Training Program for 5G Use case Labs

5G LAB

Introduction To 5G Lab

Purpose of a 5G Lab

- Advanced Research & Innovation
- Skill Development & Hands-on Learning
- Industry Collaboration (MSME, Startups)
- Testing & Deployment of Private 5G Networks
- Security & Optimization
- Prototyping & Innovation

Key Areas of Study in a 5G Lab

Network Architecture: 5G Core, RAN (Radio Access Network), and Edge Computing

Protocols & Standards: 5G NR (New Radio), mmWave, slicing etc

Security & Privacy: Encryption, authentication, and secure communication

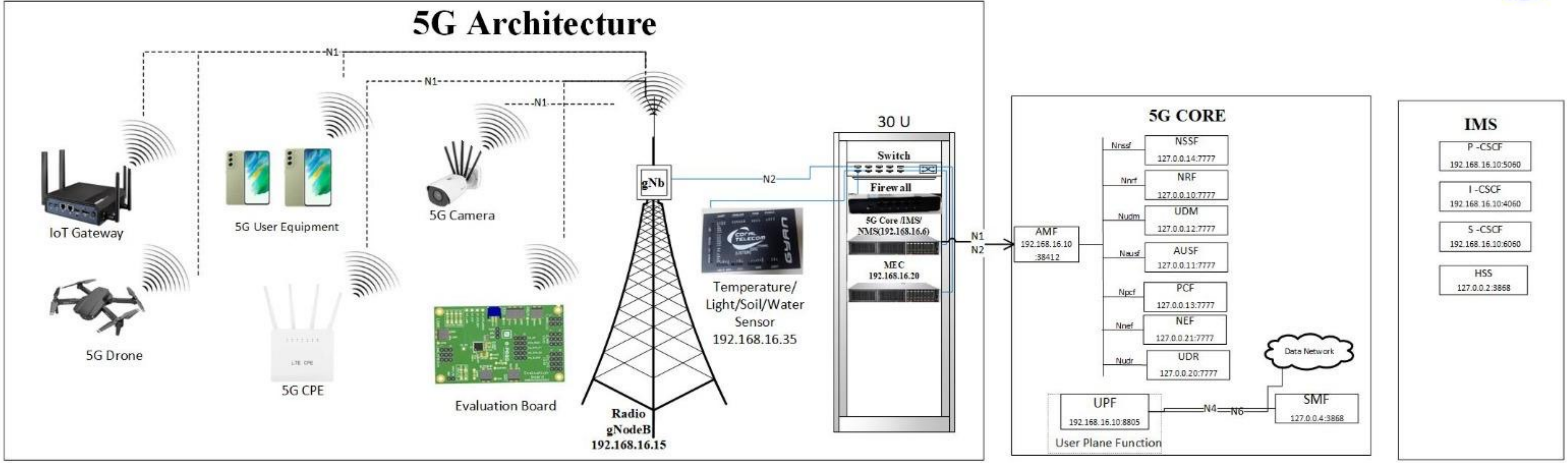
Application Development: Smart factories, connected vehicles, Drones, AR/VR , sensors etc.

Key Components of 5G Lab

- 5G Radio
- 5G Core & IMS
- MEC
- 5G Evaluation Board
- IoT gateway and Sensors
- NMS with dashboard
- Firewall & Router, 5G AI Camera
- 5G CPE, AR/VR, Mobile Phone etc

Architecture of 5G Lab

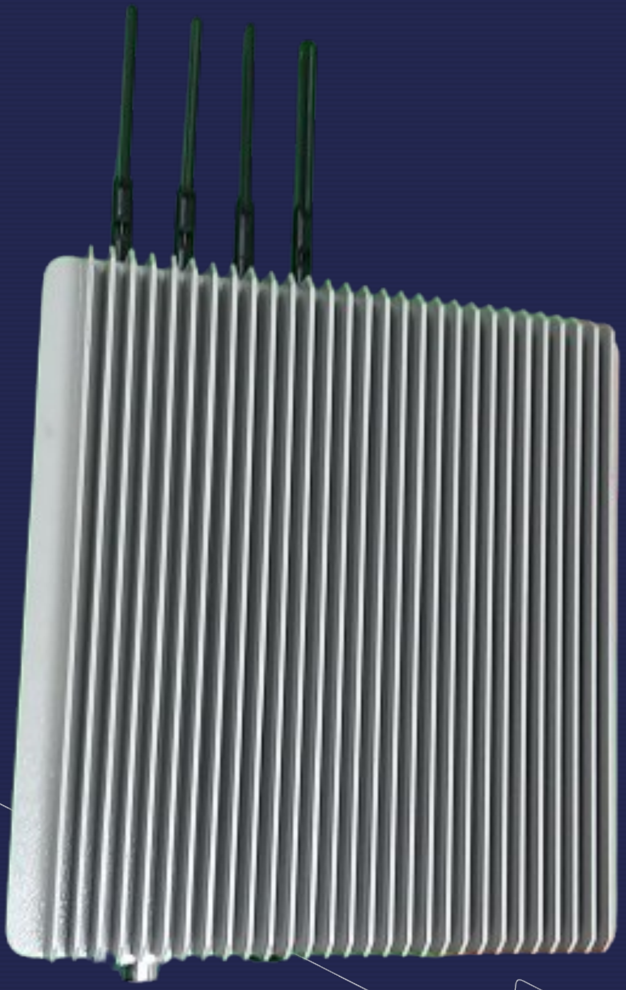
5G Architecture



Devices Available in 5G Labs

5G Radio

Band N78
Channel Width: 100 MHz
Power: 100 Mwatt
2T2R



5G Evaluation Board

A 5G evaluation board is a hardware platform, often provided by chip vendors, that allows engineers and developers to test, prototype, and develop applications for 5G technology, including modules, antennas, and other components.

5G Drone

- **5G and Wi-Fi Connectivity:** Ensures seamless operation and real-time control.
- **Advanced Processing:** Onboard AI/ML analytics for real-time data processing.
- **Autonomous Navigation:** Features VIO, advanced path planning, PX4 software, GPS-denied navigation, and BVLOS capabilities.
- **Obstacle Avoidance:** 360-degree obstacle detection and avoidance.
- **Payload Capacity:** Carries up to 500g for various tasks.
- **Outdoor Navigation:** Reliable GPS for critical missions.
- **Geo-fencing:** Virtual boundaries for safe operation.
- **High-Performance Sensors:** Captures high-quality images and videos.
- **Versatile Ports:** 5G modem, Ethernet, and dual-band Wi-Fi-6 for data transmission and management.

CPE (Customer Premises Equipment)

The CPE 5G allows users to connect to a 5G network and share the high-speed internet connection with multiple devices in a home or office setting. It acts as a bridge between the 5G network and the local area network (LAN) of the user's premises.

IoT Gateway

COSGrid IoT gateway is a cutting-edge network router designed to facilitate seamless connectivity and communication between IoT devices, its users and the cloud . By leveraging the power of 5G, our gateway ensures ultra-fast and reliable data transfers, minimizing latency and maximizing throughput. Our COSGrid IoT gateway is not only a hardware device but also encompasses powerful software programs that enhance its functionality. It is designed to seamlessly integrate with existing IoT ecosystems, making it highly versatile and adaptable to various IoT deployments.

With COSGrid, businesses and organizations can experience enhanced connectivity, improved data security, and streamlined device management. Our IoT gateway is the ultimate solution for harnessing the full potential of IoT devices and leveraging the power of the cloud for data-driven decision-making.

IoT Sensor Software

Overview:

The IoT Sensor Software is a cutting-edge device designed to bring the power of the Internet of Things into your hands. This compact and versatile gateway serves as a hub for connecting various smart devices and sensors, allowing you to integrate them into a unified and intelligent system seamlessly.

Purpose:

In an era where connectivity is key, the IoT Sensor Software(Coral Gyan) is crafted to simplify how you interact with your environment. It empowers users to monitor, control, and gather data from a myriad of IoT-enabled devices, fostering a smarter and more efficient living or working space.

Connectivity:

The IoT gateway supports a wide range of communication protocols, including Wi-Fi, Bluetooth, Zigbee, and more. This ensures compatibility with a diverse array of IoT devices, making it a central point for managing your smart ecosystem.

Seamless Integration

With its intuitive interface and compatibility with popular IoT platforms, the IoT gateway facilitates the integration of devices from different manufacturers. This interoperability allows users to create a cohesive and interconnected network of smart devices.

5G AI Camera

Features:

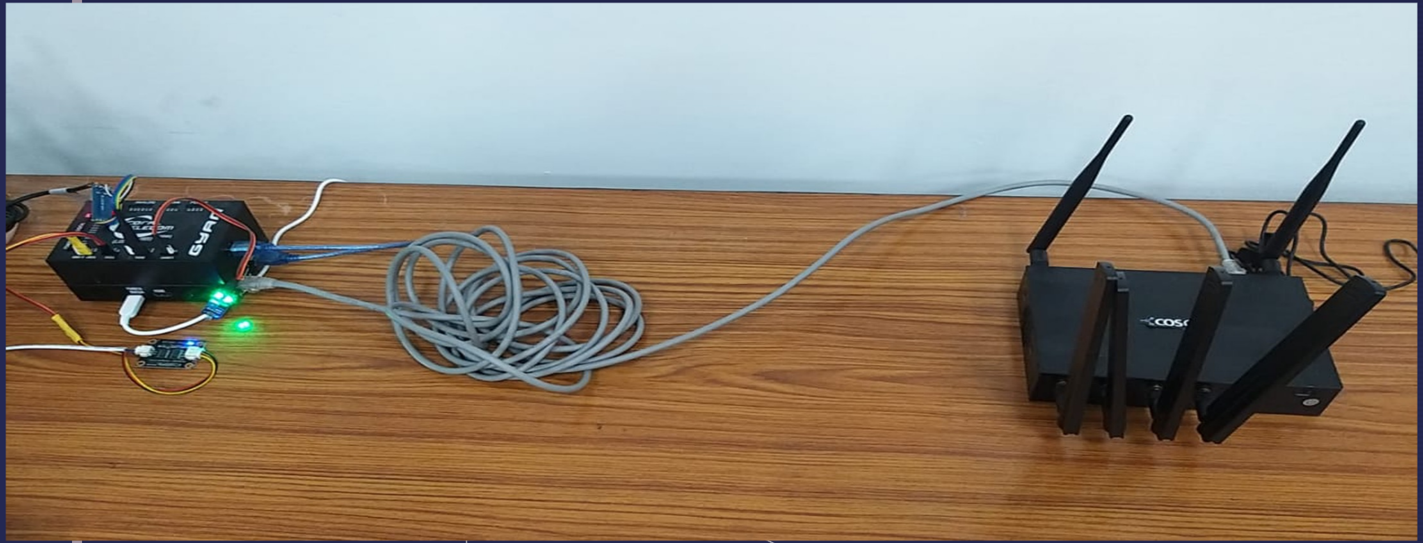
- 5MP 1/2.7" CMOS image sensor, low luminance, and high-definition image.

- Intelligent Analytics Supported: Human Detection, Intrusion Detection, Audio Detection, Object Left, Object Lost, Line crossing, Scene Change

- SD card supported up to 512GB.

- Wide Dynamic Range up to 120dB

- Digital Alarm 1 Ch In/ 1 Ch Out



IoT Sensor Software

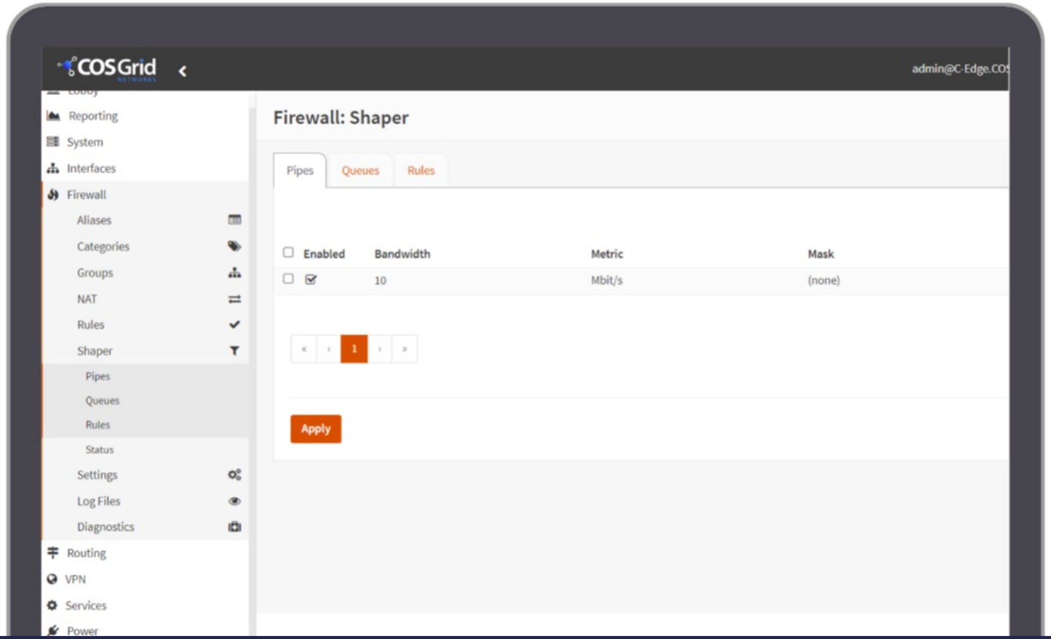
Now connect the Coral Gyan on IoT Gateway on

LAN 0 port.

Now all the sensor will send the data through the IoT Gateway to the 5G Core. The Core will then send this data to NMS for analysis & research.

AR/VR

- This VR headset uses a powerful Qualcomm XR 2 processor with an Adreno 650 GPU for smooth visuals. It has dual high-resolution displays (3200 x 1600 each) with a 90Hz refresh rate for a clear and immersive experience. The wide field of view (95-105 degrees) further enhances the feeling of being in a virtual world.
- The headset offers adjustable features for comfort, including an IPD range of 60-68 mm and diopter adjustment for users with nearsightedness. Two 16MP RGB cameras enable high-quality passthrough for viewing the real world without removing the headset.
- For tracking, it utilizes 4 infrared cameras for precise 6DOF (degrees of freedom) movement detection. Connectivity options include Wi-Fi 6 and Bluetooth 5 for wireless streaming, along with a USB-C port for wired connections. The Android 12 operating system provides a familiar platform for VR applications.
- This headset boasts 8GB of RAM and 128GB of storage, along with a long-lasting 5500mAh battery that supports over 3 hours of use. Fast charging with QC 3.0 ensures quick power-ups. The headset is compatible with OpenXR and SteamVR platforms, opening up a vast library of VR experiences.



Firewall: Shaper

□ Enabled	Bandwidth	Metric	Mask
□ ☑	10	Mbit/s	(none)

Firewall & Gateway

I. Complete next-gen firewall capability that is specifically designed to deliver the best protection and performance for the modern encrypted internet.

II. Integrates with COSGrid Netshield NDR, enabling Automated Threat Response and Synchronized Security to effectively mitigate threats before they can cause any significant damage

III. Extensive SD-WAN capabilities with ReFleX SD-WAN , allowing you to easily and securely orchestrate and interconnect your various offices and locations.

IV. Support for our SSE and SASE cloud-delivered network security solutions including MicroZAccess ZTNA, SIG/SWG

V. Secure and easy remote Access with ZTNA 2.0 feature

VI. Detailed Visibility and Network Traffic with the centralized dashboard.

IoT Gateway

COSGrid IoT gateway is a cutting-edge network router designed to facilitate seamless connectivity and communication between IoT devices, its users and the cloud . By leveraging the power of 5G, our gateway ensures ultra-fast and reliable data transfers, minimizing latency and maximizing throughput. Our COSGrid IoT gateway is not only a hardware device but also encompasses powerful software programs that enhance its functionality. It is designed to seamlessly integrate with existing IoT ecosystems, making it highly versatile and adaptable to various IoT deployments.

With COSGrid, businesses and organizations can experience enhanced connectivity, improved data security, and streamlined device management. Our IoT gateway is the ultimate solution for harnessing the full potential of IoT devices and leveraging the power of the cloud for data-driven decision-making.

Ethernet Switch

Features

•Ports:

24 x 10/100/1000Base-T ports

4 x Combo Gigabit SFP ports

•Performance:

56 Gbps switching capacity

41.67 Mpps forwarding rate

•Management:

Web-based management interface

SNMP support

•VLAN Support:

Supports up to 256 802.1Q VLANs

•QoS (Quality of Service):

•802.1p QoS for traffic prioritisation

•Security:

•Access Control Lists (ACLs)

•Storm Control

•Port Security

•Advanced Features:

•Link Aggregation (802.3ad LACP)

•STP/RSTP (Spanning Tree Protocols)

•IGMP Snooping for multicast traffic management

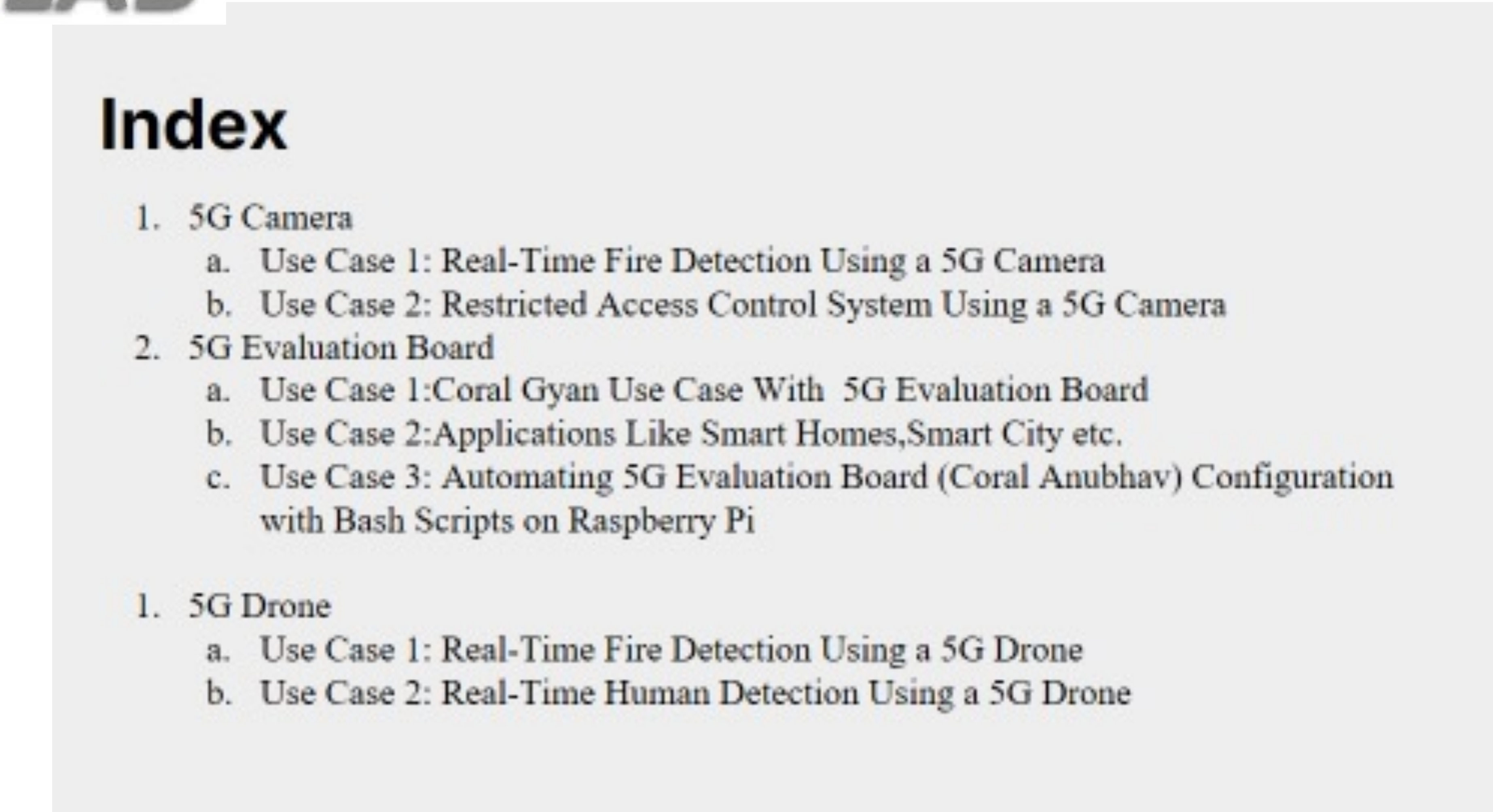
Dell Server (Core,IMS,NMS,MEC)

Powerhouse for 5G and Network Management: This server is a powerhouse built to handle the demanding workloads of 5G core networks and Network Management Systems (NMS).

Key Specs:

- **Dual Hard Disk Slots:** Provides storage flexibility for critical 5G core data and NMS logs.
- **64 GB RAM:** Enables smooth handling of real-time data processing, network simulations, and complex NMS functionalities.
- **48 CPU Cores:** Delivers exceptional processing power to manage the high volume of data traffic and tasks associated with 5G networks and NMS operations.
- **IP Address of 5G Core:** 192.168.16.10
- **IP Address of NMS**:192.168.16.6

5G Use Cases



Index

5G Camera:
Real-Time Fire Detection Using a 5G Camera

Overview

- AI-powered fire detection using a 5G-enabled camera & MEC-based VM.
- Uses YOLOv5/YOLOv9 for real-time inference.
- Ensures low latency, instant alerts, and remote monitoring.

Implementation Steps
1. Set Up VM on MEC Server

- OS: Ubuntu 20.04/22.04 LTS
- Resources: 10+ cores CPU, 16GB RAM, 100GB SSD
- Install dependencies:

```
sudo apt update && sudo apt upgrade -y

sudo apt install -y git python3 python3-pip ffmpeg

pip3 install torch torchvision torchaudio opencv-python numpy
```

2. Configure 5G Camera Connectivity

- Assign static IP to VM:
  - IP: 192.168.xx.xx
  - Subnet: 255.255.255.0
  - Gateway: 192.168.x.10 (5G Core)

5G Camera:
Real-Time Fire Detection Using a 5G Camera

Deploy Fire Detection Model

Find & Clone YOLO-based Fire Detection Repository

```
 git clone <repository_url>

             cd <repository_name>

             pip3 install -r requirements.txt
```

- Process RTSP video stream for fire detection in real-time.

Benefits

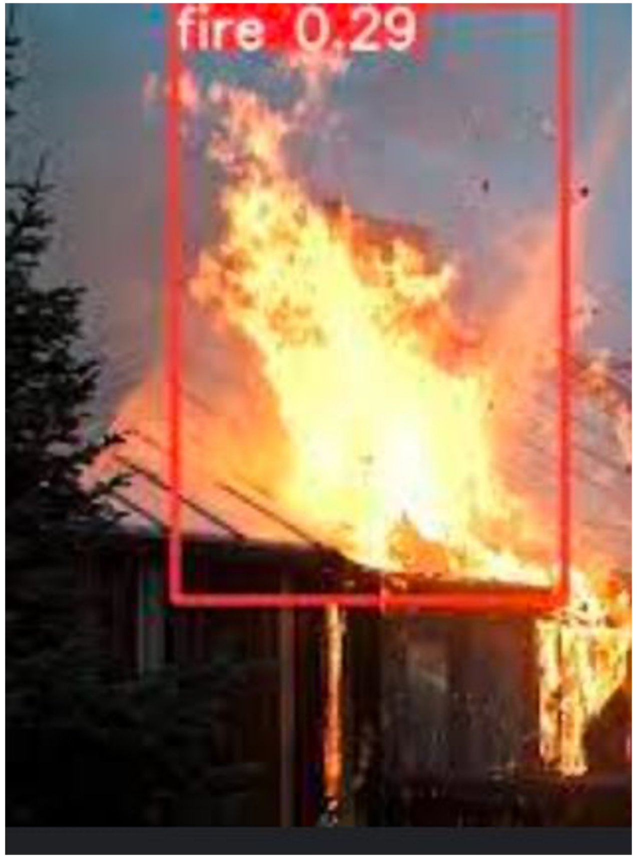
-Real-time alerts for faster response.

-Low-latency processing with MEC.

-Remote monitoring & scalability.

Challenges & Future Enhancements

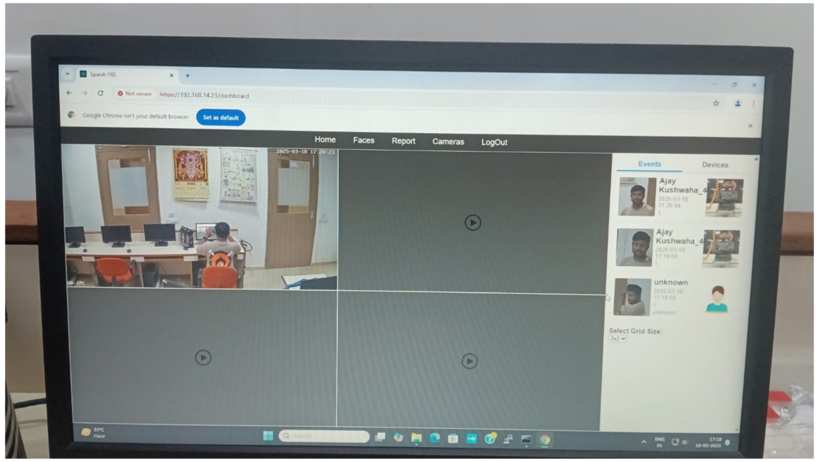
- Network dependency: Requires stable 5G.
- False positives: Needs model fine-tuning.
- Optimizations: Edge AI for faster inference & improved accuracy.



5G Camera:
Restricted Access Control System Using a 5G Camera

Overview

- AI-powered facial recognition for secure access control.
- Uses a 5G-enabled camera and MEC-based processing for real-time recognition.
- Enhances security, minimizes unauthorized entry, and automates access logs.



System Components

1. **5G-Enabled Camera** – Captures real-time video feed.
2. **MEC Server** – Runs AI facial recognition for access validation.
3. **Access Control Mechanism** – Electronic door lock integrated with the system.
4. **Cloud Database (Optional)** – Stores personnel data and access logs.

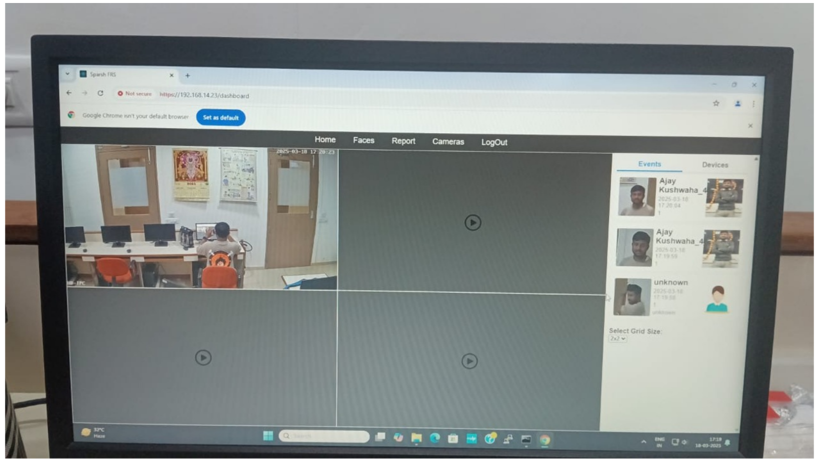
Key Features

- Real-time facial recognition ensures only authorized entry.
- Automated alerts notify in case of unauthorized access attempts.
- Scalable deployment across multiple locations with centralized monitoring.

5G Camera:
Restricted Access Control System Using a 5G Camera

Implementation Process

1. Camera & Network Setup – Configure 5G camera and RTSP streaming.
2. MEC Server Installation – Install AI-driven facial recognition software.
3. Database Configuration – Store personnel images and access levels.
4. Access Control Integration – Link AI system to electronic locks.
5. Real-time Monitoring – Log each access attempt for security.



Challenges & Solutions

- Network Latency Issues – Ensure stable 5G connectivity.
- False Positives/Negatives – Optimize AI with better datasets.
- RTSP Streaming Issues – Verify network and camera firmware.

Future Enhancements

- Edge AI integration for even faster recognition.
- Improved AI training for better accuracy.
- Cloud-based analytics for enhanced monitoring.

5G Evaluation Board:

Coral Gyan Use Case With 5G Evaluation Board

Overview

- Coral Gyan transmits sensor data via a 5G Evaluation Board to the NMS (Network Management System) over a 5G network.
- Wireless connectivity is essential for data transmission.

Requirements

1. Accessing Coral Gyan

   - IP Address, Username(gyan),
   - and Password(CgYaN@817&&) required.
   - Ensure Coral Gyan has a Wi-Fi module or use a wireless dongle.

2. Configuring Wireless LAN

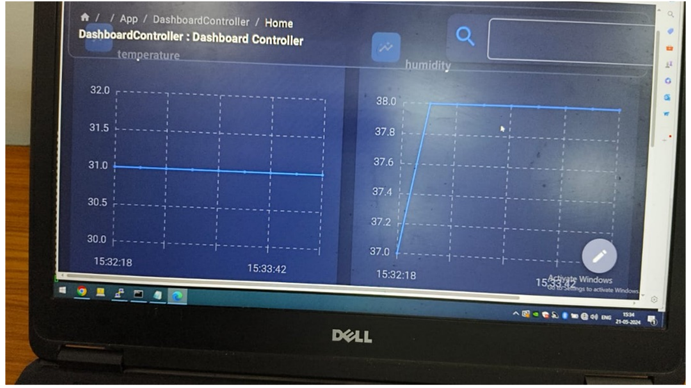
   Turn on Coral Gyan and access terminal.

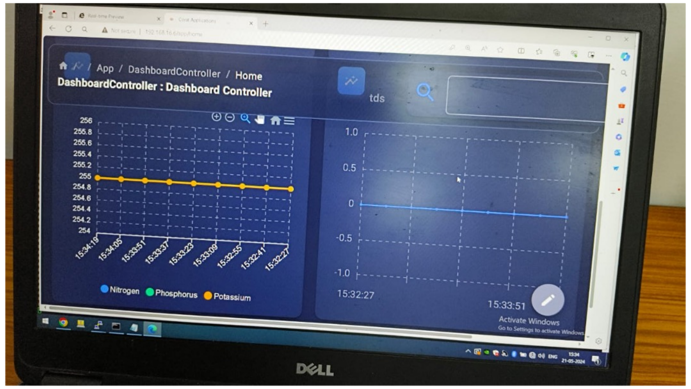
   Run the command:

```
raspi-config
```

   Navigate to System Options → Wireless LAN.

   Enter Wi-Fi SSID and Password for network connection.





5G Evaluation Board:

Coral Gyan Use Case With 5G Evaluation Board

Data Transmission Process

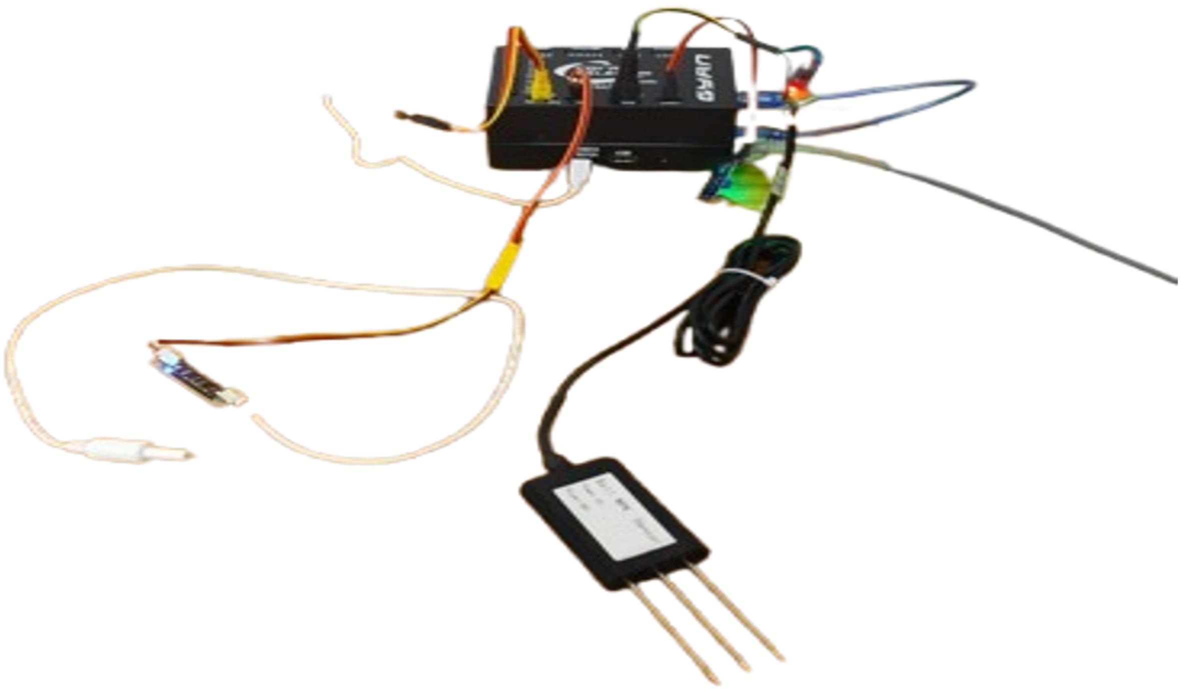
1. Connect Coral Gyan to Wifi using the configuration steps.
2. Sensor data is collected from connected devices.
3. 5G Evaluation Board transmits data securely over the 5G network.
4. Data reaches NMS for monitoring and analysis.

Key Considerations & Troubleshooting

- Check Wifi Connection – Ensure SSID(QSoftAP) & Password(1234567890) are correct.
- Verify 5G Evaluation Board Setup – Proper integration with Coral Gyan.
- Monitor Data Transfer – Use logs to verify transmission to NMS.

Conclusion

- Efficient data transmission using Coral Gyan + 5G Evaluation Board.
- Real-time monitoring and analytics via 5G network.
- Scalable for IoT applications and edge computing.



5G Evaluation Board:

Applications Like Smart Homes,Smart City etc.

Introduction

- Raspberry Pi as a low-cost, versatile device for IoT applications.
- Used in **Smart Homes, Smart Cities, and Smart Agriculture** to collect and transmit sensor data
- You can use smoke sensor, gas leak sensor & fire detection sensor .

How It Works

- Raspberry Pi connects to various sensors (Smoke Sensor, Gas Leak Sensor & Fire Detection Sensor etc)
- Data is sent to a cloud/server via Wi-Fi or a 5G Evaluation Board(Coral Anubhav)
- Enables automation and real-time monitoring for smart applications.

5G Evaluation Board:

Applications Like Smart Homes,Smart City etc.

Setup & Connectivity

- Raspberry Pi is configured to connect to WiFi or a 5G evaluation board.
- Sensors are connected to the Raspberry Pi.

Data Processing & Transmission

- A **Python script** collects real-time sensor data.
- Data is transmitted to a **server/NMS**
- The server processes and stores the data for analysis.

Applications & Benefits

- **Smart Homes**: Automates appliances, security, and climate control.
- **Smart Cities**: Air quality monitoring, traffic optimization, and energy management.
- **Smart Agriculture**: Monitors soil moisture, controls irrigation, and optimizes farming.

5G Evaluation Board :

Automating 5G Evaluation Board Configuration with Bash Scripts

Overview

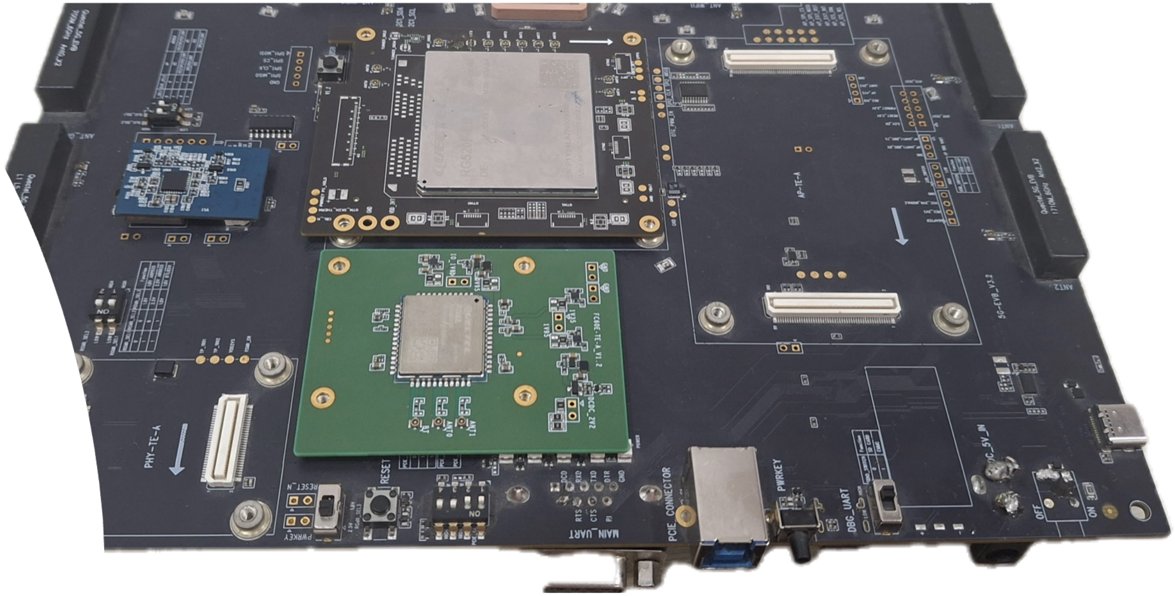
- Automates 5G Evaluation Board setup on Raspberry Pi using Bash scripts.
- Eliminates manual configuration, ensuring faster deployment & reduced errors.
- Ideal for IoT applications, industrial automation, and research projects.

Prerequisites

- Raspberry Pi with USB support.
- 5G Evaluation Board & SIM card.
- Minicom / Socat for serial communication.
- USB-to-Serial driver (if needed).

Setup Steps

1. Run as Root
   ```
   sudo -i
   ```
2. Check Device Path
   ```
   ls /dev/ttyUSB*
   ```
3. Install Required Packages
   ```
   sudo apt update && sudo apt install -y socat
   ```
4. Grant USB Permissions
   ```
   sudo chmod 777 /dev/ttyUSB*
   ```



5G Evaluation Board :

Automating 5G Evaluation Board Configuration with Bash Scripts

Key Features of Automation
Hands-free Setup – No need for manual command execution.
Faster Deployment – Reduces setup time for 5G connectivity.
Error Reduction – Minimizes human mistakes in modem configuration.
Auto-Restart on Failure – Systemd ensures continuous operation.

How It Works

1. Raspberry Pi runs predefined Bash commands to configure the modem.
2. The script automates network registration & modem setup.
3. A systemd service ensures the script runs automatically on boot.
4. The modem continuously operates without manual intervention.

Conclusion

- Automating 5G modem setup improves efficiency & reliability.
- Reduces downtime & ensures seamless IoT & industrial automation.
- Easy to implement using Bash scripting & systemd services.

5G Drone:

Real-Time Fire Detection Using a 5G Drone

Overview

- Uses a 5G-enabled drone and an MEC (Multi-access Edge Computing) server for real-time fire detection.
- AI-powered analysis using YOLOv5/v9 ensures low-latency, high-accuracy detection.
- Ideal for industrial, commercial, and remote area surveillance.

Step 1: Set Up a Virtual Machine (VM) on the MEC Server

- OS: Ubuntu 20.04/22.04 LTS (stable for AI & deep learning).
- Resources:
  - CPU: 10 cores (8+ recommended for real-time processing).
  - RAM: 12GB (16GB+ recommended).
  - Storage: 100GB SSD.
- Install Dependencies for deep learning and video processing.

Step 2: Establish Network Connectivity with the 5G Drone

- The drone streams video over RTSP (Real-Time Streaming Protocol).
- Configure the VM with a static IP to communicate with the 5G Core Gateway.
  - Example:
    - IP: 192.168.xx.xx
    - Subnet Mask: 255.255.255.0
    - Gateway: 192.168.x.10

5G Drone:

Real-Time Fire Detection Using a 5G Drone

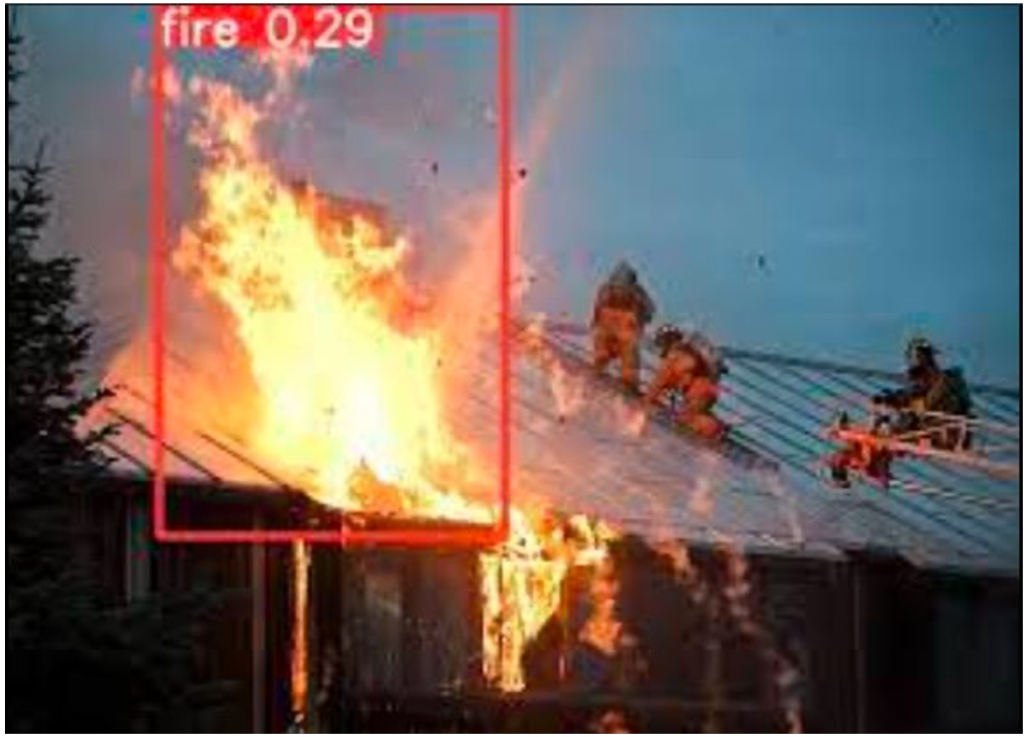
Step 3: Implement Fire Detection System

5G Drone Setup

- Equipped with an HD thermal camera.
- Streams real-time surveillance footage.

AI-Powered Fire Detection

- The MEC server processes live video streams using YOLOv5/v9.
- Detects flames and triggers visual alerts in real time.



Conclusion

High-Speed, Low-Latency Surveillance – AI detects fires instantly.

Real-Time Alerts – Immediate response to potential hazards.

Remote Monitoring – Seamless RTSP streaming over 5G.

Wide Applications – Ideal for industrial, commercial, and remote safety monitoring.

Future Optimizations:

- Edge AI integration for faster, on-device processing.
- Enhanced AI model training for improved detection accuracy.

5G Drone:

Real-Time Human Detection Using a 5G Drone

Overview

- Uses a 5G-enabled drone and an MEC (Multi-access Edge Computing) server for real-time human detection.
- AI-powered YOLOv5/v9 model ensures low-latency, high-accuracy tracking.
- Ideal for security, surveillance, and access control.

Step 1: Set Up a Virtual Machine (VM) on the MEC Server

- OS: Ubuntu 20.04/22.04 LTS (stable & AI-compatible).
- Resources:
  - CPU: 10 cores (8+ recommended for real-time AI processing).
  - RAM: 12GB (16GB+ recommended).
  - Storage: 100GB SSD.
- Install Dependencies (AI libraries, deep learning frameworks).
- Optional: Use Docker inside the VM for flexibility.

Step 2: Establish Network Connectivity with the 5G Drone

- The drone streams video over RTSP (Real-Time Streaming Protocol).
- Configure the VM with a static IP for seamless 5G Core Gateway communication.
  - Example:
    - IP: 192.168.xx.xx
    - Subnet Mask: 255.255.255.0
    - Gateway: 192.168.x.10

5G Drone:

Real-Time Human Detection Using a 5G Drone

Step 3: AI-Based Human Detection Model Deployment
Selecting the Right AI Model

- Uses YOLOv5/v9 trained for human detection from aerial views.
- Differentiates between humans and background elements.

Real-Time Processing on MEC Server

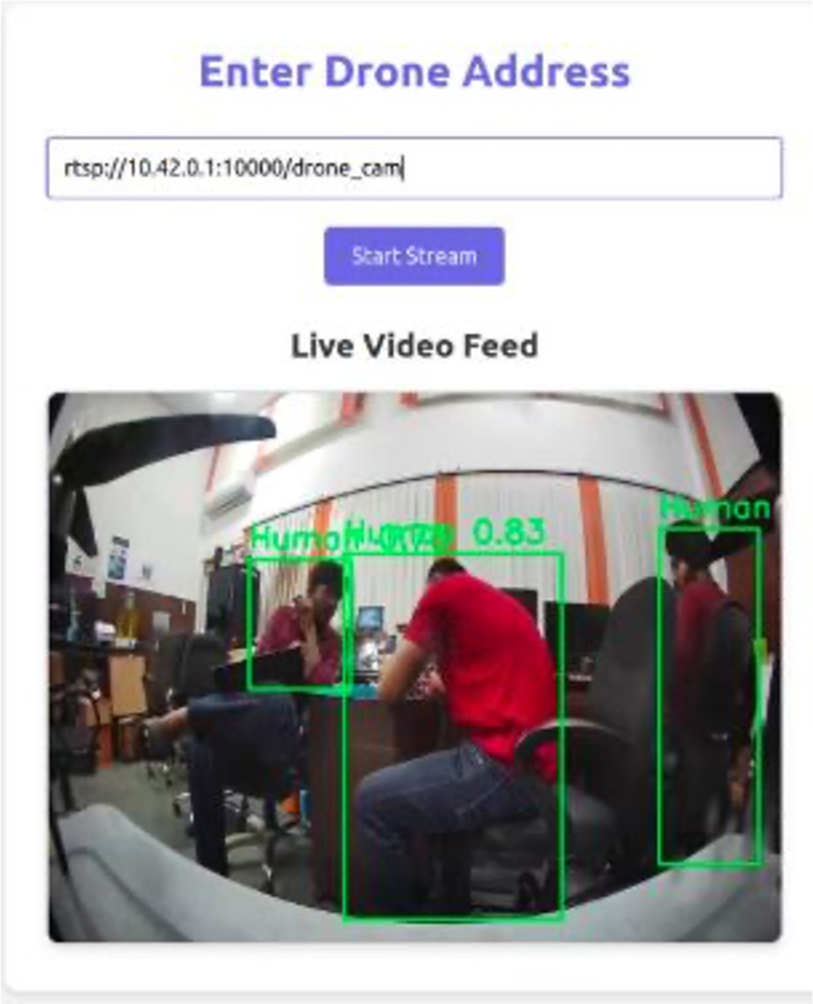
- AI model analyzes RTSP video feed in real time.
- Detects human presence, tracks movements, and flags anomalies.
- Enables security alerts and access control based on detections.

Conclusion

Fast & Accurate Surveillance – AI enhances security and monitoring.
Real-Time Alerts – Detects unauthorized individuals instantly.
5G-Powered Streaming – Ensures smooth and continuous video processing.
Scalable & Secure – Ideal for industrial, commercial, and security applications.

Future Optimizations:

- Enhanced AI training for improved detection accuracy.
- Integration with biometric recognition for access control.



Enter Drone Address

rtsp://10.42.0.1:10000/drone_cam

Protocol Deployment on Server

In 5G, protocol deployment involves installing and configuring core network functions.

All required protocols are bundled into a single ISO image for simplified deployment.

Control Plane Protocols:

Control Plane Protocols: Responsible for signaling and control information.

- Non-Access Stratum (NAS)
- Next Generation Application Protocol (NGAP)
- Stream Control Transmission Protocol (SCTP)
- Packet Forward Control Protocol(PFCP)

User Plane Protocols:
Handle the actual user data transmission.

GPRS Tunnelling Protocol – User Plane (GTP-U)

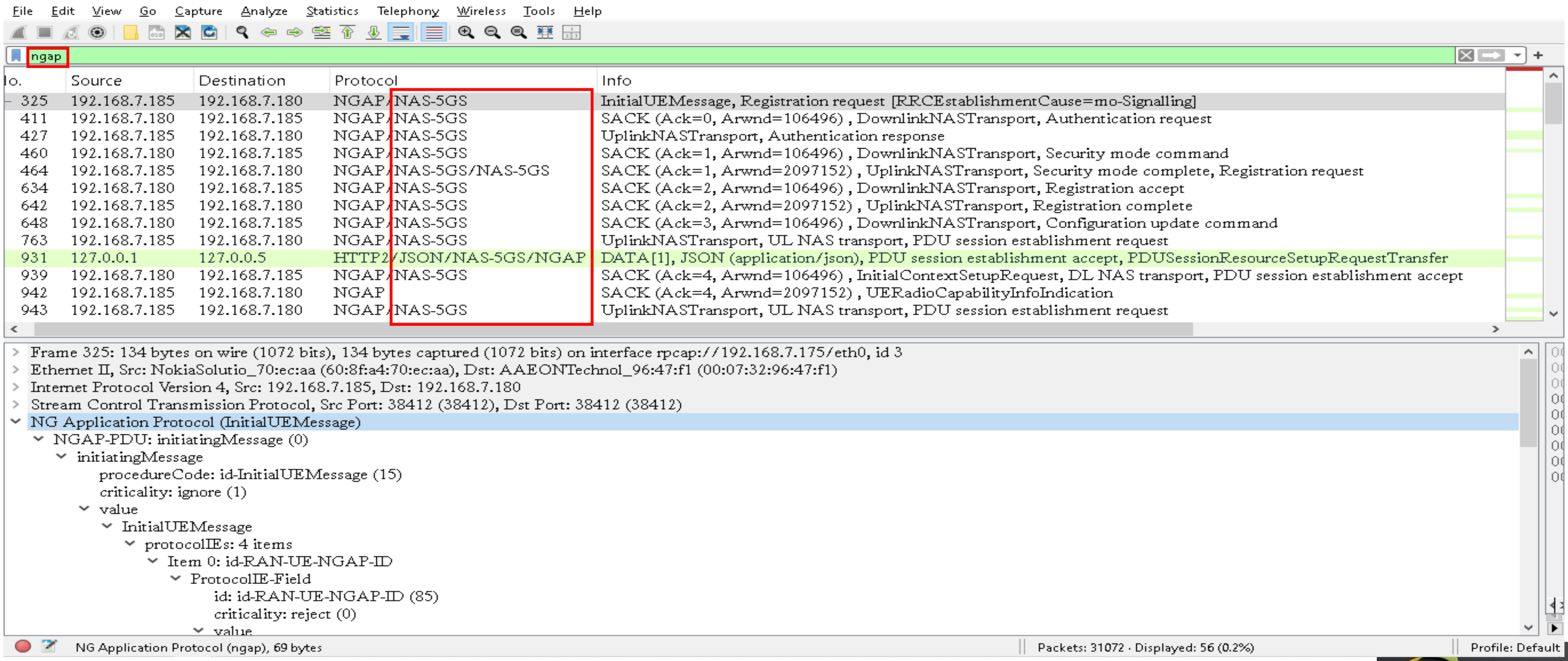
5G Service Protocols:
Manage NF communication and session policies.

HyperText Transfer Protocol /2 (HTTP/2)

NAS (Non-Access Stratum)

- It handles signaling between the User Equipment (UE) and the 5G Core Network (AMF).
- NAS operates independently of the RAN (Radio Access Network) and is responsible for UE authentication, mobility management, and session management.

