data streams.

NAS (Non-Access Stratum Protocol): A functional layer in wireless telecom protocol stacks. In 5G, NAS messages are used for signalling between the user equipment and the core network. Following are procedures supported by NAS Protocol.

- Authentication
- Registration
- UL/DL NAS Transport
- De-Registration
- Service Setup

- Configuration Update
- Identify Query
- Notification
- Security Mode Setup
- 5GMM Status

PFCP (Packet Forwarding Control Protocol): PFCP (Packet Forwarding Control Protocol) is a signalling protocol used in mobile core network, such as EPC and 5GC, to implement the CUPS architecture (Control and User Plane Separation, not a printing system).

PCF (PCF): Policy and charging function. Functions supported by PCF are

- Policy management: Manages policies for network resources, mobility, and security
- Network slicing: Defines and enables network slicing for different devices and segments
- Charging: Enables operators to charge based on the value they deliver to customers
- Analytics: Provides advanced analytics for improved services
- Policy control decision: Makes policy control decisions and flows based charging control

User Plane Protocols

GTP-U (GPRS Tunneling Protocol – User Plane): GTP-U is used for carrying user data within the GPRS core network and between the radio access network and the core network. The user data transported can be packets in any of IPv4, IPv6, or PPP formats.

UDP (User Datagram Protocol): User Datagram Protocol (UDP) is a communication protocol that sends data packets between computers on a network. It's used for applications that require speed, like gaming, video streaming, and voice over IP (VoIP).

Transport and Connectivity Protocols

IP (Internet Protocol): The Internet Protocol (IP) is a set of rules that govern how data is sent between devices on the internet. Its also part of Core/UE protocol for routing data.

TLS (Transport Layer Security): Transport Layer Security (TLS) is a cryptographic protocol that protects communication between a client and a server.

BGP (Border Gateway Protocol): Border Gateway Protocol (BGP) is a set of rules that helps data find the best route on the internet.

DNS (Domain Name System): The Domain Name System (DNS) translates human-readable domain names into machine-readable IP addresses enabling internet communication

Other Key Protocols

Diameter Protocol: Diameter is protocol that enables authentication, authorization, and accounting (AAA) for networks. It's used in telecommunications networks, mobile networks, and IP Multimedia Systems (IMS).

SCTP (Stream Control Transmission Protocol): The Stream Control Transmission Protocol (SCTP) is a transport protocol that ensures reliable data transmission between two endpoints. It's similar to TCP

b. Network Node Connectivity in 5G

Please section refer 4

c. Network Virtualization in 5G Using OpenStack & Kubernetes

Please section refer 7

4. 5G Core Description

a. 5G Core Functions

i. Description of Network Functions

ii. Interfaces between the Network Functions

iii. APIs between Network Functions

*For the above section a. Please refer to **section 1** of **NiralOS_TRG_Manual_Ver_0.5-2.pdf**.*

b. Implementation of 5G Core

i. Server specification required for 5G Core

1. Explanation of Hardware proposed for the lab

*For the above section b i. Please refer to **section 5** of **NiralOS_TRG_Manual_Ver_0.5-2.pdf**.*

ii. Provisioning of server for installation

2. OS and Virtualization software installation
3. Virtual machine for each network functions

iii. Installation of Network functions

*For the above section b ii, iii. Please refer **to section 'NiralOS 5G Core Docker Containers ' of NiralOS_5GLab_Implementation_Guide-v1.0.pdf**.*

iv. Configuring 5G Core

4. Configuration of API and interfaces
5. IE Message Tracing
a. Locating and Viewing logs
b. How to filter messages

*For the above section b iv. Please refer to **section 'Basic Configuration ' of NiralOS_5GLab_Implementation_Guide-v1.0.pdf**.*

5. 5G RAN Description

System description -Integrated (BBU&RU) Architecture

gNodeB consists of one processor board, Layer 1 Board and RF board. RF board is used for 5G analog and RF processing. 5G application running on processor board along with 5G core is responsible for complete 5G processing (until time-domain data), Layer 1 board is responsible for time-domain data exchange between processor board and RF board. Processor board and Layer 1 board share 10G interface between them. Layer 1 board and RF card share CPRI interface between them. In the Downlink path, 5G time-domain signal is generated by the 5G application running in processor board and sent to Layer 1 board through 10G interface. Layer 1 board packs the IQ to CPRI frame and sends to RF board. RF board performs analog and RF processing and transmits it out through antenna(s).

In the Uplink path, RF signal is captured with antenna(s). After RF and analog processing, time-domain IQs are sent to Layer 1 board. These time-domain IQ samples are sent to processor board via 10G for further processing by the 5G application. The 5G application running on processor board interfaces with 5G core through 1G Ethernet link.

RAN Sub-System description

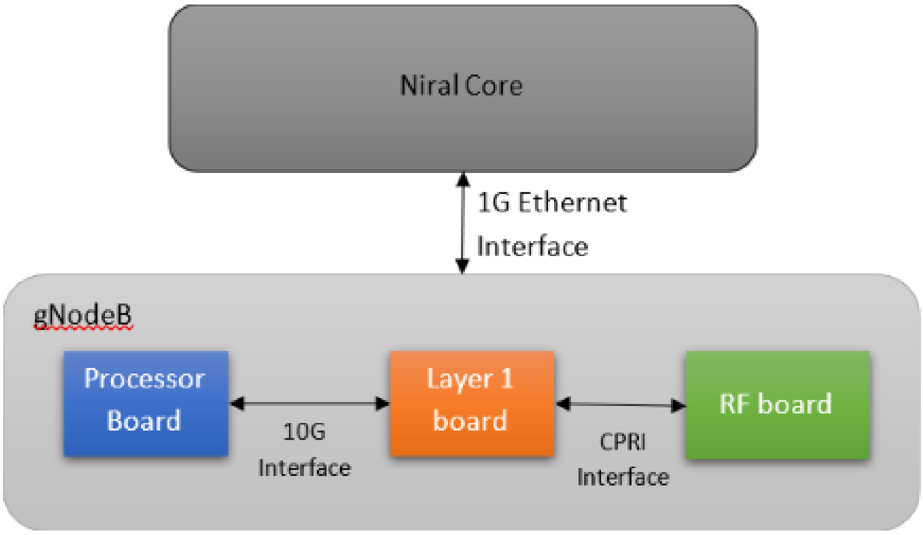


Figure 4 Core and gNodeB Setup Diagram

Functions:

- Functions for Radio Resource Management: Radio Bearer Control, Radio Admission Control, Connection, Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling).

- Encryption and integrity protection of data;.
- Selection of an AMF at UE attachment when no routing to an AMF can be determined from the information provided by the UE.
- Routing of User Plane data towards UPF(s).
- Routing of Control Plane information towards AMF.
- Connection setup and release.
- Scheduling and transmission of paging messages.
- Scheduling and transmission of system broadcast information (originated from the AMF or OAM).
- Measurement and measurement reporting configuration for mobility and scheduling.
- Transport level packet marking in the uplink.
- Session Management.
- Support of Network Slicing.
- QoS Flow management and mapping to data radio bearers.

Features and functionalities of the RAN Sub-System

STGNB2215 is an indigenously developed 5G base station based on Integrated RAN Architecture.

It is powered by the highly integrated 5G RF transceiver chipset Agumbe SCRF4502 from Signalchip which features high fidelity mixed-signal analog RF and integrated advanced signal processing functions such as DPD, CFR and QEC. This compact unit performs all the L1, L2 and L3 functions for high performance gNodeB solution. On the backhaul side the gNodeB interfaces directly with the IP network through ethernet and on the air interface side it connects directly to the antennae.

Supports 3GPP Release 15, 2x2 MIMO with support up to 100 MHz of Bandwidth in Sub-6 Band.

Features

- Supports n78 in the 5G FR1 bands
- 2T2R, 2 UL and DL Layers
- TDD support
- Bandwidth modes: 20,40,60,80 and 100MHz
- Supports Quadrature Error Correction (QEC) , Digital Pre-Distortion (DPD),CFR

Server specification required for 5G RAN

Technical Specifications

Power Details

- 230V AC,50 Hz mains
- Consumption: 125 W

Radio Support

- 50 mW per antenna
- Two antennas

- External Omni directional antenna

Interface Support

- GNSS Port
- RF Interface: SMA

Operating conditions

Operating temperature range +10°C to +35°C

- Controlled temperature to be ensured using air conditioning

Dimensions

- 2U rack mountable form factor
- 482.6 mm x 552.45 mm x 88.9 mm.
- Weight: 11.5kg

Implementation of 5G RAN

Server specification required for 5G RAN

NA

Explanation of Hardware proposed for the lab

Provisioning of server for installation

OS and Virtualization software installation

Ubuntu, Virtualization is not applicable as the gNB is integrated RAN type.

Virtual machine for each RAN sub-system

NA

Installation of 5G RAN Sub-System

The RAN software is pre-installed

Initial Connections of all the machines in 5G rack:

In this section, it is discussed about how all the machines in the rack (T1, T2, gNodeB, firewall, L-2 switch) are connected. Physical connections are explained.

- All the devices are connected with their respective power cords and are powered-on
- All the devices (T1, T2, gNodeB) are connected to the L-2 switch as shown in the below connection setup diagram
  - T-1, T-2 servers have multiple ethernet connectors, but only specific ethernet connecters need to be used as shown in the block diagram
  - Other ethernet connectors are some maintenance ports which are to be used when there is some issue with T-1 and T-2 servers
- From switch one ethernet cable goes to firewall as shown in below setup diagram
- From firewall one ethernet cable goes to the college network as shown in below setup diagram

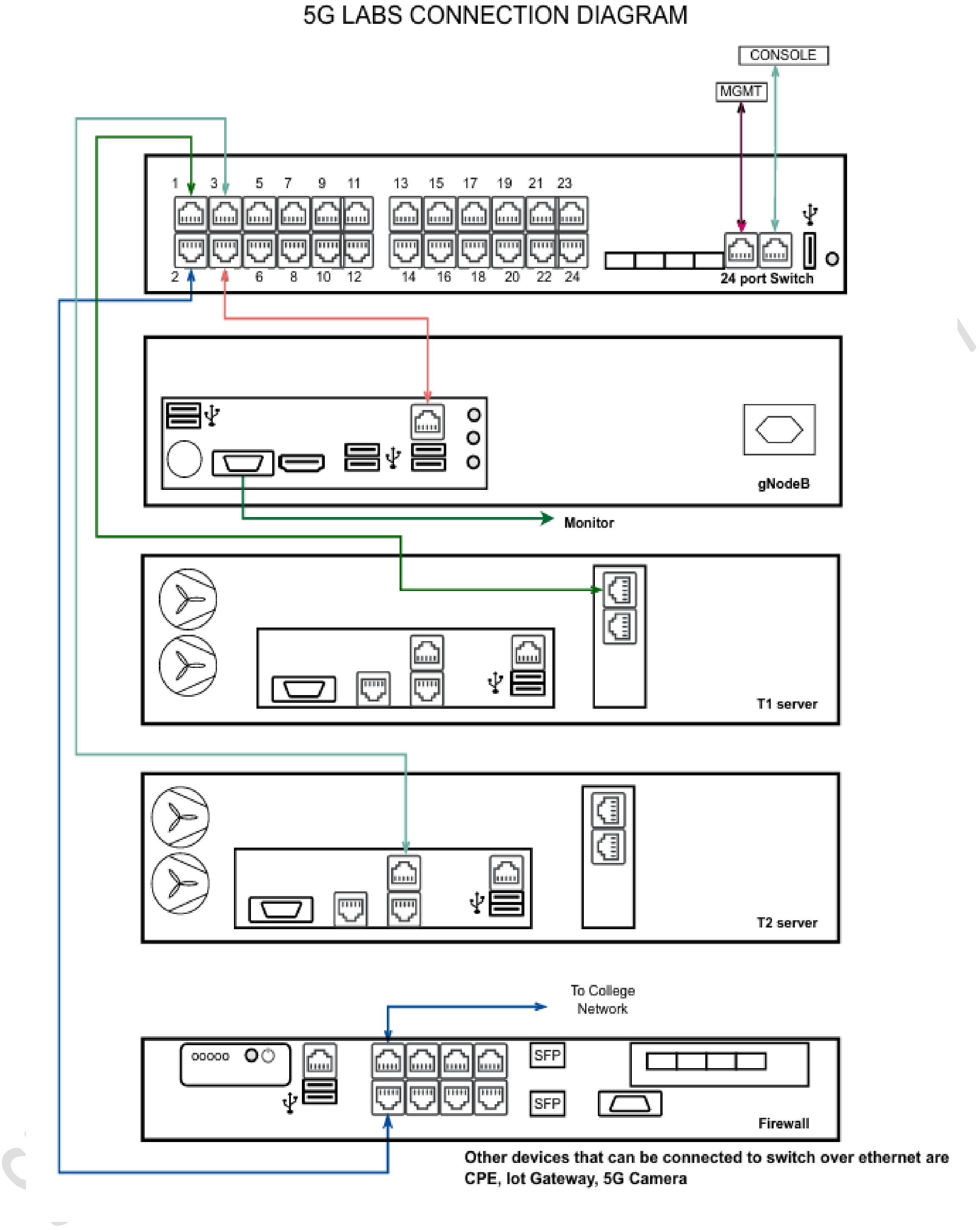


Figure 5 5G rack connection block diagram

Power on the 5G Rack and gNodeB to connect a UE

Connect monitor, keyboard and mouse to gNodeB. gNodeB can be accessed from the monitor

Power-on the rack by switching on the MCB at the back side of rack. This should automatically turn on gNodeB, T-1, T-2, firewall and L-2 switch.

gNodeB automatically boots up when power is connected. Ensure the Led light on gNodeB blinks.

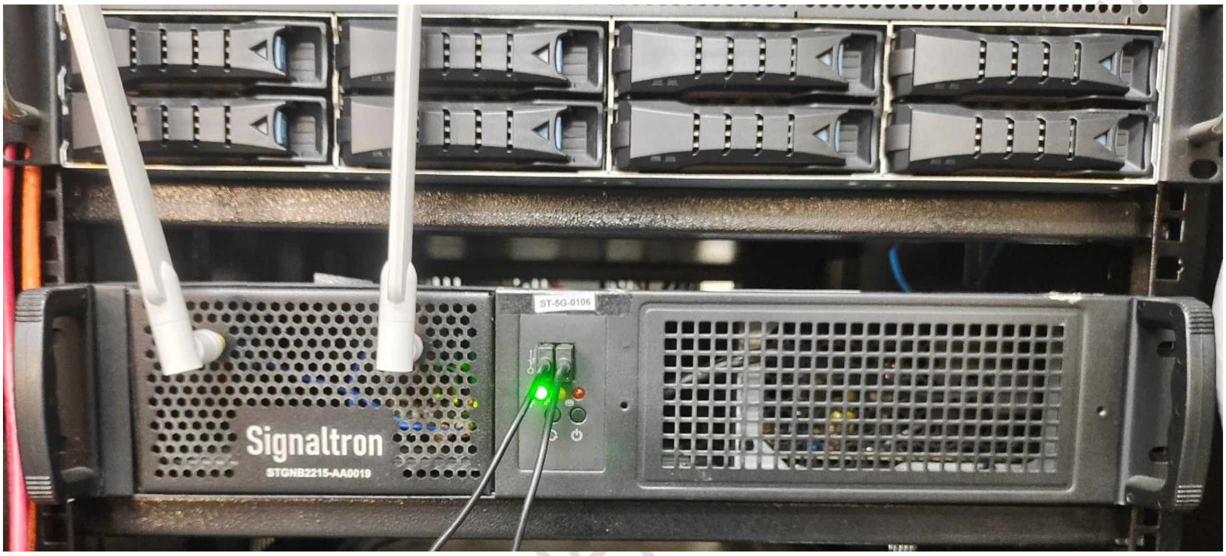


Figure 6 gNodeB with green/yellow LED light on

Ensure the firewall is turned on. Firewall gets turned on as soon as the power is connected.

If the green static LED which is situated in the left side is turned on, then that indicates firewall is operational (as seen in **Figure 7**) **Figure 1**

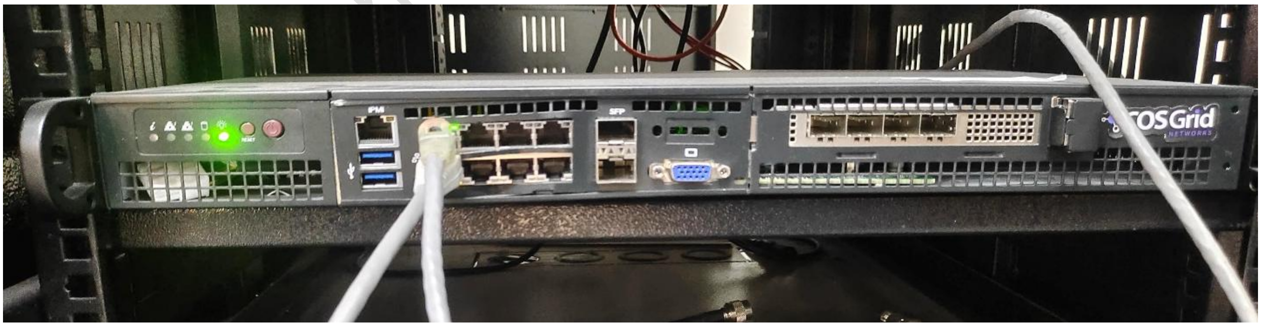


Figure 7 Firewall is in operational state

But if the green LED light is not turned on (as seen in **Figure 8**), then one must press the red colour button on left side with power symbol on it.

One must ignore the lights blinking near the ports. Those lights near ports blink irrespective of the operational state of the firewall, one must only observe the green led light which alone indicates the operational state of firewall. s

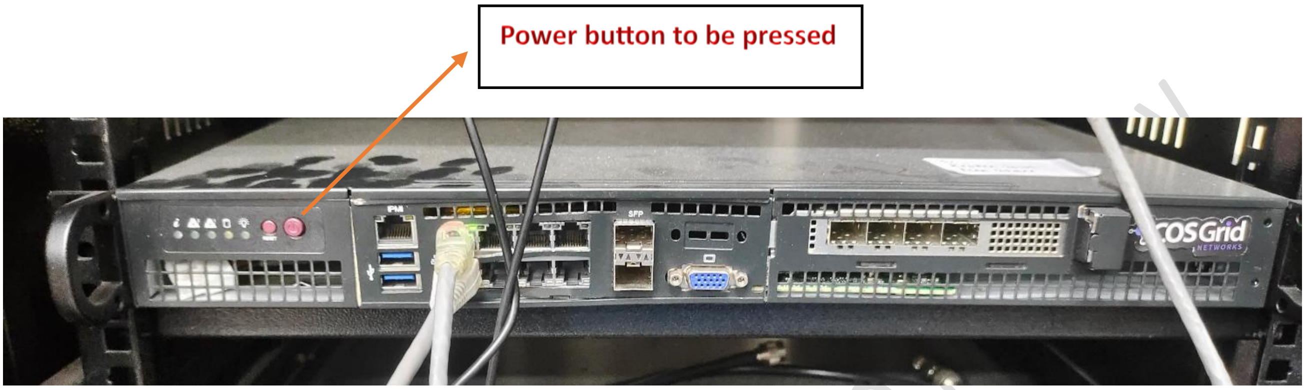

Power button to be pressed

Figure 8 Firewall not turned on completely, not in operational state

Both T-1 and T-2 servers turn on automatically. Ensure both T-1 and T-2 servers are turned on by checking the green led as shown in below image. The 5G core network software running on T-1 gets started automatically on power-on

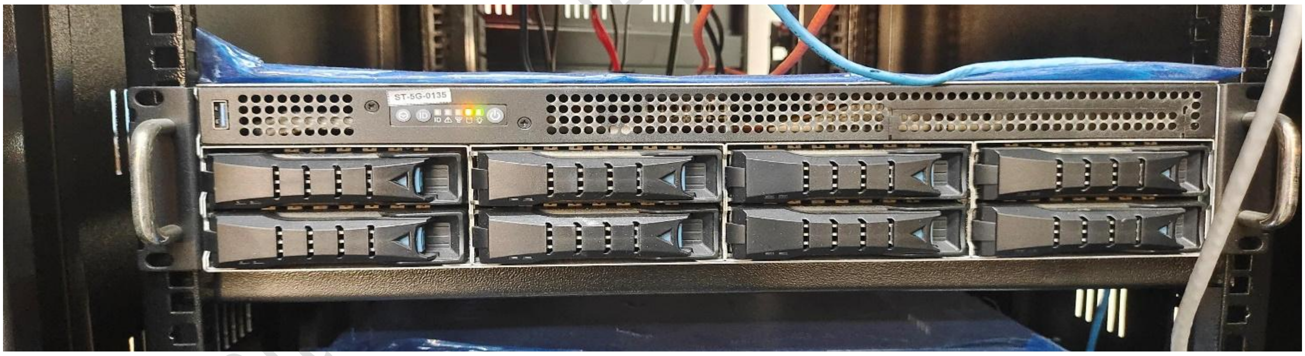


Figure 9 T-1 server with green LED on

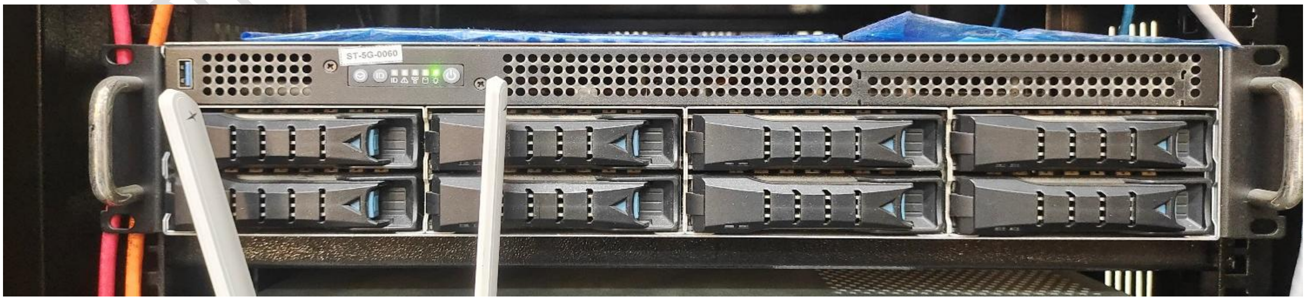


Figure 10 T2 server with green LED on

The L-2 switch also turns on automatically, when power is connected. Ensure the blue LED is turned on the L2 switch.

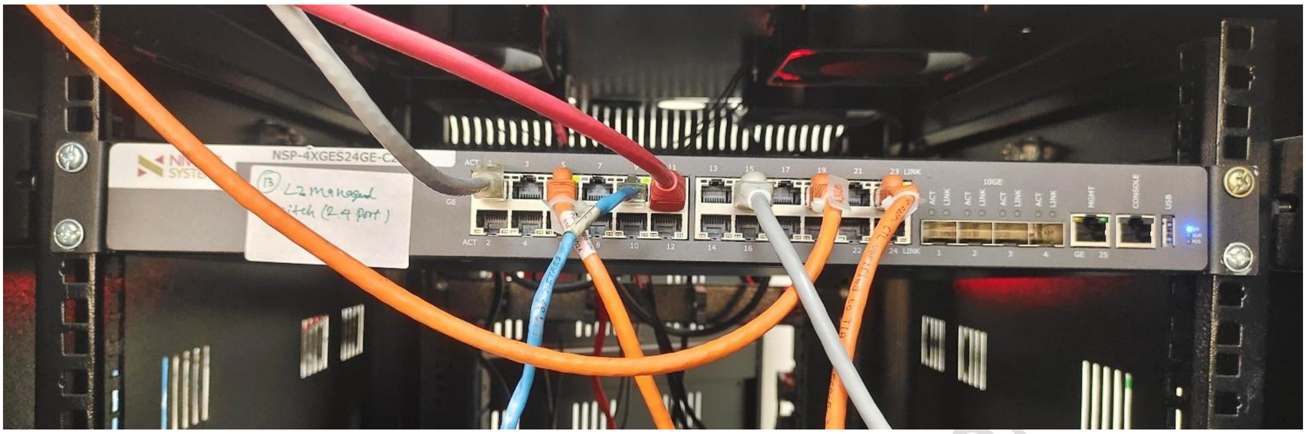


Figure 11 L2 switch with blue LED on

Ensure all mobile phones and other UEs (like CPE, UE Eval Board and IoT Gateway) are in airplane mode or turned off. Once the gNodeB is up, all these devices can be turned on one by one.

Once the power is switched on to the gNodeB, all the related software process runs automatically. To check if the gNodeB is up and radiating, follow the below steps.

Login as user1 in gNodeB.

1. User name: user1

   Password: user1

2. Open terminal.

3. gNodeB will be configured and started automatically, once it is powered-on. Monitor the log file by giving below command

```
$ tail -f /tmp/bw_change.log  #wait for 2-3 min and give
this command
```

Q

:q

4. check for **"5G network is up"** print in the logs. This line ensures that gNodeB is up and radiating

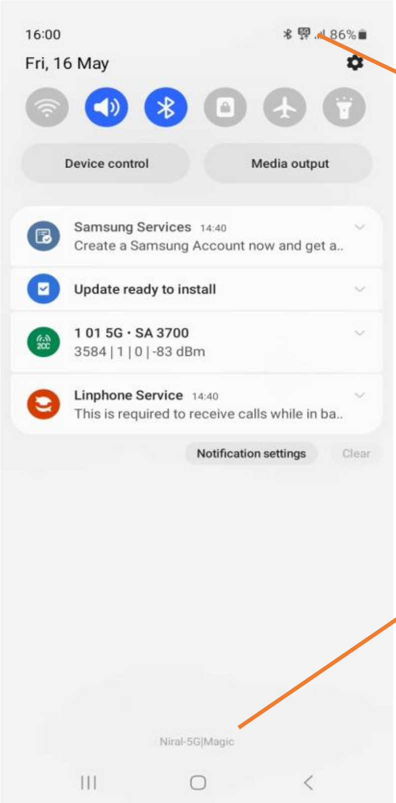
Check for the above print in the log that will open when given the above command. It usually takes 2-3 minutes for this print to come.

The above print when seen, indicates that the gNodeB configurations are done and it is radiating. The UEs (can be a mobile phone or other 5G devices) can be turned on now. Airplane mode can be switched off on the mobile phones.

Summary of the gNodeB and rack power-on procedure: -

1. Put all phones in airplane mode, turn off other UEs (IoT Gateway, CPE and 5G camera)
2. Power-on the rack by switching on the MCB
3. Ensure gNodeB, T1, T2, firewall, L2 switch are turned on properly by checking their LEDs (refer **Figure 6**, **Figure 7**, **Figure 9**, **Figure 10**, **Figure 11**)
4. Check for the print in gNodeB log file as described above
5. Turn off airplane modes on the mobile phones and start powering-on other UEs one by one

The UE should connect automatically. Check for 5G symbol on the mobile phones. Also, the network name can be seen on the mobile phone.



16:00

86%

Fri, 16 May

Samsung Services 14:40
Create a Samsung Account now and get a..

Update ready to install

1 01 5G · SA 3700
3584 | 1 | 0 | -83 dBm

Linphone Service 14:40
This is required to receive calls while in ba..

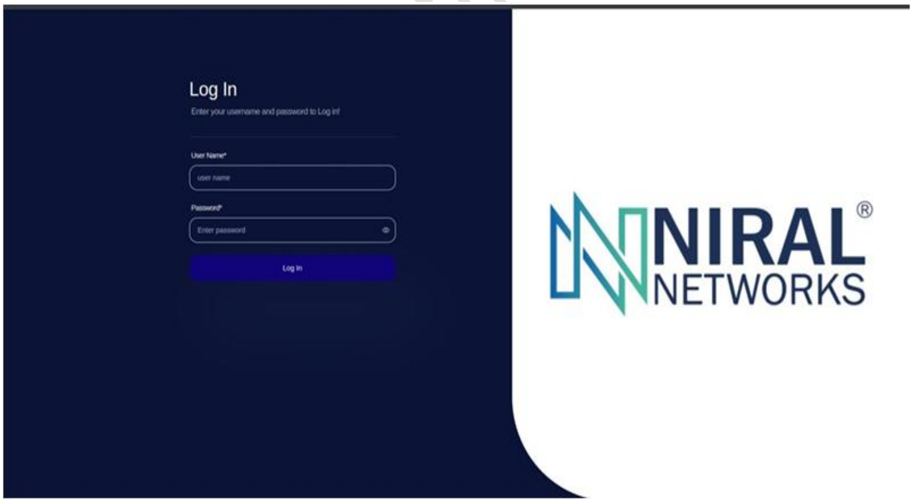
Niral-5G|Magic

5G symbol will be seen once UE is registered.
Also the network name is seen as "Niral-5G"

In some colleges the network name is kept as college name itself

The UE connectivity can also be checked on Niral NMS page

- In browser type http://192.168.10.5
- give user name as "admin" and password as "admin@1234"



Log In

Enter your username and password to Log in!

User Name*

user name

Password*

Enter password

Figure 12 Niral NMS login page

You can see in the Dashboard of Niral NMS, the number of cores, number of Radios and number of Devices.

Active Core in the below image indicates, number of cores that are connected to the NMS. **Active Radio** in below image indicates number of gNodeBs connected to NMS. **Registered Device** in below image indicates that number of UEs connected to the gNodeB.

Checking Registered Device count in NMS dashboard, will give a quick indication on whether the UE is connected to the 5G network or not.

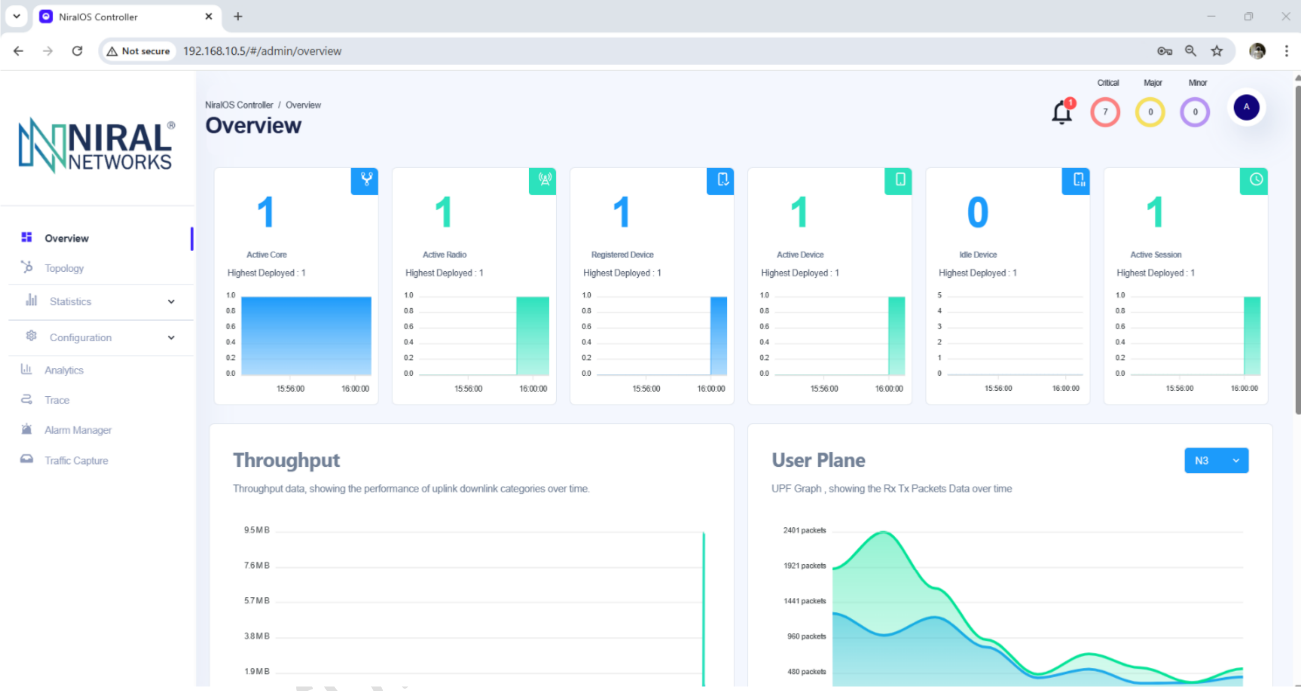


Figure 13 Niral NMS Dashboard

Different Devices and their IP addresses

S.No	Device/SW component	IP Address
1	Firewall	192.168.10.1
2	T-1 server	192.168.10.2
3	T-2 server	192.168.10.3
4	gNodeB	192.168.10.4
5	Core Controller VM	192.168.10.5
6	AMF docker	192.168.10.6
7	UPF docker	192.168.10.7
8	NMS VM on T-2 server	192.168.10.12

Table 1

General Troubleshooting tips if UE does not register:

1. Ensure all the devices are turned on, like T1, T2, Firewall, gNodeB and L-2 switch (refer **Figure 6**, **Figure 7**, **Figure 9**, **Figure 10**, **Figure 11**) by checking the LED status on respective devices

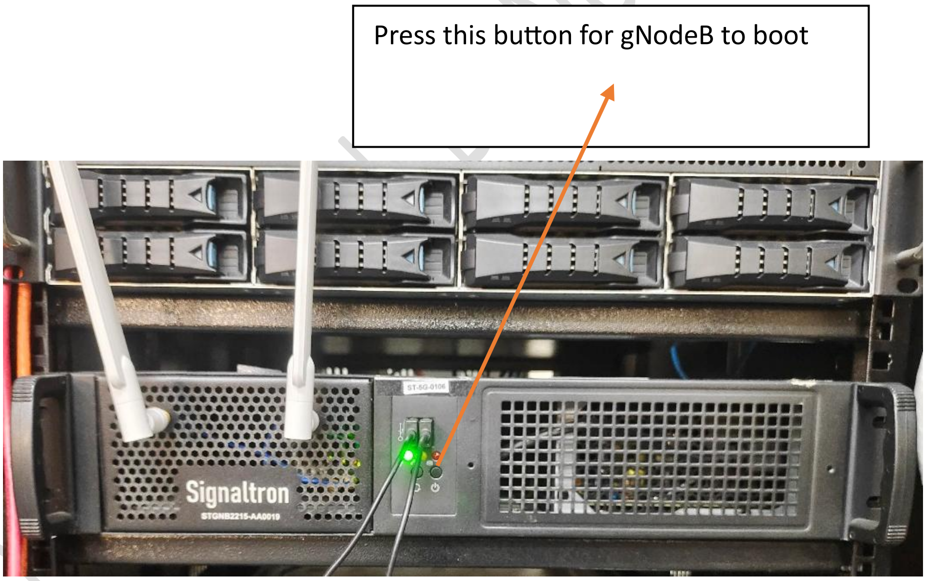
2. Wait for 3-4 min, and check for **"5G network is up"** print in gNodeB log file as described above

    a. If this print does not come even after 5 min, hard reboot the gNodeB

        i. How to hard reboot gNodeB

            1. Go to top right corner on the gNodeB console-> click on power symbol button -> power off

            2. Once the gNodeB gets shutdown, press the physical button on the gNodeB as shown in below image

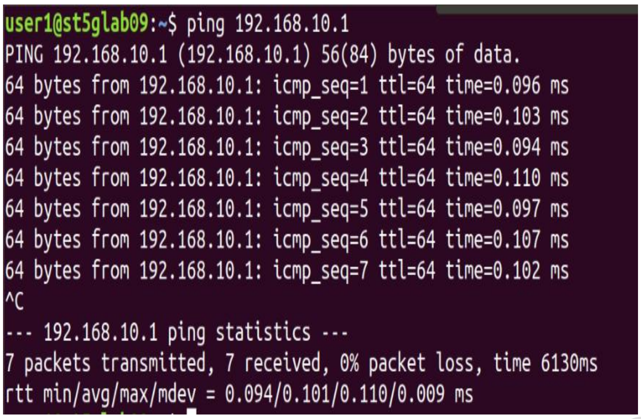


Press this button for gNodeB to boot

ss

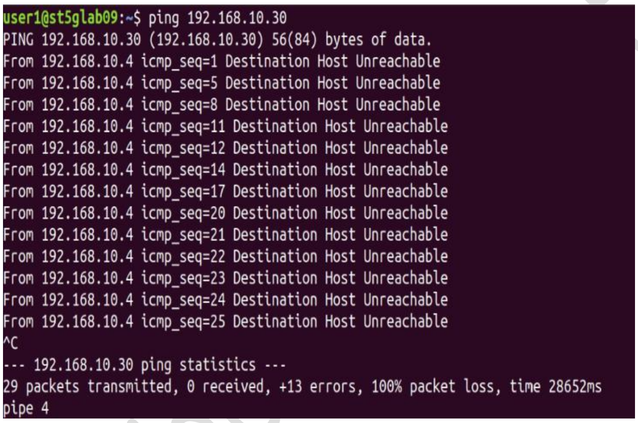
            3. Once gNodeB is up, check again for the print in gNodeB log file and try to attach again

3. Check ping to all core components from gNodeB (mainly **T-1, AMF, UPF** refer Table 1 for IP address details), you should get ping response from all the components



```
user1@st5glab09:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.096 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.103 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.094 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=0.110 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=0.097 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=0.107 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=64 time=0.102 ms
^C
--- 192.168.10.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6130ms
rtt min/avg/max/mdev = 0.094/0.101/0.110/0.009 ms
```

Figure 14 example for a proper ping response



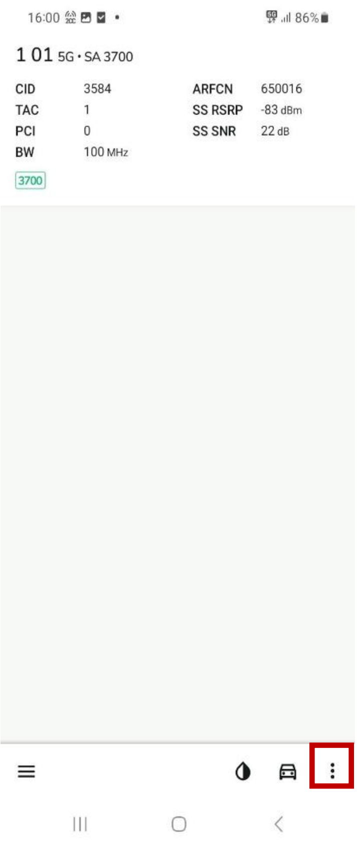
```
user1@st5glab09:~$ ping 192.168.10.30
PING 192.168.10.30 (192.168.10.30) 56(84) bytes of data.
From 192.168.10.4 icmp_seq=1 Destination Host Unreachable
From 192.168.10.4 icmp_seq=5 Destination Host Unreachable
From 192.168.10.4 icmp_seq=8 Destination Host Unreachable
From 192.168.10.4 icmp_seq=11 Destination Host Unreachable
From 192.168.10.4 icmp_seq=12 Destination Host Unreachable
From 192.168.10.4 icmp_seq=14 Destination Host Unreachable
From 192.168.10.4 icmp_seq=17 Destination Host Unreachable
From 192.168.10.4 icmp_seq=20 Destination Host Unreachable
From 192.168.10.4 icmp_seq=21 Destination Host Unreachable
From 192.168.10.4 icmp_seq=22 Destination Host Unreachable
From 192.168.10.4 icmp_seq=23 Destination Host Unreachable
From 192.168.10.4 icmp_seq=24 Destination Host Unreachable
From 192.168.10.4 icmp_seq=25 Destination Host Unreachable
^C
--- 192.168.10.30 ping statistics ---
29 packets transmitted, 0 received, +13 errors, 100% packet loss, time 28652ms
pipe 4
```

Figure 15 example for no ping response

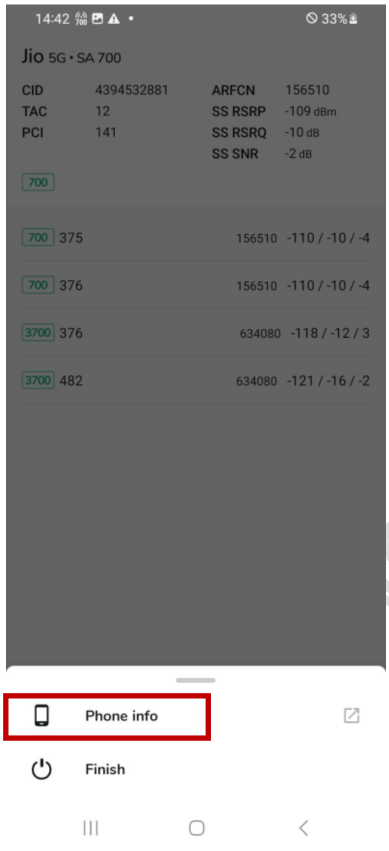
4. Set Preferred Network Type as “NR only” network mode using Netmonster application (already installed in the phones delivered to colleges, app can also be installed from Play store) and then try to do airplane mode on/off couple of times

   a. Open Net monster application

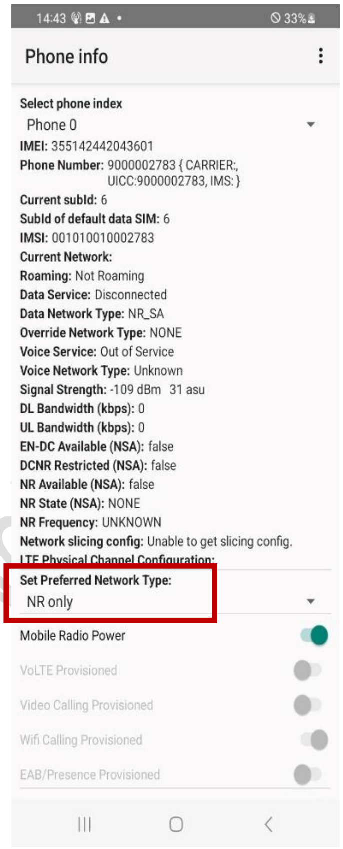
   b. Click on Three dots button on the bottom right -> Phone info -> Set preferred network type as **NR only**



```
16:00                              86%
1 01 5G • SA 3700
CID     3584            ARFCN     650016
TAC     1               SS RSRP   -83 dBm
PCI     0               SS SNR    22 dB
BW      100 MHz
3700
```

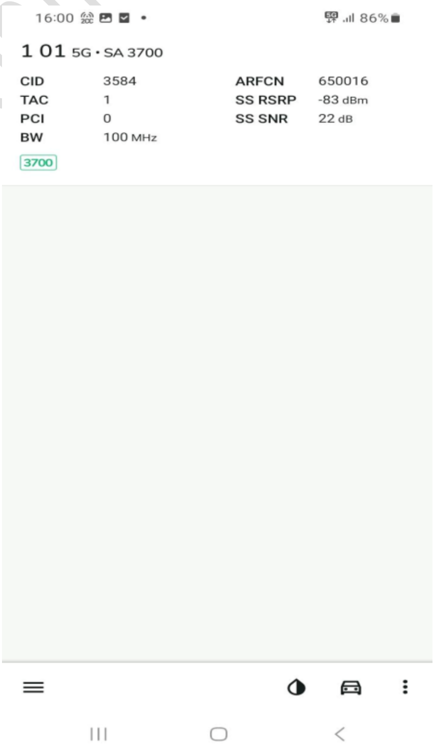


```
14:42                                 33%
Jio 5G • SA 700
CID     4394532881      ARFCN     156510
TAC     12              SS RSRP   -109 dBm
PCI     141             SS RSRQ   -10 dB
                        SS SNR    -2 dB
700

700  375          156510  -110 / -10 / -4
700  376          156510  -110 / -10 / -4
3700 376          634080  -118 / -12 / 3
3700 482          634080  -121 / -16 / -2
```



```
14:43                                 33%
Phone info
Select phone index
Phone 0
IMEI: 355142442043601
Phone Number: 9000002783 { CARRIER:,
              UICC:9000002783, IMS: }
Current subId: 6
SubId of default data SIM: 6
IMSI: 001010010002783
Current Network:
Roaming: Not Roaming
Data Service: Disconnected
Data Network Type: NR_SA
Override Network Type: NONE
Voice Service: Out of Service
Voice Network Type: Unknown
Signal Strength: -109 dBm  31 asu
DL Bandwidth (kbps): 0
UL Bandwidth (kbps): 0
EN-DC Available (NSA): false
DCNR Restricted (NSA): false
NR Available (NSA): false
NR State (NSA): NONE
NR Frequency: UNKNOWN
Network slicing config: Unable to get slicing config.
LTE Physical Channel Configuration:
Set Preferred Network Type:
NR only
Mobile Radio Power
VoLTE Provisioned
Video Calling Provisioned
Wifi Calling Provisioned
EAB/Presence Provisioned
```

5. Check that you see the cell in Net monster application. You should similar to below image in Net monster. You should see ARFCN as 650016.

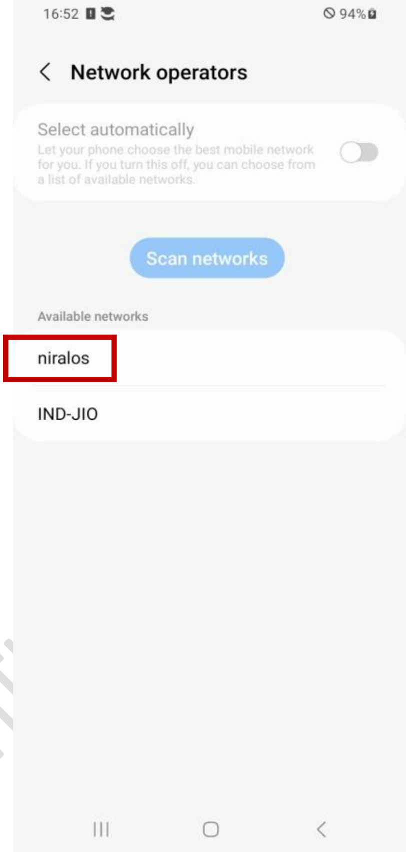


```
16:00                              86%
1 01 5G • SA 3700
CID     3584            ARFCN     650016
TAC     1               SS RSRP   -83 dBm
PCI     0               SS SNR    22 dB
BW      100 MHz
3700
```

6. Try to do airplane mode on and off couple of times, this sometimes helps in UE registration

7. Ensure the cell is visible when you do manual search of the network

    a. Go to settings of the mobile phone -> Connections -> Mobile networks -> Network Operators -> Scan Networks


16:52
94%
Network operators
Select automatically
Let your phone choose the best mobile network for you. If you turn this off, you can choose from a list of available networks.
Scan networks
Available networks
niralos
IND-JIO

8. Ensure no other device/other lab equipment operates in the same frequency of the gNodeB i.e. 3.5Ghz to 3.8Ghz in the premises of the lab

9. Swap the sim card which is present in the current UE, with a sim card that is present in another UE which was previously connecting to the network

10. Restart the UE and try again

11. Hard reboot the gNodeB and try again

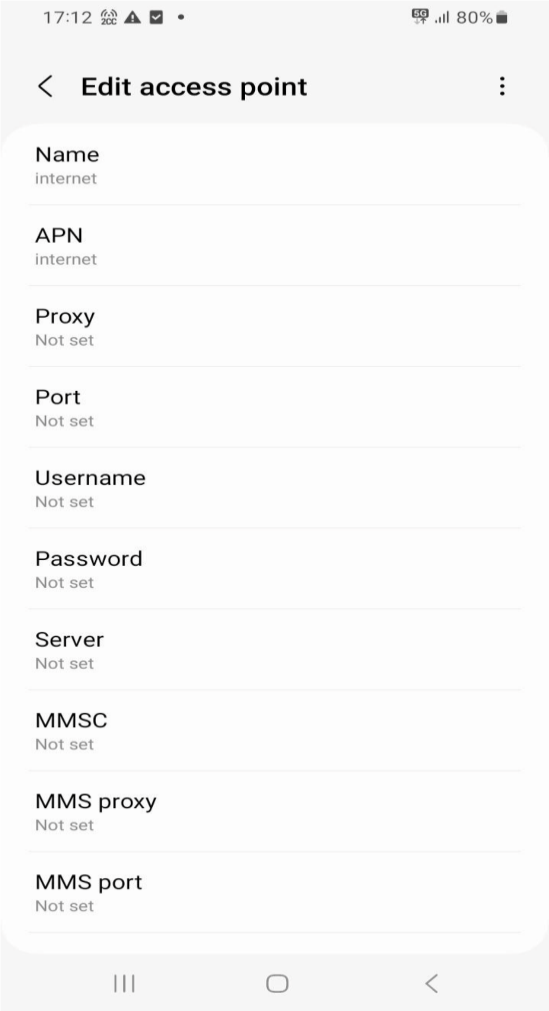
General Troubleshoot for internet connectivity on UE:

1. Check APN settings on the mobile phone or the respective device

    a. Go to Settings -> Connections -> Mobile networks -> Access Point Names

    b. If APN is not present, click on Add on top right and configure with following values:

        1. Name -> internet
        2. APN -> internet
        3. APN protocol -> IPv4
        4. APN roaming protocol -> IPv4
        5. Leave other settings as default



17:12 80%

Edit access point

Name
internet

APN
internet

Proxy
Not set

Port
Not set

Username
Not set

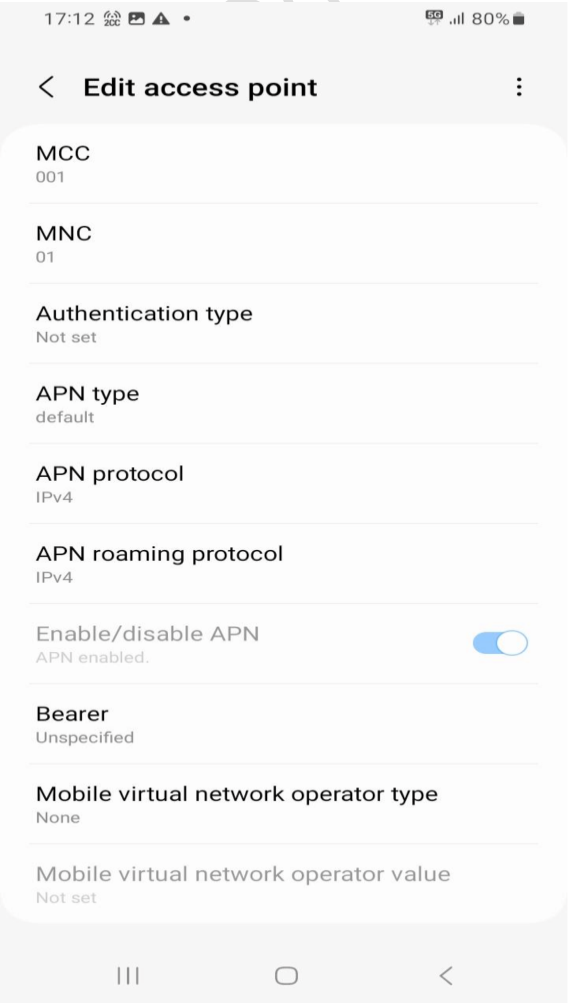
Password
Not set

Server
Not set

MMSC
Not set

MMS proxy
Not set

MMS port
Not set



17:12 80%

Edit access point

MCC
001

MNC
01

Authentication type
Not set

APN type
default

APN protocol
IPv4

APN roaming protocol
IPv4

Enable/disable APN
APN enabled.

Bearer
Unspecified

Mobile virtual network operator type
None

Mobile virtual network operator value
Not set

    c. For other devices, check in their respective sections for APN settings details

2. Ensure firewall pings from the gNodeB

   a. If ping to firewall fails ensure firewall is turned on properly and it is in operational state (refer **Figure 7**, **Figure 8**)

   b. Remove and connect back the ethernet cable going out from gNodeB to the Switch

   c. Remove and connect back the ethernet cable going from Switch to Firewall

   d. Check again if firewall pings from the gNodeB

3. Check ping to 8.8.8.8 works

   a. If this does not happen, remove the cable going out from firewall to your college network and insert it back

   b. Check again if ping works now

   c. If the issue still persists probably the college internet has some fault or the cable going to college network is faulty.

      Connect your laptop directly to the port that is connected to the firewall and check if internet comes to the laptop

4. Check ping to google.com works

   a. If this does not work, but point 3 works, that indicates there is some dns issue in the gNodeB or the firewall which can be resolved by checking dns settings of the gNodeB and the firewall

Switching off the 5G Rack and gNodeB:

- The firewall needs to be turned off first. Login to 192.168.10.1 page on Firefox browser in gNodeB (refer **Figure 17**)
- User-name: admin, password: admin@321
- Under Power -> Power Off -> Yes (refer **Figure 17**)
- Firewall takes around 2-3 min for shut down. Ping can be checked to the firewall from the gNodeB. Whenever the ping response from the firewall gets stopped, then it can be inferred that firewall got shutdown.
- The firewall page might still show “powering off” message, but that message can be ignored.

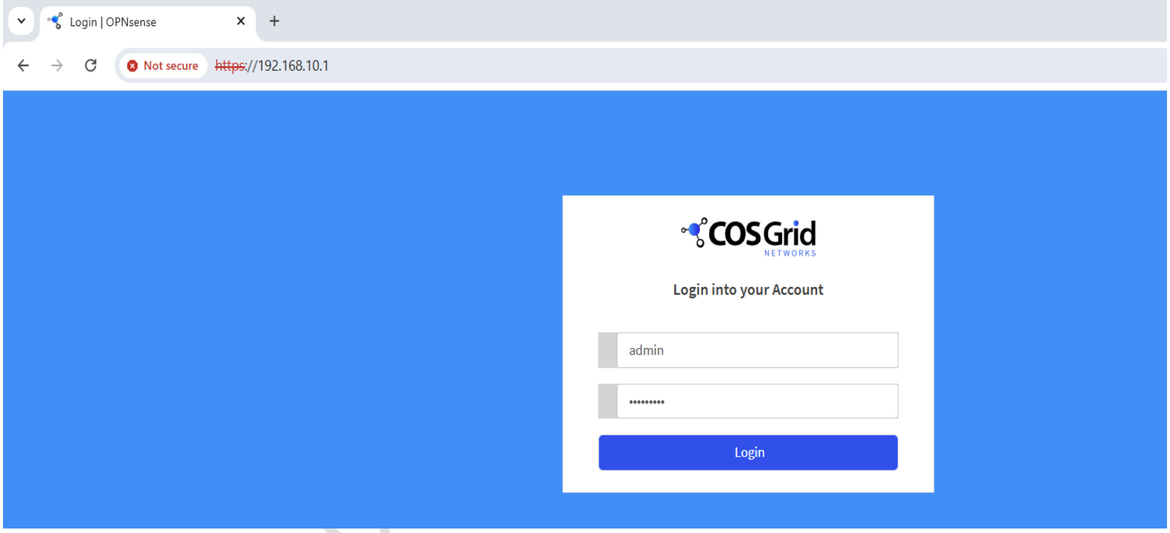
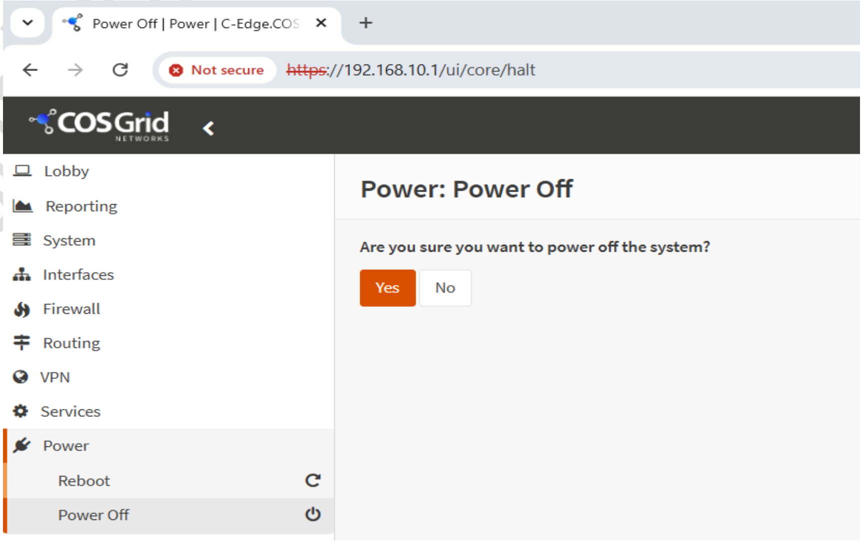


Figure 16 firewall login page



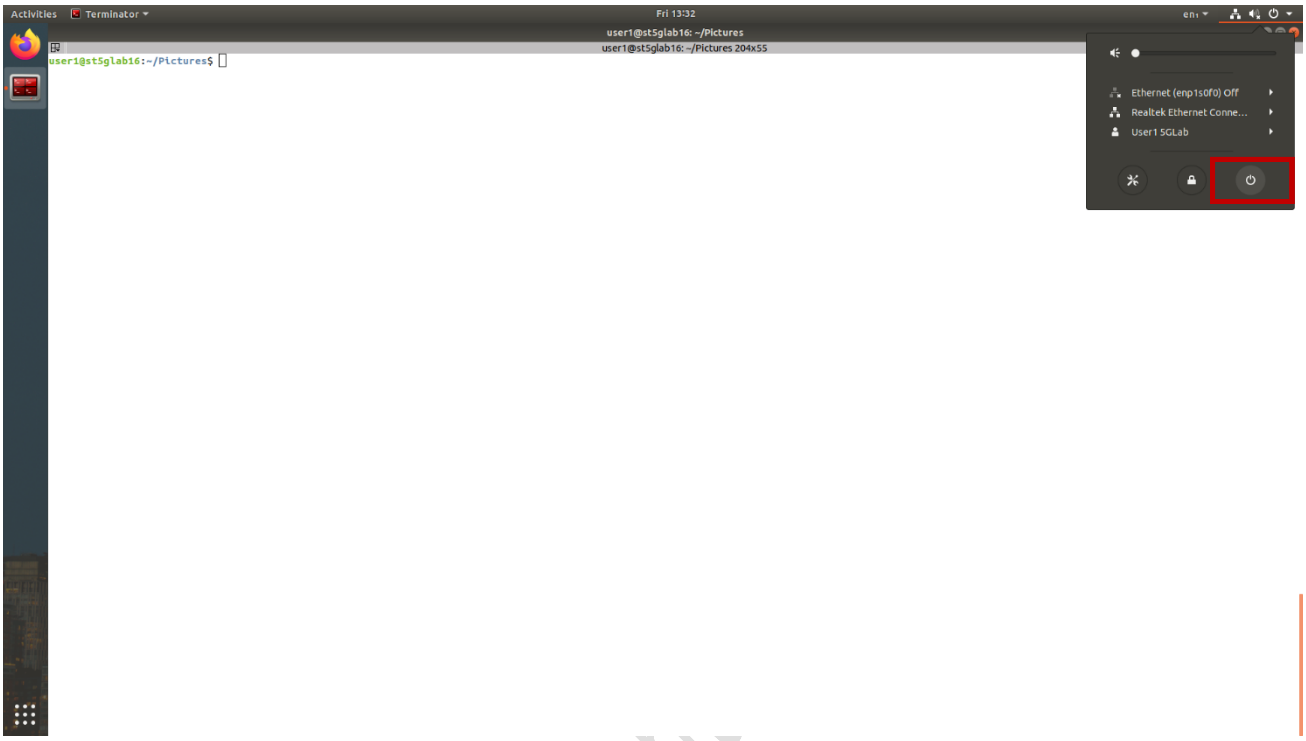
Power: Power Off

Are you sure you want to power off the system?

Yes No

Figure 17 Firewall shutdown page

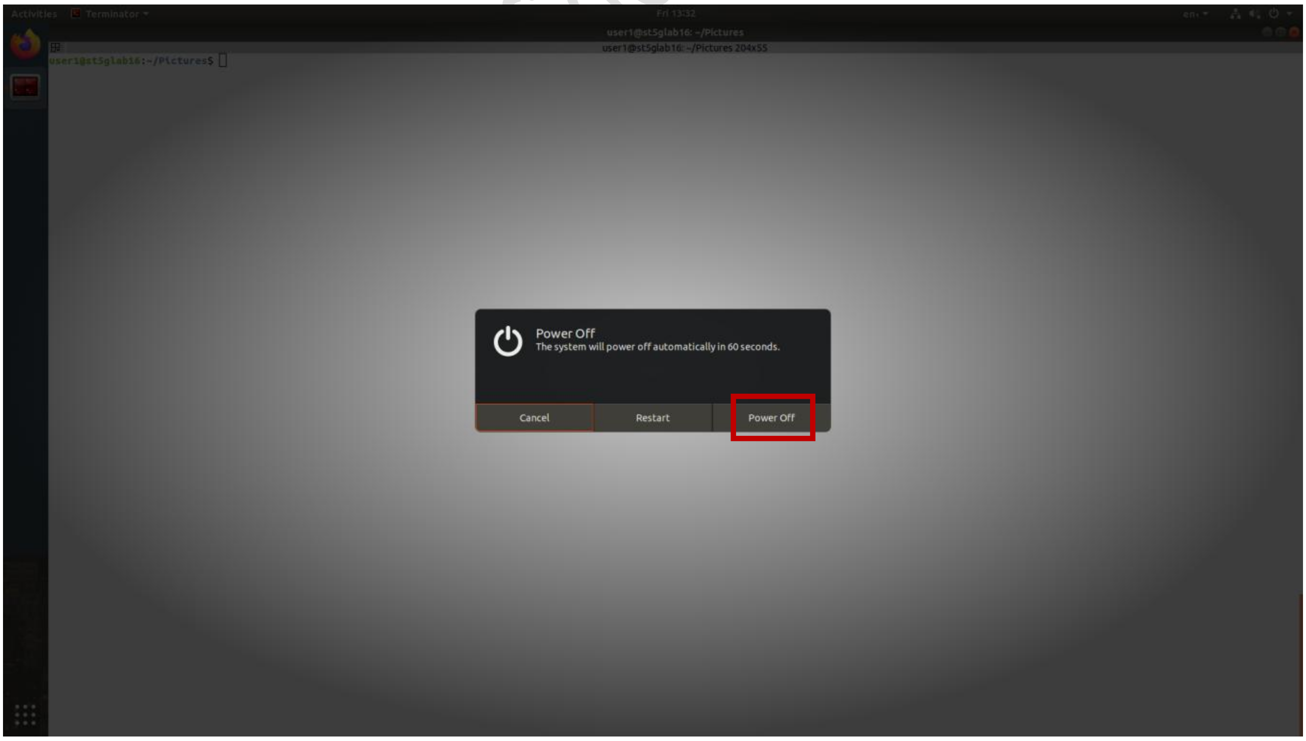
- Power-off the gNodeB, by navigating to the top right corner and clicking on power-off button



Activities
Terminator
Fri 13:32
en
user1@st5glab16: ~/Pictures
user1@st5glab16: ~/Pictures 204x55
Ethernet (enp1s0f0) Off
Realtek Ethernet Conne...
User1 5GLab

```
user1@st5glab16:~/Pictures$
```

Figure 18 gNodeB power-off step 1



Power Off
The system will power off automatically in 60 seconds.

Figure 19 gNodeB power off step-2

- Next long press the physical button (the buttons which has power symbol) on T-1 and T-2 servers till the leds on both servers gets off
- Next the Rack can be switched off

a. Different layers of RAN and their detailed functions

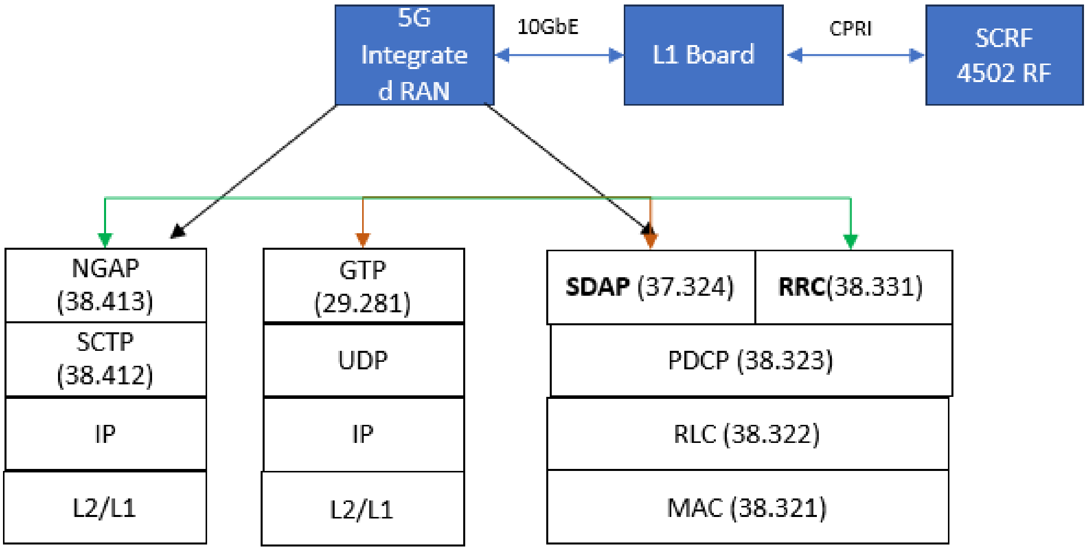


Figure 20 RAN protocol stack

b. Logical, Transport and Physical channels across the RAN protocol stacks

Logical Channels: Offered by MAC to RLC. Control channels carry CP packets. Traffic channels carry UP packets. Each logical channel maps to an RLC channel coming from RLC layer.

Transport Channels: Offered by PHY to MAC. MAC layer multiplexes one or more logical channels to a transport channel. Whereas logical channels describe what is carried, transport channels describe how they're carried.

Physical Channels: Channels that carry information on the air interface. Transport channels map to physical channels. There are also a few standalone physical channels that don't carry higher-layer information.

Downlink logical channels include Broadcast Control Channel (**BCCH**), Paging Control Channel (**PCCH**), Common Control Channel (**CCCH**), Dedicated Control Channel (**DCCH**) and Dedicated Traffic Channel (**DTCH**).

Downlink transport channels include Broadcast Channel (**BCH**), Paging Channel (**PCH**) and Downlink Shared Channel (**DL-SCH**).

Downlink physical channels include Physical Broadcast Channel (**PBCH**), Physical Downlink Control Channel (**PDCCH**) and Physical Downlink Shared Channel (**PDSCH**).

Uplink logical channels include Common Control Channel (**CCCH**), Dedicated Control Channel (**DCCH**) and Dedicated Traffic Channel (**DTCH**).

Uplink transport channels include Random Access Channel (RACH) and Uplink Shared Channel (**UL-SCH**).

Uplink physical channels include Physical Random Access Channel (**PRACH**), Physical Uplink Control Channel (**PUCCH**), and Physical Uplink Shared Channel (**PUSCH**).

c. Mapping between Logical, Transport and Physical channels

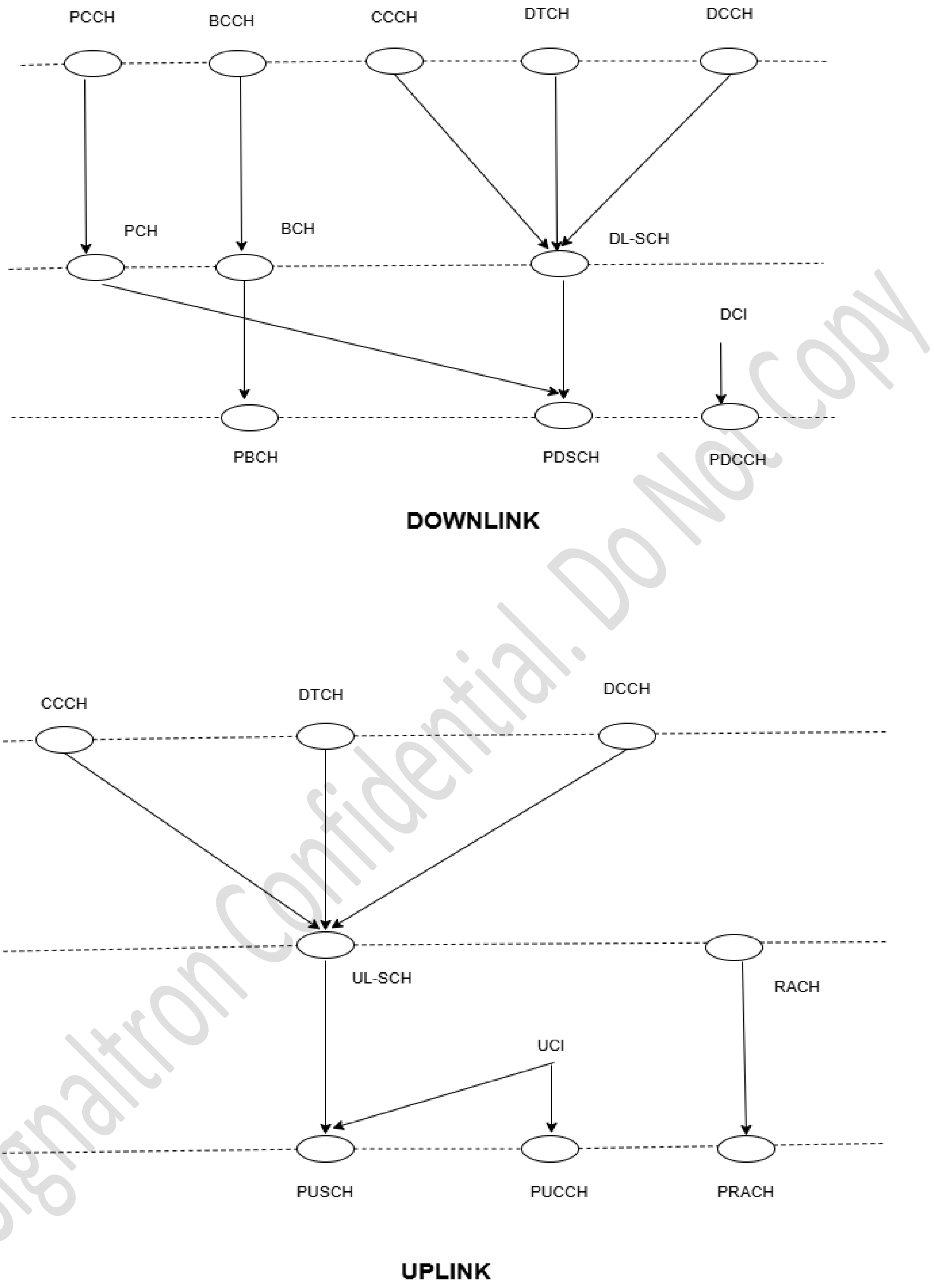


Figure 21 Channel mapping of Logical, Transport and Physical channels

6. Integration of 5G Core and RAN

c. Configuration of Core elements (IP address configuration)

Refer to NiralOS_5G_lab_Implementation-guide.pdf for configuring the 5G Core. Most of the network nodes can be configured using NMS.

After properly configuring the core and gNodeB, system can be powered on. Following sections explain on how to verify the performance of the 5G Lab Network.

d. Connection establishment between RAN – Core elements (AMF,UPF)

Message: Initial UE Message

gNB ➔ New AMF

The gNB sends the Initial UE Message to the selected AMF.

The message carries the Registration Request that was received from the UE in the RRC Setup Complete message.

The "RAN UE NGAP ID" and the "RRC Establishment Cause" are also included in the message.

Message: Initial Context Setup Request

AMF ➔ eNB

The purpose of the Initial Context Setup procedure is to establish the necessary overall initial UE Context at the NG-RAN node, when required, including PDU session context, the Security Key, Mobility Restriction List, UE Radio Capability and UE Security Capabilities, etc.

Message: Initial Context Setup Response

eNB ➔ AMF

This message is sent by the NG-RAN node to confirm the setup of a UE context.

Message: Initial Context Setup Response

eNB ➔ AMF

This message is sent by the NG-RAN node to confirm the setup of a UE context.

Message: PFCP session establishment Request

SMF ➔ UPF

The PFCP Session Establishment procedure shall be used to setup an PFCP session between CP function and UP function and configure Rules in the UP function so that the UP function can handle incoming packets.

Message: PFCP session establishment Response

UPF ➔ SMF

The PFCP Session Establishment Response shall be sent over the Sxa, Sxb, Sxc and N4 interface by the UP function to the CP function as a reply to the PFCP Session Establishment Request.

e. Verification of connection establishment between Core and RAN

The connection establishment between core and RAN can be verified with successful completion PDU session establishment procedure and GTP-U Tunnel creation.

7. MEC

a. Overview – functionalities and description

An MEC server is a critical component of 5G architecture, bringing cloud computing capabilities closer to the edge of the network. This enables faster processing of data, reduces latency, and supports applications that require real-time performance, such as augmented reality, autonomous driving, and IoT systems.

b. Implementation of MEC Platform.

i. Explanation of Hardware proposed for the lab

ii. Provisioning of server for installation

1. OS and Virtualization software installation
2. Virtual machine for each network functions

*For the above section c. Please refer to **section 'NiralOS MEC - Add and Delete VM '** of **NiralOS_5GLab_Implementation_Guide-v1.0.pdf**.*

c. Procedure for Application Installation

*For the above section c. Please refer to **section 'NiralOS Edge Installation – Key Insights '** of **NiralOS_5GLab_Implementation_Guide-v1.0.pdf**.*

d. Procedure to Route the traffic to MEC server

e. Monitor, analysis and management of application life cycle

8. Testing and Tracing tool: Wireshark

a. Introduction

gNodeB Wireshark logs can be used to view and analyse the logs on NG interface. NG interface lies between 5G Core Network & gNodeB. The control plane interface NG-C is between gNodeB and AMF and the user plane interface NG-U is between gNodeB and UPF.

b. Features and functionalities

- Run Wireshark

```
$ wireshark
```

- In Interfaces option, choose "Any"
- To view data plane packets, set packet type as "udp" (to see the GTP packets between UE and gNodeB).
- To view control plane packets, set packet type as "sctp". To view packet transmission gNodeB and core, select filter as NGAP.
- In the filter option, choose "ngap"

a. Log analysis

Following are NG-C related messages that can be viewed in Wireshark logs:

- NGSetupRequest
- NGSetupResponse
- InitialUEMessage
- InitialContextSetupRequest
- UEContextReleaseCommand
- UEContextReleaseComplete
- UplinkNASTransport
- DownlinkNASTransport
- PDUSessionResourceSetupRequest

- PDUSessionResourceSetupResponse

On NG-U interface, IP Packet exchanges between UE and IP world can be seen. GTP-U tunneling protocol is used on NG-U interface for transfer of IP packets.

9. End to End testing of system

5G system testing would be to ensure appropriate function of all nodes and function of the system. Key functions such as integrity, security, Qos, etc. And also to test the use cases which would suit the key features of a 5G network such as eMBB, uRLLC, mMTC.

a.5G Power On Procedures

Power ON: Upon powering on, a 5G UE initiates the cell search procedure.

Cell search start Start (DL): The UE scans a specific frequency range or a list of pre-configured frequencies to detect potential 5G NR cells broadcasting signals.

Decoding the Master Identity Block (MIB)(DL): During the search, the UE decodes the Master Identity Block (MIB) from any detected cell. The MIB provides essential information like the cell identity and Primary Synchronization Signal (PSS) characteristics.

Obtaining System Information Block 1 (SIB1)(DL): Using the information from the MIB, the UE identifies the Physical Downlink Control Channel (PDCCH) configuration for System Information Block 1 (SIB1). It then decodes SIB1, which contains crucial system-wide information such as neighbouring cell details and cell selection parameters.

Cell Scan End: Once the UE has gathered sufficient information from potential cells and SIB1, the cell scan process concludes.

Ranking and Camping(at UE): Based on the collected data, the UE ranks the available cells using various criteria like received signal strength and cell selection parameters. It then “camps” on the best-ranked cell, meaning it synchronizes with that cell’s timing and frequency for further communication.

Decoding SIB1 of the Best Cell(DL): After camping, the UE decodes the complete SIB1 of the chosen cell, accessing detailed information specific to that cell and its neighbouring cells.

Reading RACH Configuration(DL): From SIB1, the UE retrieves the Random Access Channel (RACH) configuration, which defines how the UE can request access to the network for data transmission or control signalling.

Initiating RACH Procedure(UL): Finally, equipped with the necessary information, the UE initiates the RACH procedure, formally requesting access to the network through the chosen cell.

b. DL and UL Synchronization

5G UL and DL synchronization are procedures that ensure seamless communication between a user device and a base station. These processes are vital for 5G networks, especially in high-end cellular communication systems.

DL synchronization:

This is the process in which UE detect the radio boundary (i.e, the exact timing when a radio frame starts) and OFDM symbol boundary(i.e, the exact timing when an OFDM symbol starts). This process is done by detecting and analysing SS Block.

There is a pair of downlink signals, the primary synchronization signal (**PSS**) and the secondary synchronization signal (**SSS**), that is used by devices to find, synchronize to, and identify a network.

There is a downlink physical broadcast channel (**PBCH**) transmitted together with the **PSS/SSS**. The **PBCH** carries a minimum amount of system information including an indication where the remaining broadcast system information is transmitted. In the context of NR, the **PSS**, **SSS**, and PBCH are jointly referred to as a synchronization signal (**SS**) block.

UL Synchronization:

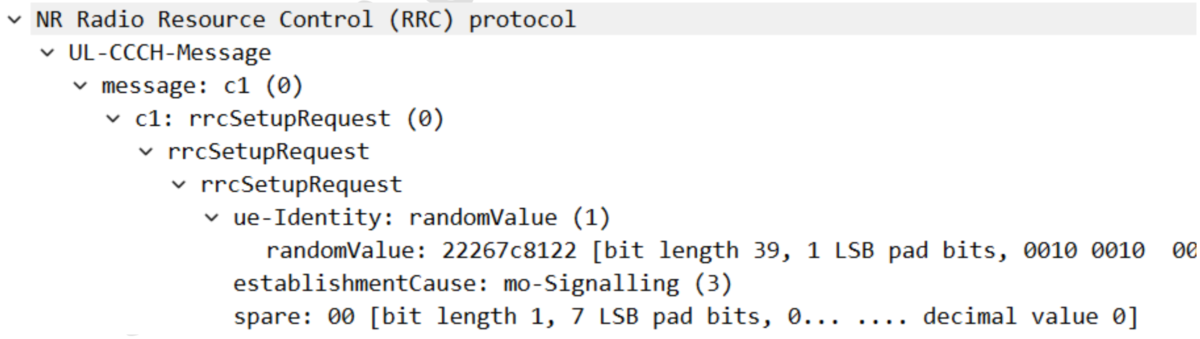
This is the process in which UE figure out the exact timing when it should send uplink data (i.e, **PUSCH / PUCCH**). Usually a network (gNB) is handling multiple UEs and the network has to ensure that the uplink signal from every UE should be aligned with a common receiver timer of the network. So this involves much more complicated process and sometimes it has to adjust UE Tx timing (uplink timing) of each UE. This is called RACH process.

c. RRC connection establishment

There is a four-stage random-access procedure, commencing with the uplink transmission of a random-access preamble.

- The UE sends a **Random Access** Preamble to request network access (**RACH**). Message 1
- The gNB responds with **a Random Access Response (RAR)** message. Message 2
- The UE sends an **RRCSetupRequest** message to the gNB. Message 3
- The gNB responds with an **RRCSetup** message. Message 4 (Contention resolved)
- The UE sends a **RRCSetupComplete** with the Registration Request message to the network.

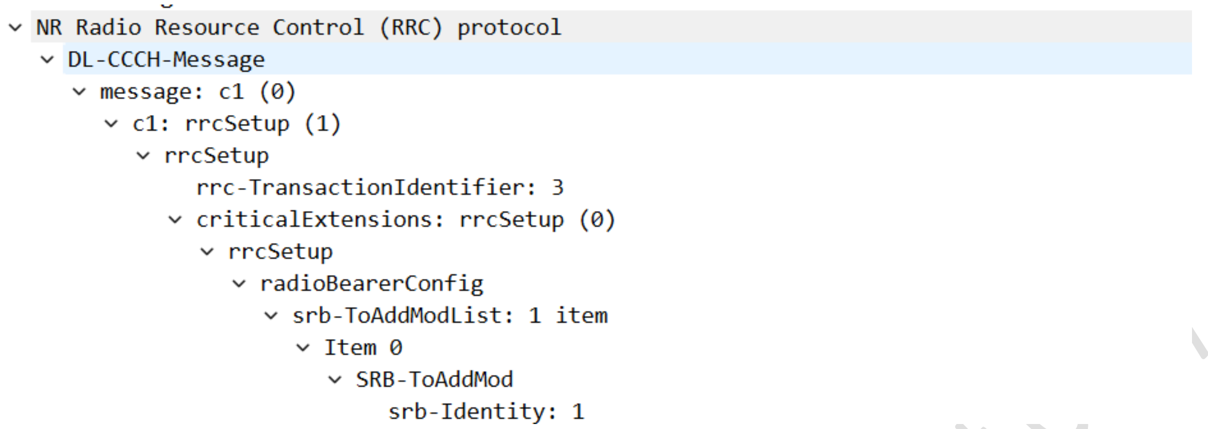
The RRCSetupRequest message is used to request the establishment of an RRC connection.



```
⌄ NR Radio Resource Control (RRC) protocol
  ⌄ UL-CCCH-Message
    ⌄ message: c1 (0)
      ⌄ c1: rrcSetupRequest (0)
        ⌄ rrcSetupRequest
          ⌄ rrcSetupRequest
            ⌄ ue-Identity: randomValue (1)
                randomValue: 22267c8122 [bit length 39, 1 LSB pad bits, 0010 0010  00
              establishmentCause: mo-Signalling (3)
              spare: 00 [bit length 1, 7 LSB pad bits, 0... .... decimal value 0]
```

Figure 22 RRCSetupRequest

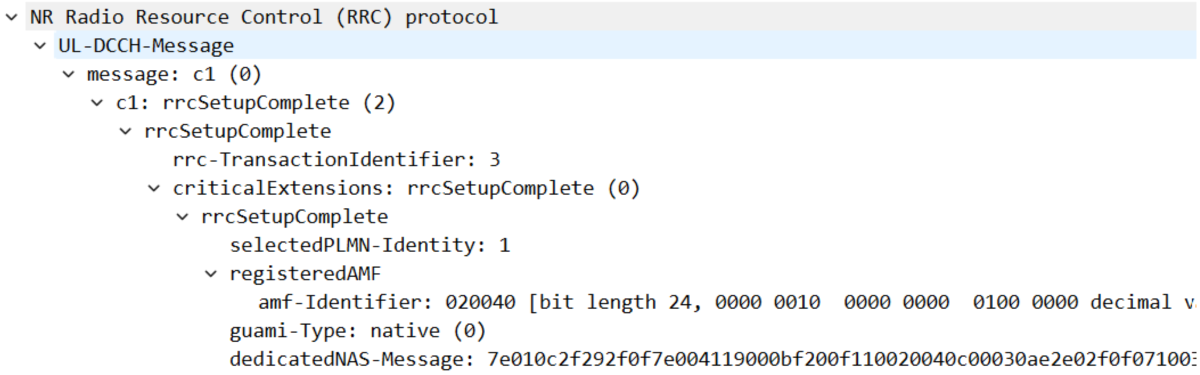
The RRCSetup message is sent to UE by gNB with SRB1 configuration to start establishing a RRC connection.



```
⌄ NR Radio Resource Control (RRC) protocol
  ⌄ DL-CCCH-Message
    ⌄ message: c1 (0)
      ⌄ c1: rrcSetup (1)
        ⌄ rrcSetup
            rrc-TransactionIdentifier: 3
          ⌄ criticalExtensions: rrcSetup (0)
            ⌄ rrcSetup
              ⌄ radioBearerConfig
                ⌄ srb-ToAddModList: 1 item
                  ⌄ Item 0
                    ⌄ SRB-ToAddMod
                        srb-Identity: 1
```

Figure 23 RRCSetup

The RRCSetupComplete message is sent from UE to gNB in response to the RRCSetup message, which also contains the UE Registration Request towards the AMF.

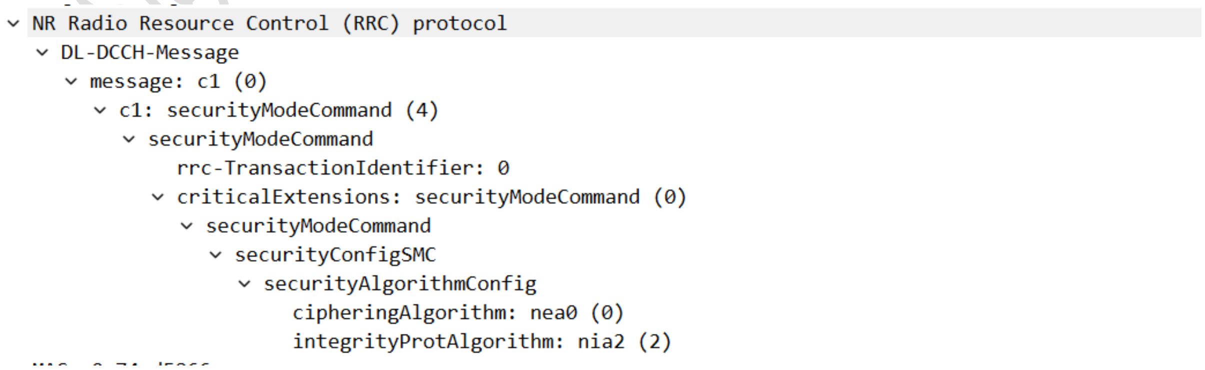


```
⌄ NR Radio Resource Control (RRC) protocol
  ⌄ UL-DCCH-Message
    ⌄ message: c1 (0)
      ⌄ c1: rrcSetupComplete (2)
        ⌄ rrcSetupComplete
            rrc-TransactionIdentifier: 3
          ⌄ criticalExtensions: rrcSetupComplete (0)
            ⌄ rrcSetupComplete
                selectedPLMN-Identity: 1
              ⌄ registeredAMF
                  amf-Identifier: 020040 [bit length 24, 0000 0010  0000 0000  0100 0000 decimal v
                guami-Type: native (0)
                dedicatedNAS-Message: 7e010c2f292f0f7e004119000bf200f110020040c00030ae2e02f0f07100
```

Figure 24 RRCSetupComplete

Security Mode Command is sent by gNB towards UE which containing security config indication of the Integrity algorithm and Ciphering algorithm negotiated during the Registration request message.

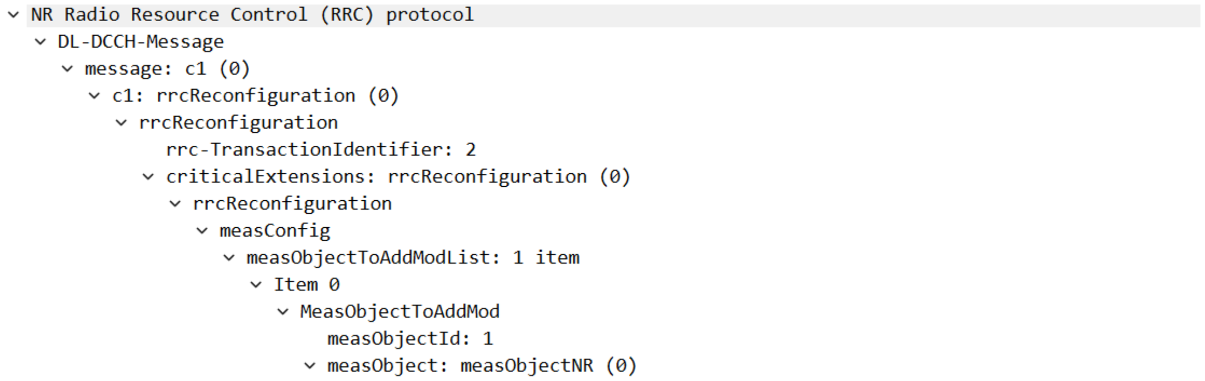
This enables the UE and the NW to enable integrity and ciphering of CP and UP messages for further communication.



```
⌄ NR Radio Resource Control (RRC) protocol
  ⌄ DL-DCCH-Message
    ⌄ message: c1 (0)
      ⌄ c1: securityModeCommand (4)
        ⌄ securityModeCommand
            rrc-TransactionIdentifier: 0
          ⌄ criticalExtensions: securityModeCommand (0)
            ⌄ securityModeCommand
              ⌄ securityConfigSMC
                ⌄ securityAlgorithmConfig
                    cipheringAlgorithm: nea0 (0)
                    integrityProtAlgorithm: nia2 (2)
```

Figure 25 Security Mode Command

RRCReconfiguration message is responsible to establish the SRB2 and DRB bearers between UE and the network.



```
⌄ NR Radio Resource Control (RRC) protocol
  ⌄ DL-DCCH-Message
    ⌄ message: c1 (0)
      ⌄ c1: rrcReconfiguration (0)
        ⌄ rrcReconfiguration
            rrc-TransactionIdentifier: 2
          ⌄ criticalExtensions: rrcReconfiguration (0)
            ⌄ rrcReconfiguration
              ⌄ measConfig
                ⌄ measObjectToAddModList: 1 item
                  ⌄ Item 0
                    ⌄ MeasObjectToAddMod
                        measObjectId: 1
                      ⌄ measObject: measObjectNR (0)
```

Figure 26 RRCReconfiguration

d. NSA and SA Procedures

The basic difference between both is that NSA(NSA-Non stand alone) relies on 4G/LTE core and SA(Stand alone) has 5GCore and both use the data path of a 5G network. Further, from use case point of view 5G SA has a wider range of applications by the virtue of Network slicing feature.

NSA-Non stand alone:

NSA is not supported by the current RAN

SA – Stand alone:

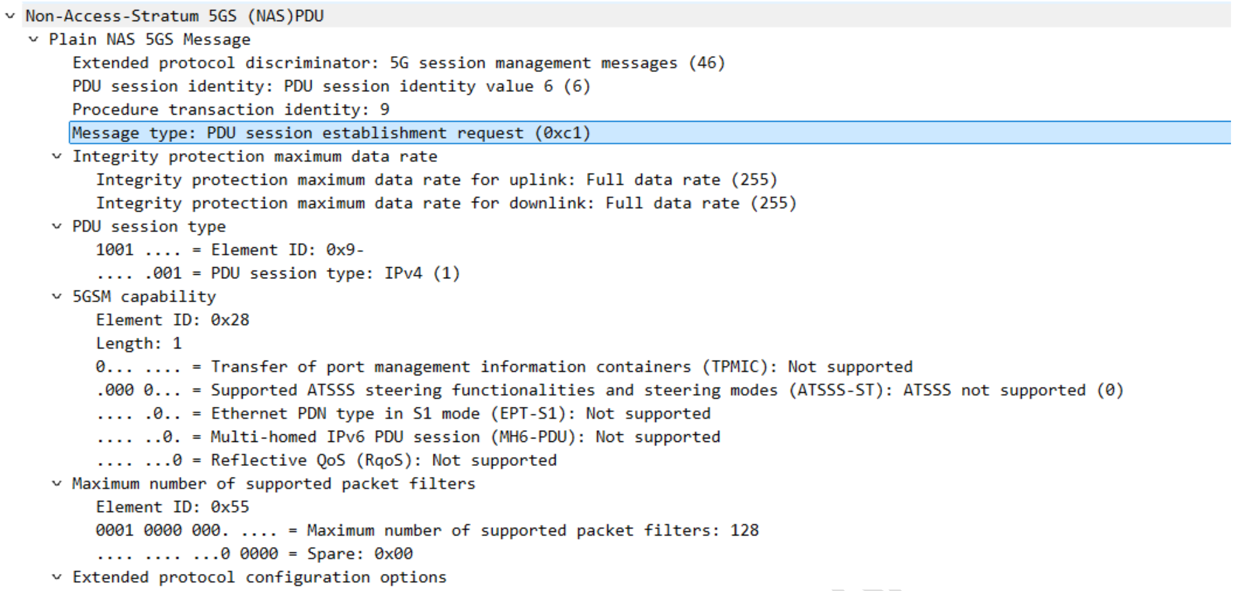
In SA mode, the 5G device communicates directly with a dedicated 5G core network, handling all aspects of connection management and data transfer through the 5G infrastructure.

e .PDU session establishment

PDU Session Establishment Request

UE →AMF

PDU Session Establishment is the process of establishing a data path between the UE and the 5G core network. A PDU session is a logical connection between the UE and a data network, such as the internet or a private network.



```
v Non-Access-Stratum 5GS (NAS)PDU
  v Plain NAS 5GS Message
      Extended protocol discriminator: 5G session management messages (46)
      PDU session identity: PDU session identity value 6 (6)
      Procedure transaction identity: 9
      Message type: PDU session establishment request (0xc1)
    v Integrity protection maximum data rate
        Integrity protection maximum data rate for uplink: Full data rate (255)
        Integrity protection maximum data rate for downlink: Full data rate (255)
    v PDU session type
        1001 .... = Element ID: 0x9-
        .... .001 = PDU session type: IPv4 (1)
    v 5GSM capability
        Element ID: 0x28
        Length: 1
        0... .... = Transfer of port management information containers (TPMIC): Not supported
        .000 0... = Supported ATSSS steering functionalities and steering modes (ATSSS-ST): ATSSS not supported (0)
        .... .0.. = Ethernet PDN type in S1 mode (EPT-S1): Not supported
        .... ..0. = Multi-homed IPv6 PDU session (MH6-PDU): Not supported
        .... ...0 = Reflective QoS (RqoS): Not supported
    v Maximum number of supported packet filters
        Element ID: 0x55
        0001 0000 000. .... = Maximum number of supported packet filters: 128
        .... .... ...0 0000 = Spare: 0x00
    v Extended protocol configuration options
```

PDU Session SM context Request

AMF → SMF

A "PDU session SM context request" refers to a message sent in a 5G network where AMF asks the Session Management Function (SMF) to retrieve or create a "Session Management Context" associated with a specific "Packet Data Unit (PDU) session," essentially requesting information about the active data connection for a particular user on the network to manage its QoS and routing details

PDU Session SM context Response

SMF → AMF

A "PDU session SM context response" refers to the data returned by a Session Management Function (SMF) in a 5G network, detailing the session context information associated with a specific PDU (Protocol Data Unit) session, which essentially represents a logical data connection between a user equipment (UE) and a data network; this response typically includes details like the PDU session ID, QoS parameters, allocated IP addresses, and other relevant information needed to manage the data flow for that session within the network.

PDU Session Resource Setup

AMF → gNB

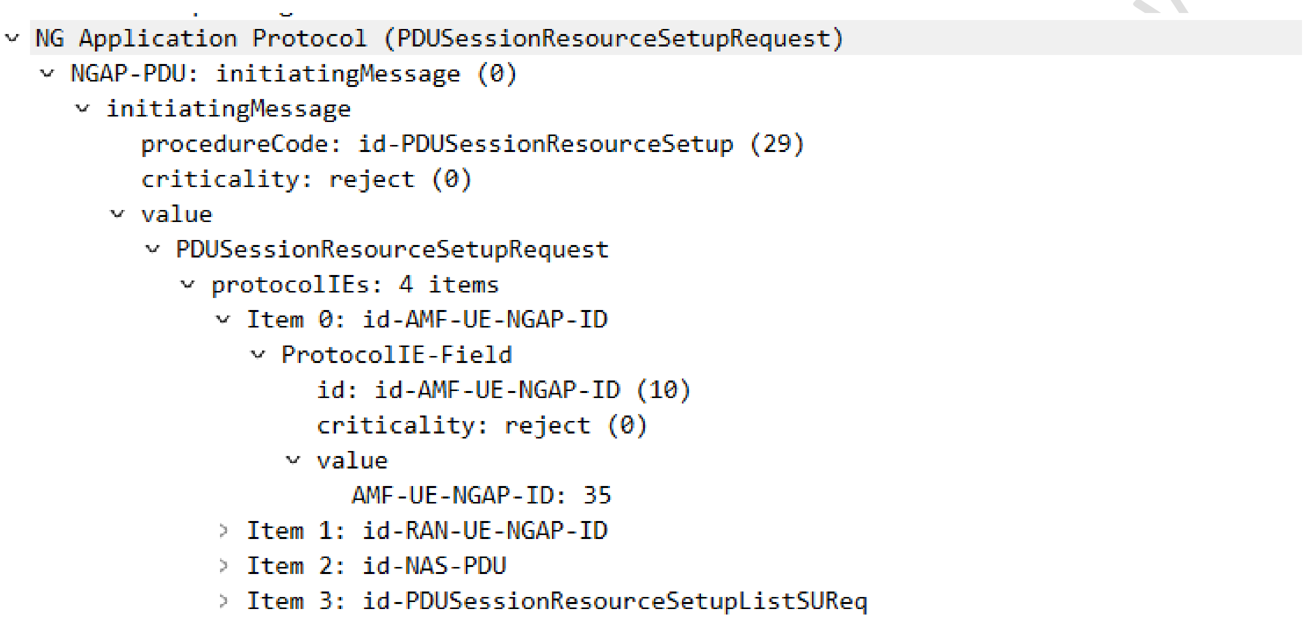
The purpose of the PDU Session Resource Setup procedure is to assign resources on Uu and NG-U for one or several PDU sessions and the corresponding QoS flows, and to setup corresponding DRBs for a given UE.

The AMF initiates the procedure by sending a PDU SESSION RESOURCE SETUP REQUEST message to the NG RAN node.

Upon reception of the PDU SESSION RESOURCE SETUP REQUEST message, if resources are available for the requested configuration, the NG-RAN node shall execute the requested NG-RAN configuration and allocate associated resources over NG and over Uu for each PDU sessions.

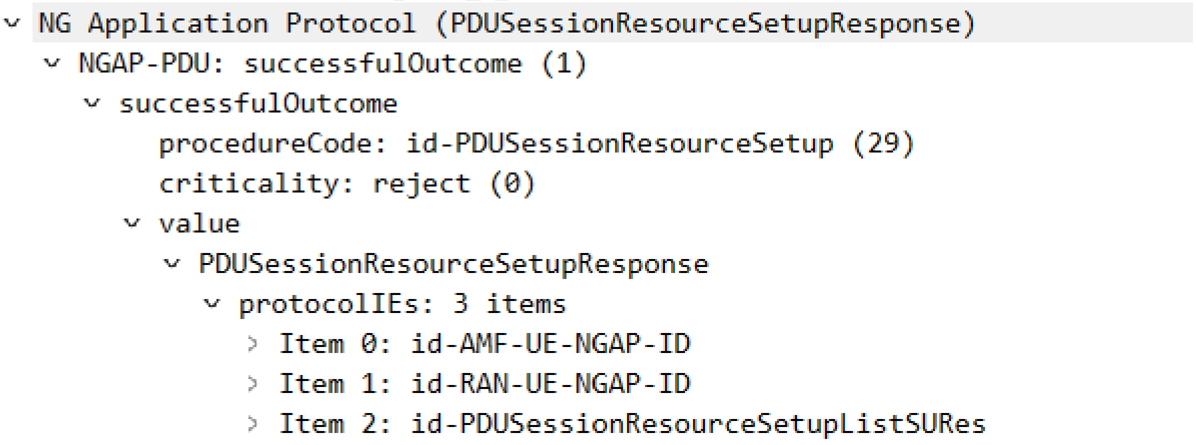
PDU Session Resource Setup

gNB → AMF



```
v NG Application Protocol (PDUSessionResourceSetupRequest)
  v NGAP-PDU: initiatingMessage (0)
    v initiatingMessage
        procedureCode: id-PDUSessionResourceSetup (29)
        criticality: reject (0)
      v value
        v PDUSessionResourceSetupRequest
          v protocolIEs: 4 items
            v Item 0: id-AMF-UE-NGAP-ID
              v ProtocolIE-Field
                  id: id-AMF-UE-NGAP-ID (10)
                  criticality: reject (0)
                v value
                    AMF-UE-NGAP-ID: 35
            > Item 1: id-RAN-UE-NGAP-ID
            > Item 2: id-NAS-PDU
            > Item 3: id-PDUSessionResourceSetupListSUReq
```

Figure 27 PDU Session Resource Setup



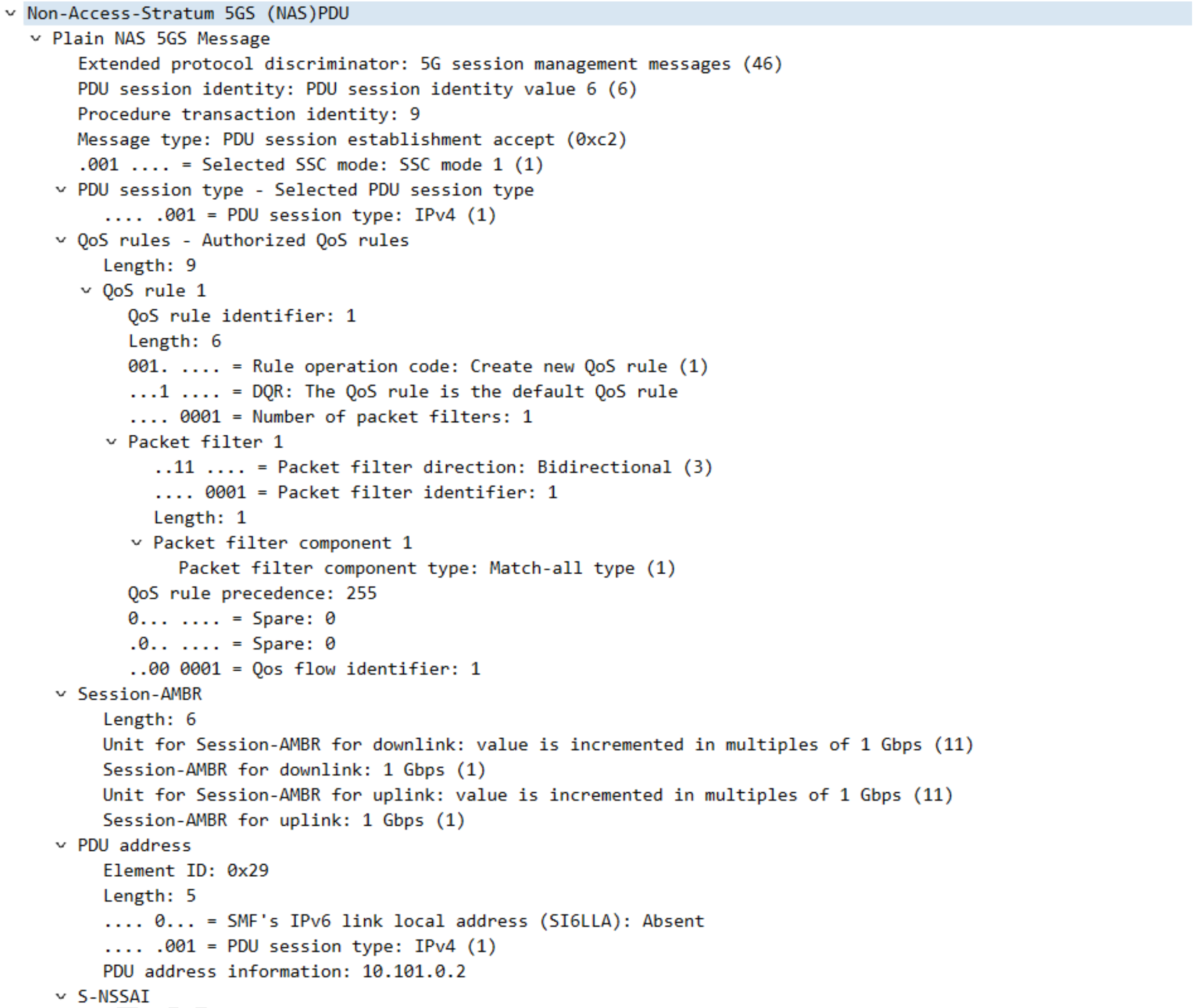
```
v NG Application Protocol (PDUSessionResourceSetupResponse)
  v NGAP-PDU: successfulOutcome (1)
    v successfulOutcome
        procedureCode: id-PDUSessionResourceSetup (29)
        criticality: reject (0)
      v value
        v PDUSessionResourceSetupResponse
          v protocolIEs: 3 items
            > Item 0: id-AMF-UE-NGAP-ID
            > Item 1: id-RAN-UE-NGAP-ID
            > Item 2: id-PDUSessionResourceSetupListSURes
```

Figure 28 PDU Session resource setup response

PDU Session Establishment Accept

AMF → UE

A PDU Session Establishment Accept is a message that the SMF sends to the UE to confirm that a PDU session has been established. The SMF includes QoS information in the PDU Session Establishment Accept message.



```
⌄ Non-Access-Stratum 5GS (NAS)PDU
  ⌄ Plain NAS 5GS Message
      Extended protocol discriminator: 5G session management messages (46)
      PDU session identity: PDU session identity value 6 (6)
      Procedure transaction identity: 9
      Message type: PDU session establishment accept (0xc2)
      .001 .... = Selected SSC mode: SSC mode 1 (1)
    ⌄ PDU session type - Selected PDU session type
        .... .001 = PDU session type: IPv4 (1)
    ⌄ QoS rules - Authorized QoS rules
        Length: 9
      ⌄ QoS rule 1
          QoS rule identifier: 1
          Length: 6
          001. .... = Rule operation code: Create new QoS rule (1)
          ...1 .... = DQR: The QoS rule is the default QoS rule
          .... 0001 = Number of packet filters: 1
        ⌄ Packet filter 1
            ..11 .... = Packet filter direction: Bidirectional (3)
            .... 0001 = Packet filter identifier: 1
            Length: 1
          ⌄ Packet filter component 1
              Packet filter component type: Match-all type (1)
          QoS rule precedence: 255
          0... .... = Spare: 0
          .0.. .... = Spare: 0
          ..00 0001 = Qos flow identifier: 1
    ⌄ Session-AMBR
        Length: 6
        Unit for Session-AMBR for downlink: value is incremented in multiples of 1 Gbps (11)
        Session-AMBR for downlink: 1 Gbps (1)
        Unit for Session-AMBR for uplink: value is incremented in multiples of 1 Gbps (11)
        Session-AMBR for uplink: 1 Gbps (1)
    ⌄ PDU address
        Element ID: 0x29
        Length: 5
        .... 0... = SMF's IPv6 link local address (SI6LLA): Absent
        .... .001 = PDU session type: IPv4 (1)
        PDU address information: 10.101.0.2
    ⌄ S-NSSAI
```

Figure 29 PDU Session establishment Accept

e. Different bearers workflow.

In 5g the concept of the bearer establishment is called PDU session establishment procedure.

PDU Session Establishment is the process of establishing a data path between the UE and the 5G core network. A PDU session is a logical connection between the UE and a data network, such as the internet or a private network.

With the successful establishment of the PDU session with the network, the UE is then provided with

- PDU session identity
- PDU address:

For eg:

PDU session type = 3 (IPv4v6)

IPv6 = ::2001:468:3000:1

IPv4 = 192.168.4.2

- QoS Flow descriptions
- S-NSSAI (slice details)
- DNN (Data Network Name)

Etc.

For each connected device, there is one or more PDU sessions, each with one or more QoS flows and data radio bearers. The IP packets are mapped to the QoS flows according to the QoS requirements, for example in terms of delay or required data rate, as part of the UDF functionality in the core network.

Each packet can be marked with a QoS Flow Identifier (QFI) to assist uplink QoS handling. The second step, mapping of QoS flows to data radio bearers, is done in the radio-access network. Thus, the core network is aware of the service requirements, while the radio-access network only maps the QoS flows to radio bearers.

The QoS-flow-to-radio-bearer mapping is not necessarily a one-to-one mapping; multiple QoS flows can be mapped to the same data radio bearer (Fig. 6.5). There are two ways of controlling the mapping from quality-of-service flows to data radio bearers in the uplink: reflective mapping and explicit configuration. In the case of reflective mapping, which is a new feature in NR when connected to the 5G core network, the device observes the QFI in the downlink packets for the PDU session. This provides the device with knowledge about which IP flows are mapped to which QoS flow and radio bearer. The device then uses the same mapping for the uplink traffic.