NAS (Non-Access Stratum)



ngap

lo.	Source	Destination	Protocol	Info
325	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
411	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request
427	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	UplinkNASTransport, Authentication response
460	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command
464	192.168.7.185	192.168.7.180	NGAP/NAS-5GS/NAS-5GS	SACK (Ack=1, Arwnd=2097152) , UplinkNASTransport, Security mode complete, Registration request
634	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Registration accept
642	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=2097152) , UplinkNASTransport, Registration complete
648	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Configuration update command
763	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	UplinkNASTransport, UL NAS transport, PDU session establishment request
931	127.0.0.1	127.0.0.5	HTTP2/JSON/NAS-5GS/NGAP	DATA[1], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequestTransfer
939	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=4, Arwnd=106496) , InitialContextSetupRequest, DL NAS transport, PDU session establishment accept
942	192.168.7.185	192.168.7.180	NGAP	SACK (Ack=4, Arwnd=2097152) , UERadioCapabilityInfoIndication
943	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	UplinkNASTransport, UL NAS transport, PDU session establishment request

```
> Frame 325: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface rpcap://192.168.7.175/eth0, id 3
> Ethernet II, Src: NokiaSolutio_70:ec:aa (60:8f:a4:70:ec:aa), Dst: AAEONTechnol_96:47:f1 (00:07:32:96:47:f1)
> Internet Protocol Version 4, Src: 192.168.7.185, Dst: 192.168.7.180
> Stream Control Transmission Protocol, Src Port: 38412 (38412), Dst Port: 38412 (38412)
v NG Application Protocol (InitialUEMessage)
  v NGAP-PDU: initiatingMessage (0)
    v initiatingMessage
        procedureCode: id-InitialUEMessage (15)
        criticality: ignore (1)
      v value
        v InitialUEMessage
          v protocolIEs: 4 items
            v Item 0: id-RAN-UE-NGAP-ID
              v ProtocolIE-Field
                  id: id-RAN-UE-NGAP-ID (85)
                  criticality: reject (0)
                v value
```

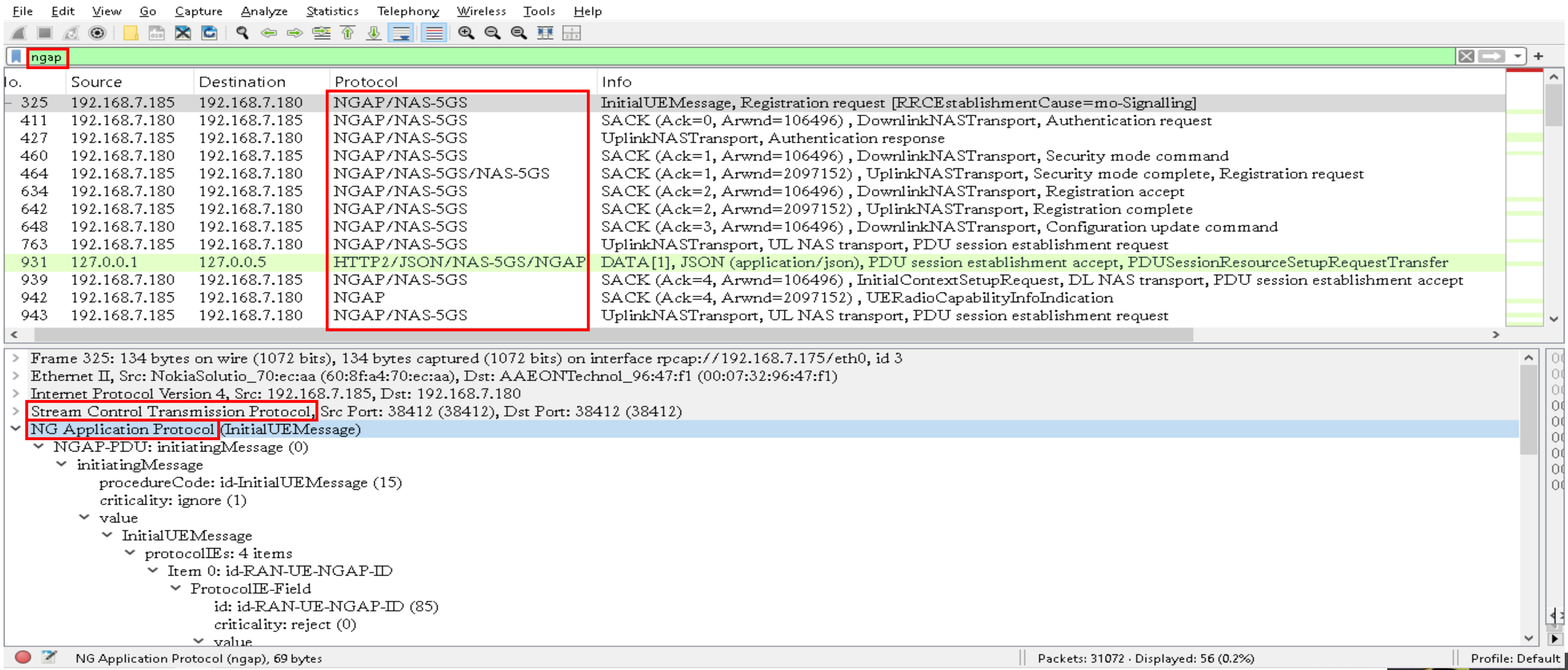
NG Application Protocol (ngap), 69 bytes | Packets: 31072 · Displayed: 56 (0.2%) | Profile: Default

Research, Design, Develop & Manufacturing in India

NGAP (Next Generation Application Protocol)

- Communication between gNB and AMF.
- Used for UE registration, mobility management, and PDU session establishment.
- Runs over SCTP.

NGAP (Next Generation Application Protocol)



lo.	Source	Destination	Protocol	Info
325	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
411	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request
427	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	UplinkNASTransport, Authentication response
460	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command
464	192.168.7.185	192.168.7.180	NGAP/NAS-5GS/NAS-5GS	SACK (Ack=1, Arwnd=2097152) , UplinkNASTransport, Security mode complete, Registration request
634	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Registration accept
642	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=2097152) , UplinkNASTransport, Registration complete
648	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Configuration update command
763	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	UplinkNASTransport, UL NAS transport, PDU session establishment request
931	127.0.0.1	127.0.0.5	HTTP2/JSON/NAS-5GS/NGAP	DATA[1], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequestTransfer
939	192.168.7.180	192.168.7.185	NGAP/NAS-5GS	SACK (Ack=4, Arwnd=106496) , InitialContextSetupRequest, DL NAS transport, PDU session establishment accept
942	192.168.7.185	192.168.7.180	NGAP	SACK (Ack=4, Arwnd=2097152) , UERadioCapabilityInfoIndication
943	192.168.7.185	192.168.7.180	NGAP/NAS-5GS	UplinkNASTransport, UL NAS transport, PDU session establishment request

```
> Frame 325: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface rpcap://192.168.7.175/eth0, id 3
> Ethernet II, Src: NokiaSolutio_70:ec:aa (60:8f:a4:70:ec:aa), Dst: AAEONTechnol_96:47:f1 (00:07:32:96:47:f1)
> Internet Protocol Version 4, Src: 192.168.7.185, Dst: 192.168.7.180
> Stream Control Transmission Protocol, Src Port: 38412 (38412), Dst Port: 38412 (38412)
v NG Application Protocol (InitialUEMessage)
    v NGAP-PDU: initiatingMessage (0)
        v initiatingMessage
            procedureCode: id-InitialUEMessage (15)
            criticality: ignore (1)
          v value
              v InitialUEMessage
                  v protocolIEs: 4 items
                      v Item 0: id-RAN-UE-NGAP-ID
                          v ProtocolIE-Field
                              id: id-RAN-UE-NGAP-ID (85)
                              criticality: reject (0)
                            v value
```

NG Application Protocol (ngap), 69 bytes

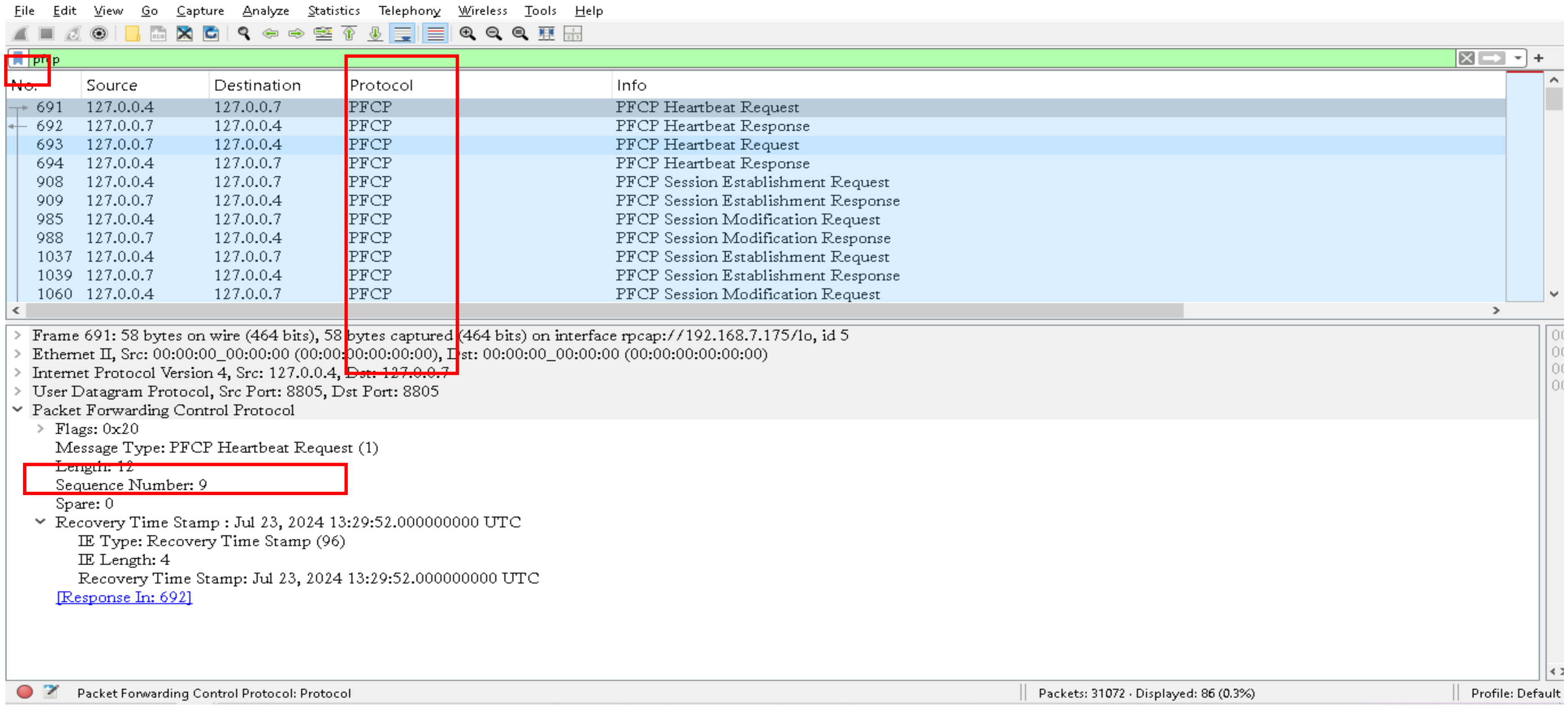
Packets: 31072 · Displayed: 56 (0.2%)

Profile: Default

PFCP (Packet Forwarding Control Protocol)

- Communication between SMF and UPF.
- Controls the establishment, modification, and deletion of PDU sessions.
- Manages QoS policies and traffic rules.

PFCP (Packet Forwarding Control Protocol)


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

pfcp

No.	Source	Destination	Protocol	Info
691	127.0.0.4	127.0.0.7	PFCP	PFCP Heartbeat Request
692	127.0.0.7	127.0.0.4	PFCP	PFCP Heartbeat Response
693	127.0.0.7	127.0.0.4	PFCP	PFCP Heartbeat Request
694	127.0.0.4	127.0.0.7	PFCP	PFCP Heartbeat Response
908	127.0.0.4	127.0.0.7	PFCP	PFCP Session Establishment Request
909	127.0.0.7	127.0.0.4	PFCP	PFCP Session Establishment Response
985	127.0.0.4	127.0.0.7	PFCP	PFCP Session Modification Request
988	127.0.0.7	127.0.0.4	PFCP	PFCP Session Modification Response
1037	127.0.0.4	127.0.0.7	PFCP	PFCP Session Establishment Request
1039	127.0.0.7	127.0.0.4	PFCP	PFCP Session Establishment Response
1060	127.0.0.4	127.0.0.7	PFCP	PFCP Session Modification Request

```
> Frame 691: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface rpcap://192.168.7.175/lo, id 5
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.4, Dst: 127.0.0.7
> User Datagram Protocol, Src Port: 8805, Dst Port: 8805
v Packet Forwarding Control Protocol
  > Flags: 0x20
    Message Type: PFCP Heartbeat Request (1)
    Length: 12
    Sequence Number: 9
    Spare: 0
  v Recovery Time Stamp : Jul 23, 2024 13:29:52.000000000 UTC
      IE Type: Recovery Time Stamp (96)
      IE Length: 4
      Recovery Time Stamp: Jul 23, 2024 13:29:52.000000000 UTC
    [Response In: 692]
```

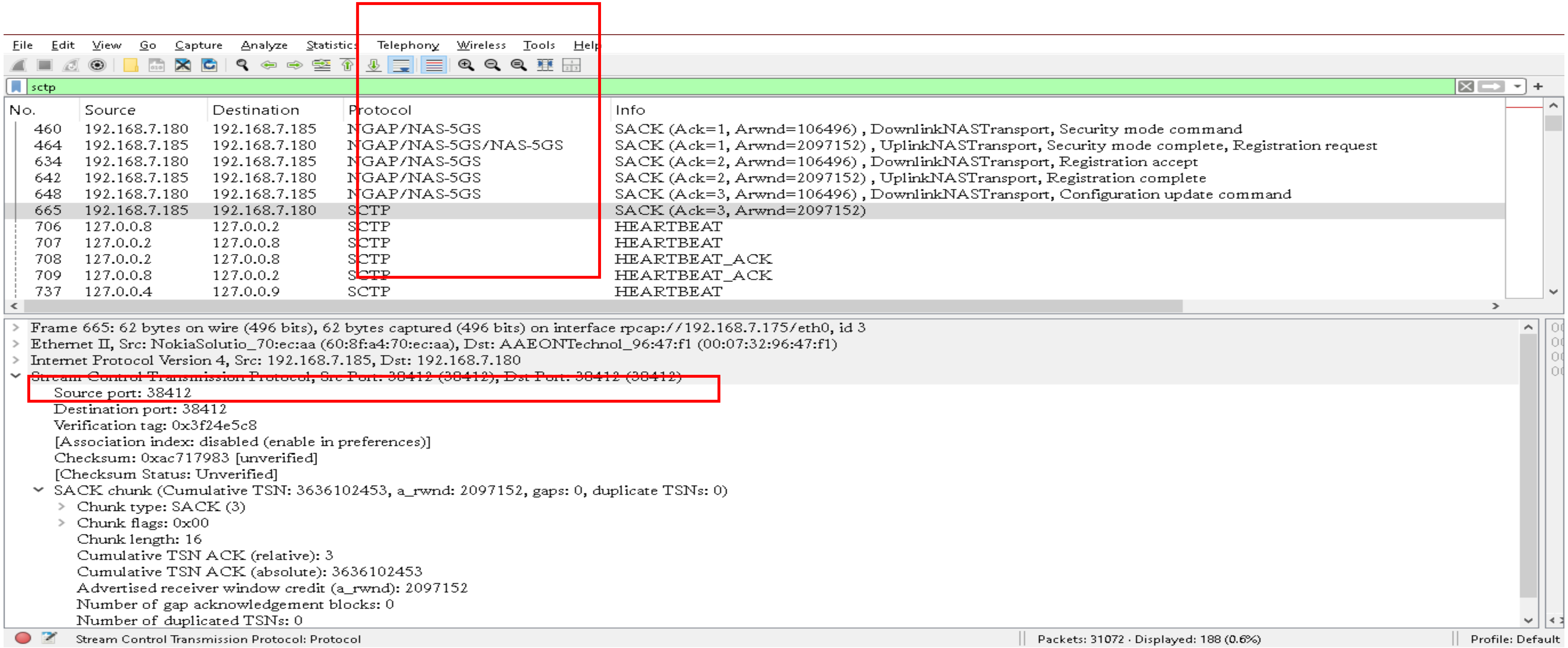
Packet Forwarding Control Protocol: Protocol | Packets: 31072 · Displayed: 86 (0.3%) | Profile: Default

Research, Design, Develop & Manufacturing in India

SCTP (Stream Control Transmission Protocol)

- Transport layer protocol for NGAP communication.
- Provides reliable message delivery between gNB and AMF.
- Supports multi-streaming to prevent head-of-line blocking.

SCTP (Stream Control Transmission Protocol)



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
sctp
```

```
No.   Source          Destination     Protocol               Info
 460  192.168.7.180   192.168.7.185   NGAP/NAS-5GS           SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command
 464  192.168.7.185   192.168.7.180   NGAP/NAS-5GS/NAS-5GS   SACK (Ack=1, Arwnd=2097152) , UplinkNASTransport, Security mode complete, Registration request
 634  192.168.7.180   192.168.7.185   NGAP/NAS-5GS           SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Registration accept
 642  192.168.7.185   192.168.7.180   NGAP/NAS-5GS           SACK (Ack=2, Arwnd=2097152) , UplinkNASTransport, Registration complete
 648  192.168.7.180   192.168.7.185   NGAP/NAS-5GS           SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Configuration update command
 665  192.168.7.185   192.168.7.180   SCTP                   SACK (Ack=3, Arwnd=2097152)
 706  127.0.0.8       127.0.0.2       SCTP                   HEARTBEAT
 707  127.0.0.2       127.0.0.8       SCTP                   HEARTBEAT
 708  127.0.0.2       127.0.0.8       SCTP                   HEARTBEAT_ACK
 709  127.0.0.8       127.0.0.2       SCTP                   HEARTBEAT_ACK
 737  127.0.0.4       127.0.0.9       SCTP                   HEARTBEAT
```

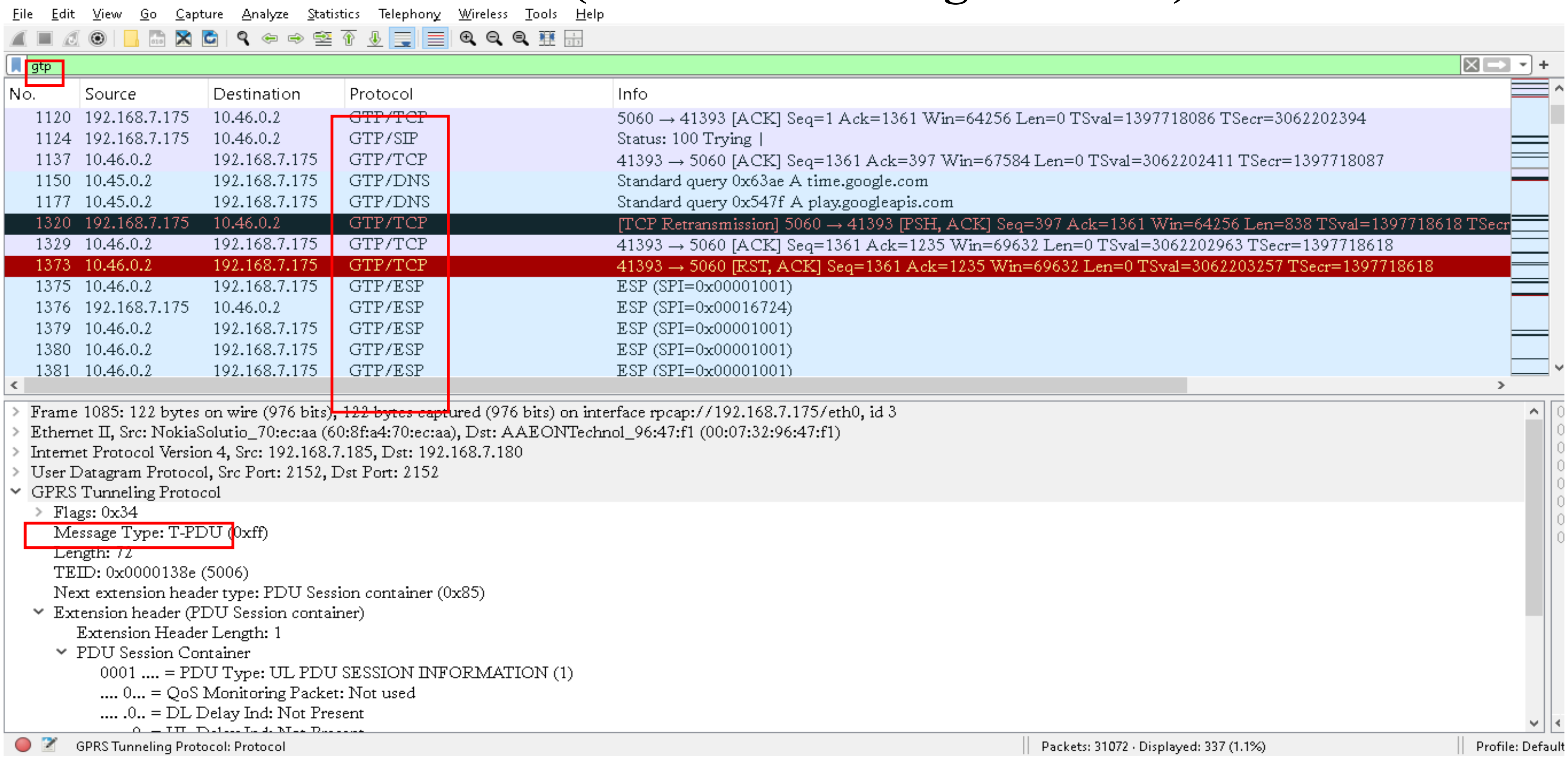
```
> Frame 665: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface rpcap://192.168.7.175/eth0, id 3
> Ethernet II, Src: NokiaSolutio_70:ec:aa (60:8f:a4:70:ec:aa), Dst: AAEONTechnol_96:47:f1 (00:07:32:96:47:f1)
> Internet Protocol Version 4, Src: 192.168.7.185, Dst: 192.168.7.180
v Stream Control Transmission Protocol, Src Port: 38412 (38412), Dst Port: 38412 (38412)
    Source port: 38412
    Destination port: 38412
    Verification tag: 0x3f24e5c8
    [Association index: disabled (enable in preferences)]
    Checksum: 0xac717983 [unverified]
    [Checksum Status: Unverified]
  v SACK chunk (Cumulative TSN: 3636102453, a_rwnd: 2097152, gaps: 0, duplicate TSNs: 0)
    > Chunk type: SACK (3)
    > Chunk flags: 0x00
      Chunk length: 16
      Cumulative TSN ACK (relative): 3
      Cumulative TSN ACK (absolute): 3636102453
      Advertised receiver window credit (a_rwnd): 2097152
      Number of gap acknowledgement blocks: 0
      Number of duplicated TSNs: 0
```

```
Stream Control Transmission Protocol: Protocol    Packets: 31072 · Displayed: 188 (0.6%)    Profile: Default
```

GTP-U (GPRS Tunneling Protocol – User Plane)

- Transfers user data between gNB and UPF.
- Encapsulates IP packets for tunneling over the 5G network.
- Carries both DL and UL traffic.

GTP-U (GPRS Tunneling Protocol)



gtp

No.	Source	Destination	Protocol	Info
1120	192.168.7.175	10.46.0.2	GTP/TCP	5060 → 41393 [ACK] Seq=1 Ack=1361 Win=64256 Len=0 TSval=1397718086 TSecr=3062202394
1124	192.168.7.175	10.46.0.2	GTP/SIP	Status: 100 Trying |
1137	10.46.0.2	192.168.7.175	GTP/TCP	41393 → 5060 [ACK] Seq=1361 Ack=397 Win=67584 Len=0 TSval=3062202411 TSecr=1397718087
1150	10.45.0.2	192.168.7.175	GTP/DNS	Standard query 0x63ae A time.google.com
1177	10.45.0.2	192.168.7.175	GTP/DNS	Standard query 0x547f A play.googleapis.com
1320	192.168.7.175	10.46.0.2	GTP/TCP	[TCP Retransmission] 5060 → 41393 [PSH, ACK] Seq=397 Ack=1361 Win=64256 Len=838 TSval=1397718618 TSecr
1329	10.46.0.2	192.168.7.175	GTP/TCP	41393 → 5060 [ACK] Seq=1361 Ack=1235 Win=69632 Len=0 TSval=3062202963 TSecr=1397718618
1373	10.46.0.2	192.168.7.175	GTP/TCP	41393 → 5060 [RST, ACK] Seq=1361 Ack=1235 Win=69632 Len=0 TSval=3062203257 TSecr=1397718618
1375	10.46.0.2	192.168.7.175	GTP/ESP	ESP (SPI=0x00001001)
1376	192.168.7.175	10.46.0.2	GTP/ESP	ESP (SPI=0x00016724)
1379	10.46.0.2	192.168.7.175	GTP/ESP	ESP (SPI=0x00001001)
1380	10.46.0.2	192.168.7.175	GTP/ESP	ESP (SPI=0x00001001)
1381	10.46.0.2	192.168.7.175	GTP/ESP	ESP (SPI=0x00001001)

```
> Frame 1085: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface rpcap://192.168.7.175/eth0, id 3
> Ethernet II, Src: NokiaSolutio_70:ec:aa (60:8f:a4:70:ec:aa), Dst: AAEONTechnol_96:47:f1 (00:07:32:96:47:f1)
> Internet Protocol Version 4, Src: 192.168.7.185, Dst: 192.168.7.180
> User Datagram Protocol, Src Port: 2152, Dst Port: 2152
v GPRS Tunneling Protocol
  > Flags: 0x34
    Message Type: T-PDU (0xff)
    Length: 72
    TEID: 0x0000138e (5006)
    Next extension header type: PDU Session container (0x85)
  v Extension header (PDU Session container)
      Extension Header Length: 1
    v PDU Session Container
        0001 .... = PDU Type: UL PDU SESSION INFORMATION (1)
        .... 0... = QoS Monitoring Packet: Not used
        .... .0.. = DL Delay Ind: Not Present
        .... ..0. = UL Delay Ind: Not Present
```

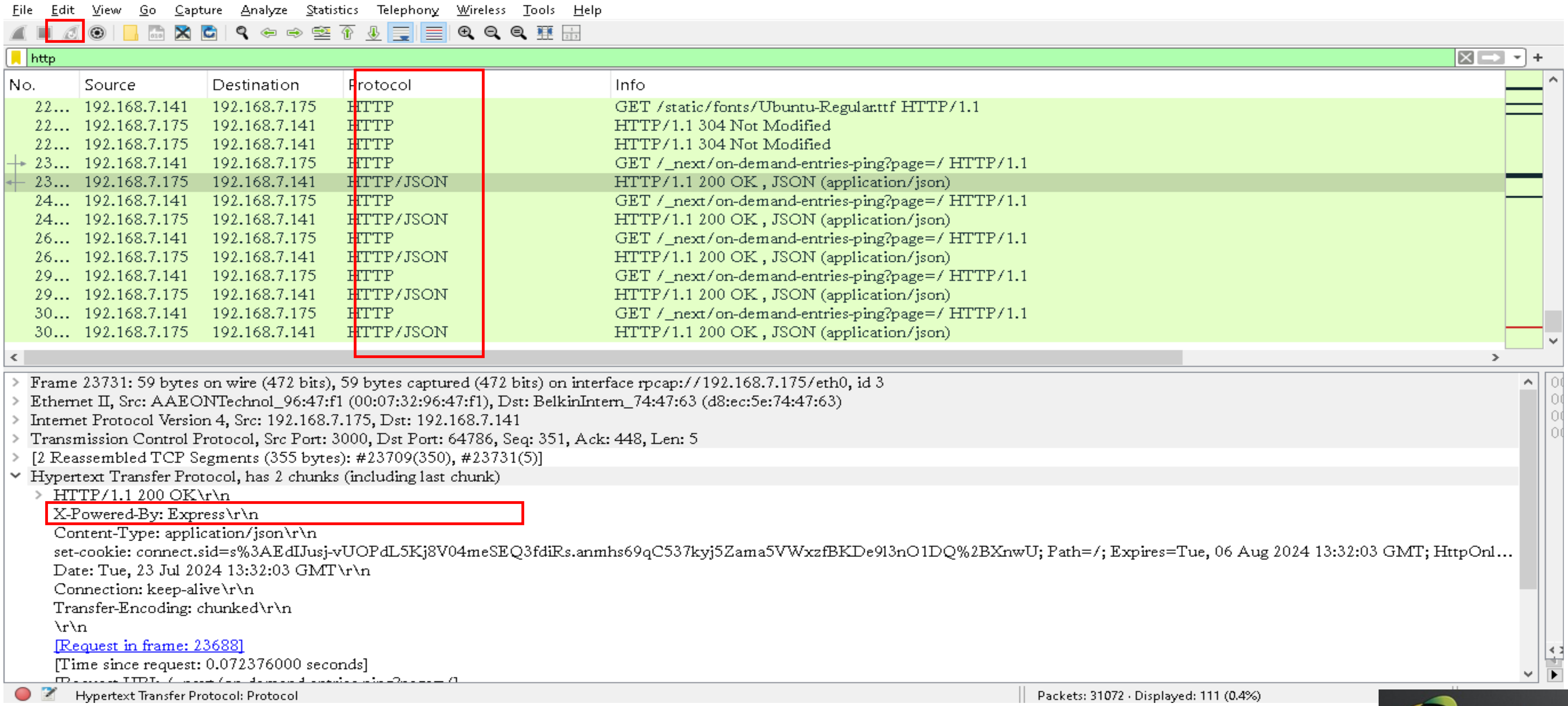
GPRS Tunneling Protocol: Protocol | Packets: 31072 · Displayed: 337 (1.1%) | Profile: Default

Research, Design, Develop & Manufacturing in India

Hypertext Transfer Protocol /2 (HTTP/2)

- Used for signaling between NFs in Service-Based Architecture.
- Supports efficient and multiplexed data communication.
- Enables faster session management.

Hypertext Transfer Protocol 2 (HTTP2)



http

```
No.     Source          Destination     Protocol     Info
  22... 192.168.7.141   192.168.7.175   HTTP         GET /static/fonts/Ubuntu-Regular.ttf HTTP/1.1
  22... 192.168.7.175   192.168.7.141   HTTP         HTTP/1.1 304 Not Modified
  22... 192.168.7.175   192.168.7.141   HTTP         HTTP/1.1 304 Not Modified
  23... 192.168.7.141   192.168.7.175   HTTP         GET /_next/on-demand-entries-ping?page=/ HTTP/1.1
  23... 192.168.7.175   192.168.7.141   HTTP/JSON    HTTP/1.1 200 OK , JSON (application/json)
  24... 192.168.7.141   192.168.7.175   HTTP         GET /_next/on-demand-entries-ping?page=/ HTTP/1.1
  24... 192.168.7.175   192.168.7.141   HTTP/JSON    HTTP/1.1 200 OK , JSON (application/json)
  26... 192.168.7.141   192.168.7.175   HTTP         GET /_next/on-demand-entries-ping?page=/ HTTP/1.1
  26... 192.168.7.175   192.168.7.141   HTTP/JSON    HTTP/1.1 200 OK , JSON (application/json)
  29... 192.168.7.141   192.168.7.175   HTTP         GET /_next/on-demand-entries-ping?page=/ HTTP/1.1
  29... 192.168.7.175   192.168.7.141   HTTP/JSON    HTTP/1.1 200 OK , JSON (application/json)
  30... 192.168.7.141   192.168.7.175   HTTP         GET /_next/on-demand-entries-ping?page=/ HTTP/1.1
  30... 192.168.7.175   192.168.7.141   HTTP/JSON    HTTP/1.1 200 OK , JSON (application/json)
```

```
> Frame 23731: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface rpcap://192.168.7.175/eth0, id 3
> Ethernet II, Src: AAEONTechnol_96:47:f1 (00:07:32:96:47:f1), Dst: BelkinIntern_74:47:63 (d8:ec:5e:74:47:63)
> Internet Protocol Version 4, Src: 192.168.7.175, Dst: 192.168.7.141
> Transmission Control Protocol, Src Port: 3000, Dst Port: 64786, Seq: 351, Ack: 448, Len: 5
> [2 Reassembled TCP Segments (355 bytes): #23709(350), #23731(5)]
v Hypertext Transfer Protocol, has 2 chunks (including last chunk)
  > HTTP/1.1 200 OK\r\n
    X-Powered-By: Express\r\n
    Content-Type: application/json\r\n
    set-cookie: connect.sid=s%3AEdIJusj-vUOPdL5Kj8V04meSEQ3fdiRs.anmhs69qC537kyj5Zama5VWxzfBKDe913nO1DQ%2BXnwU; Path=/; Expires=Tue, 06 Aug 2024 13:32:03 GMT; HttpOnl…
    Date: Tue, 23 Jul 2024 13:32:03 GMT\r\n
    Connection: keep-alive\r\n
    Transfer-Encoding: chunked\r\n
    \r\n
    [Request in frame: 23688]
    [Time since request: 0.072376000 seconds]
    [Request URI: /_next/on-demand-entries-ping?page=/
```

Hypertext Transfer Protocol: Protocol

Packets: 31072 · Displayed: 111 (0.4%)

CORAL TELECOM (LISTEN)(SEE)(THINK) Research, Design, Develop & Manufacturing in India

Network Node Connectivity in 5G

5G Core Node Connectivity – Service-Based Interfaces

- SBI uses a Service-Based Architecture NFs expose services that other NFs can consume.
- HTTP/2 over TCP/TLS is the primary protocol used for communication.
- Enables efficient, multiplexed, and secure signaling between NFs.

5G Core Node Connectivity – Service-Based Interfaces

- RBI uses point-to-point communication between specific NFs in the 5G Core.
- Ensures backward compatibility with LTE/EPC for seamless interworking.
- Utilizes GTP-U for user plane data transfer between UPFs.

5G Core Description

Reference Architecture Based Interfaces

Service Architecture Based is the foundation of 5G Core, certain interfaces still rely on Reference-Based Communication, particularly when interacting with legacy systems or non-SBA functions. These interfaces follow traditional point-to-point communication models with predefined protocols.

Interfaces of Reference Based Architecture in 5G

INTERFACE NAME	CONNECTING NODES
Uu	UE and RAN
N1	UE and AMF
N2	RAN and AMF
N3	RAN and UPF
N4	SMF and UPF
N5	PCF and AF
N6	UPF and DN
N7	SMF and PCF
N8	AMF and UDM
N9	UPF and UPF
N10	SMF and UDM
N11	AMF and SMF
N12	AMF and AUSF
N13	AUSF and UDM
N14	AMF and AMF
N15	AMF and PCF
N22	AMF and NSSF

Service Architecture Based Interfaces

5G adopts a Service-Based Architecture (SBA) to enhance flexibility, scalability, and efficiency. Unlike traditional telecom networks, SBA enables network functions (NFs) to communicate through service-based interfaces (SBI) using HTTP/2 and RESTful APIs. This architecture supports dynamic service discovery, allowing NFs to request and provide services seamlessly.

Interface of Service-Based Architecture (SBA) in 5G

INTERFACE NAME	CONNECTING NODES
Nnssf	AMF, SMF and NSSF
Nnrf	All NFs (AMF, SMF, PCF, etc.) and NRF
Npcf	AMF, SMF and PCF
Nudm	AMF, SMF, PCF and UDM
Naf	External Applications and AF
Nausf	AMF and AUSF
Namf	UE, gNB, SMF, NSSF and AMF
Nsmf	AMF and SMF

API for UE Context Management

API Endpoint: /namf-comm/v1

- **PUT /ue-contexts/{ueContextId}** - Creates a new UE context.
- **POST /ue-contexts/{ueContextId}/release** - Releases an existing UE context.
- **POST /ue-contexts/{ueContextId}/assign-ebi** - Assigns an EBI to a UE context.
- **POST /ue-contexts/{ueContextId}/transfer** - Transfers a UE context.
- **POST /ue-contexts/{ueContextId}/transfer-update** - Updates registration status for a UE context.
- **POST /ue-contexts/{ueContextId}/relocate** - Relocates a UE context.
- **POST /ue-contexts/{ueContextId}/cancel-relocate** - Cancels an ongoing UE context relocation.

**This is a sample representation of 5G APIs and does not cover the entire list of APIs used in 5G communication.

Access and Mobility Management Function(AMF)

It performs operations like Mobility Management, Registration Management, Connection Management, etc.

For UE connection, it acts as a single-entry point.

AMF selects the corresponding SMF for managing the user session context, based on the service requested by the customer.

When compared with 4G EPC, it's functionalities resembles with MME of 4G Network

SMF (Session Management Function)

- It performs operations like
  - Session management
  - IP address allocation & management for UE
  - User plane selection
  - QoS & policy enforcement for Control Plane used for Service registration/discovery/establishment
- Its functionalities resemble with SGW-C (Control Plane), MME, and PGW-C (Control Plane) of 4G Network, when compared with 4G EPC.

UPF (User Plane Function)

Maintains PDU Session, Performs packet routing & forwarding, Packet inspection, Policy enforcement for User plane, QoS handling, etc.

It's functionalities resemble with SGW-U (Serving Gateway User Plane function) and PGW-U (PDN Gateway User Plane function) of 4G Network, when compared with 4G EPC.

UDM (Unified Data Management)

It performs operations like user identification handling, subscription management, user authentication, access authorization for operations like roaming, etc.

When compared with 4G EPC, it's functionalities resemble with HSS/AAA Server of 4G network.

UDR (Unified Data Repository)

- It is central repository where data can be stores which includes
- Subscription Data
- Policy Data
- Exposure Data
- Any Application specific Data

AUSF (Authentication Server Function)

It allows the AMF to authenticate the UE.

When compared with 4G EPC, it's functionalities resemble with HSS/AAA Server of 4G Network.

NSSF (Network Slice Selection Function)

It maintains a list of the operator defined network slice instances.

Based on the subscription information stored in UDM, AMF authorizes the use of network slices.

Based on the service requirements, it can also query NSSF to authorize access to a Network slice.

NSSF redirects the traffic to an intended network slice.

NEF (Network Exposure Function)

It exposes services and resources over APIs within and outside the 5G Core.

With the help of NEF, 3rd party applications can also access the 5G services.

Other core networks can also be exposed using NEF.

NRF (NF Repository Function)

- It maintains the list of available network function instances and their profiles.
- To enable distinct network functions to find each other via APIs, it performs service registration and discovery.
- Example:
- When UE tries to access a service type served by the SMF, AMF discovers the SMF which is registered to NRF.
- Any authorized customer can access the services offered via registered network functions (Producers), since network functions are connected via service message bus in SBA.

PCF (Policy Control Function)

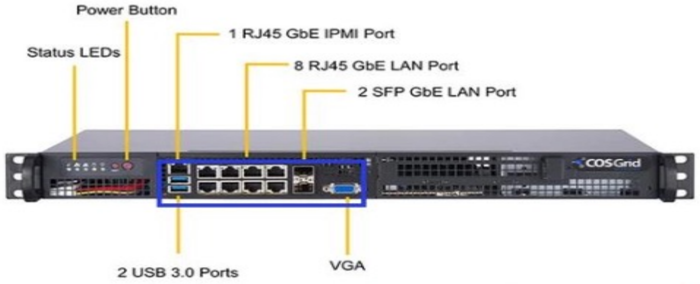
- It supports policy control framework, applying policy decisions, accessing subscription information, etc to govern the Network behavior.
- When compared with 4G EPC, it's functionalities resembles with PCRF of 4G Network.
- To govern the network behavior, it supports policy control framework, applying Policy decisions, accessing subscription information, etc.
- It's functionalities resembles with PCRF of 4G Network, when compared with 4G EPC.

Lunch Break

Firewall & Router

1 -Hardware Configuration & Support

Set Steps	Acceptance Criteria
Networking Interface	1 Gigabit Base-T (Cu) = 6 ports or higher(as required)
LAN Interface	1 Gs Fiber (SFP) = 4 ports
WAN interface	2 x 1G Gigabit Ethernet SFP+ ports
Management Port	10/100 Mbps RJ 45 Management port



8+ 4 =12 Ports [1 Gigabit Base-T (Cu) = 6 ports or higher(as required) | 1 Gs Fiber (SFP) = 4 ports]

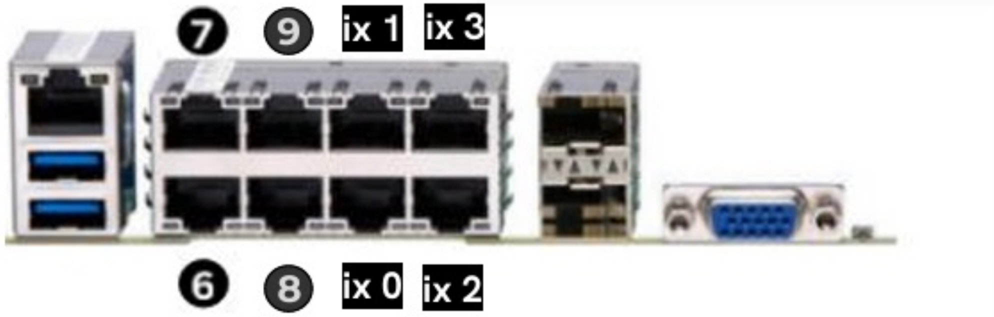
2- Hardware Configuration Setup

Set Steps	Acceptance Criteria
Connect your Internet **Ethernet Cable in the WAN Interface.** Connect your **second ethernet cable in the LAN interface** and remaining tail to your Laptop/Desktop.	The light on the ports should blink. And the Management Console / Web GUI should be accessible by the laptop/desktop. Accessing the Management Console/ Web GUI in mentioned in 2.1.3

Port 0 is usually **igb6** is LAN → 192.168.15.1/24

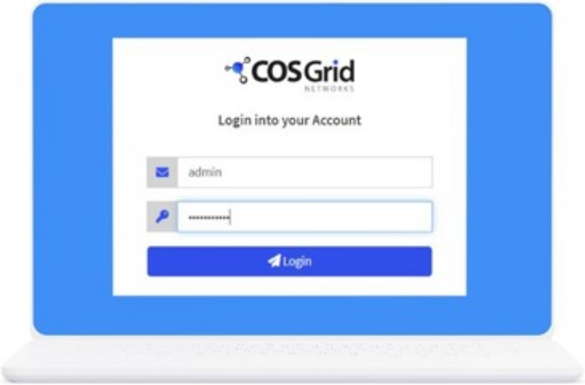
Port 1 is usually **igb7** is WAN

Additional ports available on the device which are left unconfigured, you can assign them later using the web Interface by navigating ***Interface→Assignments.***



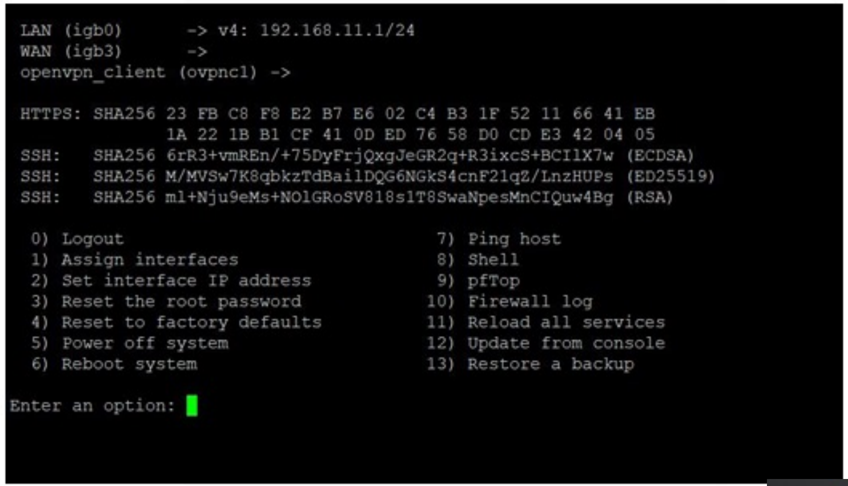
3- Accessing Web GUI / Management Console

Set Steps	Acceptance Criteria
Access the Web GUI in your browser at 192.168.15.1.	It should take you to the COSGrid Next Gen Firewall Web Interface. And the Login option should be displayed.
Access the Management Console using SSH at 192.168.15.1. If the laptop/desktop is linux / macos access it directly. For windows, you can use Putty.	In the console, you should be able to access the firewall. And prompts for login should be displayed.
Login to the GUI / Console with credentials provided by the provider.	You should be able to access the functionality of firewall



Login into your Account

admin

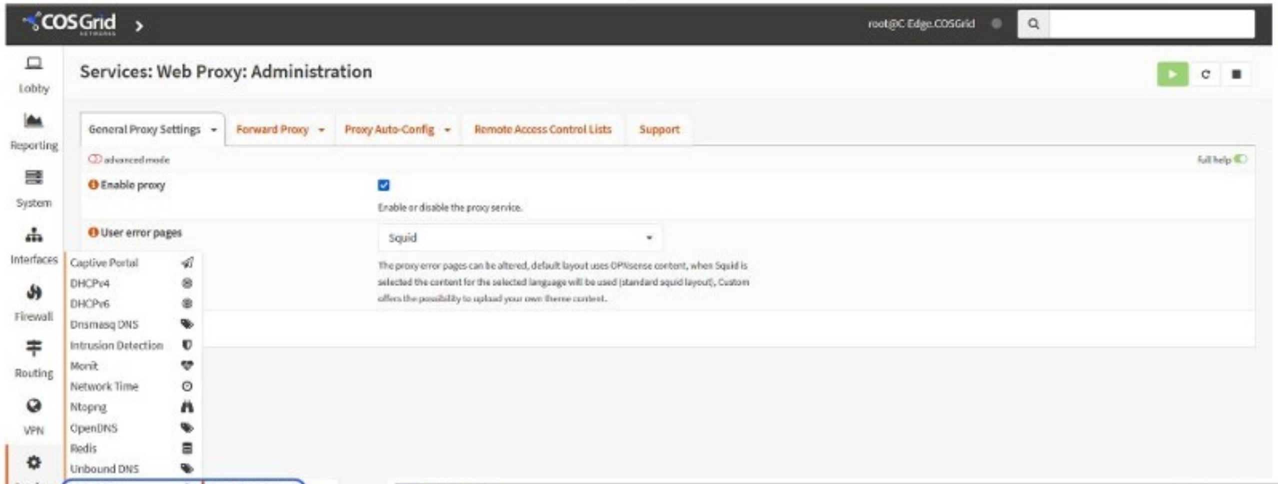


```
LAN (igb0)       -> v4: 192.168.11.1/24
WAN (igb3)       ->
openvpn_client (ovpncl) ->

HTTPS: SHA256 23 FB C8 F8 E2 B7 E6 02 C4 B3 1F 52 11 66 41 EB
              1A 22 1B B1 CF 41 0D ED 76 58 D0 CD E3 42 04 05
SSH:   SHA256 6rR3+vmREn/+75DyFrjQxgJeGR2q+R3ixcS+BCIlX7w (ECDSA)
SSH:   SHA256 M/MVSw7K8qbkzTdBailDQG6NGkS4cnF21qZ/LnzHUPs (ED25519)
SSH:   SHA256 ml+Nju9eMs+NOlGRoSV818s1T8SwaNpesMnCIQuw4Bg (RSA)

 0) Logout                              7) Ping host
 1) Assign interfaces                   8) Shell
 2) Set interface IP address            9) pfTop
 3) Reset the root password            10) Firewall log
 4) Reset to factory defaults          11) Reload all services
 5) Power off system                   12) Update from console
 6) Reboot system                      13) Restore a backup