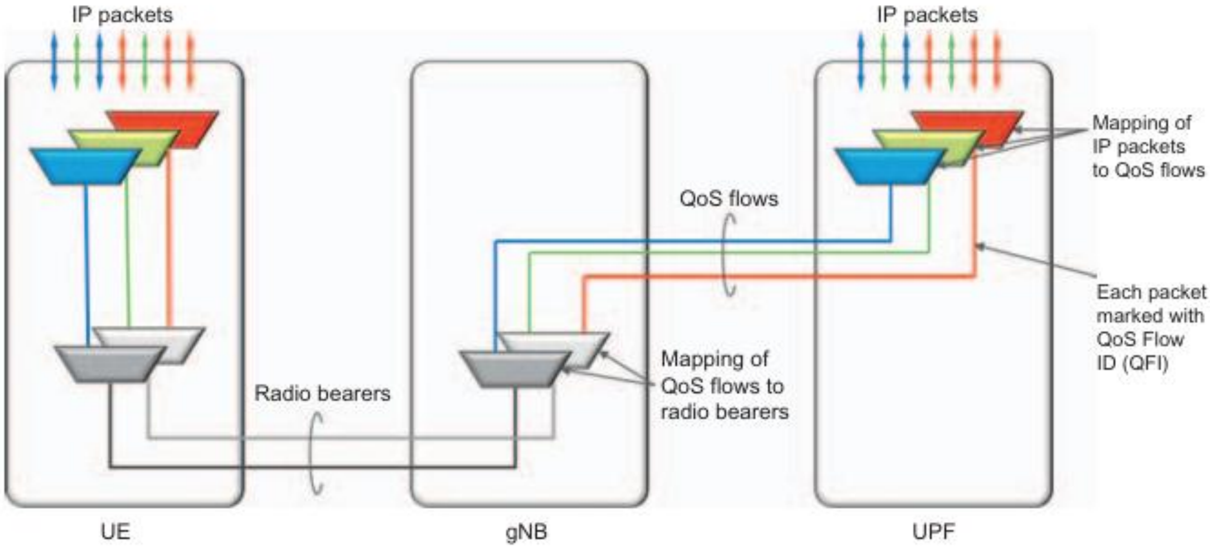

IP packets
IP packets
Mapping of IP packets to QoS flows
QoS flows
Each packet marked with QoS Flow ID (QFI)
Mapping of QoS flows to radio bearers
Radio bearers
UE
gNB
UPF

Figure 30 QoS flows in a PDU session

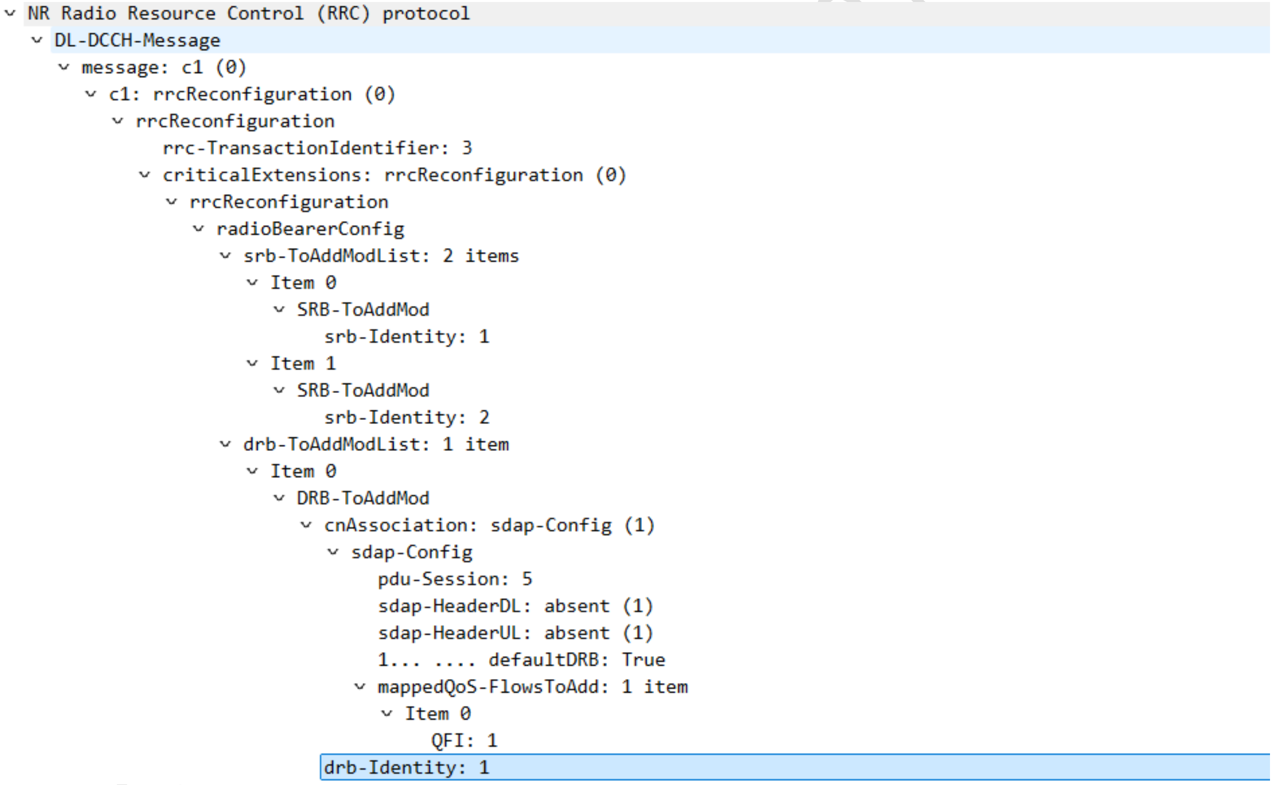
g.5G Voice Call and Data Call Connection Management Procedures

VoNR is in Roadmap.

h.5G Bearer Management Procedures

A PDU session (equivalent of the bearers in (LTE) is explained in the above sections which is at the UE and core level (NAS).

At the RAN level, the data radio bearers 'drbs' are created and sent to UE by the gNB in RRCReconfiguration message.



```
v NR Radio Resource Control (RRC) protocol
  v DL-DCCH-Message
    v message: c1 (0)
      v c1: rrcReconfiguration (0)
        v rrcReconfiguration
            rrc-TransactionIdentifier: 3
          v criticalExtensions: rrcReconfiguration (0)
            v rrcReconfiguration
              v radioBearerConfig
                v srb-ToAddModList: 2 items
                  v Item 0
                    v SRB-ToAddMod
                        srb-Identity: 1
                  v Item 1
                    v SRB-ToAddMod
                        srb-Identity: 2
                v drb-ToAddModList: 1 item
                  v Item 0
                    v DRB-ToAddMod
                      v cnAssociation: sdap-Config (1)
                        v sdap-Config
                            pdu-Session: 5
                            sdap-HeaderDL: absent (1)
                            sdap-HeaderUL: absent (1)
                            1... .... defaultDRB: True
                          v mappedQoS-FlowsToAdd: 1 item
                            v Item 0
                                QFI: 1
                      drb-Identity: 1
```

Figure 31 drbs in RRCReconfiguration.

i.5G Mobility Management and Session Management Procedures

5GMM

5G Mobile Management is involved mainly in NAS registration process and in terms of core network interface point of view, it is mostly associated with N1/N2 interface. This layer is residing on the UE and AMF.

Some of the major functions of 5GMM are:

registration

de-registration

network-initiated NAS transport

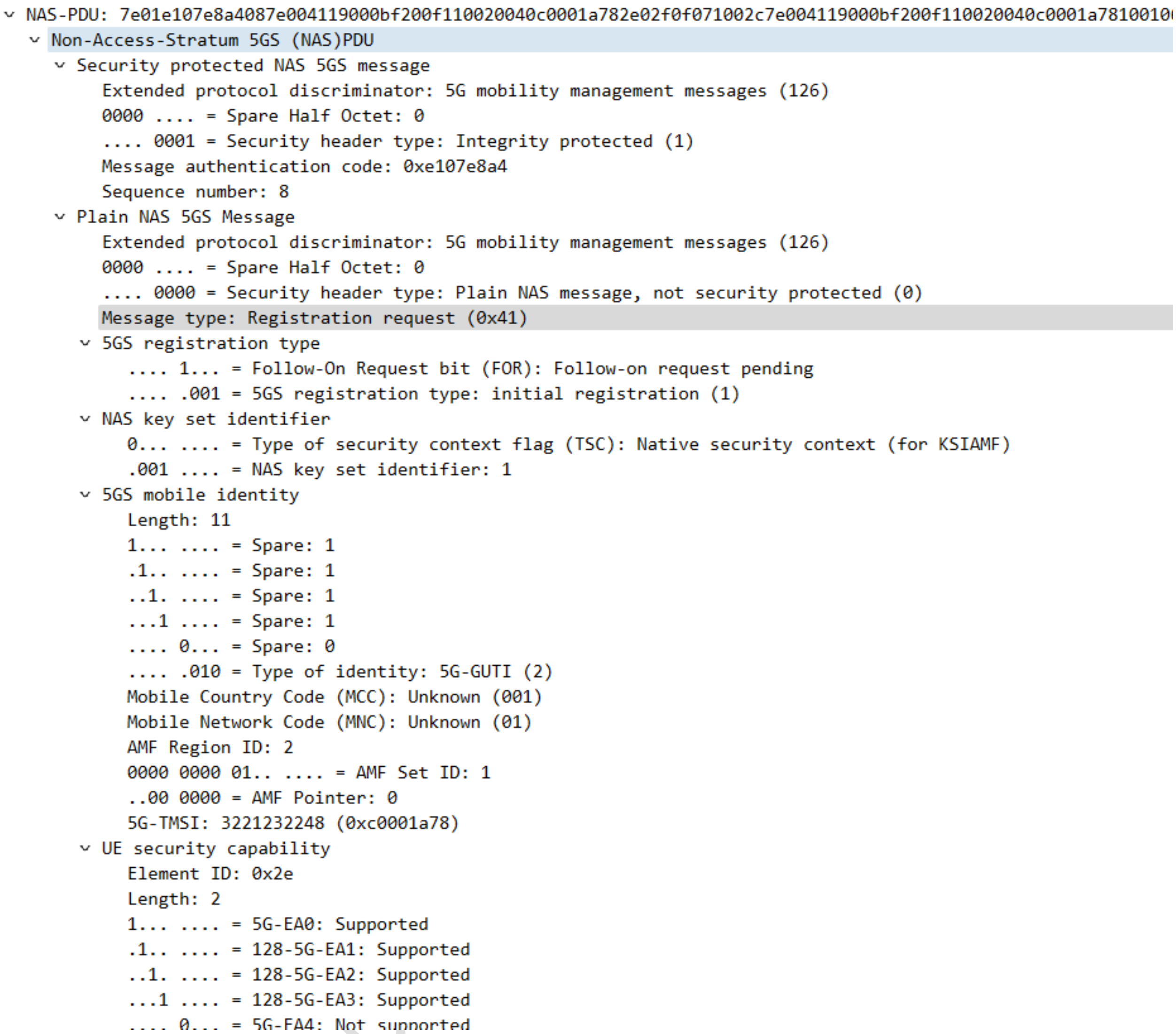
primary authentication and key agreement procedure

security mode control

identification

UE-initiated NAS transport

connection management procedure



```
v NAS-PDU: 7e01e107e8a4087e004119000bf200f110020040c0001a782e02f0f071002c7e004119000bf200f110020040c0001a7810010
  v Non-Access-Stratum 5GS (NAS)PDU
    v Security protected NAS 5GS message
        Extended protocol discriminator: 5G mobility management messages (126)
        0000 .... = Spare Half Octet: 0
        .... 0001 = Security header type: Integrity protected (1)
        Message authentication code: 0xe107e8a4
        Sequence number: 8
    v Plain NAS 5GS Message
        Extended protocol discriminator: 5G mobility management messages (126)
        0000 .... = Spare Half Octet: 0
        .... 0000 = Security header type: Plain NAS message, not security protected (0)
        Message type: Registration request (0x41)
      v 5GS registration type
          .... 1... = Follow-On Request bit (FOR): Follow-on request pending
          .... .001 = 5GS registration type: initial registration (1)
      v NAS key set identifier
          0... .... = Type of security context flag (TSC): Native security context (for KSIAMF)
          .001 .... = NAS key set identifier: 1
      v 5GS mobile identity
          Length: 11
          1... .... = Spare: 1
          .1.. .... = Spare: 1
          ..1. .... = Spare: 1
          ...1 .... = Spare: 1
          .... 0... = Spare: 0
          .... .010 = Type of identity: 5G-GUTI (2)
          Mobile Country Code (MCC): Unknown (001)
          Mobile Network Code (MNC): Unknown (01)
          AMF Region ID: 2
          0000 0000 01.. .... = AMF Set ID: 1
          ..00 0000 = AMF Pointer: 0
          5G-TMSI: 3221232248 (0xc0001a78)
      v UE security capability
          Element ID: 0x2e
          Length: 2
          1... .... = 5G-EA0: Supported
          .1.. .... = 128-5G-EA1: Supported
          ..1. .... = 128-5G-EA2: Supported
          ...1 .... = 128-5G-EA3: Supported
          .... 0... = 5G-EA4: Not supported
```

Figure 32 5G Registration Request message

5GSM

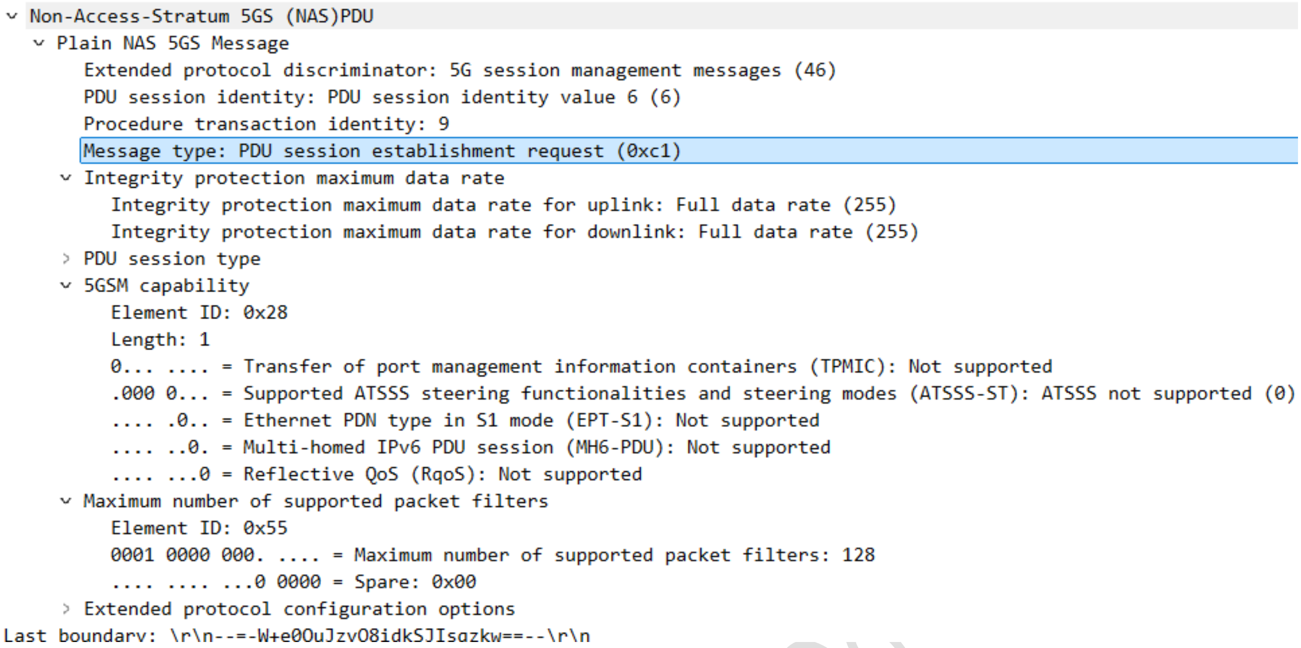
5G Session management is the layer which handles the PDN related procedures in the core network node SMF (Session Management Function).

Majorly its main functions are authentication and authorization,

PDU Session establishment

PDU Session modification

PDU session release



```
⌄ Non-Access-Stratum 5GS (NAS)PDU
  ⌄ Plain NAS 5GS Message
      Extended protocol discriminator: 5G session management messages (46)
      PDU session identity: PDU session identity value 6 (6)
      Procedure transaction identity: 9
      Message type: PDU session establishment request (0xc1)
    ⌄ Integrity protection maximum data rate
        Integrity protection maximum data rate for uplink: Full data rate (255)
        Integrity protection maximum data rate for downlink: Full data rate (255)
    › PDU session type
    ⌄ 5GSM capability
        Element ID: 0x28
        Length: 1
        0... .... = Transfer of port management information containers (TPMIC): Not supported
        .000 0... = Supported ATSSS steering functionalities and steering modes (ATSSS-ST): ATSSS not supported (0)
        .... .0.. = Ethernet PDN type in S1 mode (EPT-S1): Not supported
        .... ..0. = Multi-homed IPv6 PDU session (MH6-PDU): Not supported
        .... ...0 = Reflective QoS (RqoS): Not supported
    ⌄ Maximum number of supported packet filters
        Element ID: 0x55
        0001 0000 000. .... = Maximum number of supported packet filters: 128
        .... .... ...0 0000 = Spare: 0x00
    › Extended protocol configuration options
Last boundary: \r\n--=-W+e0OuJzvO8idkSJIsgzkw==--\r\n
```

Figure 18. PDU Session establishment

j. Testing of Data bearers

If user does Ping request from UE to Data Network (www.google.com), following can be seen in PCAP logs.

Echo (ping) request id=0x002a, seq=2/512, ttl=64 (reply in 11)

GPRS Tunneling Protocol
Flags: 0x34
Message Type: T-PDU (0xff)
Length: 92
TEID: 0x00002f82 (12162)
Next extension header type: PDU Session container (0x85)
Extension header (PDU Session container)

Internet Protocol Version 4, **Src: 101.202.0.2 (101.202.0.2), Dst: dns.google (8.8.8.8)**
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x662f (26159)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x5e9e [validation disabled]

[Header checksum status: Unverified]
Source Address: 101.202.0.2 (101.202.0.2)
Destination Address: dns.google (8.8.8.8)
[Stream index: 0]

Ping reply from DN to UE:

Echo (ping) reply id=0x002a, seq=2/512, ttl=55 (request in 6)

```
GPRS Tunneling Protocol
    Flags: 0x34
    Message Type: T-PDU (0xff)
    Length: 92
```

If user does Ping request from UE to Data Network (www.google.com), following can be seen in PCAP logs.

Echo (ping) request id=0x002a, seq=2/512, ttl=64 (reply in 11)

```
GPRS Tunneling Protocol
    Flags: 0x34
    Message Type: T-PDU (0xff)
    Length: 92
    TEID: 0x00002f82 (12162)
    Next extension header type: PDU Session container (0x85)
    Extension header (PDU Session container)

Internet Protocol Version 4, Src: 101.202.0.2 (101.202.0.2), Dst: dns.google (8.8.8.8)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x662f (26159)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x5e9e [validation disabled]


    [Header checksum status: Unverified]
    Source Address: 101.202.0.2 (101.202.0.2)
    Destination Address: dns.google (8.8.8.8)
    [Stream index: 0]
```

Ping reply from DN to UE:

Echo (ping) reply id=0x002a, seq=2/512, ttl=55 (request in 6)

```
GPRS Tunneling Protocol
    Flags: 0x34
    Message Type: T-PDU (0xff)
    Length: 92
    TEID: 0x00000001 (1)
    Next extension header type: PDU Session container (0x85)
    Extension header (PDU Session container)
Internet Protocol Version 4, Src: dns.google (8.8.8.8), Dst: 101.202.0.2 (101.202.0.2)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0000 (0)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 55
    Protocol: ICMP (1)
    Header Checksum: 0x0dce [validation disabled]
    [Header checksum status: Unverified]
    Source Address: dns.google (8.8.8.8)
    Destination Address: 101.202.0.2 (101.202.0.2)

    [Stream index: 0]
```

k. Verification of function blocks, APIs and Interfaces

Downlink and Uplink throughput tests

To test downlink and uplink throughput tests, iPerf application can be utilised. iPerf measures data between two peers by continuously sending the data. One of the peers will be the server and the other peer will be the client. The iPerf server will listen for the data and the iPerf client will pump the data.

```
#iPerf server-side command:

$ iperf -s -u -i 1 -I 1400 -p 10001

#iPerf client-side command:

$ iperf -c <ip addr of server> -u -I 1 -l 1400 -p
10001 -t 100000 -b <data rate to be tested in Mbps>
```

To test the data-rate in the downlink, UE should receive the data, so UE will act as the iPerf server, and gNodeB will act as the iPerf client.

To test the data rate in uplink, UE should transfer the data, so UE will act as the iPerf client and gNodeB will act as the iPerf server.

l. Multiple UE connections

Multiple UEs with preprogrammed SIM cards that are provided with 5G Lab can be connected to 5G Network.

l. Integration of application functions – Linphone for VoIP

Audio and video calls can be tested with VoIP server running on MEC. Linphone application can be installed on mobile phone to be able to connect with the VoIP server. App can be downloaded from App store or internet. Open the Linphone app on mobile phone and click on 4 horizontal bars as shown in the figure below:

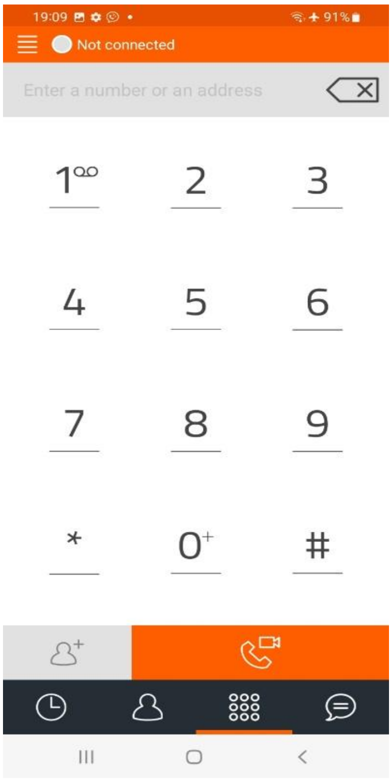
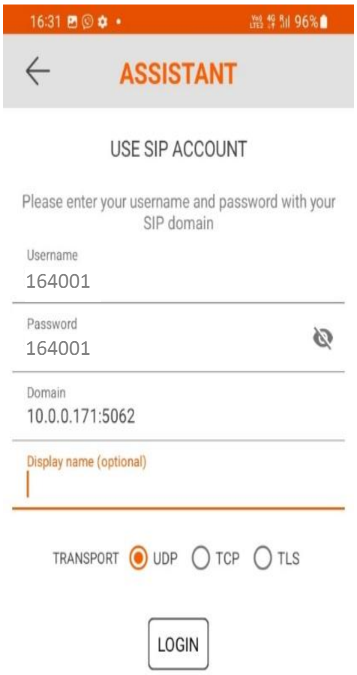


Figure 33 Linphone Default Screen

Then follow Assistant -> USE SIP ACCOUNT -> I Understand and fill information as shown below:



ASSISTANT

USE SIP ACCOUNT

Please enter your username and password with your SIP domain

Username
164001

Password
164001

Domain
10.0.0.171:5062

Display name (optional)

TRANSPORT ● UDP ○ TCP ○ TLS

Figure 34 Linphone User Settings

The default username and password set currently are for 2 Linphone users

User: 164001, Pwd: 164001

User: 164002, Pwd: 164002

m. Verification of use case applications

5G use case labs also contain other equipment that seamlessly integrates with the base station.

1 5G Core, 5G sims, 5G handsets and other network infrastructure: It enables data transfer and internet access services.

2 IoT gateway: With the rise in IoT technology, a lot of applications pertaining to remote farming, rural healthcare and many more can be developed using IoT sensors and can be integrated with 5G network using IoT gateway. Few relevant applications are described below-

Smart Home Automation/Smart Building/Smart Cities: Solutions can be done to better the traffic monitoring and control, energy-efficient street/building lighting, and connected appliances (smart refrigerators, ovens etc).

Healthcare and Wearable Technology: Remote health monitoring with wearable technology and smart medical devices like insulin implants help remote doctors check and treat patients.

Agriculture: IoT systems can enable precision farming, crop monitoring, livestock monitoring, automated irrigation etc. This solution along with data analysis will help farmers to get better yields.

Along with the above use cases, IoT technology will also make huge differences in automated and connected vehicles, energy management, environmental monitoring etc.

3 **5G Drone:** Drone technology is revolutionizing the fields of agriculture, delivery systems, surveillance etc. It is also enabling creation of accurate digital twin in massive scales.

4 **5G Indoor CPE:** It acts as a bridge between the 5G network and the user's devices, providing a local Wi-Fi network or wired connections for various devices within the premises. With this, non 5G based applications running on Wi-Fi/ Ethernet can also be integrated and developed.

5 **5G Camera:** With 5G camera and URLLC applications like remote surgery and diagnosis can be developed. This will be a crucial factor in improving rural healthcare.

10.AI/ML and IoT

1. Overview of AI/ML techniques

TBD

2. AI/ML applications for 5G

3. IoT Technology overview

TBD

4. IoT Use-cases and Deployment scenarios

TBD

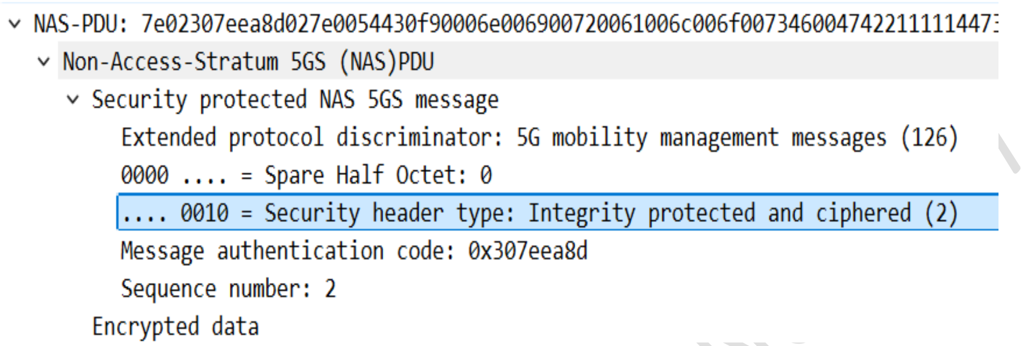
5. Integration of IoT in 3GPP Standards framework

TBD

11.QoS and Security

a. Security features for Core, RAN and devices

The AMF plays an important role in security, managing the encryption protocols and authentication mechanisms.



```
v NAS-PDU: 7e02307eea8d027e0054430f90006e006900720061006c006f0073460047422111114473
  v Non-Access-Stratum 5GS (NAS)PDU
    v Security protected NAS 5GS message
        Extended protocol discriminator: 5G mobility management messages (126)
        0000 .... = Spare Half Octet: 0
        .... 0010 = Security header type: Integrity protected and ciphered (2)
        Message authentication code: 0x307eea8d
        Sequence number: 2
      Encrypted data
```

Figure 35 Security Header in an AMF message

A "security protected NAS message" means that the signalling information exchanged between your mobile device and the cellular network is protected against tampering and unauthorized viewing. This is a fundamental part of maintaining the security and privacy of mobile communications.

b. Solution for internal and external attack vectors

TBD

c. Proactive security monitoring

TDB

d. Reporting and alarms

TBD

e. Security alerts storage including supporting data & logs

TBD

f. Security considerations in deployment of solution; interface and application level

TBD

12.Network Management System

a. Unified management layer across the 5G RAN and the 5G-Core xNFs (Virtual Network Functions: VNFs & Physical Network Functions: PNFs) providing functions such as

Resource Management (RM)

Fault Management (FM)

Performance Management (PM)

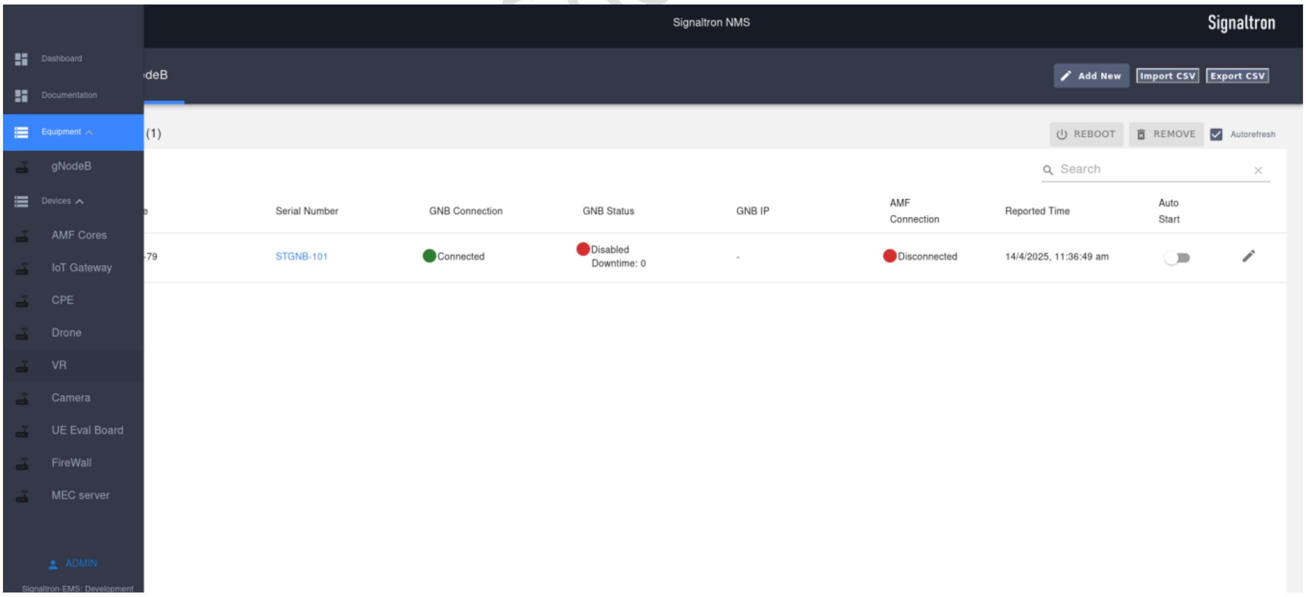
Configuration Management (CM)

The NMS (Network Management System) for gNodeB is the web server running on MEC through which we can monitor the gNodeB 5G statistics (currently: uptime, gNodeB run state and AMF/Core Connection state) and change specific gNodeB configurations (currently: Bandwidth and Centre frequency).

The NMS is installed on the MEC VM with ip address **192.168.10.12**; and is accessible on the entire 192 series local network with the following web address, just put the following after opening firefox:

192.168.10.12:3005

Username: admin; Password: admin



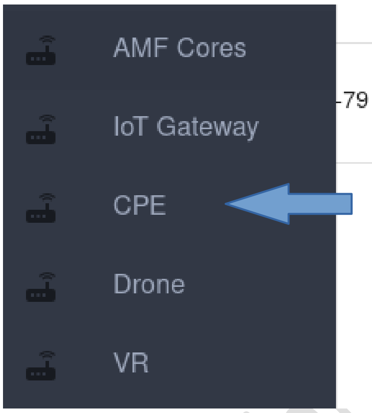
e	Serial Number	GNB Connection	GNB Status	GNB IP	AMF Connection	Reported Time	Auto Start
-79	STGNB-101	● Connected	● Disabled Downtime: 0	-	● Disconnected	14/4/2025, 11:36:49 am	

This is a one-stop shop to monitor all the devices that are part of the 5G Lab kit. The user can log into this portal and monitor the status of the connected devices such as CPE, drone, MEC, gNodeB, VR, camera, Firewall, IoT Gateway, etc.

The dashboard provides a comprehensive real-time view of all connected devices and the operational status of the devices within the network infrastructure. This default view shows the gNodeB status; rest of the devices can be accessed by going to left side navigation bar and selecting the desired device.

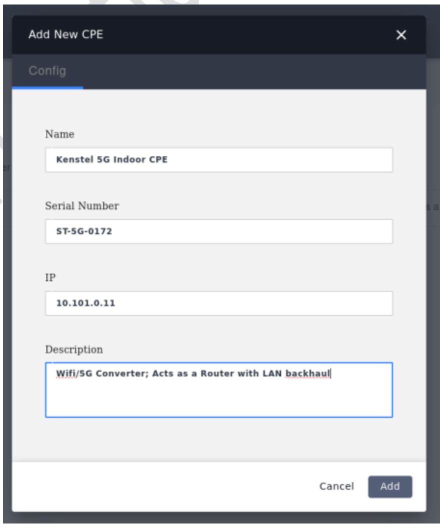
Setting up a device for status monitoring and accessing it's GUI can be done after following the steps given below. The prerequisites in the process are knowing the IP addresses (LAN and Sim Card) of the device.

1. Let's say we wish to set up a CPE device in our NMS. First, Click on CPE in the navigation bar.



2. Now the CPE dashboard page will open up. Click on button on the top right. A pop-up with details regarding CPE (device) will open up.

3. Fill the details as follows. We have used a default IP Address, enter the details according to your Lab setup.



Add New CPE ✕

Config

Name: Kenstel 5G Indoor CPE

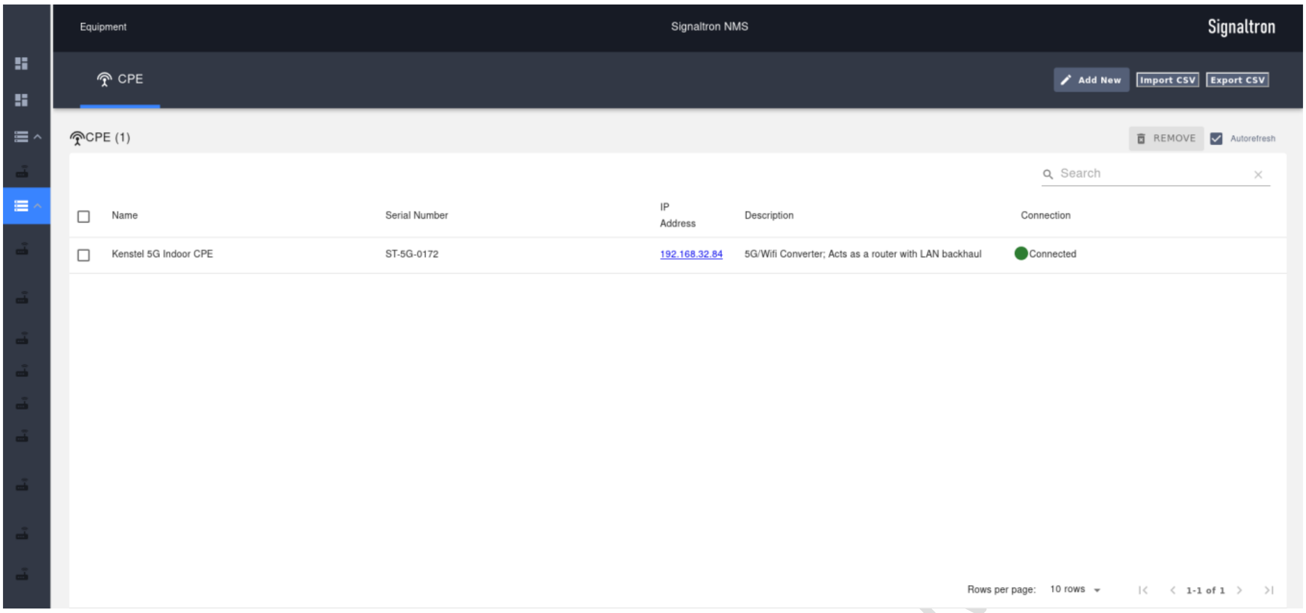
Serial Number: ST-5G-0172

IP: 10.101.0.11

Description: Wifi/5G Converter; Acts as a Router with LAN backhaul

Cancel Add

4. After pressing **Add**, on CPE dashboard you will be able to see a new row added. It shows the connection status and hyperlink to redirect to the device GUI.



Equipment — Signaltron NMS — Signaltron

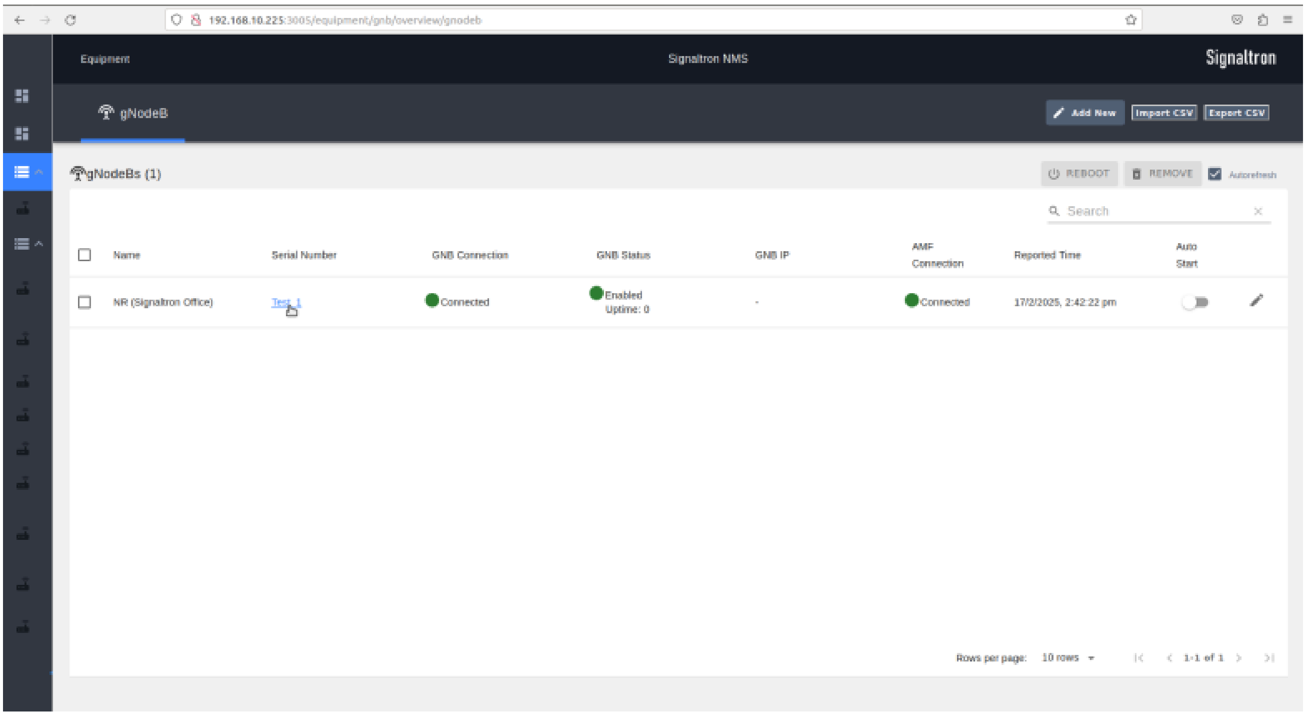
CPE (1)

□	Name	Serial Number	IP Address	Description	Connection
□	Kenstel 5G Indoor CPE	ST-5G-0172	192.168.32.84	5G/Wifi Converter; Acts as a router with LAN backhaul	● Connected

b. Configuring gNodeB

i. Changing Bandwidth of the gNodeB

After login, the gNodeB dashboard will be visible. The page would look as follows:



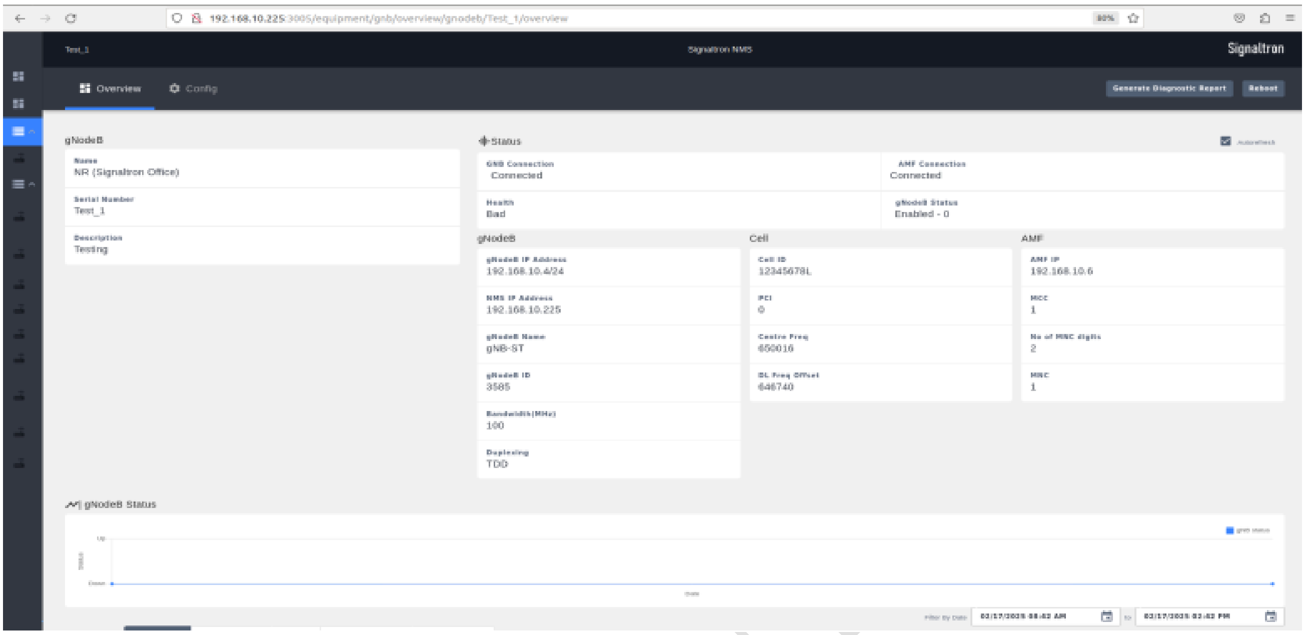
192.168.10.225:3005/equipment/gnb/overview/gnodeb

Equipment — Signaltron NMS — Signaltron

gNodeBs (1)

□	Name	Serial Number	GNB Connection	GNB Status	GNB IP	AMF Connection	Reported Time	Auto Start
□	NR (Signaltron Office)	Test_1	● Connected	● Enabled Uptime: 0	-	● Connected	17/2/2025, 2:42:22 pm	

Now, for gNodeB specific configurations; click on the Serial Number's (Here, Test_1) hyperlink. It will take you to the gNodeB overview page where the following information is visible:



192.168.10.225:3005/equipment/gnb/overview/gnodeb/Test_1/overview

Test_1 — Signaltron NMS

gNodeB

Name: NR (Signaltron Office)
Serial Number: Test_1
Description: Testing

Status

GNB Connection: Connected
AMF Connection: Connected
Health: Bad
gNodeB Status: Enabled - 0

gNodeB

gNodeB IP Address: 192.168.10.4/24
NMS IP Address: 192.168.10.225
gNodeB Name: gNB-ST
gNodeB ID: 3585
Bandwidth(MHz): 100
Duplexing: TDD

Cell

Cell ID: 12345678L
PCI: 0
Centre Freq: 650016
DL Freq Offset: 646740

AMF

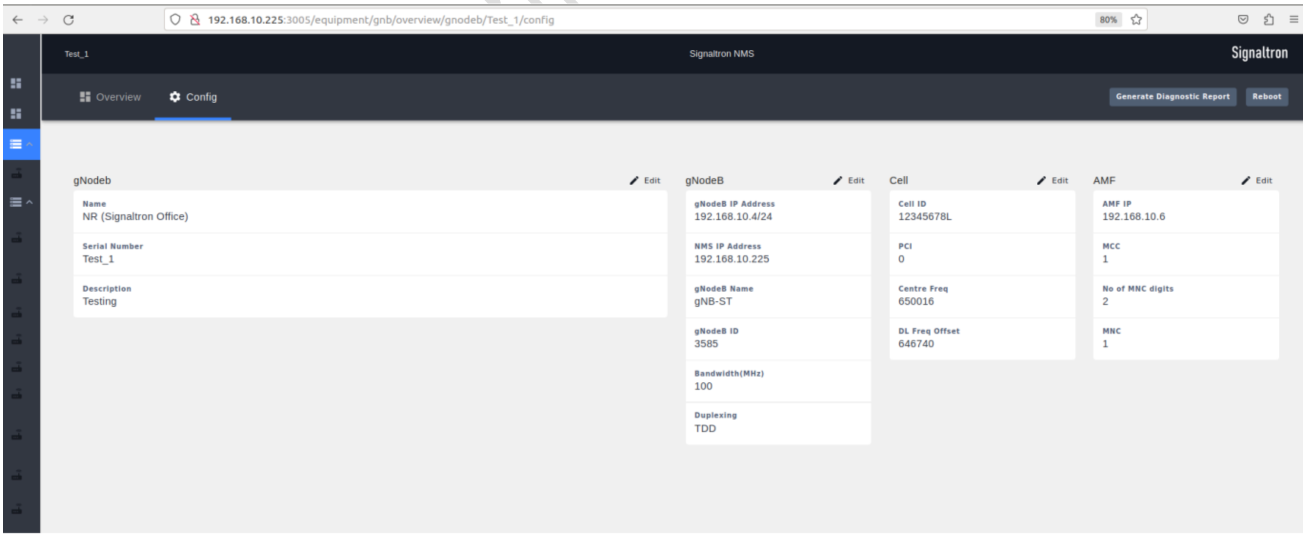
AMF IP: 192.168.10.6
MCC: 1
No of MNC digits: 2
MNC: 1

gNodeB Status

This information includes, connection states, IP addresses of gNodeB and NMS, gNB ID, Bandwidth, Duplexing, Cell ID, PCI, Centre Frequency, DL absolute frequency point A, PLMN details of Core.

The gNodeB status graph reflects the uptime and downtime of the gNodeB process. Some of the above parameters, Bandwidth and Centre Frequency are configurable.

They can be configured from the following config page:



192.168.10.225:3005/equipment/gnb/overview/gnodeb/Test_1/config

Test_1 — Signaltron NMS

gNodeb

Name: NR (Signaltron Office)
Serial Number: Test_1
Description: Testing

gNodeB

gNodeB IP Address: 192.168.10.4/24
NMS IP Address: 192.168.10.225
gNodeB Name: gNB-ST
gNodeB ID: 3585
Bandwidth(MHz): 100
Duplexing: TDD

Cell

Cell ID: 12345678L
PCI: 0
Centre Freq: 650016
DL Freq Offset: 646740

AMF

AMF IP: 192.168.10.6
MCC: 1
No of MNC digits: 2
MNC: 1

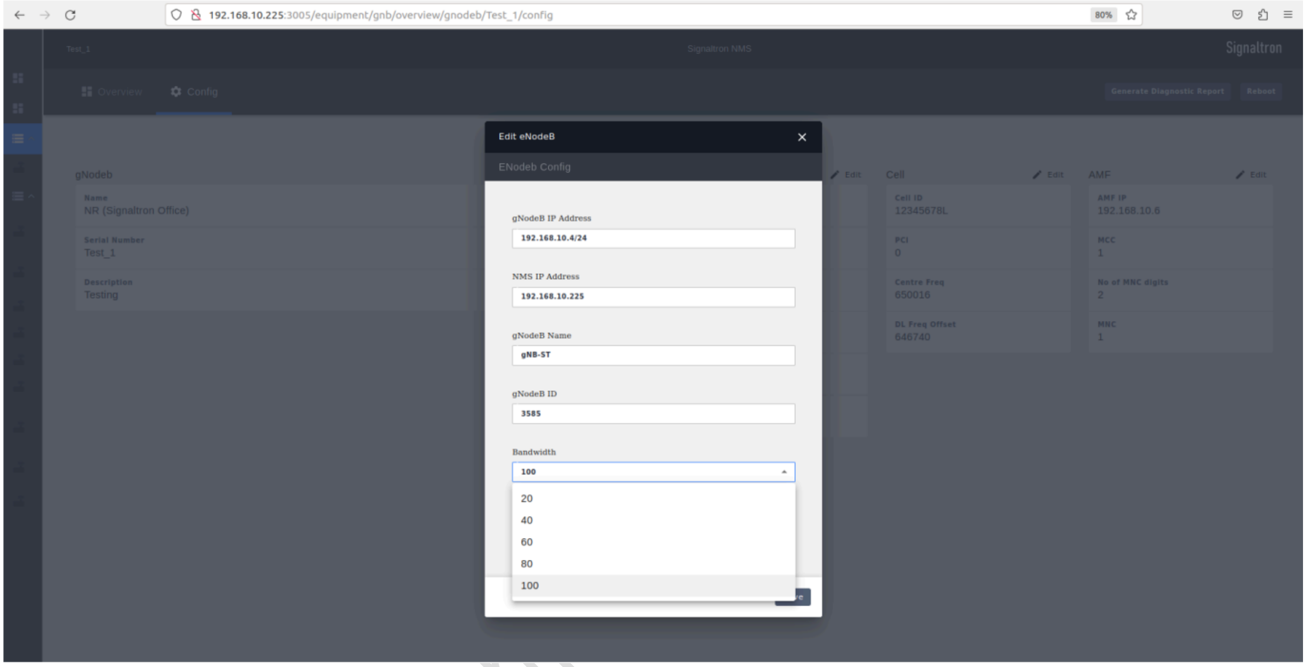
Configurability

Steps to Change Bandwidth of gNodeB:

1. Navigate to the config tab of a gNodeB, a page same as the above figure will open.

2. Click on the Edit button on top of the gNodeB table on the page.

3. Following dialog box will open up:



192.168.10.225:3005/equipment/gnb/overview/gnodeb/Test_1/config

Test_1 — Signaltron NMS — Signaltron

Overview | Config | Generate Diagnostic Report | Reboot

gNodeb
Name: NR (Signaltron Office)
Serial Number: Test_1
Description: Testing

Cell
Cell ID: 12345678L
PCI: 0
Centre Freq: 650016
DL Freq Offset: 646740

AMF
AMF IP: 192.168.10.6
MCC: 1
No of MNC digits: 2
MNC: 1

Edit eNodeB
ENodeb Config
gNodeB IP Address: 192.168.10.4/24
NMS IP Address: 192.168.10.225
gNodeB Name: gNB-ST
gNodeB ID: 3585
Bandwidth: 100

Select the appropriate bandwidth that you wish to run the gNodeB on, and press save on the bottom right of the dialog box.

4. The gNodeB will shut down after 10s. Manually press the power button on gNodeB to start it again. It will now boot with the newly selected bandwidth.

5. Wait for 3 minutes after gNodeB bootup, the gNodeB process will now start, the GNB status will show connected on the dashboard and you can start connecting devices.

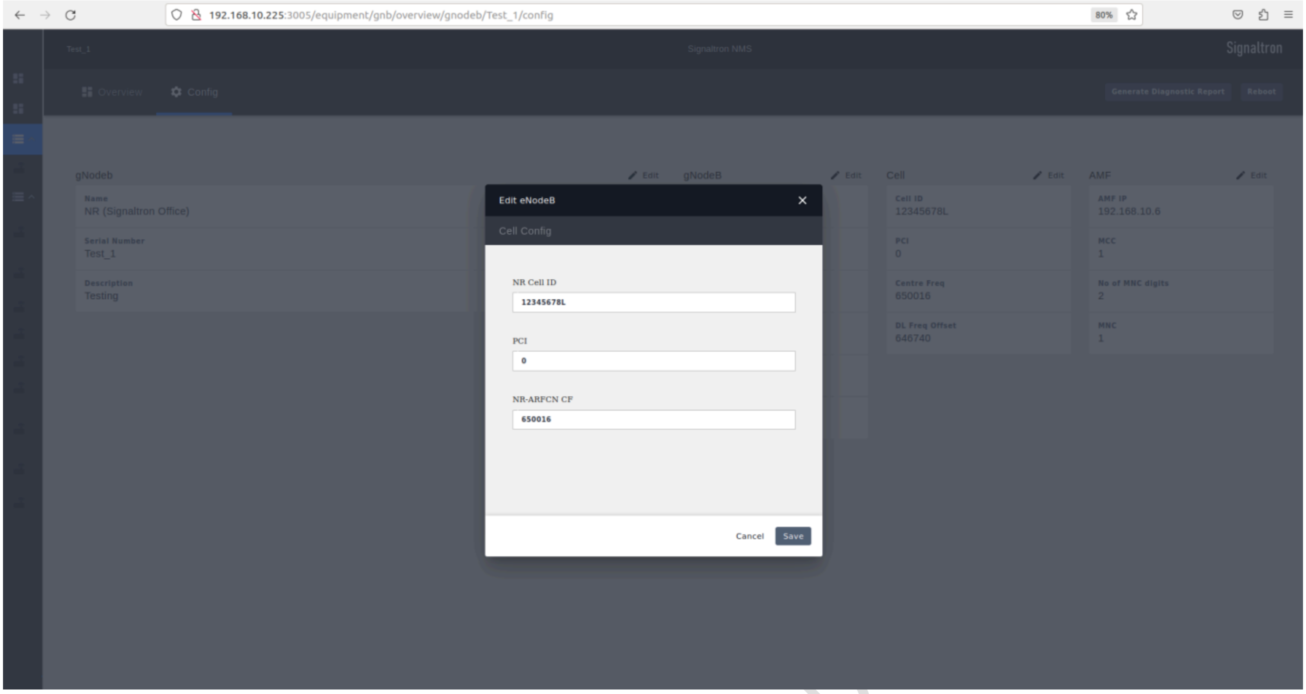
ii. Changing centre frequency of the gNodeB

Steps to change Centre Frequency of gNodeB:

Although the best frequency to run the gNodeB without clashing with any live networks (Jio, Airtel) is 3750 Mhz, there is provision to change the Centre Frequency of the gNodeB using NMS. The steps involved are as follows:

1. Click on the Cell Edit button on top of the Cell table in the config page.

2. Following dialog box will open up:



192.168.10.225:3005/equipment/gnb/overview/gnodeb/Test_1/config

Test_1

Signaltron NMS

Signaltron

Overview | Config

Generate Diagnostic Report | Reboot

gNodeb

Name: NR (Signaltron Office)

Serial Number: Test_1

Description: Testing

Cell

Cell ID: 12345678L

PCI: 0

Centre Freq: 650016

DL Freq Offset: 646740

AMF

AMF IP: 192.168.10.6

MCC: 1

No of MNC digits: 2

MNC: 1

Edit eNodeB

Cell Config

NR Cell ID: 12345678L

PCI: 0

NR-ARFCN CF: 650016

Cancel | Save

Input the appropriate Centre Frequency that you wish to run the gNodeB on, and press save on the bottom right of the dialog box.