Enter an option:
```

4- Prerequisite for Web filtering - Firewall rule enablement

Go to ***Services > Web Proxy > Administration > General Proxy Settings .***

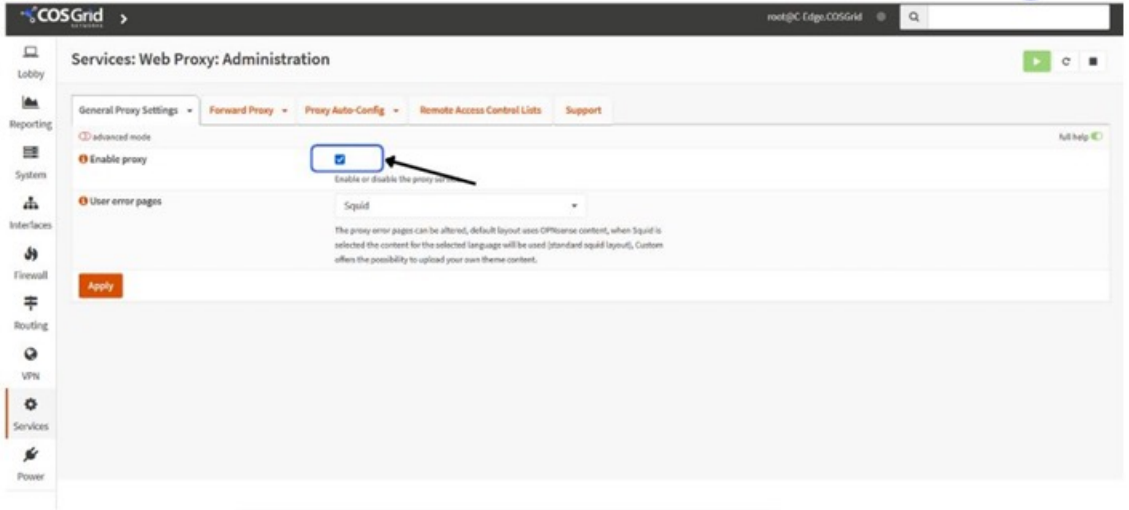
Configure proxy by checked the Enable Proxy Check in Box



1

Services: Web Proxy: Administration

- Enable proxy: ☑ Enable or disable the proxy service.
- User error pages: Squid. The proxy error pages can be altered, default layout uses OPNsense content, when Squid is selected the content for the selected language will be used (standard squid layout), Custom offers the possibility to upload your own theme content.



2

Services: Web Proxy: Administration

- Enable proxy: ☑ Enable or disable the proxy service.
- User error pages: Squid. The proxy error pages can be altered, default layout uses OPNsense content, when Squid is selected the content for the selected language will be used (standard squid layout), Custom offers the possibility to upload your own theme content.

5- Prerequisite for Web filtering - Firewall NAT Rule

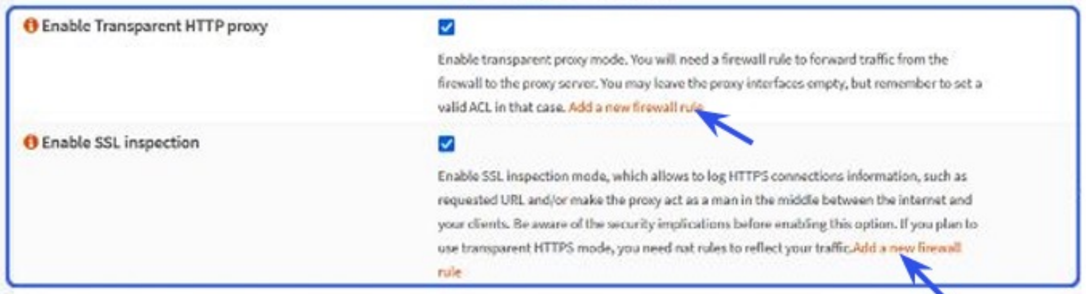
After Enable the Transparent HTTP Proxy & SSL Inspection, You can add the firewall rule for each by clicking Add a new Firewall

Firewall: NAT Port Forward window pops up where you can

- Add firewall rule for Transparent Proxy,
- Add firewall rule for SSL inspection to redirect network Traffic

And Scroll down click **Save** button

5



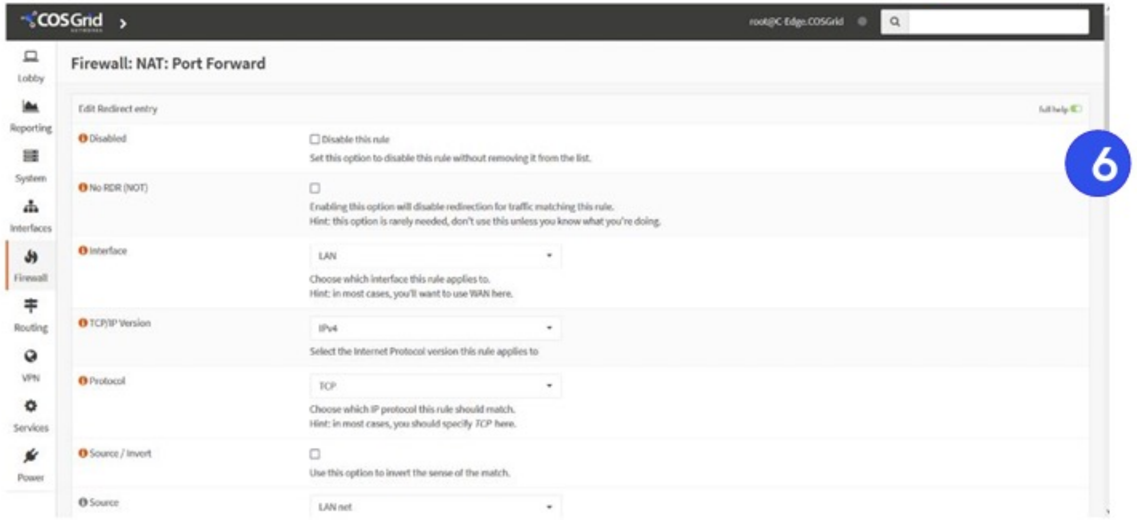
Enable Transparent HTTP proxy ☑

Enable transparent proxy mode. You will need a firewall rule to forward traffic from the firewall to the proxy server. You may leave the proxy interfaces empty, but remember to set a valid ACL in that case. Add a new firewall rule

Enable SSL inspection ☑

Enable SSL inspection mode, which allows to log HTTPS connections information, such as requested URL and/or make the proxy act as a man in the middle between the internet and your clients. Be aware of the security implications before enabling this option. If you plan to use transparent HTTPS mode, you need nat rules to reflect your traffic.Add a new firewall rule

6



Firewall: NAT: Port Forward

Edit Redirect entry

Disabled: ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

No RDR (NOT): ☐
Enabling this option will disable redirection for traffic matching this rule.
Hint: this option is rarely needed, don't use this unless you know what you're doing.

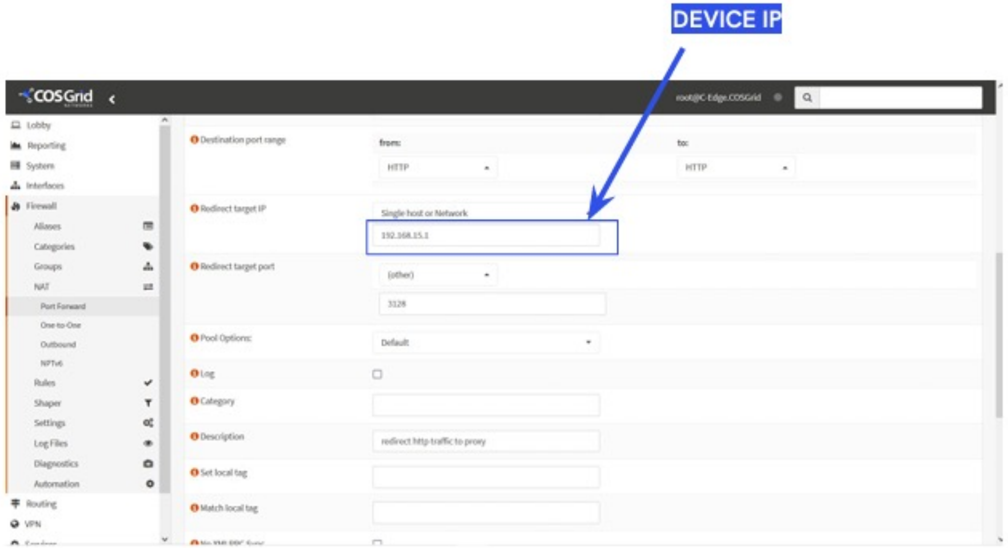
Interface: LAN
Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

TCP/IP Version: IPv4
Select the Internet Protocol version this rule applies to

Protocol: TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify *TCP* here.

Source / Invert: ☐
Use this option to invert the sense of the match.

Source: LAN net



Destination port range: from: HTTP to: HTTP

Redirect target IP: Single host or Network
192.168.15.1

Redirect target port: (other)
3128

Pool Options: Default

Log: ☐

Category:

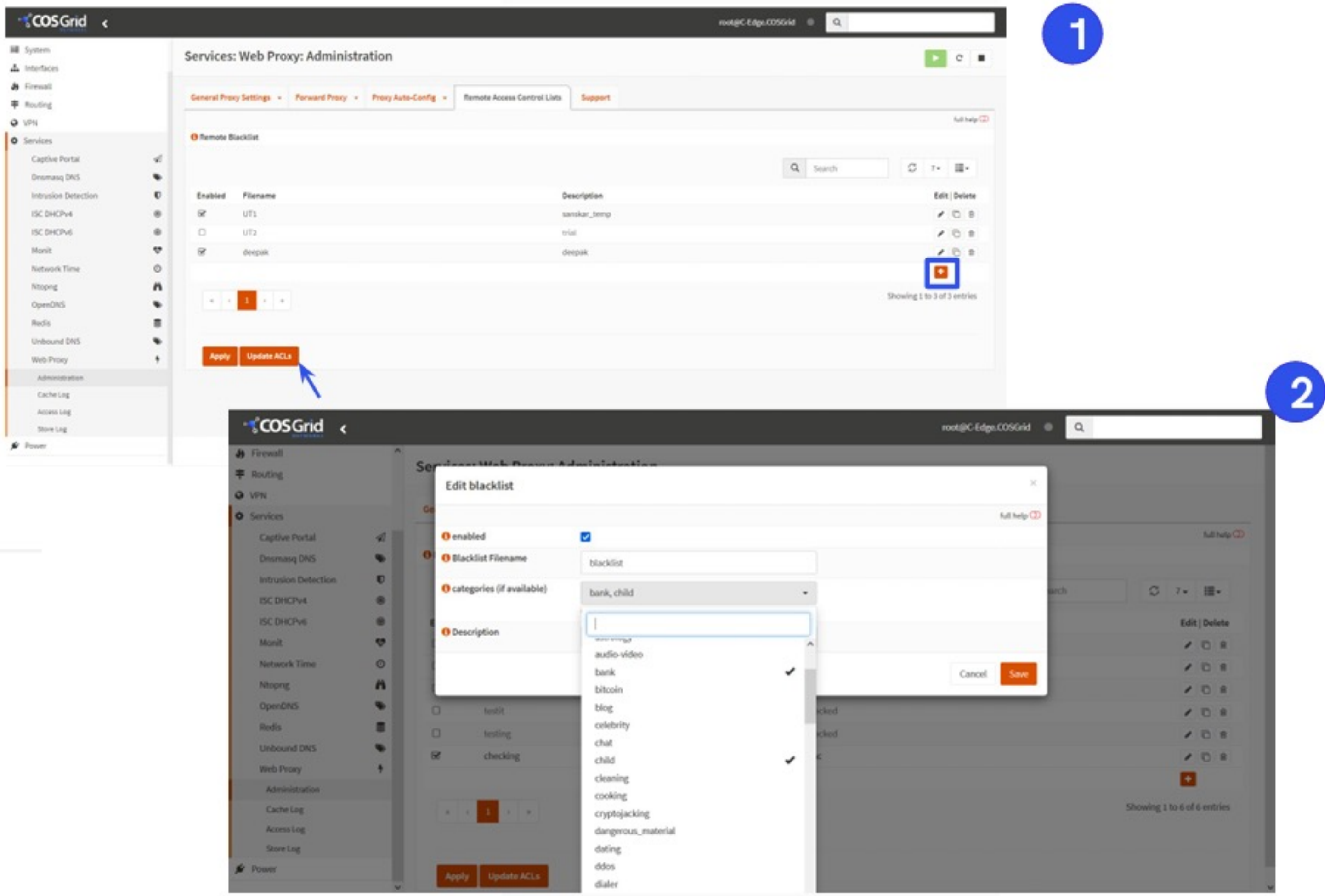
Description: redirect http traffic to proxy

Set local tag:

Match local tag:

6 - Filtering by Category

Set Steps	Acceptance Criteria
Go to *Services > Web Proxy > Administration > Remote Access Control Lists.* Configure filtering rules to block specific categories of websites (e.g., social media, gambling, adult content). Do not forget to press the *Update ACLs button*.	After applying the rule, the loading icon on the button should be invisible. **Note :** *Sometimes the results may get a little more time to get implemented if the selected category is bulky.*
Attempt to access websites belonging to the blocked categories.	Websites in blocked categories should be inaccessible.



1. Services: Web Proxy: Administration

Remote Blacklist

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

Showing 1 to 3 of 3 entries

2. Edit blacklist

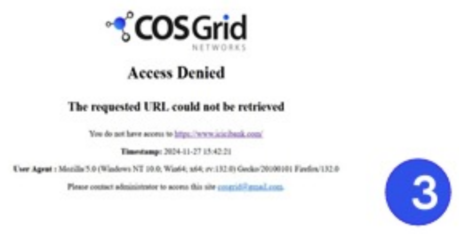
enabled ☑

Blacklist Filename: blacklist

categories (if available): bank, child

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

Description



Access Denied

The requested URL could not be retrieved

You do not have access to https://www.icicibank.com/

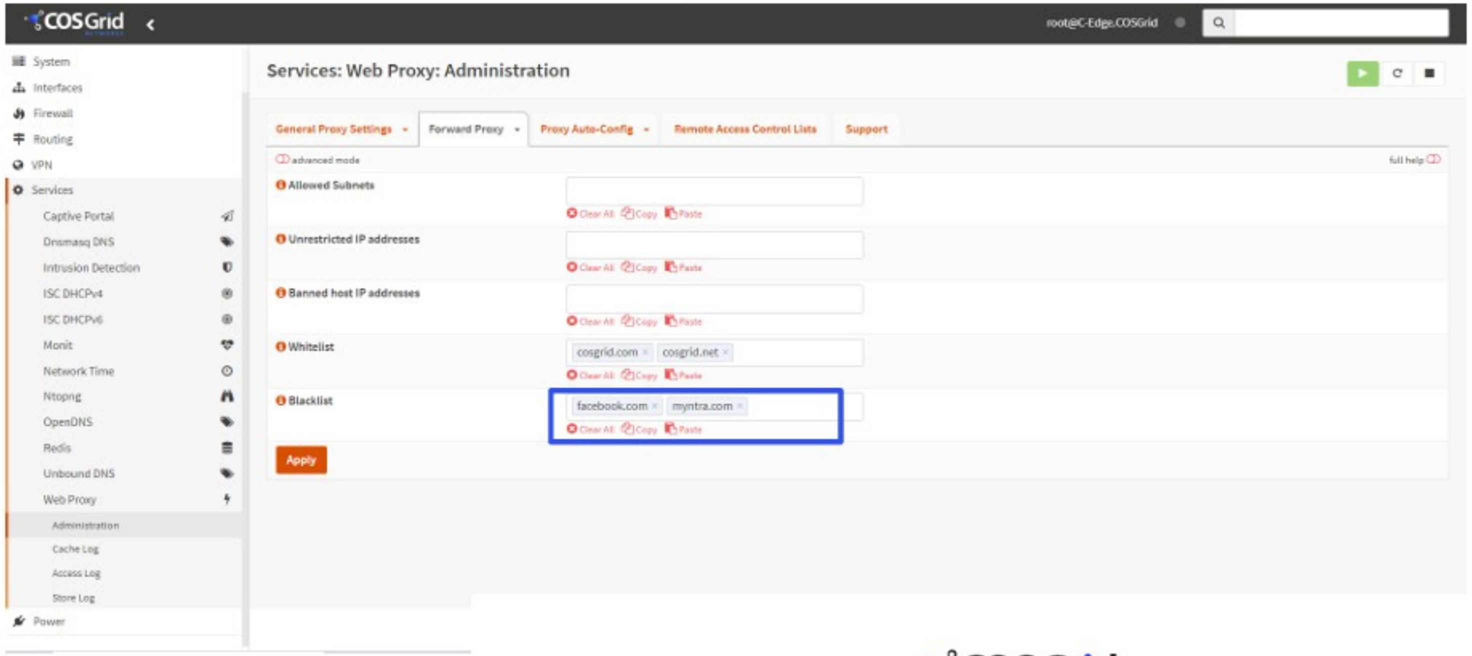
Timestamp: 2024-11-27 15:42:21

User Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0

Please contact administrator to access this site cosgrid@gmail.com.

7- Blocking Access to Restricted Websites

Set Steps	Acceptance Criteria
In Side Bar ***Services > Web Proxy > Administration > Forward Proxy > Access Control List***. Input the **website URL in Blacklist** and click Apply. Now Attempt to access a website in your browser that is explicitly blocked by the filtering rules.Figure:1 Check for a clear and informative message indicating that the website is blocked.	The website should be inaccessible. A clear blocking message should be displayed.



Services: Web Proxy: Administration

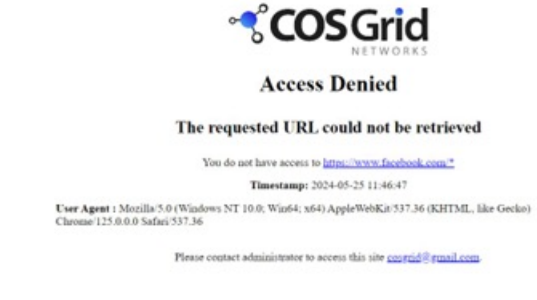
Allowed Subnets

Unrestricted IP addresses

Banned host IP addresses

Whitelist: cosgrid.com × cosgrid.net ×

Blacklist: facebook.com × myntra.com ×



Access Denied

The requested URL could not be retrieved

You do not have access to https://www.facebook.com/*

Timestamp: 2024-05-25 11:46:47

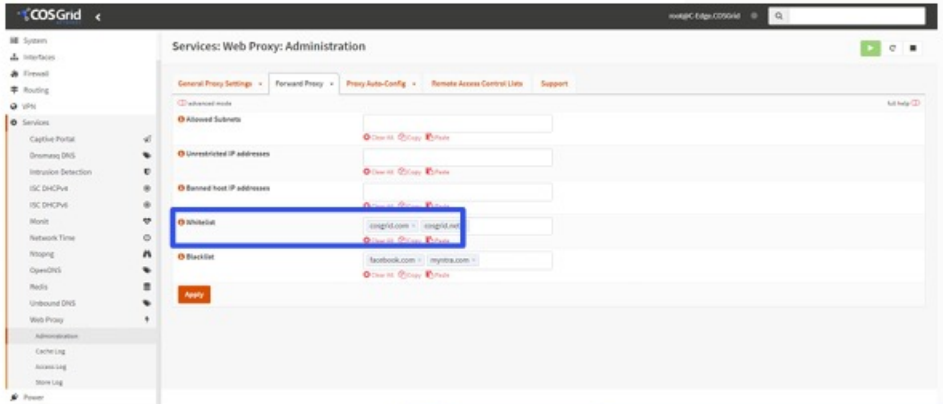
User Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36

Please contact administrator to access this site cosgrid@gmail.com.

COSGrid NETWORKS

8 - Accessing Allowed Websites

Set Steps	Acceptance Criteria
Attempt to access a website in your browser that is not restricted by the filtering rules.	The website should be accessible without any restrictions.
Verify that the website loads and functions as expected.	The website should be rendered properly.
Go to ***Services > Web Proxy > Access Log.*** Check the firewall logs to ensure that the website access is not logged as blocked. Figure:2	The firewall logs should not show any blocked entries for allowed websites



Services: Web Proxy: Administration

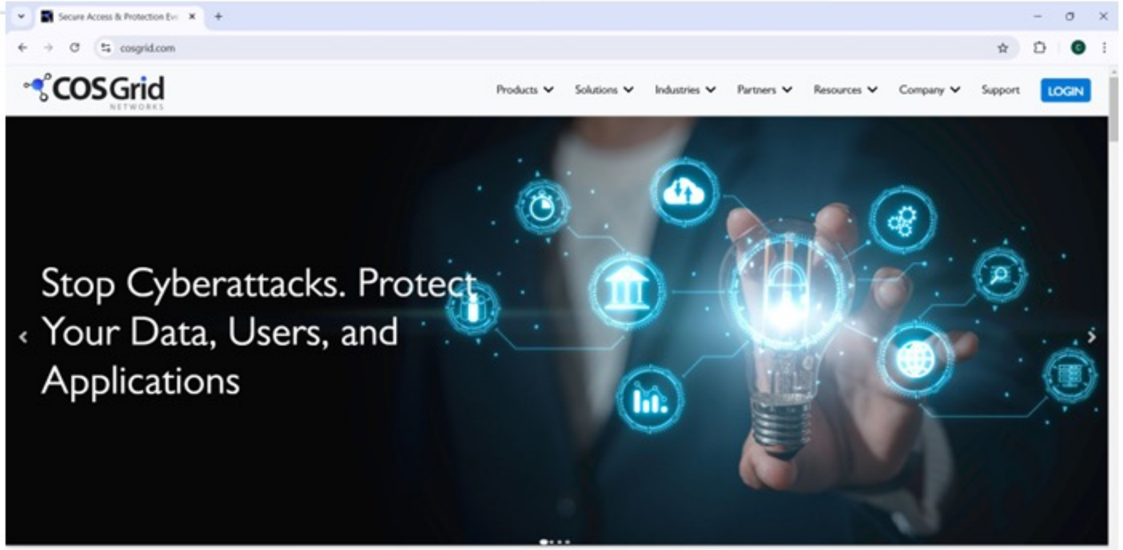
Allowed Subnets:

Unrestricted IP addresses:

Banned host IP addresses:

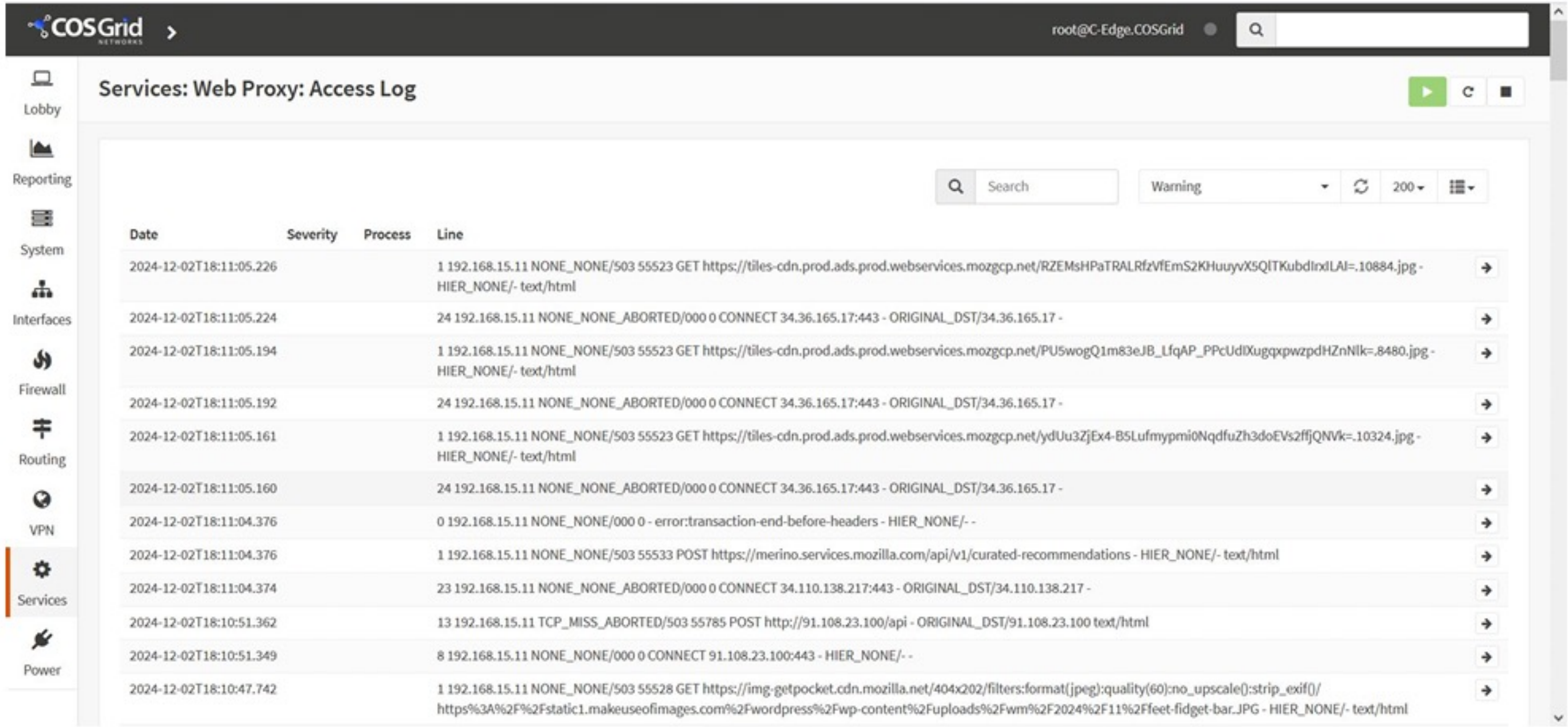
Whitelist: cosgrid.com, cosgrid.net

Blacklist: facebook.com, myntra.com


Secure Access & Protection Ev
cosgrid.com
COSGrid NETWORKS
Products
Solutions
Industries
Partners
Resources
Company
Support
LOGIN
Stop Cyberattacks. Protect Your Data, Users, and Applications

9 - Web Proxy Access Logs

Set Steps	Acceptance Criteria
Attempt to access websites that do not belong to the blocked categories.	Websites not in blocked categories should be accessible.
Go to ***Services > Web Proxy > Access Log***.Check the firewall logs for accurate logging of blocked and allowed traffic.	Firewall logs should accurately reflect blocked and allowed traffic based on categories, Whitelisted & Blacklisted URLs



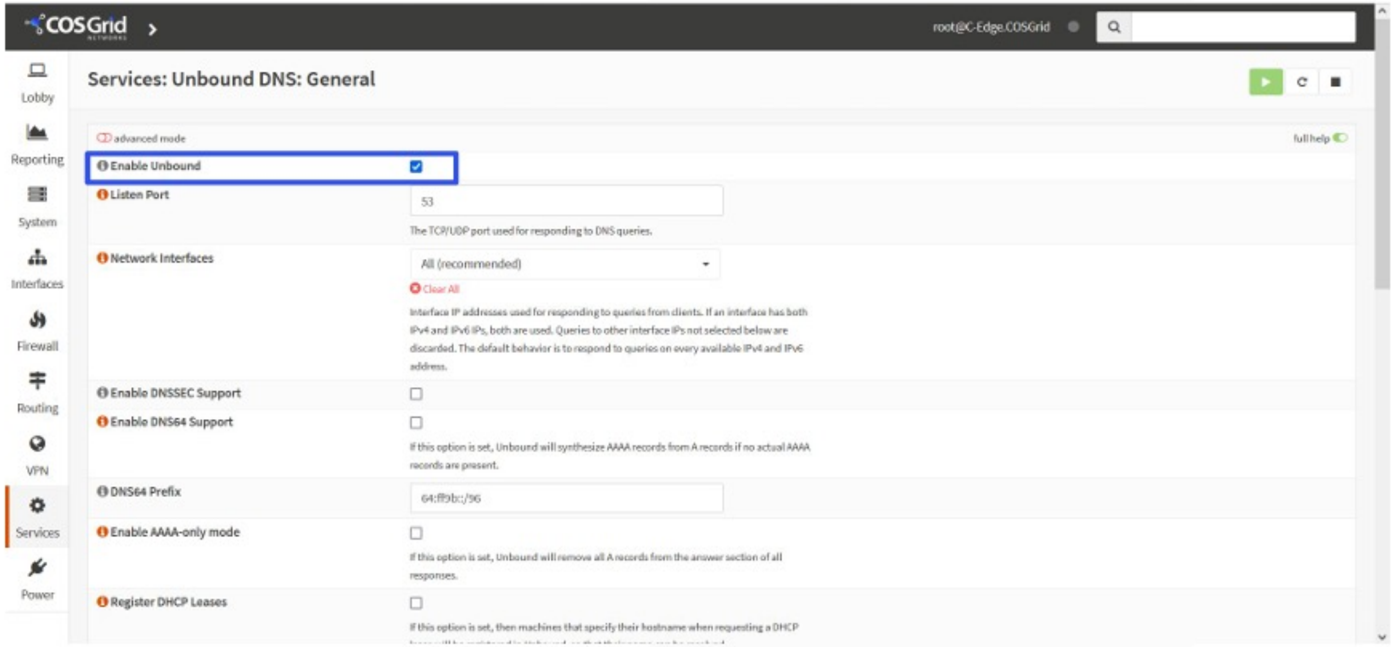
Services: Web Proxy: Access Log

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/RZEMsHPaTRALRfzVfEmS2KHuuyvX5QlTKubdIrxILAI=.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_PPcUdIXugqxpwzpdHZnNlk=.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

10 - Enforce Safe Search

1

Go to ***Services > Unbound DNS > General*** and make sure the "*Enable Unbound*" box is checked.



Services: Unbound DNS: General

Enable Unbound ☑

Listen Port: 53
The TCP/UDP port used for responding to DNS queries.

Network Interfaces: All (recommended)
Clear All
Interface IP addresses used for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

Enable DNSSEC Support ☐

Enable DNS64 Support ☐
If this option is set, Unbound will synthesize AAAA records from A records if no actual AAAA records are present.

DNS64 Prefix: 64:ff9b::/96

Enable AAAA-only mode ☐
If this option is set, Unbound will remove all A records from the answer section of all responses.

Register DHCP Leases ☐
If this option is set, then machines that specify their hostname when requesting a DHCP

10 - Enforce Safe Search

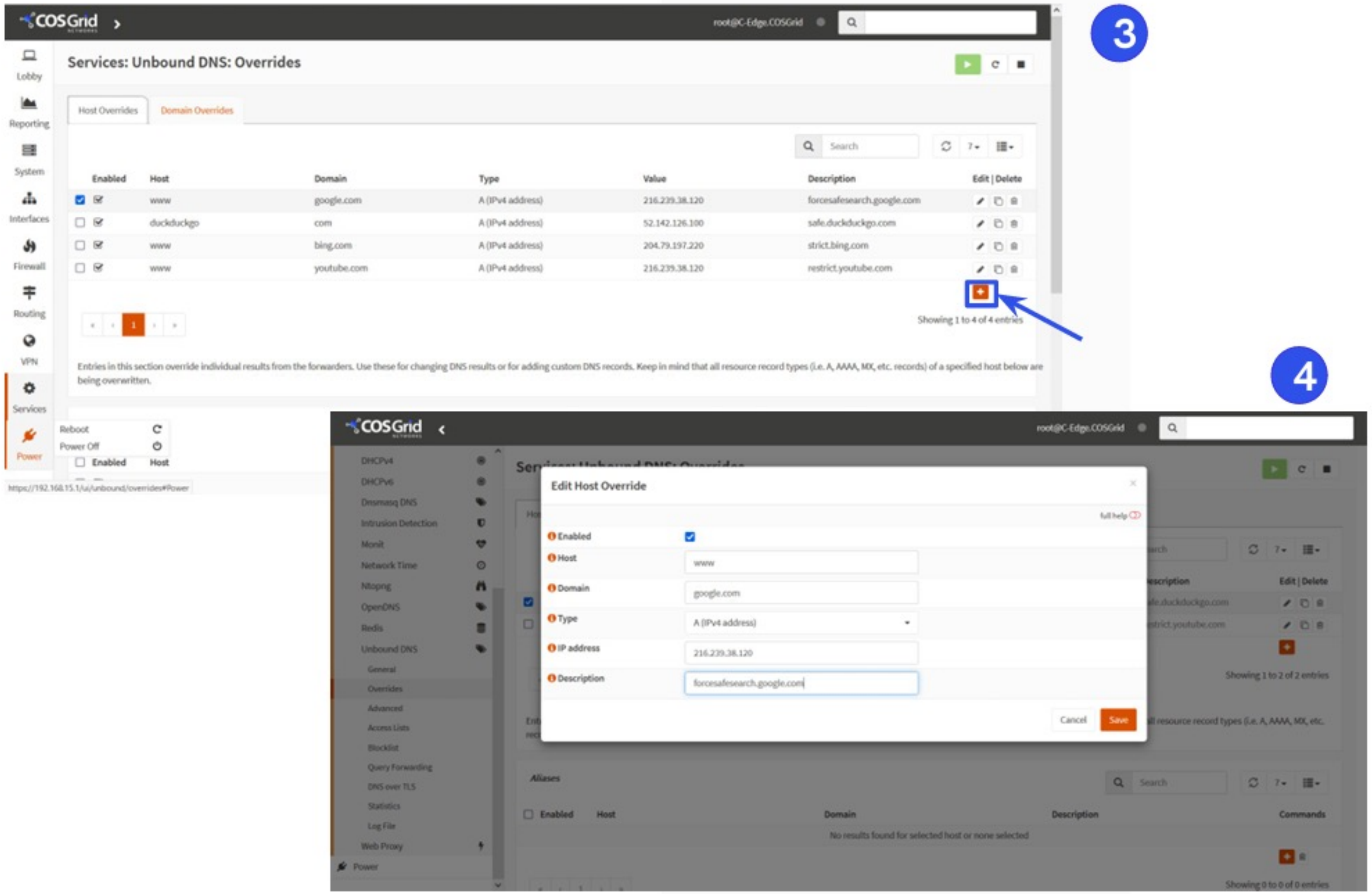
Go to ***Services / Unbound DNS / Overrides*** and create "Host overrides" to put up the moderation

Create a Host override

Example : Google.

Click Add then apply the following settings:

Host = www
Domain = google.com
IP = 216.239.38.120
Description = forcesafesearch.google.com



Services: Unbound DNS: Overrides

Host Overrides | Domain Overrides

	Enabled	Host	Domain	Type	Value	Description	Edit | Delete
☑	☑	www	google.com	A (IPv4 address)	216.239.38.120	forcesafesearch.google.com	
□	☑	duckduckgo	com	A (IPv4 address)	52.142.126.100	safe.duckduckgo.com	
□	☑	www	bing.com	A (IPv4 address)	204.79.197.220	strict.bing.com	
□	☑	www	youtube.com	A (IPv4 address)	216.239.38.120	restrict.youtube.com	

Showing 1 to 4 of 4 entries

Entries in this section override individual results from the forwarders. Use these for changing DNS results or for adding custom DNS records. Keep in mind that all resource record types (i.e. A, AAAA, MX, etc. records) of a specified host below are being overwritten.

https://192.168.15.1/ui/unbound/overrides#Power

Edit Host Override

Enabled	☑
Host	www
Domain	google.com
Type	A (IPv4 address)
IP address	216.239.38.120
Description	forcesafesearch.google.com

Aliases

□ Enabled	Host	Domain	Description	Commands
		No results found for selected host or none selected		

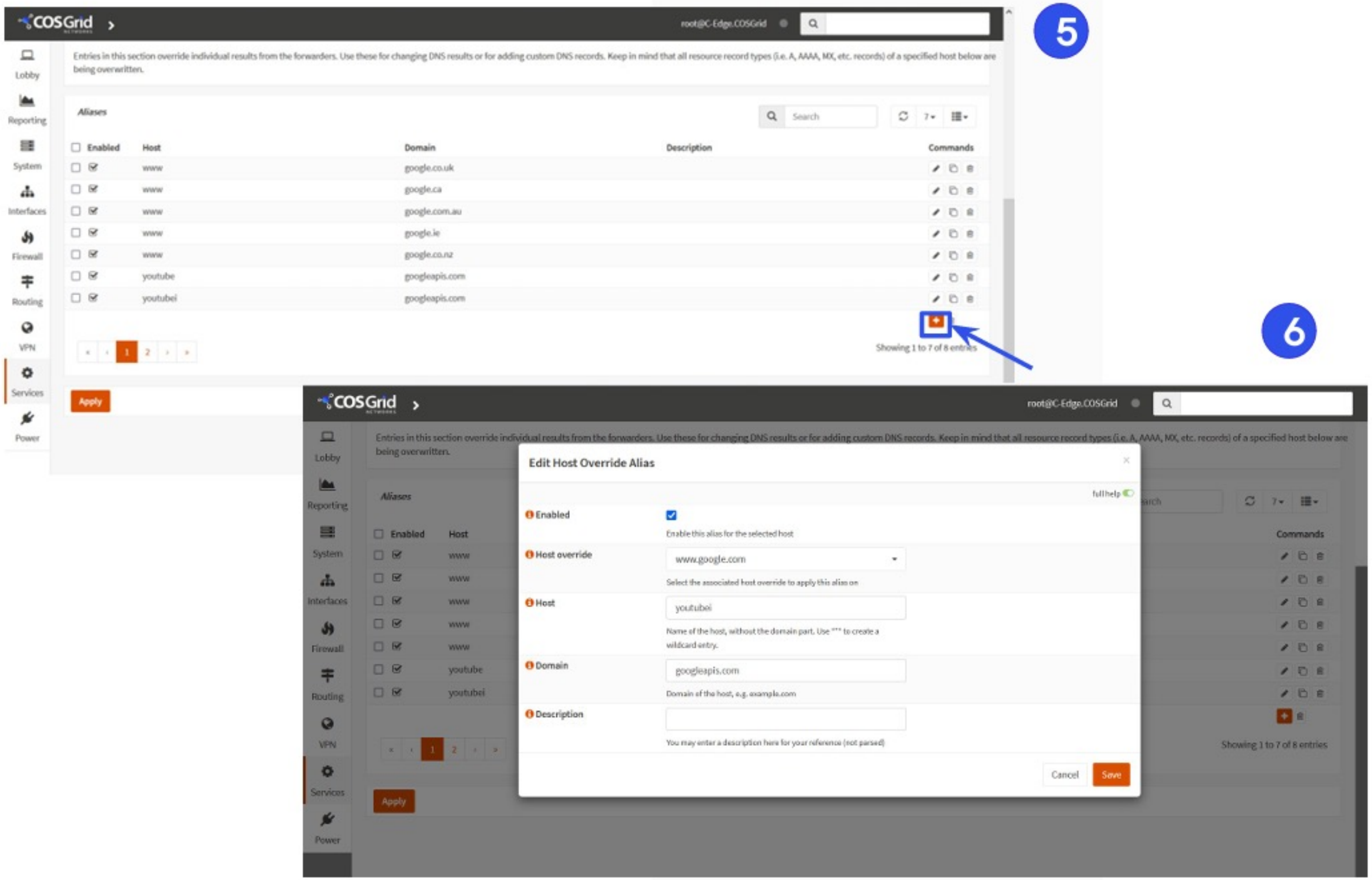
Showing 0 to 0 of 0 entries

10 - Enforce Safe Search

Go to ***Services > Unbound DNS > Overrides*** and create "Host overrides Alias " to put up the

Alias: Host = www / Domain = google.co.uk
Alias: Host = www / Domain = google.ca

Alias: Host = www / Domain = google.com.au
Alias: Host = www / Domain = google.ie
Alias: Host = www / Domain = google.co.nz



Entries in this section override individual results from the forwarders. Use these for changing DNS results or for adding custom DNS records. Keep in mind that all resource record types (i.e. A, AAAA, MX, etc. records) of a specified host below are being overwritten.

Aliases

□	Enabled	Host	Domain	Description	Commands
□	☑	www	google.co.uk		
□	☑	www	google.ca		
□	☑	www	google.com.au		
□	☑	www	google.ie		
□	☑	www	google.co.nz		
□	☑	youtube	googleapis.com		
□	☑	youtubei	googleapis.com		

Showing 1 to 7 of 8 entries

Edit Host Override Alias

full help

Enabled ☑
Enable this alias for the selected host

Host override: www.google.com
Select the associated host override to apply this alias on

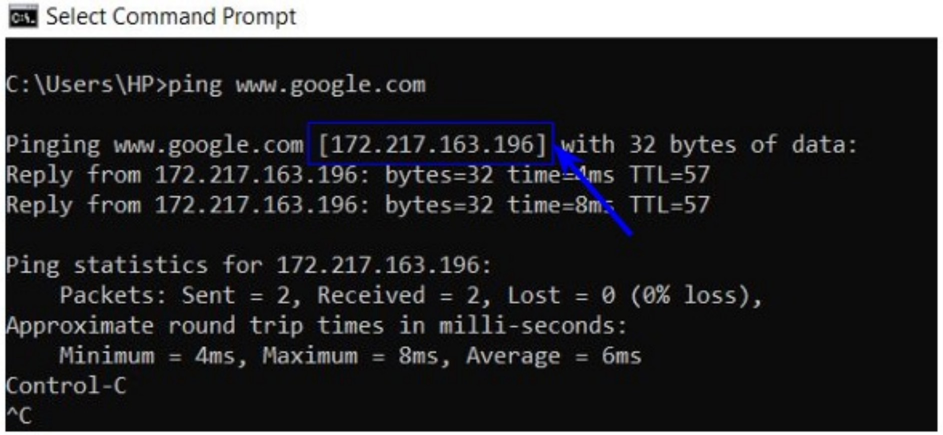
Host: youtubei
Name of the host, without the domain part. Use "*" to create a wildcard entry.

Domain: googleapis.com
Domain of the host, e.g. example.com

Description:
You may enter a description here for your reference (not parsed)

Cancel Save

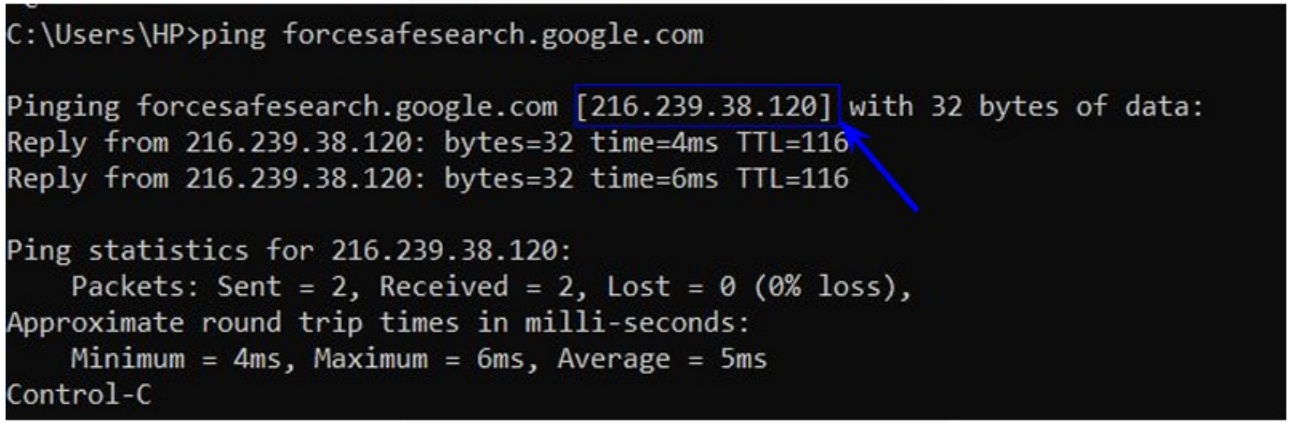
10 - Enforce Safe Search



Select Command Prompt

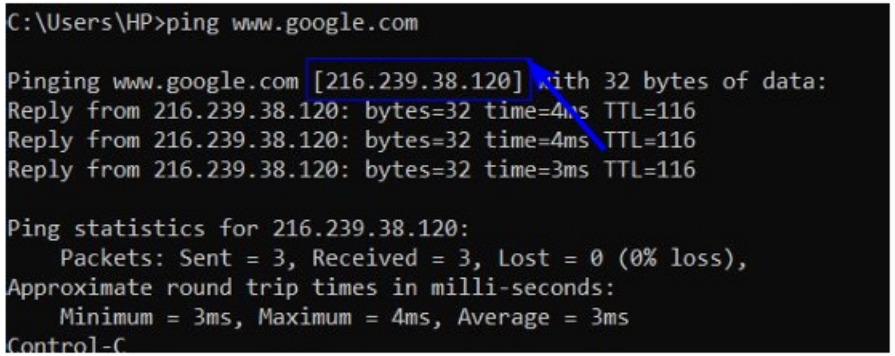
```
C:\Users\HP>ping www.google.com

Pinging www.google.com [172.217.163.196] with 32 bytes of data:
Reply from 172.217.163.196: bytes=32 time=4ms TTL=57
Reply from 172.217.163.196: bytes=32 time=8ms TTL=57

Ping statistics for 172.217.163.196:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 6ms
Control-C
^C
```

Before Enforcing Safe Search



```
C:\Users\HP>ping forcesafesearch.google.com

Pinging forcesafesearch.google.com [216.239.38.120] with 32 bytes of data:
Reply from 216.239.38.120: bytes=32 time=4ms TTL=116
Reply from 216.239.38.120: bytes=32 time=6ms TTL=116

Ping statistics for 216.239.38.120:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 6ms, Average = 5ms
Control-C
```

Before applying Rules - Add this IP in the rules



```
C:\Users\HP>ping www.google.com

Pinging www.google.com [216.239.38.120] with 32 bytes of data:
Reply from 216.239.38.120: bytes=32 time=4ms TTL=116
Reply from 216.239.38.120: bytes=32 time=4ms TTL=116
Reply from 216.239.38.120: bytes=32 time=3ms TTL=116

Ping statistics for 216.239.38.120:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
Control-C
```

After Enforcing Safe Search-
IP Changed

Note* : Same procedure for other search Engines like Bing, Yahoo

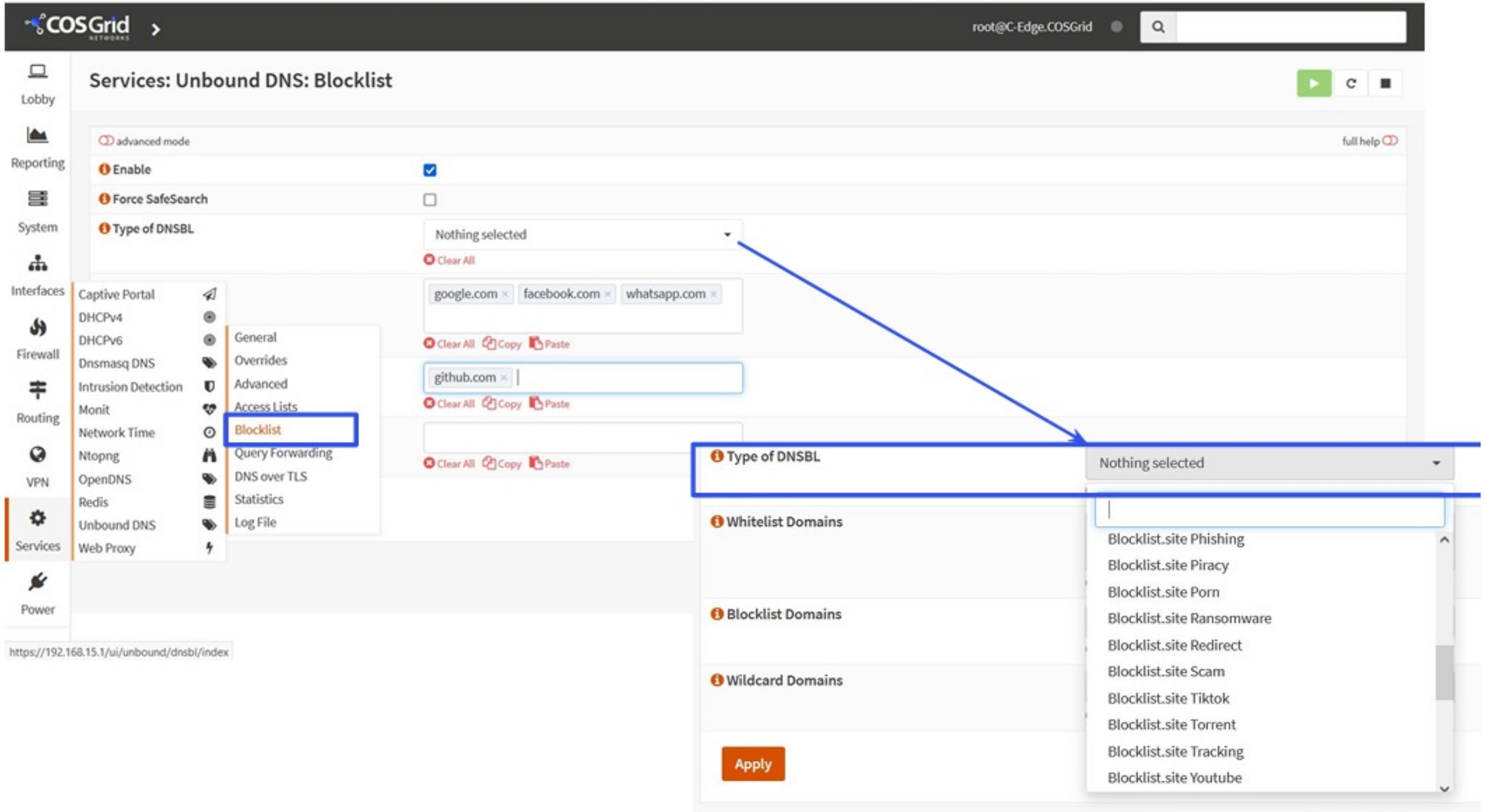
भारत दूरसंचार DOT INDIA TELECOM

COSGrid NETWORKS

11 - Block Access to Cloud Services

Navigate ***Services > Unbound DNS > Blocklist***

Select Type of DNSBL / Cloud Services to block from the Dropdown



Services: Unbound DNS: Blocklist

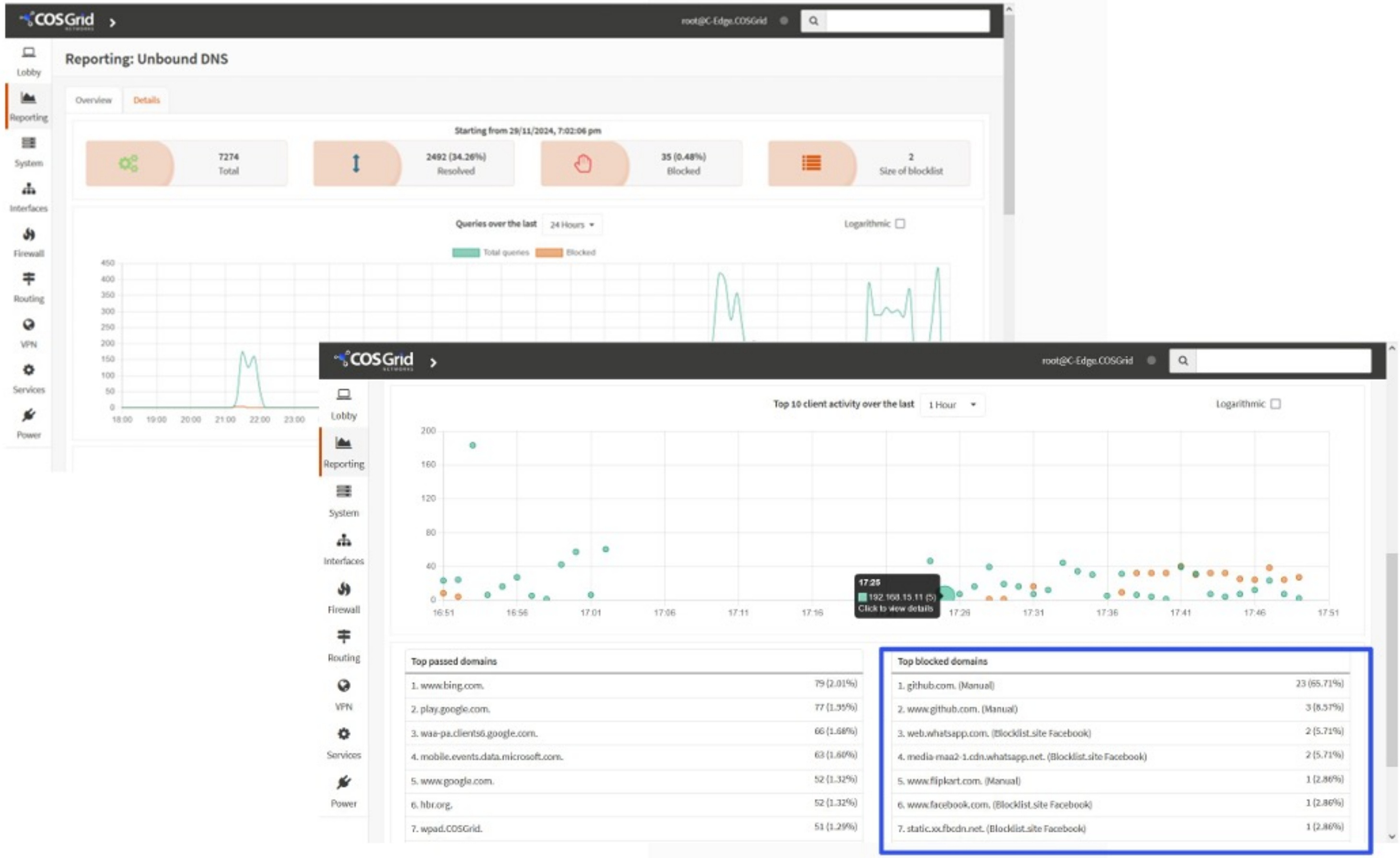
Enable	☑
Force SafeSearch	□
Type of DNSBL	Nothing selected
	google.com × facebook.com × whatsapp.com ×
	github.com ×
Whitelist Domains	
Blocklist Domains	
Wildcard Domains	

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

12 - Detailed Web Access Reports - User, groups & Website

Navigate ***Reporting > Unbound DNS***

Scroll Down to see the detailed Web access reports



Reporting: Unbound DNS

Overview | Details

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

7274 Total

2492 (34.26%) Resolved

35 (0.48%) Blocked

2 Size of blocklist

Queries over the last 24 Hours ▾ Logarithmic □

🟩 Total queries 🟧 Blocked

Top 10 client activity over the last 1 Hour ▾ Logarithmic □

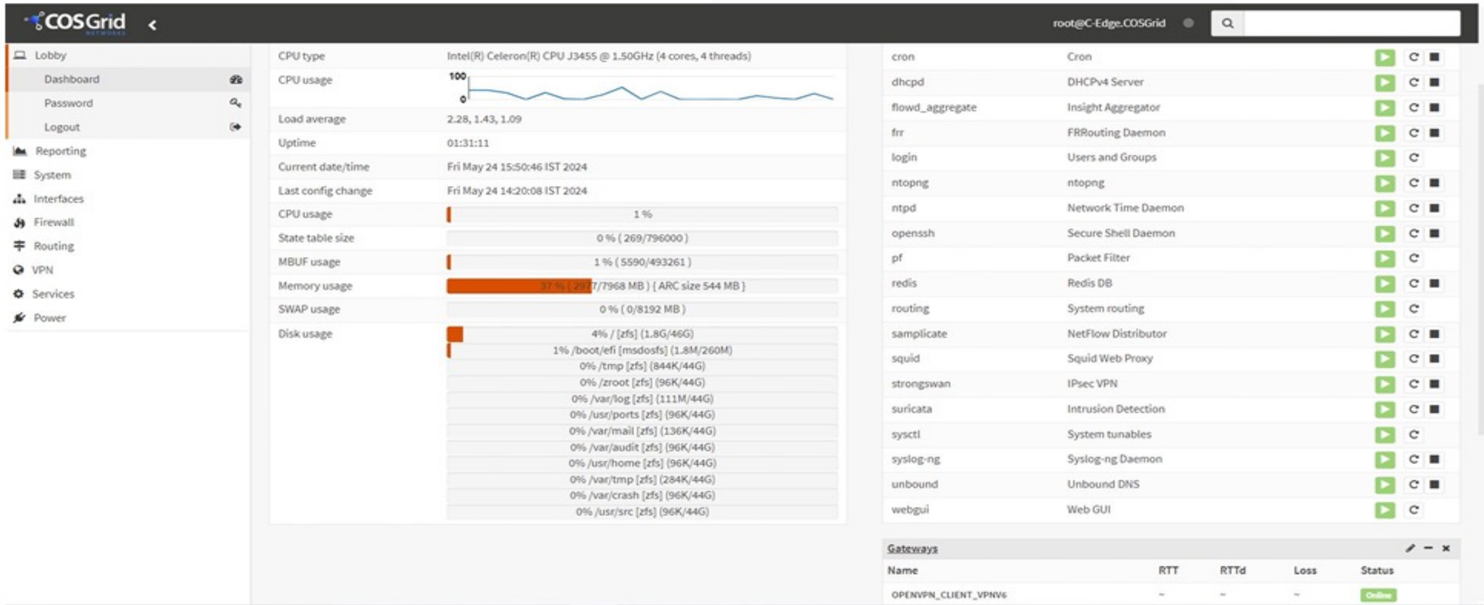
Top passed domains	
1. www.bing.com.	79 (2.01%)
2. play.google.com.	77 (1.95%)
3. waa-pa.clients6.google.com.	66 (1.68%)
4. mobile.events.data.microsoft.com.	63 (1.60%)
5. www.google.com.	52 (1.32%)
6. hbr.org.	52 (1.32%)
7. wpad.COSGrid.	51 (1.29%)

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%)

Research, Design, Develop & Manufacturing in India

13 - Performance & Stability

Set Steps	Acceptance Criteria
Simulate heavy web traffic with a mix of blocked and allowed websites.	The firewall should **maintain stable performance** and **responsiveness under load.**
Go to ***Lobby > Dashboard.*** Monitor the firewall's performance and resource usage during filtering.	There should be **no significant impact on overall network performance due to web filtering.**



CPU type	Intel(R) Celeron(R) CPU J3455 @ 1.50GHz (4 cores, 4 threads)
CPU usage	
Load average	2.28, 1.43, 1.09
Uptime	01:31:11
Current date/time	Fri May 24 15:50:46 IST 2024
Last config change	Fri May 24 14:20:08 IST 2024
CPU usage	1 %
State table size	0 % (269/796000)
MBUF usage	1 % (5590/493261)
Memory usage	37 % (2977/7968 MB) { ARC size 544 MB }
SWAP usage	0 % (0/8192 MB)
Disk usage	4% / [zfs] (1.8G/46G) 1% /boot/efi [msdosfs] (1.8M/260M) 0% /tmp [zfs] (844K/44G) 0% /zroot [zfs] (96K/44G) 0% /var/log [zfs] (111M/44G) 0% /usr/ports [zfs] (96K/44G) 0% /var/mail [zfs] (136K/44G) 0% /var/audit [zfs] (96K/44G) 0% /usr/home [zfs] (96K/44G) 0% /var/tmp [zfs] (284K/44G) 0% /var/crash [zfs] (96K/44G) 0% /usr/src [zfs] (96K/44G)

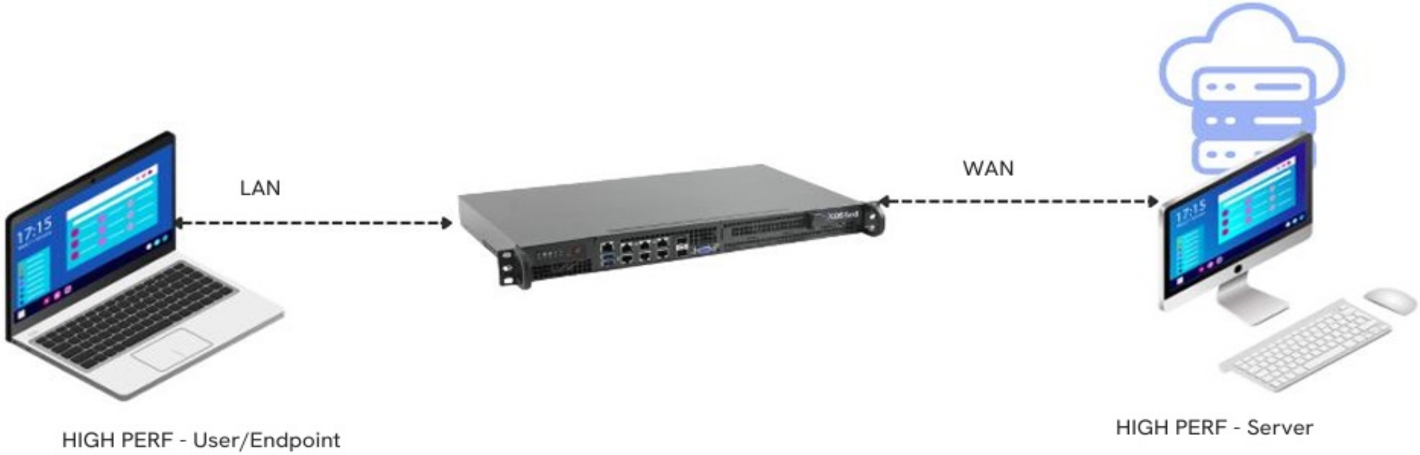
cron	Cron
dhcpd	DHCPv4 Server
flowd_aggregate	Insight Aggregator
frr	FRRouting Daemon
login	Users and Groups
ntopng	ntopng
ntpd	Network Time Daemon
openssh	Secure Shell Daemon
pf	Packet Filter
redis	Redis DB
routing	System routing
samplicate	NetFlow Distributor
squid	Squid Web Proxy
strongswan	IPsec VPN
suricata	Intrusion Detection
sysctl	System tunables
syslog-ng	Syslog-ng Daemon
unbound	Unbound DNS
webgui	Web GUI

Gateways

Name	RTT	RTTd	Loss	Status
OPENVPN_CLIENT_VPNV6	~	~	~	Online

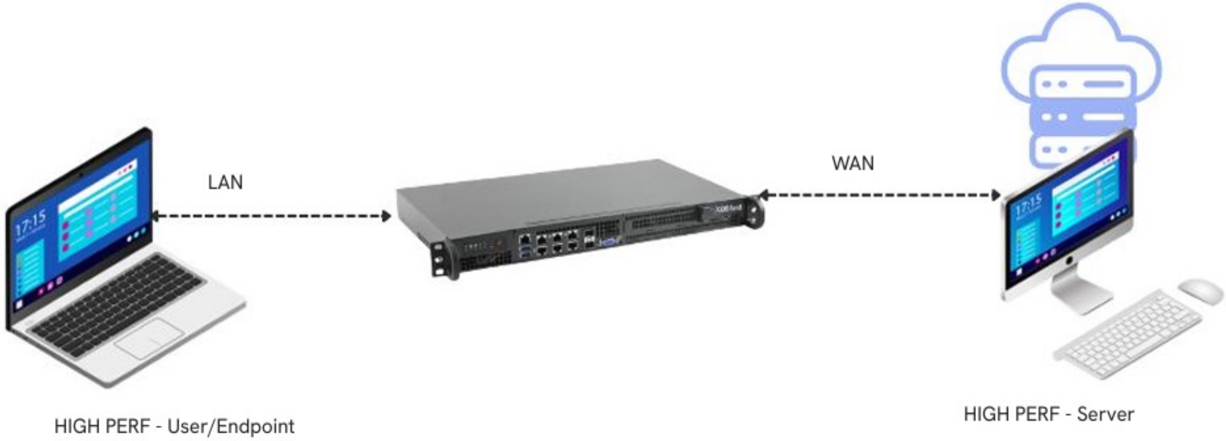
14 - Performance - Baseline Throughput

Set Steps	Acceptance Criteria
Establish a baseline for network throughput without the COSGrid Firewall activated. Use standard benchmarking tools like iPerf3 **or** SpeedTest to measure network speed in both directions (upload and download). Repeat the measurements at different times of the day to account for network fluctuations.	Record the baseline throughput values for **upload and download** speeds. Note the speed test data using different softwares.



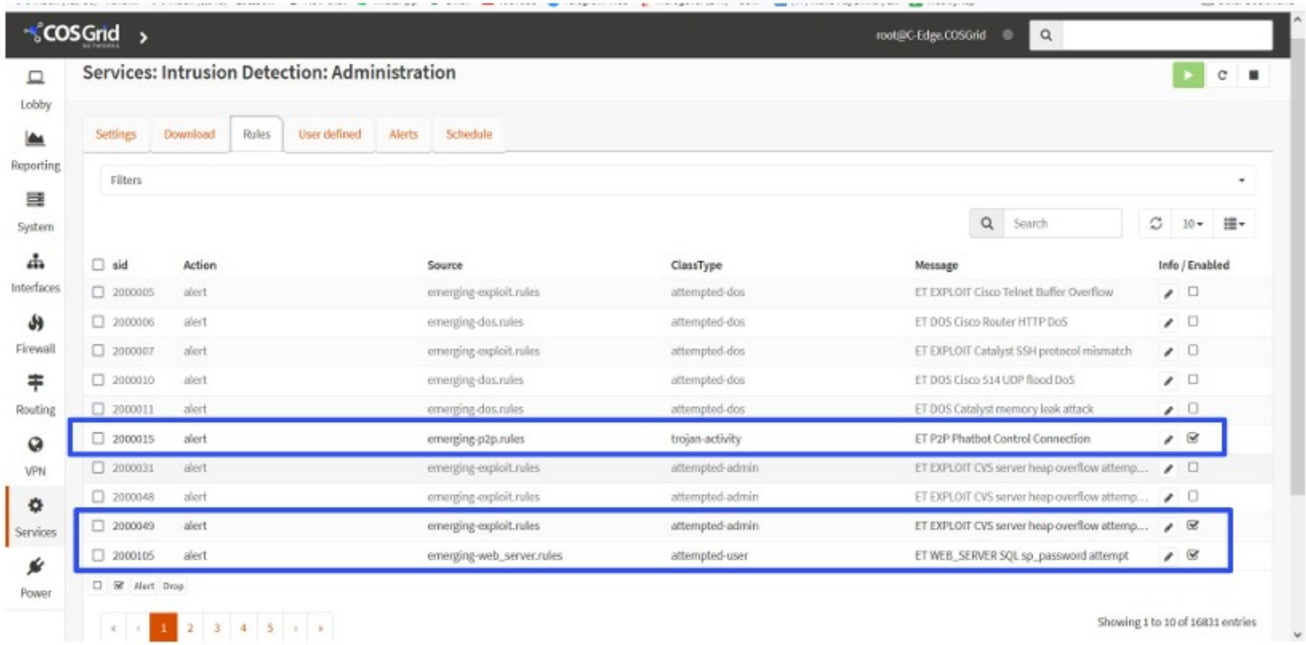
15 - Performance - NG Firewall Throughput

Set Steps	Acceptance Criteria
Activate the COSGrid Firewall with relevant security policies configured.	The network throughput with the COSGrid Firewall should not be significantly **lower than the baseline** values (ideally within a pre-defined acceptable range, e.g., 5-10% decrease).
Repeat the throughput measurements using the same benchmarking tools and methodology as in Case 1 (iPerf3 or SpeedTest).	Throughput degradation should not impact user experience in terms of application responsiveness, file transfers, or overall network performance.
Compare the obtained throughput values with the baseline measurements.	Firewall Throughput - 1Gbps



16 - Performance - Threat Protection

Set Steps	Acceptance Criteria
Navigate ***Services > Intrusion Detection > Rules*** Enable the rules. Test the Performance of Firewall Threat Protection as like NG Firewall Throughput	Threat Protection - 500 Mbps



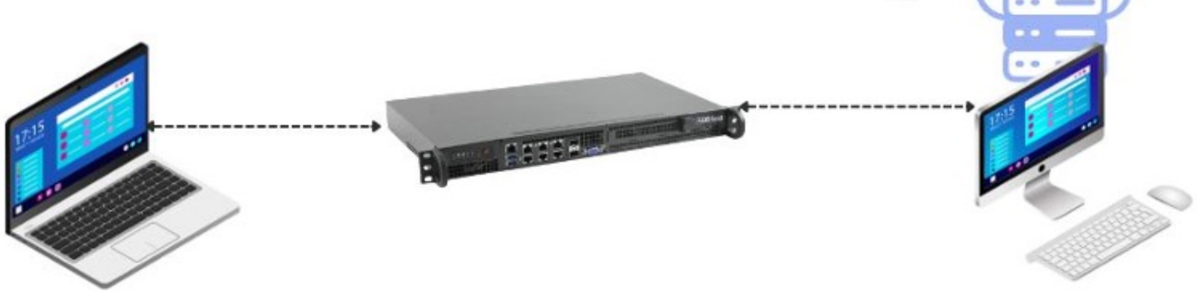
Services: Intrusion Detection: Administration

sid	Action	Source	ClassType	Message	Info / Enabled
□ 2000005	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT Cisco Telnet Buffer Overflow	□
□ 2000006	alert	emerging-dos.rules	attempted-dos	ET DOS Cisco Router HTTP DoS	□
□ 2000007	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT Catalyst SSH protocol mismatch	□
□ 2000010	alert	emerging-dos.rules	attempted-dos	ET DOS Cisco 514 UDP flood DoS	□
□ 2000011	alert	emerging-dos.rules	attempted-dos	ET DOS Catalyst memory leak attack	□
□ 2000015	alert	emerging-p2p.rules	trojan-activity	ET P2P Phatbot Control Connection	☑
□ 2000031	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT CVS server heap overflow attemp...	□
□ 2000048	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT CVS server heap overflow attemp...	□
□ 2000049	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT CVS server heap overflow attemp...	☑
□ 2000105	alert	emerging-web_server.rules	attempted-user	ET WEB_SERVER SQL sp_password attempt	☑

□ ☑ Alert Drop

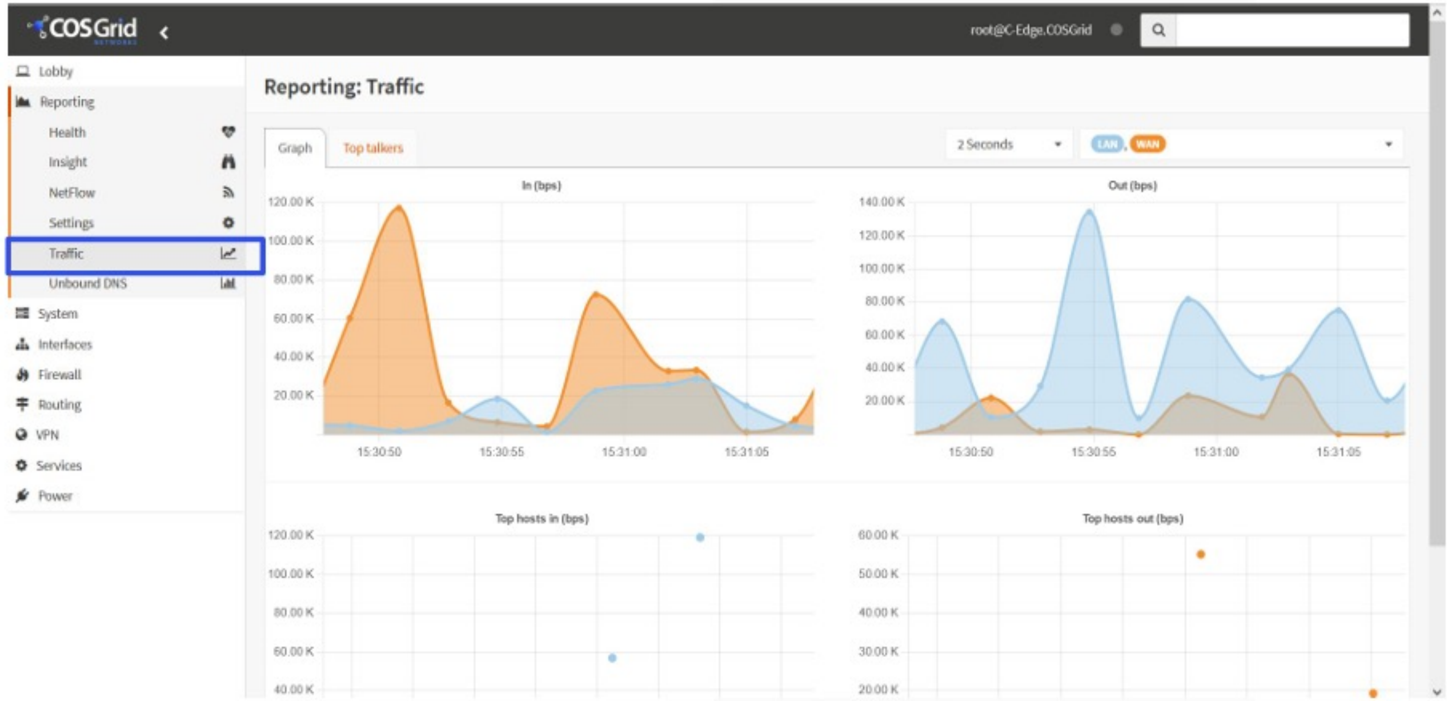
« ‹ 1 2 3 4 5 › »

Showing 1 to 10 of 16831 entries



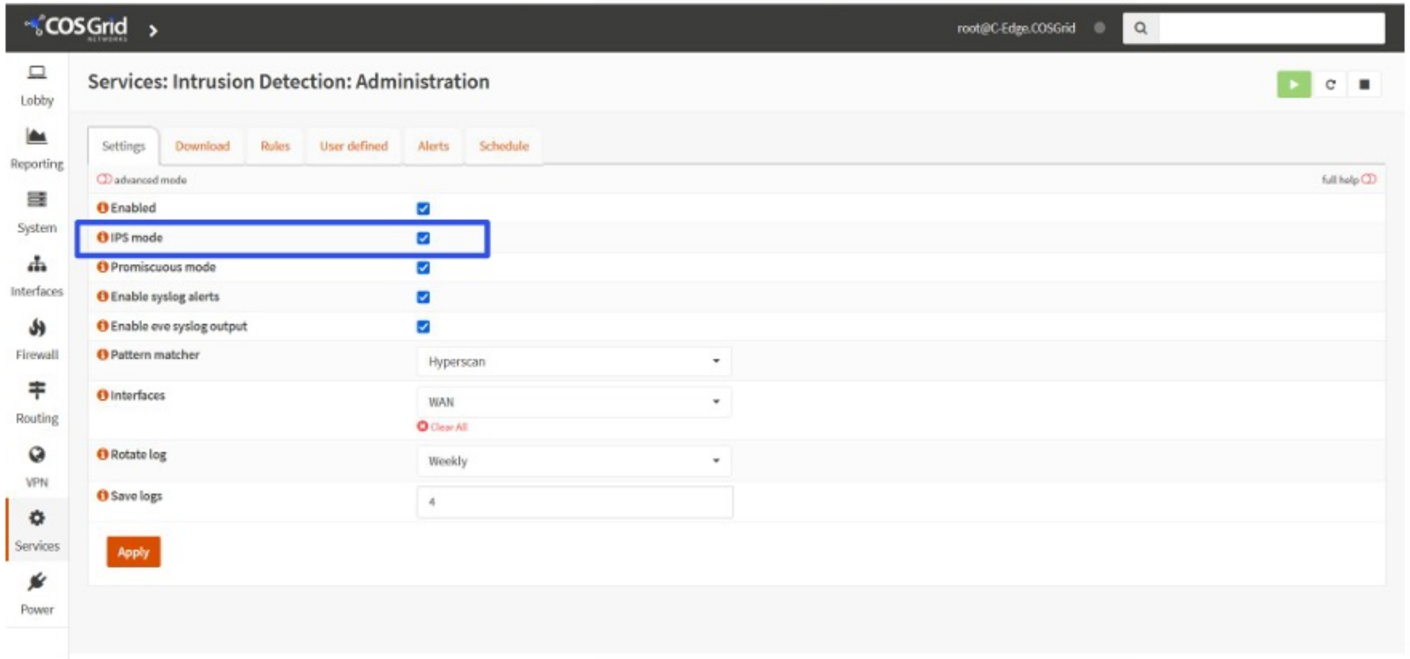
17 - Application Specific Throughput

Set Steps	Acceptance Criteria
Identify critical applications or services heavily reliant on network performance. Go to ***Reporting > Traffic.*** Measure the throughput experienced by these applications with and without the COSGrid Firewall active.	COSGrid Firewall should not significantly impact the performance of critical applications. **Latency and responsiveness** should remain within acceptable ranges for optimal user experience.



18 - Preventing Intrusion Attempts

Set Steps	Acceptance Criteria
Go to ***Services > Intrusion Detection > Administration.*** Enable the **IPS**. Simulate common intrusion techniques, such as port scanning, vulnerability scanning, and password cracking.	The firewall should detect and block **intrusion attempts**.

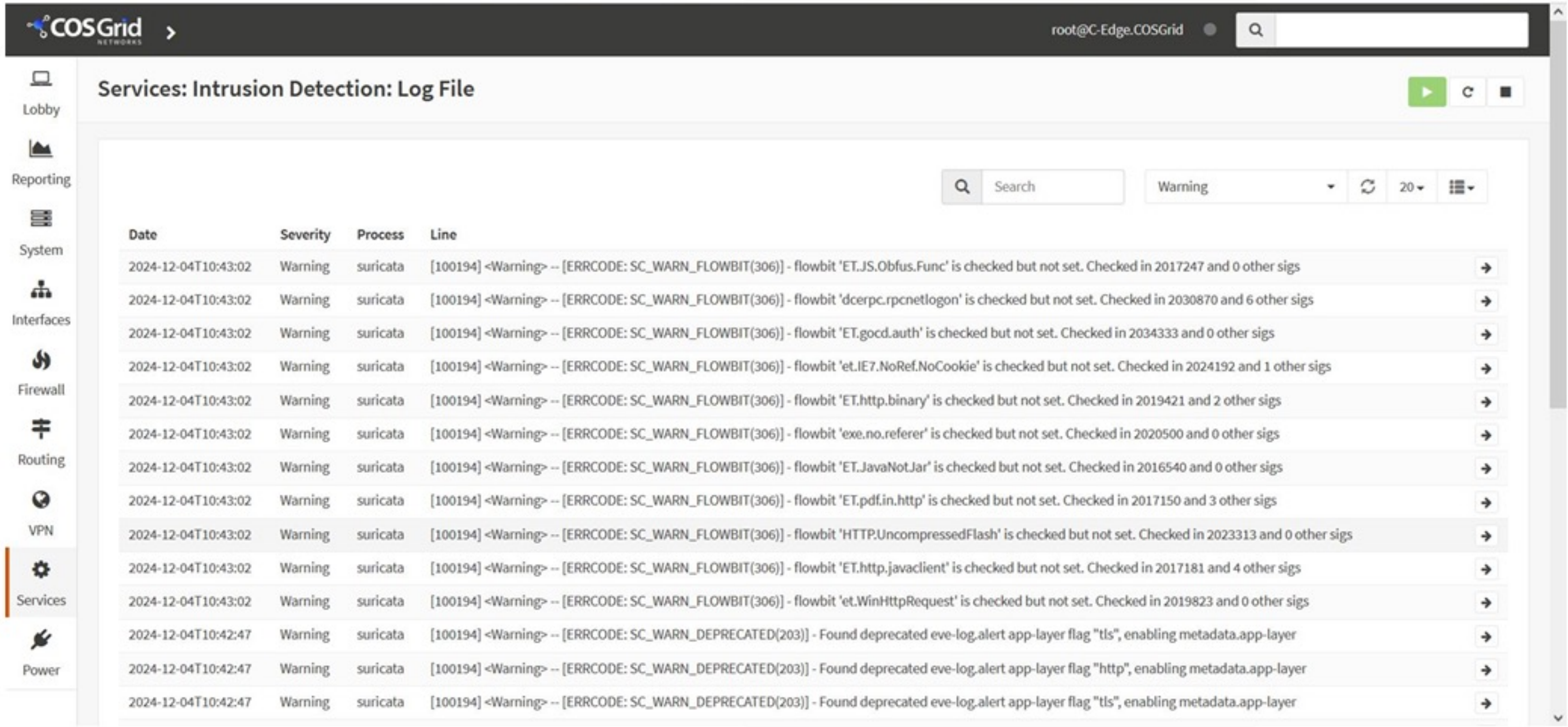


Services: Intrusion Detection: Administration

- Enabled ☑
- IPS mode ☑
- Promiscuous mode ☑
- Enable syslog alerts ☑
- Enable eve syslog output ☑
- Pattern matcher: Hyperscan
- Interfaces: WAN
- Rotate log: Weekly
- Save logs: 4

18 - Preventing Intrusion Attempts - Log Files

Set Steps	Acceptance Criteria
Use tools like Nmap, Nessus, and Metasploit. Go to ***Services > Intrusion Detection > Log File***. Monitor the firewall's response and logging.	It should generate alerts or notifications for security events. Logs should provide detailed information about the intrusion attempts and actions taken by the firewall.



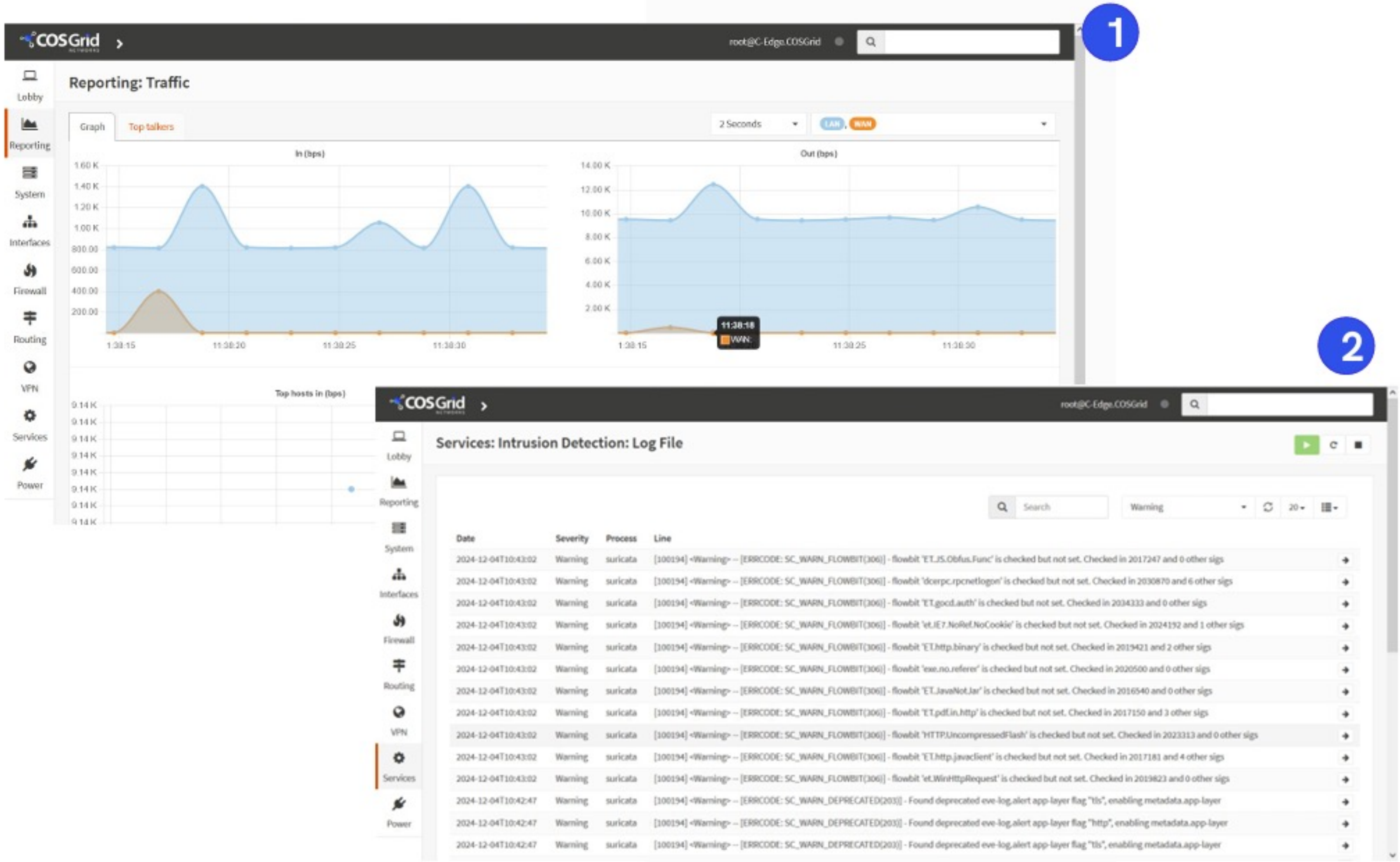
Services: Intrusion Detection: Log File

Date	Severity	Process	Line
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.JS.Obfus.Func' is checked but not set. Checked in 2017247 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'dcerpc.rpcnetlogon' is checked but not set. Checked in 2030870 and 6 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.gocd.auth' is checked but not set. Checked in 2034333 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'et.IE7.NoRef.NoCookie' is checked but not set. Checked in 2024192 and 1 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.http.binary' is checked but not set. Checked in 2019421 and 2 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'exe.no.referer' is checked but not set. Checked in 2020500 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.JavaNotJar' is checked but not set. Checked in 2016540 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.pdf.in.http' is checked but not set. Checked in 2017150 and 3 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'HTTP.UncompressedFlash' is checked but not set. Checked in 2023313 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.http.javaclient' is checked but not set. Checked in 2017181 and 4 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'et.WinHttpRequest' is checked but not set. Checked in 2019823 and 0 other sigs
2024-12-04T10:42:47	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_DEPRECATED(203)] - Found deprecated eve-log.alert app-layer flag "tls", enabling metadata.app-layer
2024-12-04T10:42:47	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_DEPRECATED(203)] - Found deprecated eve-log.alert app-layer flag "http", enabling metadata.app-layer
2024-12-04T10:42:47	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_DEPRECATED(203)] - Found deprecated eve-log.alert app-layer flag "tls", enabling metadata.app-layer

COSGrid NETWORKS

19 - DDoS Attack Prevention

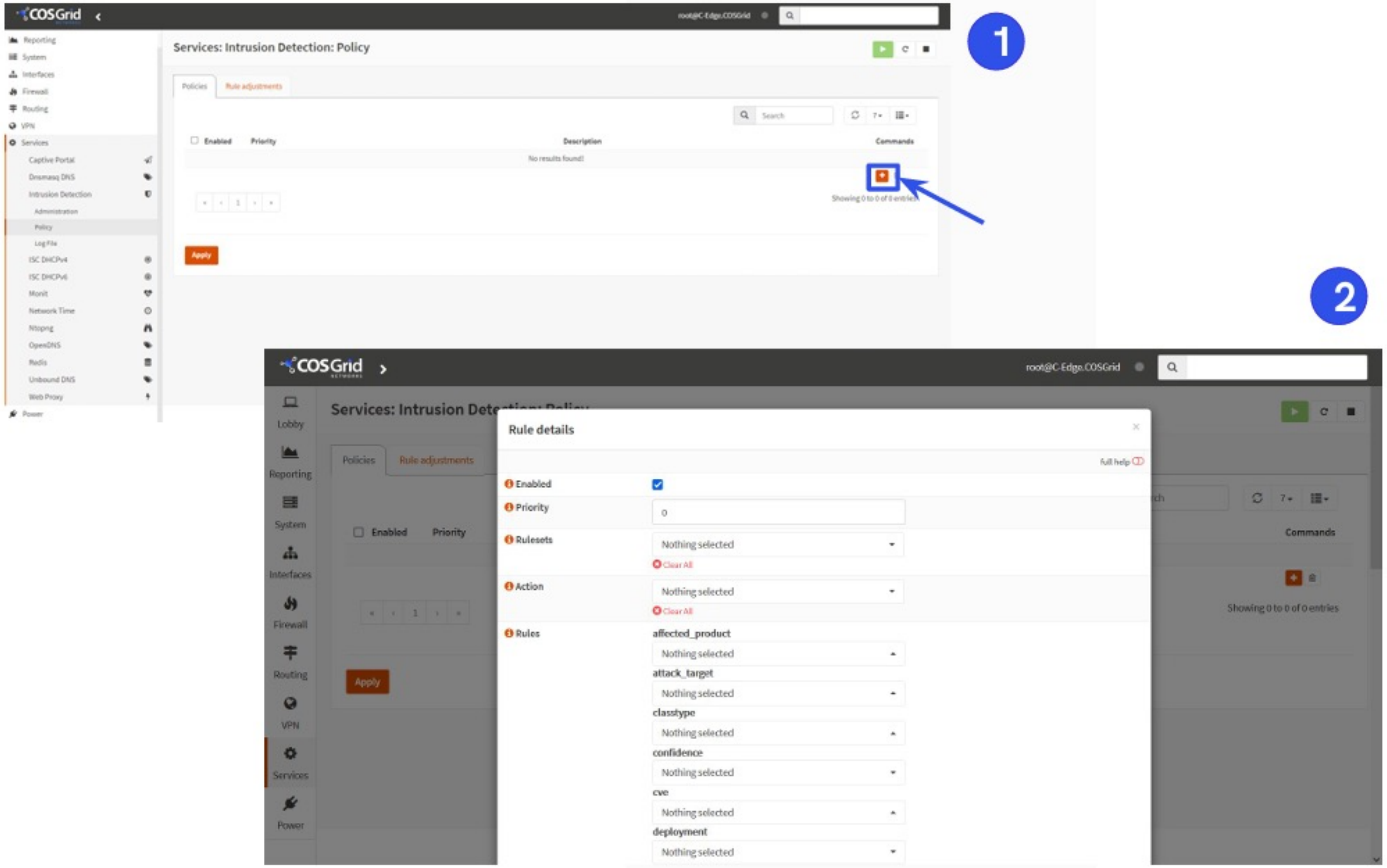
Set Steps	Acceptance Criteria
Generate a high volume of traffic (e.g., **UDP, ICMP, SYN** floods) to simulate a volumetric attack.	Detects and blocks network borne attacks. Discussed in the third step .
Go to ***Reporting > Traffic.*** Monitor firewall's response, including traffic analysis, rate limiting, and traffic shaping.	There should be **high traffic flow** in the graphs.
Go to ***Services > Intrusion Detection > Log File.*** Monitor firewall's detection and response mechanisms, such as protocol-specific filtering and anomaly detection. Verify that the firewall effectively blocks or mitigates the attack.	There should be **alert logs in the file** that should contain the information about the specific protocol.



Date	Severity	Process	Line
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.JS.Obfus.Func' is checked but not set. Checked in 2017247 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'dcerpc.rpcnetlogon' is checked but not set. Checked in 2030870 and 6 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.gocd.auth' is checked but not set. Checked in 2034333 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'et.IE7.NoRef.NoCookie' is checked but not set. Checked in 2024192 and 1 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.http.binary' is checked but not set. Checked in 2019421 and 2 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'exe.no.referer' is checked but not set. Checked in 2020500 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.JavaNotJar' is checked but not set. Checked in 2016540 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.pdf.in.http' is checked but not set. Checked in 2017150 and 3 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'HTTP.UncompressedFlash' is checked but not set. Checked in 2023313 and 0 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.http.javaclient' is checked but not set. Checked in 2017181 and 4 other sigs
2024-12-04T10:43:02	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'et.WinHttpRequest' is checked but not set. Checked in 2019823 and 0 other sigs
2024-12-04T10:42:47	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_DEPRECATED(203)] - Found deprecated eve-log.alert app-layer flag "tls", enabling metadata.app-layer
2024-12-04T10:42:47	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_DEPRECATED(203)] - Found deprecated eve-log.alert app-layer flag "http", enabling metadata.app-layer
2024-12-04T10:42:47	Warning	suricata	[100194] <Warning> -- [ERRCODE: SC_WARN_DEPRECATED(203)] - Found deprecated eve-log.alert app-layer flag "tls", enabling metadata.app-layer

20 - Application Level Attack Protection

Set Steps	Acceptance Criteria
Go to ***Services > Intrusion Detection > Policy.*** Create application control policies to allow, deny, or restrict specific applications or categories.	Protect mail, web and remote-access servers from attacks (IIS, Exchange, Citrix).
Test application access under different policy configurations.	Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat).
Go to ***Services > Intrusion Detection > Log File.*** Verify that the firewall enforces policies accurately and blocks unauthorized applications.	The logs should indicate the attack and the response action.



Services: Intrusion Detection: Policy

☐ Enabled	Priority	Description	Commands
No results found!			

Showing 0 to 0 of 0 entries

Rule details

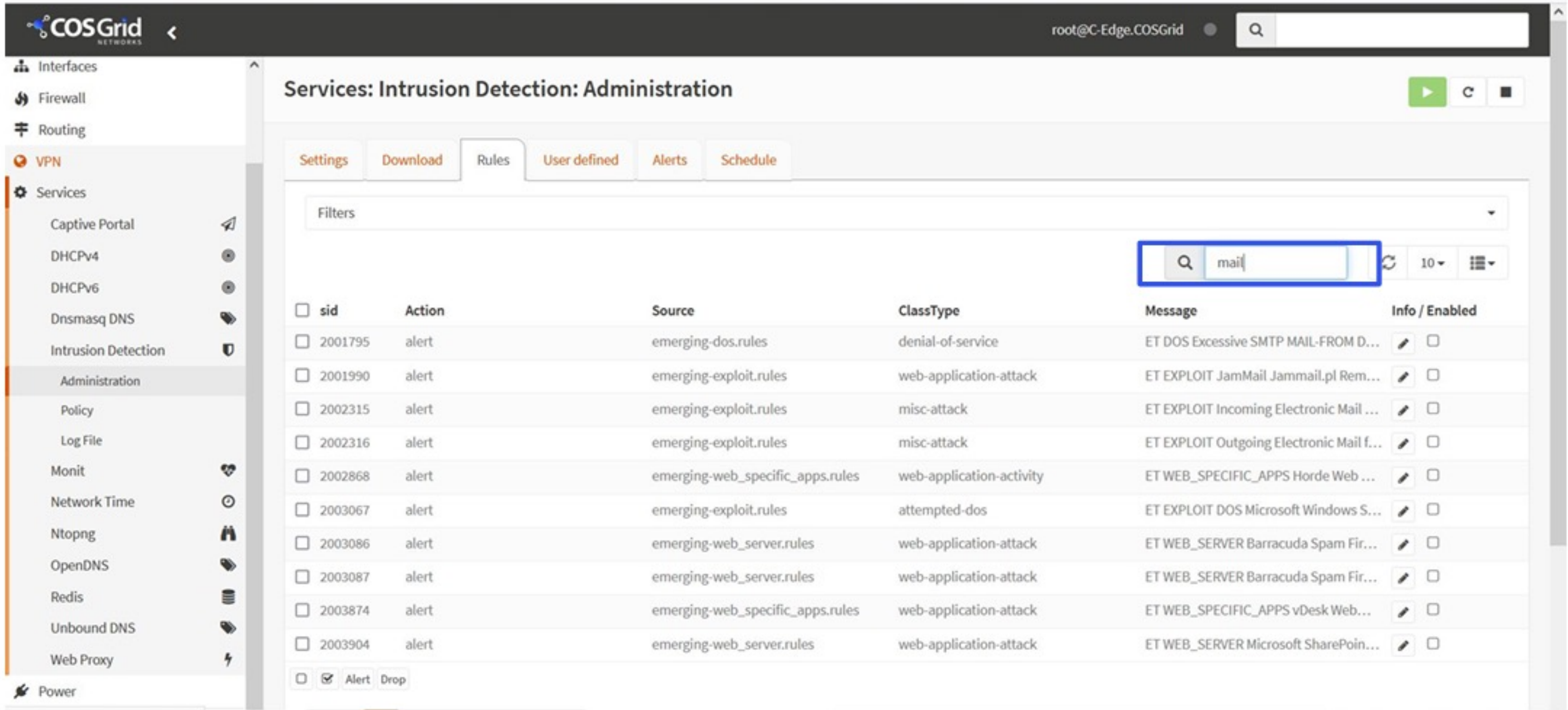
- Enabled: ☑
- Priority: 0
- Rulesets: Nothing selected (Clear All)
- Action: Nothing selected (Clear All)
- Rules:
  - affected_product: Nothing selected
  - attack_target: Nothing selected
  - classtype: Nothing selected
  - confidence: Nothing selected
  - cve: Nothing selected
  - deployment: Nothing selected

20 - Application Level Attack Protection- Protect mail, web and remote-access servers from attacks (IIS, Exchange, Citrix)

Set Steps

Go to ***Services > Intrusion Detection > Administration > Rules tab.***

In the search bar have to search rules related to Mail, Citrix etc...



Services: Intrusion Detection: Administration

mail

☐ sid	Action	Source	ClassType	Message	Info / Enabled
☐ 2001795	alert	emerging-dos.rules	denial-of-service	ET DOS Excessive SMTP MAIL-FROM D...	☐
☐ 2001990	alert	emerging-exploit.rules	web-application-attack	ET EXPLOIT JamMail Jammail.pl Rem...	☐
☐ 2002315	alert	emerging-exploit.rules	misc-attack	ET EXPLOIT Incoming Electronic Mail ...	☐
☐ 2002316	alert	emerging-exploit.rules	misc-attack	ET EXPLOIT Outgoing Electronic Mail f...	☐
☐ 2002868	alert	emerging-web_specific_apps.rules	web-application-activity	ET WEB_SPECIFIC_APPS Horde Web ...	☐
☐ 2003067	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT DOS Microsoft Windows S...	☐
☐ 2003086	alert	emerging-web_server.rules	web-application-attack	ET WEB_SERVER Barracuda Spam Fir...	☐
☐ 2003087	alert	emerging-web_server.rules	web-application-attack	ET WEB_SERVER Barracuda Spam Fir...	☐
☐ 2003874	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS vDesk Web...	☐
☐ 2003904	alert	emerging-web_server.rules	web-application-attack	ET WEB_SERVER Microsoft SharePoin...	☐

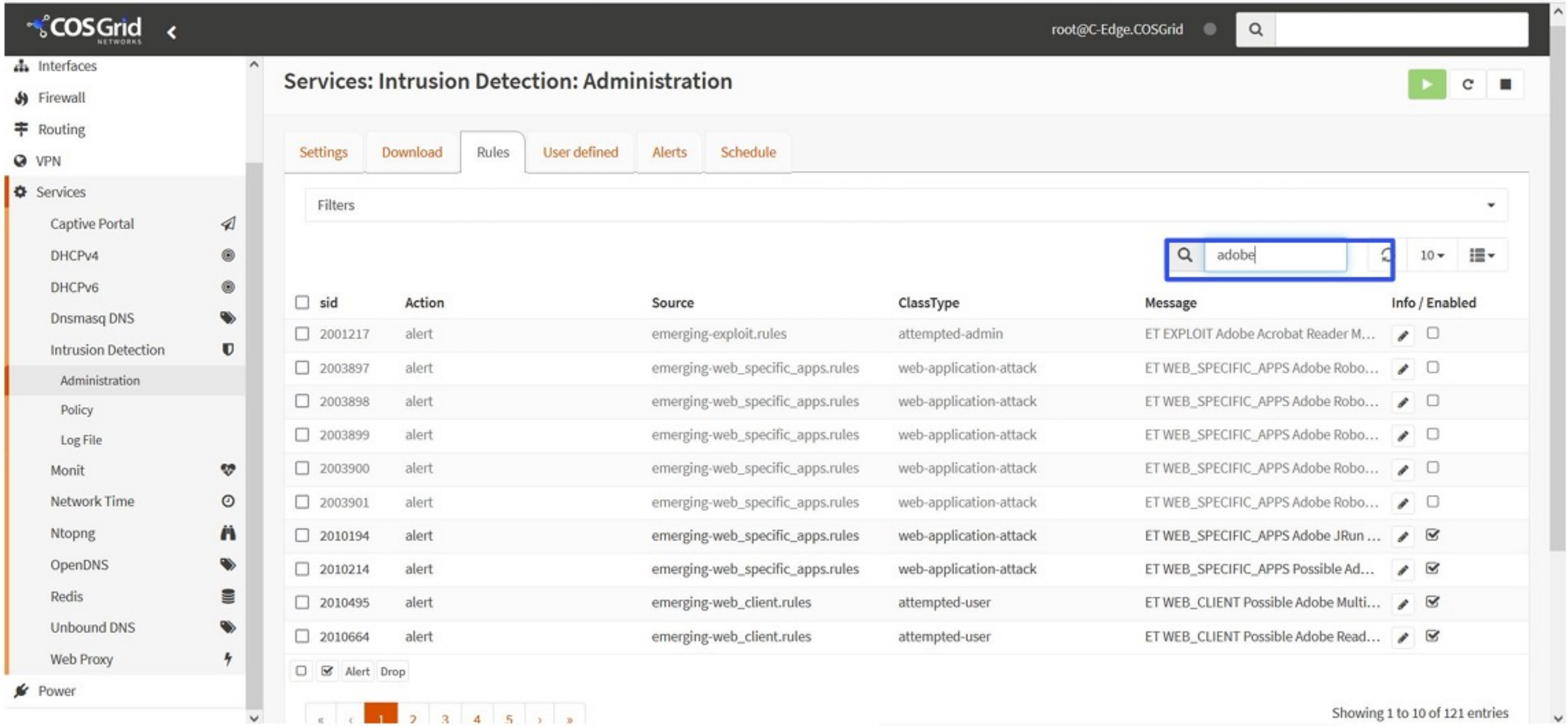
☐ ☑ Alert Drop

20 - Application Level Attack Protection- Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat).

Set Steps

Go to ***Services > Intrusion Detection > Administration > Rules tab.***

In the search bar have to search rules related to adobe, office etc...



Services: Intrusion Detection: Administration

adobe

☐ sid	Action	Source	ClassType	Message	Info / Enabled
☐ 2001217	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT Adobe Acrobat Reader M...	☐
☐ 2003897	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Adobe Robo...	☐
☐ 2003898	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Adobe Robo...	☐
☐ 2003899	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Adobe Robo...	☐
☐ 2003900	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Adobe Robo...	☐
☐ 2003901	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Adobe Robo...	☐
☐ 2010194	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Adobe JRun ...	☑
☐ 2010214	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Possible Ad...	☑
☐ 2010495	alert	emerging-web_client.rules	attempted-user	ET WEB_CLIENT Possible Adobe Multi...	☑
☐ 2010664	alert	emerging-web_client.rules	attempted-user	ET WEB_CLIENT Possible Adobe Read...	☑

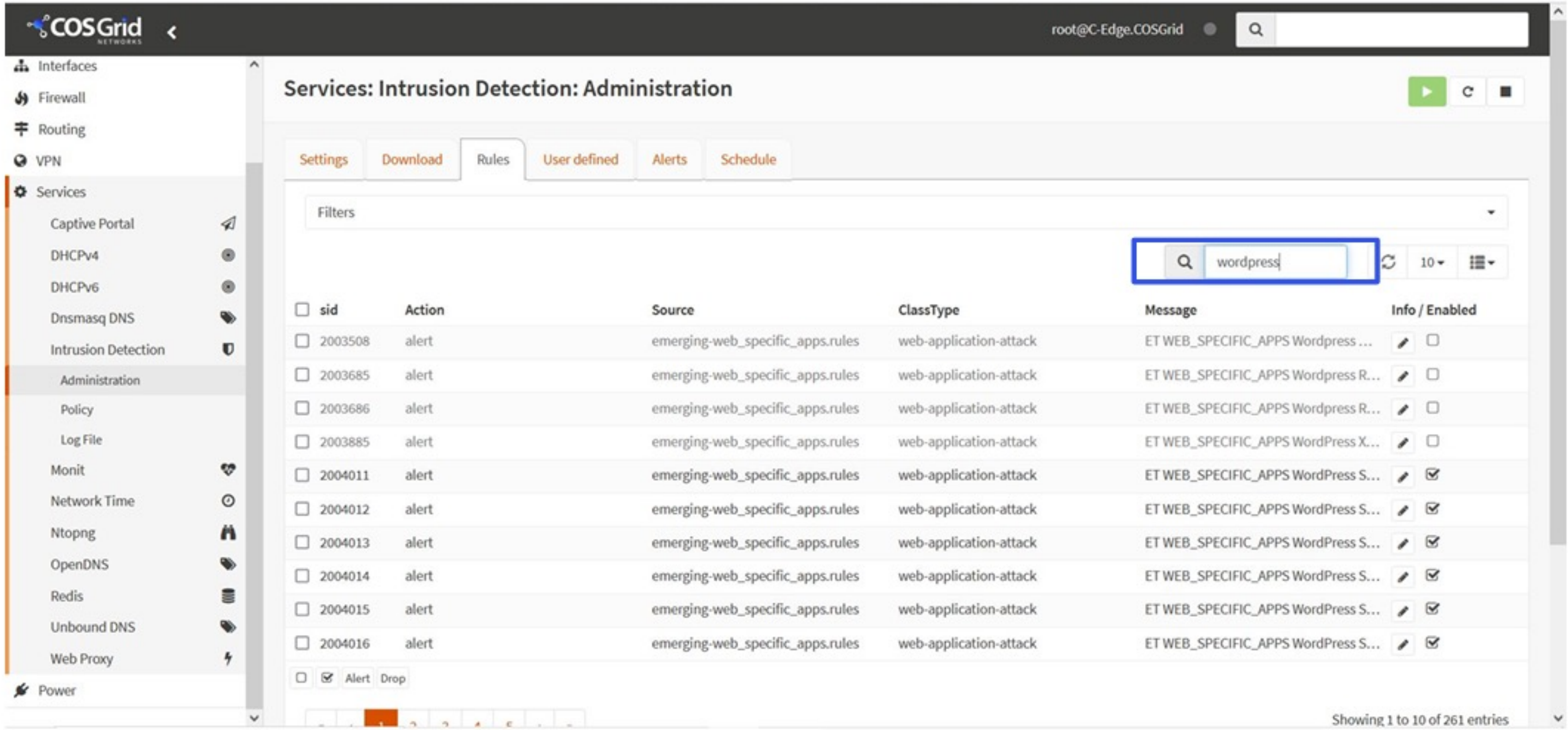
Showing 1 to 10 of 121 entries

20 - Application Level Attack Protection- Common Web platform Protection (Wordpress,.net)

Set Steps

Go to ***Services > Intrusion Detection > Administration > Rules tab.***

In the search bar have to search rules related to wordpress , dot net etc...



Services: Intrusion Detection: Administration

wordpress

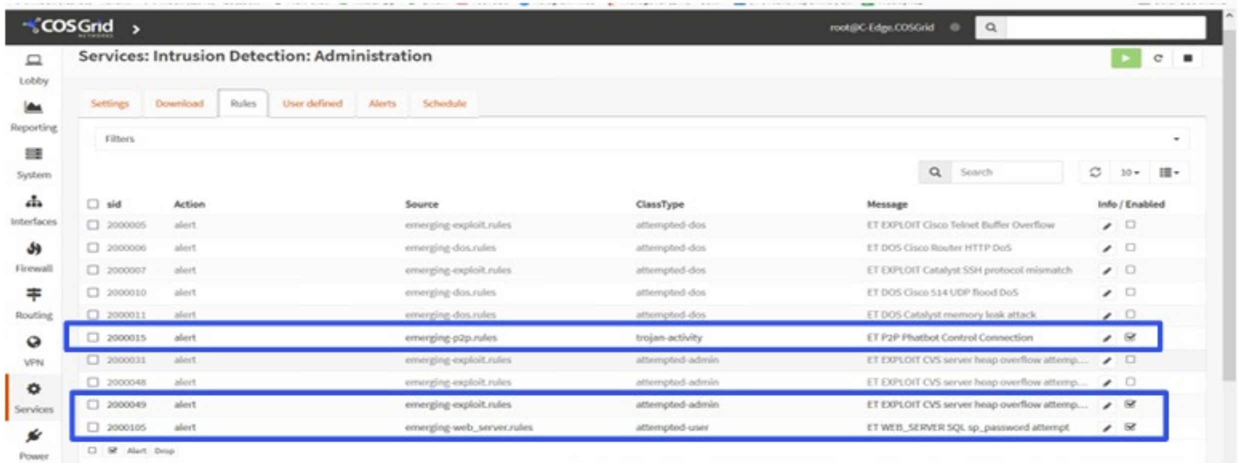
□ sid	Action	Source	ClassType	Message	Info / Enabled
□ 2003508	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Wordpress ...	□
□ 2003685	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Wordpress R...	□
□ 2003686	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS Wordpress R...	□
□ 2003885	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS WordPress X...	□
□ 2004011	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS WordPress S...	☑
□ 2004012	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS WordPress S...	☑
□ 2004013	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS WordPress S...	☑
□ 2004014	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS WordPress S...	☑
□ 2004015	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS WordPress S...	☑
□ 2004016	alert	emerging-web_specific_apps.rules	web-application-attack	ET WEB_SPECIFIC_APPS WordPress S...	☑

□ ☑ Alert Drop

Showing 1 to 10 of 261 entries

21 - Detect & Block Network Borne attacks

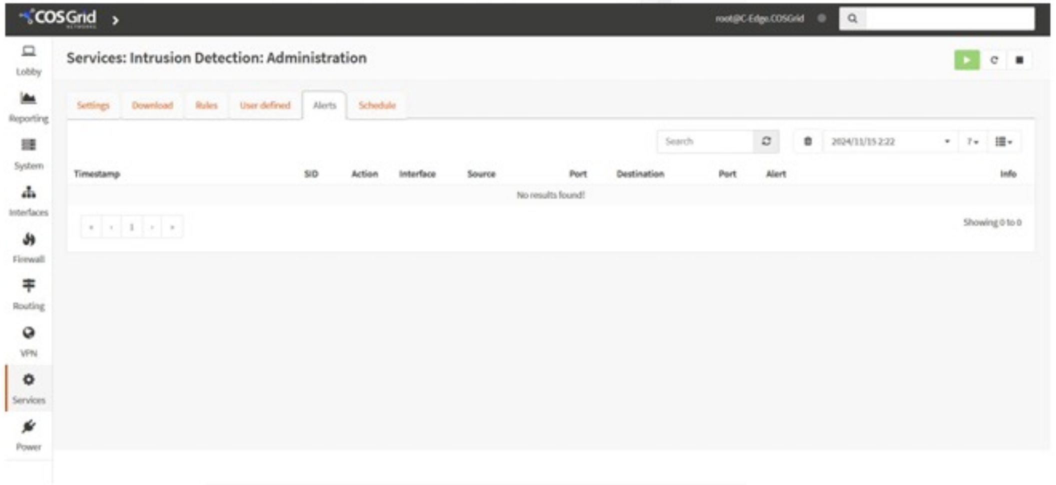
Navigate ***Services > Intrusion Detection > Administration*** . In the ***"Alerts"*** tab you can view the alerts triggered by the IDS/IPS system. Use the info button here to collect details about the detected event or threat.



Services: Intrusion Detection: Administration

□ sid	Action	Source	ClassType	Message	Info / Enabled
□ 2000005	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT Cisco Telnet Buffer Overflow	□
□ 2000006	alert	emerging-dos.rules	attempted-dos	ET DOS Cisco Router HTTP DoS	□
□ 2000007	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT Catalyst SSH protocol mismatch	□
□ 2000010	alert	emerging-dos.rules	attempted-dos	ET DOS Cisco 514 UDP flood DoS	□
□ 2000011	alert	emerging-dos.rules	attempted-dos	ET DOS Catalyst memory leak attack	□
□ 2000015	alert	emerging-p2p.rules	trojan-activity	ET P2P Phatbot Control Connection	☑
□ 2000031	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT CVS server heap overflow attemp...	□
□ 2000048	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT CVS server heap overflow attemp...	□
□ 2000049	alert	emerging-exploit.rules	attempted-admin	ET EXPLOIT CVS server heap overflow attemp...	☑
□ 2000105	alert	emerging-web_server.rules	attempted-user	ET WEB_SERVER SQL sp_password attempt	☑

□ ☑ Alert Drop



Services: Intrusion Detection: Administration

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
No results found!									

Showing 0 to 0

22 - Customisable Rule Set & Signatures

Navigate ***Services > Intrusion Detection > Administration > Settings*** and Enable IPS Mode

Click on the User Defined Tab and click add button to add rule

Find out the SSL fingerprint of a website. For demonstration we will block facebook and use Firefox to determine the fingerprint.

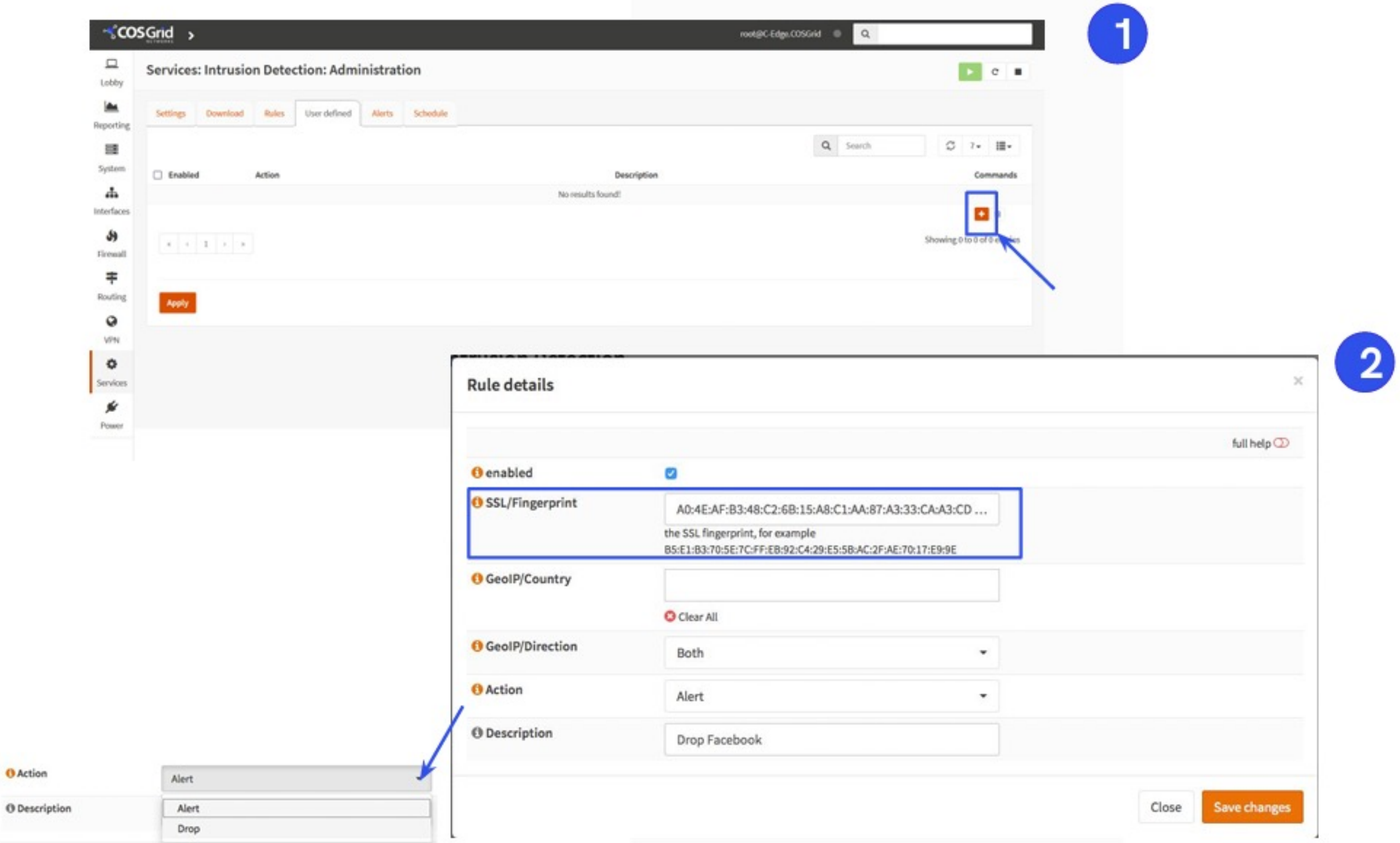
Open your browser and go to https://facebook.com when loaded click on the lock next to the address :

🔒 https://www.facebook.com/?_rdr=p

Copy the SHA1 certificate fingerprint (A0:4E:AF:B3:48:C2:6B:15:A8:C1:AA:87:A3:33:CA:A3:CD:EE:C9:C9).

Paste this into the SSL/Fingerprint field of rule details

.



1

Services: Intrusion Detection: Administration

No results found!

2

Rule details

enabled ☑

SSL/Fingerprint: A0:4E:AF:B3:48:C2:6B:15:A8:C1:AA:87:A3:33:CA:A3:CD ...

the SSL fingerprint, for example B5:E1:B3:70:5E:7C:FF:EB:92:C4:29:E5:5B:AC:2F:AE:70:17:E9:9E

GeoIP/Country:

GeoIP/Direction: Both

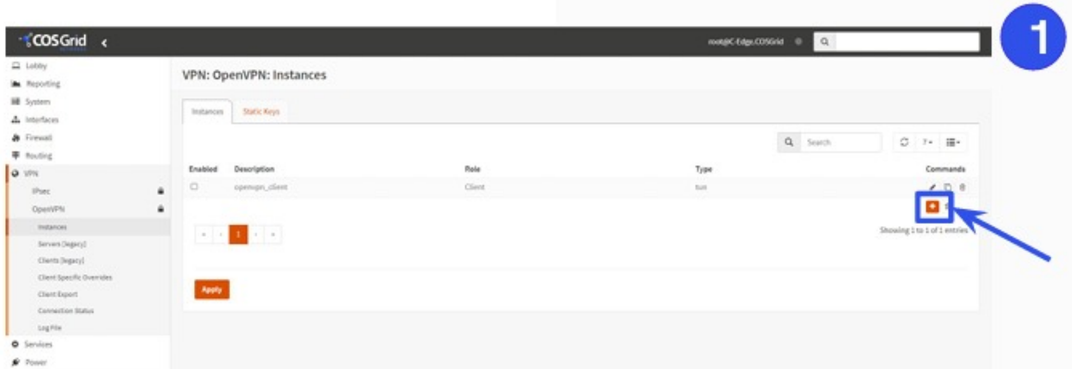
Action: Alert

Description: Drop Facebook

COSGrid
NETWORKS

23 - Configuration & Setup -OpenVPN

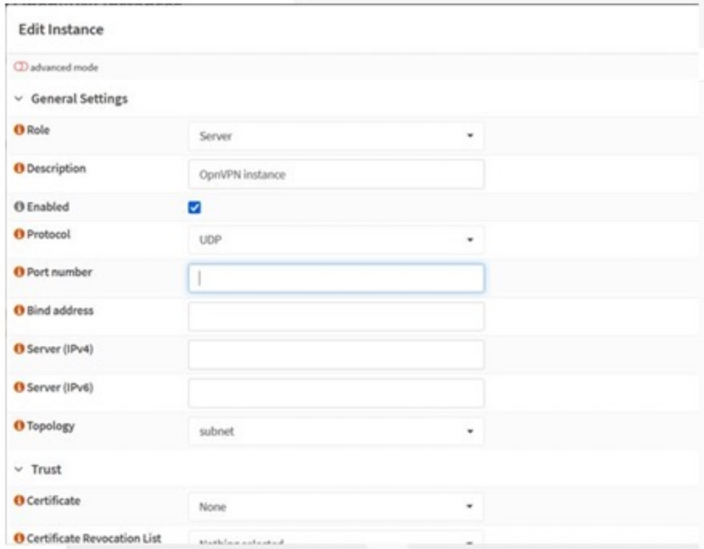
Set Steps	Acceptance Criteria
Access the COSGrid Firewall's configuration interface.	User-friendly options for enabling and configuring all three features.
Go to *VPN > OpenVPN*. Verify the presence of options to enable and configure OpenVPN and authentication services. Figure:9	Comprehensive configuration options to meet various security requirements.
Go to *VPN > OpenVPN > Instances.* Attempt to create VPN connections using protocols.	Successful creation of VPN connections enabled without errors or unexpected behavior.



VPN: OpenVPN: Instances

Enabled	Description	Role	Type	Commands
□	openvpn_client	Client	tun	

Showing 1 to 1 of 1 entries



Edit Instance

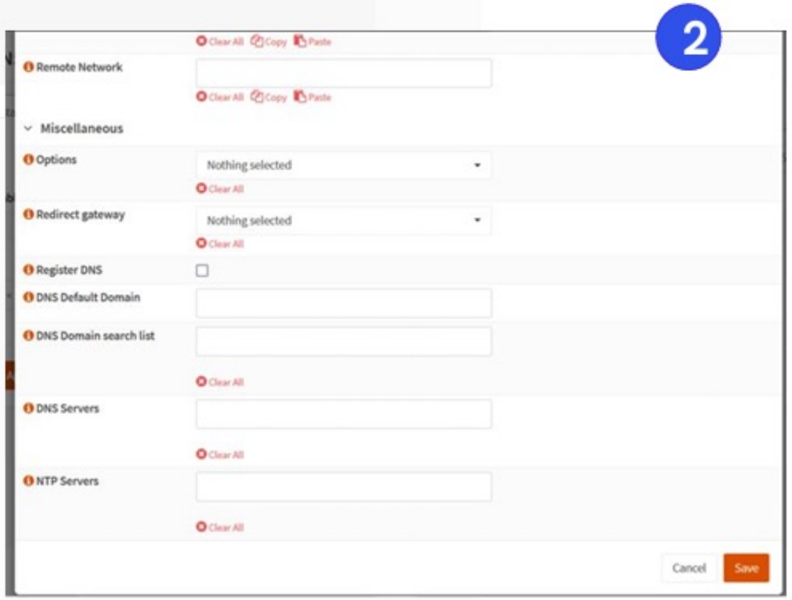
advanced mode

General Settings

- Role: Server
- Description: OpnVPN instance
- Enabled: ☑
- Protocol: UDP
- Port number:
- Bind address:
- Server (IPv4):
- Server (IPv6):
- Topology: subnet

Trust

- Certificate: None
- Certificate Revocation List: Nothing selected



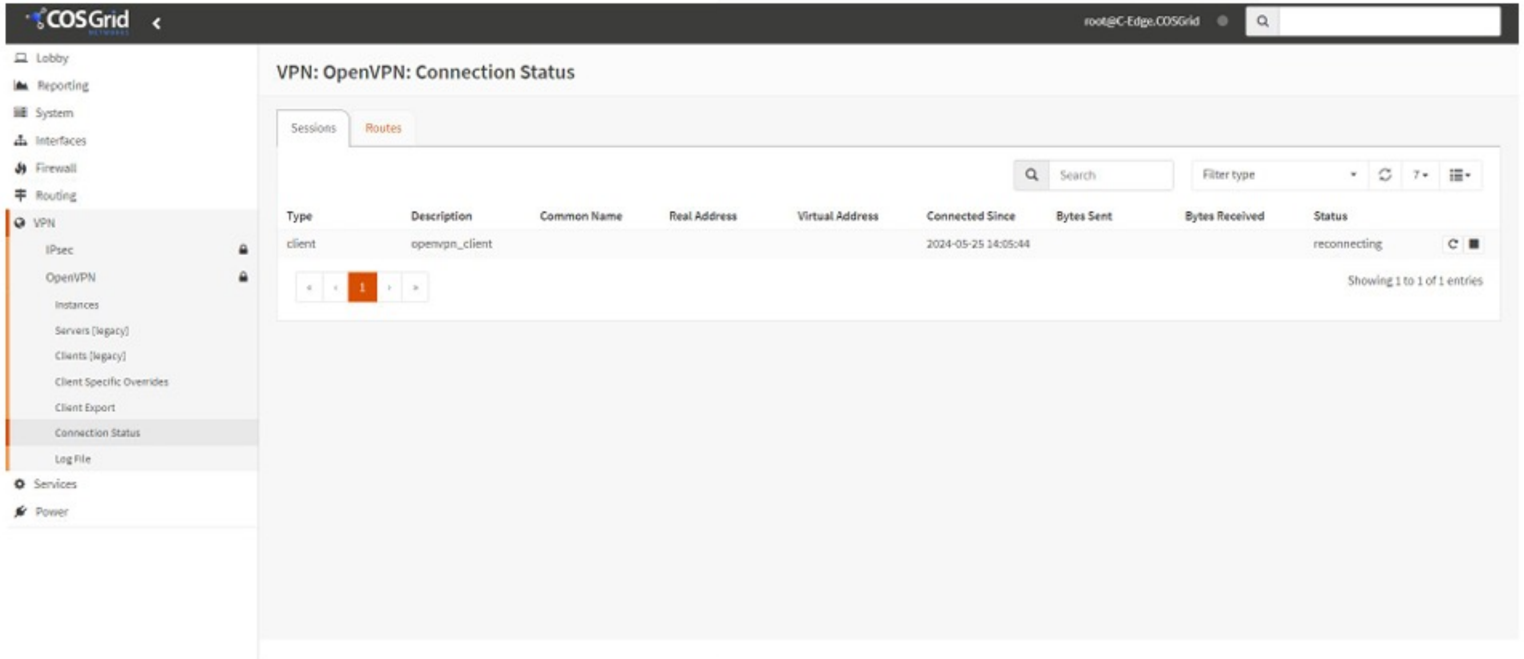
- Remote Network:

Miscellaneous

- Options: Nothing selected
- Redirect gateway: Nothing selected
- Register DNS: □
- DNS Default Domain:
- DNS Domain search list:
- DNS Servers:
- NTP Servers:

24 - OpenVPN Connection Status

Set Steps	Acceptance Criteria
Go to ***VPN > OpenVPN > Connection Status.*** See the status of your configuration.	The connection configuration made by you should be visible in the table. Note : The status will depend on the configurations you have done.



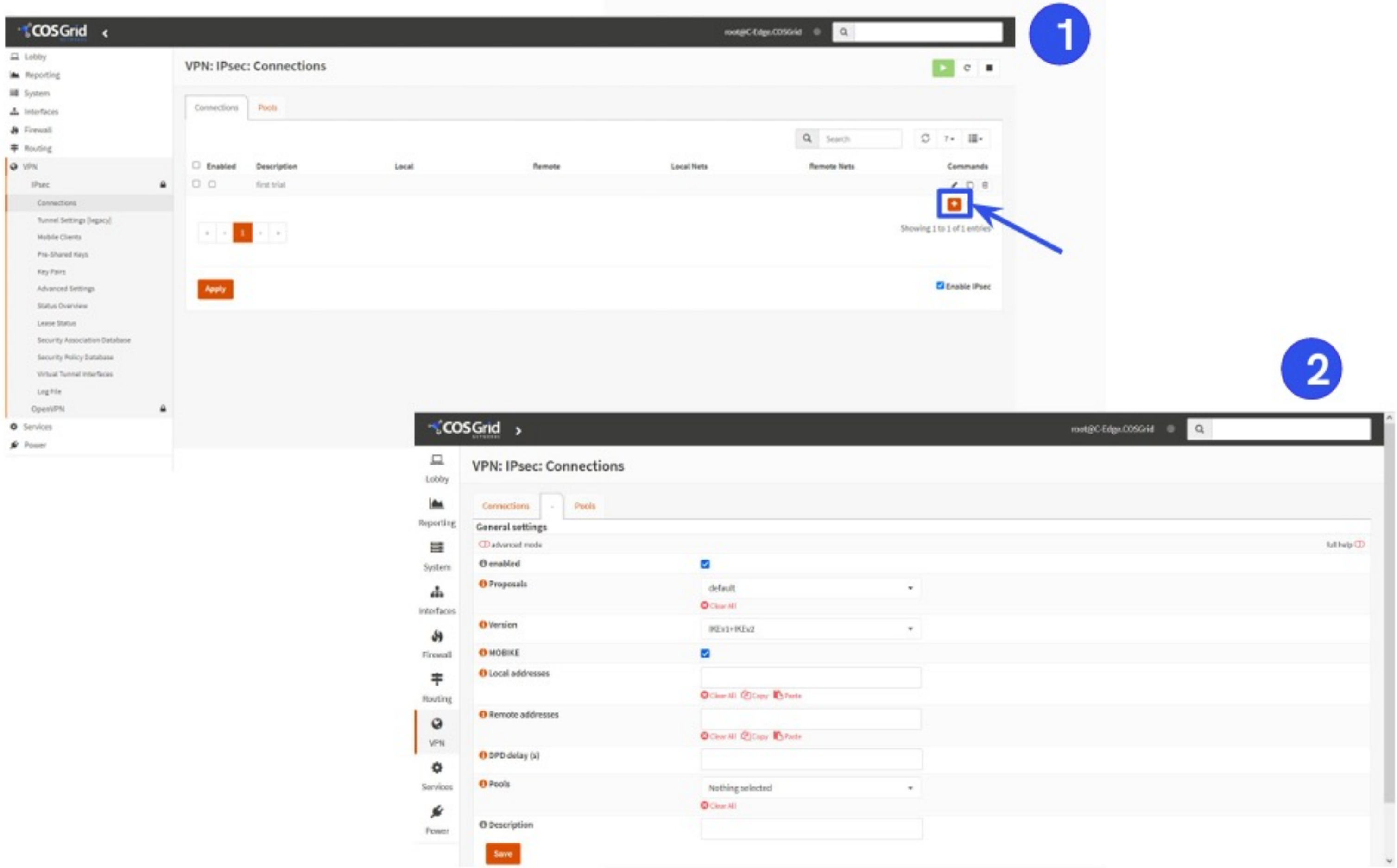
VPN: OpenVPN: Connection Status

Type	Description	Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	Status
client	openvpn_client				2024-05-25 14:05:44			reconnecting

Showing 1 to 1 of 1 entries

25 - Configuration & Setup - IPSec

Set Steps	Acceptance Criteria
Go to ***VPN > IPsec.*** Verify the presence of options to enable and configure IPsec, and authentication services.	Comprehensive configuration options to meet various security requirements.
Go to ***VPN > IPsec > Connections*** . Attempt to create VPN connections using protocols.	Successful creation of VPN connections enabled without errors or unexpected behavior.



VPN: IPsec: Connections

□	Enabled	Description	Local	Remote	Local Nets	Remote Nets	Commands
□	□	first trial					

Showing 1 to 1 of 1 entries

☑ Enable IPsec

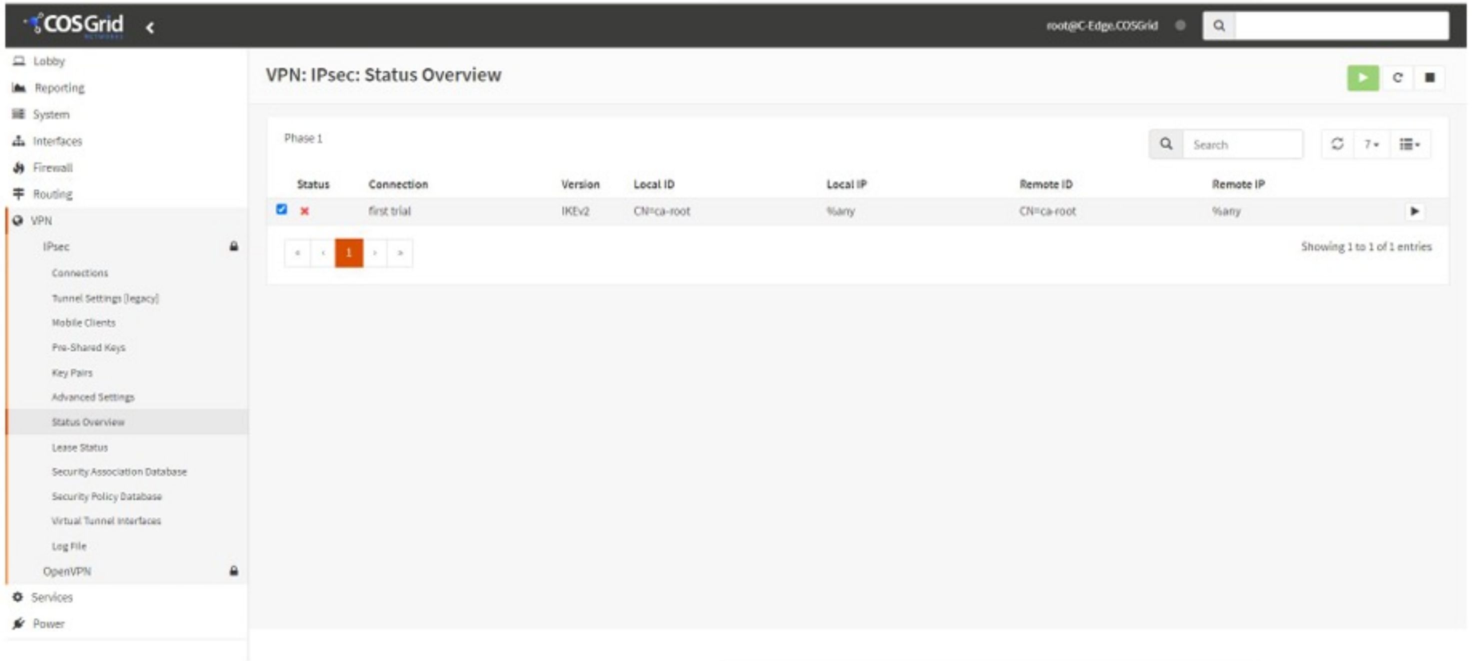
VPN: IPsec: Connections

General settings

- enabled: ☑
- Proposals: default
- Version: IKEv1+IKEv2
- MOBIKE: ☑
- Local addresses:
- Remote addresses:
- DPD delay (s):
- Pools: Nothing selected
- Description:

26 - IPSec Status Overview

Set Steps	Acceptance Criteria
Go to ***VPN > IPsec > Status Overview***. See the status of your connection	Comprehensive configuration options to meet various security requirements



VPN: IPsec: Status Overview

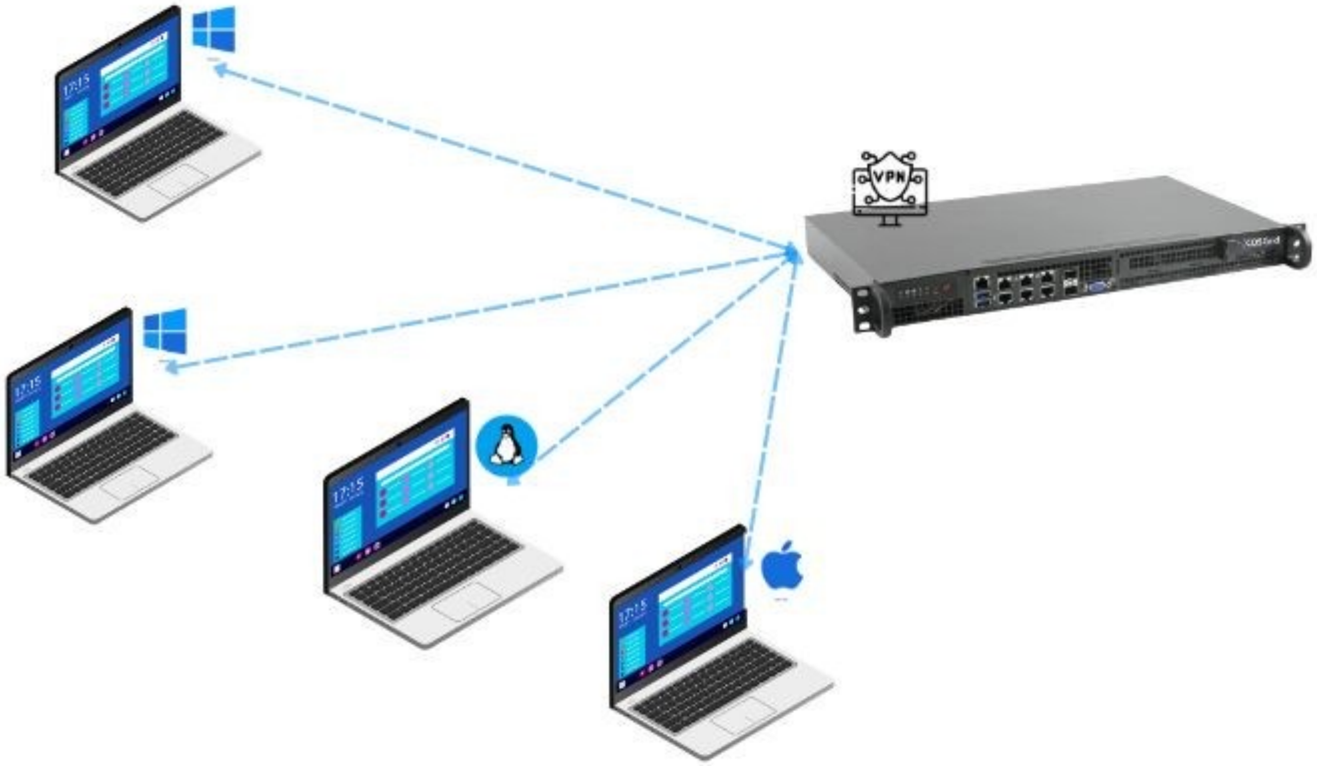
Phase 1

	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

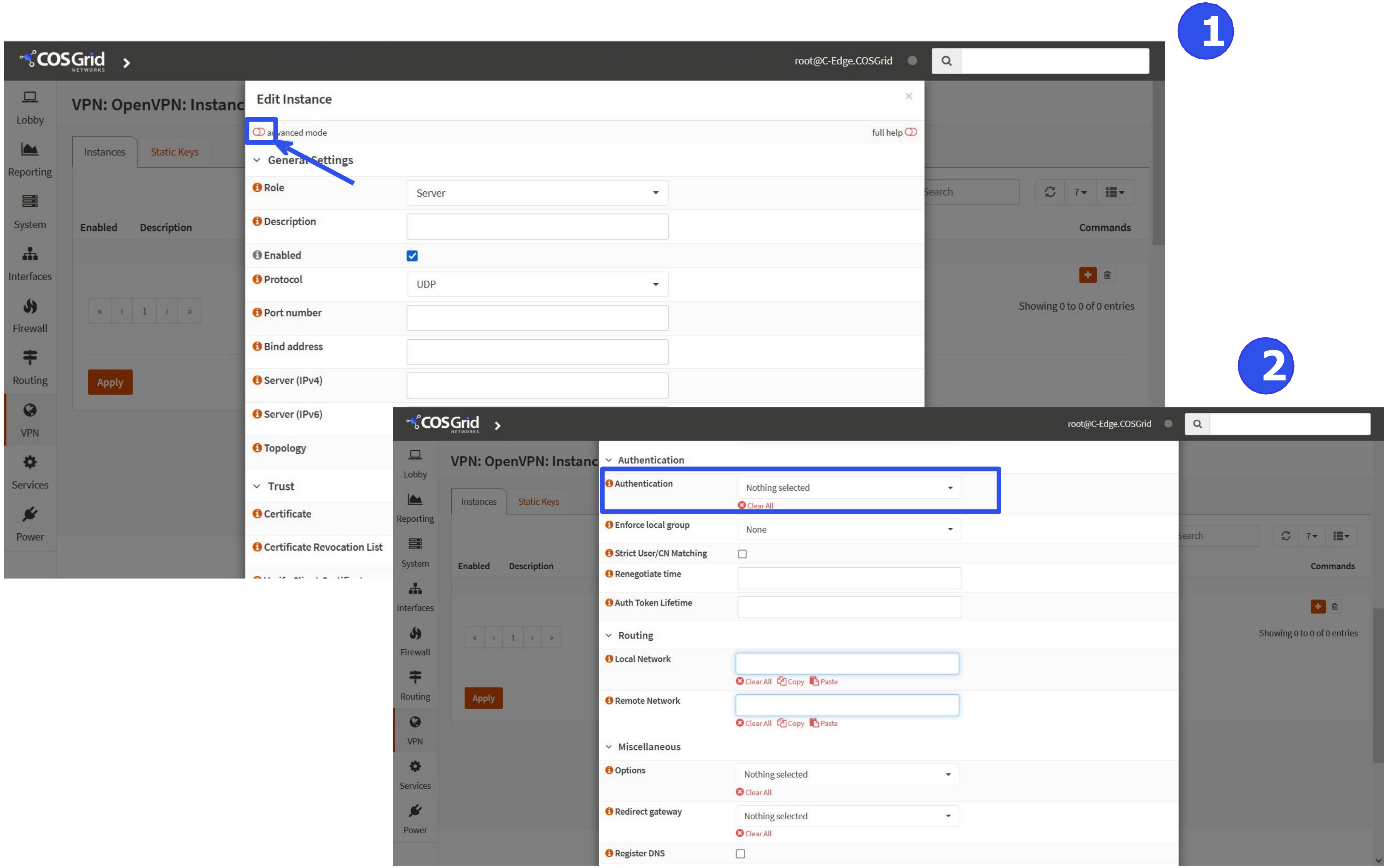
27 - Client Compatibility

Set Steps	Acceptance Criteria
Attempt to establish VPN connections using **different client devices and operating systems** (Windows, macOS, Linux, iOS, Android).	Successful connection establishment with various client devices and platforms.
Use official and **third-party** OpenVPN and IPsec clients.	**No compatibility issues** with different client software.



28 - Encryption & Access Control - OpenVPN

Set Steps	Acceptance Criteria
Go to *VPN > OpenVPN > Instances >* **(Go to one instance) Auth** Dropdown (Advanced Mode)	All VPN traffic encrypted with robust algorithms should be present in the options.
Establish VPN connections using your desired encryption algorithms and initiate data transfer.	The connection between two devices should only be established if they share the same encryption techniques.



1

COSGrid NETWORKS

root@C-Edge.COSGrid

VPN: OpenVPN: Instanc

Instances | Static Keys

Enabled | Description | Commands

Showing 0 to 0 of 0 entries

Apply

Edit Instance

advanced mode | full help

General Settings

Role	Server
Description	
Enabled	☑
Protocol	UDP
Port number	
Bind address	
Server (IPv4)	
Server (IPv6)	
Topology	

Trust

- Certificate
- Certificate Revocation List

2

COSGrid NETWORKS

root@C-Edge.COSGrid

VPN: OpenVPN: Instanc

Instances | Static Keys

Enabled | Description | Commands

Showing 0 to 0 of 0 entries

Apply

Authentication

Authentication	Nothing selected Clear All
Enforce local group	None
Strict User/CN Matching	□
Renegotiate time	
Auth Token Lifetime	

Routing

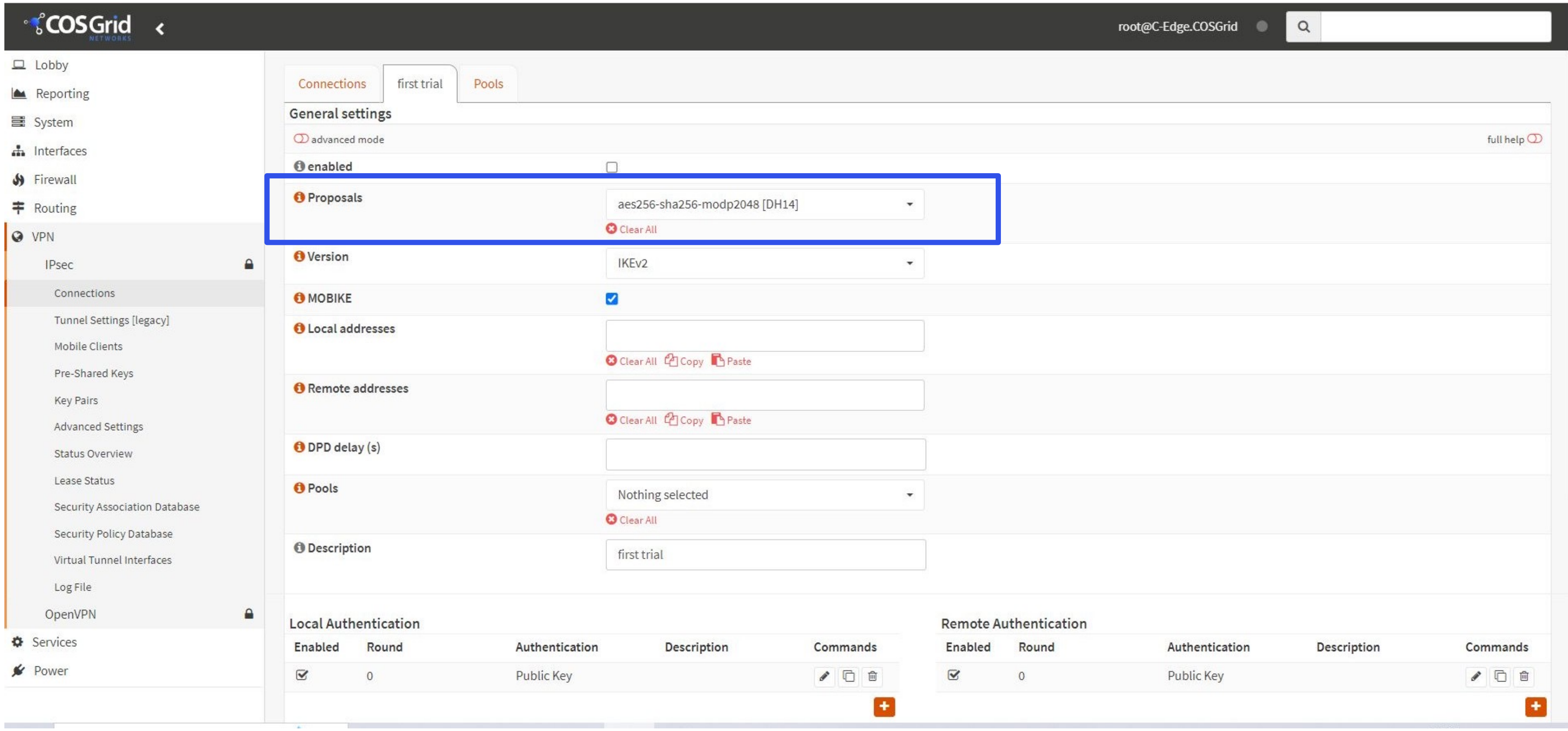
Local Network	Clear All Copy Paste
Remote Network	Clear All Copy Paste

Miscellaneous

Options	Nothing selected Clear All
Redirect gateway	Nothing selected Clear All
Register DNS	□

29 - Encryption & Access Control - IPSec

Set Steps	**Acceptance Criteria**
Go to ***VPN > IPsec > Connections>*** (Go to one connection) ***> Proposals.***	All VPN proposals should be listed down.
Establish VPN connections using specific proposals and initiate data transfer.	The connection between two devices should only be established if they share the same encryption techniques.



General settings

enabled □

Proposals: aes256-sha256-modp2048 [DH14]

Version: IKEv2

MOBIKE ☑

Local addresses:

Remote addresses:

DPD delay (s):

Pools: Nothing selected

Description: first trial

Local Authentication

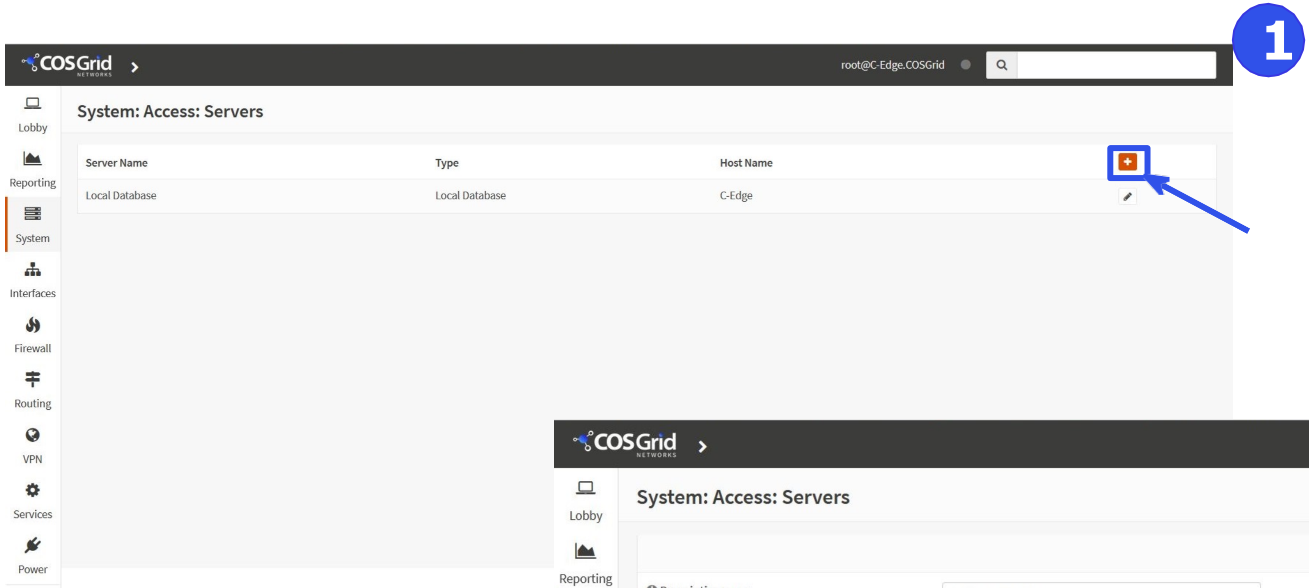
Enabled	Round	Authentication	Description	Commands
☑	0	Public Key		

Remote Authentication

Enabled	Round	Authentication	Description	Commands
☑	0	Public Key		

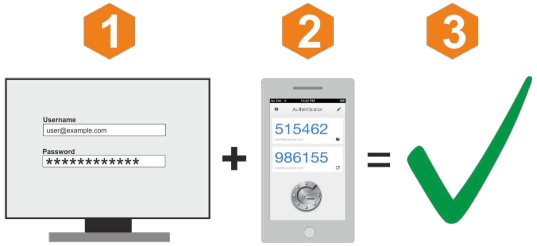
30 - Two Factor Authentication Support

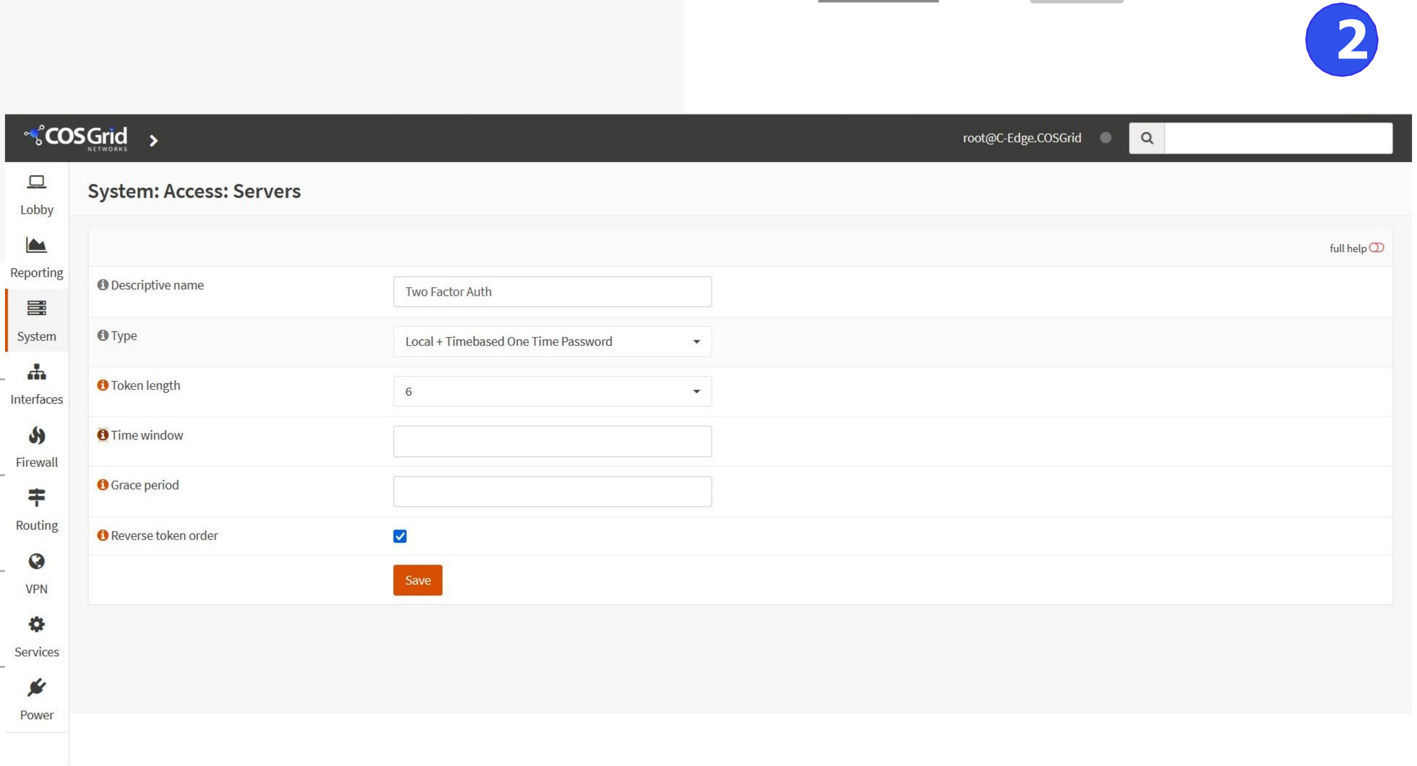
Navigate ***System › Access › Servers*** and press **Add server** in the top right corner.



System: Access: Servers

Server Name	Type	Host Name
Local Database	Local Database	C-Edge





System: Access: Servers

Descriptive name	Two Factor Auth
Type	Local + Timebased One Time Password
Token length	6
Time window	
Grace period	
Reverse token order	☑

Descriptive name	TOTP Server	*Choore a rerver name*
Type	Local+Timebased One Time Password	*Selecī īhe TOTP rerver Type*
Token length	6	*6 for Google Auīhenīicaīor*
Time window		*Leave Empīy for Google Auīhenīicaīor*
Grace period		*Leave Empīy for Google Auīhenīicaīor*

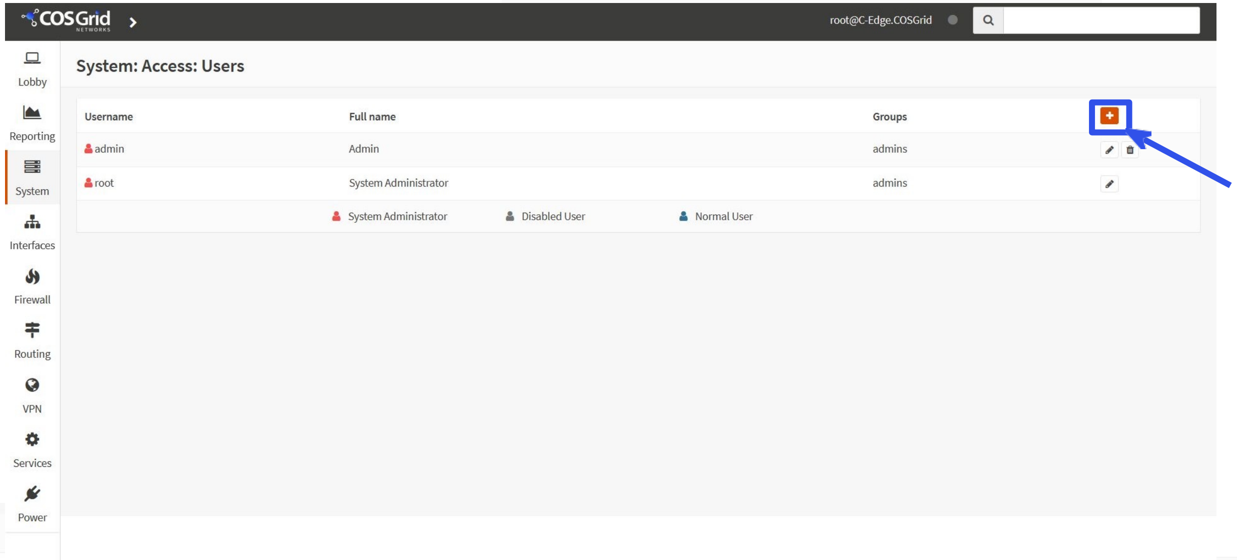
30 - Two Factor Authentication Support

Create a new user, go to *System ‣ Access ‣ Users* and click on the plus sign in the lower right corner.

Enter a **Username** and **Password** and fill in the other fields just as you would do for any other user. Then select the **Generate new (160bit) secret** under **OTP seed**.

Later press **Save**.

3

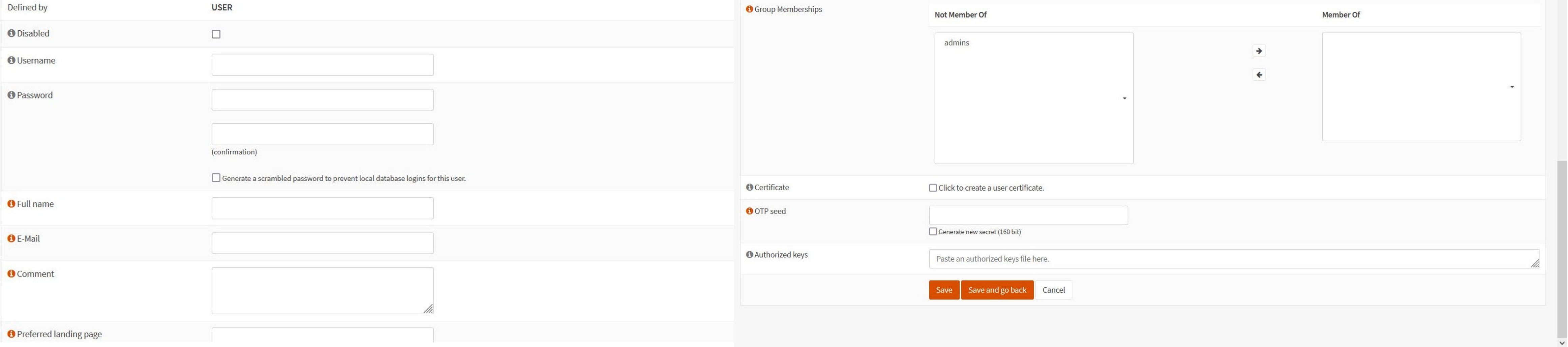


System: Access: Users

Username	Full name	Groups
admin	Admin	admins
root	System Administrator	admins

System Administrator   Disabled User   Normal User

4



Defined by	USER
Disabled	□
Username	
Password	 (confirmation) □ Generate a scrambled password to prevent local database logins for this user.
Full name	
E-Mail	
Comment	
Preferred landing page	
Group Memberships	Not Member Of: admins Member Of:
Certificate	□ Click to create a user certificate.
OTP seed	□ Generate new secret (160 bit)
Authorized keys	Paste an authorized keys file here.

30 - Two Factor Authentication Support

To activate your new OTP seed on the Google Authenticator,

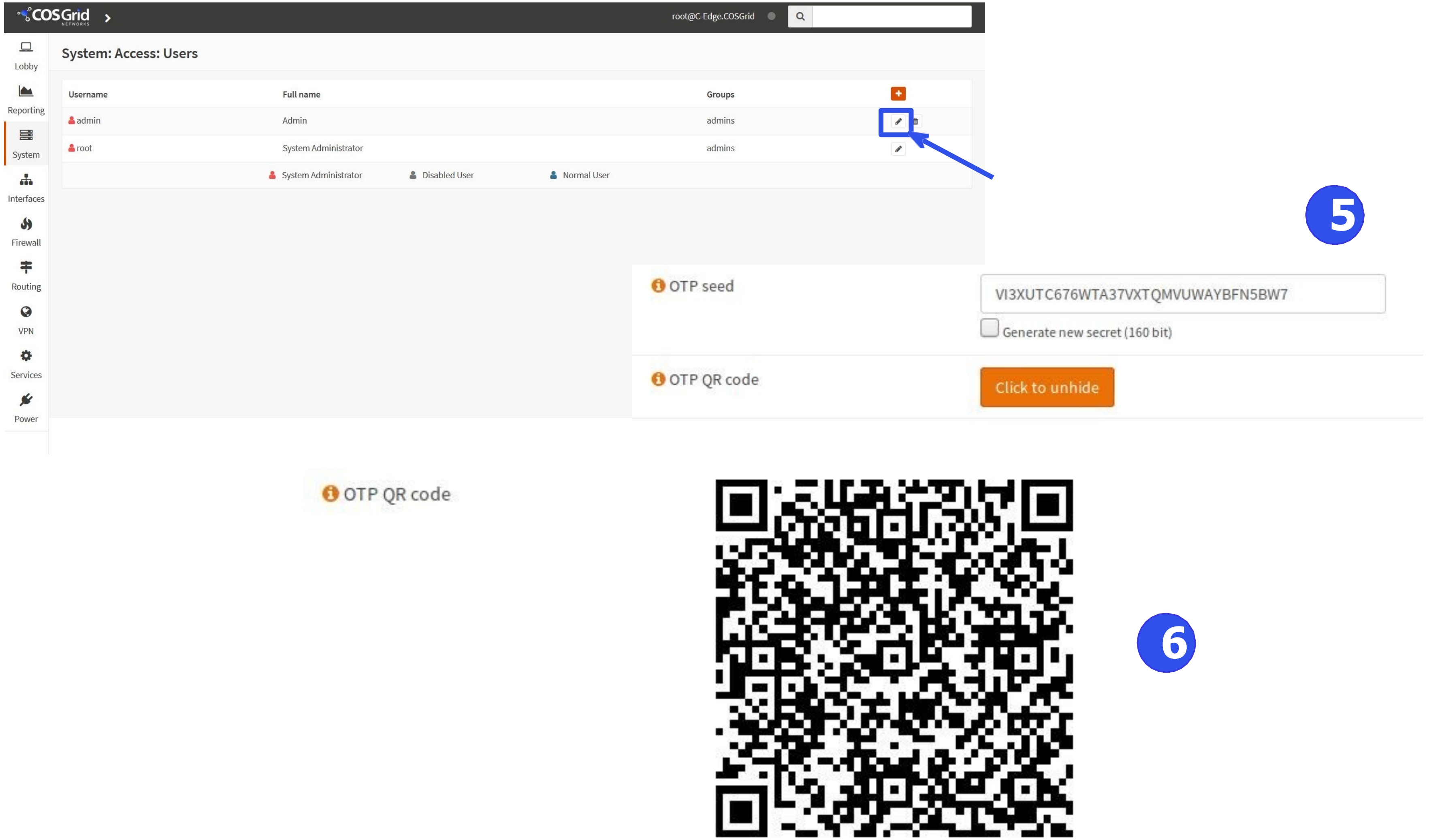
Navigate ***System ‣ Access ‣ Servers*** and press **Add server**.

Later,Navigate **System > Access > Add users**

Then enable Generate New secret Checkbox , You will get a OTP QR Code

or

reopen the created user you just created by clicking on the pencil icon.



System: Access: Users

Username	Full name	Groups
admin	Admin	admins
root	System Administrator	admins

System Administrator · Disabled User · Normal User

OTP seed: VI3XUTC676WTA37VXTQMVUWAYBFN5BW7

☐ Generate new secret (160 bit)

OTP QR code: Click to unhide

OTP QR code

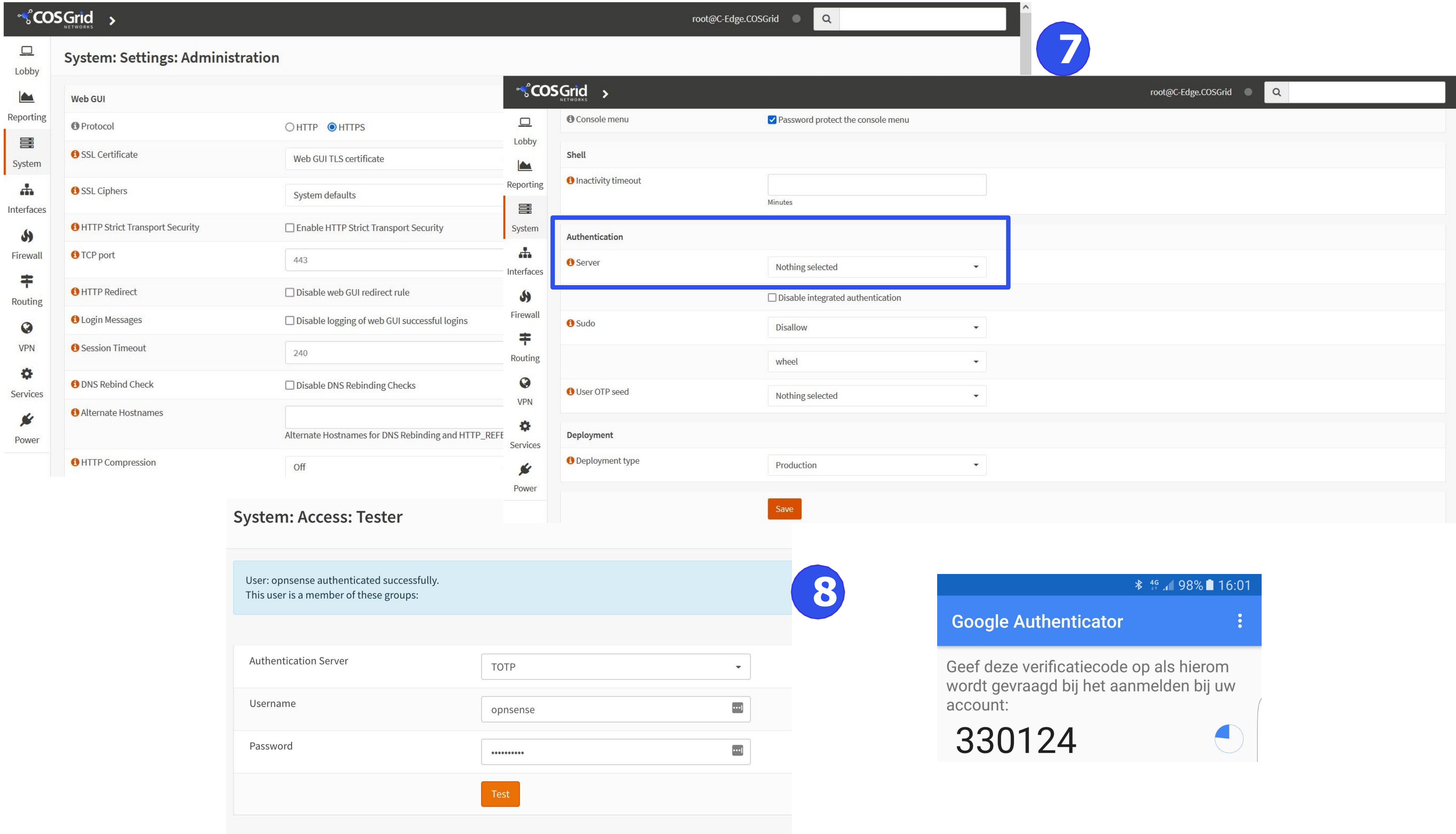
30 - Two Factor Authentication Support

Navigate ***System* ‣ *Settings* ‣ *Administration***, Scroll down section **Authentication** you should change this to your newly added authentication server to make sure no local user can gain access without 2FA.

Note : Make sure you tested token

Install Google Authenticator, then Go to ***System* ‣ *Access* ‣ *Tester***

Select the Authentication server you have configured, and enter the user name by Scanning the QR Code . Then enter the ***token + password**, remember the order is token and then password **in the same field**.



System: Settings: Administration

Web GUI

Protocol	○ HTTP ● HTTPS
SSL Certificate	Web GUI TLS certificate
SSL Ciphers	System defaults
HTTP Strict Transport Security	□ Enable HTTP Strict Transport Security
TCP port	443
HTTP Redirect	□ Disable web GUI redirect rule
Login Messages	□ Disable logging of web GUI successful logins
Session Timeout	240
DNS Rebind Check	□ Disable DNS Rebinding Checks
Alternate Hostnames	Alternate Hostnames for DNS Rebinding and HTTP_REFE
HTTP Compression	Off

Console menu	☑ Password protect the console menu

Shell

Inactivity timeout	Minutes

Authentication

Server	Nothing selected
	□ Disable integrated authentication
Sudo	Disallow
	wheel
User OTP seed	Nothing selected

Deployment

Deployment type	Production

Save

System: Access: Tester

User: opnsense authenticated successfully.
This user is a member of these groups:

Authentication Server	TOTP
Username	opnsense
Password	••••••••••

Test

98% 16:01

Google Authenticator

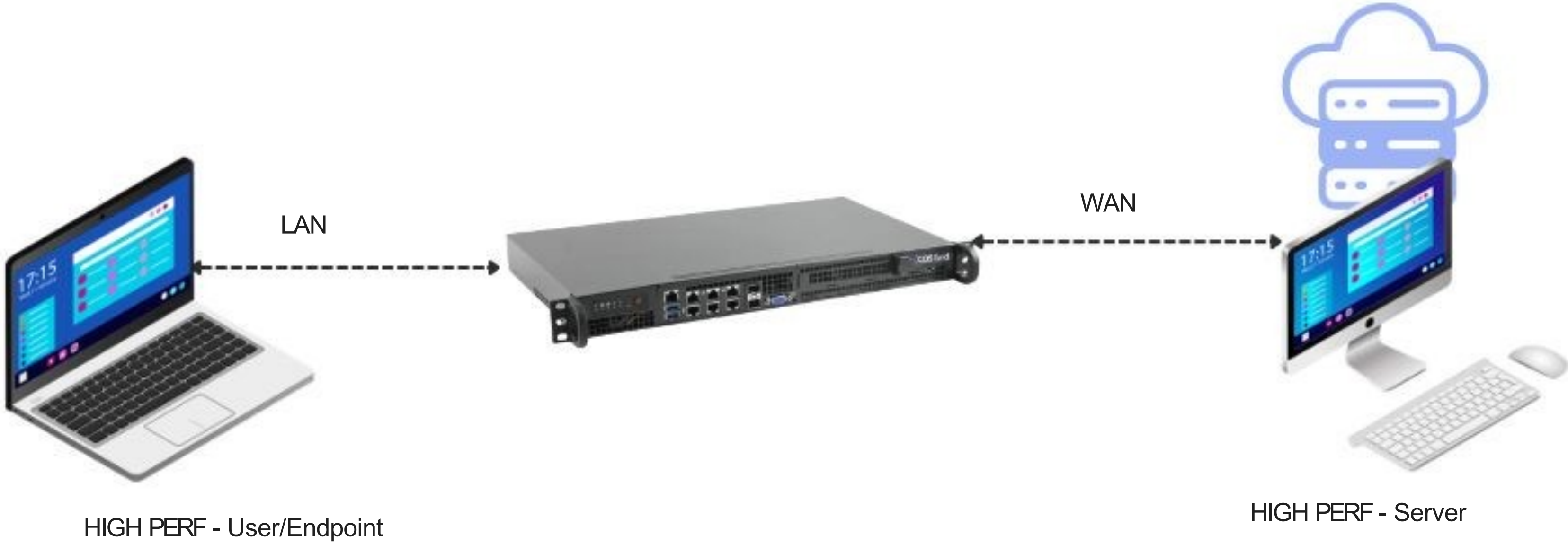
Geef deze verificatiecode op als hierom wordt gevraagd bij het aanmelden bij uw account:

330124

31 - Performance & User Experience

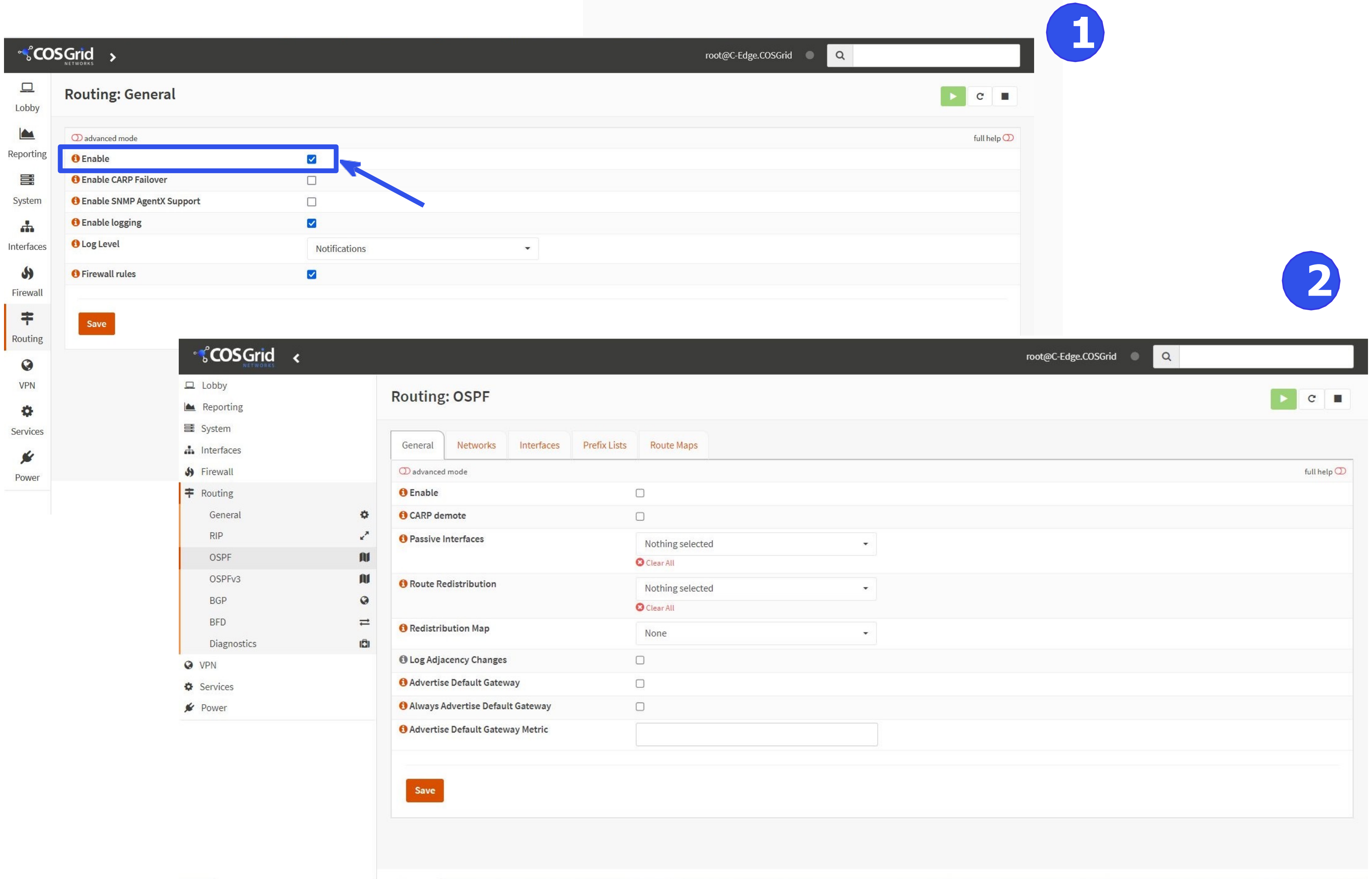
Set Steps	Acceptance Criteria
Measure throughput and **latency of VPN connections** under different network conditions. Evaluate the ease of setup and **usage, connection stability, responsiveness**, and any issues during usage.	Acceptable throughput and latency for VPN connections. No significant performance degradation compared to direct network access.

- Server: iperf -p 5000 -f m -s
- Client: iperf -p 5000 -f m -c <IP-des-Servers> -t 180 -P 10



32 - Dynamic Routing - General & OSPF

Set Steps	Acceptance Criteria
To enable Routing Go to ***Routing > General.*** Then, Go to ***Routing > OSPF*** Configure a dynamic routing protocol -OSPF	Should be able to configure routing with different functionalities like **CARP and AS Number.**
Test neighbor establishment, route exchange, and route convergence.	Check the running configuration



1

Routing: General

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

2

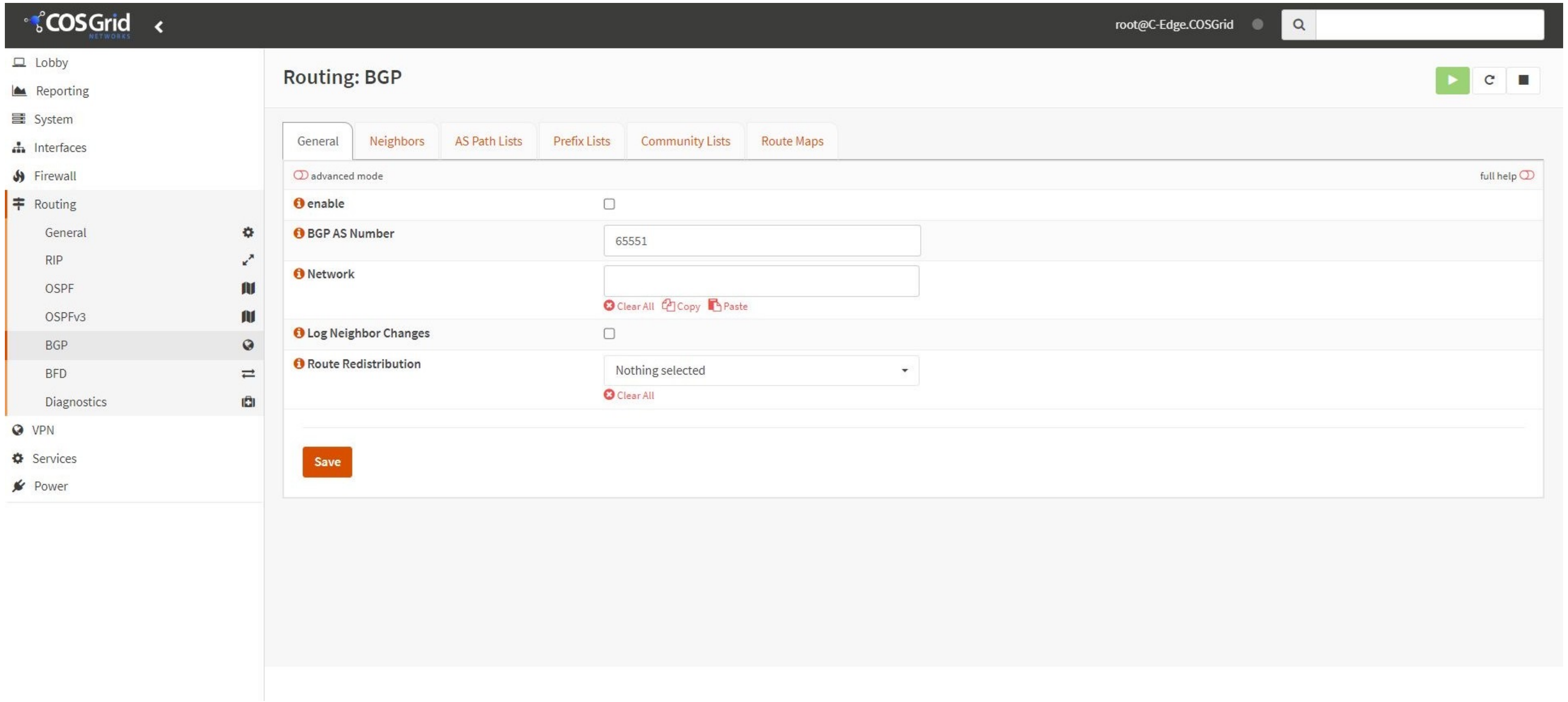
Routing: OSPF

General | Networks | Interfaces | Prefix Lists | Route Maps

- 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:

33 - Dynamic Routing - BGP

Set Steps	Acceptance Criteria
To enable Routing Go to ***Routing > General.*** Then, Go to ***Routing > BGP*** Configure a dynamic routing protocol - BGP.	Should be able to configure routing with different functionalities like **CARP and AS Number.**
Test neighbor establishment, route exchange, and route convergence.	Check the running configuration



Routing: BGP

enable □

BGP AS Number: 65551

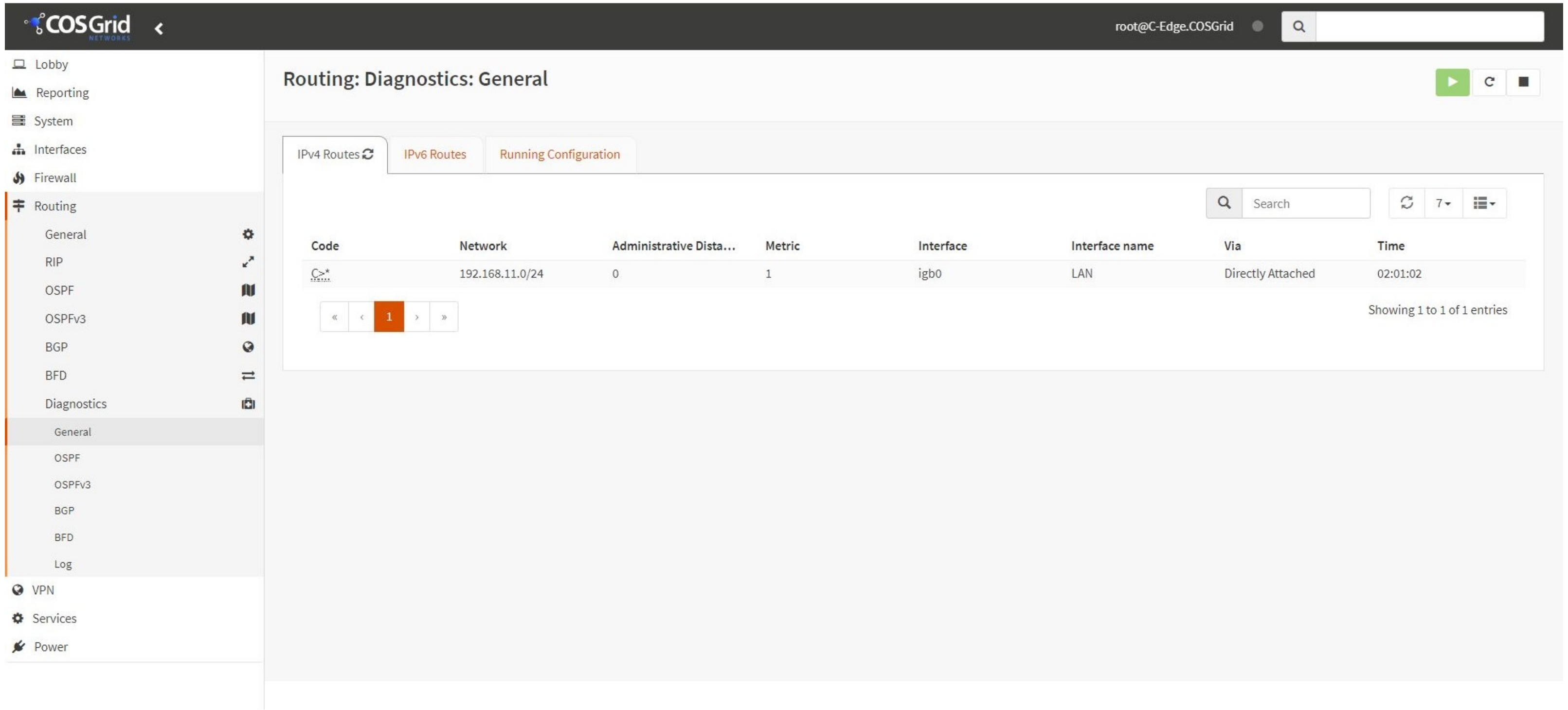
Network:

Log Neighbor Changes □

Route Redistribution: Nothing selected

35 - Routing - Diagnostics

Set Steps	Acceptance Criteria
Simulate network changes and observe dynamic route updates. Go to ***Routing > Diagnostics > General***.	You should be able to see the routing configuration and which configuration in running (**Running Configuration** tab)



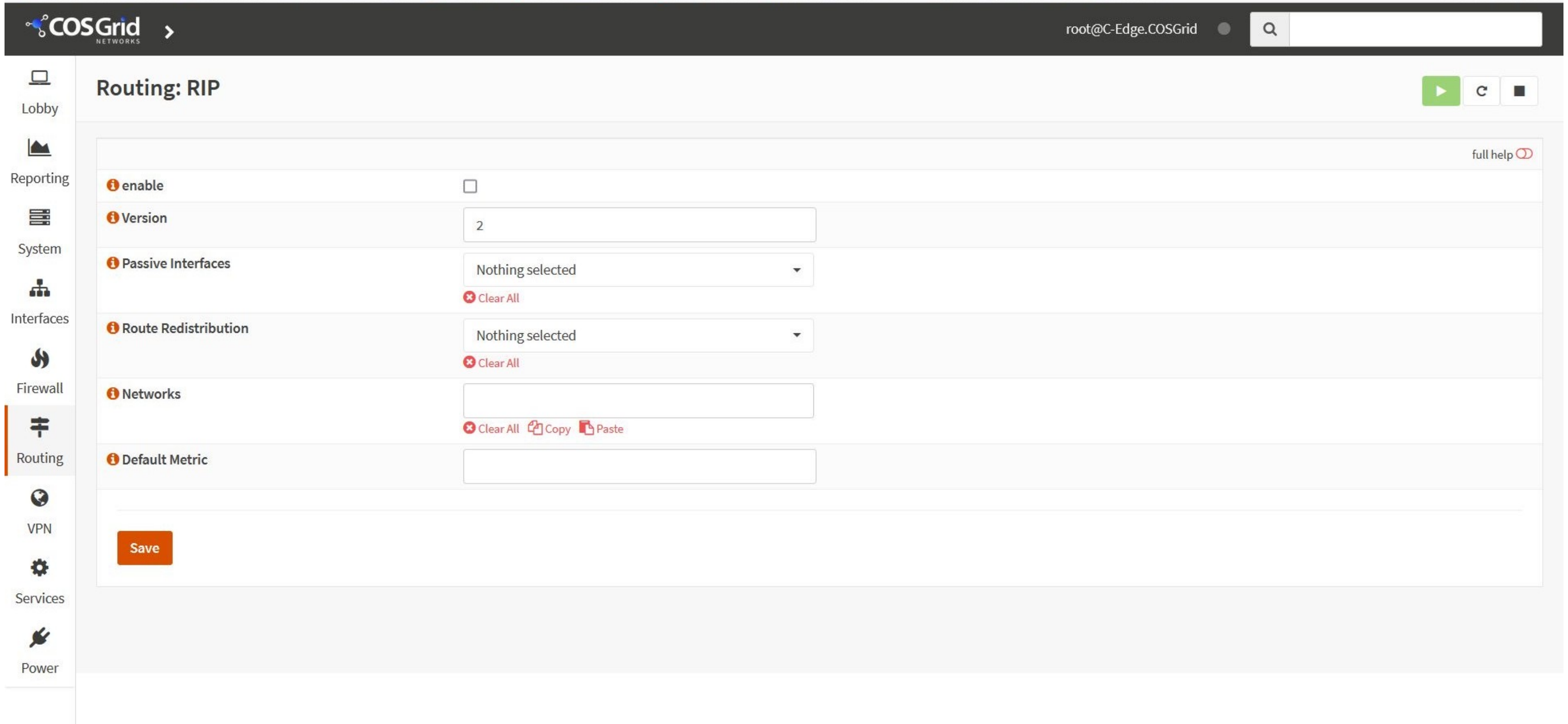
Routing: Diagnostics: General

Code	Network	Administrative Dista…	Metric	Interface	Interface name	Via	Time
C>*	192.168.11.0/24	0	1	igb0	LAN	Directly Attached	02:01:02

Showing 1 to 1 of 1 entries

34 - Dynamic Routing - RIP

Set Steps	**Acceptance Criteria**
To enable Routing Go to ***Routing > General.*** Then, Go to ***Routing > RIP*** Configure a dynamic routing protocol - RIP. Test neighbor establishment, route exchange, and route convergence.	Should be able to configure routing with different functionalities Check the running configuration



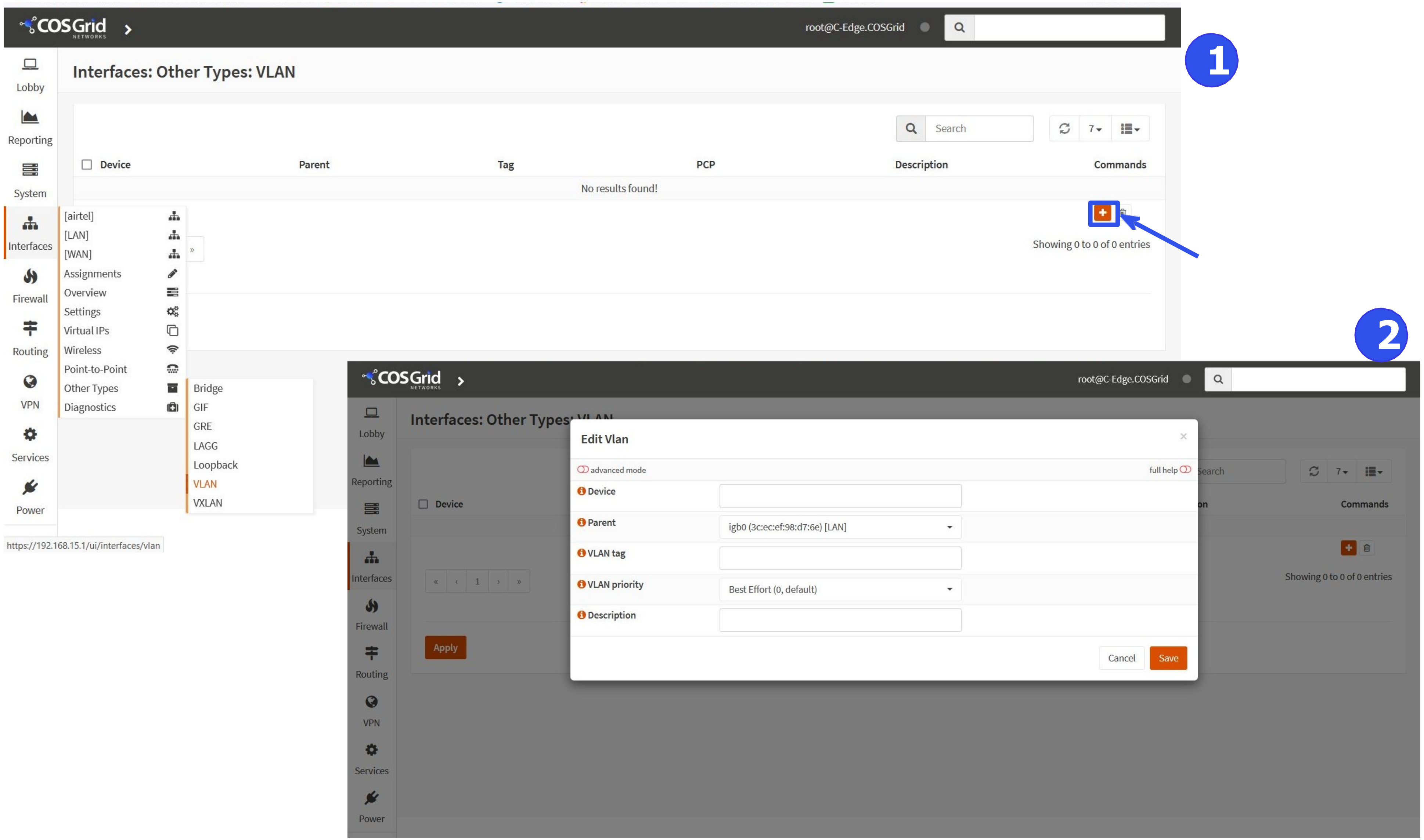
Routing: RIP

enable	□
Version	2
Passive Interfaces	Nothing selected Clear All
Route Redistribution	Nothing selected Clear All
Networks	 Clear All Copy Paste
Default Metric	

Save

36 - VLAN

Set Steps	Acceptance Criteria
Go to ***Interfaces > Other Types > VLAN***. Create VLANs as required. You can add VLAN by adding a **parent, tag and priority**.	802.1Q VLAN and Layer2 switching support



1

Interfaces: Other Types: VLAN

Device	Parent	Tag	PCP	Description	Commands
No results found!					

Showing 0 to 0 of 0 entries

https://192.168.15.1/ui/interfaces/vlan

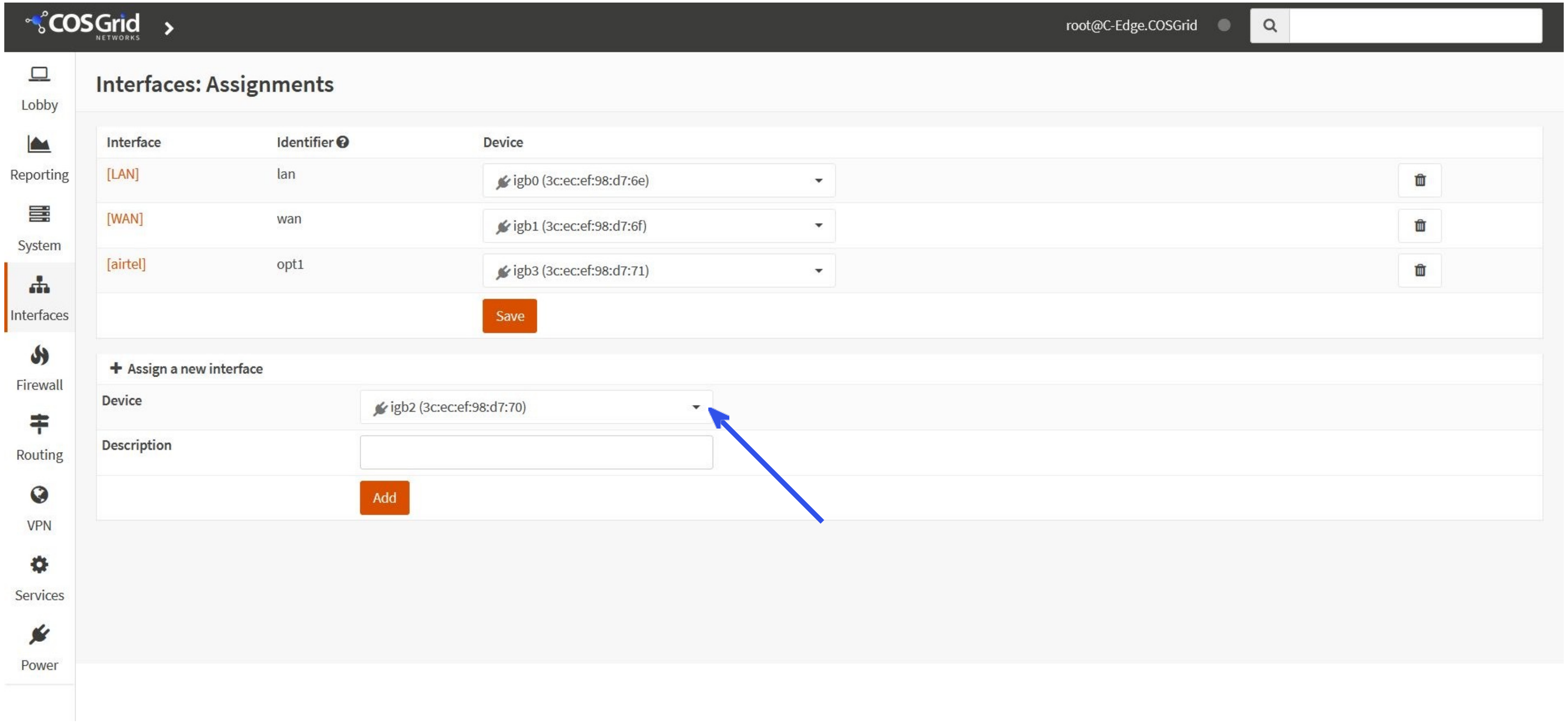
2

Edit Vlan

Device	
Parent	igb0 (3c:ec:ef:98:d7:6e) [LAN]
VLAN tag	
VLAN priority	Best Effort (0, default)
Description	

37 - VLAN Assignments

Set Steps	Acceptance Criteria
Go to ***Interfaces > Assignments***. Assign the VLAN by selecting in the drop down list	802.1Q VLAN and Layer2 switching support



Interfaces: Assignments

Interface	Identifier	Device
[LAN]	lan	igb0 (3c:ec:ef:98:d7:6e)
[WAN]	wan	igb1 (3c:ec:ef:98:d7:6f)
[airtel]	opt1	igb3 (3c:ec:ef:98:d7:71)

Save

+ Assign a new interface

Device: igb2 (3c:ec:ef:98:d7:70)

Description:

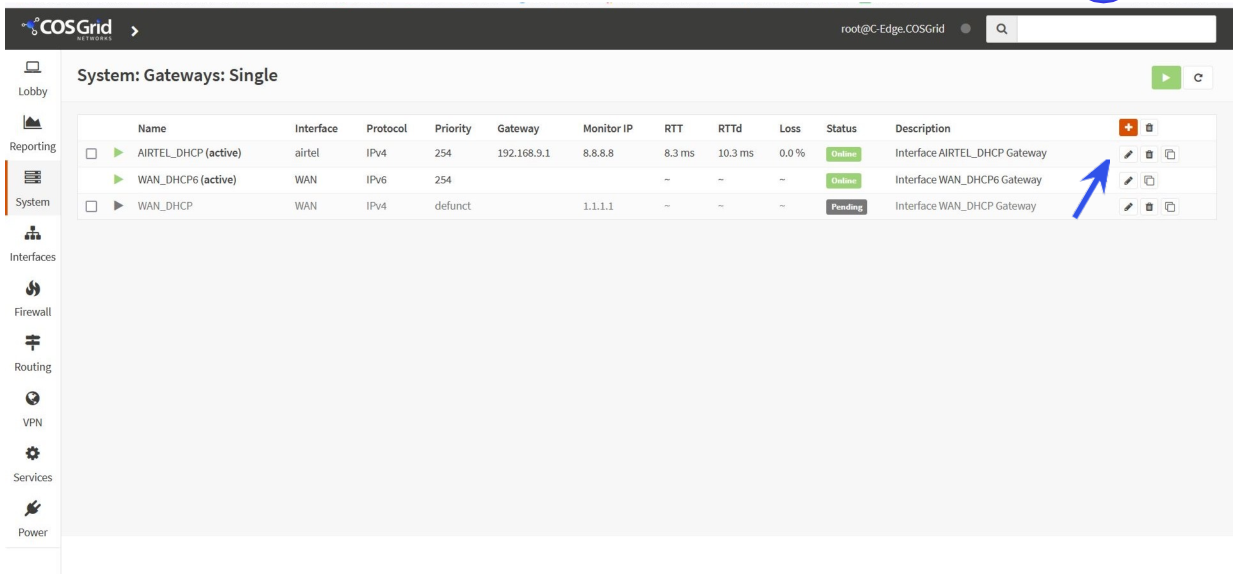
Add

42 - Load Balancing & ECMP

Go to ***System*** ‣ ***Gateways*** ‣ ***Configuration*** and click on the pencil symbol to edit the first gateway.

Now make sure the following is configured:

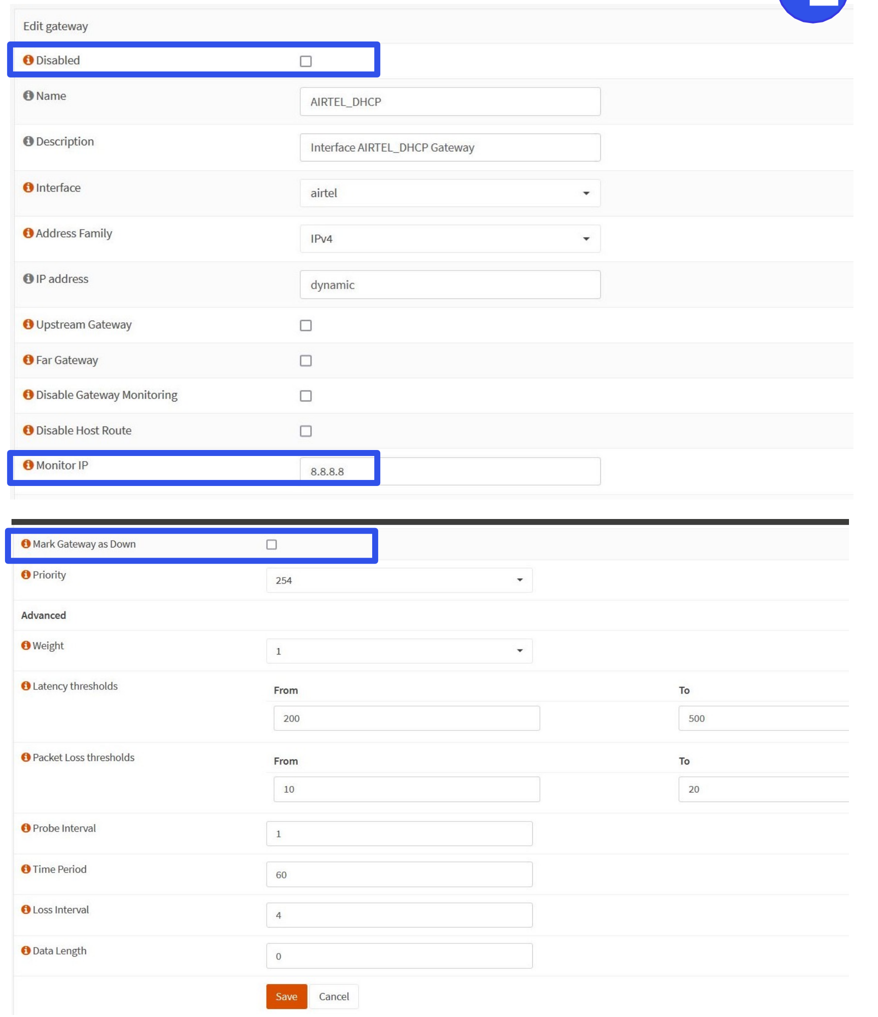
1



System: Gateways: Single

	Name	Interface	Protocol	Priority	Gateway	Monitor IP	RTT	RTTd	Loss	Status	Description
□	AIRTEL_DHCP **(active)**	airtel	IPv4	254	192.168.9.1	8.8.8.8	8.3 ms	10.3 ms	0.0 %	Online	Interface AIRTEL_DHCP Gateway
	WAN_DHCP6 **(active)**	WAN	IPv6	254			~	~	~	Online	Interface WAN_DHCP6 Gateway
□	WAN_DHCP	WAN	IPv4	defunct		1.1.1.1	~	~	~	Pending	Interface WAN_DHCP Gateway

2



Edit gateway

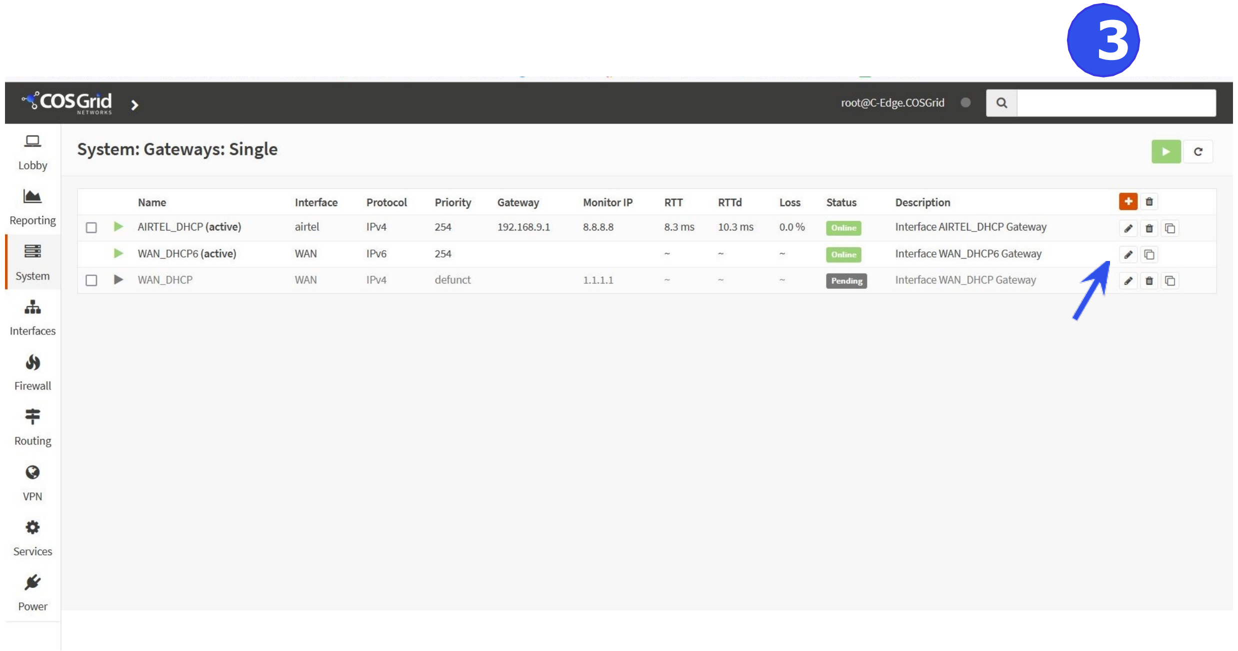
Disabled	□
Name	AIRTEL_DHCP
Description	Interface AIRTEL_DHCP Gateway
Interface	airtel
Address Family	IPv4
IP address	dynamic
Upstream Gateway	□
Far Gateway	□
Disable Gateway Monitoring	□
Disable Host Route	□
Monitor IP	8.8.8.8
Mark Gateway as Down	□
Priority	254
Advanced	
Weight	1
Latency thresholds	From 200 To 500
Packet Loss thresholds	From 10 To 20
Probe Interval	1
Time Period	60
Loss Interval	4
Data Length	0

Disable Gateway Monitoring	Unchecked	*Make гuгe moniĩoring iг enabled*
Monitor IP	8.8.8.8	*We uгe Google′г DNS*
Mark Gateway as Down	Unchecked	

42 - Load Balancing & ECMP

Go to *System* ▸ *Gateways* ▸ *Configuration* and click on the pencil symbol to edit the second gateway.

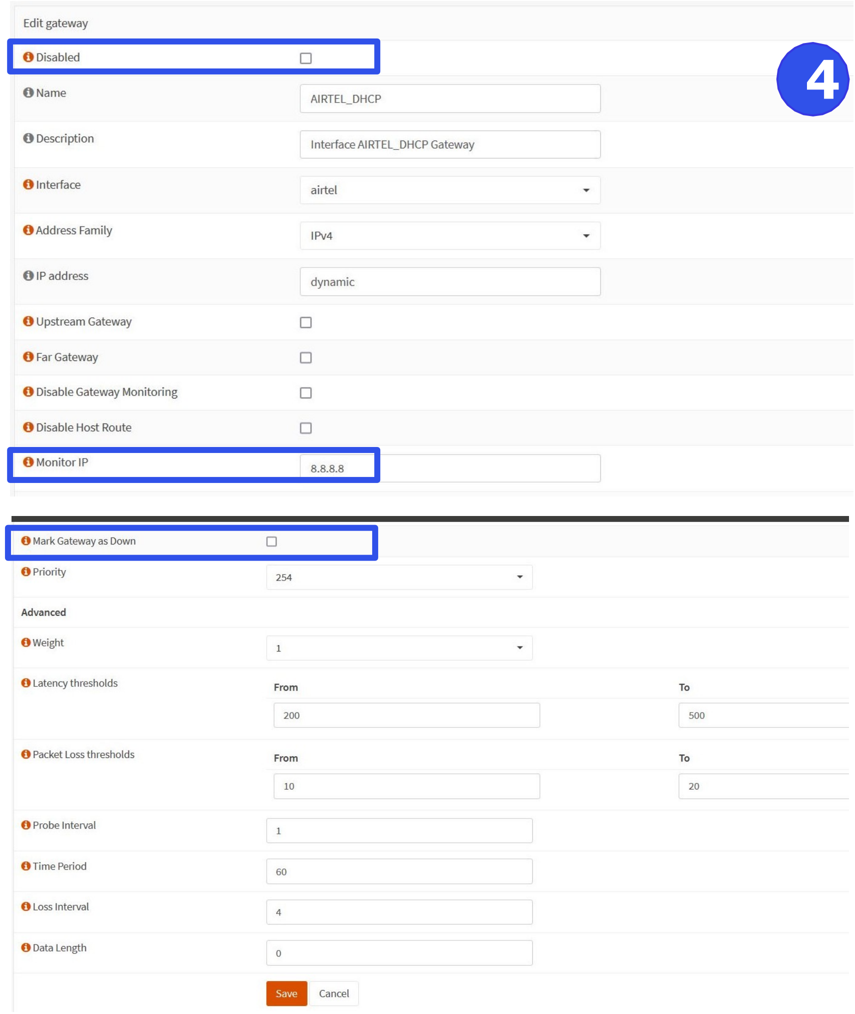
Now make sure the following is configured:



3

System: Gateways: Single

		Name	Interface	Protocol	Priority	Gateway	Monitor IP	RTT	RTTd	Loss	Status	Description
□	▶	AIRTEL_DHCP **(active)**	airtel	IPv4	254	192.168.9.1	8.8.8.8	8.3 ms	10.3 ms	0.0 %	Online	Interface AIRTEL_DHCP Gateway
	▶	WAN_DHCP6 **(active)**	WAN	IPv6	254			~	~	~	Online	Interface WAN_DHCP6 Gateway
□	▶	WAN_DHCP	WAN	IPv4	defunct		1.1.1.1	~	~	~	Pending	Interface WAN_DHCP Gateway



4

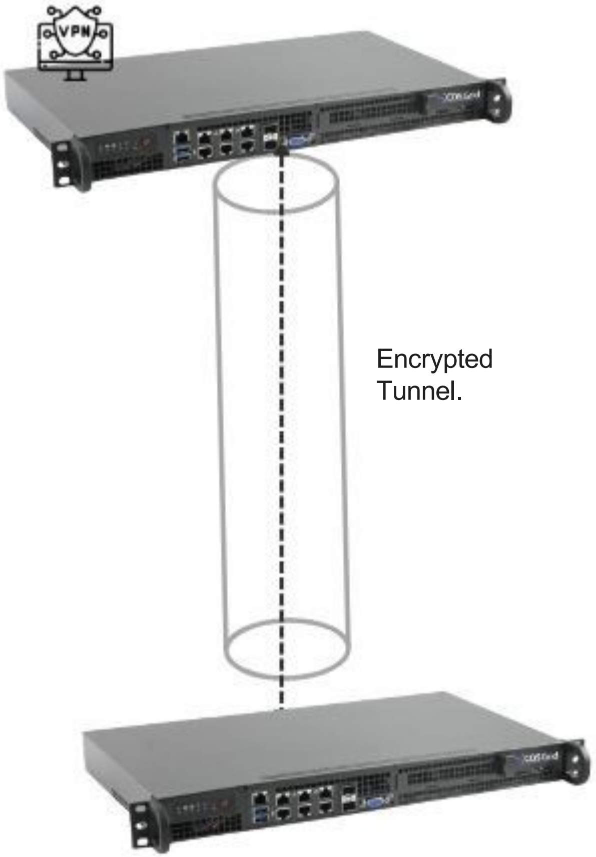
Edit gateway

Disabled	□	
Name	AIRTEL_DHCP	
Description	Interface AIRTEL_DHCP Gateway	
Interface	airtel	
Address Family	IPv4	
IP address	dynamic	
Upstream Gateway	□	
Far Gateway	□	
Disable Gateway Monitoring	□	
Disable Host Route	□	
Monitor IP	8.8.8.8	
Mark Gateway as Down	□	
Priority	254	
Advanced		
Weight	1	
Latency thresholds	From 200	To 500
Packet Loss thresholds	From 10	To 20
Probe Interval	1	
Time Period	60	
Loss Interval	4	
Data Length	0	

Disable Gateway Monitoring	Unchecked	*Make rure moniĭoring ir enabled*
Monitor IP	8.8.4.4	*We ure Google’r recond DNS*
Mark Gateway as Down	Unchecked	

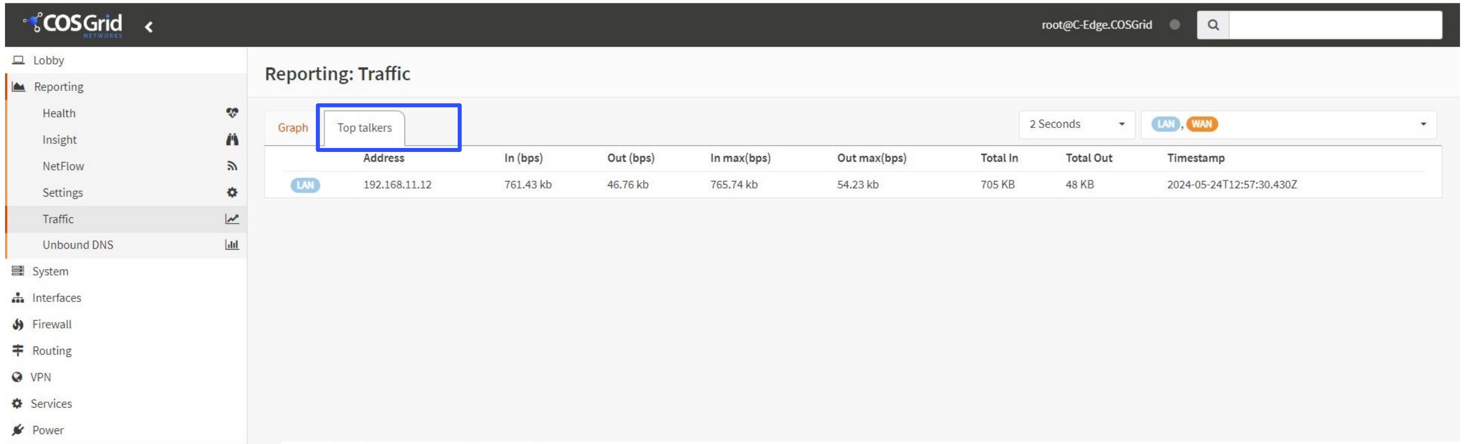
43 - Dynamic Routing Over VPN- OSPF

Set Steps	**Acceptance Criteria**
Configure the VPN -IpSec VPN To enable Routing Go to ***Routing > General.*** Then, Go to ***Routing > OSPF*** Configure a dynamic routing protocol -OSPF Test neighbor establishment, route exchange, and route convergence.	Successful creation of VPN connections enabled without errors or unexpected behavior. Should be able to configure routing with different functionalities like **CARP and AS Number.** Check the running configuration



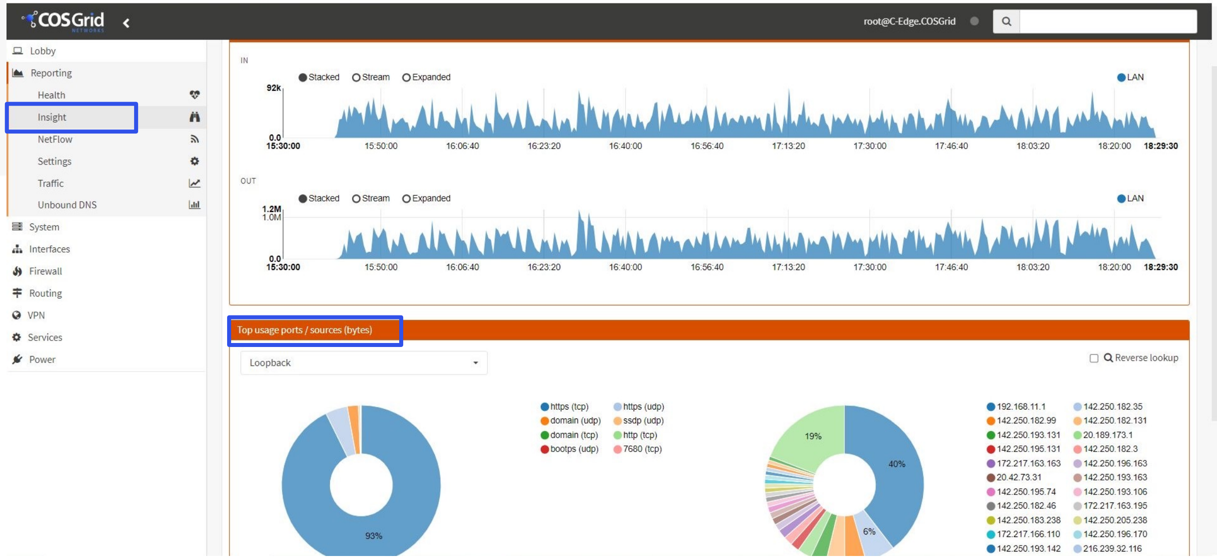
44 - Reporting & Visibility

Set Steps	Acceptance Criteria
Go to ***Reporting > Traffic > Top Talkers.*** Generate various types of network traffic	Detailed Network Visibility
Go to ***Reporting > Insight***.Utilize visual tools to observe traffic flows, including • Source and destination devices • Application types • Traffic volumes • Bandwidth utilization	Full network visibility of different interface traffic Clear and informative visual representations of network traffic flows.
Go to ***Reporting > Insight > Details***. Filter and drill down into specific traffic patterns for detailed analysis.	Should be able to use **filters** and see **detailed** traffic information.

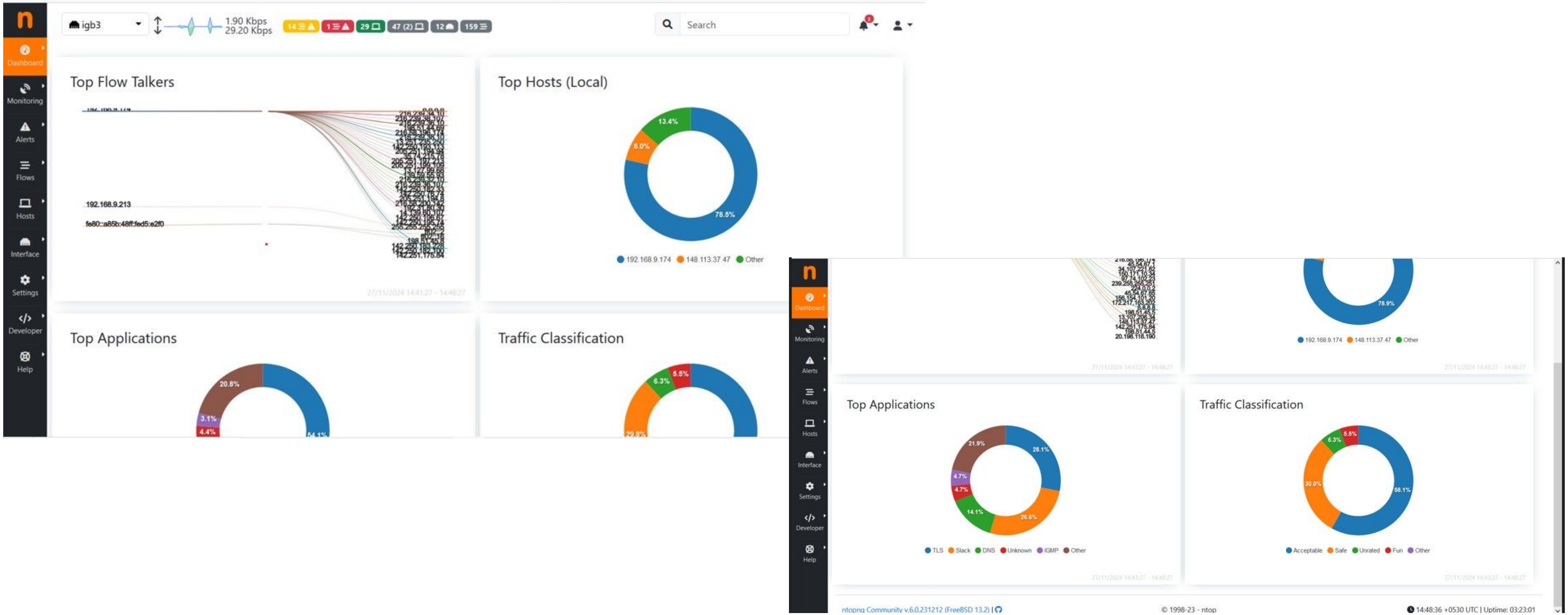


Reporting: Traffic

	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

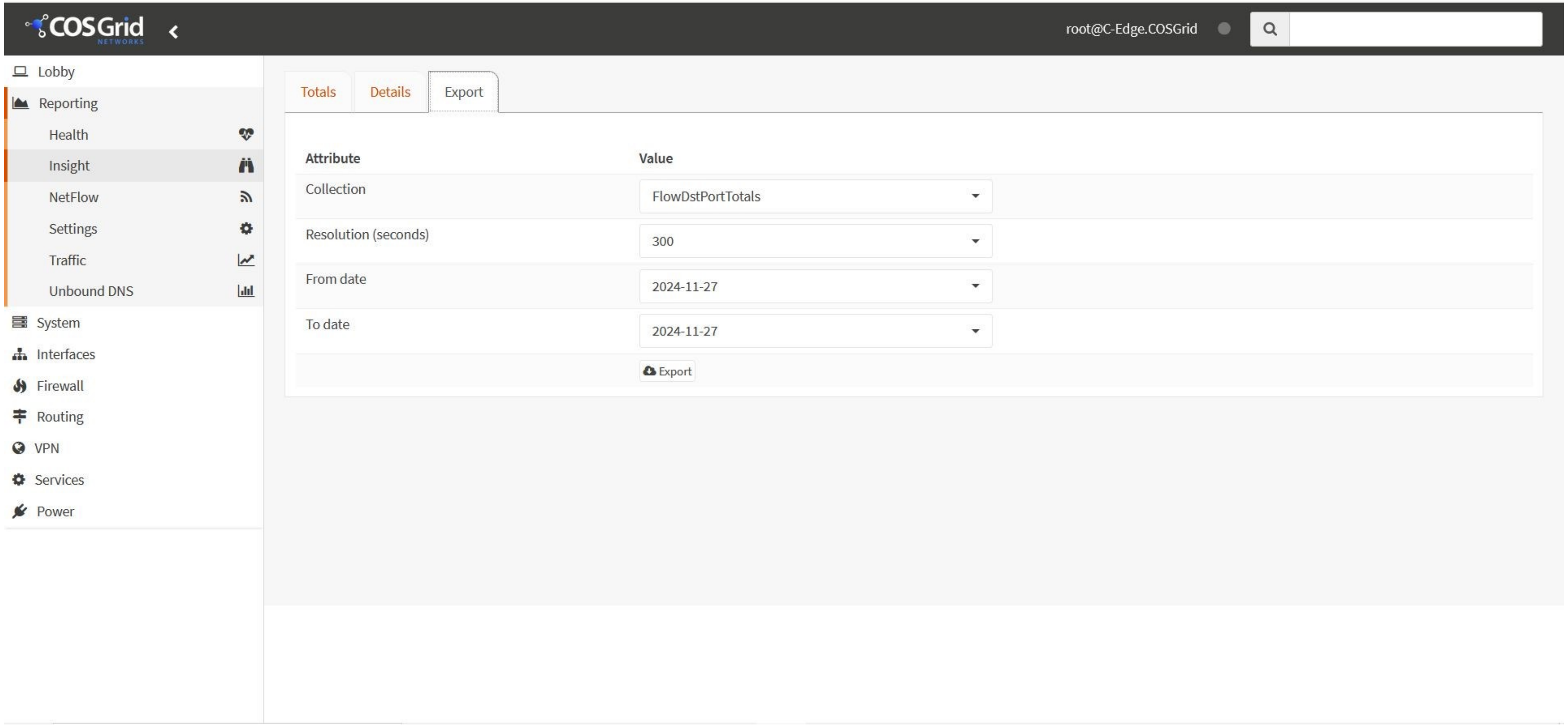


45 - Network Visibility



46 - Reporting- Export

Set Steps	**Acceptance Criteria**
Go to ***Reporting > Insight > Export***. Generate various types of reports available in the firewall (e.g., traffic logs, security events, policy violations, resource usage, performance metrics). Inspect the generated reports for accuracy and completeness of data.	Reports should be generated successfully **without errors or omissions**. The reports will be in **csv format** Data in reports should accurately reflect firewall activity and configuration.



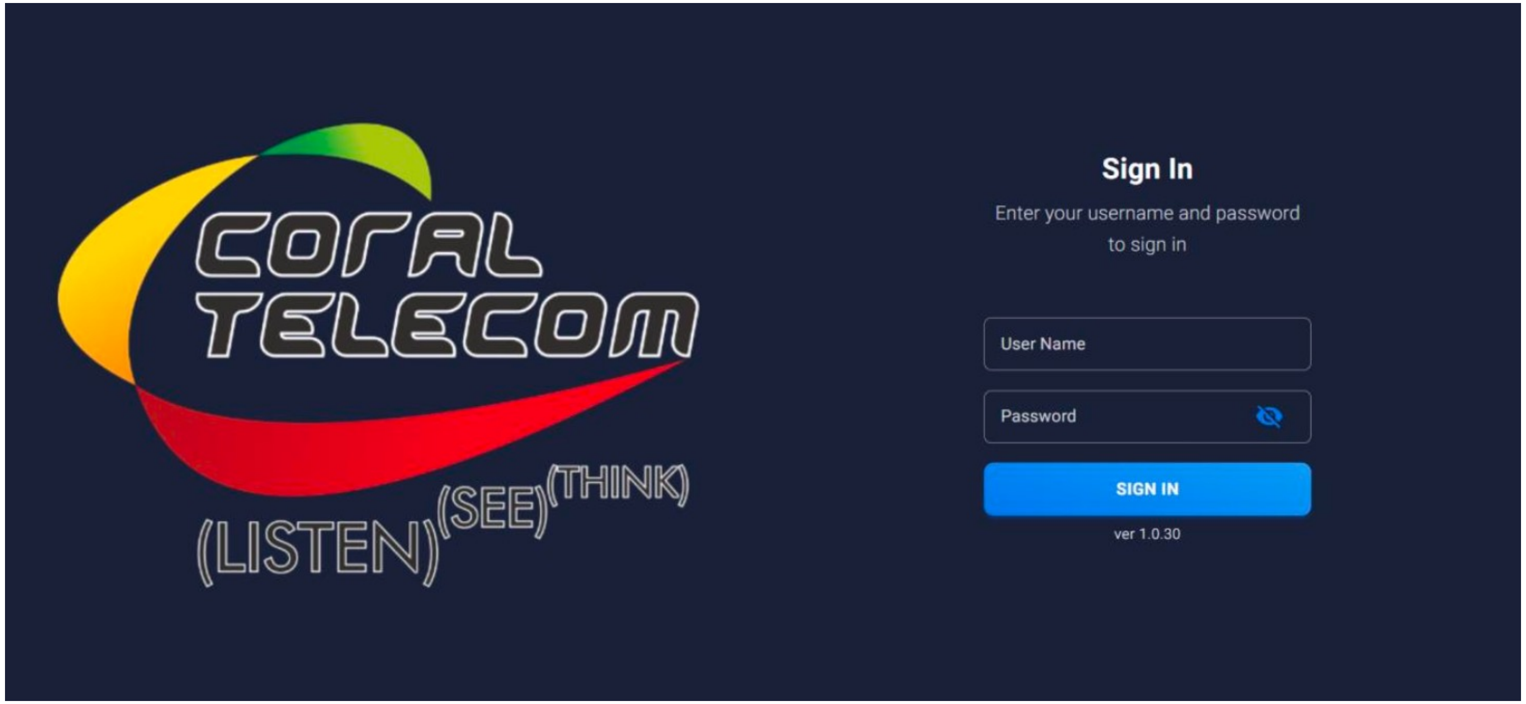
Attribute	Value
Collection	FlowDstPortTotals
Resolution (seconds)	300
From date	2024-11-27
To date	2024-11-27

5G LAB

NMS

Logging into the NMS

Step 1: - Open the URL with the Link
URL: - https://<virtual IP>
Step 2: - Login with the credentials
Username: - admin



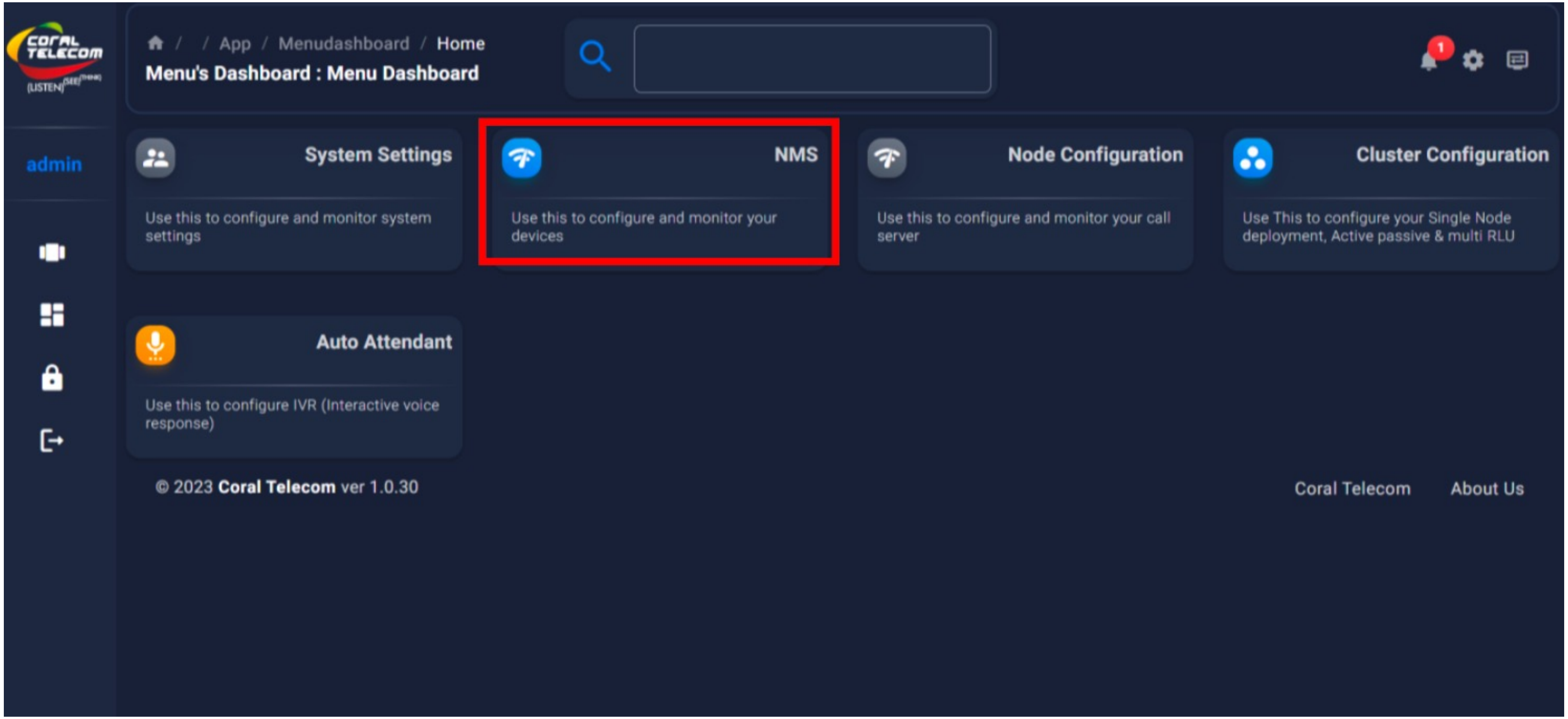
Sign In

Enter your username and password to sign in

User Name

Password

Dashboard opens up. Go to NMS



System Settings

Use this to configure and monitor system settings

NMS

Use this to configure and monitor your devices

Node Configuration

Use this to configure and monitor your call server

Cluster Configuration

Use This to configure your Single Node deployment, Active passive & multi RLU

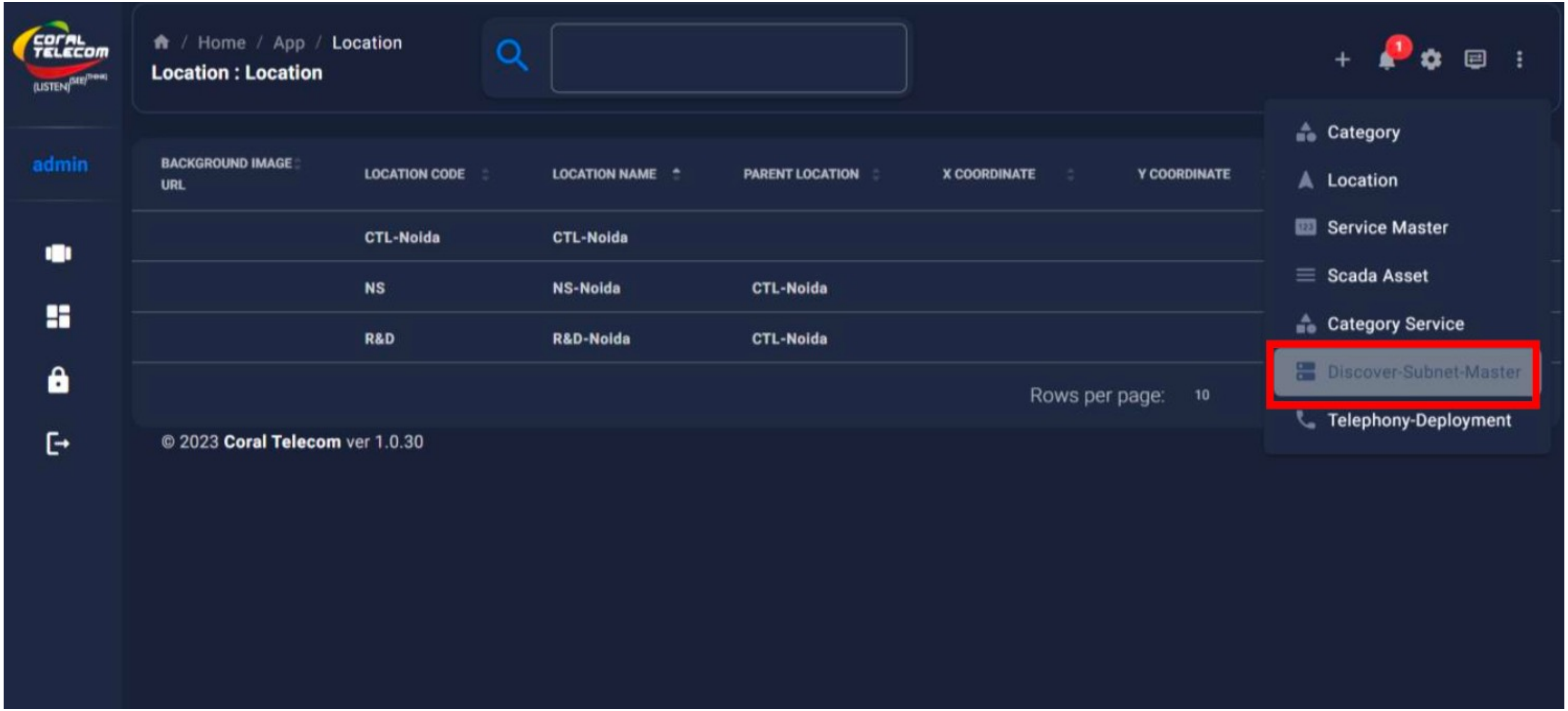
Auto Attendant

Use this to configure IVR (Interactive voice response)

© 2023 **Coral Telecom** ver 1.0.30

Coral Telecom About Us

- go to **Discovery-Subnet- Master –** To auto discover all the available elements in the network

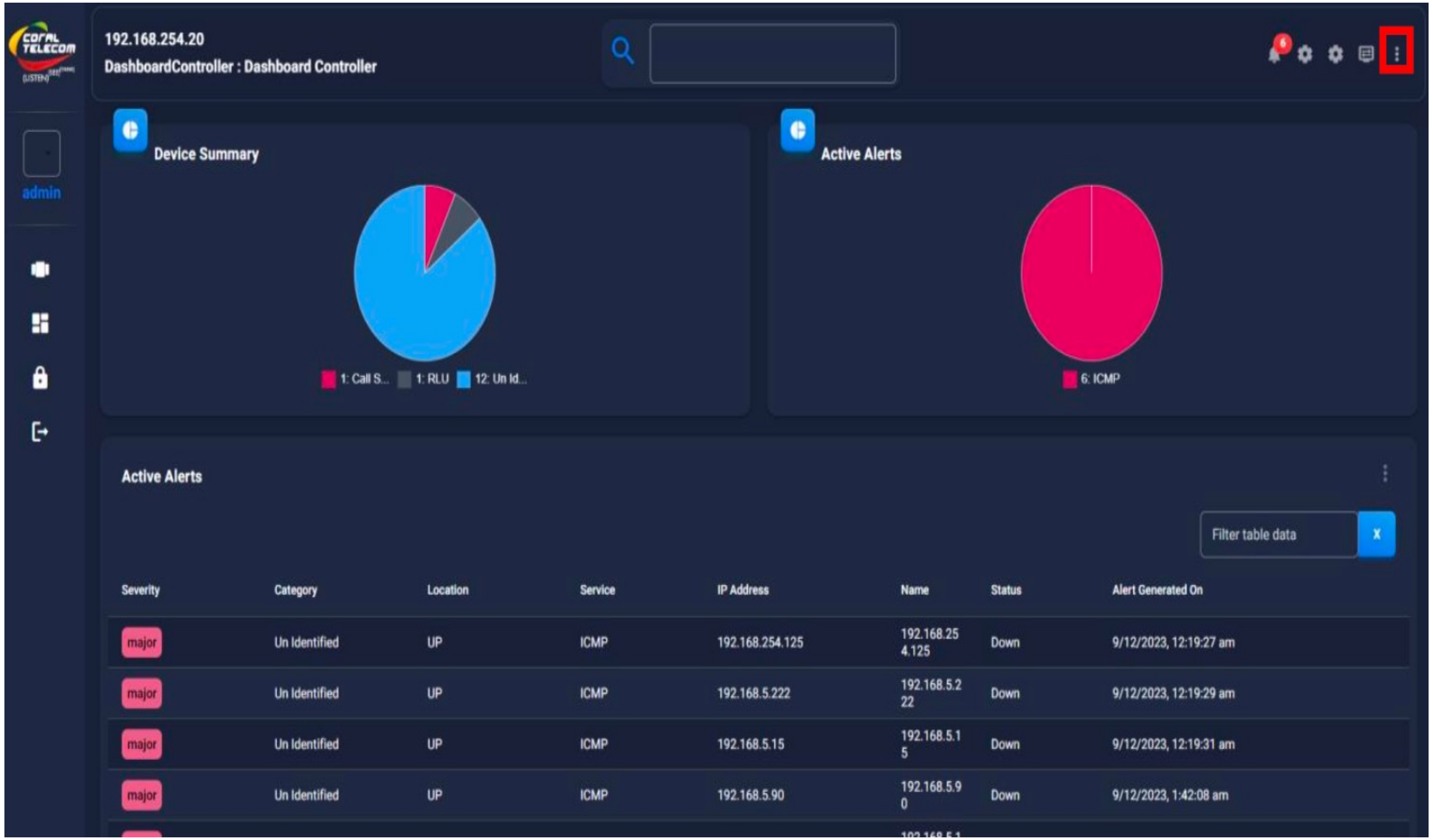


Location : Location

BACKGROUND IMAGE URL	LOCATION CODE	LOCATION NAME	PARENT LOCATION	X COORDINATE	Y COORDINATE
	CTL-Noida	CTL-Noida			
	NS	NS-Noida	CTL-Noida		
	R&D	R&D-Noida	CTL-Noida		

Rows per page: 10

© 2023 Coral Telecom ver 1.0.30

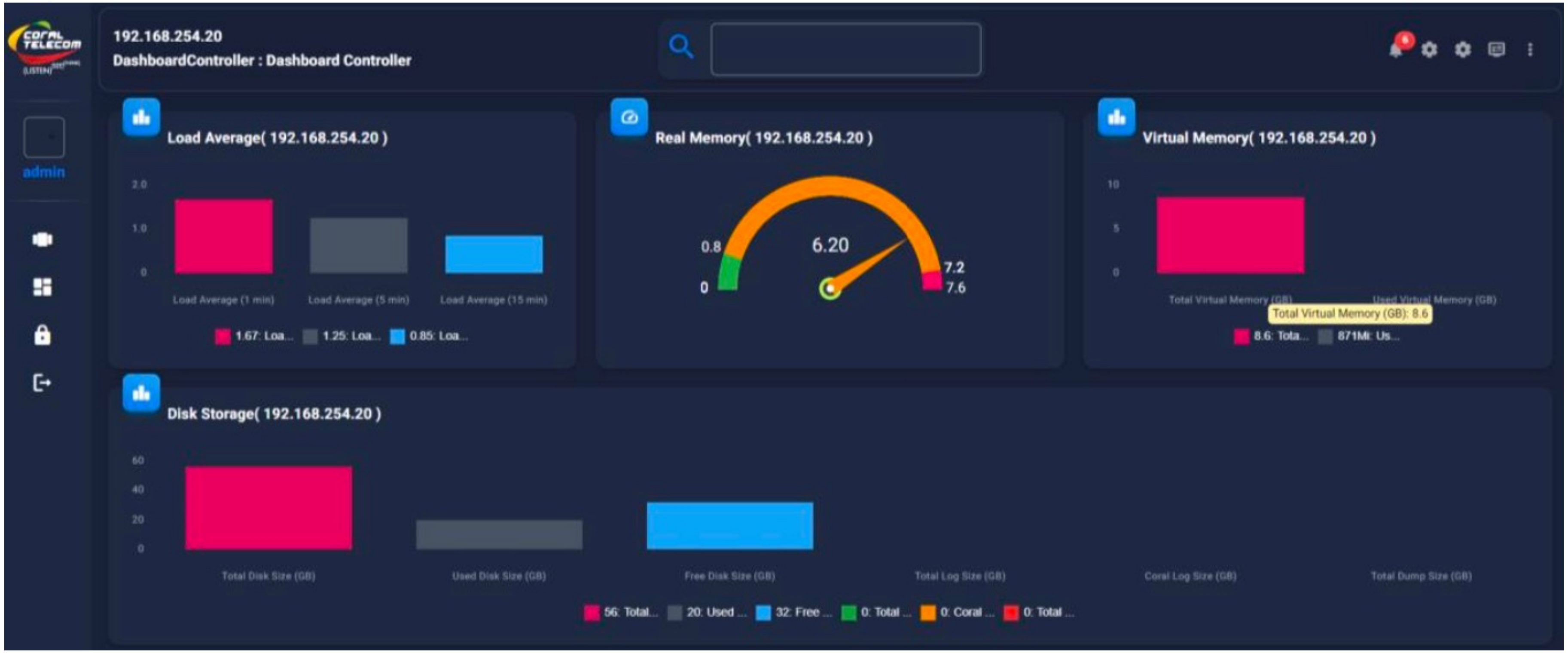


Active Alerts

Severity	Category	Location	Service	IP Address	Name	Status	Alert Generated On
major	Un Identified	UP	ICMP	192.168.254.125	192.168.254.125	Down	9/12/2023, 12:19:27 am
major	Un Identified	UP	ICMP	192.168.5.222	192.168.5.222	Down	9/12/2023, 12:19:29 am
major	Un Identified	UP	ICMP	192.168.5.15	192.168.5.15	Down	9/12/2023, 12:19:31 am
major	Un Identified	UP	ICMP	192.168.5.90	192.168.5.90	Down	9/12/2023, 1:42:08 am

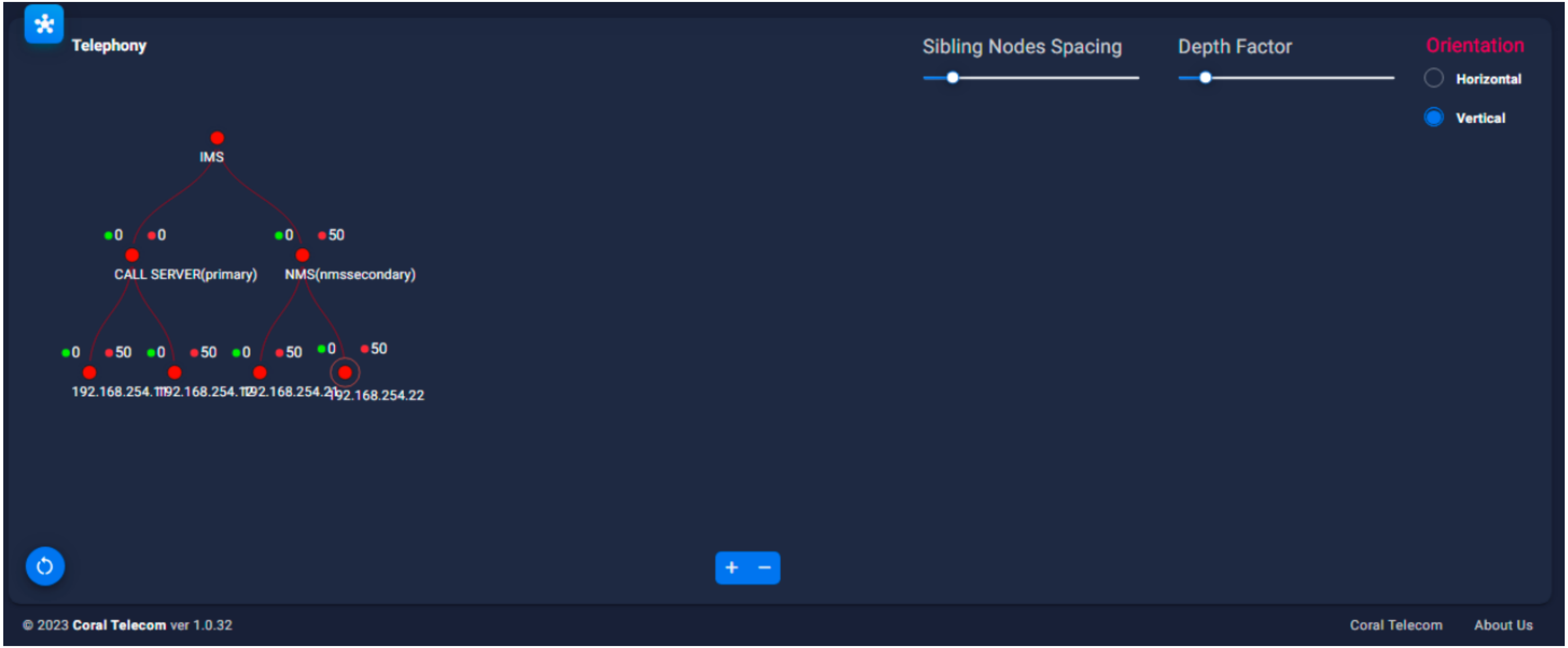
- **Servers Health Graph**
- **Step 1: -** Check for the cluster key in coral file as above
- **Step 2: -** Now define the Servers Physical IP as Call server in the Category
- **Step 3: -** Open NMS Dashboard. Click on the three dots on right hand side

Dashboard- system Health Status



192.168.254.20
DashboardController : Dashboard Controller

Topology View of NMS



Telephony

Sibling Nodes Spacing

Depth Factor

Orientation

○ Horizontal

● Vertical

© 2023 **Coral Telecom** ver 1.0.32

Coral Telecom

About Us

Live Training on NMS

Testing
&
Tracing Tools

Wireshark

Context

Introduction

- Wireshark – A Powerful Network Analysis Tool

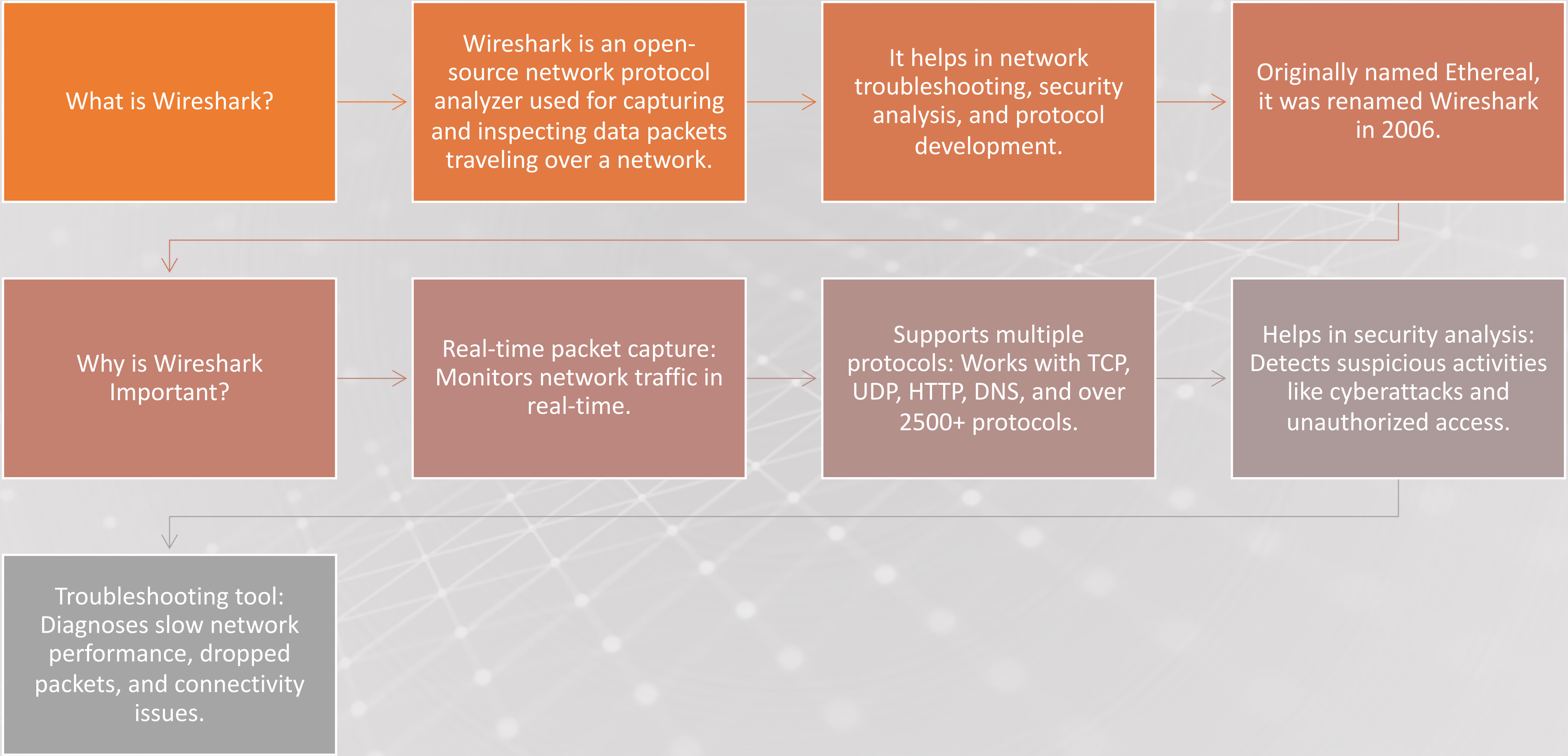
Features and functionalities

- Key Features of Wireshark
- Functionalities of Wireshark

Log analysis

- WireShark Packet-Capture

Wireshark – A Powerful Network Analysis Tool



What is Wireshark?

Wireshark is an open-source network protocol analyzer used for capturing and inspecting data packets traveling over a network.

It helps in network troubleshooting, security analysis, and protocol development.

Originally named Ethereal, it was renamed Wireshark in 2006.

Why is Wireshark Important?

Real-time packet capture: Monitors network traffic in real-time.

Supports multiple protocols: Works with TCP, UDP, HTTP, DNS, and over 2500+ protocols.

Helps in security analysis: Detects suspicious activities like cyberattacks and unauthorized access.

Troubleshooting tool: Diagnoses slow network performance, dropped packets, and connectivity issues.

Features & Functionalities of Wireshark: Key Features of Wireshark

- **Key Features of Wireshark**
- **1. Real-Time Packet Capture:**
  - Captures live network traffic from various interfaces (Ethernet, Wi-Fi, etc.).
  - Allows users to analyze packet data in real time.
- **2. Protocol Support:**
  - Supports over **2500+ network protocols** including TCP, UDP, HTTP, DNS, and more.
  - Automatically detects and decodes protocol structures.
- **3. Advanced Filtering Options:**
  - **Display Filters:** Used to focus on specific packets (e.g., tcp.port == 80).
  - **Capture Filters:** Helps reduce the volume of data collected at capture time.
  - **Color Coding:** Highlights different types of traffic for easy identification.

Features & Functionalities of Wireshark: Functionalities of Wireshark

- **1. Deep Packet Inspection:**

  Examines packet headers and payloads for detailed analysis.
  Helps in diagnosing network and security issues.

- **2. Packet Reconstruction & Export:**

  Rebuilds entire network sessions for analysis.
  Exports data in formats like **PCAP, JSON, CSV, and XML**.

- **3. Security & Network Troubleshooting:**

  Detects network anomalies, dropped packets, and latency issues.
  Identifies **suspicious activities** like unauthorized access and cyberattacks.
  Helps in forensic investigation and penetration testing.

- **Conclusion:** Wireshark is an essential tool for network engineers, security analysts, and IT professionals. Its **powerful filtering, protocol analysis, and security features** make it indispensable for troubleshooting and monitoring networks.

Logs Analysis : WireShark Packet-Capture

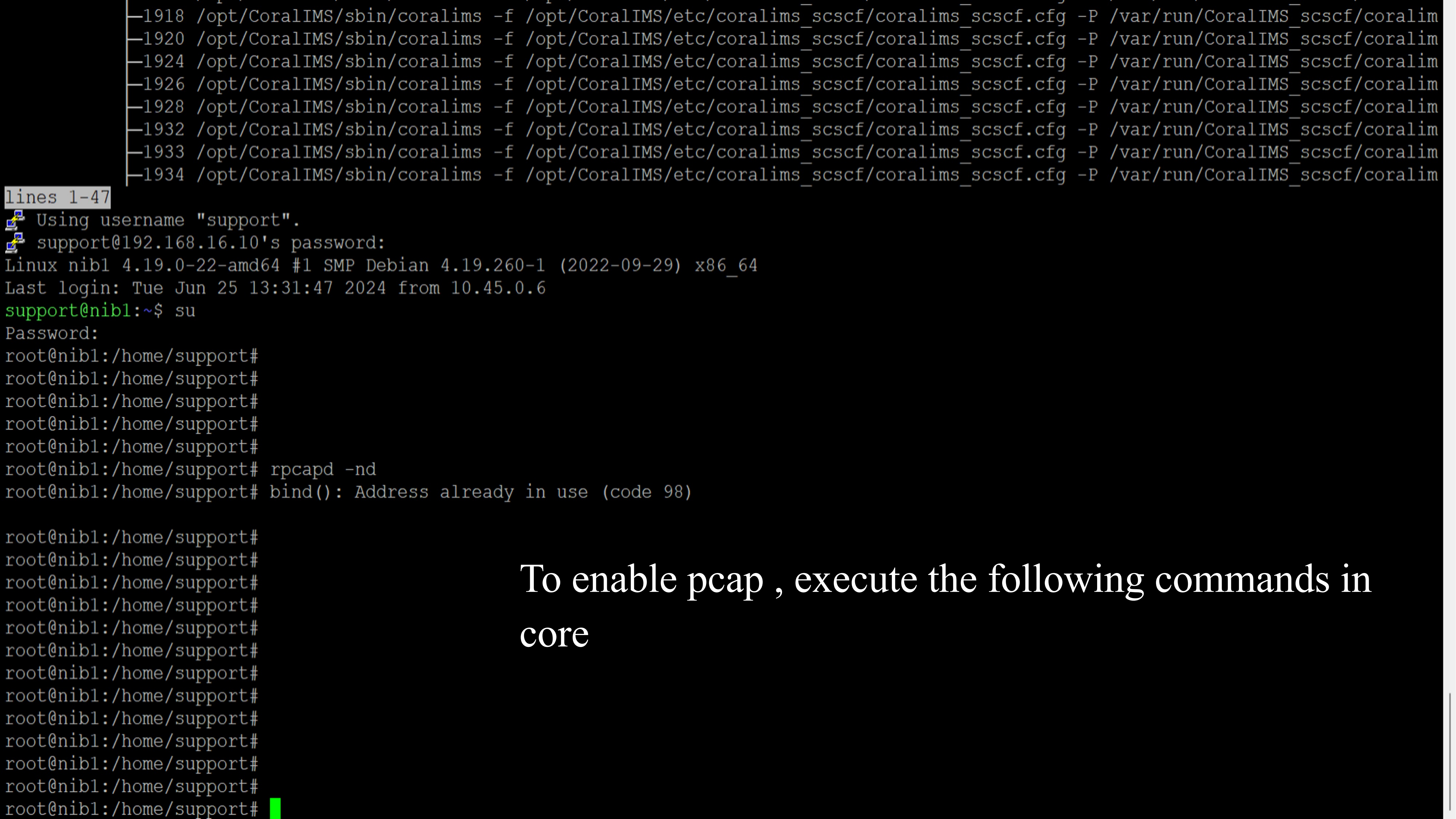
- **What is Log Analysis in Wireshark?**

  Log analysis in Wireshark involves **analyzing captured network packets** to diagnose network issues and detect security threats.
  Every network packet is logged and can be inspected for anomalies, dropped connections, and performance bottlenecks.

- **Why is Packet Capture Important?**

  Helps in troubleshooting **slow connections, packet loss, and unauthorized access**.
  Assists in **security analysis** by identifying unusual traffic patterns.
  Provides detailed insights into network behavior and communication protocols.

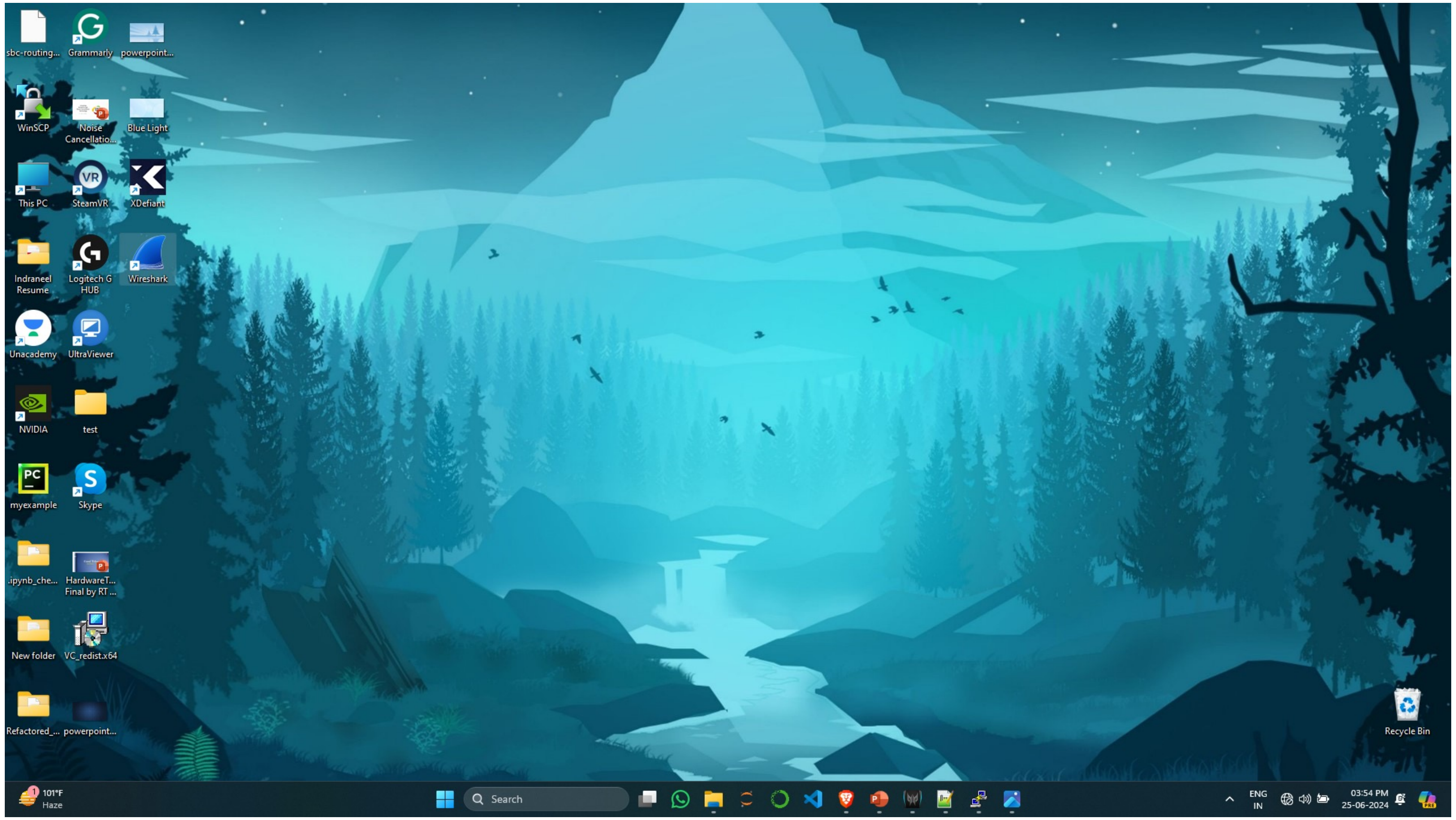
- NOTE: Before starting the wireshark application and continue with packet tracing make sure to ncap command on the 5G Core

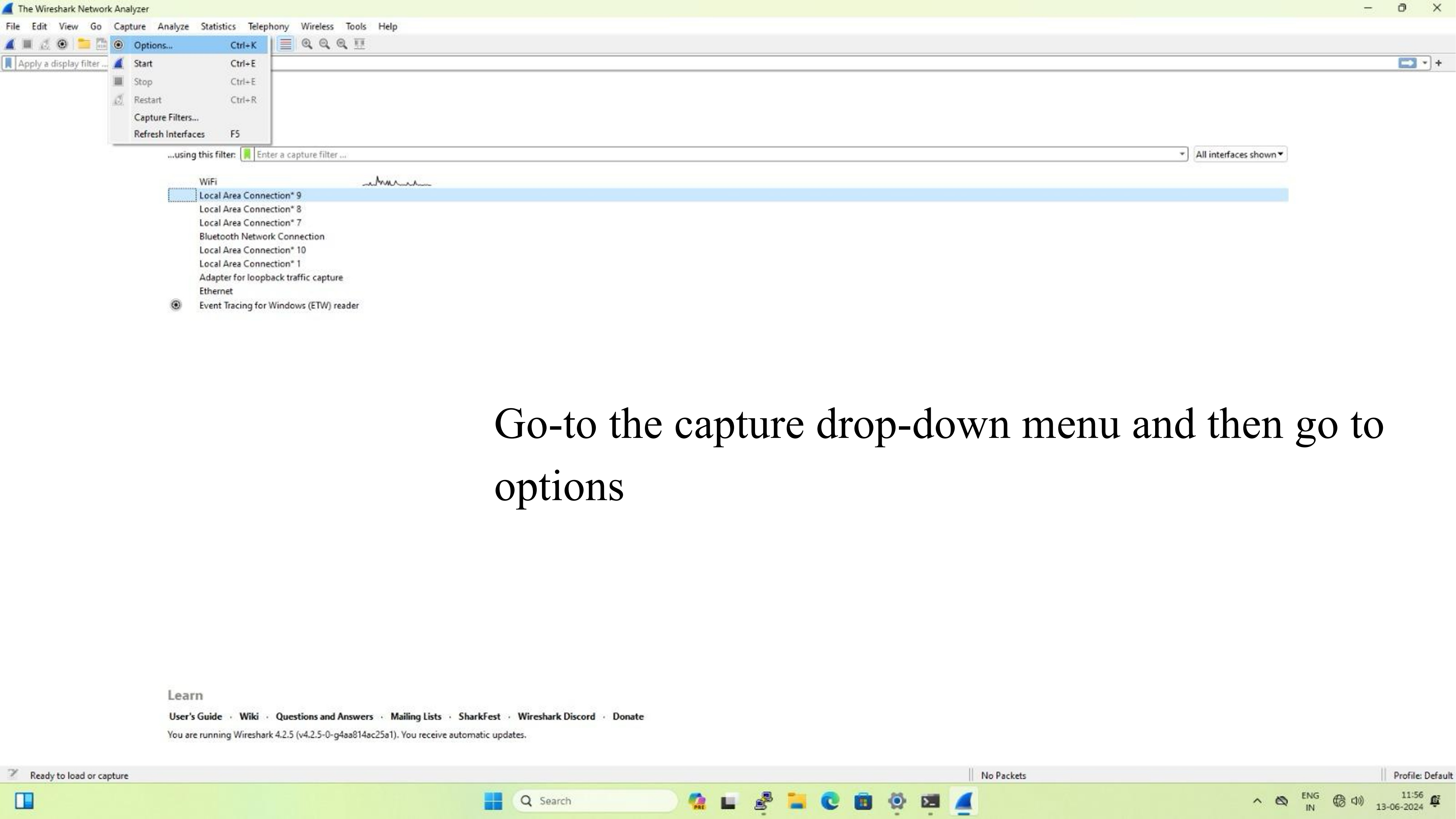