3. The gNodeB will shut down after 10s. Manually press the power button on gNodeB to start it again. It will now boot with the newly set Centre Frequency.

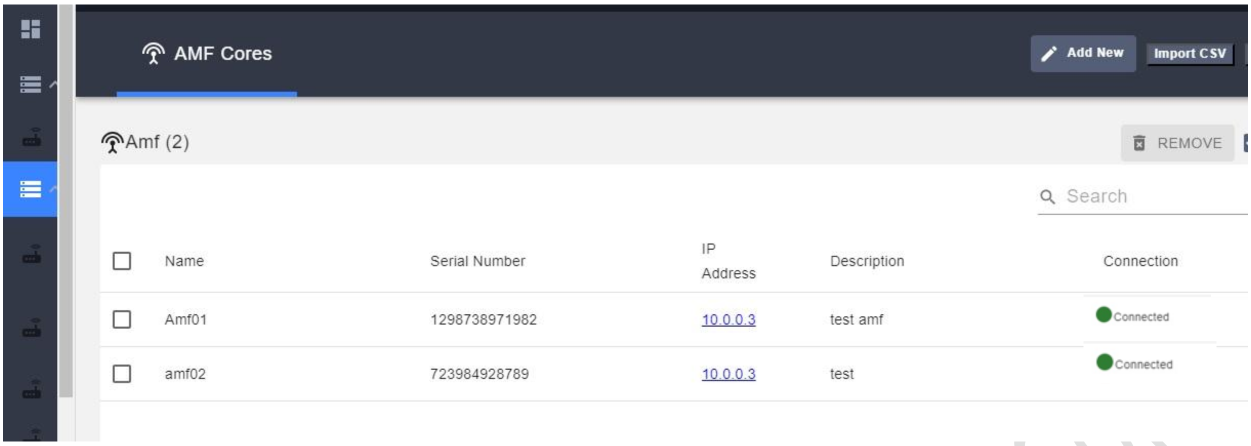
4. Wait for 3 minutes after gNodeB bootup, the gNodeB process will now start, the GNB status will show connected on the dashboard and you can start connecting devices.

Once the gNodeB is up, you can follow section-5, subsection- “Power on gNodeB and connect a UE” page.

The value 650016 in ARFCN corresponds to 3750 Mhz; run in this configuration for the most stable run.

Adding AMF and accessing AMF from NMS :-

The AMF (Access and Mobility Management Function), provides users with the ability to configure and manage the AMF settings for seamless mobility management and access control in 5G networks. It is a key component of the 5G core network that handles registration, connection, mobility, and access control for devices.



□	Name	Serial Number	IP Address	Description	Connection
□	Amf01	1298738971982	10.0.0.3	test amf	● Connected
□	amf02	723984928789	10.0.0.3	test	● Connected

Figure 36 AMF View

Open the Network Management System (NMS) application to begin the process of adding the AMF to dashboard.

On the left sidebar click on the devices section.

Then click on the AMF icon that will open its page.

Click on the "Add New" button to initiate the addition of AMF.

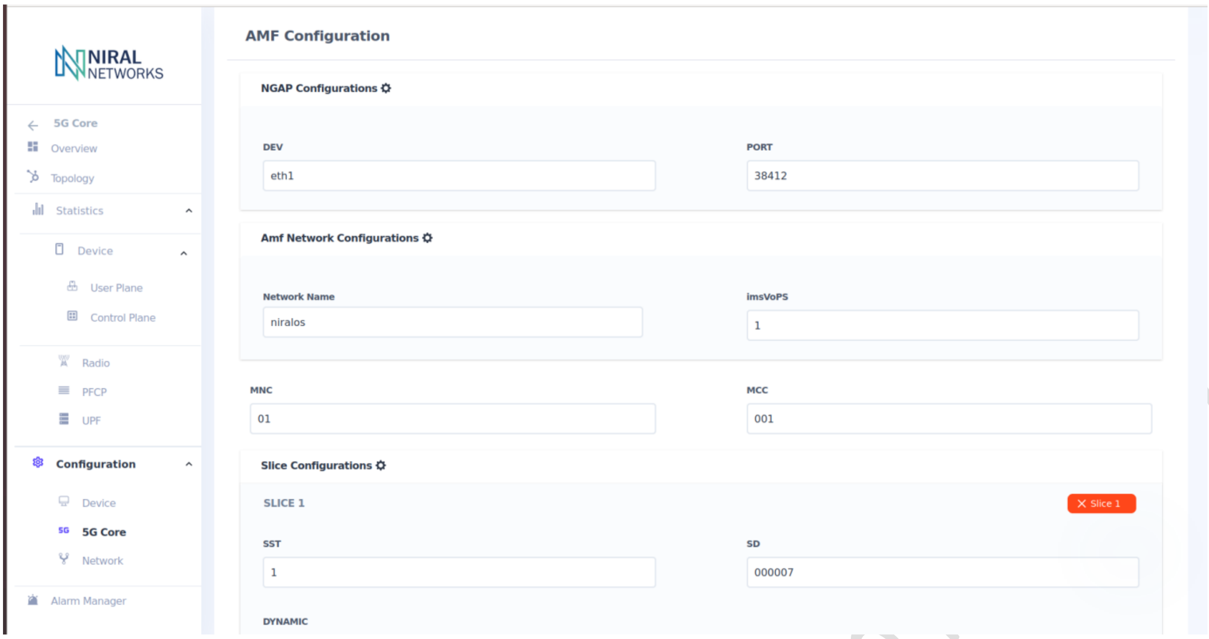
You will be prompted to enter key information about the AMF:

- Device Name
- IP Address

After entering the required details, click save.

The AMF will be added to the NMS dashboard.

Once the AMF is added to the NMS dashboard, by clicking on the IP link in the NMS dashboard, you will be taken directly to the configuration page of the AMF.



AMF Configuration

NGAP Configurations ⚙

DEV: eth1

PORT: 38412

Amf Network Configurations ⚙

Network Name: niralos

imsVoPS: 1

MNC: 01

MCC: 001

Slice Configurations ⚙

SLICE 1

SST: 1

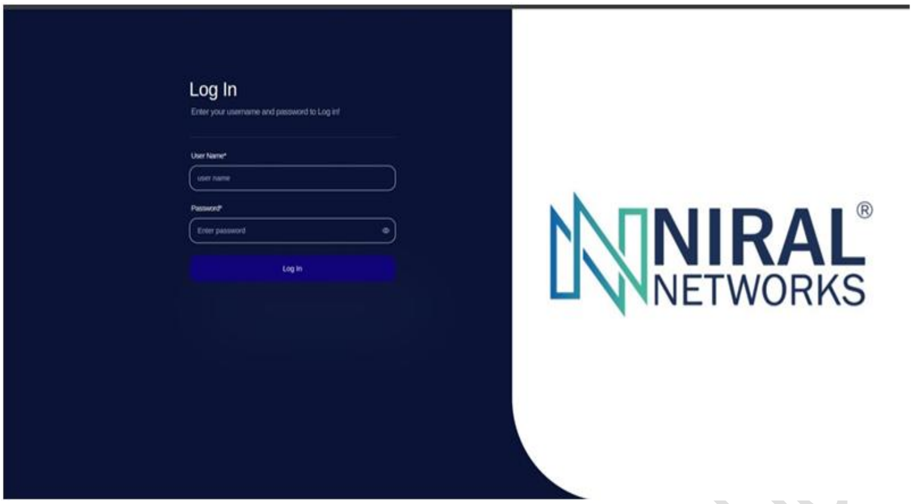
SD: 000007

DYNAMIC

Figure 37 AMF Dashboard

c. Accessing the Niral NMS

- In browser type http://192.168.10.5
- give user name as admin and password as admin@1234



Log In

Enter your username and password to Log in!

You can see in the Dashboard of Niral NMS, the number of cores, number of Radios and number of Devices.

Active Core in the below image indicates, number of cores that are connected to the NMS. **Active Radio** in below image indicates number of gNodeBs connected to NMS. **Registered Device** in below image indicates that number of UEs connected to the gNodeB.

Checking Registered Device count in NMS dashboard, will give a quick indication on whether the UE is connected to the 5G network or not.

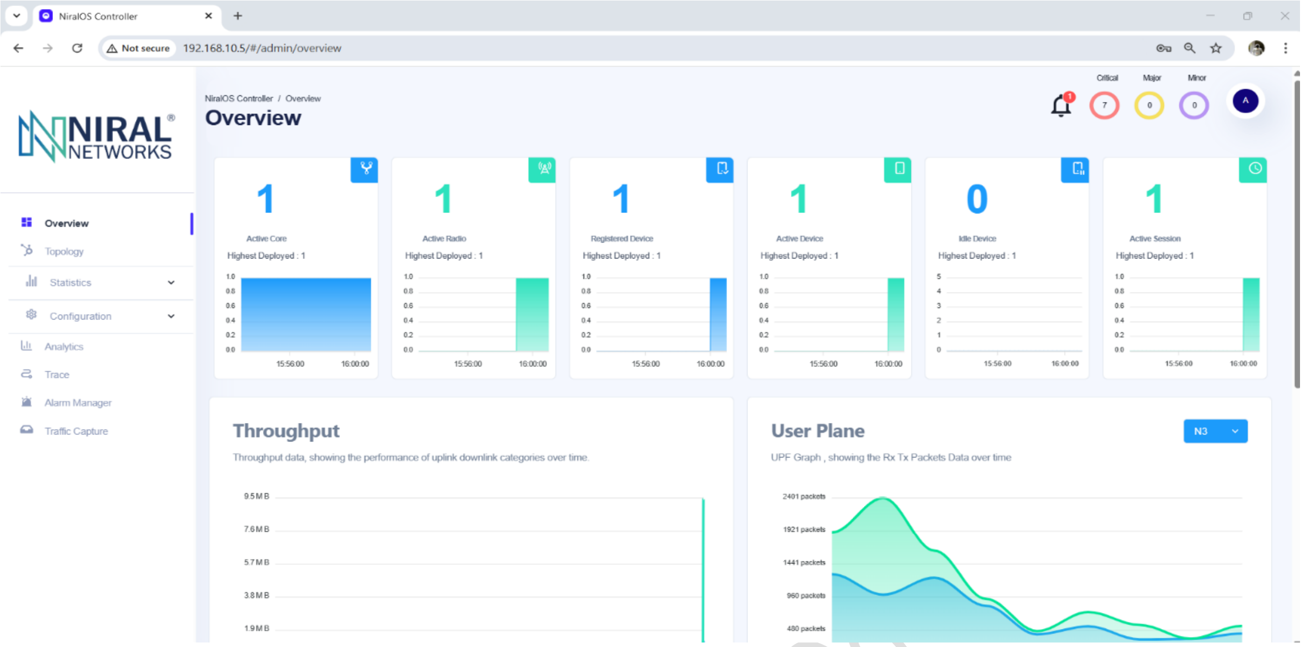


Figure 38 NMS Dashboard

Configuring of 5G Core

Configuring AMF PLMN ID

White listing of SIM cards with Authentication Keys

i. Map a fixed IP address (static ip address) to a SIM card

Steps to Hardcode SIM IP Address from Niral NMS:

1. Login to Niral NMS page
2. From the left-hand side menu, navigate as follows: **Configuration** -> **Sim** (refer **Figure 40**)
3. You will find a list of IMSIs of all the SIM Cards, note down the last four digits printed on the sim card and search for the same in search bar.
    a. For example, in the given image search for 2767 in the list

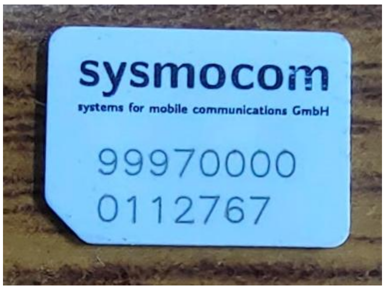
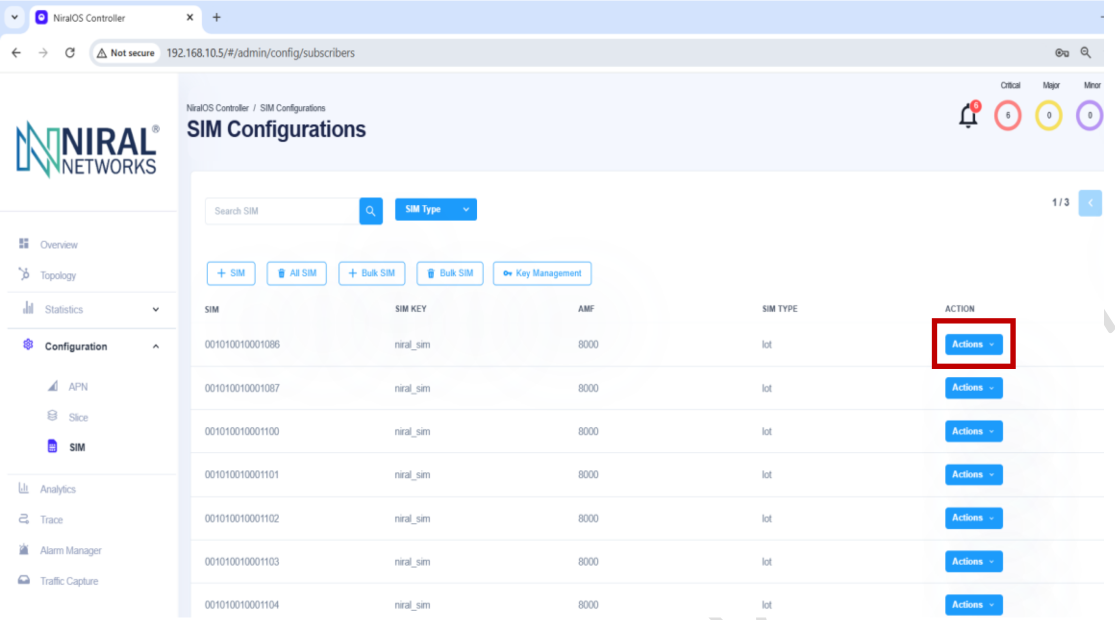


Figure 39 Adding camera in Core

4. Select the **Actions** button against your search result sim -> **Update Sim** in the drop-down menu which appears once **Actions** button is pressed



192.168.10.5/#/admin/config/subscribers

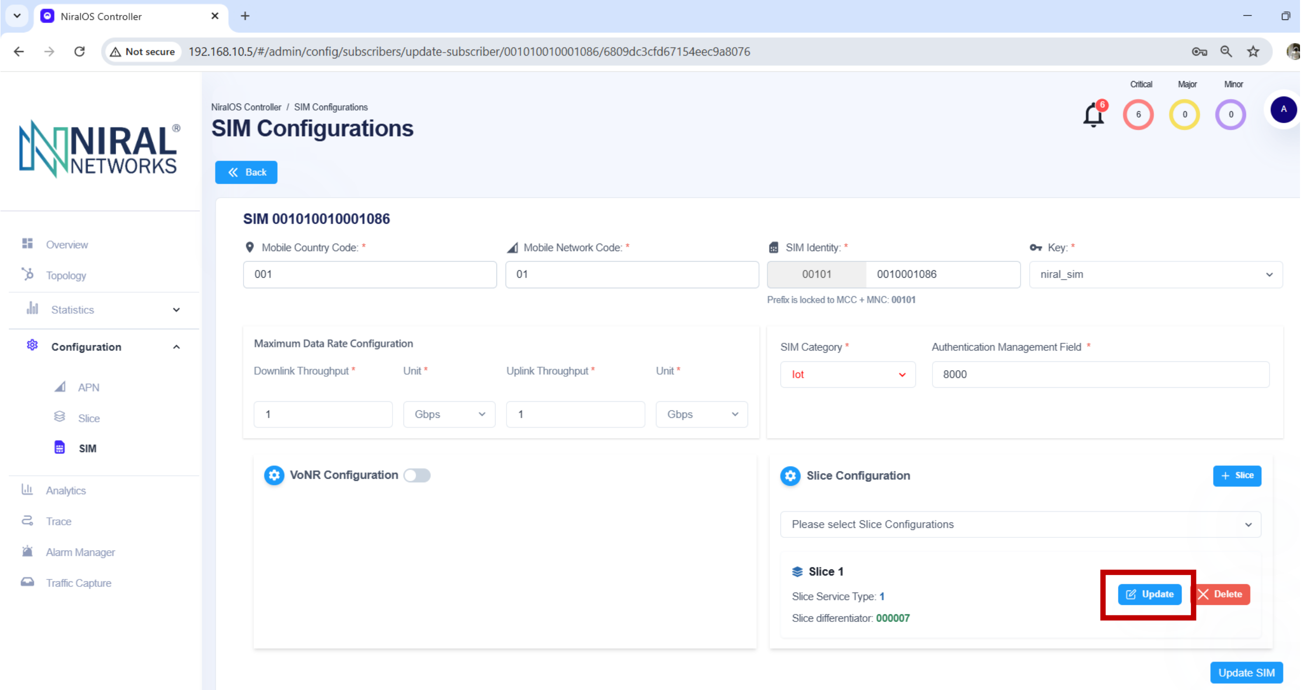
NiralOS Controller / SIM Configurations

SIM Configurations

SIM	SIM KEY	AMF	SIM TYPE	ACTION
001010010001086	niral_sim	8000	Iot	Actions
001010010001087	niral_sim	8000	Iot	Actions
001010010001100	niral_sim	8000	Iot	Actions
001010010001101	niral_sim	8000	Iot	Actions
001010010001102	niral_sim	8000	Iot	Actions
001010010001103	niral_sim	8000	Iot	Actions
001010010001104	niral_sim	8000	Iot	Actions

Figure 40 Sim configuration through NMS

5. Click on **Update** button as highlighted below



192.168.10.5/#/admin/config/subscribers/update-subscriber/001010010001086/6809dc3cfd67154eec9a8076

NiralOS Controller / SIM Configurations

SIM Configurations

SIM 001010010001086

Mobile Country Code: * 001

Mobile Network Code: * 01

SIM Identity: * 00101 0010001086

Prefix is locked to MCC + MNC: 00101

Key: * niral_sim

Maximum Data Rate Configuration

Downlink Throughput * 1 Unit * Gbps

Uplink Throughput * 1 Unit * Gbps

SIM Category * Iot

Authentication Management Field * 8000

VoNR Configuration

Slice Configuration

Please select Slice Configurations

Slice 1

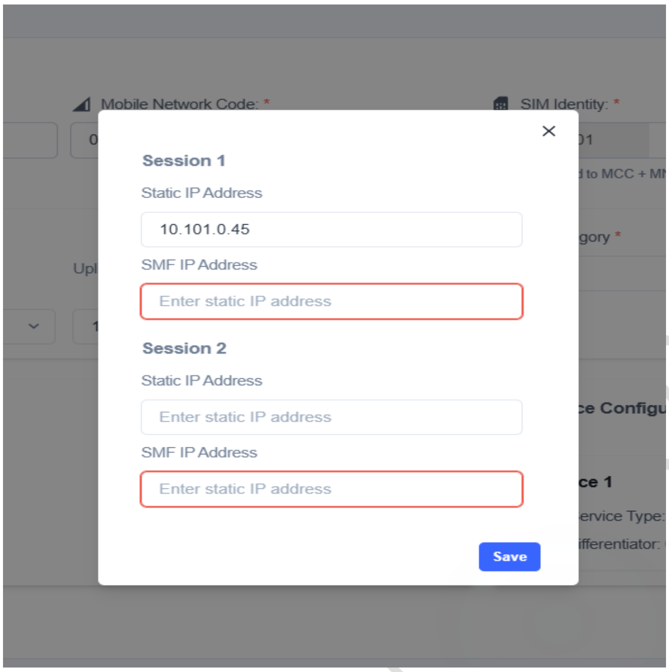
Slice Service Type: 1

Slice differentiator: 000007

Figure 41 SIM card page

6. Now enter the **static ip address** in **session-1**. The IP address should be in 10.101.0.x range (do not give 10.101.0.1 because that is the core network tunnel IP address)

7. Leave the SMF IP address blank and also session-2 values blank. Press on **save** button



Session 1

Static IP Address: 10.101.0.45

SMF IP Address: Enter static IP address

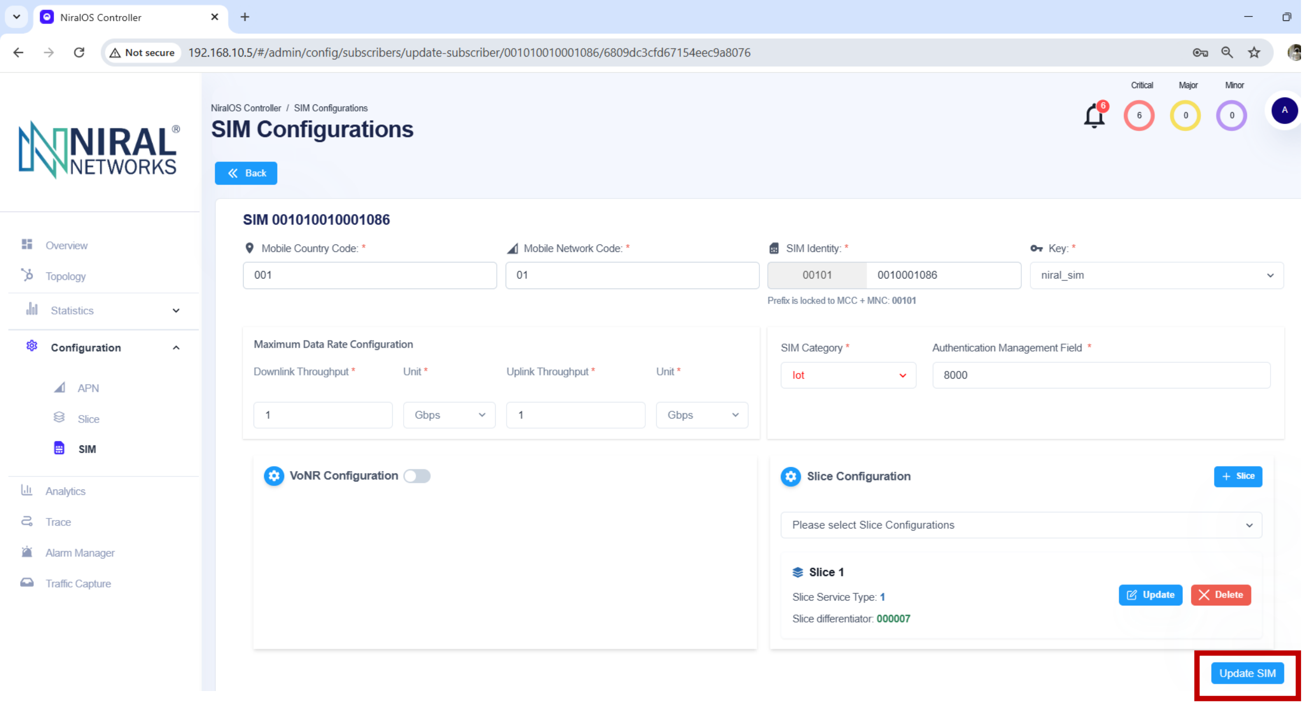
Session 2

Static IP Address: Enter static IP address

SMF IP Address: Enter static IP address

Figure 42 SIM static Ip configuration

8. Then press on **update sim** button at the bottom right
9. This will do a one-to-one mapping between SIM and its static IP address. This leads to hardcoding of the IP address of the device which has the mapped SIM in it.



192.168.10.5/#/admin/config/subscribers/update-subscriber/001010010001086/6809dc3cfd67154eec9a8076

NiralOS Controller / SIM Configurations

SIM Configurations

SIM 001010010001086

Mobile Country Code: * 001

Mobile Network Code: * 01

SIM Identity: * 00101 0010001086

Prefix is locked to MCC + MNC: 00101

Key: * niral_sim

Maximum Data Rate Configuration

Downlink Throughput * 1 Unit * Gbps

Uplink Throughput * 1 Unit * Gbps

SIM Category * Iot

Authentication Management Field * 8000

VoNR Configuration

Slice Configuration

Please select Slice Configurations

Slice 1

Slice Service Type: 1

Slice differentiator: 000007

Figure 43 SIM static IP configuration

d. Monitoring of 5G Network

a. Number of active devices

Can be verified from the dashboard of Niral NMS

b. Data Usage per device

TBD

c. Resource Management

TBD

d. Performance Management

TBD

e. Fault Management

TBD

13.5G Evaluation board/Hardware & Software development Kit

A 5G UE Evaluation board has been provided in the lab setup. This is a UE platform to help student learn for developing software and applications. A hardware evaluation board is a crucial hardware tool that allows users to test, prototype, and validate 5G technology or components in a controlled environment before full deployment. This board replicates the final hardware setup but offers flexibility for development and testing.

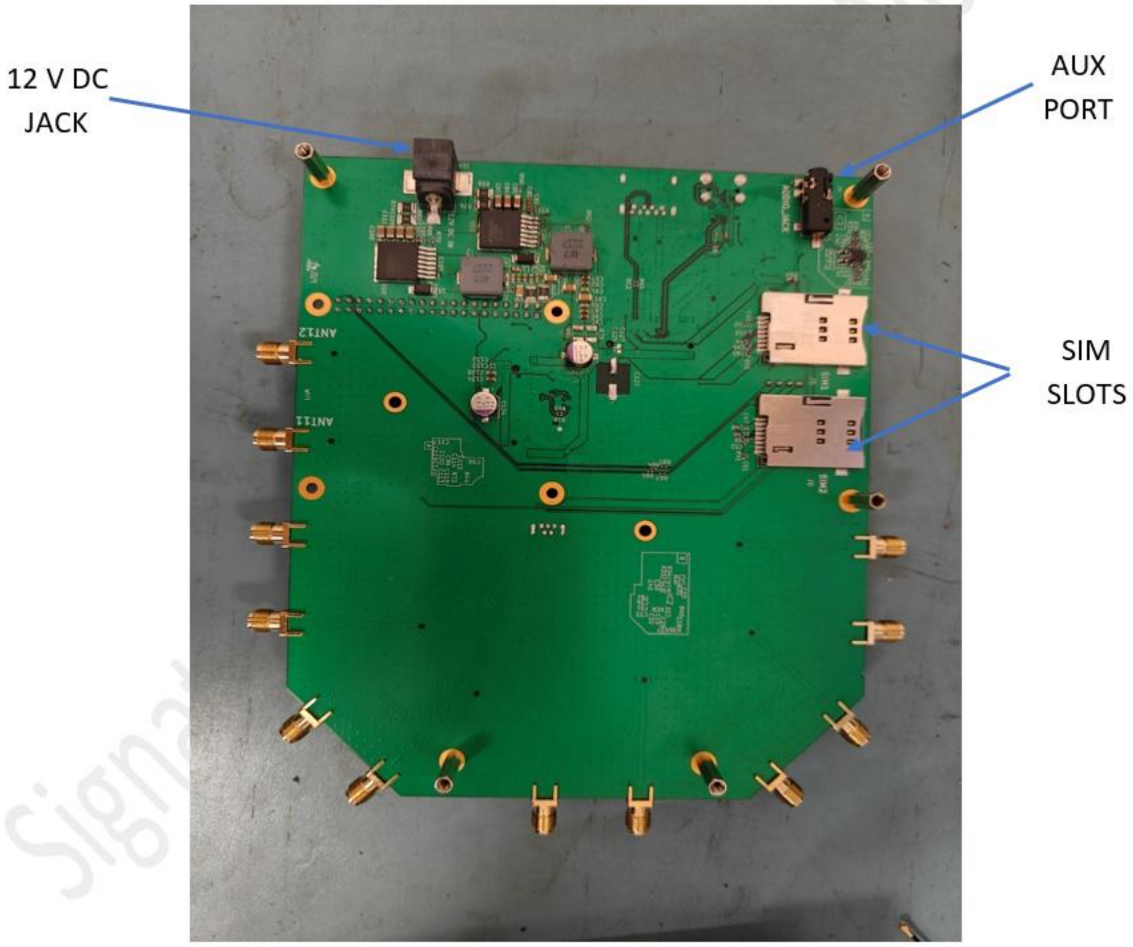


Figure 44 Eval board bottom

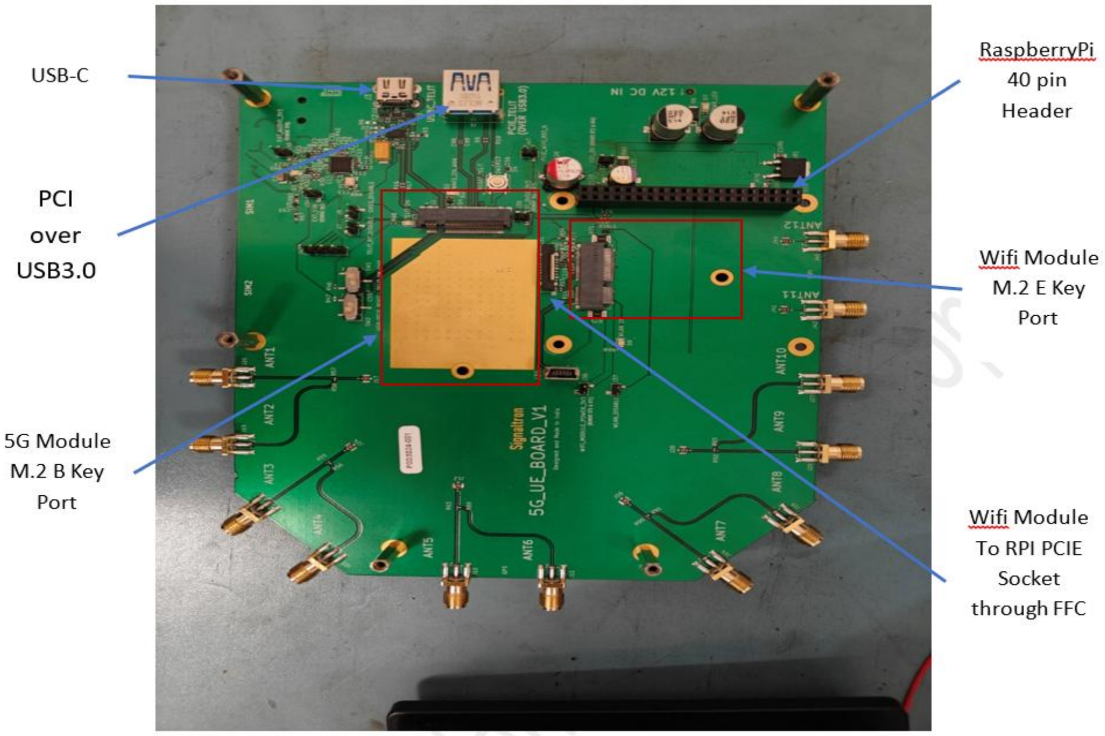

USB-C
PCI over USB3.0
5G Module M.2 B Key Port
RaspberryPi 40 pin Header
Wifi Module M.2 E Key Port
Wifi Module To RPI PCIE Socket through FFC

Figure 45 Eval board Top

Power Supply

The Eval Board has a DC Jack (8) on board which needs a power supply of at least 12V, 4A output. Connectors J34, 46, 30, 32, 36 are test points for the various power domains in the Eval Board, nothing should to be connected to these pins. The various expected voltages are marked on the silkscreen beside the connectors.

5G Module

The Eval board has a 5G Module which provides 5G connectivity to systems. After booting up the Pi, if the board has a sim card inserted, mobile broadband settings will show up in the network settings accessed from the top right corner of the screen. If the APN settings are valid then the RPI will gain 5G Connectivity. The LED color of Green indicates that the evaluation board has completed the bootup

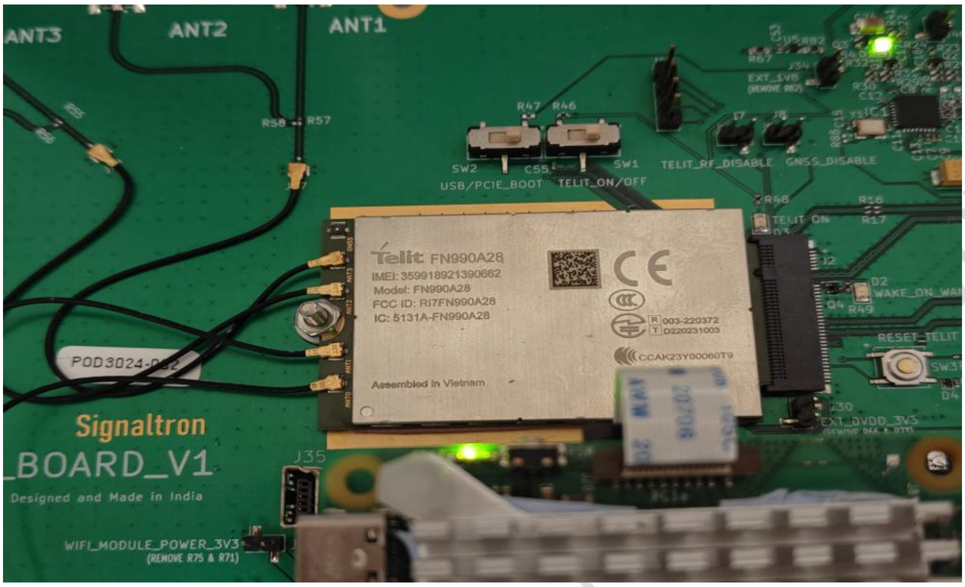


Figure 46 5G modem on the Evalboard

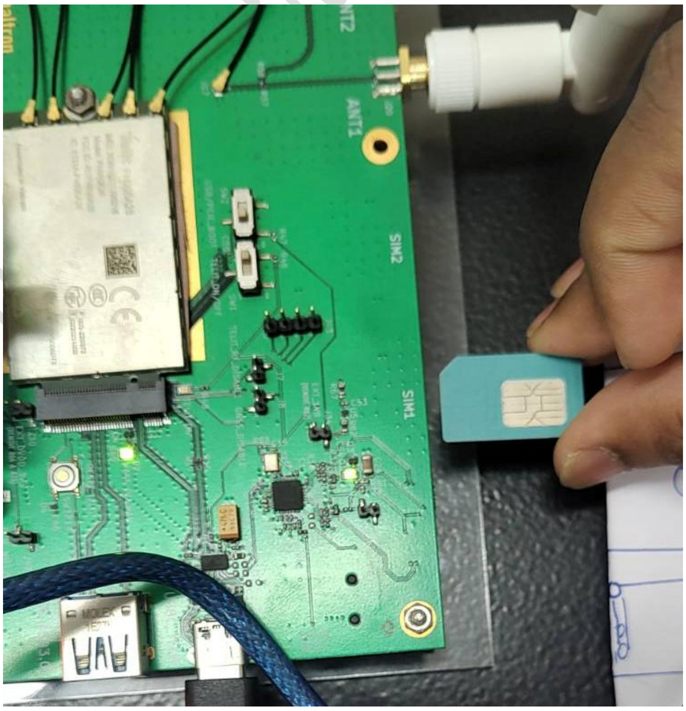


Figure 47 Direction to insert Sim card

Important note:

Do not connect power supply directly to Raspberry pi, only power supply should be connected to UE Evaluation Board. The Raspberry pi gets power from USB cable

Connections for 5G connectivity:

Before powering on the 5G UE Evaluation board ensure that below ones are as follows (refer: **Figure 48**)

1. Connect 5G Antennas to ANT1&9

2. Point the switch towards the marked pin for USB Boot (Figure 48)

3. Move the switch to on position (Figure 48)

4. Connect the module to the Raspberry pi via USBC-USBA Cable

5. Connect a micro-HDMI to HDMI cable from raspberry pi to a monitor.

6. Connect a mouse and keyboard to Raspberry Pi

7. Insert sim card as shown in Figure 47 Direction to insert Sim card

8. Connect a DC Power Supply (12V-5A)

9. Connect earphones for sound

10. Check how to configure each of the peripherals in their respective sections in the USER GUIDE.

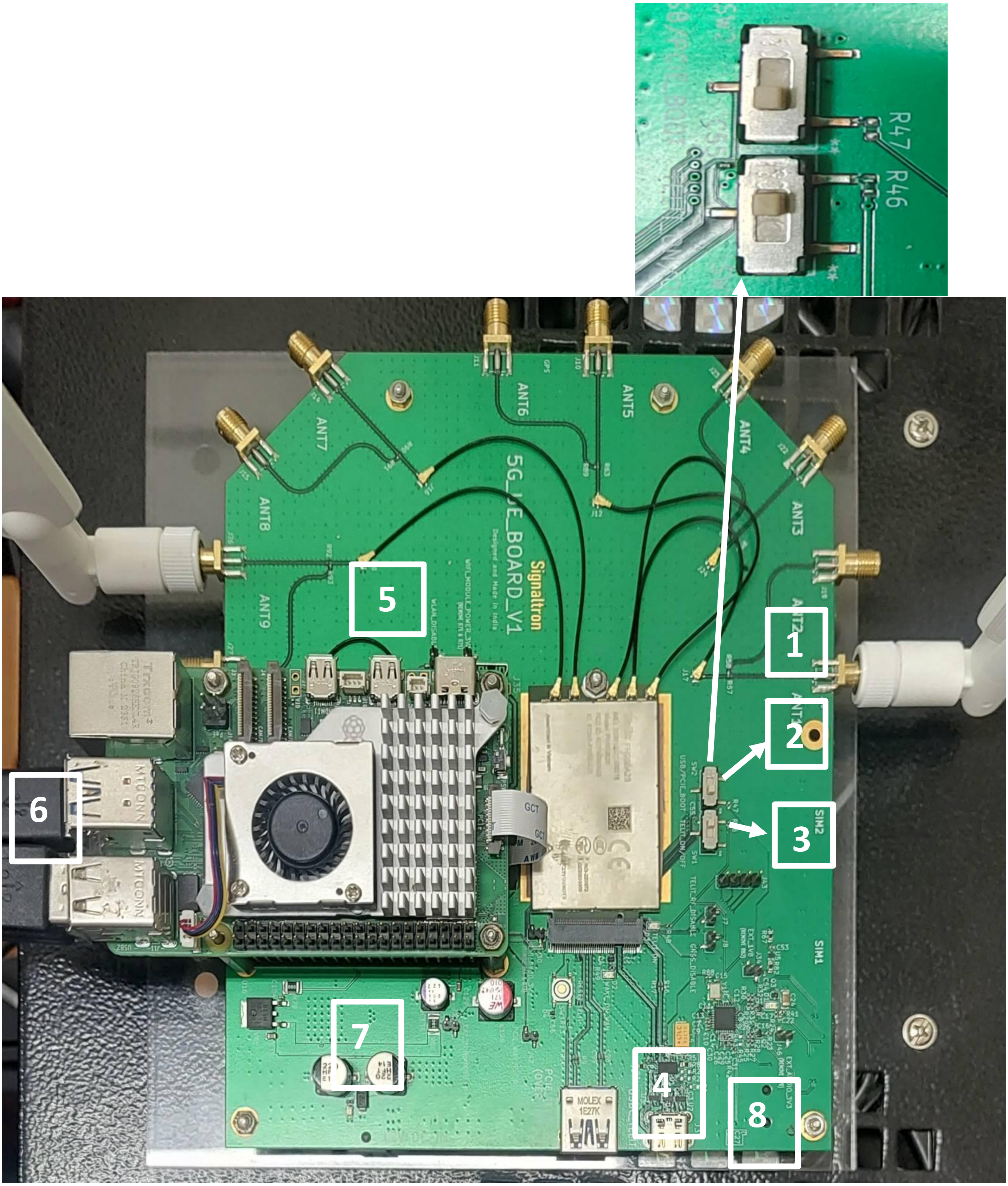


Figure 48 Evaluation board with Raspberry Pi

Connecting Eval Board to 5G network:-

1. Connect mouse, keyboard and monitor to the Evaluation board
2. Login to the console on monitor
   - **Username: aryaman**
   - **Password: 12345678**
3. Ensure all the connections are made as described above
4. Configure APN as internet
   - On top right bottom -> Under mobile broadband settings -> Access Point Names -> internet -> give APN details -> save

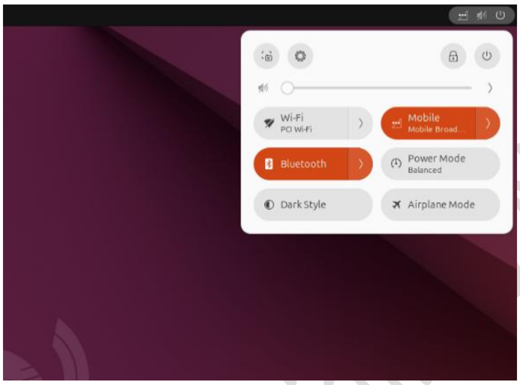


Figure 49 APN step-1

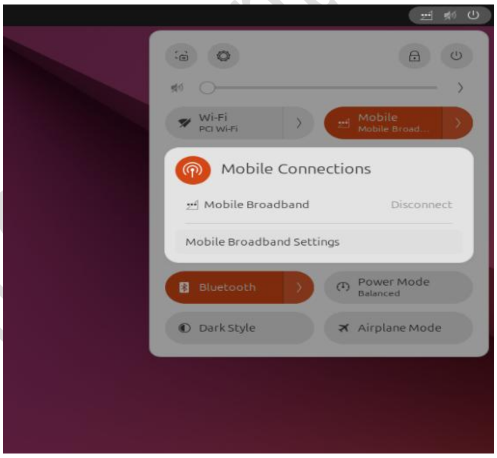
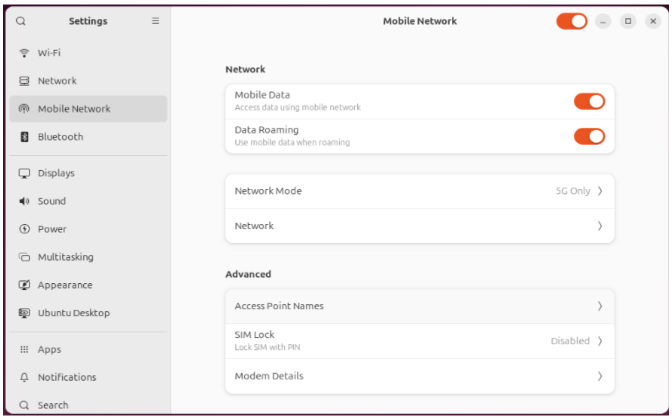


Figure 50 APN step-2



Mobile Network

Network

Mobile Data — Access data using mobile network — On

Data Roaming — Use mobile data when roaming — On

Network Mode: 5G Only

Network

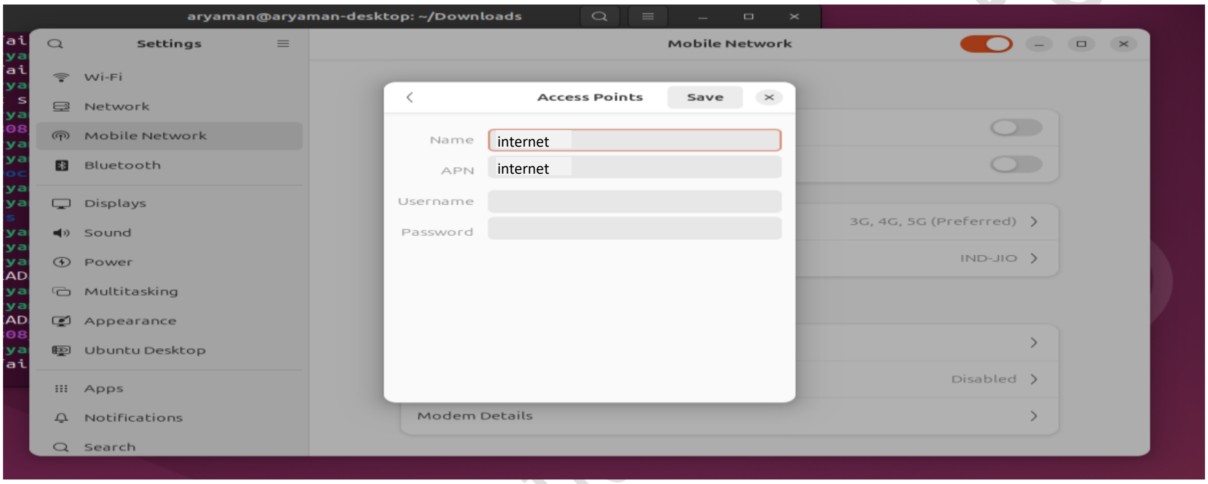
Advanced

Access Point Names

SIM Lock — Lock SIM with PIN: Disabled

Modem Details

Figure 51 APN step-3



Access Points — Save

Name: internet

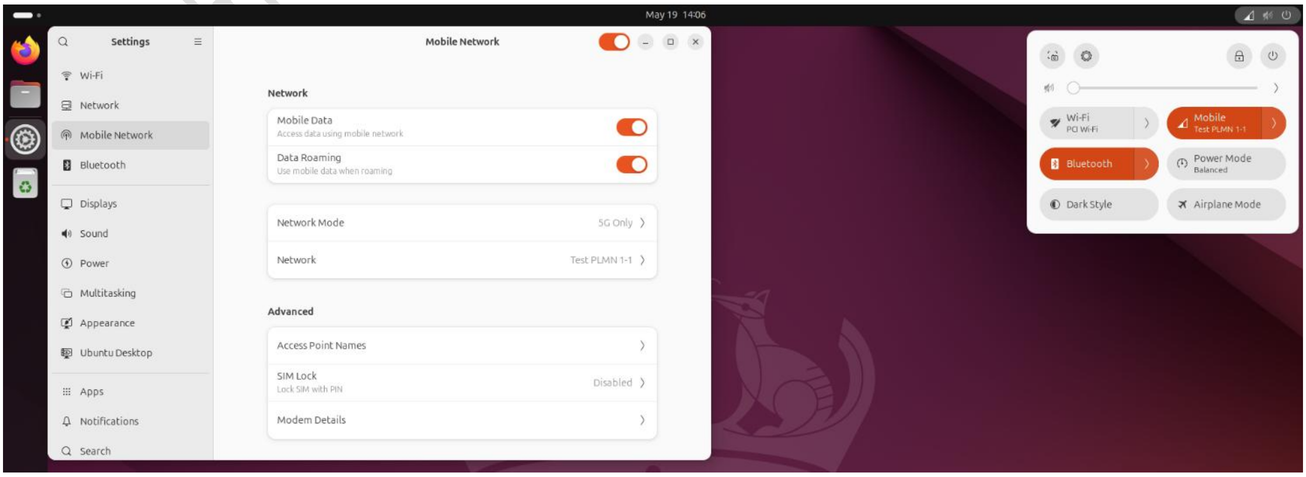
APN: internet

Username:

Password:

Figure 52 APN step-4

5. Once the APN settings are given the evaluation board should connect automatically.
6. UE Evaluation board should now be connecting, observe that symbol with a bar on top right as shown below and also an Ip address will be assigned **Figure 54**



Mobile Network

Network

Mobile Data — Access data using mobile network — On

Data Roaming — Use mobile data when roaming — On

Network Mode: 5G Only

Network: Test PLMN 1-1

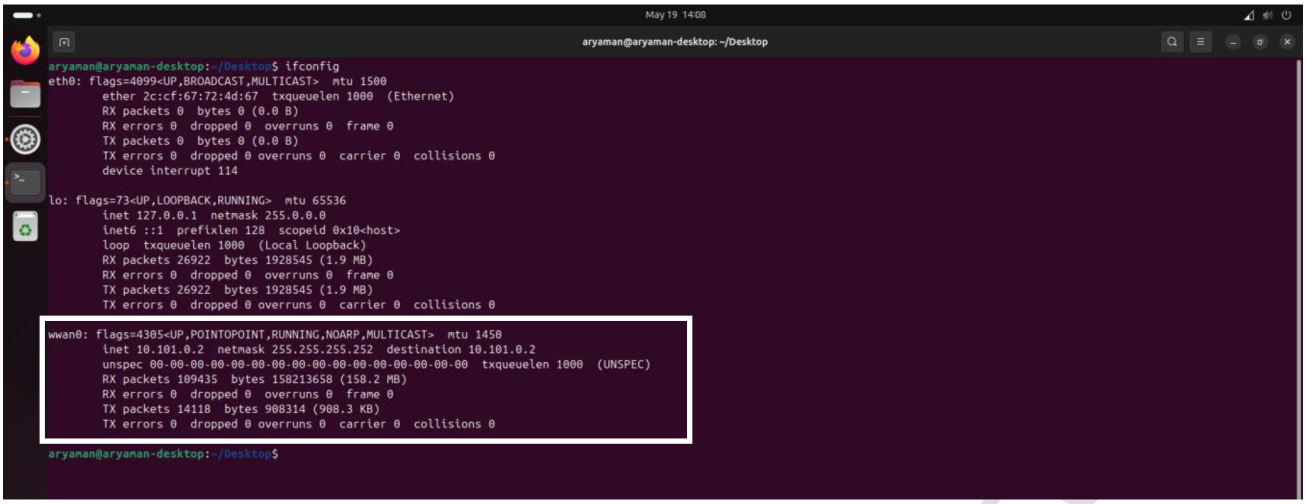
Advanced

Access Point Names

SIM Lock — Lock SIM with PIN: Disabled

Modem Details

Figure 53 UE evaluation board connected to 5G network

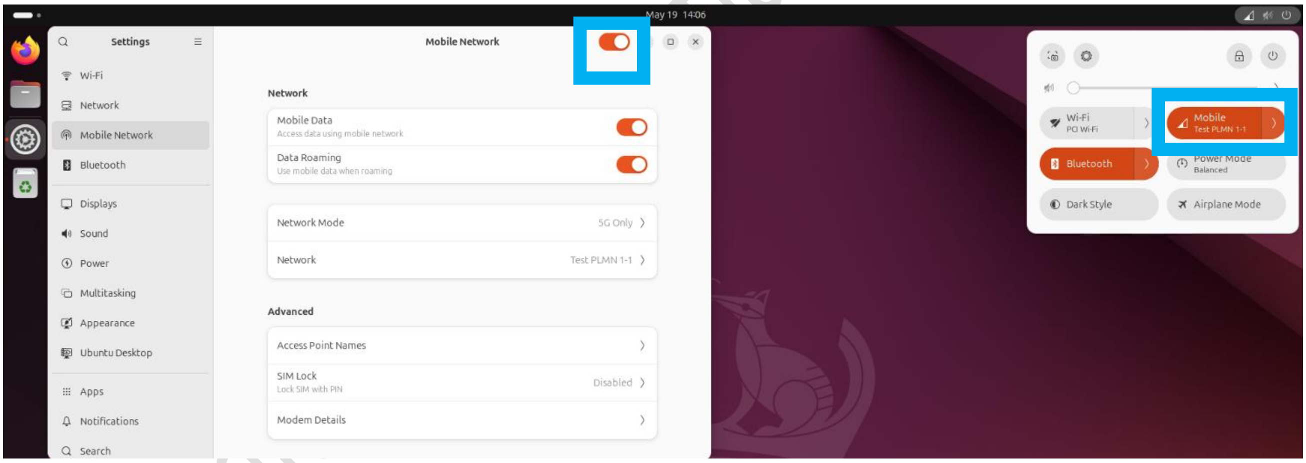


```
aryaman@aryaman-desktop:~/Desktop$ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 2c:cf:67:72:4d:67  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 114

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 26922  bytes 1928545 (1.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26922  bytes 1928545 (1.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wwan0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1450
        inet 10.101.0.2  netmask 255.255.255.252  destination 10.101.0.2
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 109435  bytes 158213658 (158.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14118  bytes 908314 (908.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

aryaman@aryaman-desktop:~/Desktop$
```

Figure 54 Ip address assigned to UE Eval board

Trouble shoot tips for evaluation board 5G connectivity:-

1. Ensure gNodeB is powered-on and radiating refer section-5, Power on the 5G Rack and gNodeB to connect to UE sub-section
2. If the Evaluation board does not connect automatically, try to turn off and turn on mobile network and mobile data as highlighted below



Mobile Network

Network

Mobile Data
Access data using mobile network

Data Roaming
Use mobile data when roaming

Network Mode 5G Only

Network Test PLMN 1-1

Advanced

Access Point Names

SIM Lock Disabled
Lock SIM with PIN

Modem Details

3. Ensure Data Roaming and Mobile data are turned on
4. Ensure APN settings are proper
5. If the issue still persists, do a hard power-off the UE evaluation board and power-on to try again

Wifi Module

The Eval Board has a wifi module onboard connected to the Raspberry Pi using its PCIe lane. After booting up the eval board, the wifi module will be available in wifi menu which drops down after left clicking the wifi symbol in the top right corner of the screen.

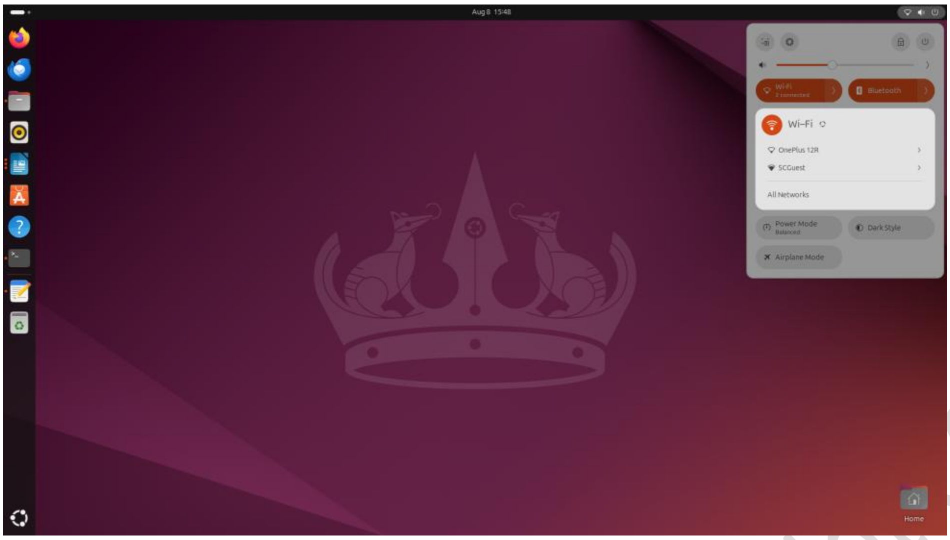


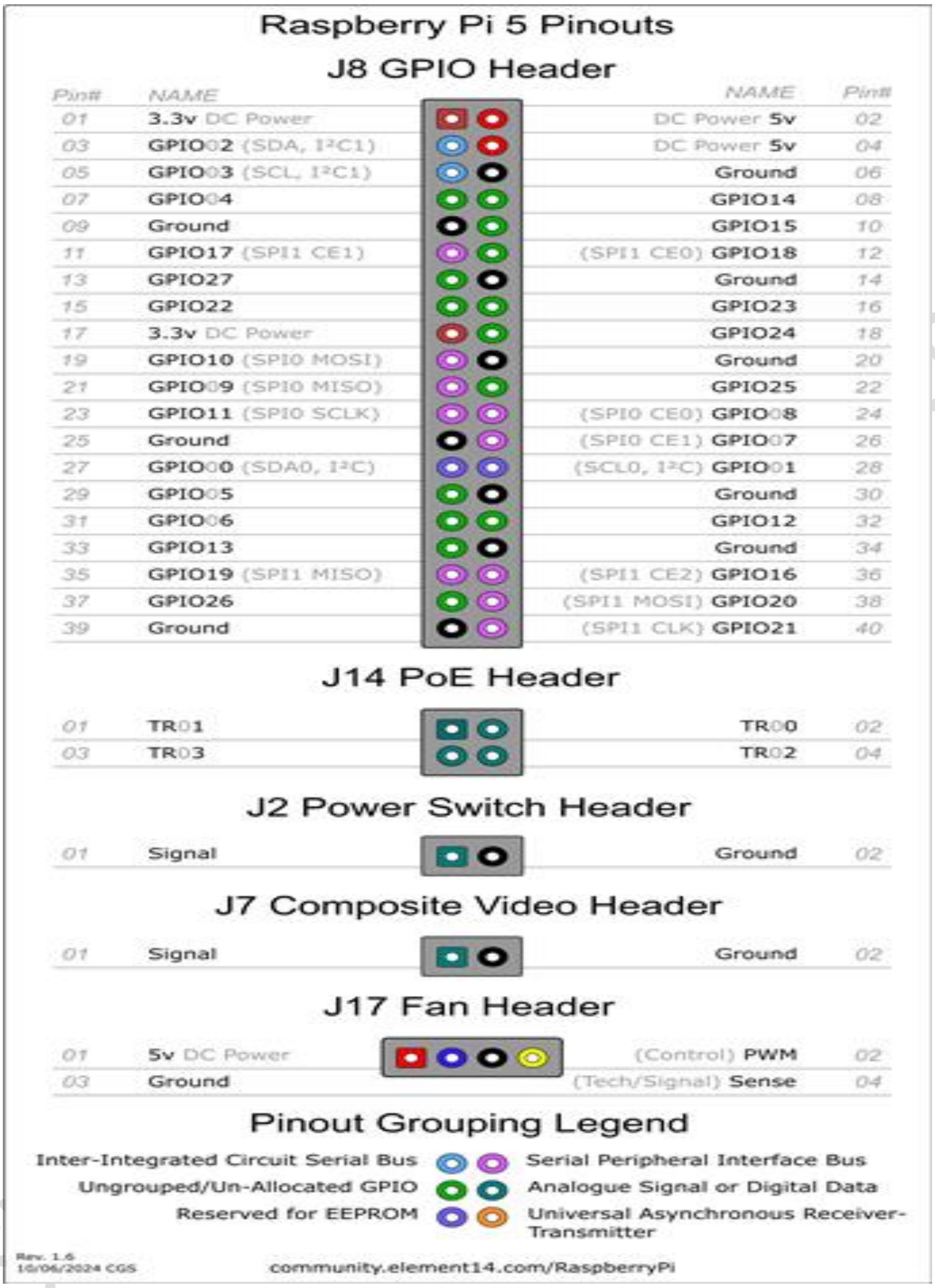
Figure 55 Wifi on Eval board

b) Use case: IoT sensor usage over 5G Evaluation board

Sensors could be directly connected to gpio interface of RPi5 sitting on top of the eval kit. Else, sensors could be connected to Arduino board and Arduino board could be connected to RPi via USB interface.

Minicom module can be used to communicate and retrieve data from these interfaces. This same data can be broadcasted or sent on a socket to MEC through some python script and further processing of this data can be done on MEC as per the requirements of students.

Raspberry Pi pinout: -



Raspberry Pi 5 Pinouts

J8 GPIO Header

Pin#	NAME	NAME	Pin#
01	3.3v DC Power	DC Power 5v	02
03	GPIO02 (SDA, I^{2}C1)	DC Power 5v	04
05	GPIO03 (SCL, I^{2}C1)	Ground	06
07	GPIO04	GPIO14	08
09	Ground	GPIO15	10
11	GPIO17 (SPI1 CE1)	(SPI1 CE0) GPIO18	12
13	GPIO27	Ground	14
15	GPIO22	GPIO23	16
17	3.3v DC Power	GPIO24	18
19	GPIO10 (SPI0 MOSI)	Ground	20
21	GPIO09 (SPI0 MISO)	GPIO25	22
23	GPIO11 (SPI0 SCLK)	(SPI0 CE0) GPIO08	24
25	Ground	(SPI0 CE1) GPIO07	26
27	GPIO00 (SDA0, I^{2}C)	(SCL0, I^{2}C) GPIO01	28
29	GPIO05	Ground	30
31	GPIO06	GPIO12	32
33	GPIO13	Ground	34
35	GPIO19 (SPI1 MISO)	(SPI1 CE2) GPIO16	36
37	GPIO26	(SPI1 MOSI) GPIO20	38
39	Ground	(SPI1 CLK) GPIO21	40

J14 PoE Header

01	TR01	TR00	02
03	TR03	TR02	04

J2 Power Switch Header

01	Signal	Ground	02

J7 Composite Video Header

01	Signal	Ground	02

J17 Fan Header

01	5v DC Power	(Control) PWM	02
03	Ground	(Tech/Signal) Sense	04

Pinout Grouping Legend

Inter-Integrated Circuit Serial Bus	○	○	Serial Peripheral Interface Bus
Ungrouped/Un-Allocated GPIO	○	○	Analogue Signal or Digital Data
Reserved for EEPROM	○	○	Universal Asynchronous Receiver-Transmitter

Rev. 1.6
16/06/2024 CGS

community.element14.com/RaspberryPi

Figure 56 Pinout diagram of Raspberry pi on top of UE evaluation board

3.2AT Commands

To send AT Commands to the Module, open terminal, there is a python file kept on the Desktop, type:-

sudo python3 AT_Commands.py

Initially, the file will send Edit Line x and replace AT with any other command to send it to the module.

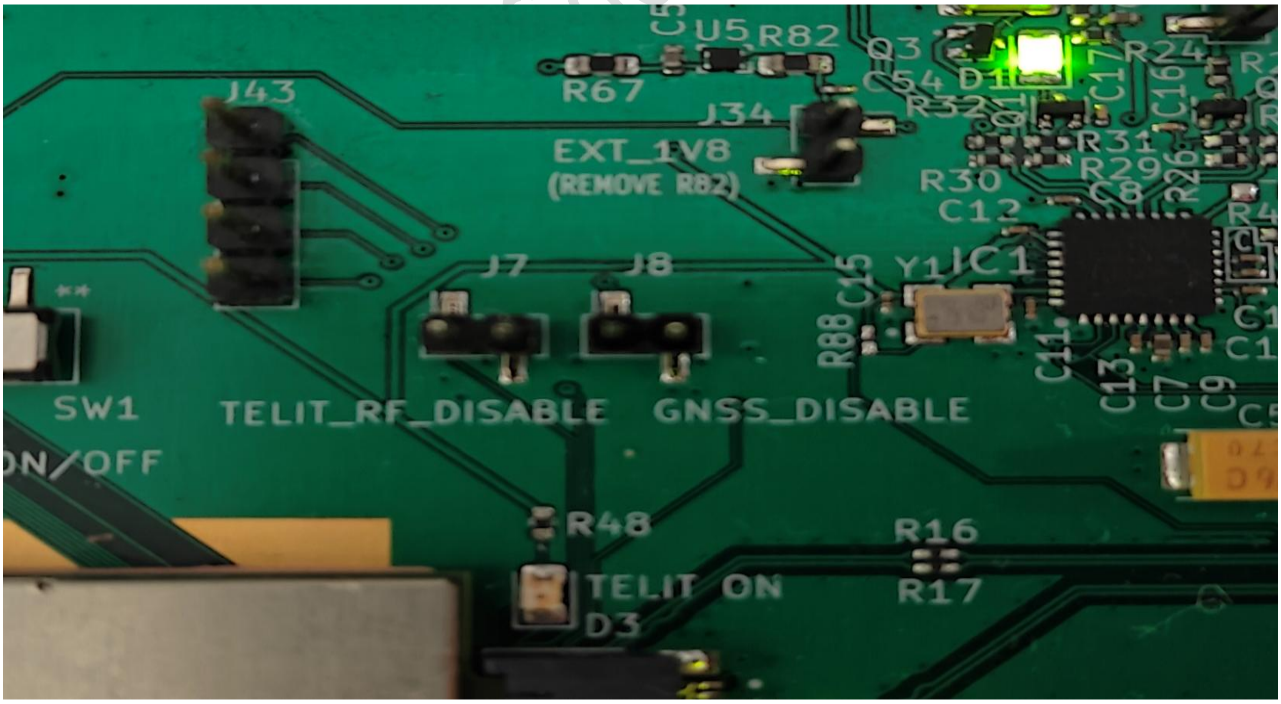
3.3GNSS_DISABLE

Adding a jumper on the J8 Connector will disable gnss in the telit module.

3.4RF_DISABLE

Adding a jumper on the J7 Connector will disable mobile networks in the telit module.

Fig3.3 J7&J8 Connectors



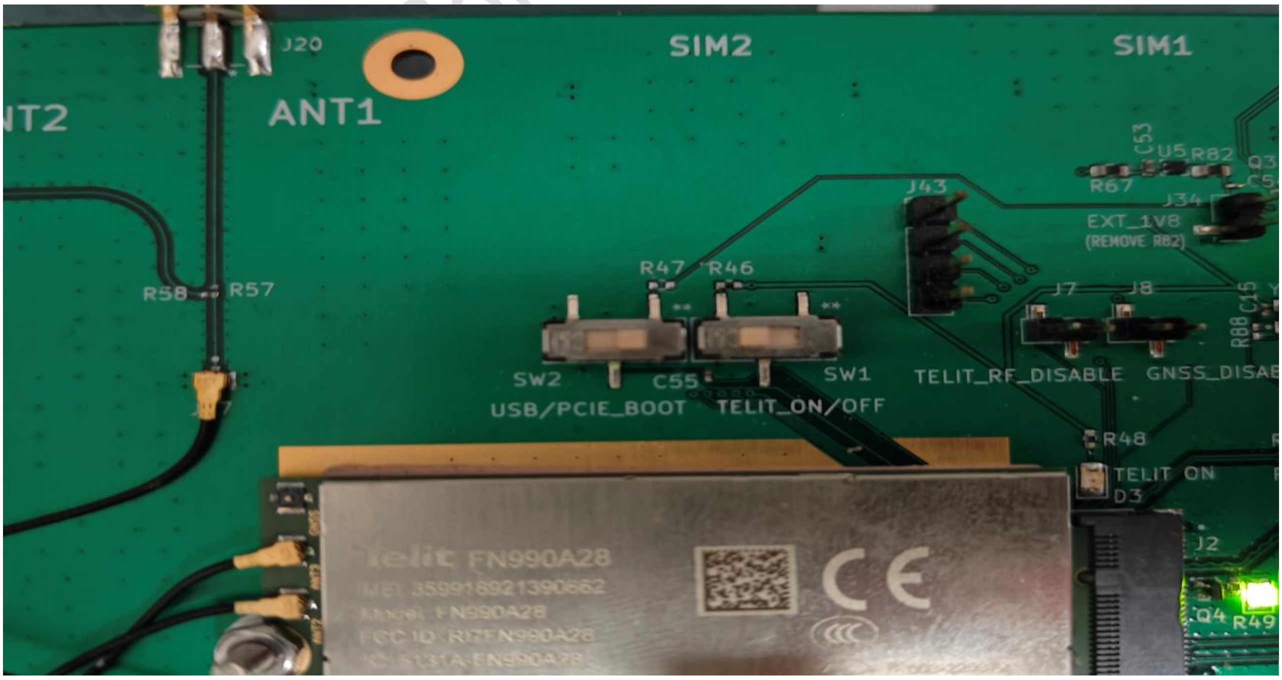
3.5ON/OFF SWITCH

Switch R46 will turn the module on/off, the top right corner of the switch is marked with two stars, which indicate the off position of the switch. After the module is switched on , the WOW(WAKE_ON_WAN) LED will also switch after a while.

3.6USB/PCIE SWITCH

Switch R47 will toggle the module between USB/PCIE mode, in the USB mode the module boots up using the provided J3 USB C connector connected the USB 3.0 ports of the Raspberry Pi. In the PCIE mode, the module will act as an end point and can be connected to a PC using one its PCIE slots. The top right corner of the Switch is marked with two stars indicating the USB position of the Switch.

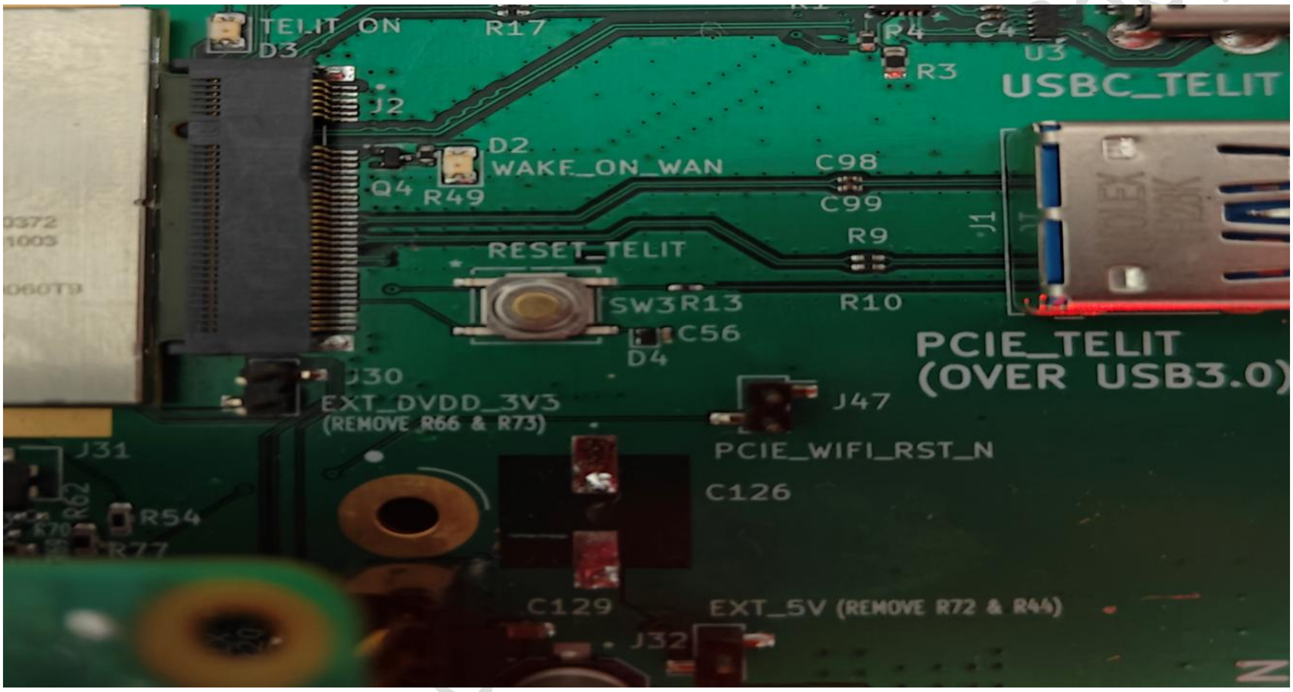
Fig3.4 Switches



3.7Reset Button

The SW3 reset button can be held for a few seconds to reset the telit module

Fig3.5 RESET Button



3.8Telit Antenna

Ant 5 and Ant 6 are supposed to be GNSS antennas. Ant 1,2,3,4,7,8,9,10 are all 4G/5G Antennas.

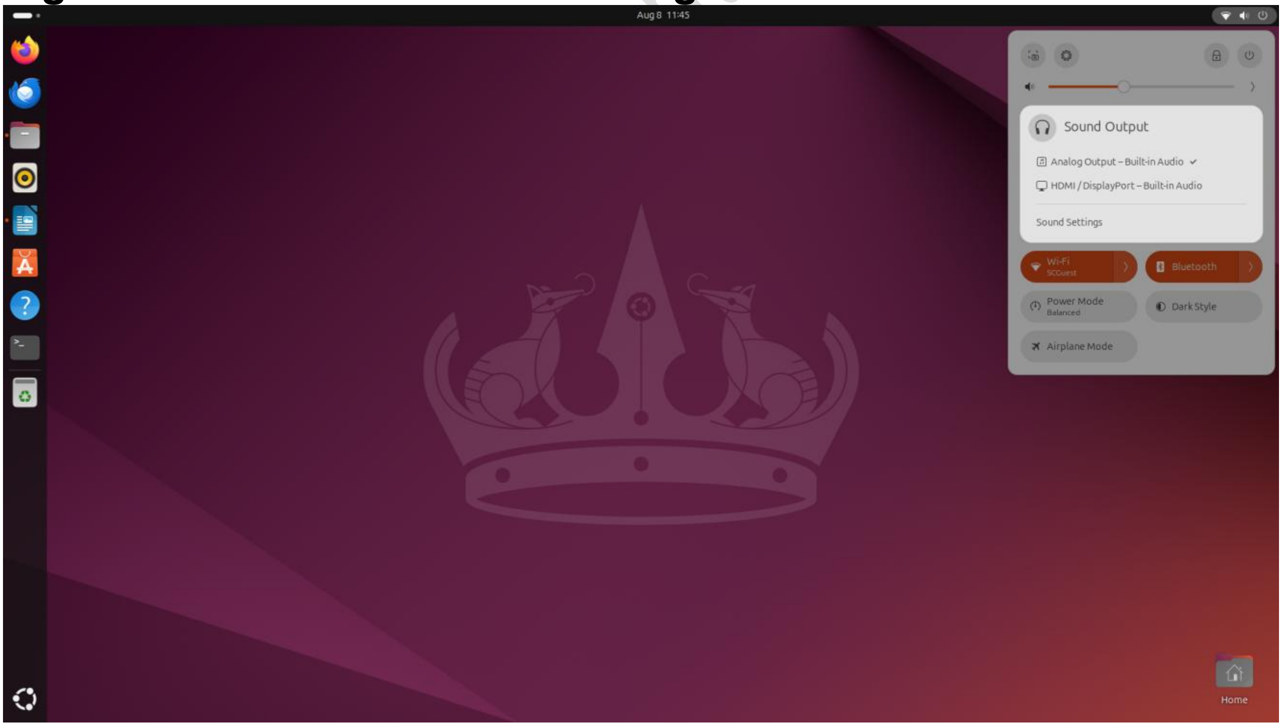
5.Audio Section

The Eval Board comes equipped with an audio codec which is controlled using the raspberry pi. After booting the pi the configuration file for the codec should run at startup, if in case of failure, i2c_codec.py can found in the desktop.
To run the file, open terminal and type:

```
sudo python3 i2c_codec.py
```

This will configure the codec, after which the audio output should be set to analog audio out from the drop down menu which appears upon right clicking the speaker symbol on the top right corner of the screen. The user must plug in an audio output device via the aux jack provided on the board.

Fig.5.1 Audio Settings Menu



In case the raspberry pi configuration file is reset, the file will have to be edited before running the codec configuration file.
To edit the rpi configuration file, open terminal and type:

```
sudo nano /boot/firmware/config.txt
```

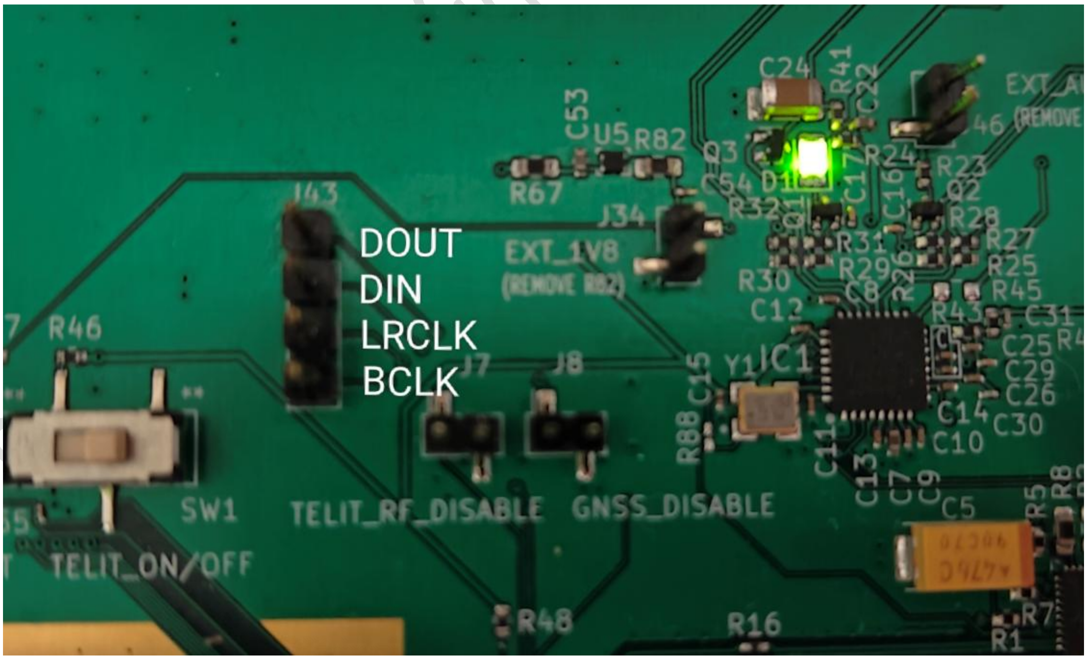
Then add these lines to the file:

dtoverlay=i2s-mmap
dtoverlay=hifiberry-dac
add a # before dtparam=audio=on

Save the file using Ctrl+s and exit using Ctrl+x

5.1External Audio

Fig 5.2 J43 Connector



Connector J43 can be used to send external digital audio to the codec.

Pinout:-

1.)SDOUT
2.)SDIN
3.)LRCLK
4.)BCLK
The pinout is the standard pinout for i2s communication.

NOTE:-
Turn off raspberry pi analog audio from the audio settings before using the external Connector.

8.RTOS

This section is for installation of RTOS on Raspberry pi -4. RTOS is a real time OS which is useful for time dependent data like sensors data.

8.1Installing Dependencies

1. If using an Ubuntu version older than 22.04, it is necessary to add extra repositories to meet the minimum required versions for the main dependencies listed above. In that case, download, inspect and execute the Kitware archive script to add the Kitware APT repository to your sources list.

   ```
   wget https://apt.kitware.com/kitware-archive.sh
   ```

   ```
   sudo bash kitware-archive.sh
   ```

2. Use apt to install the required dependencies:

   ```
   sudo apt install --no-install-recommends git cmake ninja-build
   gperf \ ccache dfu-util device-tree-compiler wget \ python3-dev
   python3-pip python3-setuptools python3-tk python3-wheel xz-utils
   file \ make gcc gcc-multilib g++-multilib libsdl2-dev libmagic1
   ```

8.2Installing Zephyr and Python dependencies

1. Use apt to install Python venv package:

   ```
   sudo apt install python3-venv
   ```

2. Create a new virtual environment:

   ```
   python3 -m venv ~/zephyrproject/.venv
   ```

3. Activate the virtual environment:

   ```
   source ~/zephyrproject/.venv/bin/activate
   ```

   Once activated your shell will be prefixed with (.venv). The virtual environment can be deactivated at any time by running deactivate.

Note

Remember to activate the virtual environment every time you start working.

4. Install west:

```
pip install west
```

5. Get the Zephyr source code:

```
west init ~/zephyrproject
cd ~/zephyrproject
west update
```

6. Export a Zephyr CMake package. This allows CMake to automatically load boilerplate code required for building Zephyr applications.

```
west zephyr-export
```

7. Zephyr’s scripts/requirements.txt file declares additional Python dependencies. Install them with pip.

```
pip install -r ~/zephyrproject/zephyr/scripts/requirements.txt
```

8.3Installing Zephyr SDK

1. Download and verify the Zephyr SDK bundle:

```
cd ~
```

wget *https://github.com/zephyrproject-rtos/sdk-ng/releases/download/v0.16.8/zephyr-sdk-0.16.8_linux-aarch64.tar.xz*

```
wget -O - https://github.com/zephyrproject-rtos/sdk-ng/releases/download/v0.16.8/sha256.sum | shasum --check --ignore-missing
```

2. Extract the Zephyr SDK bundle archive:

```
tar xvf zephyr-sdk-0.16.8_linux-aarch64.tar.xz
```

Note

It is recommended to extract the Zephyr SDK bundle at one of the following locations:

- $HOME
- $HOME/.local
- $HOME/.local/opt
- $HOME/bin
- /opt
- /usr/local

The Zephyr SDK bundle archive contains the zephyr-sdk-<version> directory and, when extracted under $HOME, the resulting installation path will be $HOME/zephyr-sdk-<version>.

3. Run the Zephyr SDK bundle setup script:

```
cd zephyr-sdk-0.16.8

./setup.sh
```

Note

You only need to run the setup script once after extracting the Zephyr SDK bundle.

You must rerun the setup script if you relocate the Zephyr SDK bundle directory after the initial setup.

4. Install udev rules, which allow you to flash most Zephyr boards as a regular user:

```
sudo cp ~/zephyr-sdk-0.16.8/sysroots/x86_64-pokysdk-
linux/usr/share/openocd/contrib/60-openocd.rules
/etc/udev/rules.d

sudo udevadm control –reload
```

8.4Building Blinky

Build the Blinky with west build:

```
cd ~/zephyrproject/zephyr
west build -p always -b rpi_4b samples/basic/blinky
```

8.5Run the Program Prepare a SD card with MBR and FAT32. In the root directory of the SD card:

1. Download and place these firmware files:
   - bcm2711-rpi-4-b.dtb
   - bootcode.bin
   - start4.elf
2. Copy build/zephyr/zephyr.bin
3. Create a config.txt:

4. kernel=zephyr.bin
5. arm_64bit=1
6. enable_uart=1

```
uart_2ndstage=1
```

The green ACT LED can be seen blinking on the RPi4 on Startup.

14.Router with Firewall

COSGrid's Next Generation firewall is a Network Security appliance that processes network traffic and is capable of detecting and blocking sophisticated attacks by enforcing security policies. COSGrid Next Generation Firewall augments the traditional firewall along with enhanced features and network routing. COSGrid Next Generation Firewall is designed to allow businesses/organizations that range in scale from mid-sized networks to distributed enterprises and data centers with advanced threat prevention in a high-performance security platform.

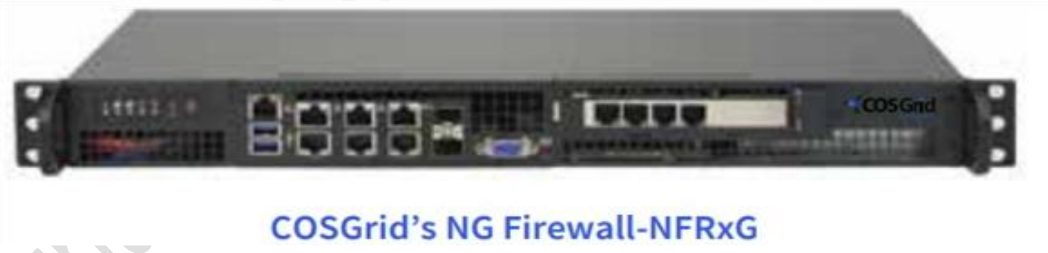


Figure 57 CosGrid Firewall

Also, it can offer them a cost-effective option to improve basic Network security through the use of application awareness, inspection services, protection systems and awareness tools.

a. Router and Firewall Architecture

The COSGrid Next-Generation Firewall (NGFW) integrates routing and security features into a single appliance. It goes beyond traditional firewalls by supporting deep packet inspection, intrusion prevention, and advanced traffic filtering. It works at both Layer 3 (routing) and Layer 7 (application filtering), allowing administrators to define precise security policies.

Usability:

- The firewall allows configuring WAN, LAN, and DMZ zones with specific policies.
- It provides both static and dynamic routing (OSPF, BGP, RIP) to efficiently manage network traffic.
- The system supports load balancing, ensuring optimal utilization of multiple network links.

b. Intelligent Networking

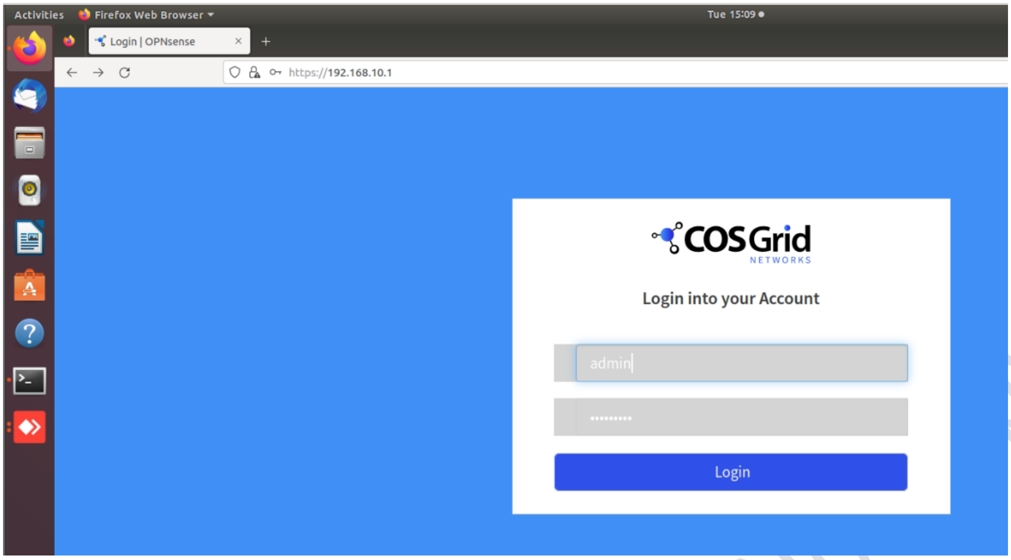
COSGrid NGFW offers intelligent networking features, including VLAN support, traffic shaping (QoS), and real-time monitoring of network flows. It ensures optimized data transmission by prioritizing critical applications like VoIP and business-critical cloud services.

Usability:

- **VLAN Configuration:** The firewall supports 802.1Q VLAN tagging to segment networks for improved security and performance.
- **QoS Support:** Traffic shaping rules can be applied to prioritize bandwidth for essential services like video conferencing while restricting less critical traffic.
- **Load Balancing:** The firewall can distribute traffic across multiple ISPs, preventing bottlenecks and improving redundancy.

c. Logging into firewall web page

The firewall can be accessed via the web browser at 192.168.10.1 (LAN interface).



Activities Firefox Web Browser Tue 15:09

Login | OPNsense

https://192.168.10.1

COSGrid NETWORKS

Login into your Account

admin

•••••••••

Figure 58 Cosgrid login

Login Credentials: -

Username: admin

Password: admin@321

LAN and WAN interfaces could be configured through the interfaces section in the Web User Interface. DHCP settings can also be applied in the LAN interface as per the user requirements.

Rules for inbound/outbound traffic, specifying allowed services and other configurations could be modified from this interface.

d. Connecting the firewall to production networks with Security Zones

Security zones define boundaries within the network to restrict unauthorized access. COSGrid NGFW allows segmentation between internal (LAN), external (WAN), and demilitarized zone (DMZ) networks.

 Creating Security Zones: Configure different interfaces with policies restricting traffic between zones.

 Example Use Case: A web server in the DMZ can be accessed from the internet but should have restricted access to internal systems.

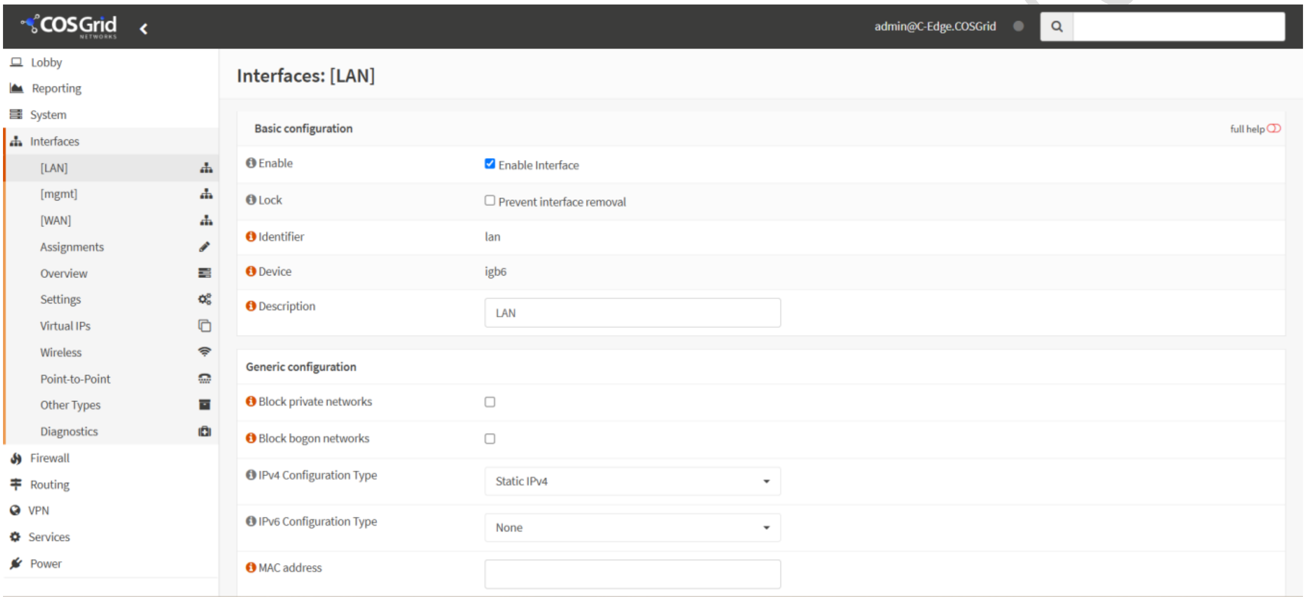
 Zone-Based Policies: Administrators can create policies to block unnecessary traffic between zones while allowing critical services like DNS and HTTP/S.

e. Firewall Functionalities

i. Managing firewall configurations

The firewall settings include interface assignments, NAT rules, and security policies, which can be managed through the web UI.

All the Interfaces related configurations, services (blocking , traffic limiting , QOS etc.), firewall rules , VLAN and other rules can be easily configured from the Web UI.



Interfaces: [LAN]

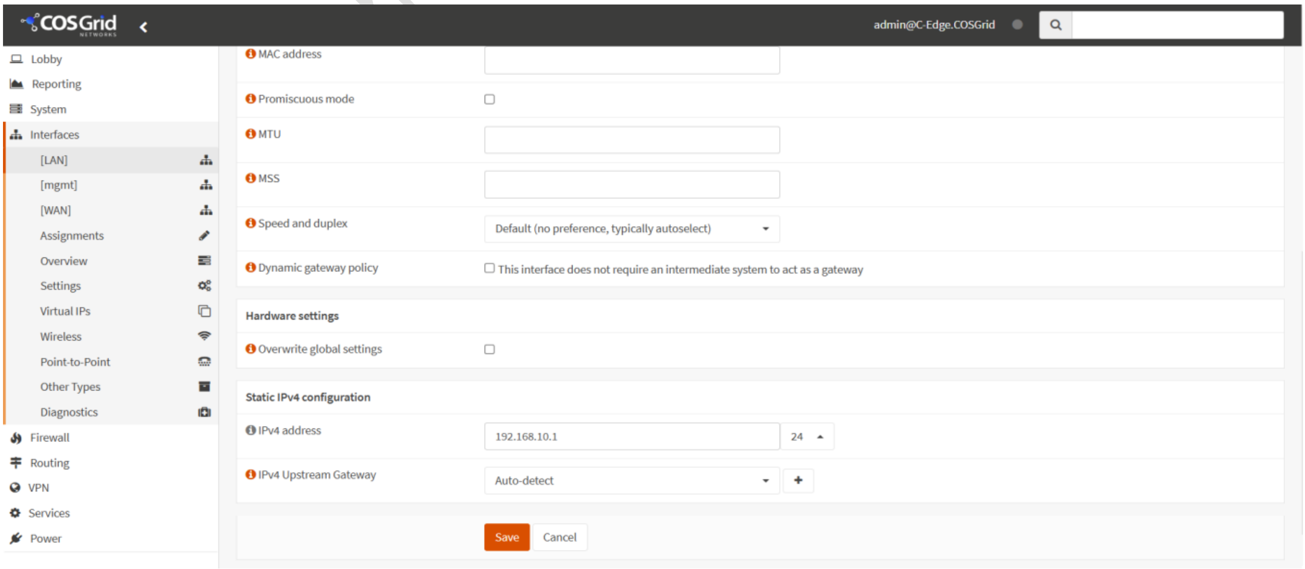
Basic configuration

Enable	☑ Enable Interface
Lock	□ Prevent interface removal
Identifier	lan
Device	igb6
Description	LAN

Generic configuration

Block private networks	□
Block bogon networks	□
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC address	

Figure 59 Initial LAN port configuration part-1



MAC address	
Promiscuous mode	□
MTU	
MSS	
Speed and duplex	Default (no preference, typically autoselect)
Dynamic gateway policy	□ This interface does not require an intermediate system to act as a gateway

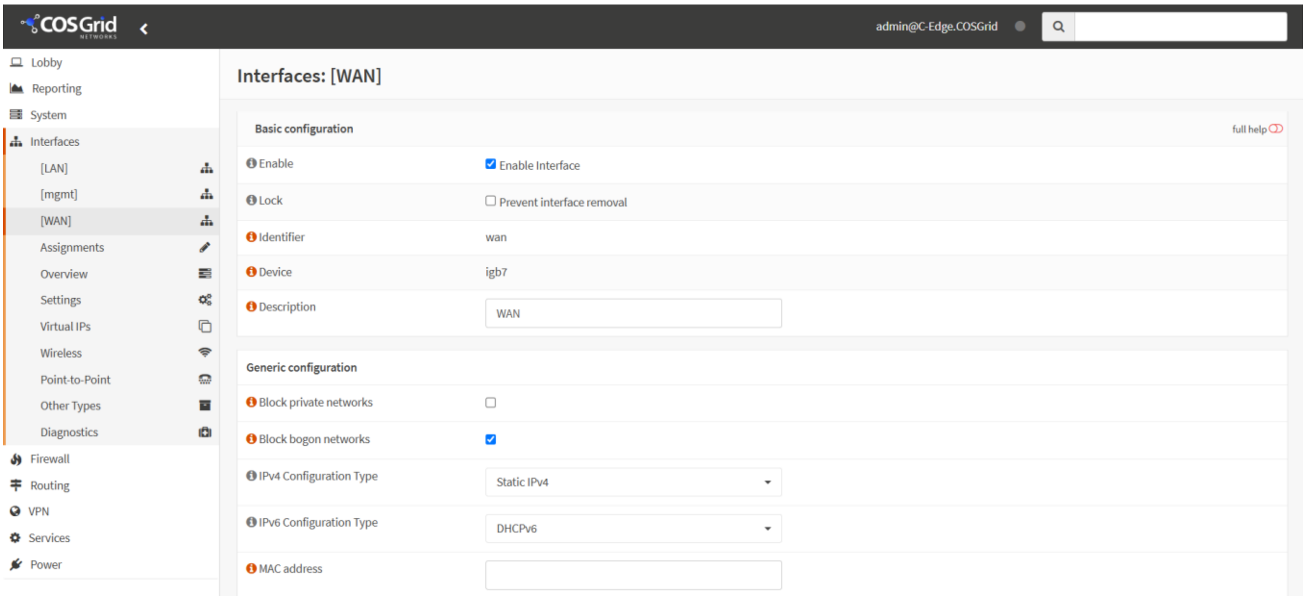
Hardware settings

Overwrite global settings	□

Static IPv4 configuration

IPv4 address	192.168.10.1 / 24
IPv4 Upstream Gateway	Auto-detect

Figure 60 Initial LAN configuration part-2



Interfaces: [WAN]

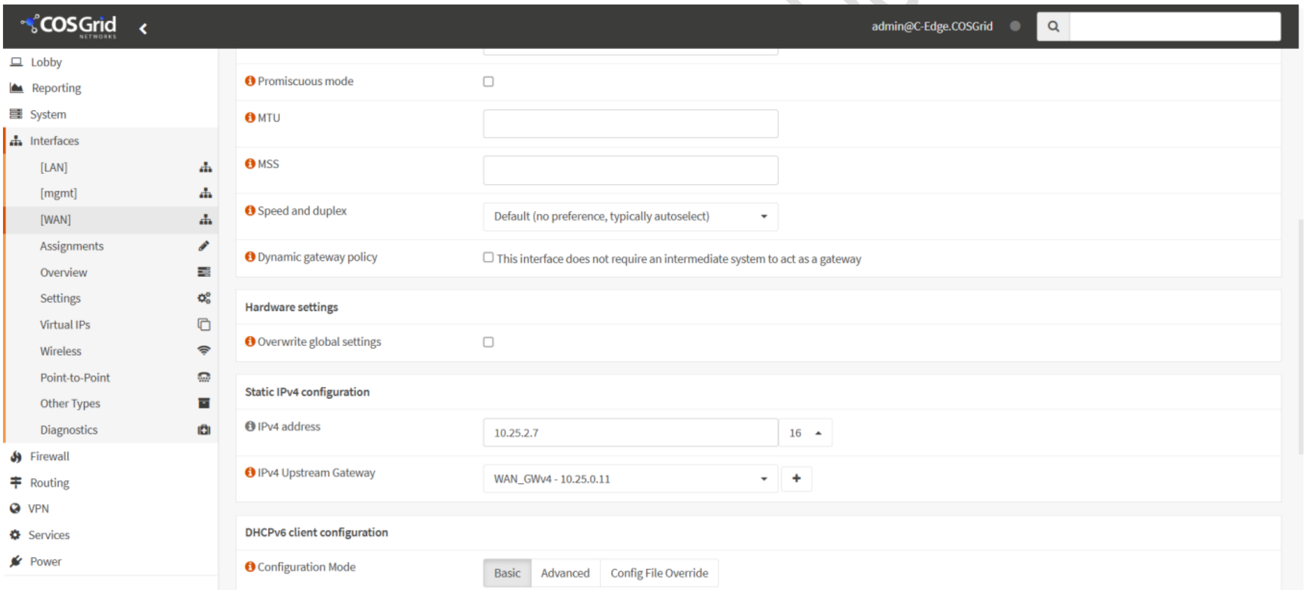
Basic configuration

- Enable: ☑ Enable Interface
- Lock: □ Prevent interface removal
- Identifier: wan
- Device: igb7
- Description: WAN

Generic configuration

- Block private networks: □
- Block bogon networks: ☑
- IPv4 Configuration Type: Static IPv4
- IPv6 Configuration Type: DHCPv6
- MAC address:

Figure 61 Initial WAN configuration part-1



- Promiscuous mode: □
- MTU:
- MSS:
- Speed and duplex: Default (no preference, typically autoselect)
- Dynamic gateway policy: □ This interface does not require an intermediate system to act as a gateway

Hardware settings

- Overwrite global settings: □

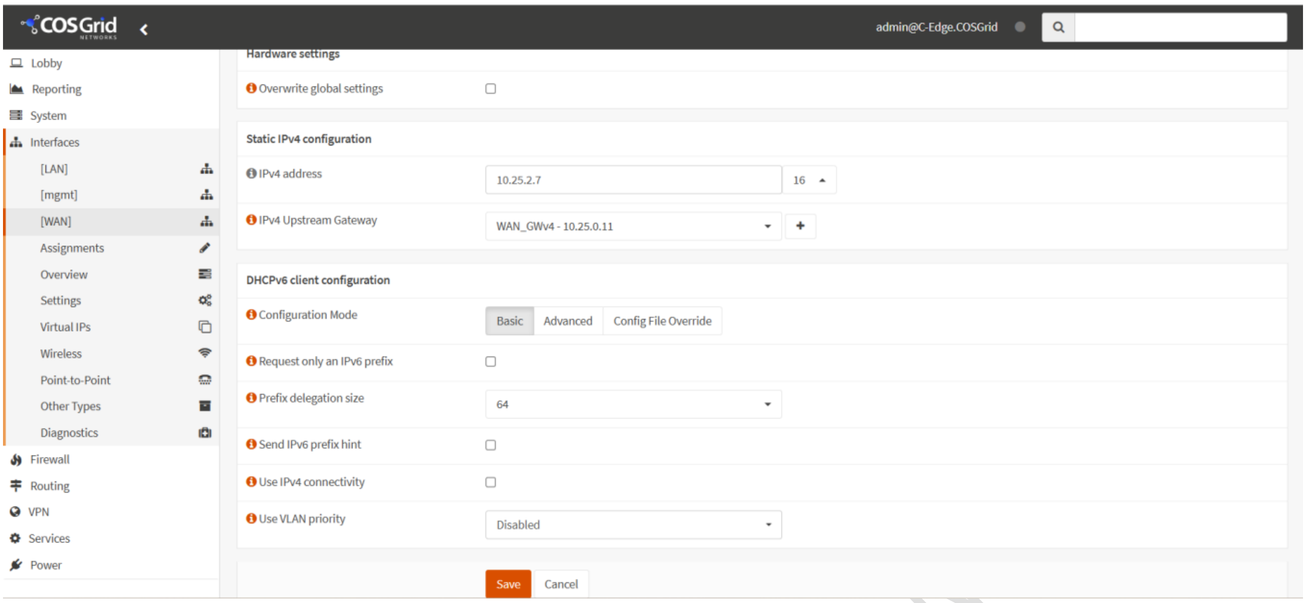
Static IPv4 configuration

- IPv4 address: 10.25.2.7 / 16
- IPv4 Upstream Gateway: WAN_GWv4 - 10.25.0.11

DHCPv6 client configuration

- Configuration Mode: Basic | Advanced | Config File Override

Figure 62 Initial WAN port configuration part-2



Hardware settings

Overwrite global settings	☐

Static IPv4 configuration

IPv4 address	10.25.2.7 / 16
IPv4 Upstream Gateway	WAN_GWv4 - 10.25.0.11

DHCPv6 client configuration

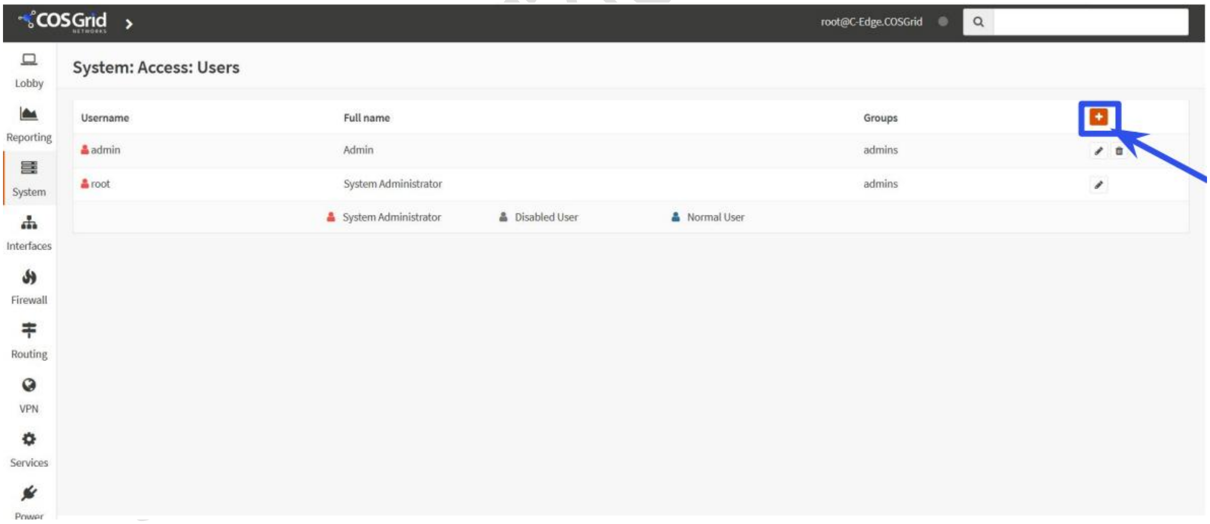
Configuration Mode	Basic · Advanced · Config File Override
Request only an IPv6 prefix	☐
Prefix delegation size	64
Send IPv6 prefix hint	☐
Use IPv4 connectivity	☐
Use VLAN priority	Disabled

Save Cancel

Figure 63 Initial WAN configuration part-3

ii. Managing firewall administrator accounts

The firewall supports multiple administrator roles with role-based access control (RBAC).



System: Access: Users

Username	Full name	Groups
admin	Admin	admins
root	System Administrator	admins

System Administrator · Disabled User · Normal User

Figure 64 Firewall administrator

Different privileges can be assigned to users (e.g., read-only access for auditors, full access for security administrators).

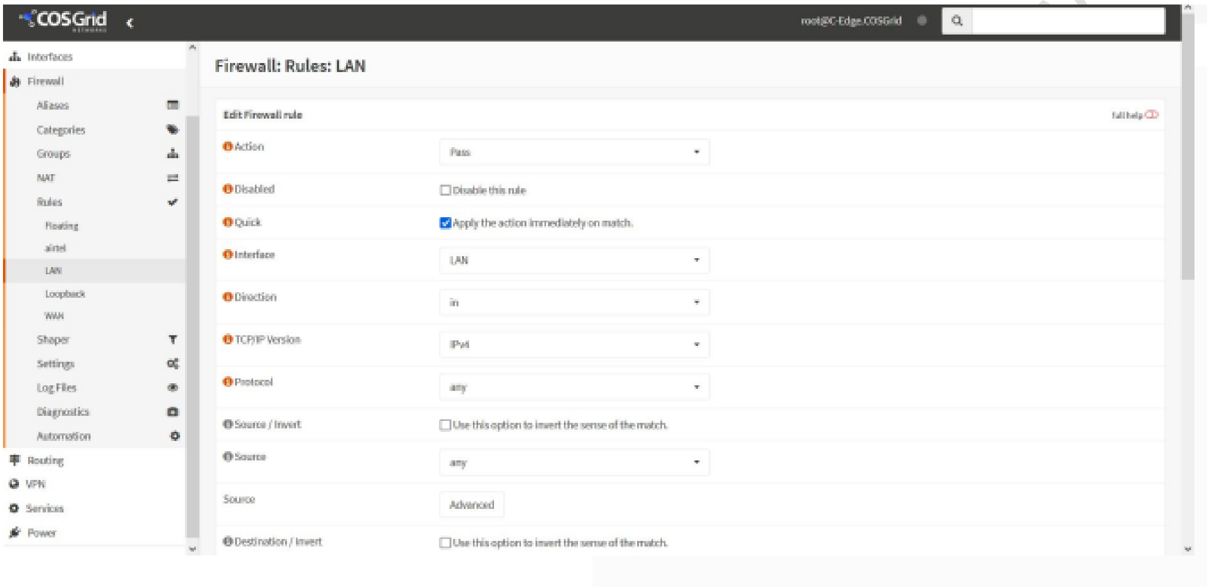
Admins can enable two-factor authentication (2FA) to enhance security.

iii. Creating and managing security and policy rules

Security policies define allowed and blocked traffic based on source, destination, protocol, and application.

Usability:

- Rules can be created for specific IP ranges, users, or applications.
- Example: Allow HTTPS (443) from the internal network to the internet while blocking SSH (22).



Firewall: Rules: LAN

Edit Firewall rule

Action	Pass
Disabled	☐ Disable this rule
Quick	☑ Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	any
Source / Invert	☐ Use this option to invert the sense of the match.
Source	any
Source	Advanced
Destination / Invert	☐ Use this option to invert the sense of the match.

Figure 65 Firewall LAN

iv. Full network visibility of HTTP and HTTPS Traffic

You can view the network traffic and its analytics through the firewall and can generate the analytical reports. To view the Network Visibility of the firewall, access the web interface IP with Port 3000- 192.168.15.1:3000. The Network Analytics window of the Firewall opens . In the Dashboard section itself, you can view the ovevriew of Network parameters like Top hosts, Applications, flow talkers, Traffic classifications etc.