```
          ├─1918 /opt/CoralIMS/sbin/coralims -f /opt/CoralIMS/etc/coralims_scscf/coralims_scscf.cfg -P /var/run/CoralIMS_scscf/coralim
          ├─1920 /opt/CoralIMS/sbin/coralims -f /opt/CoralIMS/etc/coralims_scscf/coralims_scscf.cfg -P /var/run/CoralIMS_scscf/coralim
          ├─1924 /opt/CoralIMS/sbin/coralims -f /opt/CoralIMS/etc/coralims_scscf/coralims_scscf.cfg -P /var/run/CoralIMS_scscf/coralim
          ├─1926 /opt/CoralIMS/sbin/coralims -f /opt/CoralIMS/etc/coralims_scscf/coralims_scscf.cfg -P /var/run/CoralIMS_scscf/coralim
          ├─1928 /opt/CoralIMS/sbin/coralims -f /opt/CoralIMS/etc/coralims_scscf/coralims_scscf.cfg -P /var/run/CoralIMS_scscf/coralim
          ├─1932 /opt/CoralIMS/sbin/coralims -f /opt/CoralIMS/etc/coralims_scscf/coralims_scscf.cfg -P /var/run/CoralIMS_scscf/coralim
          ├─1933 /opt/CoralIMS/sbin/coralims -f /opt/CoralIMS/etc/coralims_scscf/coralims_scscf.cfg -P /var/run/CoralIMS_scscf/coralim
          ├─1934 /opt/CoralIMS/sbin/coralims -f /opt/CoralIMS/etc/coralims_scscf/coralims_scscf.cfg -P /var/run/CoralIMS_scscf/coralim
lines 1-47
  Using username "support".
  support@192.168.16.10's password:
Linux nib1 4.19.0-22-amd64 #1 SMP Debian 4.19.260-1 (2022-09-29) x86_64
Last login: Tue Jun 25 13:31:47 2024 from 10.45.0.6
support@nib1:~$ su
Password:
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support# rpcapd -nd
root@nib1:/home/support# bind(): Address already in use (code 98)