Login IP: 192.168.10.1:3000 user: **admin** password : **admin**

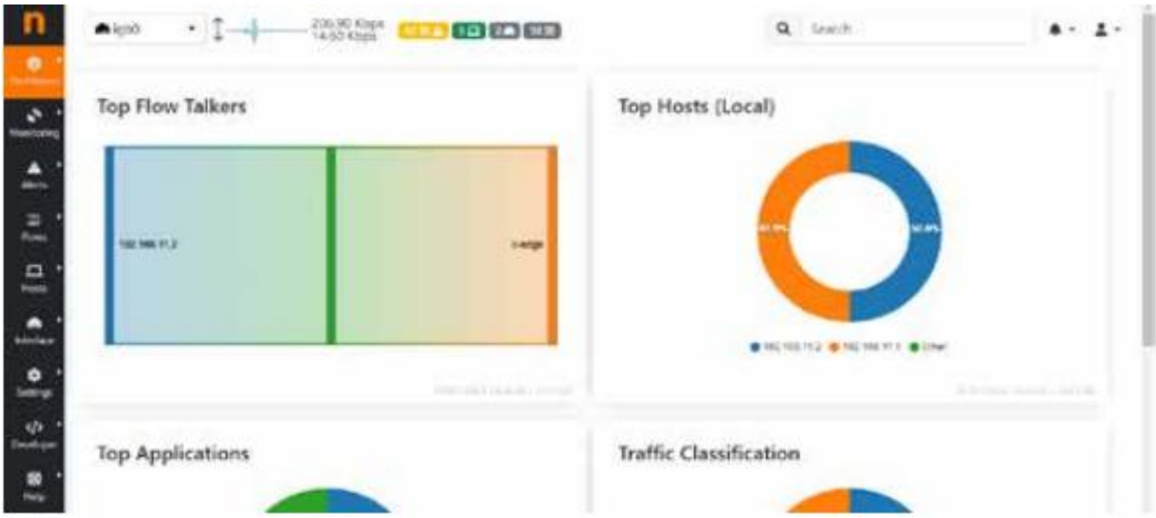


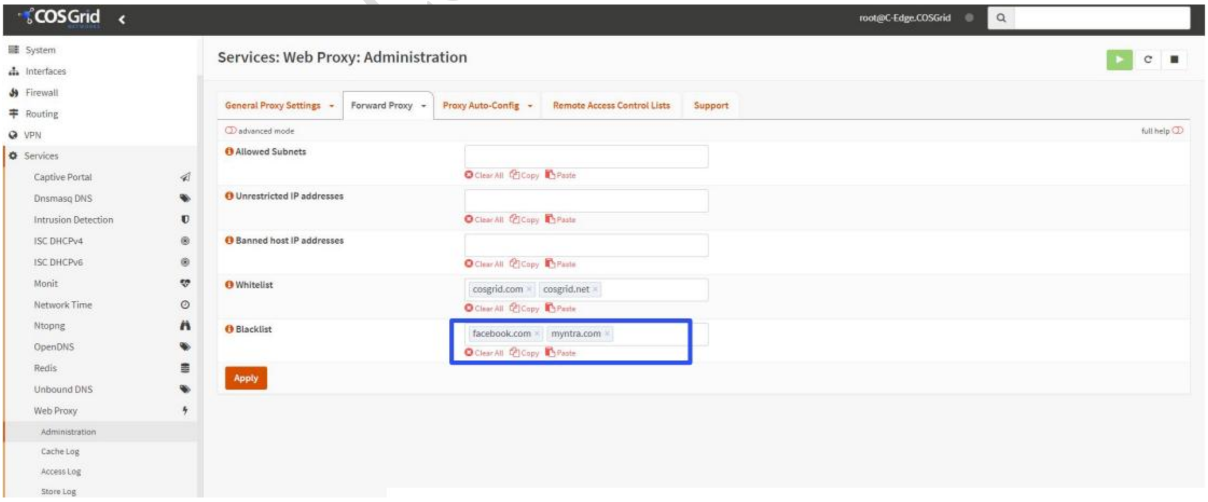
Figure 66 Firewall monitoring

v. Blocking known threats (Security Profiles, URL Filtering, etc.)

The firewall includes an intrusion detection and prevention system (IDPS) and URL filtering capabilities.

Usability:

- Administrators can block access to malware-infected websites and phishing domains.
- Predefined threat signatures can automatically update to detect the latest cyber threats.



Services: Web Proxy: Administration

Allowed Subnets:

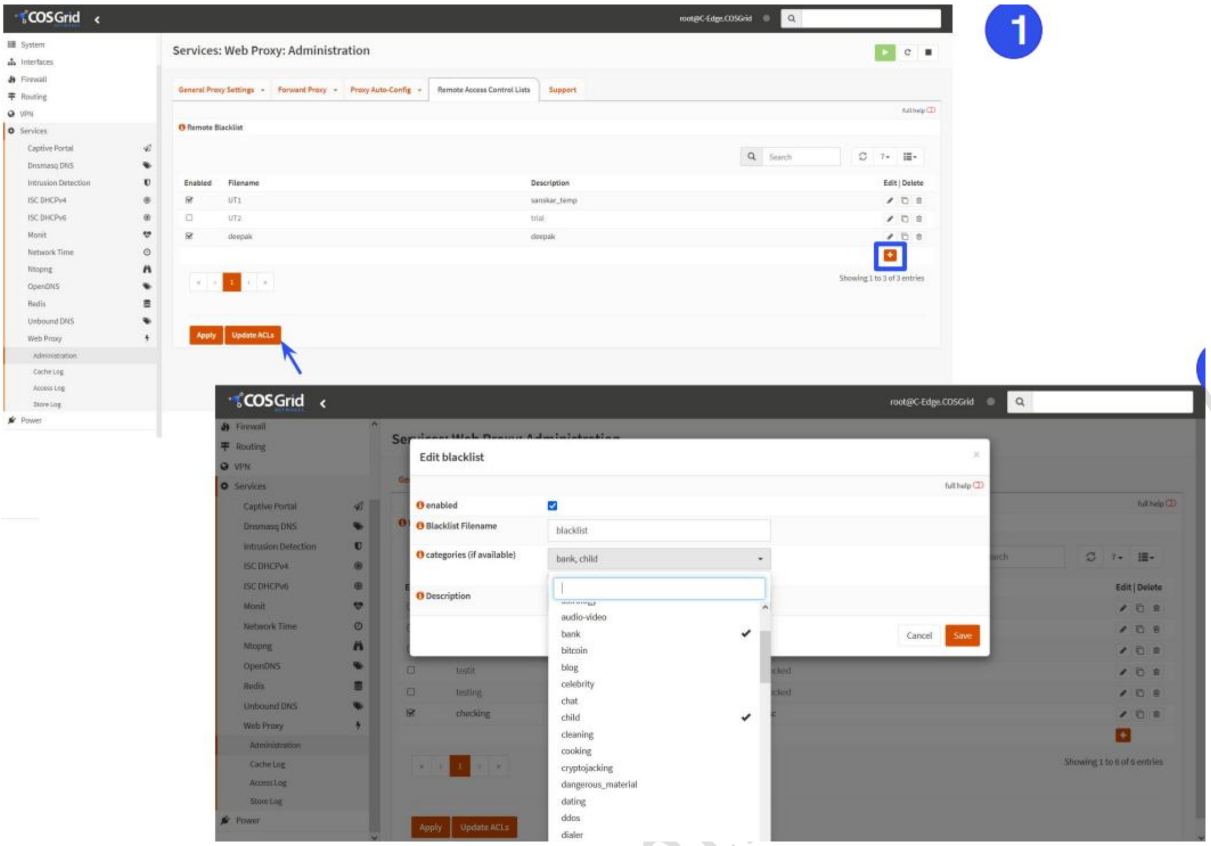
Unrestricted IP addresses:

Banned host IP addresses:

Whitelist: cosgrid.com, cosgrid.net

Blacklist: facebook.com, myntra.com

Figure 67 Firewall administration (blacklisting)



Services: Web Proxy: Administration

Remote Blacklist

Enabled	Filename	Description
☑	UT1	sanskar_temp
□	UT2	trial
☑	deepak	deepak

Showing 1 to 3 of 3 entries

Edit blacklist

- enabled ☑
- Blacklist Filename: blacklist
- categories (if available): bank, child
- Description

audio-video, bank ✓, bitcoin, blog, celebrity, chat, child ✓, cleaning, cooking, cryptojacking, dangerous_material, dating, ddos, dialer

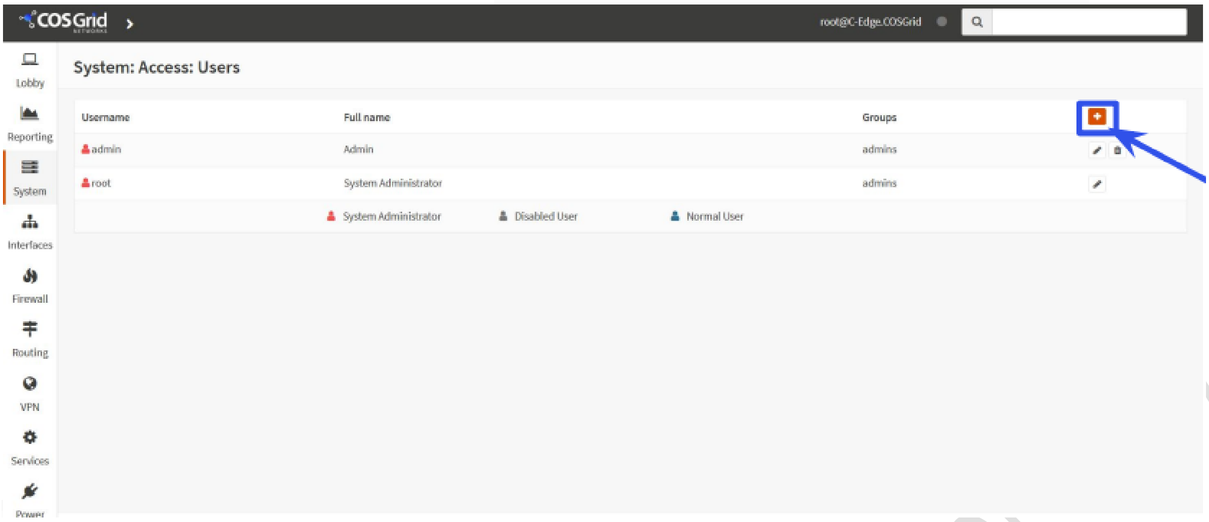
Showing 1 to 6 of 6 entries

Figure 68 Firewall administration (blacklisting)

vi. Controlling Access and Usage of Network Resources with User-ID

threat User-ID allows policies to be applied based on authenticated user identities rather than just IP addresses.

The firewall can integrate with Active Directory to apply role-based access policies. Example: Developers may be allowed SSH access, while non-IT staff are restricted.

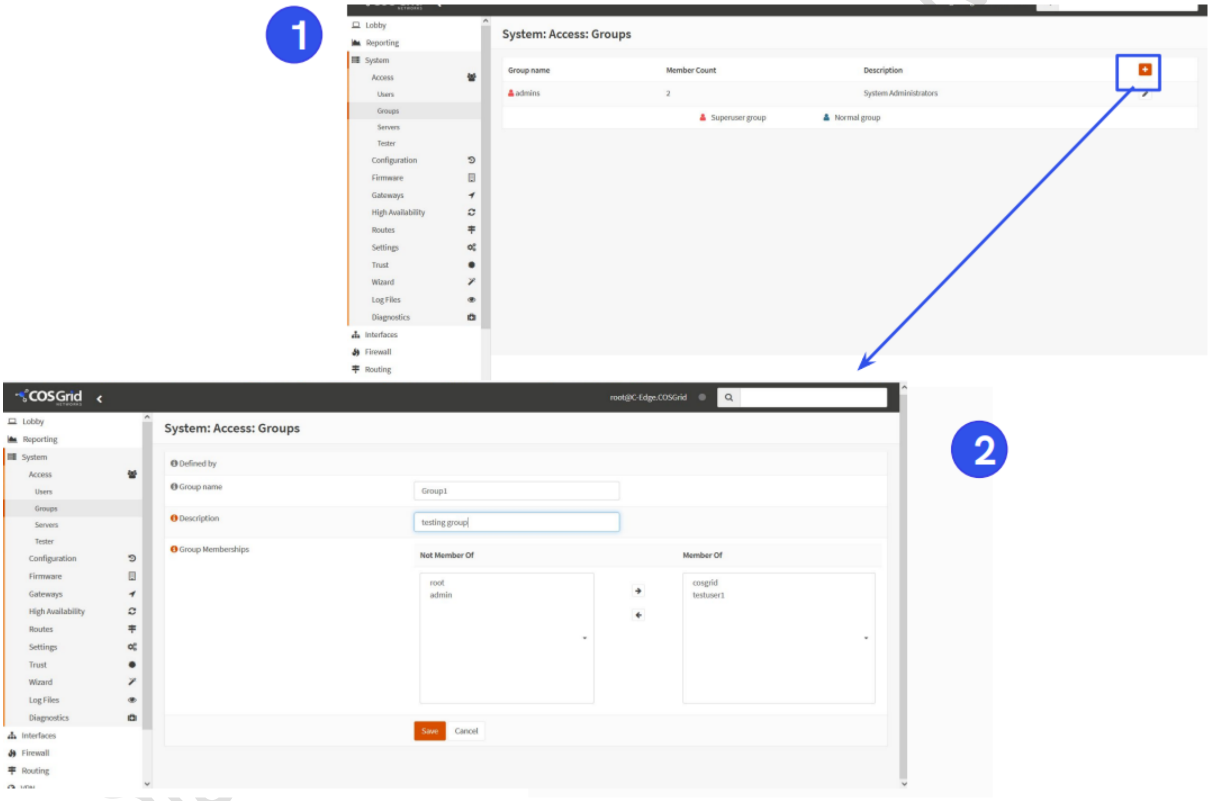


System: Access: Users

Username	Full name	Groups
admin	Admin	admins
root	System Administrator	admins

System Administrator · Disabled User · Normal User

Figure 69 Firewall - adding users



System: Access: Groups

Group name	Member Count	Description
admins	2	System Administrators

Superuser group · Normal group

System: Access: Groups

Defined by

Group name: Group1

Description: testing group

Group Memberships

Not Member Of	Member Of
root admin	cosgrid testuser1

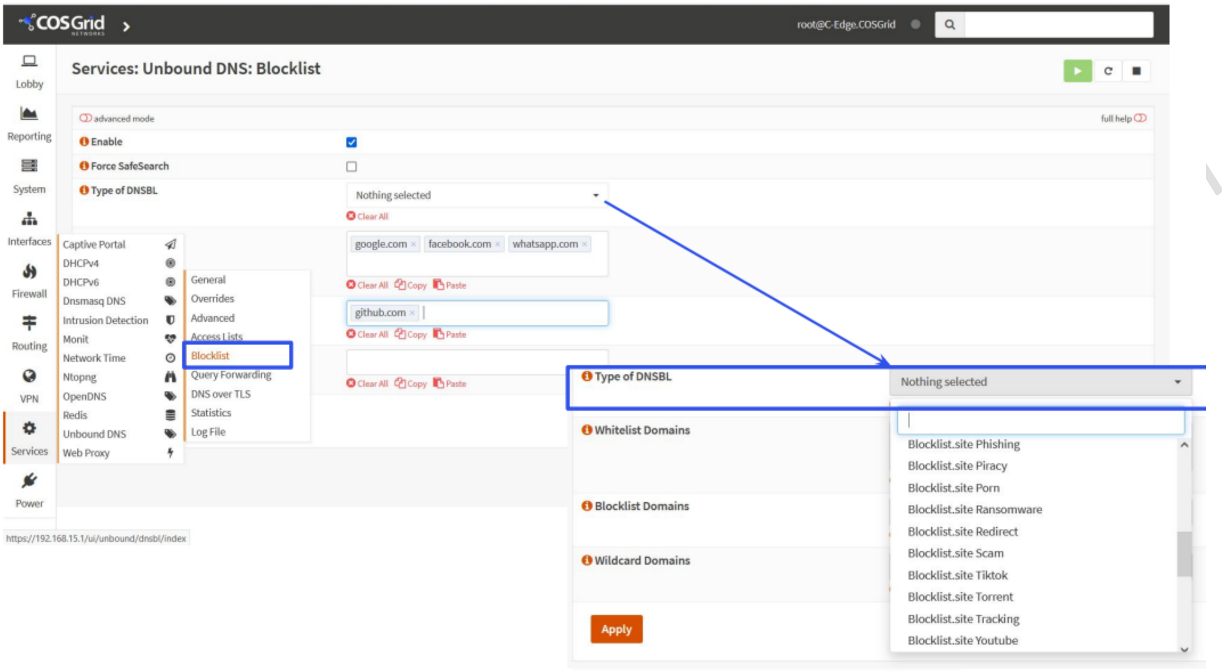
Save   Cancel

Figure 70 Firewall - adding users

vii. Control access to specific applications

Application control helps restrict access to non-business-related applications like social media or P2P sharing.

Administrators can block applications like torrents and online gaming to conserve bandwidth.

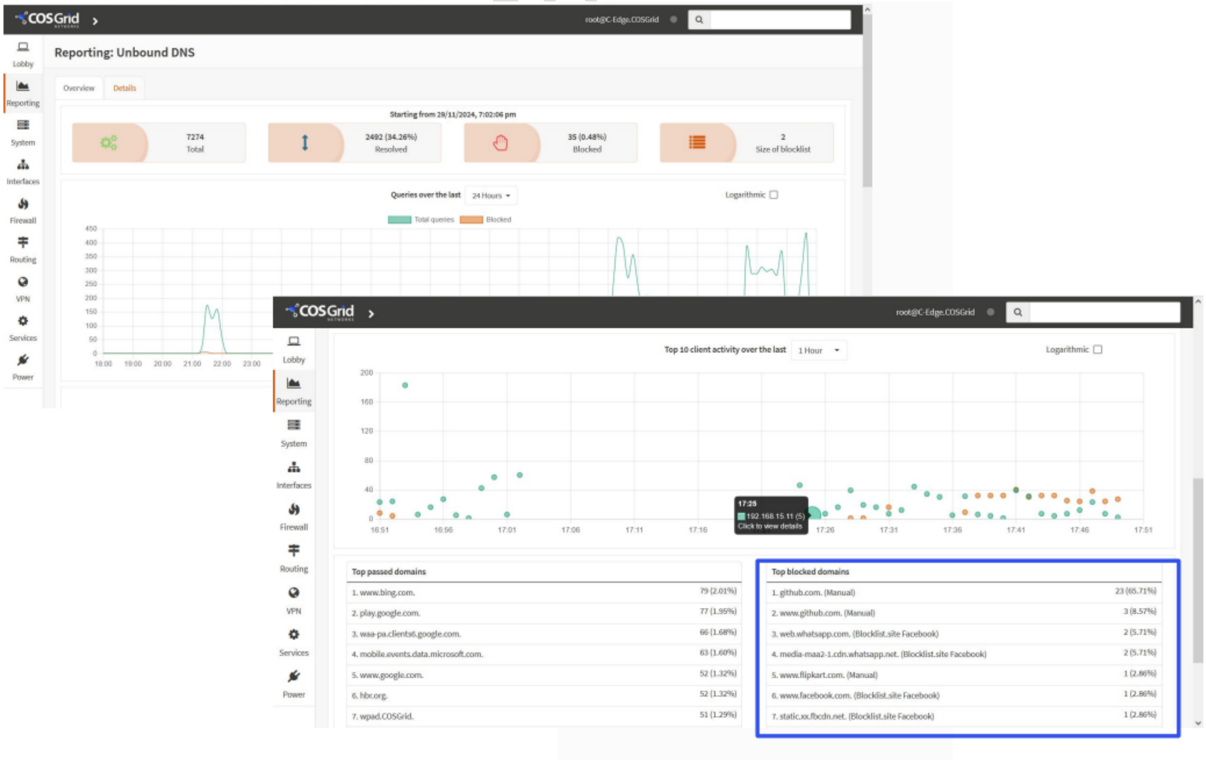


Services: Unbound DNS: Blocklist

- Enable: ☑
- Force SafeSearch: □
- Type of DNSBL: Nothing selected
- Whitelist Domains: google.com, facebook.com, whatsapp.com
- Blocklist Domains: github.com

https://192.168.15.1/ui/unbound/dnsbl/index

Figure 71 Firewall blocking applications



Reporting: Unbound DNS

Starting from 29/11/2024, 7:02:06 pm

7274 Total	2492 (34.26%) Resolved	35 (0.48%) Blocked	2 Size of blocklist

Top passed domains	
1. www.bing.com.	79 (2.01%)
2. play.google.com.	77 (1.95%)
3. waa-pa.clients6.google.com.	66 (1.68%)
4. mobile.events.data.microsoft.com.	63 (1.60%)
5. www.google.com.	52 (1.32%)
6. hbr.org.	52 (1.32%)
7. wpad.COSGrid.	51 (1.29%)

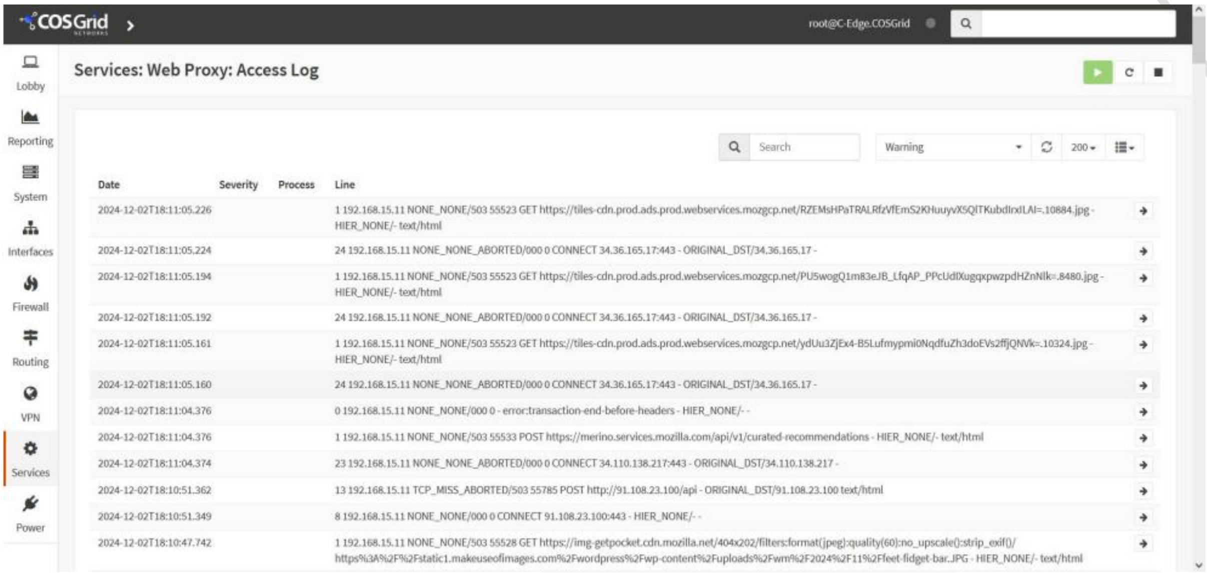
Top blocked domains	
1. github.com. (Manual)	23 (65.71%)
2. www.github.com. (Manual)	3 (8.57%)
3. web.whatsapp.com. (Blocklist.site Facebook)	2 (5.71%)
4. media-maa2-1.cdn.whatsapp.net. (Blocklist.site Facebook)	2 (5.71%)
5. www.flipkart.com. (Manual)	1 (2.86%)
6. www.facebook.com. (Blocklist.site Facebook)	1 (2.86%)
7. static.xx.fbcdn.net. (Blocklist.site Facebook)	1 (2.86%)

Figure 72 Firewall statistics

viii. Locating Valuable Information Using Logs and Reports

The firewall maintains detailed logs of all network activity, helping with security audits and troubleshooting.

Go to Services > Web Proxy > Access Log. Check the firewall logs for accurate logging of blocked and allowed traffic.



Services: Web Proxy: Access Log

Date	Severity	Process	Line
2024-12-02T18:11:05.226			1 192.168.15.11 NONE_NONE/503 55523 GET https://tiles-cdn.prod.ads.prod.webservices.mozgcp.net/RZEMsHPaTRALRfzVfEmS2KHuuyvX5QITKubdIrxILAI=.10884.jpg - HIER_NONE/- text/html
2024-12-02T18:11:05.224			24 192.168.15.11 NONE_NONE_ABORTED/000 0 CONNECT 34.36.165.17:443 - ORIGINAL_DST/34.36.165.17 -
2024-12-02T18:11:05.194			1 192.168.15.11 NONE_NONE/503 55523 GET https://tiles-cdn.prod.ads.prod.webservices.mozgcp.net/PU5wogQ1m83eJB_LfqAP_PPcUdlXugqxpwzpdHZnNlk=.8480.jpg - HIER_NONE/- text/html
2024-12-02T18:11:05.192			24 192.168.15.11 NONE_NONE_ABORTED/000 0 CONNECT 34.36.165.17:443 - ORIGINAL_DST/34.36.165.17 -
2024-12-02T18:11:05.161			1 192.168.15.11 NONE_NONE/503 55523 GET https://tiles-cdn.prod.ads.prod.webservices.mozgcp.net/ydUu3ZjEx4-B5Lufmypmi0NqdfuZh3doEVs2ffjQNVk=.10324.jpg - HIER_NONE/- text/html
2024-12-02T18:11:05.160			24 192.168.15.11 NONE_NONE_ABORTED/000 0 CONNECT 34.36.165.17:443 - ORIGINAL_DST/34.36.165.17 -
2024-12-02T18:11:04.376			0 192.168.15.11 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
2024-12-02T18:11:04.376			1 192.168.15.11 NONE_NONE/503 55533 POST https://merino.services.mozilla.com/api/v1/curated-recommendations - HIER_NONE/- text/html
2024-12-02T18:11:04.374			23 192.168.15.11 NONE_NONE_ABORTED/000 0 CONNECT 34.110.138.217:443 - ORIGINAL_DST/34.110.138.217 -
2024-12-02T18:10:51.362			13 192.168.15.11 TCP_MISS_ABORTED/503 55785 POST http://91.108.23.100/api - ORIGINAL_DST/91.108.23.100 text/html
2024-12-02T18:10:51.349			8 192.168.15.11 NONE_NONE/000 0 CONNECT 91.108.23.100:443 - HIER_NONE/- -
2024-12-02T18:10:47.742			1 192.168.15.11 NONE_NONE/503 55528 GET https://img-getpocket.cdn.mozilla.net/404x202/filters:format(jpeg):quality(60):no_upscale():strip_exif()/https%3A%2F%2Fstatic1.makeuseofimages.com%2Fwordpress%2Fwp-content%2Fuploads%2Fwm%2F2024%2F11%2Ffeet-fidget-bar.JPG - HIER_NONE/- text/html

Figure 73 Firewall logs

f. Secure Remote Access

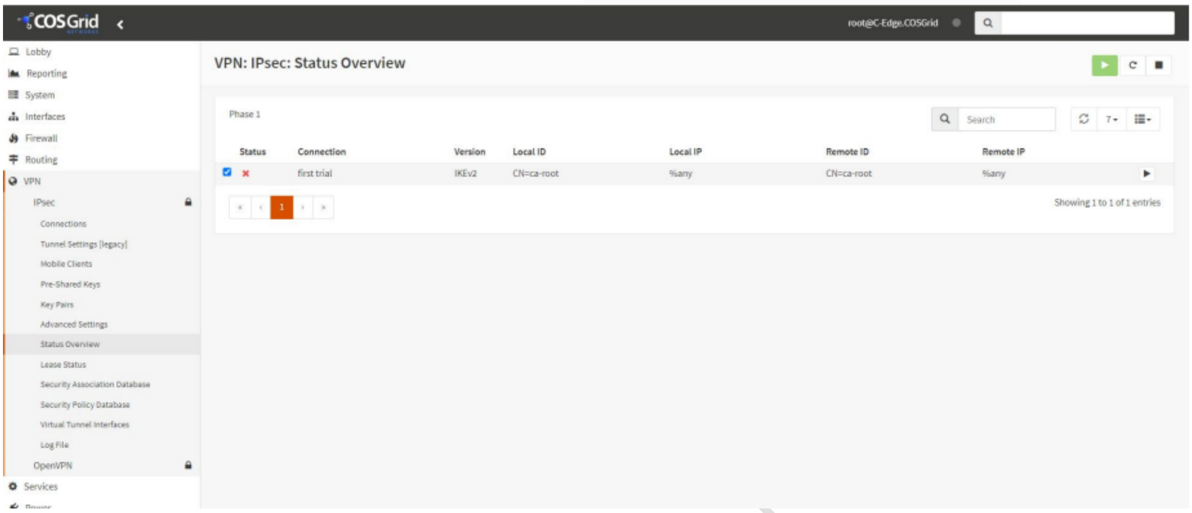
VPN connections are commonly utilized by companies to establish connections between branch offices and remote users. The COSGrid Firewall is designed to support these VPN connections, catering to both branch offices and remote users. With its user-friendly graphical interface, it allows for the seamless setup of a secure private network, enabling multiple branch offices to connect to a central site. Additionally, the firewall provides the capability to create and revoke certificates for remote users, and a convenient export utility simplifies the client configuration process.

i. SSL and IPSec VPN Support

SSL VPN provides a web-based portal for users to access internal resources from a browser via the LAN interface IP Address.

To configure IPSec VPN, select the VPN-> IPSec on the navigation bar. IPSec VPN configurations has Pre-shared keys, key pairs, Lease status, Mobile clients, connection status, logfiles etc.

Pre Shared Keys: Define secrets to be used for local authentication. Navigate to the menu VPN -> IPSec -> Pre-shared keys. The Pre-Shared Keys window appears and you can add/ configure the pre-shared keys parameters by clicking Add button available on the right bottom of the window



VPN: IPsec: Status Overview

Phase 1

	Status	Connection	Version	Local ID	Local IP	Remote ID	Remote IP	
☑	✗	first trial	IKEv2	CN=ca-root	%any	CN=ca-root	%any	▶

Showing 1 to 1 of 1 entries

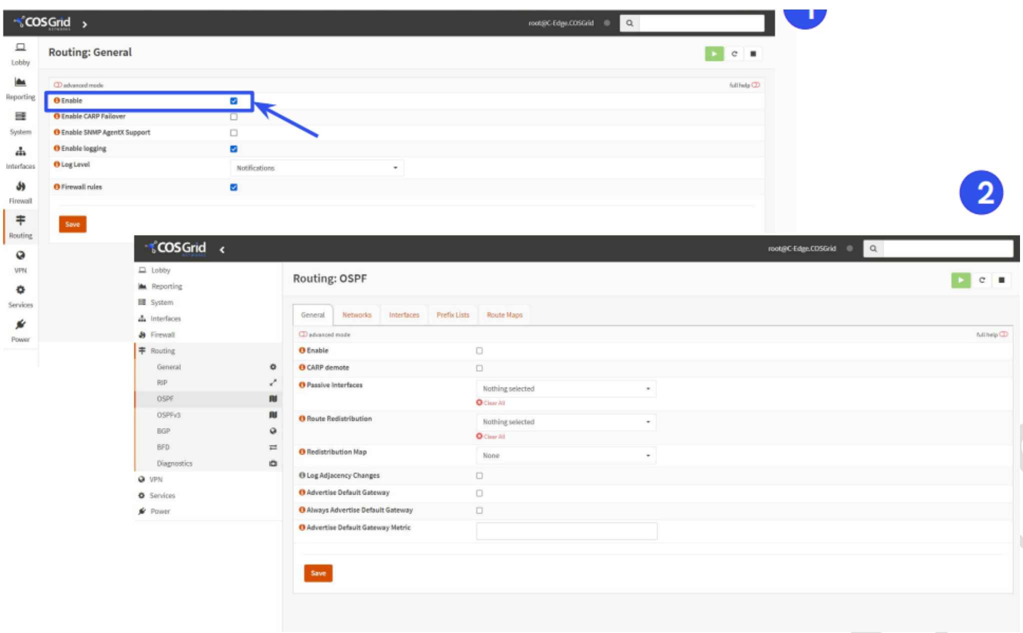
Figure 74 Configuring IPSec in Firewall

ii. Web-Portal and Full VPN Client Application

A web-based VPN portal allows remote users to access internal applications securely. Users can connect using a web browser without needing additional software.

iii. Site-to-Site IPSec VPN (with Dynamic Routing)

Dynamic routing, or adaptive routing, is the intelligent redirection of data through an alternative path to reach a specific destination. Here you go to configure Dynamic routing of the firewall’s BGP, OSPF, RIP.



Routing: General

- Enable ☑
- Enable CARP Failover ☐
- Enable SNMP AgentX Support ☐
- Enable logging ☑
- Log Level: Notifications
- Firewall rules ☑

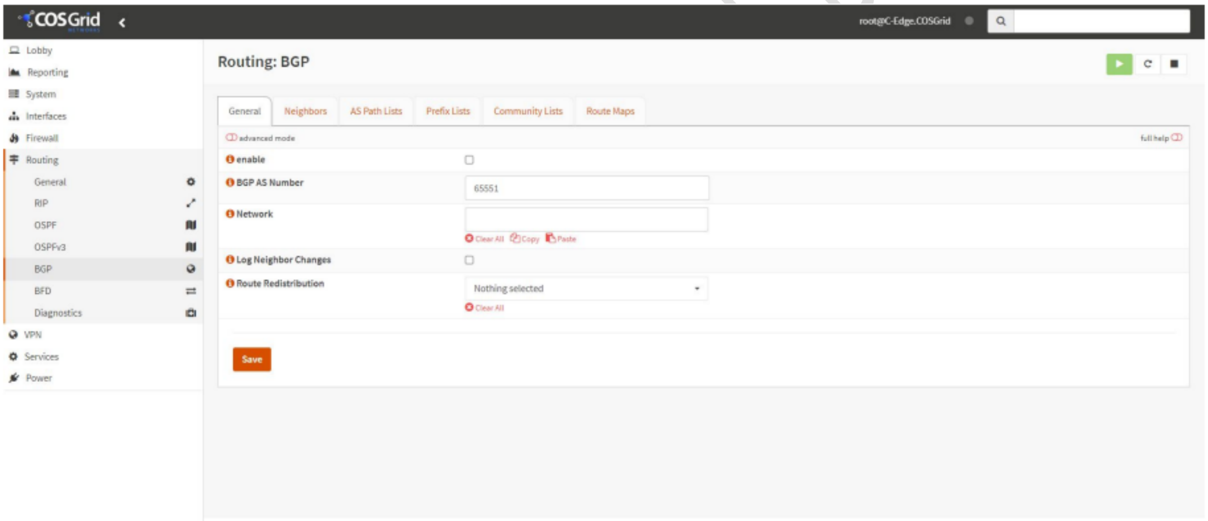
Save

Routing: OSPF

- Enable ☐
- CARP demote ☐
- Passive Interfaces: Nothing selected (Clear All)
- Route Redistribution: Nothing selected (Clear All)
- Redistribution Map: None
- Log Adjacency Changes ☐
- Advertise Default Gateway ☐
- Always Advertise Default Gateway ☐
- Advertise Default Gateway Metric:

Save

Figure 75 Firewall routing



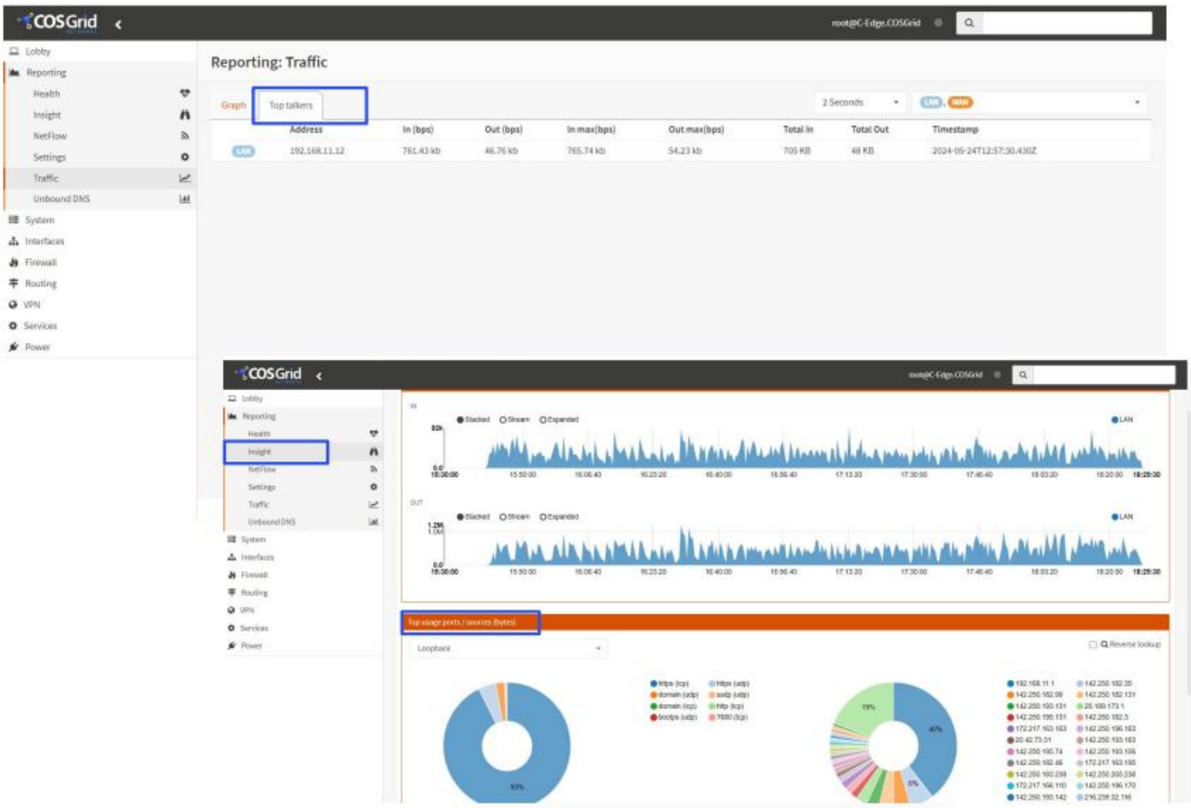
Routing: BGP

- enable ☐
- BGP AS Number: 65551
- Network: (Clear All, Copy, Paste)
- Log Neighbor Changes ☐
- Route Redistribution: Nothing selected (Clear All)

Save

g. Detailed reporting and network visibility

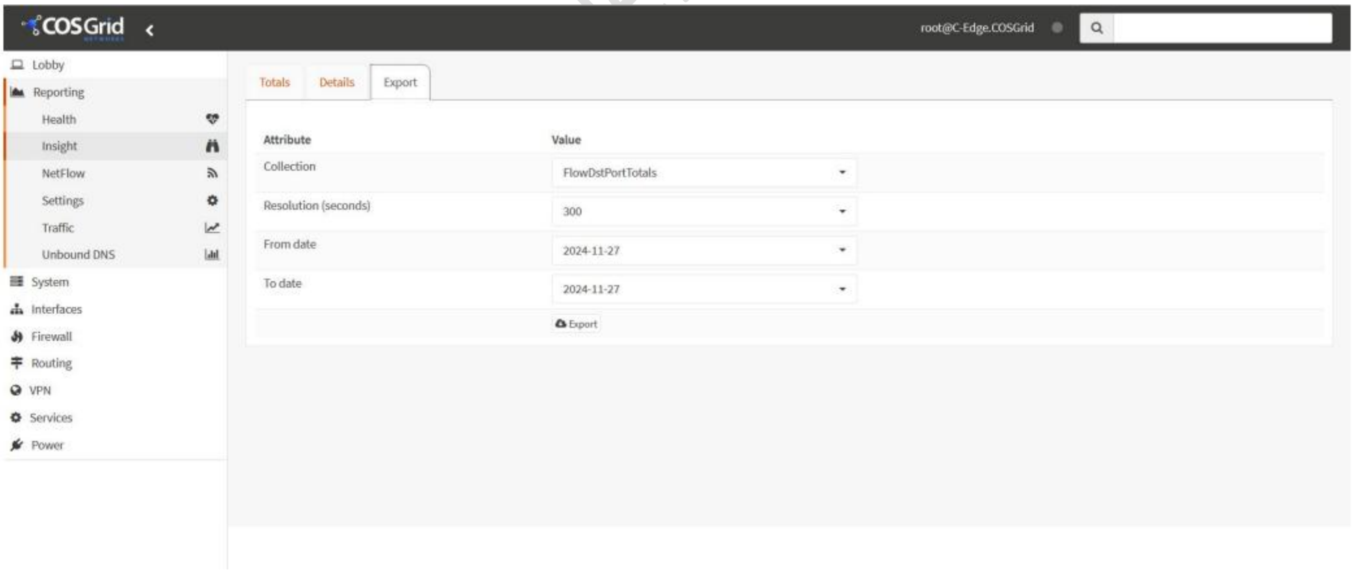
The firewall provides real-time analytics and historical reports on network activity. Dashboards display top talkers, application usage, and potential security threats. Logs can be exported for compliance audits and forensic analysis.



Reporting: Traffic

	Address	In (bps)	Out (bps)	In max(bps)	Out max(bps)	Total In	Total Out	Timestamp
LAN	192.168.11.12	761.43 kb	46.76 kb	765.74 kb	54.23 kb	705 KB	48 KB	2024-05-24T12:57:30.430Z

Figure 76 Firewall reporting



Attribute	Value
Collection	FlowDstPortTotals
Resolution (seconds)	300
From date	2024-11-27
To date	2024-11-27
	Export

Figure 77 Insight

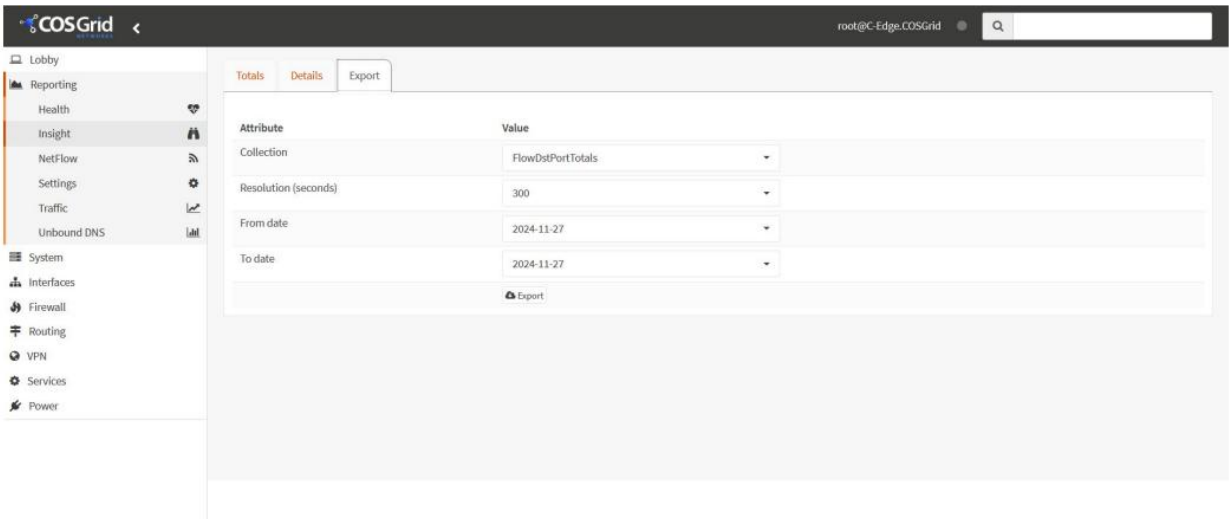
h. Guidelines for the usage

After booting up the system, the firewall will be up and running automatically after around 10 minutes.

While turning off the setup, it is necessary to power off the firewall manually before turning off the power supply.

Login into the Web UI is required.

Step to power off: In the options available in the left tab, power option is available, click on that, option to gracefully power off the firewall will be visible in the dropdown menu.



Attribute	Value
Collection	FlowDstPortTotals
Resolution (seconds)	300
From date	2024-11-27
To date	2024-11-27

Figure 78 Option to power off the firewall through gui

i. Trouble shooting

The firewall includes built-in diagnostic tools for resolving network issues.

Usability:

- **Ping and Traceroute:** Test network connectivity.
- **Packet Capture:** Analyse traffic for troubleshooting complex issues.
- **System Logs:** Review error messages to identify misconfigurations.

For more details refer to Firewall user manual

15.5G IoT Gateway

The **COSGrid IG4XG 5G IoT Gateway** is a high-performance networking device designed for **secure, fast, and reliable connectivity** in IoT ecosystems. It acts as a bridge between **IoT devices, cloud platforms, and enterprise networks**, facilitating **seamless data exchange** using **5G, Ethernet, and Wi-Fi**.

IoT gateways like **IG4XG** play a crucial role in managing **device communication, security, and data routing**, ensuring that IoT deployments are **scalable, secure, and efficient**. The gateway supports multiple protocols, allowing it to communicate with different types of IoT devices across industries such as **smart cities, healthcare, industrial automation, and enterprise networking**.

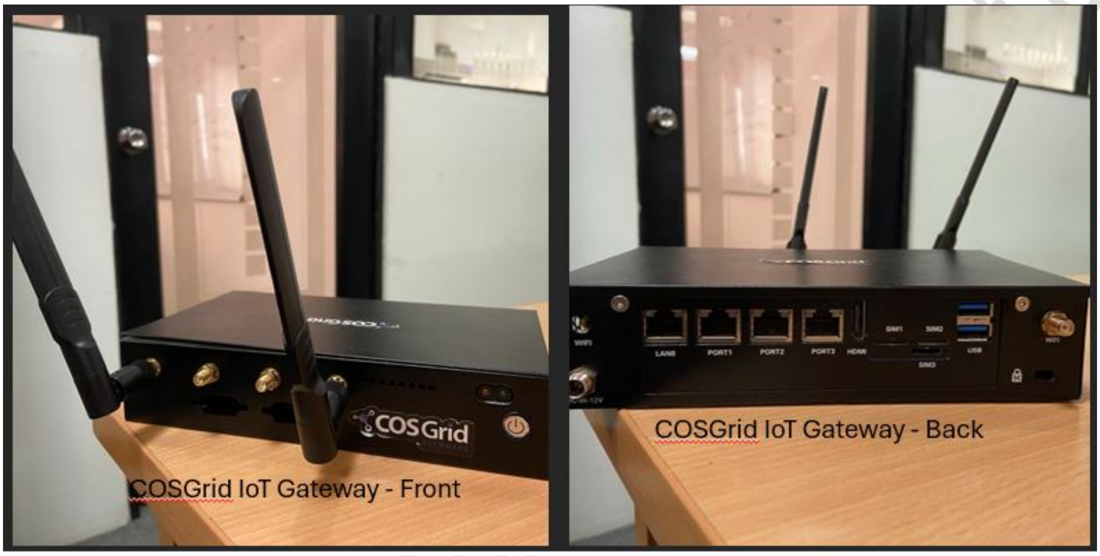


Figure 79 IoT Gateway

a. Features of IoT Gateway

The **IG4XG** offers a wide range of features that enhance **connectivity, security, and management** in IoT applications.

Key Features

- **5G & Multi-Network Support**
  - Supports 5G Sub-6 GHz with SA (Standalone) & NSA (Non-Standalone) modes.
  - Compatible with LTE (4G) for fallback connectivity.
  - Dual SIM support for network redundancy.
- **High-Speed Wireless & Wired Connectivity**
  - Wi-Fi 802.11b/g/n/ac (2.4 GHz & 5 GHz) for wireless IoT devices.
  - 4 Gigabit Ethernet ports for stable wired connections.
- **Security & Firewall**

  - IP Filtering, NAT, ACLs, and Stateful Firewall.
  - DDoS protection to prevent cyber-attacks.
  - Web Filtering to block malicious or unwanted websites.
- **VPN & VLAN Capabilities**
  - WireGuard, OpenVPN, and IPSec VPN for secure remote access.
  - Tag-based VLAN (802.1Q) & Port-based VLAN for network segmentation.
- **IoT Protocol Support**
  - Supports MQTT, CoAP, HTTP/HTTPS, and Modbus for IoT device communication.
- **Cloud & Edge Computing**
  - Seamless cloud integration with AWS, Azure, and private clouds.
  - Local data processing to reduce latency and optimize bandwidth.
- **Management & Monitoring**
  - Zero-touch provisioning for easy deployment.
  - Web GUI, Mobile App, SSH, and SNMP for remote management.
  - Firmware updates and traffic flow analytics.

b. IoT Gateway Architecture

The **COSGrid IG4XG Gateway** has a **modular architecture**, ensuring **high performance, security, and adaptability** in IoT environments.

Hardware Architecture

1. **Processor & Memory**
   - Intel® Celeron® J3455 Quad-Core CPU (1.5GHz–2.3GHz).
   - 8GB DDR3L RAM for smooth data processing.
   - 60GB SSD storage for firmware and local processing.
2. **Networking Interfaces**
   - 4 x Gigabit Ethernet LAN ports for wired IoT devices.
   - Dual-band Wi-Fi (2.4GHz & 5GHz) for wireless devices.
   - 5G/4G LTE module with Dual SIM slots for mobile network connectivity.
3. **Antenna Configuration**
   - 6 LTE/5G antennas for strong cellular reception.
   - 2 Wi-Fi antennas for enhanced wireless performance.
4. **Power & Environmental Specs**

- 12V DC, 60W Adapter.
- Rugged industrial design, suitable for indoor and outdoor deployments.

Software & Security Architecture

The software side of the gateway includes **multiple security layers, device management tools, and data optimization features**:

- Multi-layer firewall protection to filter and control traffic.
- Built-in DDoS protection against cyber threats.
- IP Filtering & Access Control Lists (ACLs) for network security.
- Cloud & Edge computing support for real-time IoT data processing.

c. Communication protocols used in IoT gateway

The COSGrid IG4XG supports multiple IoT communication protocols, ensuring seamless integration with industrial and cloud platforms.

d. Accessing the web page of IoT gateway via ethernet

- There are four ethernet ports on IoT gateway, connect the ethernet cable to **LAN-0 port** (refer **Figure 79**) and the other end can be connected to the L-2 switch
- Ensure your host device has an ip address with 192.168.11.x(not 192.168.11.1) series with 255.255.255.0 netmask and 192.168.11.1 as gateway
- Check if the IoT gateway pings from the gNodeB/ host machine, by pinging 192.168.11.1

  User: root

  Password: ecsd-edge@3682

The password for Wifi created by IOT Gateway is “COS-WAN@945”, the Wifi name is C-Edge

e. VLAN (Virtual Local Area Network)

VLANs allow network segmentation to improve security and performance in IoT deployments.

i. Simultaneous Server and Multiple Clients

- Supports multiple VLANs on Ethernet and Wi-Fi interfaces.
- VLANs can be used to separate IoT sensors, industrial controllers, and cloud services.

ii. VPN Client and Server Support

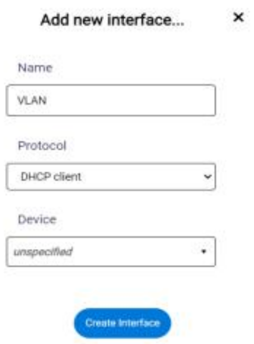
- Supports WireGuard, OpenVPN, and IPSec VPN.
- Can be used for secure remote device access and site-to-site networking.

iii. Port and Tag-Based VLAN

- Port-based VLAN: Assign specific LAN ports to separate VLANs.
- Tag-based VLAN (802.1Q): Packets are tagged with VLAN IDs for dynamic network segmentation.

Configuration of VLAN:

Click ***Network -> Interfaces.*** The Interfaces overview page appears as given below. Click **Add** Button Avaialble on the right bottom of the window.



Add new interface... ×

Name

VLAN

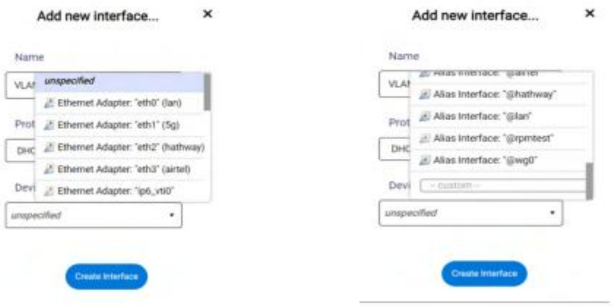
Protocol

DHCP client

Device

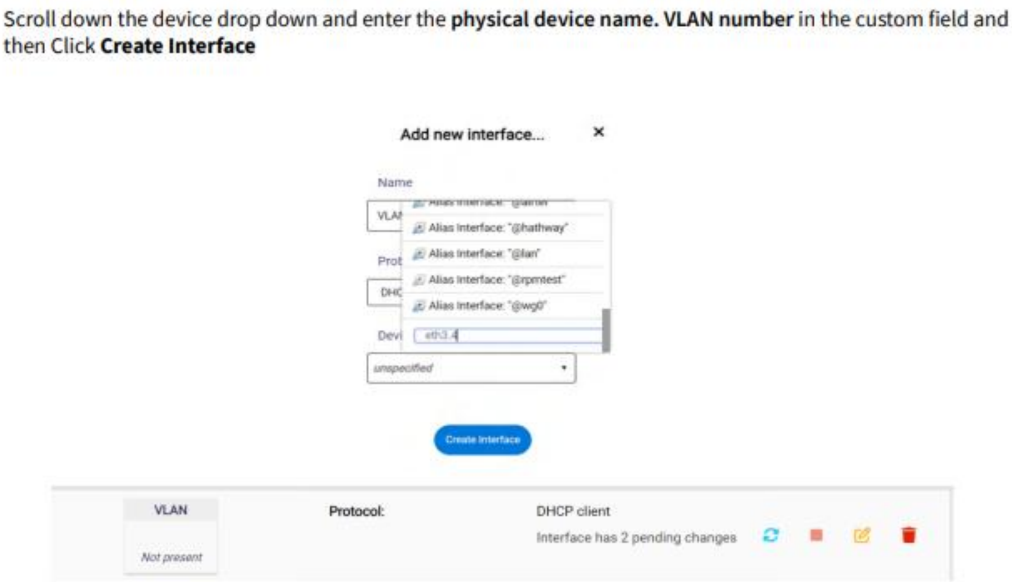
unspecified

Name the Interface and select anyone of the protcol in the protocol dropdown. Select the device dropdown.



Add new interface... ×
Name
VLAN
Prot
DHC
Devi
unspecified
Ethernet Adapter: "eth0" (lan)
Ethernet Adapter: "eth1" (5g)
Ethernet Adapter: "eth2" (hathway)
Ethernet Adapter: "eth3" (airtel)
Ethernet Adapter: "ip6_vti0"
unspecified
Create Interface
Add new interface... ×
Name
VLAN
Prot
DHC
Devi
Alias Interface: "@airtel"
Alias Interface: "@hathway"
Alias Interface: "@lan"
Alias Interface: "@rpmtest"
Alias Interface: "@wg0"
-- custom --
unspecified
Create Interface

Figure 80 VLAN configuration



Scroll down the device drop down and enter the **physical device name. VLAN number** in the custom field and then Click **Create Interface**

Add new interface... ×

Name: VLAN

Protocol: DHCP

Alias Interface: "@hathway"
Alias Interface: "@lan"
Alias Interface: "@rpmtest"
Alias Interface: "@wg0"

Device: eth3.4

unspecified

Create Interface

VLAN	Protocol:	DHCP client
Not present		Interface has 2 pending changes

Figure 81 VLAN configuration

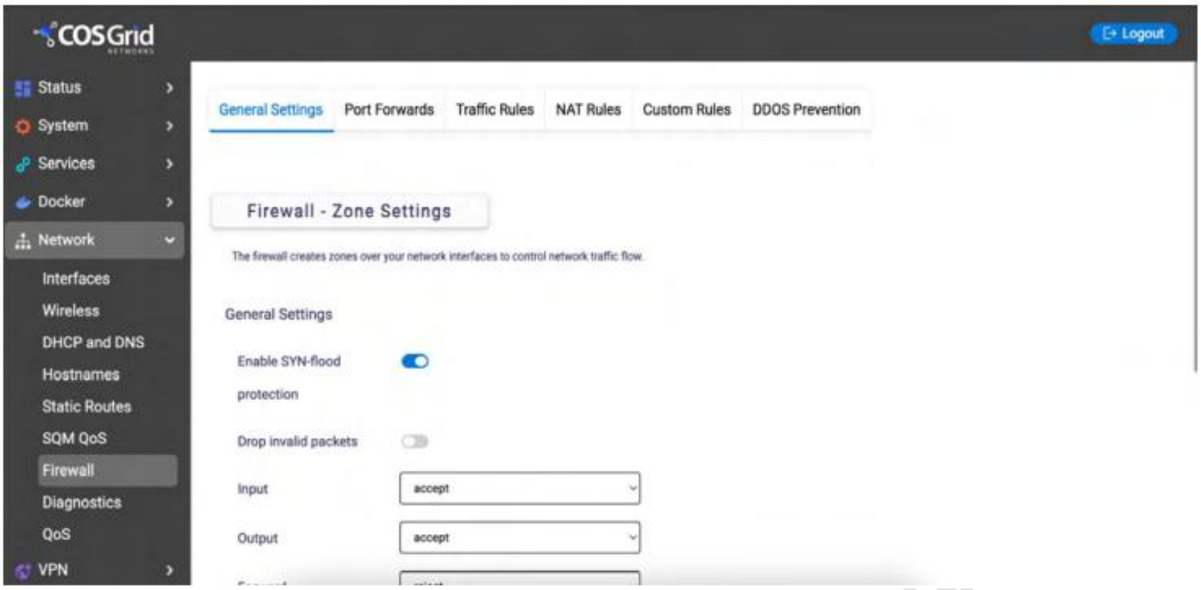
e. Security

i. Firewall Rules

- Built-in Stateful Firewall to allow/block traffic.
- Supports custom traffic filtering & NAT rules.
- Managed via Web UI or CLI.

Configuring firewall using the web interface:

Navigate the menu Network ->Firewall . The Firewall Configuration window appears . It has 5 sections namely General Settings, Port Forwards, Traffic Rules, NAT Rules , Custom Rules and DDOS Prevention.



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection ●

Drop invalid packets ○

Input: accept

Output: accept

Figure 82 Firewall setting

ii. DDoS Prevention

- Protection against SYN floods, port scans, and malformed packets.

iii. Data Limit for SIM Card

iv. Blocking of Unwanted Websites

- Web filtering allows blacklisting & whitelisting of URLs.
- Managed via Services →URL Blocking.

f. Guideline for SIM Insertion

Steps to Insert SIM Card Properly:

1. Power Off the Gateway before inserting the SIM.
2. Locate the SIM slot -1
3. Insert the Nano SIM in the correct orientation.
4. Power on the device and check SIM detection in the Web UI.

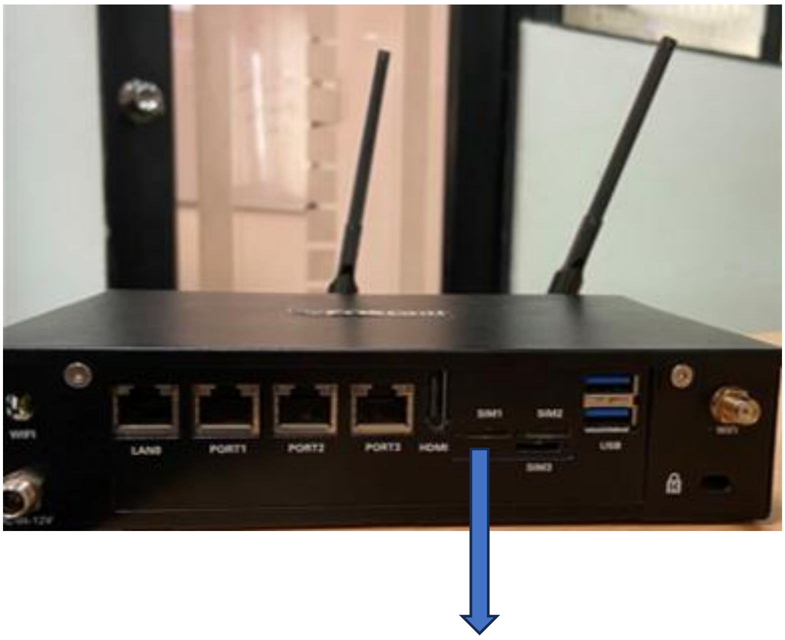
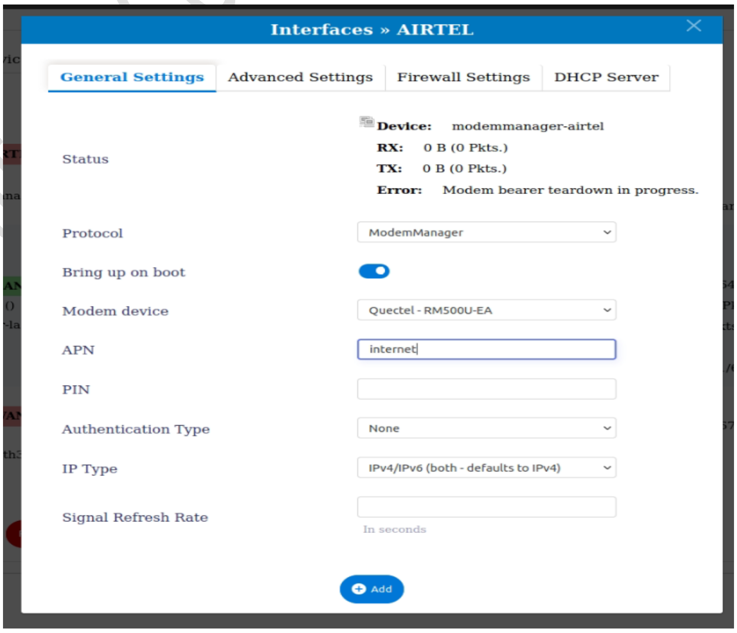


Figure 83 Slot to insert the SIM Card for 5g connectivity

g. APN Settings

Navigate the menu Network -> Interface. Click on the Edit icon available right to the created Mobile Interface . The dialog box will appears. In that Select General Settings tab. In the General Settings You can setup the mobile interface APN ,PIN , Authentication Type and status area shown the current status of the mobile interface.



Interfaces » AIRTEL

Status
Device: modemmanager-airtel
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Error: Modem bearer teardown in progress.

Protocol: ModemManager
Bring up on boot: ●
Modem device: Quectel - RM500U-EA
APN: internet
PIN:
Authentication Type: None
IP Type: IPv4/IPv6 (both - defaults to IPv4)
Signal Refresh Rate:
In seconds

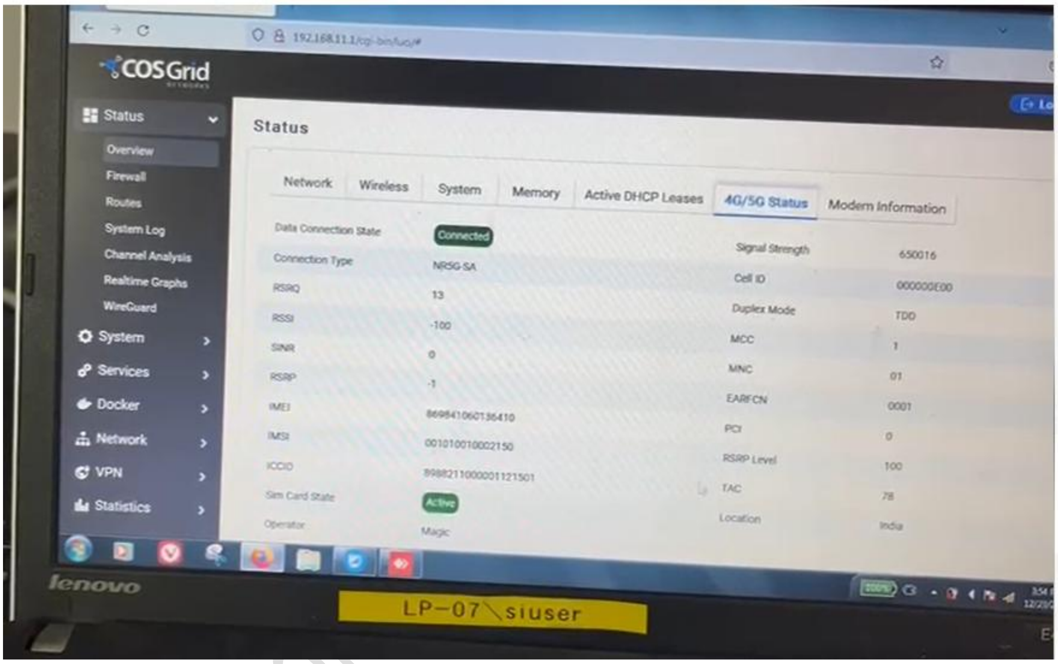
Figure 84 APN setting

For Singaltron gNB, APN is internet and PIN field is left empty.

h. Registering IoT Gateway to 5G Network

Steps to Connect to 5G:

1. Insert SIM Card & Power On the device.
2. Login to Web UI via 192.168.11.1
3. Configure APN Settings (as per Step g).
4. Monitor Connection Status under Network → Mobile.
5. Check Signal Strength via RSSI, SINR, RSRP indicators.



Status

Data Connection State: Connected
Connection Type: NR5G-SA
RSRQ: 13
RSSI: -100
SINR: 0
RSRP: -1
IMEI: 869841060136410
IMSI: 001010010002150
ICCID: 89882110000011215 01
Sim Card State: Active
Operator: Magic

Signal Strength: 650016
Cell ID: 000000E00
Duplex Mode: TDD
MCC: 1
MNC: 01
EARFCN: 0001
PCI: 0
RSRP Level: 100
TAC: 78
Location: India

Figure 85 Status of IoT Gateway

i. Trouble shooting

Issue	**Possible Cause**	**Solution**
No 5G Connection	Weak signal, incorrect APN	Adjust device location, verify APN settings
SIM Not Detected	Faulty SIM, incorrect insertion	Reinsert SIM, restart device
Slow Internet	Network congestion, poor signal	Change network mode (Auto/5G/4G)
VPN Not Connecting	Firewall block, incorrect config	Verify firewall rules, check VPN logs

For more information about IoT Gateway, refer the User manual of IoT Gateway

16.5G Indoor CPE

KCP-5G-510 is a two-radio, 4x4 MIMO 802.11ax 5G CPE. Designed for general-purpose, next-generation deployments in harsh outdoor locations and industrial conditions, the KCP-5G-510 offers performance, enterprise-grade security, and intuitive management.KCP-5G-510 delivers the high throughput, reliability, and flexibility required by the most demanding business applications like voice and high-definition streaming video, even in the harshest outdoor environments.

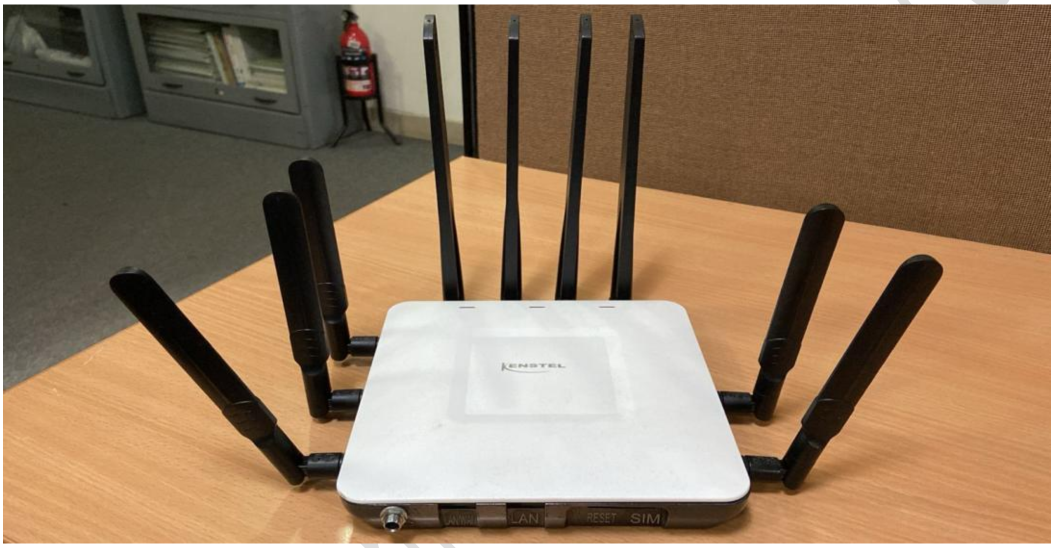


Figure 86 CPE connected with private 5G network and providing WiFi

a. CPE system architecture

A 5G Indoor CPE serves as a bridge between the 5G network and end-user devices, facilitating high-speed internet access within indoor environments. Its architecture typically comprises the following components:

- **5G Modem:** Connects to the 5G cellular network, enabling data transmission and reception.
- **Processor and Memory:** Handles data processing tasks and manages device operations.
- **Wi-Fi Module:** Distributes the received 5G signal to local devices via Wi-Fi.

- **Ethernet Ports:** Provide wired connections for devices requiring stable and high-speed links.
- **Power Supply:** Powers the CPE device.

This integrated design ensures seamless conversion of 5G signals into Wi-Fi or Ethernet, catering to various user requirements.

b. Wireless access interfaces

The **Kenstel KCP-5G-510I** provides multiple wireless connectivity options:

- **5G NR Connectivity**:
  - Supports mm Wave and sub-6 GHz bands.
  - Peak Download Speed: 7500 Mbps, Peak Upload Speed: 3000 Mbps.
  - Performance Enhancements: Qualcomm 5G PowerSave, Smart Transmit, Wideband Envelope Tracking.
- **Wi-Fi Access**:
  - Wi-Fi 6 (802.11ax) support for high-speed local connectivity.
  - 2.4GHz Wi-Fi: 2x2 MIMO up to 600Mbps.
  - 5GHz Wi-Fi: 4x4 MIMO up to 4.8Gbps.
  - Supports Mesh Networking with self-configuring and self-healing capabilities.

c. Security

i. Latest WPA Support

- Supports WPA2 AES-PSK and WPA2 Enterprise for secure Wi-Fi authentication.
- MAC Address Filtering: Allows up to 32 MAC addresses per SSID for access control.

ii. Rogue Access Point Detection and Prevention

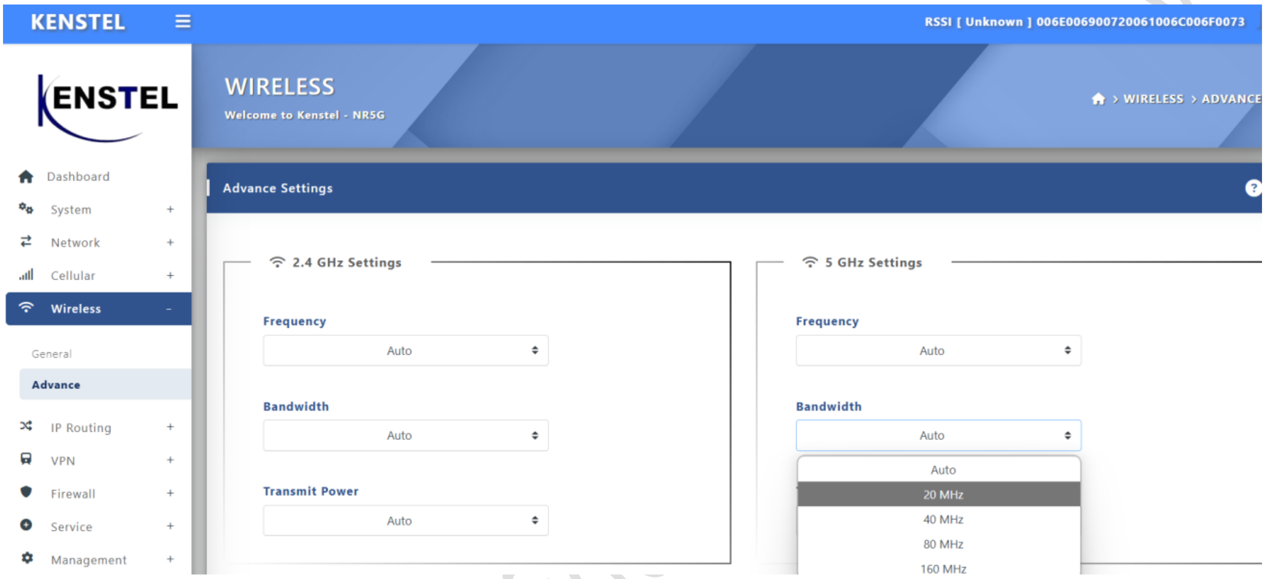
- Hides SSID in Beacons to prevent unauthorized scanning.
- Client Isolation: Restricts communication between connected devices, preventing lateral attacks.

iii. IP Security (IPSec), PPTP, IP-Filtering

- VPN Client Support: L2TP, PPTP for encrypted remote access.
- IP Filtering: Blocks unauthorized IP addresses from accessing the network.
- HTTPS and SSH Support: Secure web and terminal management.

iv. MAC Address Authentication

- Whitelist trusted MAC addresses to prevent unauthorized devices from connecting.



Advance Settings

2.4 GHz Settings

Frequency: Auto

Bandwidth: Auto

Transmit Power: Auto

5 GHz Settings

Frequency: Auto

Bandwidth: Auto

Figure 87 CPE setup

d. Registering CPE to 5G network:

Configuring **5G connectivity** on the CPE involves the following steps:

1. Connect power to CPE
2. Connect ethernet cable from 24 port switch to LAN port of the CPE

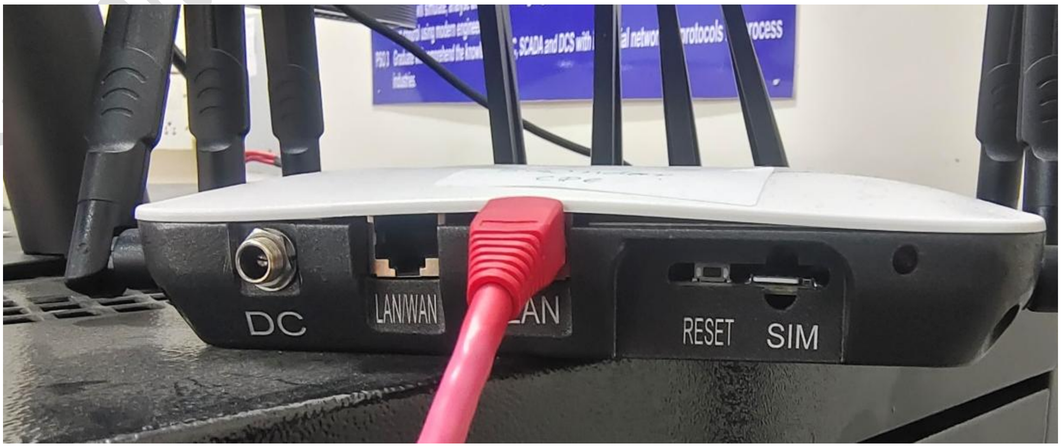


Figure 88 CPE Ethernet port

3. Insert SIM Card into the provided slot

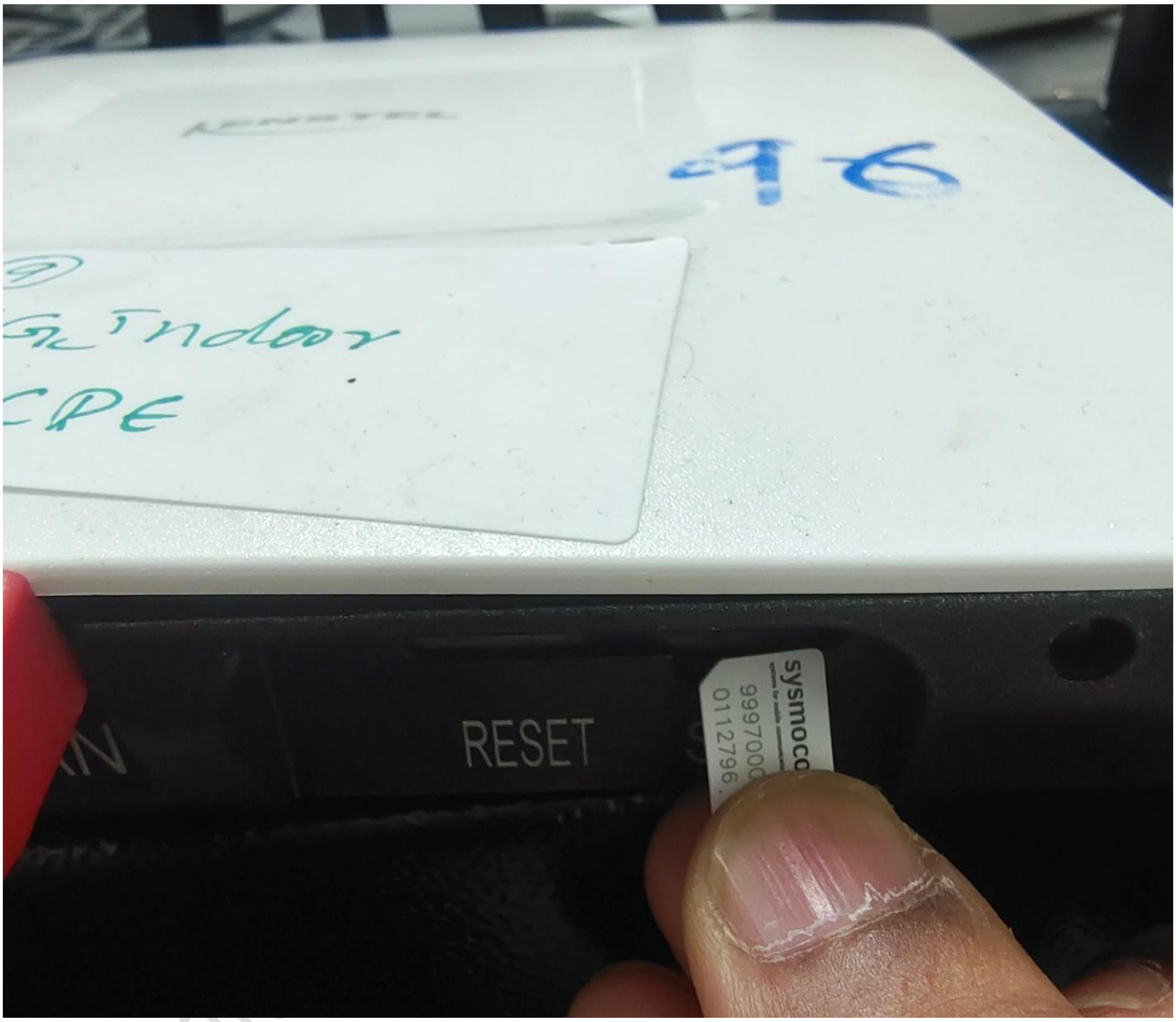
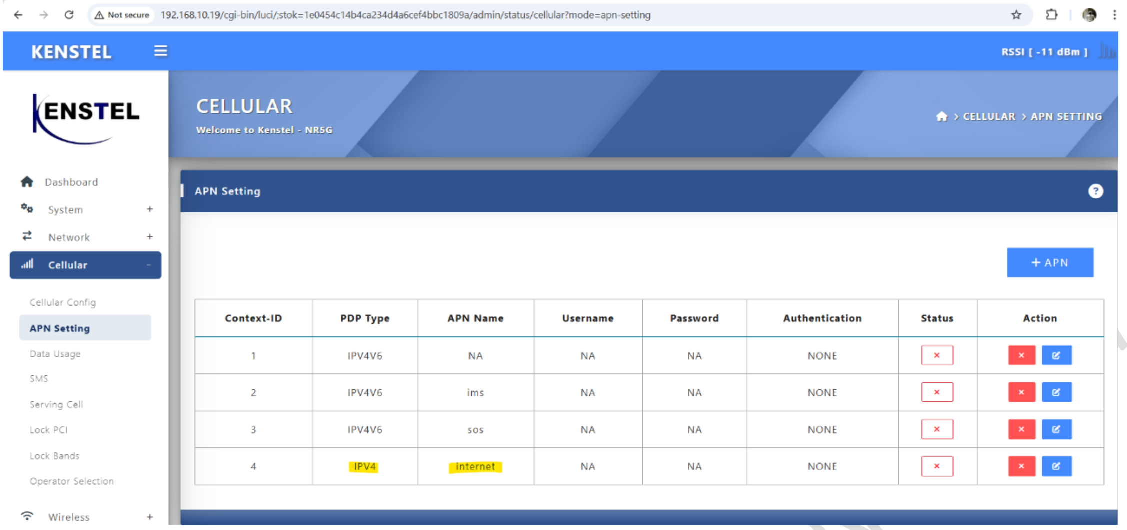


Figure 89 CPE sim card orientation

4. Login to the Web UI via an Ethernet-connected device using a web browser
   - URL: 192.168.10.19 (just type this in your browser in gNodeB)
   - Username: root
   - Password: Signaltron
5. Set APN (Access Point Name) according to the mobile network provider’s settings. (internet in case of Signaltron gNodeB)

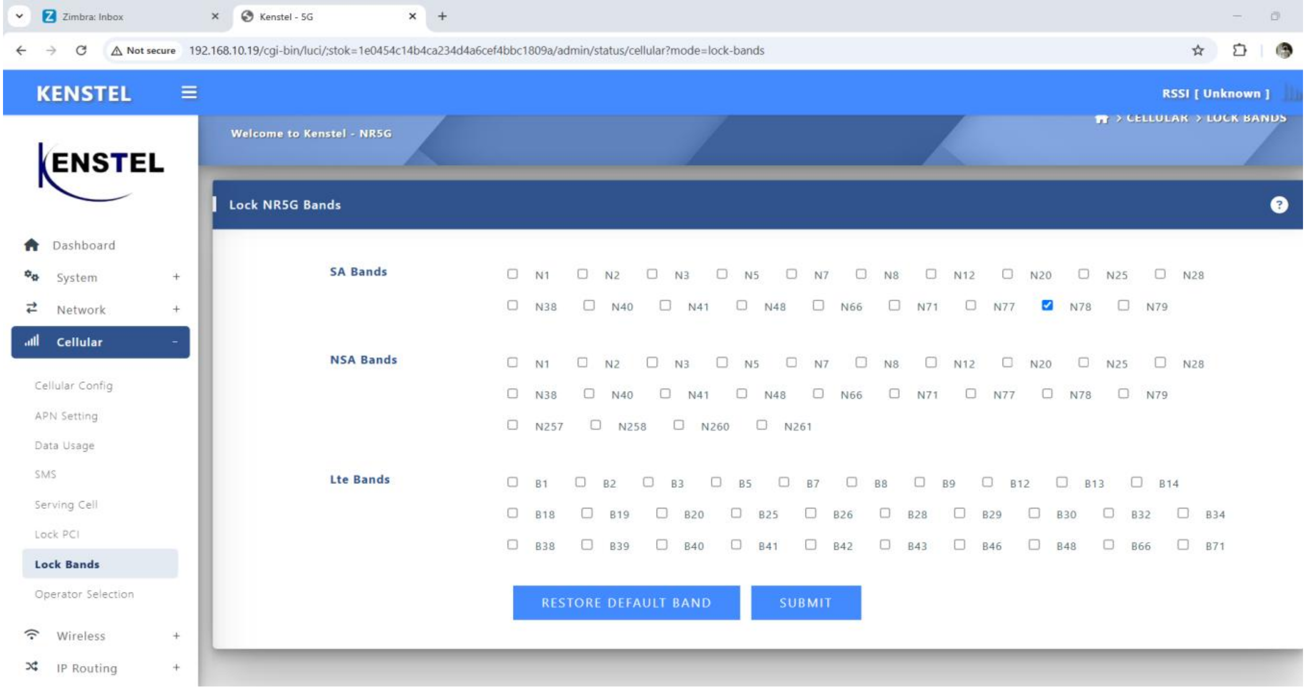
- Under Cellular - > APN Setting -> apn should be “internet”



APN Setting

Context-ID	PDP Type	APN Name	Username	Password	Authentication	Status	Action
1	IPV4V6	NA	NA	NA	NONE	×	× ✎
2	IPV4V6	ims	NA	NA	NONE	×	× ✎
3	IPV4V6	sos	NA	NA	NONE	×	× ✎
4	IPV4	internet	NA	NA	NONE	×	× ✎

6. Select only N-78 band in Lock Bands for faster search and faster registration.
    - Under Cellular -> Lock Bands -> select only n78 in SA and deselect all other bands -> submit



Lock NR5G Bands

SA Bands
□ N1 □ N2 □ N3 □ N5 □ N7 □ N8 □ N12 □ N20 □ N25 □ N28
□ N38 □ N40 □ N41 □ N48 □ N66 □ N71 □ N77 ☑ N78 □ N79

NSA Bands
□ N1 □ N2 □ N3 □ N5 □ N7 □ N8 □ N12 □ N20 □ N25 □ N28
□ N38 □ N40 □ N41 □ N48 □ N66 □ N71 □ N77 □ N78 □ N79
□ N257 □ N258 □ N260 □ N261

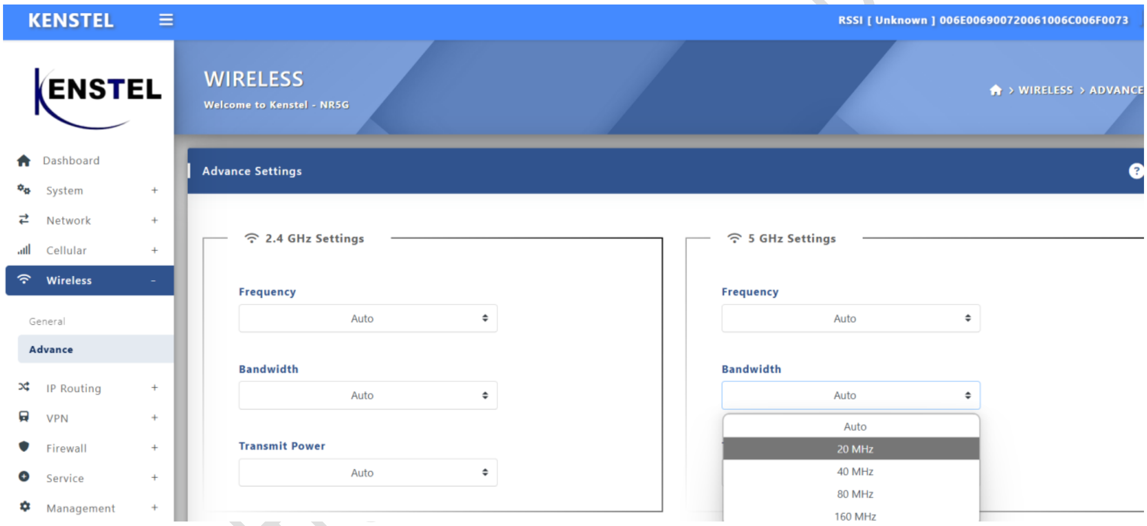
Lte Bands
□ B1 □ B2 □ B3 □ B5 □ B7 □ B8 □ B9 □ B12 □ B13 □ B14
□ B18 □ B19 □ B20 □ B25 □ B26 □ B28 □ B29 □ B30 □ B32 □ B34
□ B38 □ B39 □ B40 □ B41 □ B42 □ B43 □ B46 □ B48 □ B66 □ B71

7. The CPE should register automatically, if it fails, one can do manual search in operator selection and select the network manually

e. Wi-Fi Settings

To configure Wi-Fi settings:

1. SSID Configuration:
   - Set up 8 SSIDs per band (2.4GHz & 5GHz).
   - Assign VLANs to SSIDs for network segmentation.
2. Channel Selection:
   - 2.4GHz Range: 2400 MHz – 2482 MHz.
   - 5GHz Range: 5150 MHz – 5850 MHz.
   - Auto-select optimal channels to reduce interference.
3. Enable WPA2 Security with a strong password.
4. Enable Client Isolation to prevent direct communication between connected devices.
5. Activate QoS (Quality of Service) to prioritize critical applications.



2.4 GHz Settings

Frequency: Auto

Bandwidth: Auto

Transmit Power: Auto

5 GHz Settings

Frequency: Auto

Bandwidth: Auto

Figure 90 Connecting 5G Indoor CPE to 5G and Wi-Fi Network

To set up the Kenstel KCP-5G-510I:

a. Power On the device using PoE or DC Adapter.

b. Connect to the Web Interface:
   - Open a web browser and enter the default IP address.
   - Log in with default credentials (if applicable).

c. Insert and Configure SIM Card.

d. Set APN & Network Mode (SA/NSA, Auto, LTE fallback).

e. Configure LAN & WAN Settings:

  - Set WAN type as DHCP, Static, or PPPoE.
  - Assign LAN IP & DHCP server settings.

f. Enable Wi-Fi and Configure SSID.

g. Test connectivity with a speed test or network diagnostics.

Trouble Flexible guest access with device isolation Captive

f. Trouble shooting

Issue Possible Cause Solution

No 5G Signal	Weak coverage, incorrect APN settings	Reposition CPE, check SIM, reconfigure APN
Slow Wi-Fi Speed	Interference, incorrect channel settings	Use **5GHz Wi-Fi**, select an optimal channel
Frequent Disconnections	Firmware bugs, poor signal strength	Update firmware, check **RSSI LEDs** for signal strength
LAN Port Not Working	Faulty cable, incorrect port settings	Try a different cable, ensure LAN settings are correct
Cannot Access Web UI	Wrong IP, network misconfiguration	Reset CPE and use default IP for login

For detailed information please refer to CPE user manual

17.5G SIM Cards

To work with the 5G private network created by Signaltron gNodeB and Niral Core, preconfigured and pre-programmed SIMs are provided. Details of these SIMs are loaded in the Core's database such that when these are used with any User Equipment (UE), they are able to register to the 5G network.

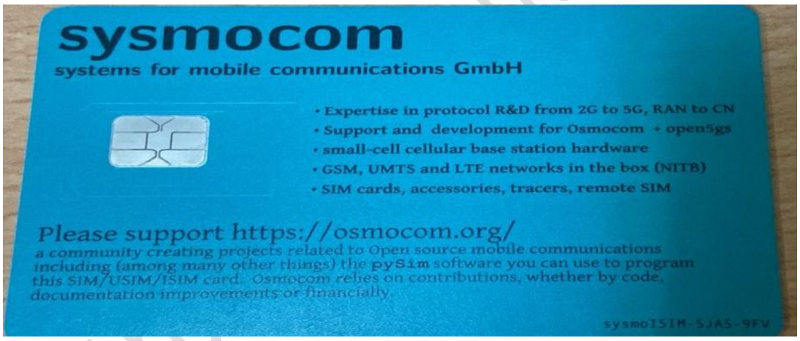

sysmocom
systems for mobile communications GmbH
• Expertise in protocol R&D from 2G to 5G, RAN to CN
• Support and development for Osmocom + open5gs
• small-cell cellular base station hardware
• GSM, UMTS and LTE networks in the box (NITB)
• SIM cards, accessories, tracers, remote SIM
Please support https://osmocom.org/
a community creating projects related to Open source mobile communications including (among many other things) the pySim software you can use to program this SIM/USIM/ISIM card. Osmocom relies on contributions, whether by code, documentation improvements or financially.
sysmoISIM-SJA5-9FV

Figure 91 5G simcard

a. Programming the SIM card

Programming a 5G SIM card involves configuring its identity and authentication parameters to work with a network. The sysmoISIM-SJA5 SIM card can be programmed using tools like pySim-prog.py and sysmo-usim-tool. These tools allow modification of key parameters such as IMSI (International Mobile Subscriber Identity), MSISDN (Mobile Subscriber Integrated Services Digital Network Number), and authentication keys (K, OPC).

To program the SIM:

1. Use a smart card reader compatible with the pcsc-lite software stack.

2. Install pySim-prog.py and sysmo-usim-tool from their respective repositories.
3. Provide the ADM1 PIN to authenticate access.
4. Execute the programming command to modify IMSI, Ki, and OPC values.

E.g../pySim-prog.py -p 0 -t sysmoISIM-SJA5 -a 32627241 -x 901 -y 71 -i 901710000011000 -s 8988211000000110000 -o 398153093661279FB1FC74BE07059FEF -k 1D8B2562B992549F20D0F42113EAA6FB

This modifies the IMSI, authentication key (Ki), and operator-specific keys (OPC)

(Although the SIM cards provided are already programmed and above steps would not be required).

b. Testing for 5G Connectivity

5G connectivity of these sim cards can be easily tested by inserting the provided sim cards in the handsets provided (Samsung M13) or any of the other devices and following the procedures mentioned above. (Just verify that APN internet is added in the devices).

The devices should be able to connect to Signaltron gNB and the same could be verified using the User interface of the devices or through the Niral NMS(registered sim card IMSI will be visible in web UI).

(These sim cards are specifically programmed for this Signaltron gNB and Niral core and would not be able to latch to commercial networks).

Devices that have command line interface, below commands can be used to check 5G connectivity:

Verify connectivity using commands like:

```
mmcli -m 0 --simple-connect="apn=<APN>"
```

Check network registration using:

```
mmcli -m 0 --command="AT+COPS?"
```

These steps ensure that the 5G SIM card is configured correctly and can connect securely to a 5G network.

18.5G Drone

The 5G drone is an Unmanned Aerial Vehicle (UAV) that uses the 5G cellular network for communication and control instead of traditional radio frequency systems like Wi-Fi. This integration with 5G technology offers several advantages over previous generations of drones.

a. Drone System Architecture

The Signaltron drone is a Quadcopter designed for education & research using 5G technologies. The system comprises the following key components:

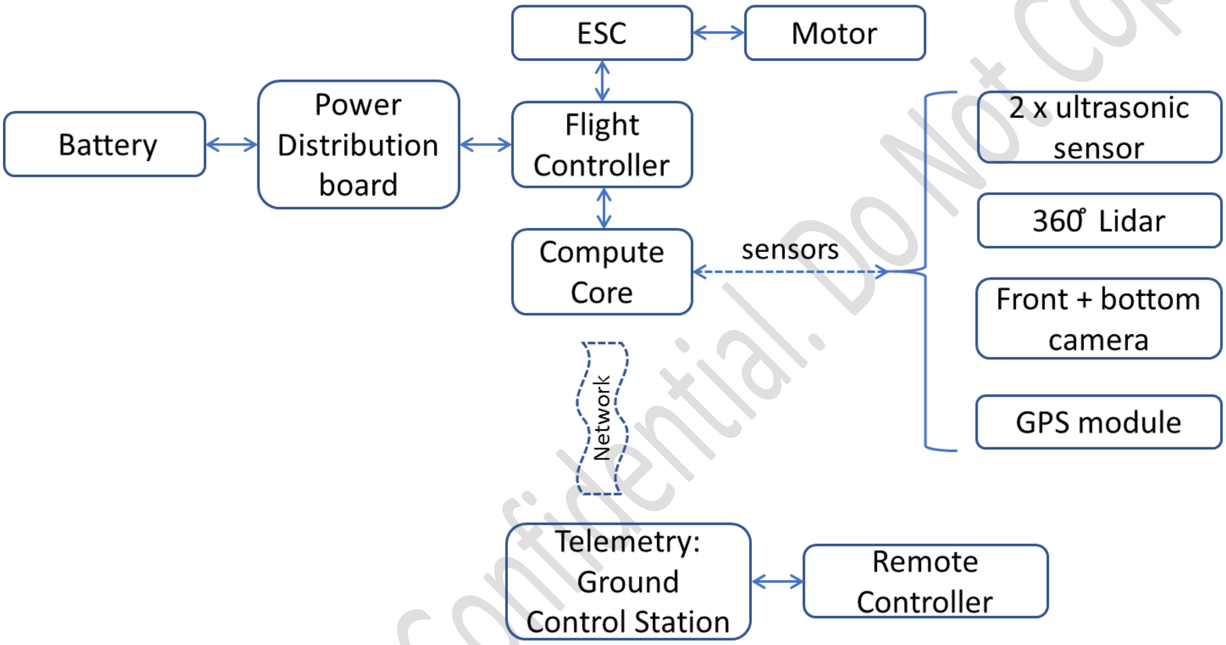


Figure 92 Drone Architecture

- **Compute Core:** Drone is equipped with 2.4GHz quad-core, 64-bit Arm Cortex-A76 CPU. This allows for onboard data processing for AI/ML analytics and running applications. It’s equipped with camera transceivers for low latency video feed and enabling object detection.

  https://datasheets.raspberrypi.com/rpi5/raspberry-pi-5-product-brief.pdf

  - 2.4GHz quad-core, 64-bit Arm Cortex-A76 CPU
  - Video Core VII GPU
  - 5G Cellular connectivity
  - 2.4 GHz and 5.0 GHz 802.11ac Wi-Fi connectivity
  - 2 × 4 lane MIPI camera/display transceivers

- Remote firmware upgrade.

- **Power Distribution Board (PDB):** The Power Distribution Board (PDB) is responsible for distributing power from the battery to the various components of the drone, including the motors, flight controller, ESCs, and other electronics.
  - Type: CDAC PDB
  - Input Voltage: 3S‑6S LiPo (11.1V‑22.2V)
  - BEC (Battery Eliminator Circuit): BEC Output: 3.3V(6A), 5V(6A), 9V(1A) ,12V(1A) (for powering flight controller, receiver, and FPV equipment)
  - Power Input: XT60 connector for battery input

- **Propulsion System:** This BLDC motor has a motor rating of 935kV which is suitable for multirotor. This BLDC motor comes in two variants one with black cap for Clockwise rotation and another pink cap or CCW rotation.
  - Motor Type: Brushless Motor
  - Compatible LiPO Batteries: 3S to 4S
  - Compatible Prop (inch): 8

  Note:

  - The BLDC motor rotation is always opposite to the direction of Thread.
  - In case the motor rotation direction is CCW, so the Thread tightening direction will be CW (“ Left-handed-thread”) and vice versa for CW motor rotation.

- **Flight Controller:** Flight Controller is the brain of the Signaltron drone, responsible for stabilizing the drone and interpreting control inputs. It reads sensor data and adjusts the motor outputs to keep the drone stable and to follow commands. It also manages GPS navigation, failsafe, and mission planning.

  Specifications:

  - Built-in Sensors: 3-axis accelerometer, 3-axis gyroscope, 3-axis magnetometer, barometer, voltage measurement.
  - Flight Modes: Altitude Hold, Head Lock.
  - Flight Planning: Geo fencing, Path planning,
  - Safety Features: Failsafe modes, 360-degree Lidar obstacle detection, ground and ceiling detection.

- **Electronic Speed Controller (ESC):** The Electronic Speed Controller (ESC) is a critical component in a drone’s power system. It regulates the speed of the motors by interpreting signals from the flight controller and adjusting the power sent to each motor accordingly.
    - Type: Brushless
    - Motor Compatibility: Brushless (DC)
- **Battery:** Orange 4500mah 4S 35C Lithium polymer battery Pack (LiPo) batteries are equipped with heavy-duty discharge leads to minimize resistance and sustain high current loads. Orange batteries stand up to the punishing extremes of aerobatic flight and RC vehicles.
    - Type: Lithium Polymer Battery Pack
    - Capacity: 4500mAh
    - Output Voltage(V): 4S (14.8V – 16V)
    - Discharge Plug: XT60
    - Balance Plug: JST-XH
- Note:
    - Always monitor the battery during flight to ensure that it is not discharged completely below the safe voltage
    - For optimal battery life, avoid charging the battery at higher rates than recommended in user guide.
- **Remote Controller:** The drone comes with a Zebronics Max Fury remote controller. It has Type C wired input with RGB LED modes and features an ergonomic and comfortable design. It has dual vibration motors and dual analog sticks.
    - Interface: Detachable Type C to USB cable
    - Compatible OS: Windows/Android
- **Camera System:** The Drone is equipped with two cameras, one at the front and another at the bottom. This allows for RPV (Remote Pilot vehicle) mode, general surveillance, safe landing, aerial photography etc. Front camera comes with tilt feature for extended vision equipped with a 12MP 120° diagonal wide angle of view Sony sensor. Bottom camera is equipped with a Sony 5MP sensor with 60° field of view.

  Refer to “camera module v1” and “camera module v3” in the below link.
  https://www.raspberrypi.com/documentation/accessories/camera.html#hardware-specification
- **GPS Module:** The GPS module is responsible for providing the drone with positioning data.
    - Type: GPS Module

- Input Voltage (V): 3.5 to 3.6
- Position Accuracy (m): 2, 2.5

- Notes: For optimal performance, ensure the GPS module has a clear line of sight to the sky, avoiding obstructions such as large metal objects or dense foliage.

b. System/Sensors specification

The Drone consists built-in Sensors: 3-axis accelerometer, 3-axis gyroscope, 3-axis magnetometer, barometer, voltage measurement.

c. Sensitivity of sensors

d. Limitation of IoT/Sensor devices

e. Flight and Companion Controller

Flight Controller is the brain of the Signaltron drone, responsible for stabilizing the drone and interpreting control inputs. It reads sensor data and adjusts the motor outputs to keep the drone stable and to follow commands. It also manages GPS navigation, fail safes, and mission planning.

Flight controller operation:

- **Left Stick (Throttle/Yaw):**
  - Throttle (Vertical Movement): Controls the drone's altitude. Pushing the stick up increases altitude (ascends), pushing it down decreases altitude (descends).
  - Yaw (Rotation): Controls the drone's rotation around its vertical axis. Moving the stick left rotates the drone counterclockwise (left), moving it right rotates it clockwise (right).
- **Right Stick (Pitch/Roll):**
  - Pitch (Forward/Backward Movement): Controls the drone's forward and backward movement. Pushing the stick forward moves the drone forward, pulling it back moves the drone backward.
  - Roll (Left/Right Movement): Controls the drone's lateral movement (left and right). Moving the stick left moves the drone left, moving it right moves the drone right.
- **Left top button (Arm):**
  - Press the button once to activate the drone with least throttle. Note: the drone will not take off.
- **Right top button (Disarm):**
  - Press the button once to turn off the drone motors. **Note: the drone will be in free fall if in flight. Use with caution.**
- **Button X (Head Lock):**
  - Press the button to activate “Head Lock” mode. Yaw for the drone will be fixed in this mode.
- **Button A (Altitude Hold):**

  - Press the button to activate "Altitude Hold" mode. The drone will hover at the current altitude position once engaged.
- **D-Pad (camera servo):**
  - Front camera can move on its horizontal axis. Use the D-pad up and down to control the camera movement.

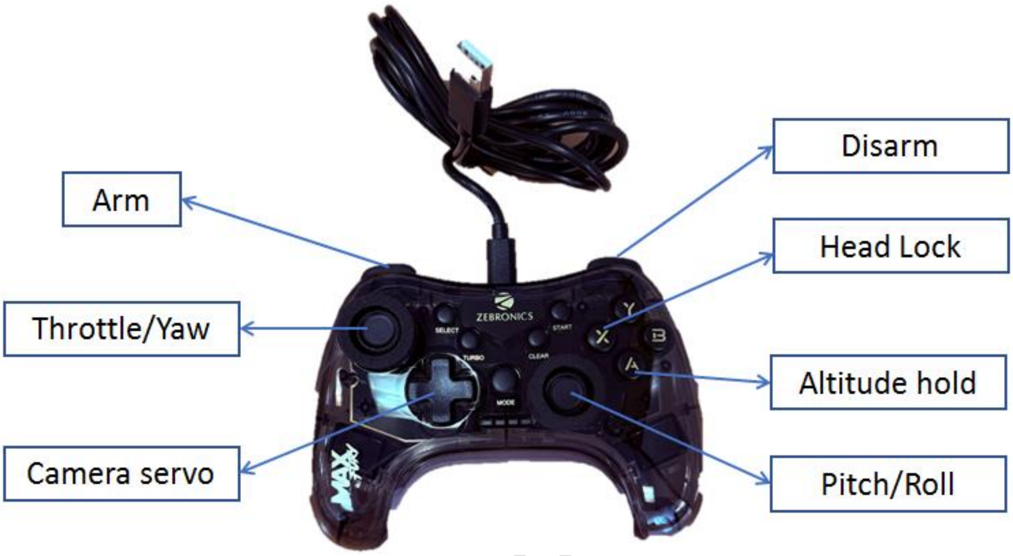


Figure 93 controller

Battery Information:

Orange 4500mah 4S 35C Lithium polymer battery Pack (LiPo) batteries are equipped with heavy-duty discharge leads to minimize resistance and sustain high current loads. Orange batteries stand up to the punishing extremes of aerobatic flight and RC vehicles. Each pack is equipped with gold-plated connectors and JST-XH style balance connectors. All Orange Lithium Polymer batteries packs are assembled using IR match cells.

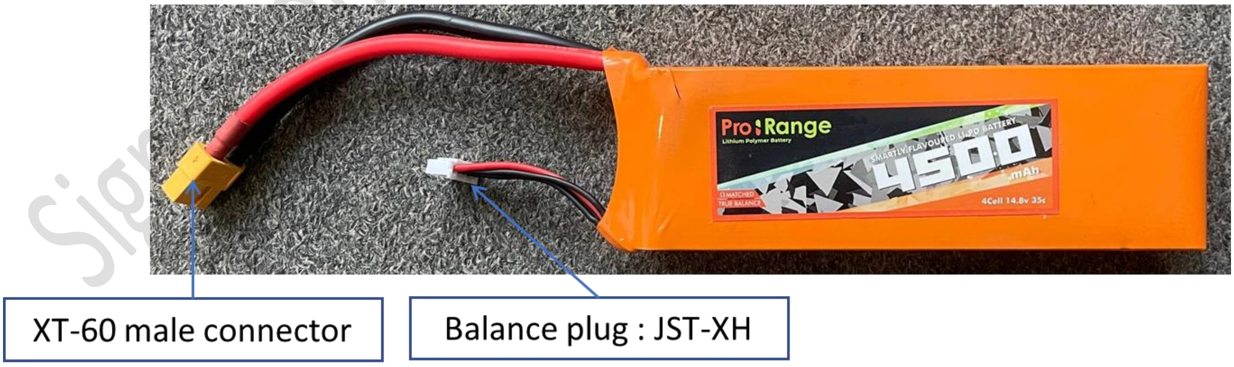


Figure 94 Drone Battery

Parameter	Rating
Model No	Orange 4500mah 4S 35C
Capacity	4500 mAh
Voltage	14.8v

Balance plug	JST-XH

f. Data and Control Flow Architecture

g. On-board Processing

Drone is equipped with 2.4GHz quad-core, 64-bit Arm Cortex-A76 CPU. This allows for onboard data processing for AI/ML analytics and running applications. Its equipped with camera transceivers for low latency video feed and enabling object detection.

https://datasheets.raspberrypi.com/rpi5/raspberry-pi-5-product-brief.pdf

a. 2.4GHz quad-core, 64-bit Arm Cortex-A76 CPU

b. Video Core VII GPU

c. 5G Cellular connectivity

d. 2.4 GHz and 5.0 GHz 802.11ac Wi-Fi connectivity

e. 2 × 4 lane MIPI camera/display transceivers

f. Remote firmware upgrade.

h. Mission Protocol

NA

i. Drone Communication

Telemetry System: Transmits real-time flight data to the ground station (e.g., altitude, speed, battery level). GCS is equipped with a telemetry system which has a dashboard showing all the necessary flight parameters such as

a. Camera feed from both front and bottom cameras.

b. Sensors & connectivity information

c. LIDAR & Map view data.

d. Statistics: Throttle, Roll, Yaw, Pitch, GPS coordinates, barometer altitude, battery percentage.

j. Geo-Fencing

Drone geofencing is a system that uses GPS technology to establish virtual geographical boundaries, known as geofences, within which drones can operate.

k. Autonomy Architecture

i. Visual Inertial Odometry (VIO)

VIO is a computer vision technique that estimates the 3D pose (position and orientation) and velocity of a moving vehicle relative to a local starting point.

ii. path planning

TBD

iii. PX4

TBD

iv. GPS-denied navigation

In situations where GPS signals are unavailable or unreliable (GPS-denied environments), navigation relies on alternative methods, including sensor fusion, Inertial Measurement Units (IMUs), visual odometry, and landmark-based systems to maintain accurate localization and guidance.

v. BVLOS

TBD

vi. follow me

TBD

l. 360 obstacle avoidance Architecture

TBD

19. 5G camera:

The document provided is a technical specification sheet detailing the Sparsh SC-IW860BM-5G, an 8MP 5G Bullet Camera, part of Sparsh's Wireless and Silver Series. This camera is engineered for high-definition surveillance, emphasizing detailed image capture, robust environmental resilience, and advanced connectivity options, including 5G, positioning it as a forward-looking solution for comprehensive security needs.

High-Resolution Imaging: At the heart of the SC-IW860BM-5G's capabilities is its commitment to high-resolution imaging.

- **Camera Sensor:** It incorporates a 1/2.7" Progressive CMOS Sensor. This sensor type is known for its good performance in capturing moving objects and progressive scanning, which helps in delivering clearer images compared to interlaced sensors.
- **Effective Pixels:** The sensor delivers an impressive 8 Megapixel resolution with effective pixels of 3840(H)x2160(V). This high pixel count translates to 4K image clarity, allowing for significant detail in the captured footage, which is crucial for identification and analytical purposes.
- **HD Resolution Performance:** The camera is marketed under the "HD Resolution" banner, with the assurance that "regardless of the moving pace, the camera does a good job of capturing detailed images". This suggests image processing capabilities optimized for clarity in dynamic scenes.