root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
root@nib1:/home/support#
```

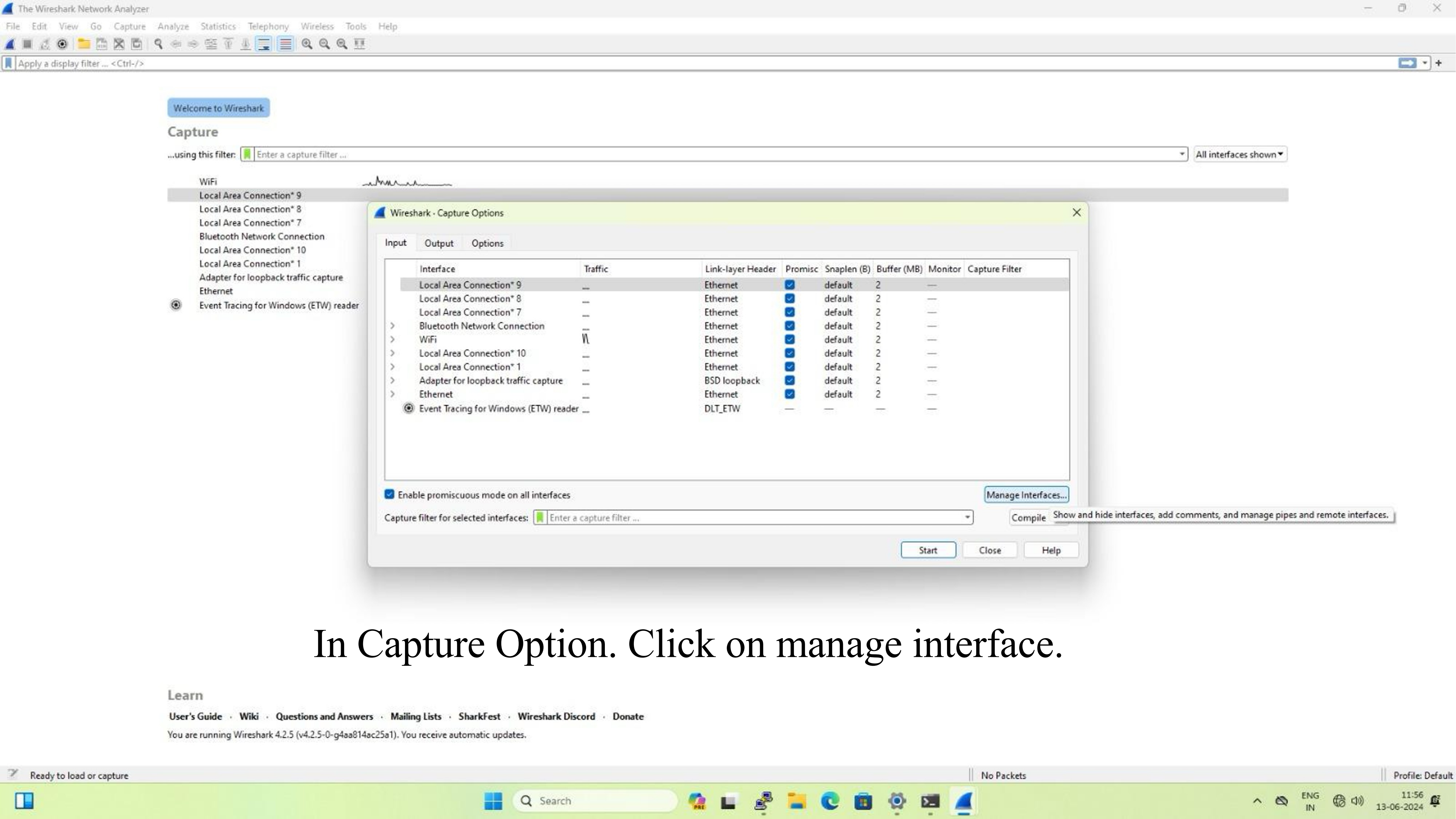
To enable pcap , execute the following commands in core

Double-click on WIRESHARK icon to open it




The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
Apply a display filter ...
...using this filter: Enter a capture filter ...
All interfaces shown
WiFi
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
Local Area Connection* 10
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.5 (v4.2.5-0-g4aa814ac25a1). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
Search
ENG IN
11:56
13-06-2024

Go-to the capture drop-down menu and then go to options



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
WiFi
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
Local Area Connection* 10
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
Event Tracing for Windows (ETW) reader
Wireshark · Capture Options
Input
Output
Options

Interface	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
Local Area Connection* 9		Ethernet	☑	default	2	—	
Local Area Connection* 8		Ethernet	☑	default	2	—	
Local Area Connection* 7		Ethernet	☑	default	2	—	
Bluetooth Network Connection		Ethernet	☑	default	2	—	
WiFi		Ethernet	☑	default	2	—	
Local Area Connection* 10		Ethernet	☑	default	2	—	
Local Area Connection* 1		Ethernet	☑	default	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	
Ethernet		Ethernet	☑	default	2	—	
Event Tracing for Windows (ETW) reader		DLT_ETW	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

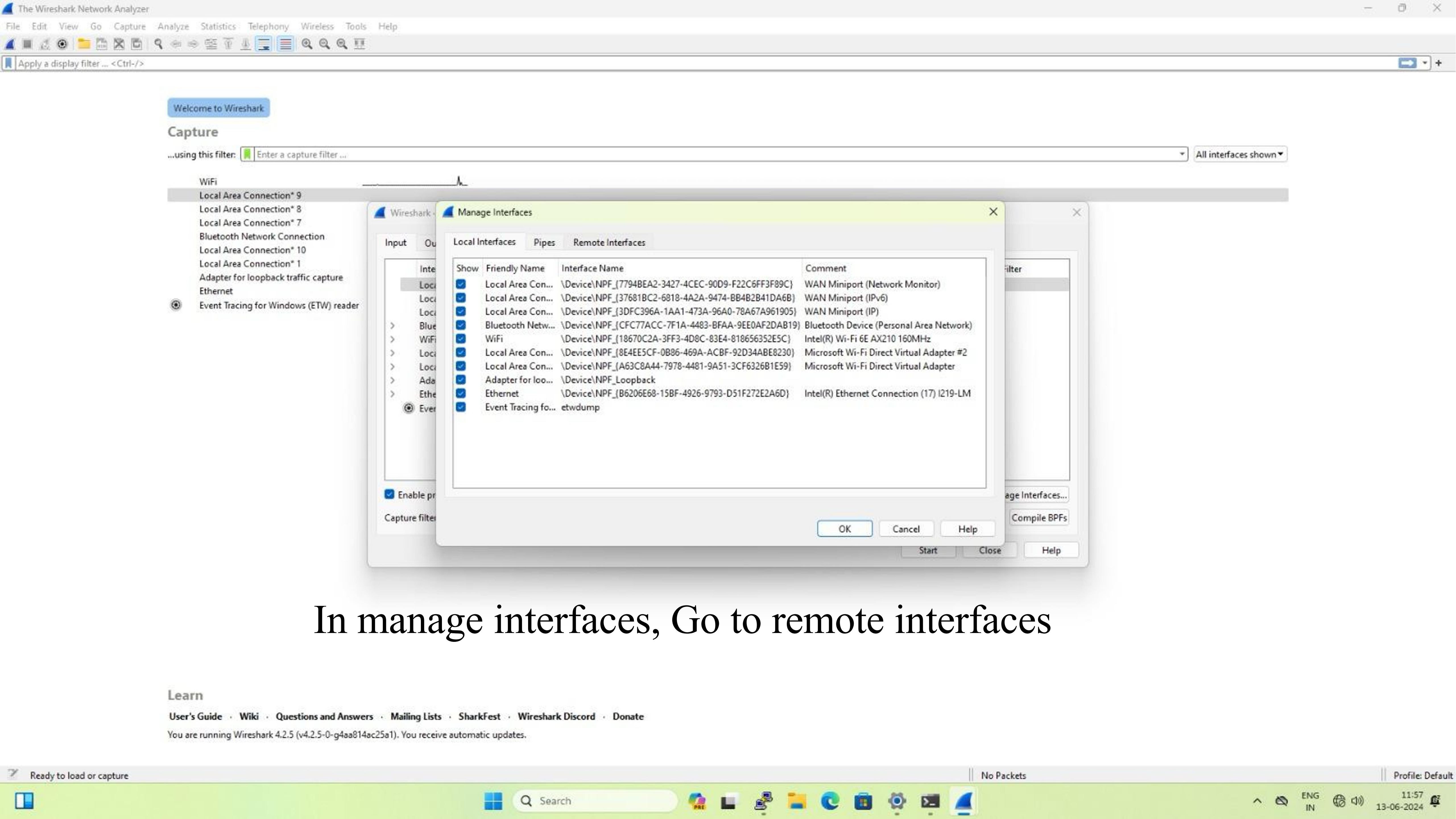
Capture filter for selected interfaces: Enter a capture filter ...

Manage Interfaces...
Compile
Show and hide interfaces, add comments, and manage pipes and remote interfaces.
Start
Close
Help

In Capture Option. Click on manage interface.

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.5 (v4.2.5-0-g4aa814ac25a1). You receive automatic updates.



WiFi
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
Local Area Connection* 10
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
Event Tracing for Windows (ETW) reader

Show	Friendly Name	Interface Name	Comment
☑	Local Area Con...	\Device\NPF_{7794BEA2-3427-4CEC-90D9-F22C6FF3F89C}	WAN Miniport (Network Monitor)
☑	Local Area Con...	\Device\NPF_{37681BC2-6818-4A2A-9474-BB4B2B41DA6B}	WAN Miniport (IPv6)
☑	Local Area Con...	\Device\NPF_{3DFC396A-1AA1-473A-96A0-78A67A961905}	WAN Miniport (IP)
☑	Bluetooth Netw...	\Device\NPF_{CFC77ACC-7F1A-4483-BFAA-9EE0AF2DAB19}	Bluetooth Device (Personal Area Network)
☑	WiFi	\Device\NPF_{18670C2A-3FF3-4D8C-83E4-818656352E5C}	Intel(R) Wi-Fi 6E AX210 160MHz
☑	Local Area Con...	\Device\NPF_{8E4EE5CF-0B86-469A-ACBF-92D34ABE8230}	Microsoft Wi-Fi Direct Virtual Adapter #2
☑	Local Area Con...	\Device\NPF_{A63C8A44-7978-4481-9A51-3CF6326B1E59}	Microsoft Wi-Fi Direct Virtual Adapter
☑	Adapter for loo...	\Device\NPF_Loopback	
☑	Ethernet	\Device\NPF_{B6206E68-15BF-4926-9793-D51F272E2A6D}	Intel(R) Ethernet Connection (17) I219-LM
☑	Event Tracing fo...	etwdump	

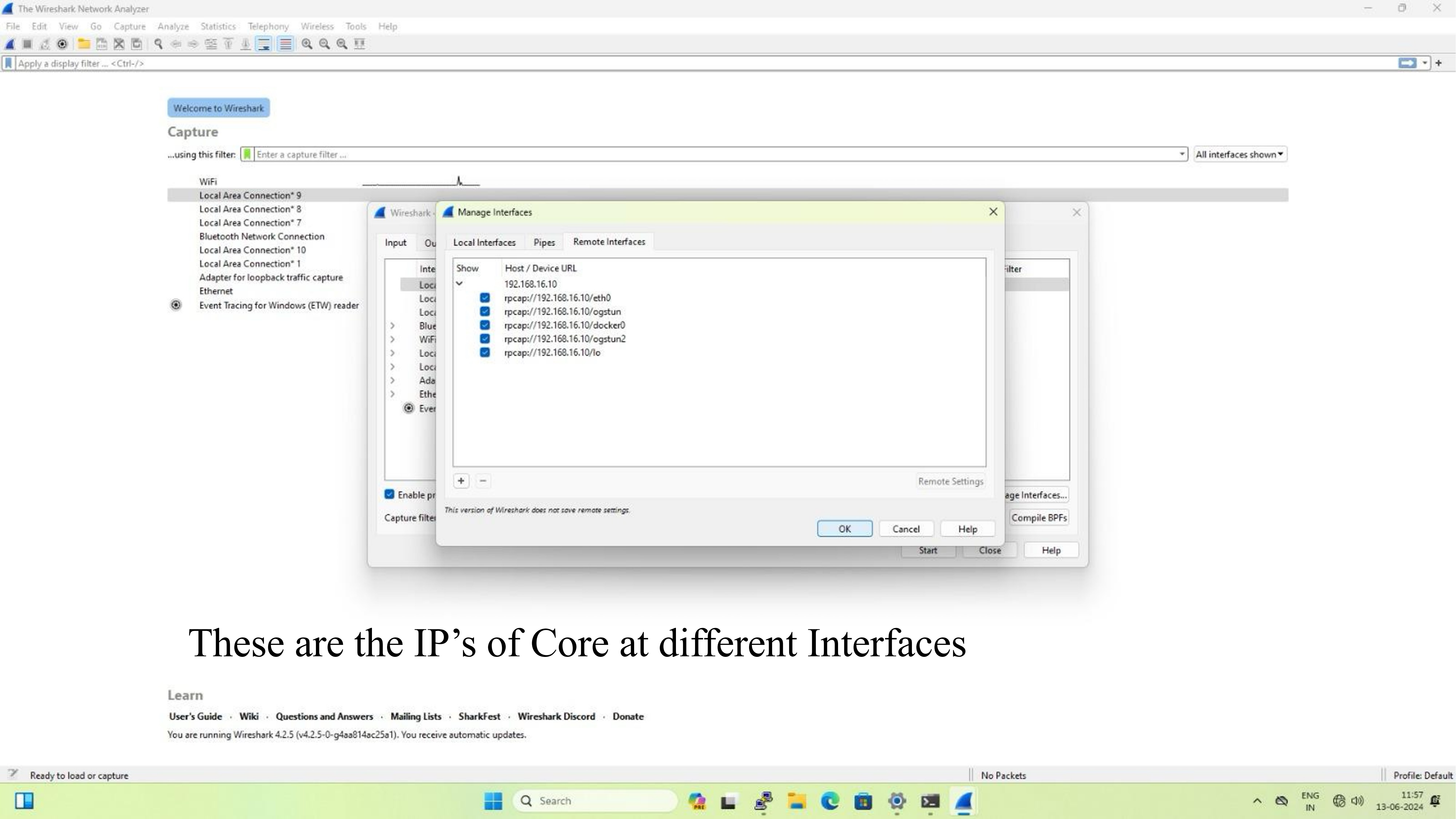
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.5 (v4.2.5-0-g4aa814ac25a1). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

In manage interfaces, Go to remote interfaces


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Input
Ou
Inte
Enable pr
Capture filte
ilter
age Interfaces...
Compile BPFs
Start
Close
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default
Search
ENG IN
11:57
13-06-2024

WiFi
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
Local Area Connection* 10
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
Event Tracing for Windows (ETW) reader

Manage Interfaces

Local Interfaces | Pipes | Remote Interfaces

Show	Host / Device URL
	192.168.16.10
☑	rpcap://192.168.16.10/eth0
☑	rpcap://192.168.16.10/ogstun
☑	rpcap://192.168.16.10/docker0
☑	rpcap://192.168.16.10/ogstun2
☑	rpcap://192.168.16.10/lo

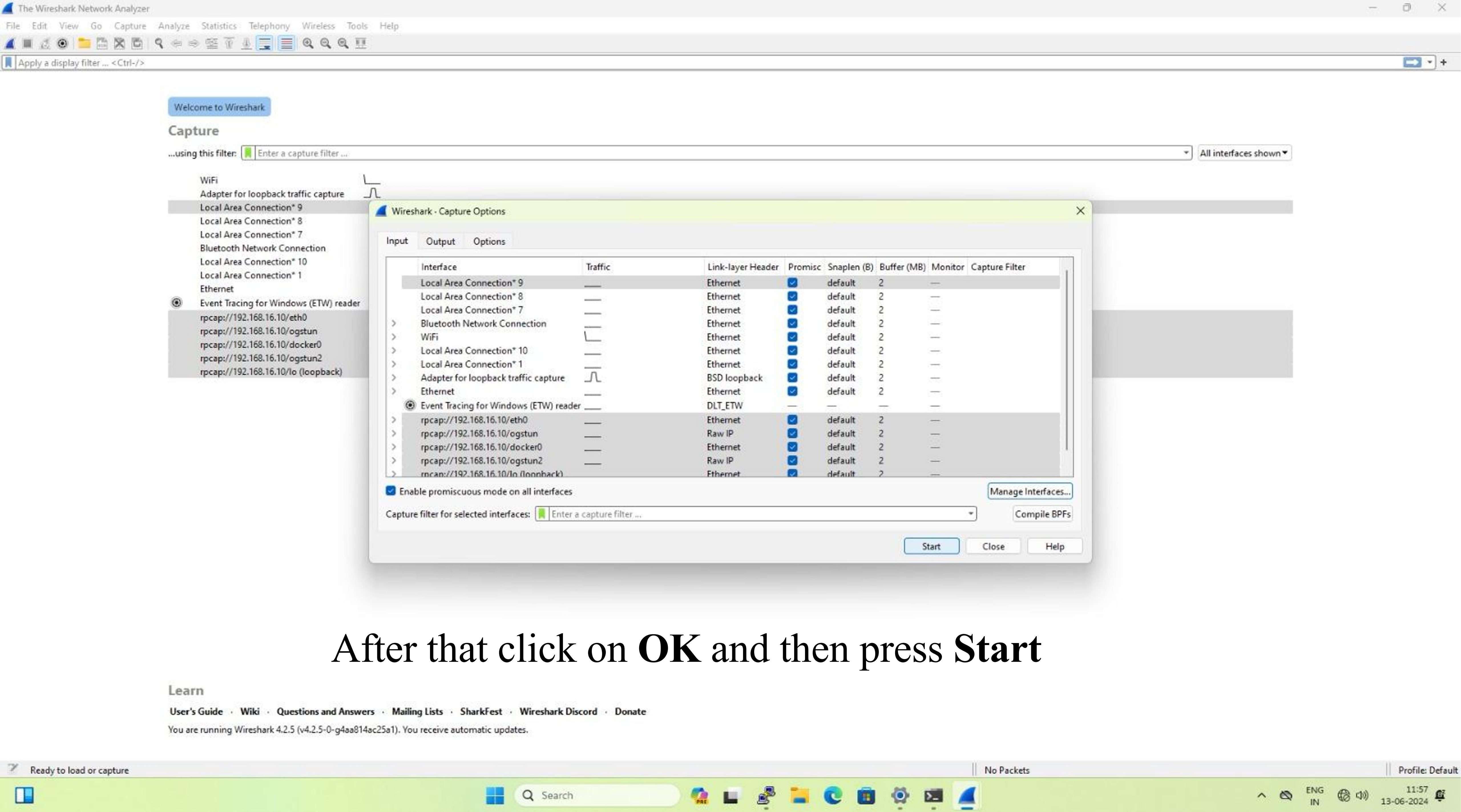
+ − Remote Settings

This version of Wireshark does not save remote settings.

OK Cancel Help

These are the IP’s of Core at different Interfaces

You are running Wireshark 4.2.5 (v4.2.5-0-g4aa814ac25a1). You receive automatic updates.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default
Search
ENG IN
11:57
13-06-2024

WiFi
Adapter for loopback traffic capture
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
Local Area Connection* 10
Local Area Connection* 1
Ethernet
Event Tracing for Windows (ETW) reader
rpcap://192.168.16.10/eth0
rpcap://192.168.16.10/ogstun
rpcap://192.168.16.10/docker0
rpcap://192.168.16.10/ogstun2
rpcap://192.168.16.10/lo (loopback)

You are running Wireshark 4.2.5 (v4.2.5-0-g4aa814ac25a1). You receive automatic updates.

Wireshark · Capture Options

Input | Output | Options

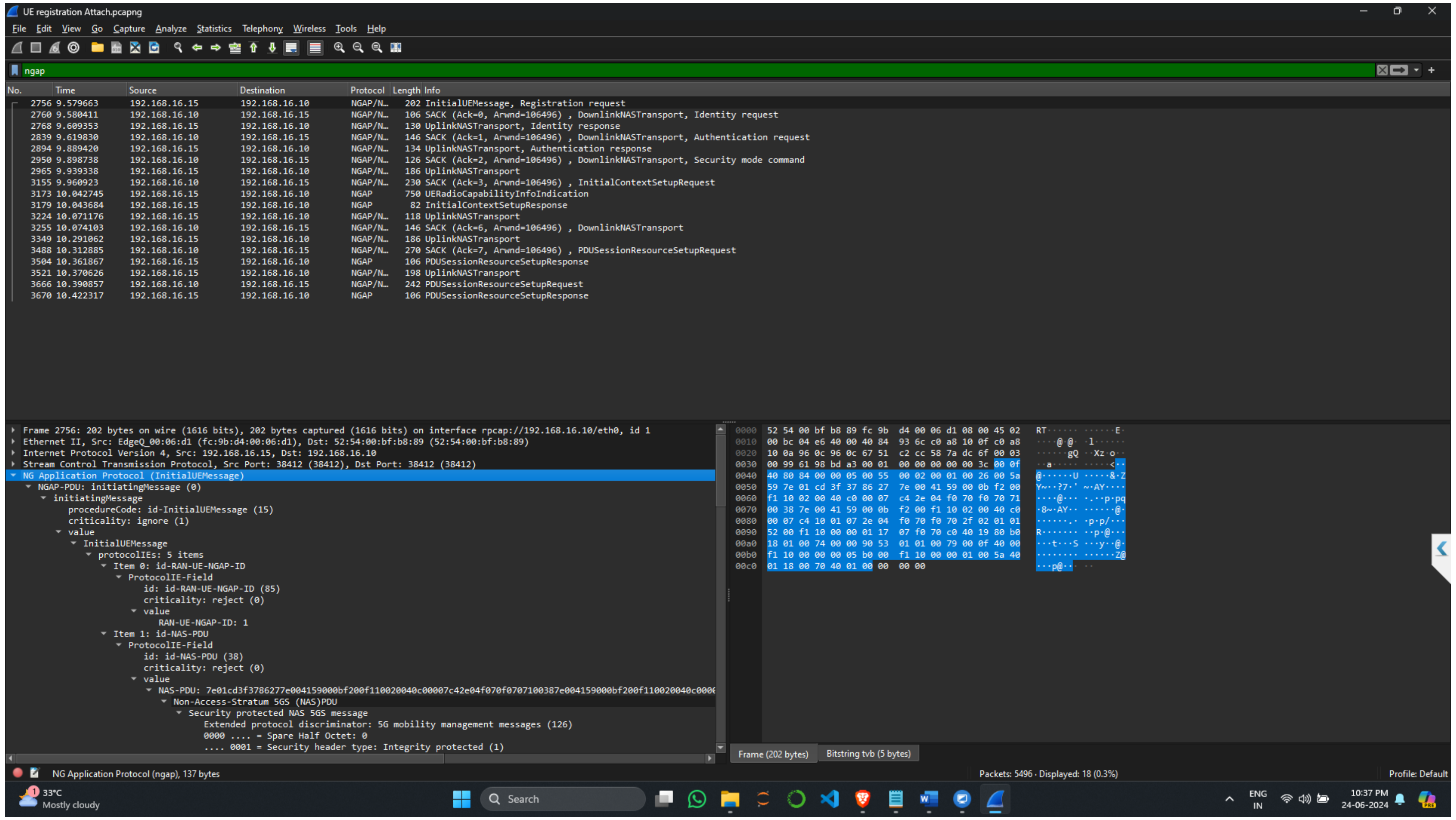
Interface	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
Local Area Connection* 9		Ethernet	☑	default	2	—	
Local Area Connection* 8		Ethernet	☑	default	2	—	
Local Area Connection* 7		Ethernet	☑	default	2	—	
Bluetooth Network Connection		Ethernet	☑	default	2	—	
WiFi		Ethernet	☑	default	2	—	
Local Area Connection* 10		Ethernet	☑	default	2	—	
Local Area Connection* 1		Ethernet	☑	default	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	
Ethernet		Ethernet	☑	default	2	—	
Event Tracing for Windows (ETW) reader		DLT_ETW	—	—	—	—	
rpcap://192.168.16.10/eth0		Ethernet	☑	default	2	—	
rpcap://192.168.16.10/ogstun		Raw IP	☑	default	2	—	
rpcap://192.168.16.10/docker0		Ethernet	☑	default	2	—	
rpcap://192.168.16.10/ogstun2		Raw IP	☑	default	2	—	
rpcap://192.168.16.10/lo (loopback)		Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

After that click on **OK** and then press **Start**

- UE Registration:
- In the filter type ngap protocol to capture UE Registration packets


UE registration Attach.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ngap
Frame (202 bytes)
Bitstring tvb (5 bytes)
33°C
Mostly cloudy
Search
ENG
IN
10:37 PM
24-06-2024