Advanced Lens System: The optical system of the camera is designed for flexibility and high performance.

- **Lens Type and Control:** It features a motorized lens, allowing for remote adjustments to the field of view. The mount type is M14.
- **Focal Length:** The motorized lens has a focal length range of 2.7mm to 13.5mm. This varifocal capability allows users to adjust between a wide-angle view for broader coverage and a telephoto view for focusing on distant objects.
- **Maximum Aperture:** A wide maximum aperture of F1.2 is specified. This large aperture allows more light to enter the lens, which is particularly beneficial for improving image quality in low-light conditions.
- **Angle of View:** The adjustable focal length provides a versatile angle of view:
  - Horizontal: 98∘ (wide) to 34∘ (telephoto).
  - Vertical: 52∘ (wide) to 19∘ (telephoto).
  - Diagonal: 116∘ (wide) to 40∘ (telephoto).
- **Focus Control:** The camera supports both Auto and Manual focus control, giving users the option for automatic adjustment or precise manual tuning.

Superior Low-Light Performance and Illumination: The SC-IW860BM-5G is designed to perform effectively even in challenging lighting conditions.

- **Minimum Illumination:**
  - Color Mode: 0.01 Lux @F1.2.

  - Black & White Mode: 0.001 Lux @F1.2.
  - IR ON: 0 Lux, meaning it can operate in complete darkness with its infrared illuminators.
- **Signal-to-Noise Ratio (S/N Ratio):** The camera has an S/N Ratio of >60dB, indicating a strong signal quality relative to noise, which contributes to clearer images, especially in low light.
- **IR Distance and Control:** It is equipped with 4 Array LEDs providing an effective IR illumination distance of 50-60 meters. The IR On/Off control can be set to Auto or Manual.
- **Shutter Speed:** The shutter speed ranges from 1/25 to 1/100000 seconds, allowing for crisp capture of both slow and fast-moving objects.

Video Processing, Storage, and Intelligent Analytics

Beyond its optical capabilities, the Sparsh SC-IW860BM-5G integrates advanced video processing, ample storage solutions, and a powerful suite of intelligent analytics to enhance its surveillance effectiveness.

Video Compression and Streaming: Efficient video management is crucial for high-resolution cameras.

- **Compression Standards:** The camera supports multiple compression formats, including H.265SE, H.265, and H.264. H.265 (HEVC) and its variants offer significant improvements in compression efficiency over H.264, reducing storage and bandwidth requirements for the 8MP video stream.
- **Streaming Capability:** It can output up to 3 simultaneous video streams, allowing for different resolutions and frame rates to be configured for live viewing, recording, and remote access.
- **Resolution Options:** A wide range of resolutions are available, including 8MP, 5MP, 4MP, 2MP, D1, VGA, and CIF.
- **Detailed Stream Information:**
  - **Mainstream:** Can be configured for 3840x2160 (4K) resolution at 15 frames per second (fps), or 2592x1944 (5MP), 2560x1440 (4MP), 2304x1296 (3MP), and 1920x1080 (2MP) at 25/30fps. This provides flexibility in balancing resolution with frame rate and bandwidth.
  - **Sub Stream:** Supports VGA (640x480) or CIF (352x288) resolutions at 15/25fps, suitable for mobile viewing or low-bandwidth connections.
  - **Third Stream:** Offers D1 (704x576), VGA (640x480), CIF (352x288), or 720P (1280x720) at 15/25fps, providing another option for specific recording or streaming needs.
- **Bit Rate Management:** The bit rate can range from 221Kbps to 8Mbps, with control options for Constant Bit Rate (CBR) or Variable Bit Rate (VBR).

Image Enhancement and Control: The camera offers a comprehensive set of image adjustment features.

- **Exposure and Light Handling:** Includes Day/Night settings (Automatic/Color/Black and white), Exposure Mode (Automatic/Manual), BLC Mode (On/Off), HLC Mode (On/Off), and various Profiles (Auto, Low Light Priority, High Light Priority).

- **Color and Noise Management:** White Balance settings (Indoor/Outdoor/Automatic), Gain Control (Auto/Manual), and an Auto Noise Filter with 1-6 levels are available.
- **Other Image Adjustments:** Features include a 16X Digital Zoom with area selection via mouse, Anti-Flicker (On/Off), AE Reference (1-255 Level), AE Sensitivity (1-10 Level), Flip (Off/On), IR Reverse support, and Mirror (Off/On) functionality.
- **Information Overlay:** Text Overlay for Title, Date & Time, and Weekday can be displayed on the video. Privacy Masking for up to 4 zones is also supported to protect sensitive areas from being viewed or recorded.

Storage Solutions:

- **Edge Storage:** The camera supports a microSD card up to 512GB. Sparsh positions this as a "high performing edge storage solution option for recording video and other functions". This allows for decentralized recording, reducing network load and providing a backup if network connectivity is lost.
- **PC Recording:** Users can also use a local PC for instant recording.

Intelligent Analytics and Smart Functions: This is a key area where the SC-IW860BM-5G excels, transforming it into a proactive security tool.

- **Supported Analytics:** The camera supports a comprehensive suite of intelligent analytics including Human Detection, Intrusion Detection, Line crossing, Object Lost, Object Left, Scene Change, and Audio Detection. These features enable automated monitoring and alerts for specific events.
- **Standard Event Detection:** In addition to advanced analytics, it supports Motion Detection configurable in 22x18 zones and Video Blind detection.
- **Abnormality Alerts:** The system can also detect and alert for various operational abnormalities such as No Disk, Disk Error, Disk No Space, Network Cable Disconnected, and IP Address Conflict.
- **Event Actions:** Upon detection of an event or abnormality, the camera can perform several actions: Record alarm, Linkage alarm output, Sound alarm, Email link, Upload to FTP, and Snapshot (including one-click triple Snapshot).

Connectivity, Network Features, 5G/IoT Integration, and General Specifications

The Sparsh SC-IW860BM-5G is designed for robust connectivity and seamless integration into diverse network environments, with a particular emphasis on leveraging 5G and IoT capabilities. It also includes features for comprehensive system management and security.

Network Connectivity:

- **Wired and Wireless Options:** It includes a 10/100M adaptive Ethernet interface for wired connections. Crucially, it boasts "5G Support" and is part of the "5G wireless Connectivity" series, supporting 3G/4G/5G mobile networks. The document highlights that "5G wireless systems need to handle a variety of traffic types, including enhanced mobile broadband, massive machine communication, and low-latency, high-reliability applications", indicating the camera's suitability for these demanding scenarios.

- **Supported Protocols:** A comprehensive list of network protocols is supported, including TCP/IP, UDP, RTP, RTSP, RTCP, HTTP, HTTPS, DNS, DDNS, DHCP, FTP, NTP, SMTP, UPNP, and IPv4, ensuring compatibility with various network infrastructures.

Interoperability and Management:

- **Standard Compliance:** The camera is ONVIF Profile S & G compliant, which allows for interoperability with a wide range of third-party VMS (Video Management Software) and NVRs (Network Video Recorders).
- **User Access and Software:** It supports up to 20 concurrent users. Management can be performed via Web Viewer (compatible with IE, Chrome, Firefox, Safari), the dedicated Sparsh VMS, and the SVMS APP for iPhone and Android mobile devices.

Audio Capabilities:

- **Two-Way Communication:** The camera supports G.711A/U audio compression and Talk Back functionality, enabling two-way audio communication.
- **Audio Interface:** An optional audio interface providing 1 input and 1 output is available.

Comprehensive Security Features: Security is paramount in surveillance systems, and this camera incorporates multiple layers of protection.

- **Authentication Mechanisms:** It supports ONVIF Authentication (configurable On/Off) and RTSP Authentication (Digest, None).
- **Data and Access Security:** Features include authorized username and password access, HTTPS with password for encrypted web communication, RTSP Validation, User Access Logs, User Authentication, Watermark embedding, IP address filtering, and 802.1x network access control.
- **System Integrity:** Further security measures include IP/MAC filtering, HTTPS for secure data transmission, trusted upgrade processes, trusted boot, firmware encryption, and the capability for generation of X.509 certification for secure device identity.

Physical and Environmental Specifications:

- **Adjustability:** The camera offers manual Pan adjustment from 0◦ to 360◦ and Tilt adjustment from 0◦ to 90◦.
- **Alarm Interface:** An optional alarm interface with 1 input and 1 output is available for integration with external alarm systems.
- **Operating and Storage Conditions:** It is designed to operate in temperatures ranging from −30◦C to +60◦C (−22◦F to +140◦F) with less than 95% relative humidity. Storage conditions are identical.

- **Durability:** The camera is IP67 compliant, signifying a high level of protection against dust and water ingress, making it suitable for outdoor deployment. Vandalism protection is listed as NA (Not Applicable).
- **Power:** It can be powered by DC 12V±10% or optionally via PoE (Power over Ethernet - 802.3af, class 3), with a maximum power consumption of 12W.
- **Physical Dimensions:** The camera measures approximately 182mm×75mm×75mm and weighs around 0.55kg.

Usefulness with 5G and IoT (Elaborated): The SC-IW860BM-5G's features are particularly beneficial in 5G and IoT contexts.

- **5G Integration Benefits:** The camera's native 5G support directly addresses the need for high-bandwidth, low-latency communication. This is essential for reliably transmitting 8MP video streams and facilitating real-time responses based on its intelligent analytics. 5G enables deployment in diverse locations, including those lacking wired infrastructure, making it ideal for smart city applications, remote industrial monitoring, or temporary event surveillance where rapid deployment and high performance are key. The ability of 5G to handle "massive machine communication" and provide "high-reliability" aligns perfectly with the data-intensive and critical nature of advanced video surveillance.
- **IoT Ecosystem Role:** Within an IoT ecosystem, the camera functions as an intelligent edge device or sensor. Its sophisticated analytics (Human Detection, Intrusion Detection, etc.) can generate alerts and data that trigger automated actions in other connected IoT devices (e.g., lighting, alarms, access control). ONVIF compliance and broad protocol support ensure smooth integration with various IoT platforms and VMS systems. Edge storage (512GB SD card) coupled with intelligent analytics can reduce the need for constant high-bandwidth data transmission to the cloud, processing events locally and sending only relevant data or alerts, a crucial aspect for scalable IoT deployments. Remote management via mobile apps and VMS, enhanced by 5G connectivity, allows for a truly connected and responsive security infrastructure.

Concluding Remarks: The Sparsh SC-IW860BM-5G, as detailed in the provided specification sheet, is a technologically advanced bullet camera. Its combination of high-resolution imaging, comprehensive intelligent analytics, robust construction, and, critically, its integrated 5G wireless connectivity, make it a highly versatile and powerful tool for modern surveillance. It is well-equipped to meet the demands of complex security environments and to serve as a key component in integrated 5G-enabled IoT solutions. The product is also noted as "MADE IN INDIA". Product specifications and appearance are subject to change without prior notice

Accessing the web page of camera:

- The camera has both ways of connectivity. One through ethernet and one via 5G network.
- Just type the Ip address of the camera in browser
    - URL: 192.168.128.10 or the 5G ip address the camera gets assigned
    - User: admin
    - Password: admin123

The details about how to connect the camera with 5G network are explained in Section-20, Subsection Use case development with 5G camera

For more details refer the user manual of 5G camera

20.5G Use cases

a. Use case development with 5G Camera

Devices used for development of use cases

Device parts

Sensor Specifications

Utilities and Limitations

Computing available in device for analytics

Analytics software split between device and MEC

Process of software installation at device and MEC

Demonstration of Use cases

Analysis of data and trouble shooting

5G camera setup overview

Overall setup consists of a 5G Camera with SIM provisioned to connect with 5G Lab Network.

The video feed from the camera is uploaded to MEC server over 5G Network. The video feed is processed at MEC using AI ML algorithms to detect Face, Hand and Objects. The same is marked with bounding boxes displaying message when they are detected in the monitor connected to MEC.

MEC is equipped with 24 Cores and 64GB of RAM. Using this high-end infrastructure helps in quick processing of the video feed and mark the face or object in real time.

A typical illustration of the setup is shown below.

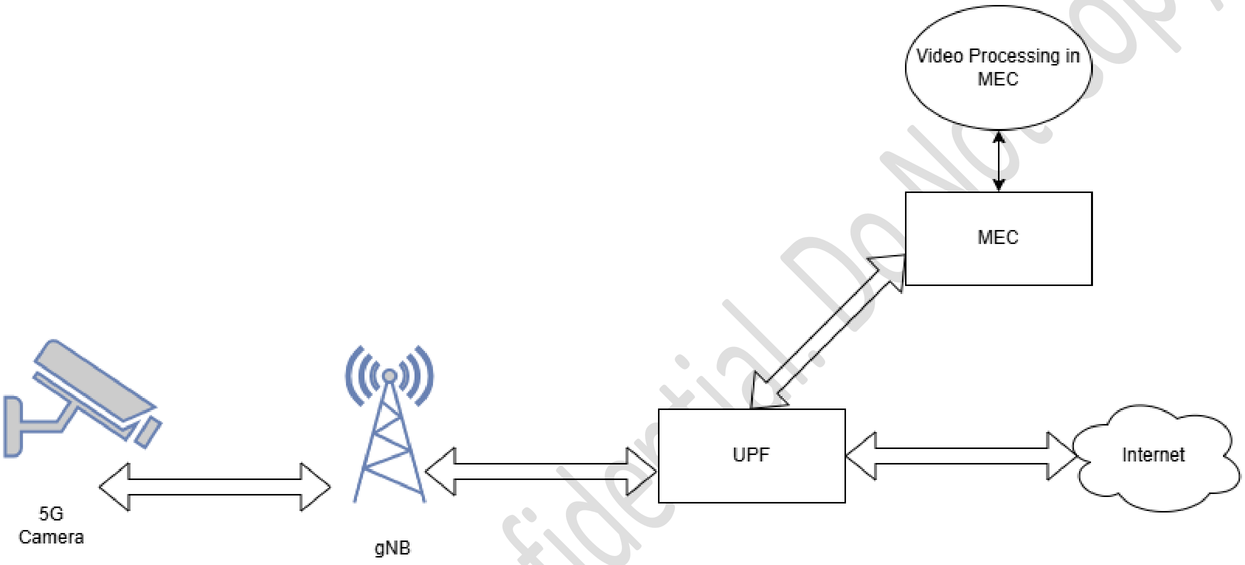


Figure 95 Use case Setup

Detailed steps of Operation

The **Sparsh CCTV Camera** is a surveillance solution designed for seamless integration into modern networks. Equipped with both **5G connectivity** and **Ethernet support**, this camera ensures high-speed data transmission, even in remote or challenging environments. It features an embedded web server, allowing users to access the live feed and configure settings via the camera's IP address through any web browser.

The CCTV Camera has a built in 5G Module which can connect to the 5G network in most bands (our band is n78)

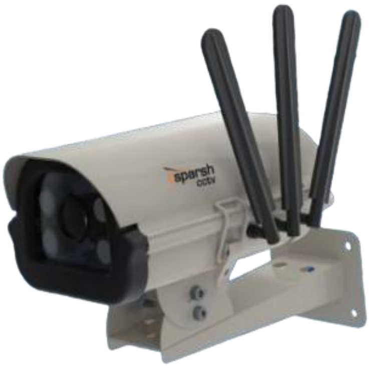


Figure 96 Sparsh Camera

The camera needs to be connected to a power adapter. Later 4 antennas needs to be connected as shown in the below figure. The SIM Card has to be inserted in form of nano SIM. The upper metal portion of the camera needs to be opened for insertion of sim. First the latch needs to be opened and then the upper portion can be opened as shown in the below figure.

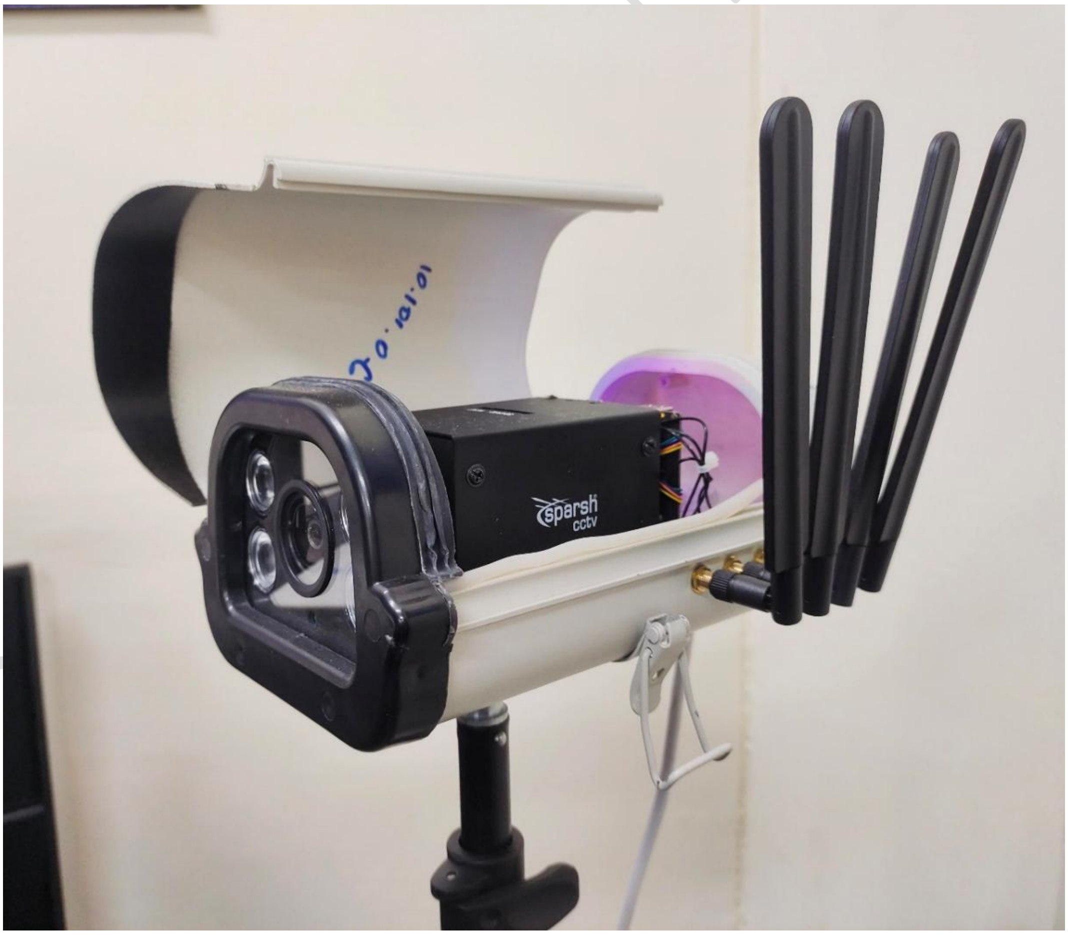


Figure 97 Accessing sim card slot by opening upper metal enclosure

Now the sim card can be inserted as shown in the below figure.

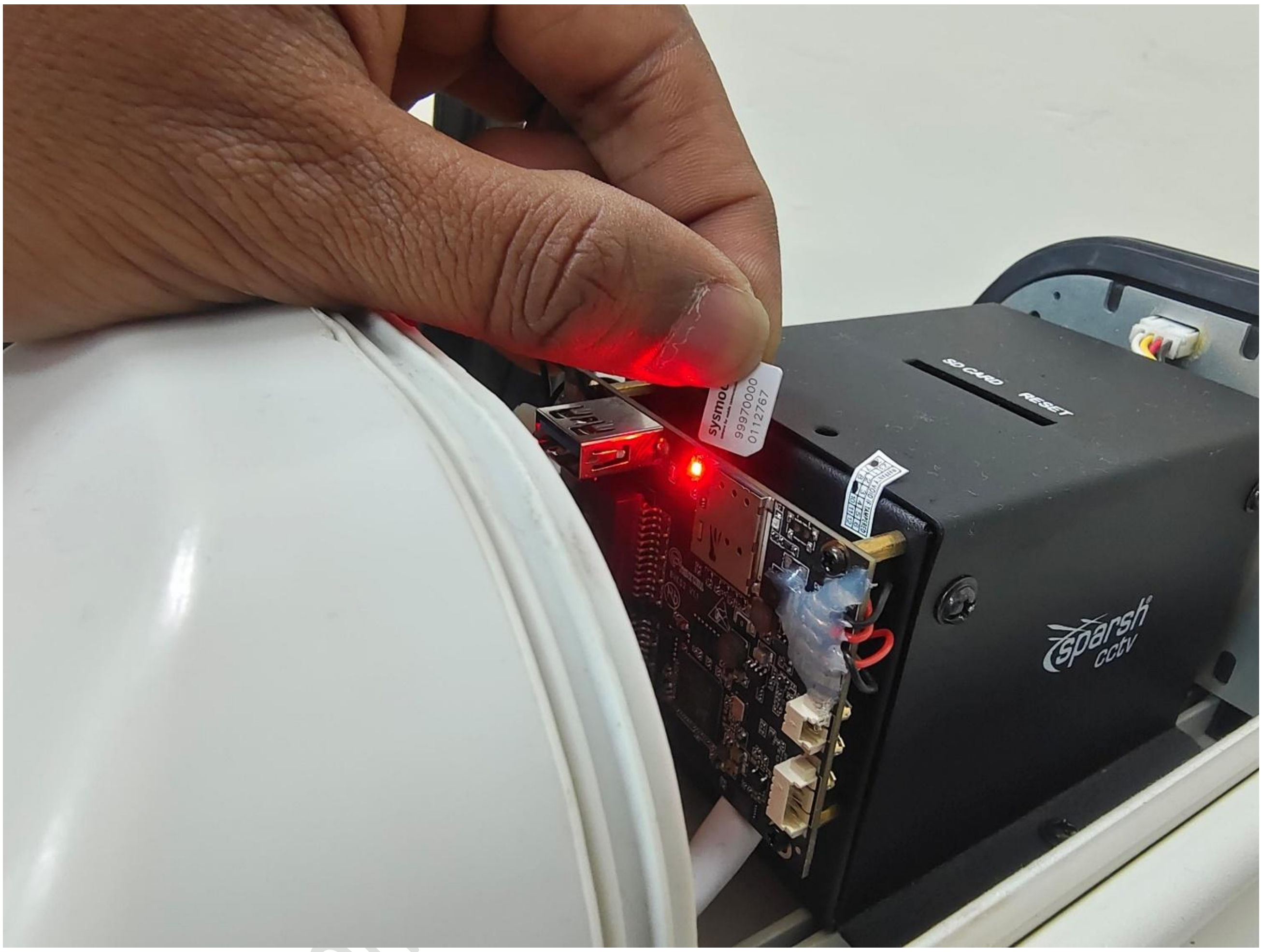


Figure 98 Orientation to insert sim card

Once the camera is powered on, red light becomes stable inside the Camera. Red led light can be seen in the above figure.

After the sim card is inserted, blue light starts to blink inside the Camera indicating that the SIM is detected by the Camera. Once the SIM latches on to the 5g Network, the blue light becomes stable indicating that the camera is connected to 5G. This can be verified in the below figure.

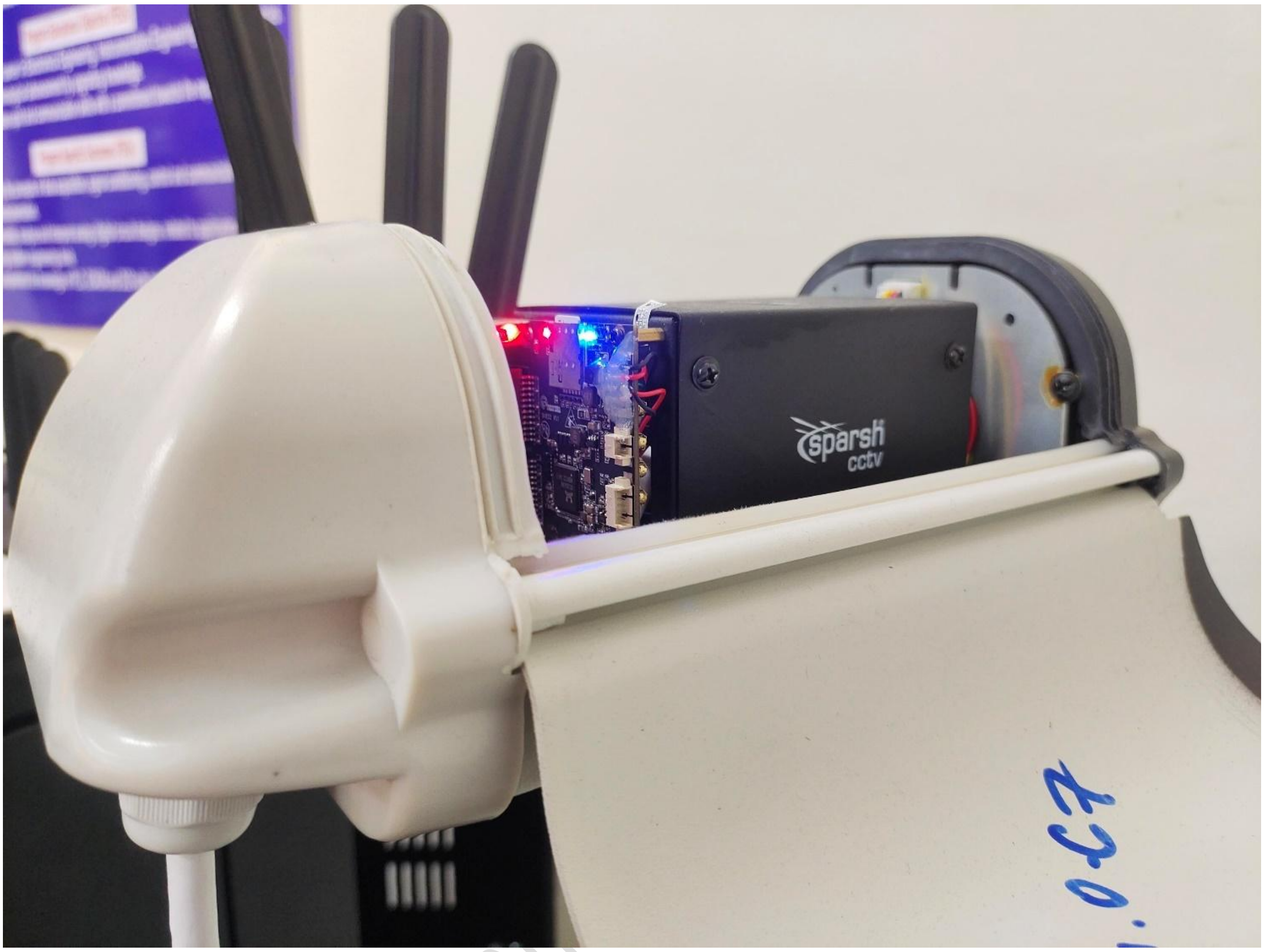


Figure 99 Blue color led light can be seen

Summary of the steps described above, to connect the 5G camera to the gNodeB:-

1. Power the Camera by connecting the Power Adapter
2. Open the Metal Cover of Camera (refer **Figure 97**)
3. Ensure that the SIM is nano SIM, push it into the SIM slot till a latching sound is observed (refer **Figure 98**)
4. Make sure the gNodeB is powered on and it is radiating (check section -5, sub section “Power on gNodeB and connect a UE”)
5. When the Blue light becomes stable, your Camera is connected to 5G (refer **Figure 99**)
6. Also check if the 5G camera is connected to gNodeB by checking NMS page (check section -5, sub section “Power on gNodeB and connect a UE”)

In our setup, we are using the RTSP protocol to get the Camera’s video feed. The MEC accesses the 5G camera feed via a RTSP URL. The URL contains 5G camera’s IP address in it. When UEs connect to the Core Network in 5G Architecture, they are allotted a new IP Address every time a new connection is made to the network. This way a **new URL** needs to be used at MEC every time the 5G camera connects to the gNodeB.

To avoid changing the RTSP URL every time, we need to hardcode a fixed IP address to the SIM card

This hardcoding can be achieved by mapping the IMSI of a sim card to a particular IP address in the core network. This configuration at core network can be done through Niral NMS. Refer to section-12, subsection -D and heading “**Map a fixed IP address (static ip address) to a sim card”**

After the hardcoding of the IP address, check for the led status, if the blue light is stable then the 5G camera should be pingable from the MEC. The Camera’s inbuilt web stream can be viewed by putting the Camera’s IP into the browser.

```
 $ ping <camera ip address>

# ping response should be seen in the console
```

Model in the MEC; We have developed the following python code which shows the Camera’s stream with Object detection in real time:

The camera supports **RTSP streaming** using the following URL format:

rtsp://admin:admin123@<5g_camera_ip_address>:554/avstream/channel=1/stream=0.sdp

As a Use case, a python-based media player which implements ML based facial and hand recognition using the mediapipe library of python. The following modules have been installed on the MEC server (192.168.10.12):

pip install opencv-python

pip install mediapipe

The following code uses MediaPipe and OpenCV to detect hands and faces in a live video stream from an RTSP (Real-Time Streaming Protocol) source. It highlights the detected hands with landmarks and faces with bounding boxes, displaying a message when they are detected.

What does the script do:

- RTSP Stream Input: Connects to an RTSP video stream (e.g., from an IP camera) using cv2.VideoCapture()
- Hand and Face Detection:

  Hand Detection: Tracks up to 2 hands and draws landmarks.

  Face Detection: Detects faces and draws bounding boxes.

- Display Processed Frame: Processes each frame, draws landmarks/bounding boxes, and displays text ("Hand Detected" or "Face Detected").
- Resize and Show: Resizes the frame to 1980x900 and displays it in a window.

This real-time processing allows you to visually detect hands and faces from an RTSP stream.

Copy the below python code into a file and name it show_camera.py. Then execute the command by giving below commands.

In the below yellow box, the lines start with "#" are comments. The lines that start with "$" are bash commands.

```
 $ssh -X st@192.168.10.12 #command to SSH into MEC from gNodeB
                          # give password "mec@5glabs"


 $ chmod a+x show_camera.py
# Go to the path where the file is created and give above executable
command. This command should be given only one time during initial
setup


$ python3 show_camera.py # command to start the execution
```

Python code to be copied for 5G camera object detection:

```
import cv2

import mediapipe as mp

from multiprocessing import Process, Queue, Value
```

Add the actual 5g camera ip address here.

```
from collections import deque

import time


# RTSP stream URL

rtsp_url =
"rtsp://admin:admin123@5g_camera_ip_address:554/avstream/channel=1/
stream=0.sdp"


# Desired display dimensions

display_width = 1280  # Adjusted for better smoothness

display_height = 720


# MediaPipe initialization

mp_hands = mp.solutions.hands

mp_face_detection = mp.solutions.face_detection

mp_drawing = mp.solutions.drawing_utils




def capture_frames (frame_queue, stop_flag):

    """Captures frames from the RTSP stream and adds them to the
frame queue."""

    cap = cv2.VideoCapture(rtsp_url, cv2.CAP_FFMPEG) # Use FFmpeg
backend for better RTSP handling

    if not cap.isOpened():

        print("Error: Could not open the video stream.")

        stop_flag.value = True

        return
    while not stop_flag.value:
        ret, frame = cap.read()
        if not ret:
            print("Error: Could not read frame.")
            time.sleep(0.1) # Prevent busy-wait if no frame is read
            continue

        if frame_queue.qsize() < 5:  # Avoid overfilling the queue
            frame_queue.put(frame)

    cap.release()



def process_frames(frame_queue, processed_frame_queue, stop_flag):
    """Processes frames to detect hands and faces using
MediaPipe."""
    hands = mp_hands.Hands(static_image_mode=False,
max_num_hands=2, min_detection_confidence=0.5)
    face_detection =
mp_face_detection.FaceDetection(min_detection_confidence=0.5)

    while not stop_flag.value:
        if not frame_queue.empty():
            frame = frame_queue.get()
            frame_rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
            # Detect hands
            hand_results = hands.process(frame_rgb)
            if hand_results.multi_hand_landmarks:
                for hand_landmarks in
hand_results.multi_hand_landmarks:
                    mp_drawing.draw_landmarks(frame,
hand_landmarks, mp_hands.HAND_CONNECTIONS)

            # Detect faces
            face_results = face_detection.process(frame_rgb)
            if face_results.detections:
                for detection in face_results.detections:
                    mp_drawing.draw_detection(frame, detection)

            if processed_frame_queue.qsize() < 5:  # Avoid
overfilling the queue
                processed_frame_queue.put(frame)

    hands.close()
    face_detection.close()


def display_frames(processed_frame_queue, stop_flag, fps_queue):
    """Displays processed frames."""
    while not stop_flag.value:
        if not processed_frame_queue.empty():
            start_time = time.time()
            frame = processed_frame_queue.get()

            resized_frame = cv2.resize(frame, (display_width, display_height))
            cv2.imshow("MediaPipe Processed Stream", resized_frame)

            # Calculate and display FPS
            end_time = time.time()
            fps = 1 / (end_time - start_time)
            fps_queue.append(fps)
            avg_fps = sum(fps_queue) / len(fps_queue)
            cv2.putText(
                resized_frame,
                f"FPS: {avg_fps:.2f}",
                (10, 30),
                cv2.FONT_HERSHEY_SIMPLEX,
                1,
                (0, 255, 0),
                2,
            )

            # Stop when 'q' is pressed
            if cv2.waitKey(1) & 0xFF == ord('q'):
                stop_flag.value = True

                break


    cv2.destroyAllWindows()



if __name__ == "__main__":

    # Queues for inter-process communication

    frame_queue = Queue(maxsize=5)

    processed_frame_queue = Queue(maxsize=5)


    # Shared flag to signal processes to stop

    stop_flag = Value('b', False)


    # FPS tracking

    fps_queue = deque(maxlen=30)  # Store last 30 frames for FPS
smoothing


    # Processes for each stage

    capture_process = Process(target=capture_frames,
args=(frame_queue, stop_flag))

    process_process = Process(target=process_frames,
args=(frame_queue, processed_frame_queue, stop_flag))

    display_process = Process(target=display_frames,
args=(processed_frame_queue, stop_flag, fps_queue))


    # Start processes
    capture_process.start()

    process_process.start()

    display_process.start()


    # Wait for processes to complete

    capture_process.join()

    process_process.join()

    display_process.join()
```

Sample Output

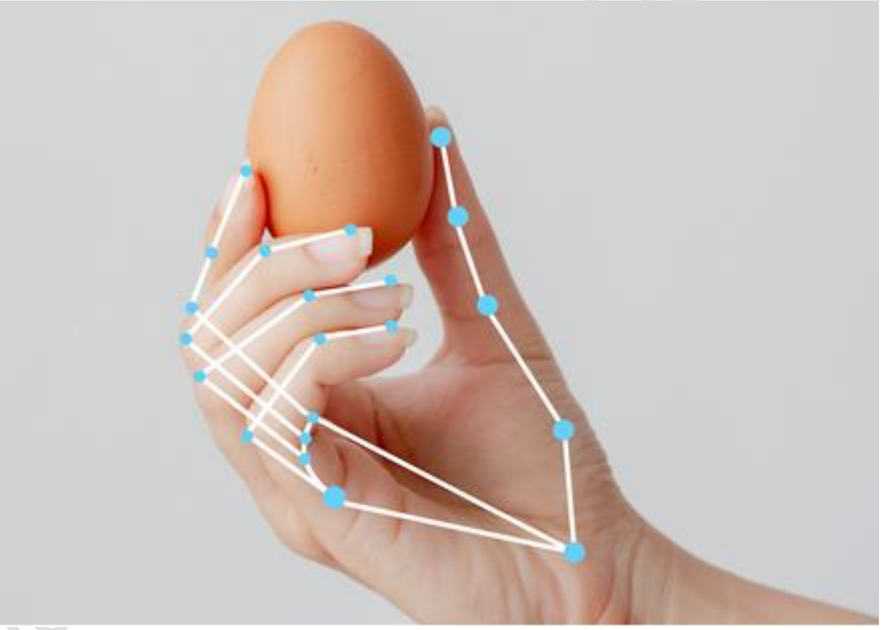


Figure 100 Sample Output 1

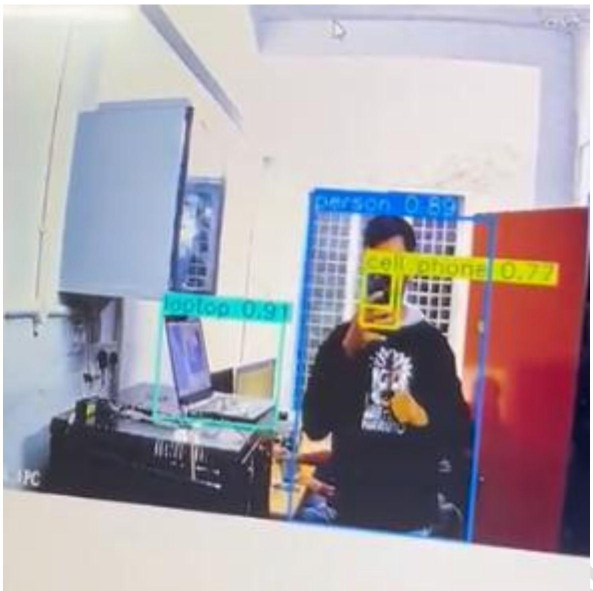


Figure 101 Sample Output 2

b. Use case development with 5G Evaluation board

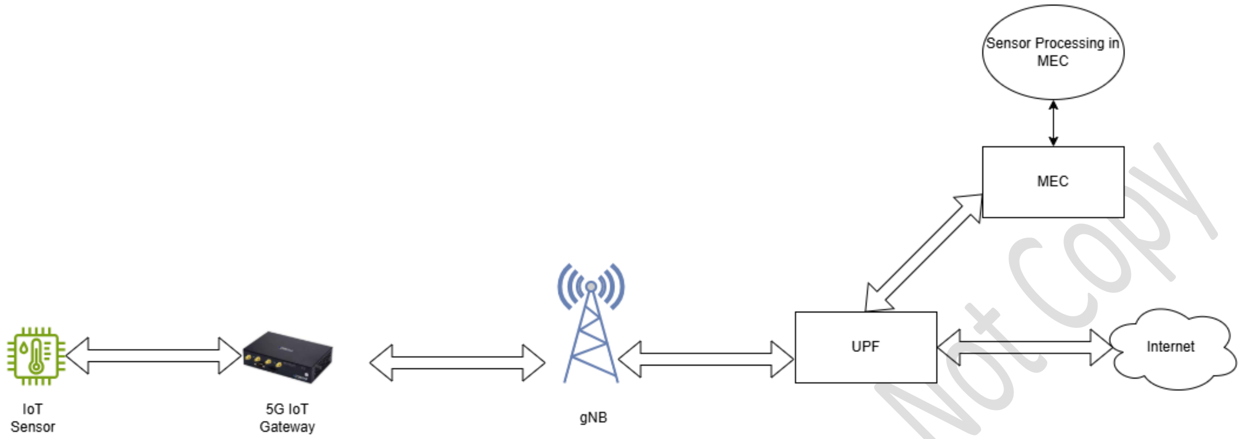


Figure 102 IoT setup

IoT Temperature Sensor and Humidity Sensor is connected to 5G IoT Gateway using WiFi.

5G IoT Gateway sends the received data from IoT sensors and forwards them to MEC

MEC has the algorithm to process the information sent over 5G Network and notify other elements or take appropriate action. In this specific use case, the temperature and humidity information are displayed on MEC dashboard or on the smartphone.

An IoT Gateway acts as a bridge between IoT devices and the cloud or local network. It facilitates communication, data processing, and protocol translation.

In this use case:

- The IoT gateway provides wireless connection to the raspberry pi which is inside UE Evaluation board
- Other network clients (MEC Server / IP: 192.168.10.12) can subscribe to this broadcast for real-time data visualization or further processing.

Overall setup of the use case:

DHT11 Sensor connected to Arduino for collecting the sensor data. Arduino is not supplied to colleges. The same use case can be performed by directly connecting sensor to Raspberry Pi. But in our use case we have demonstrated with Arduino.

Arduino is connected to Raspberry Pi (present in UE Evaluation board) via USB. Raspberry Pi is then connected to IoT Gateway via Wifi. IoT Gateway is connected to the 5G network as it has a sim card. Once on the 5G network, the data can be accessed via the MEC Server which has connectivity to the network.

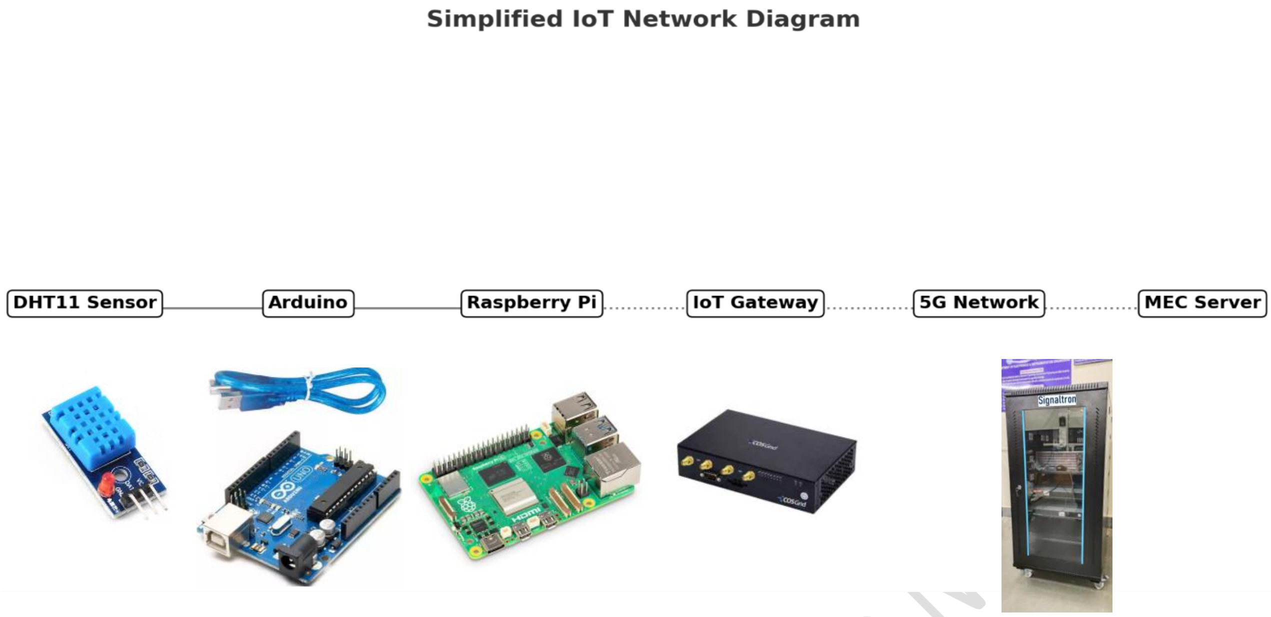


Figure 103 Detailed Setup

Arduino Connections

Arduino is an open-source electronics platform designed to make it easy for anyone, from beginners to experts, to create interactive hardware projects. It consists of both a hardware programmable circuit board (microcontroller) and an integrated development environment (IDE) that allows users to write and upload code to the board.

DHT11 Sensor produces digital data based on its real time readings of temperature and humidity. This data is fed into Arduino by making appropriate connections which are as follows:

Connect the Sensor's VCC to 5V pin on Arduino, Ground to the Ground pin on the Arduino and the Data pin of the sensor to the DIGITAL 50 pin

Steps to Connect DHT11 Sensor to Arduino:

1. Make sure you have 3 male-to-female jumper wires.
2. Connect the female endpoint of a jumper wire to DHT11’s VCC and connect the male endpoint on the Arduino at 5V.
3. Connect the female endpoint of the next jumper wire to DHT11’s GND, and the other end to GND on the Arduino board as marked above.
4. Connect the third wire from DATA end of DHT11 sensor to DIGITAL 50 Pin on the Arduino.
5. Program the Arduino beforehand with the following code to get temperature and humidity readings as serial data in Arduino. Look for DHT11 library in Arduino and install it

- Links for Arduino IDE installation- https://support.arduino.cc/hc/en-us/articles/360019833020-Download-and-install-Arduino-IDE
- Selecting a correct board and port- https://support.arduino.cc/hc/en-us/articles/4406856349970-Select-board-and-port-in-Arduino-IDE
- How to install additional libraries in Arduino - https://docs.arduino.cc/software/ide-v1/tutorials/installing-libraries/

Arduino Programming Code

```
  #include "DHT.h"


#define DHTPIN 50

#define DHTTYPE DHT11


DHT dht(DHTPIN, DHTTYPE);


void setup() {

  Serial.begin(9600);

  dht.begin();

}


void loop() {

  float humidity = dht.readHumidity();

  float temperature = dht.readTemperature();


  if (!isnan(humidity) && !isnan(temperature)) {

    Serial.print("Humidity: ");
```

```
      Serial.print(humidity);
      Serial.print("% Temperature: ");
      Serial.println(temperature);
    }
  }
```

Raspberry Pi Connections

Connect the Arduino board via USB to a Raspberry Pi (in this use case, we are using the Raspberry Pi which is present inside UE Evaluation board) which has Ubuntu installed on it. It should have python with version >3.8. pyserial module is needed on the Raspberri pi. It is already installed in all the colleges during UAT.

Also connect monitor, keyboard and mouse to Raspberry pi. Connect the Wifi created by IoT Gateway. On top right you can see Wifi options.

Command to install: -

```
pip install pyserial
```

What does the Raspberry pi do:

The code reads data from an Arduino via a serial port (`/dev/ttyACM0`) and broadcasts it over a network using UDP (`255.255.255.255:5005`). It continuously listens for serial data, decodes it, and sends it as a broadcast message, enabling real-time data sharing across devices on the network.

Steps to transmit serial data over Wifi

1. Turn on the raspberry pi and connect a monitor, keyboard and mouse to it.
2. Raspberry pi should have Ubuntu version which satisfies installation on python 3.8.
3. Install the module pyserial with the command given above.
4. Using a Serial to USB cable, connect the now programmed Arduino board to raspberry pi on the top left USB slot
5. Connect the raspberry pi to IoT Gateway’s Wifi, make sure the Raspberry pi gets an Ip address in the 192.168.10.x series
6. Copy the below code and paste it a new file in Raspberry pi and give a name send_data.py
7. Run the following python code which transmits data from Raspberry pi to the MEC server in the local network

```
In Raspberry pi

$ chmod a+x send_data.py

# Go to the path where the file is created and give above executable
command. This command should be given only one time during initial
setup


$ python3 send_data.py # command to start the processing at Raspberry
Pi
```

Python code which runs on Raspberry pi to broadcast data over Wifi

```
import serial

import socket


# Serial Configuration

SERIAL_PORT = '/dev/ttyACM0’ # Update with your Arduino's port

BAUD_RATE = 9600


# Network Configuration

UDP_IP = '192.168.10.12’ # Broadcast address // MEC’s IP

UDP_PORT = 5005 # Port for broadcasting



def read_serial_data():
    """

    Reads data from the serial port and yields each line.

    """

    try:

        with serial.Serial(SERIAL_PORT, BAUD_RATE, timeout=1) as ser:
            print(f"Listening on {SERIAL_PORT} at {BAUD_RATE} baud rate...")
            while True:
                line = ser.readline().decode('utf-8').strip()
                if line:
                    print(f"Received: {line}")
                    yield line
    except serial.SerialException as e:
        print(f"Serial error: {e}")
        return


def broadcast_data(data):
    """
    Broadcasts data over the network using UDP.
    """
    with socket.socket(socket.AF_INET, socket.SOCK_DGRAM) as sock:
        sock.setsockopt(socket.SOL_SOCKET, socket.SO_BROADCAST, 1)
        sock.sendto(data.encode('utf-8'), (UDP_IP, UDP_PORT))
        print(f"Broadcasted: {data}")


if __name__ == '__main__':
    for serial_data in read_serial_data():
        broadcast_data(serial_data)
```

Steps to run MEC python code for graph plotting:

1. Copy the below python code and paste in a new file and give a new name like get_data.py

```
 $ ssh -X st@192.168.10.12 #password is "mec@5glabs"
$ chmod a+x get_data.py
# Go to the path where the file is created and give above executable
command. This command should be given only one time during initial
setup


$ python3 get_data.py #
```

Python code for displaying code as a graphical plot in MEC

```
import socket
from collections import deque
import matplotlib.pyplot as plt
from matplotlib.animation import FuncAnimation
import re

# Network Configuration
UDP_IP = ''  # Listen on all available interfaces
UDP_PORT = 5005

# Storage for temperature and humidity data
max_values = 2000
temperature_data = deque(maxlen=max_values)  # Store up to 2000
temperature values
humidity_data = deque(maxlen=max_values)  # Store up to 2000
humidity values
time_data = deque(maxlen=max_values)  # Store time indices
```

```
# Initialize time index
time_index = 0


def receive_broadcast():
    """
    Listens for UDP broadcast data and appends to the temperature
and humidity queues.
    """
    global time_index
    with socket.socket(socket.AF_INET, socket.SOCK_DGRAM) as sock:
        sock.bind((UDP_IP, UDP_PORT))
        print(f"Listening for broadcasts on port {UDP_PORT}...")
        while True:
            data, addr = sock.recvfrom(1024)  # Buffer size is 1024
bytes
            try:
                # Decode and clean the data
                decoded_data = data.decode('utf-8').strip()
                print(f"Raw data received: {decoded_data}")

                match = re.search(
r"Humidity:\s*([\d.]+)%\s*Temperature:\s*([\d.]+)°C",
                    decoded_data,)

                if match:
                    hum = float(match.group(1))  # Extract and
convert humidity to float
                    temp = float(match.group(2))  # Extract and
convert temperature to float
```

```
                    print(f"Humidity: {hum}, Temperature: {temp}")
                    time_index += 1

                    temperature_data.append(temp)
                    humidity_data.append(hum)
                    time_data.append(time_index)
                else:
                    print("No match found.")
            except Exception as e:
                print(f"Error processing data: {e}")


def update_graph(frame):
    """
    Updates the Matplotlib graphs with the latest data.
    """
    ax1.clear()
    ax2.clear()

    # Plot temperature data
    ax1.plot(time_data, temperature_data, label="Temperature (°C)",
color="red")
    ax1.set_title("Temperature vs Time")
    ax1.set_xlabel("Time")
    ax1.set_ylabel("Temperature (°C)")
    ax1.legend(loc="upper left")
    ax1.grid()

    # Plot humidity data
    ax2.plot(time_data, humidity_data, label="Humidity (%)",
color="blue")
    ax2.set_title("Humidity vs Time")
    ax2.set_xlabel("Time")
    ax2.set_ylabel("Humidity (%)")
    ax2.legend(loc="upper left")
    ax2.grid()


if __name__ == '__main__':
    # Start the UDP listener in a separate thread
    import threading

    listener_thread = threading.Thread(target=receive_broadcast,
daemon=True)
    listener_thread.start()

    # Set up Matplotlib for dual graphs
    plt.style.use('seaborn-darkgrid')
    fig, (ax1, ax2) = plt.subplots(2, 1, figsize=(10, 8),
sharex=True)  # Two subplots stacked vertically
    ani = FuncAnimation(fig, update_graph, interval=100)  # Update
every 100 ms

    # Display the plots
    print("Starting the live plots...")
    plt.tight_layout()
    plt.show()
```

Code for python-based web server for sensor data

```
import re
import socket
from collections import deque
from flask import Flask, render_template, jsonify

# Network Configuration
UDP_IP = '0.0.0.0'  # Listen on all available interfaces
UDP_PORT = 5005

# Storage for temperature and humidity data
temperature_data = deque(maxlen=2000)
humidity_data = deque(maxlen=2000)
time_data = deque(maxlen=2000)

# Flask app
app = Flask(__name__)

# Initialize time index
time_index = 0

def receive_broadcast():
    """
    Listens for UDP broadcast data and appends to the temperature and humidity queues.
    """
    global time_index
    with socket.socket(socket.AF_INET, socket.SOCK_DGRAM) as sock:
        sock.bind((UDP_IP, UDP_PORT))
        print(f"Listening for broadcasts on port {UDP_PORT}...")
        while True:
            data, addr = sock.recvfrom(1024)  # Buffer size is 1024
bytes
            try:
                # Decode and clean the data
                decoded_data = data.decode('utf-8',
errors='ignore').strip()
                print(f"Raw data received: {decoded_data}")
                match =
re.search(r"Humidity:\s*([\d.]+)%\s*Temperature:\s*([\d.]+)°C",
decoded_data)

                if match:
                    hum = float(match.group(1))  # Extract and
convert humidity to float
                    temp = float(match.group(2))  # Extract and
convert temperature to float
                    print(f"Humidity: {hum}, Temperature: {temp}")

                    # Append the new data to the queues
                    temperature_data.append(temp)
                    humidity_data.append(hum)
                    time_data.append(time_index)
                    time_index += 1
                else:
                    print("No match found.")
            except Exception as e:
                print(f"Error processing data: {e}")
@app.route('/')
def index():
    """
    Renders the HTML page that will display the data.
    """
    return render_template('index.html')
@app.route('/data')
def get_data():
    """Returns the latest temperature and humidity data as JSON."""
    return jsonify({
        "temperature_data": list(temperature_data),
        "humidity_data": list(humidity_data)
    })

if __name__ == '__main__':
    # Start the UDP listener in a separate thread
    import threading
    listener_thread = threading.Thread(target=receive_broadcast, daemon=True)
    listener_thread.start()

    # Start Flask app
    app.run(host='0.0.0.0', port=5000)
```

Use case development with 5G Drone

TBD

i. Drone sensors/IoT used for development of use cases
   1. Device parts
   2. Sensor Specifications
   3. Utilities and Limitations

ii. Computing available in device for analytics

iii. Analytics software split between device and MEC

iv. Process of software installation at device and MEC

v. Demonstration of Use cases

vi. Analysis of data and trouble shooting

XR Headset

TBD

vii. XR Devices

viii. Augmented reality, Virtual reality, Mixed reality

ix. XR Foundation Features for design and development

x. Setting up dev environment.

xi. Configuration required for connecting to WiFi network

xii. Install and built application usage

xiii. Trouble shooting