```
No.   Time       Source         Destination    Protocol Length Info
 2756 9.579663   192.168.16.15  192.168.16.10  NGAP/N…    202 InitialUEMessage, Registration request
 2760 9.580411   192.168.16.10  192.168.16.15  NGAP/N…    106 SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request
 2768 9.609353   192.168.16.15  192.168.16.10  NGAP/N…    130 UplinkNASTransport, Identity response
 2839 9.619830   192.168.16.10  192.168.16.15  NGAP/N…    146 SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request
 2894 9.889420   192.168.16.15  192.168.16.10  NGAP/N…    134 UplinkNASTransport, Authentication response
 2950 9.898738   192.168.16.10  192.168.16.15  NGAP/N…    126 SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command
 2965 9.939338   192.168.16.15  192.168.16.10  NGAP/N…    186 UplinkNASTransport
 3155 9.960923   192.168.16.10  192.168.16.15  NGAP/N…    230 SACK (Ack=3, Arwnd=106496) , InitialContextSetupRequest
 3173 10.042745  192.168.16.15  192.168.16.10  NGAP       750 UERadioCapabilityInfoIndication
 3179 10.043684  192.168.16.15  192.168.16.10  NGAP        82 InitialContextSetupResponse
 3224 10.071176  192.168.16.15  192.168.16.10  NGAP/N…    118 UplinkNASTransport
 3255 10.074103  192.168.16.10  192.168.16.15  NGAP/N…    146 SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport
 3349 10.291062  192.168.16.15  192.168.16.10  NGAP/N…    186 UplinkNASTransport
 3488 10.312885  192.168.16.10  192.168.16.15  NGAP/N…    270 SACK (Ack=7, Arwnd=106496) , PDUSessionResourceSetupRequest
 3504 10.361867  192.168.16.15  192.168.16.10  NGAP       106 PDUSessionResourceSetupResponse
 3521 10.370626  192.168.16.15  192.168.16.10  NGAP/N…    198 UplinkNASTransport
 3666 10.390857  192.168.16.10  192.168.16.15  NGAP/N…    242 PDUSessionResourceSetupRequest
 3670 10.422317  192.168.16.15  192.168.16.10  NGAP       106 PDUSessionResourceSetupResponse
```

```
> Frame 2756: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits) on interface rpcap://192.168.16.10/eth0, id 1
> Ethernet II, Src: EdgeQ_00:06:d1 (fc:9b:d4:00:06:d1), Dst: 52:54:00:bf:b8:89 (52:54:00:bf:b8:89)
> Internet Protocol Version 4, Src: 192.168.16.15, Dst: 192.168.16.10
> Stream Control Transmission Protocol, Src Port: 38412 (38412), Dst Port: 38412 (38412)
v NG Application Protocol (InitialUEMessage)
    v NGAP-PDU: initiatingMessage (0)
        v initiatingMessage
              procedureCode: id-InitialUEMessage (15)
              criticality: ignore (1)
            v value
                v InitialUEMessage
                    v protocolIEs: 5 items
                        v Item 0: id-RAN-UE-NGAP-ID
                            v ProtocolIE-Field
                                  id: id-RAN-UE-NGAP-ID (85)
                                  criticality: reject (0)
                                v value
                                      RAN-UE-NGAP-ID: 1
                        v Item 1: id-NAS-PDU
                            v ProtocolIE-Field
                                  id: id-NAS-PDU (38)
                                  criticality: reject (0)
                                v value
                                    v NAS-PDU: 7e01cd3f3786277e004159000bf200f110020040c00007c42e04f070f0707100387e004159000bf200f110020040c0000
                                        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)
```

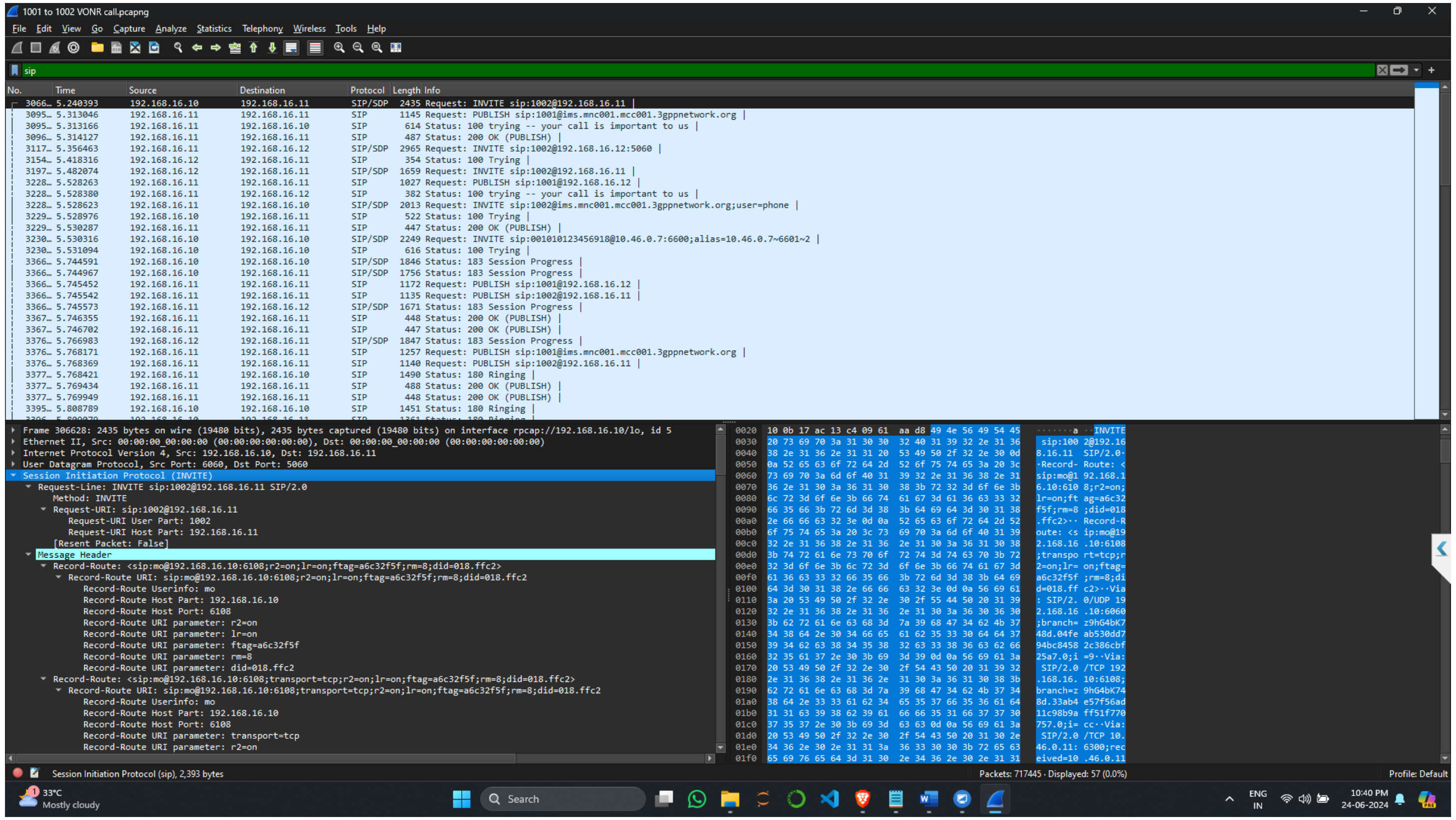
```
0000  52 54 00 bf b8 89 fc 9b  d4 00 06 d1 08 00 45 02   RT······ ······E·
0010  00 bc 04 e6 40 00 40 84  93 6c c0 a8 10 0f c0 a8   ····@·@· ·l······
0020  10 0a 96 0c 96 0c 67 51  c2 cc 58 7a dc 6f 00 03   ······gQ ··Xz·o··
0030  00 99 61 98 bd a3 00 01  00 00 00 00 00 3c 00 0f   ··a····· ·····<··
0040  40 80 84 00 00 05 00 55  00 02 00 01 00 26 00 5a   @······U ·····&·Z
0050  59 7e 01 cd 3f 37 86 27  7e 00 41 59 00 0b f2 00   Y~··?7·' ~·AY····
0060  f1 10 02 00 40 c0 00 07  c4 2e 04 f0 70 f0 70 71   ····@··· ·.··p·pq
0070  00 38 7e 00 41 59 00 0b  f2 00 f1 10 02 00 40 c0   ·8~·AY·· ······@·
0080  00 07 c4 10 01 07 2e 04  f0 70 f0 70 2f 02 01 01   ·······. ·p·p/···
0090  52 00 f1 10 00 00 01 17  07 f0 70 c0 40 19 80 b0   R······· ··p·@···
00a0  18 01 00 74 00 00 90 53  01 01 00 79 00 0f 40 00   ···t···S ···y··@·
00b0  f1 10 00 00 00 05 b0 00  f1 10 00 00 01 00 5a 40   ········ ······Z@
00c0  01 18 00 70 40 01 00 00  00 00                     ···p@··· ··
```

NG Application Protocol (ngap), 137 bytes

Packets: 5496 · Displayed: 18 (0.3%)

Profile: Default

- **VoNR Call:**
- **Call from UE1 to UE2**
- **via WIRESHARK Logs**



```
No.     Time      Source          Destination     Protocol Length Info
3066… 5.240393  192.168.16.10   192.168.16.11   SIP/SDP  2435 Request: INVITE sip:1002@192.168.16.11 |
3095… 5.313046  192.168.16.11   192.168.16.11   SIP      1145 Request: PUBLISH sip:1001@ims.mnc001.mcc001.3gppnetwork.org |
3095… 5.313166  192.168.16.11   192.168.16.10   SIP       614 Status: 100 trying -- your call is important to us |
3096… 5.314127  192.168.16.11   192.168.16.11   SIP       487 Status: 200 OK (PUBLISH) |
3117… 5.356463  192.168.16.11   192.168.16.12   SIP/SDP  2965 Request: INVITE sip:1002@192.168.16.12:5060 |
3154… 5.418316  192.168.16.12   192.168.16.11   SIP       354 Status: 100 Trying |
3197… 5.482074  192.168.16.12   192.168.16.11   SIP/SDP  1659 Request: INVITE sip:1002@192.168.16.11 |
3228… 5.528263  192.168.16.11   192.168.16.11   SIP      1027 Request: PUBLISH sip:1001@192.168.16.12 |
3228… 5.528380  192.168.16.11   192.168.16.12   SIP       382 Status: 100 trying -- your call is important to us |
3228… 5.528623  192.168.16.11   192.168.16.10   SIP/SDP  2013 Request: INVITE sip:1002@ims.mnc001.mcc001.3gppnetwork.org;user=phone |
3229… 5.528976  192.168.16.10   192.168.16.11   SIP       522 Status: 100 Trying |
3229… 5.530287  192.168.16.11   192.168.16.11   SIP       447 Status: 200 OK (PUBLISH) |
3230… 5.530316  192.168.16.10   192.168.16.10   SIP/SDP  2249 Request: INVITE sip:001010123456918@10.46.0.7:6600;alias=10.46.0.7~6601~2 |
3230… 5.531094  192.168.16.10   192.168.16.10   SIP       616 Status: 100 Trying |
3366… 5.744591  192.168.16.10   192.168.16.10   SIP/SDP  1846 Status: 183 Session Progress |
3366… 5.744967  192.168.16.10   192.168.16.11   SIP/SDP  1756 Status: 183 Session Progress |
3366… 5.745452  192.168.16.11   192.168.16.11   SIP      1172 Request: PUBLISH sip:1001@192.168.16.12 |
3366… 5.745542  192.168.16.11   192.168.16.11   SIP      1135 Request: PUBLISH sip:1002@192.168.16.11 |
3366… 5.745573  192.168.16.11   192.168.16.12   SIP/SDP  1671 Status: 183 Session Progress |
3367… 5.746355  192.168.16.11   192.168.16.11   SIP       448 Status: 200 OK (PUBLISH) |
3367… 5.746702  192.168.16.11   192.168.16.11   SIP       447 Status: 200 OK (PUBLISH) |
3376… 5.766983  192.168.16.12   192.168.16.11   SIP/SDP  1847 Status: 183 Session Progress |
3376… 5.768171  192.168.16.11   192.168.16.11   SIP      1257 Request: PUBLISH sip:1001@ims.mnc001.mcc001.3gppnetwork.org |
3376… 5.768369  192.168.16.11   192.168.16.11   SIP      1140 Request: PUBLISH sip:1002@192.168.16.11 |
3377… 5.768421  192.168.16.11   192.168.16.10   SIP      1490 Status: 180 Ringing |
3377… 5.769434  192.168.16.11   192.168.16.11   SIP       488 Status: 200 OK (PUBLISH) |
3377… 5.769949  192.168.16.11   192.168.16.11   SIP       448 Status: 200 OK (PUBLISH) |
3395… 5.808789  192.168.16.10   192.168.16.10   SIP      1451 Status: 180 Ringing |
3396… 5.809079  192.168.16.10   192.168.16.11   SIP      1361 Status: 180 Ringing |
```

```
> Frame 306628: 2435 bytes on wire (19480 bits), 2435 bytes captured (19480 bits) on interface rpcap://192.168.16.10/lo, id 5
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.16.10, Dst: 192.168.16.11
> User Datagram Protocol, Src Port: 6060, Dst Port: 5060
v Session Initiation Protocol (INVITE)
  v Request-Line: INVITE sip:1002@192.168.16.11 SIP/2.0
      Method: INVITE
    v Request-URI: sip:1002@192.168.16.11
        Request-URI User Part: 1002
        Request-URI Host Part: 192.168.16.11
      [Resent Packet: False]
  v Message Header
    v Record-Route: <sip:mo@192.168.16.10:6108;r2=on;lr=on;ftag=a6c32f5f;rm=8;did=018.ffc2>
      v Record-Route URI: sip:mo@192.168.16.10:6108;r2=on;lr=on;ftag=a6c32f5f;rm=8;did=018.ffc2
          Record-Route Userinfo: mo
          Record-Route Host Part: 192.168.16.10
          Record-Route Host Port: 6108
          Record-Route URI parameter: r2=on
          Record-Route URI parameter: lr=on
          Record-Route URI parameter: ftag=a6c32f5f
          Record-Route URI parameter: rm=8
          Record-Route URI parameter: did=018.ffc2
    v Record-Route: <sip:mo@192.168.16.10:6108;transport=tcp;r2=on;lr=on;ftag=a6c32f5f;rm=8;did=018.ffc2>
      v Record-Route URI: sip:mo@192.168.16.10:6108;transport=tcp;r2=on;lr=on;ftag=a6c32f5f;rm=8;did=018.ffc2
          Record-Route Userinfo: mo
          Record-Route Host Part: 192.168.16.10
          Record-Route Host Port: 6108
          Record-Route URI parameter: transport=tcp
          Record-Route URI parameter: r2=on
```

```
0020  10 0b 17 ac 13 c4 09 61  aa d8 49 4e 56 49 54 45   ·······a ··INVITE
0030  20 73 69 70 3a 31 30 30  32 40 31 39 32 2e 31 36    sip:100 2@192.16
0040  38 2e 31 36 2e 31 31 20  53 49 50 2f 32 2e 30 0d   8.16.11  SIP/2.0·
0050  0a 52 65 63 6f 72 64 2d  52 6f 75 74 65 3a 20 3c   ·Record- Route: <
0060  73 69 70 3a 6d 6f 40 31  39 32 2e 31 36 38 2e 31   sip:mo@1 92.168.1
0070  36 2e 31 30 3a 36 31 30  38 3b 72 32 3d 6f 6e 3b   6.10:610 8;r2=on;
0080  6c 72 3d 6f 6e 3b 66 74  61 67 3d 61 36 63 33 32   lr=on;ft ag=a6c32
0090  66 35 66 3b 72 6d 3d 38  3b 64 69 64 3d 30 31 38   f5f;rm=8 ;did=018
00a0  2e 66 66 63 32 3e 0d 0a  52 65 63 6f 72 64 2d 52   .ffc2>·· Record-R
00b0  6f 75 74 65 3a 20 3c 73  69 70 3a 6d 6f 40 31 39   oute: <s ip:mo@19
00c0  32 2e 31 36 38 2e 31 36  2e 31 30 3a 36 31 30 38   2.168.16 .10:6108
00d0  3b 74 72 61 6e 73 70 6f  72 74 3d 74 63 70 3b 72   ;transpo rt=tcp;r
00e0  32 3d 6f 6e 3b 6c 72 3d  6f 6e 3b 66 74 61 67 3d   2=on;lr= on;ftag=
00f0  61 36 63 33 32 66 35 66  3b 72 6d 3d 38 3b 64 69   a6c32f5f ;rm=8;di
0100  64 3d 30 31 38 2e 66 66  63 32 3e 0d 0a 56 69 61   d=018.ff c2>··Via
0110  3a 20 53 49 50 2f 32 2e  30 2f 55 44 50 20 31 39   : SIP/2. 0/UDP 19
0120  32 2e 31 36 38 2e 31 36  2e 31 30 3a 36 30 36 30   2.168.16 .10:6060
0130  3b 62 72 61 6e 63 68 3d  7a 39 68 47 34 62 4b 37   ;branch= z9hG4bK7
0140  34 38 64 2e 30 34 66 65  61 62 35 33 30 64 64 37   48d.04fe ab530dd7
0150  39 34 62 63 38 34 35 38  32 63 33 38 36 63 62 66   94bc8458 2c386cbf
0160  32 35 61 37 2e 30 3b 69  3d 39 0d 0a 56 69 61 3a   25a7.0;i =9··Via:
0170  20 53 49 50 2f 32 2e 30  2f 54 43 50 20 31 39 32    SIP/2.0 /TCP 192
0180  2e 31 36 38 2e 31 36 2e  31 30 3a 36 31 30 38 3b   .168.16. 10:6108;
0190  62 72 61 6e 63 68 3d 7a  39 68 47 34 62 4b 37 34   branch=z 9hG4bK74
01a0  38 64 2e 33 33 61 62 34  65 35 37 66 35 36 61 64   8d.33ab4 e57f56ad
01b0  31 31 63 39 38 62 39 61  66 66 35 31 66 37 37 30   11c98b9a ff51f770
01c0  37 35 37 2e 30 3b 69 3d  63 63 0d 0a 56 69 61 3a   757.0;i= cc··Via:
01d0  20 53 49 50 2f 32 2e 30  2f 54 43 50 20 31 30 2e    SIP/2.0 /TCP 10.
01e0  34 36 2e 30 2e 31 31 3a  36 33 30 30 3b 72 65 63   46.0.11: 6300;rec
01f0  65 69 76 65 64 3d 31 30  2e 34 36 2e 30 2e 31 31   eived=10 .46.0.11
```

Session Initiation Protocol (sip), 2,393 bytes

Packets: 717445 · Displayed: 57 (0.0%)

5G LAB

Live Training on Wireshark

Thank You
For
Your
Time & Patience

5G LAB

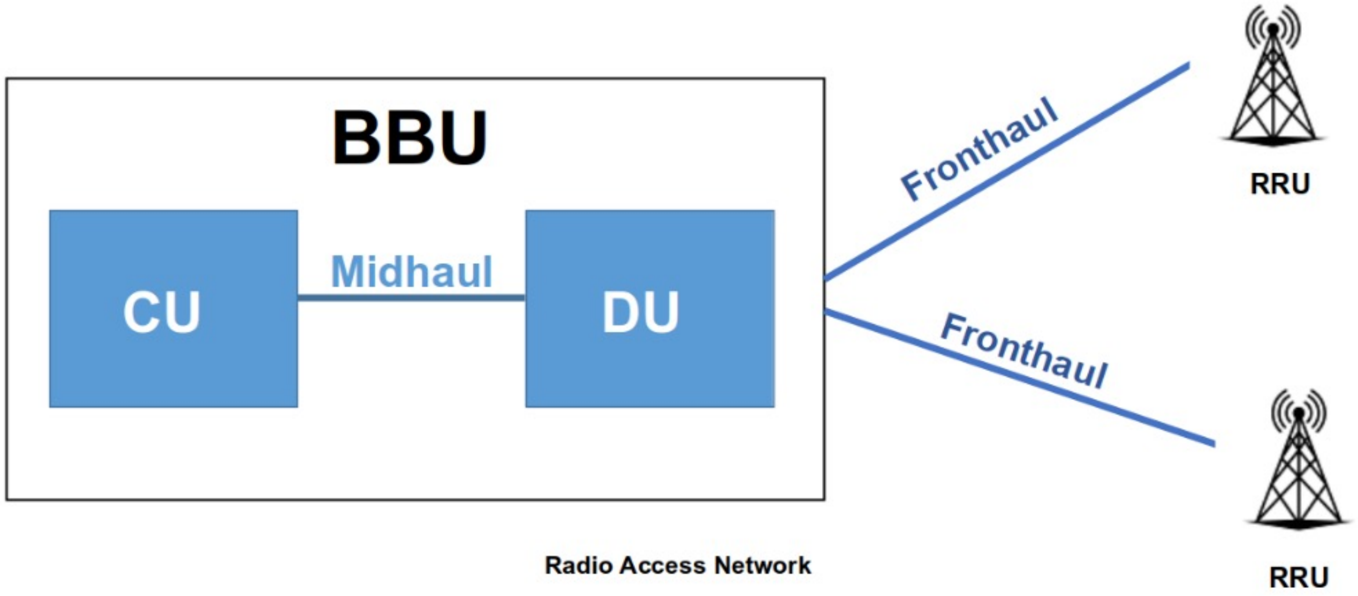
Day 2

Training

5G LAB

5G RAN Description

System description -Integrated (BBU&RU) Architecture:



Components of Integrated Architecture:

- BBU (Baseband Unit): Handles signal processing, protocol stack, and communication with the core network.
- RU (Radio Unit): Manages radio frequency (RF) functions, like sending/receiving wireless signals to/from UEs (User Equipment).
- DU (Distributed Unit): Processes Layer 1 (PHY) and part of Layer 2 functions.
- CU (Centralized Unit): Handles higher Layer 2 and Layer 3 functions, managing control-plane and user-plane traffic.

System Description of Integrated Architecture

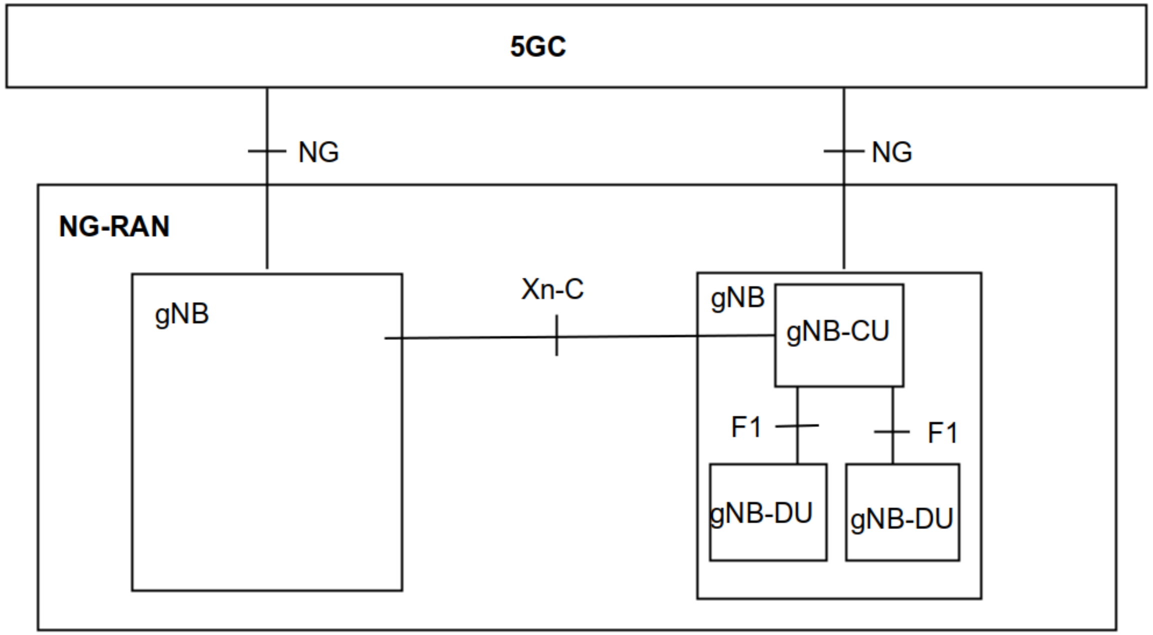
- **Physical Setup:**
  - BBU and RU in a Single Unit: Both the baseband processing and RF functions are handled within the same hardware.
- **Connectivity:**
  - Direct Interface to 5G Core (5GC): The integrated node connects directly to the 5G Core via
- the NG Interface (NG-C for control, NG-U for user data).
- **Protocol Stack:**
  - PHY, MAC, RLC, PDCP, RRC in One Unit: The complete 5G NR stack is processed in the same
- physical hardware, reducing communication delays.
- **Interfaces:**
  - NG Interface (N2/N3): Connects the integrated gNB to the 5G core.
  - Xn Interface: Connects to other neighboring gNBs for mobility and handovers.

- **RAN Sub-System description:**

- The Radio Access Network (RAN) is the part of the telecom system that connects user devices
- (UE — User Equipment) to the mobile core network over the air.
- It handles the transmission, processing, and management of radio signals between
- UEs and the core, enabling all mobile services like voice, data, and messaging.

- **RAN Architecture in 5G**
- The **5G RAN** is more flexible and distributed compared to previous generations.
- It consists of three main components:
- **Radio Unit (RU)**
- **Distributed Unit (DU)**
- **Centralized Unit (CU)**

RAN Architecture in 5G



Next-Generation RAN (NG-RAN):
The RAN is responsible for wireless communication between UEs (User Equipment) and the 5G Core. It includes the following elements:

gNB (Next Generation Node B): The base station in 5G, which can be implemented as:

1. Monolithic gNB: All functions in a single unit (left side of the diagram).
2. Disaggregated gNB (CU/DU Split): Split into smaller units for flexibility and scalability (right side of the diagram).

RAN Architecture in 5G

gNB-CU (Centralized Unit):

- Handles higher-layer functions (Layer 2 and Layer 3).
- Manages the RRC (Radio Resource Control) and handles mobility, security, and QoS policies.

gNB-DU (Distributed Unit):

- Processes lower-layer functions (PHY, MAC, and parts of RLC).

NG Interface:

- NG-C (Control Plane): For signaling messages (e.g., registration, authentication).
- NG-U (User Plane): For user data traffic.

F1 Interface:

- Connects the CU to the DU.

Xn Interface:

- Xn-C (Control Plane): Supports handovers and mobility management.
- Xn-U (User Plane): Transfers data between gNBs.

Features and functionalities of the RAN Sub-System:

- A 5G Radio Access Network (RAN) features functionalities like beamforming, massive MIMO, network
- slicing, dynamic spectrum sharing, small cells,and the use of millimeter wave (mmWave) technology to deliver
- high-speed, low-latency connectivity by efficiently managing radio signals between user devices and the
- 5G core network, enabling applications like augmented reality, autonomous driving, and high-bandwidth
- streaming with improved coverage and capacity compared to previous generations.

- **Features of 5G RAN:**
  - **Massive MIMO**
  - **Network Slicing**
  - **Small Cells**
  - **mmWave Technology**
  - **Dynamic Spectrum Sharing (DSS)**
  - **Centralized Unit (CU) and Distributed Unit (DU)**

Features and functionalities of the RAN Sub-System:

- **5G RAN functions:**
  - **Radio signal transmission and reception**
  - **Resource allocation**
  - **Mobility management**
  - **Quality of service (QoS) control**

specifications BBU/RU

General	**Description**
3gpp release	16
Technology	5G NR
Band	N78(3.3-3.8GHz)
Architecture	Integrated RAN
Mode	TDD
Sectors	1
Users (connected/Active)	Min 32
MIMO	Min 2T2R
Mimo modes	SU-MIMO
RF power	Min 100mW
No. of CC	1
Bandwidth	Up to 100MHz
SubCarrier Spacing	30 KHz
Synchronization	GPS,Synce and IEEE1588v2
Throughput	200 Mbps
Interfaces	1x10G copper or 1x10G optical
NO.of layers(DL/UL)	2/1
QAM(DL/UL)	256/64
Users/TTI	4

Implementation of 5G RAN

- **Server specification required for 5G RAN**
- To support the 5G RAN-in-a-Box system in the lab, the server must meet specific hardware and software requirements. The server will handle processing, networking, and storage needs for 5G RAN functions, baseband processing, and potential integration with the 5G Core (if applicable).
- **Explanation of Hardware proposed for the lab**
- The proposed hardware is a compact 5G RAN-in-a-Box solution designed for lab testing and small-scale deployments. This unit integrates Radio Access Network (RAN) and Baseband functionalities into a single enclosure, simplifying setup and operation. It features an internal antenna system, reducing the need for external RF components while ensuring efficient signal transmission.
- ption.

Key Features and Capabilities of 5G RAN

- **Key Features and Capabilities**
- **1. Integrated RAN Design**
- Combines radio unit (RU) and distributed unit (DU) into a single hardware unit, minimizing infrastructure complexity.
- Eliminates the need for separate baseband processing units, making it ideal for lab environments.
- **2. Internal Antenna System**
- Active Antenna Configuration: Enhances signal coverage and performance through beamforming and optimized RF output.
- Supports 2T2R MIMO, ensuring stable connectivity and efficient spectrum usage.
- Internal antenna design reduces deployment challenges and eliminates external RF cabling.
- **3. Frequency and Bandwidth**
- Operates in 5G NR Band N78 (3.3–3.8 GHz), a key mid-band frequency for 5G networks.
- Supports up to 100 MHz bandwidth, allowing high data throughput in lab simulations.

Implementation of 5G RAN

- **Key Features and Capabilities**
- **4. Connectivity and Interfaces**
- 10G Ethernet (Copper/Optical) for high-speed backhaul and data transfer.
- GPS, SyncE, and IEEE1588v2 support for accurate timing synchronization.
- IP65-rated enclosure, ensuring protection against dust and moisture even in rugged conditions.
- **5. Performance and User Capacity**
- Minimum 32 concurrent users supported, making it ideal for multi-user testing scenarios.
- Downlink throughput of 200+ Mbps, simulating real-world 5G performance.
- 4 users per TTI, optimizing scheduling and resource allocation.
- **6. Power and Mechanical Design**
- Compact form factor (1ft x 1ft, <5 kg) for easy portability and installation.
- 48V, 60W power input, ensuring efficient energy consumption.

Coral Telecom (LISTEN)(SEE)(THINK)

Research, Design, Develop & Manufacturing in India

Implementation of 5G RAN

- **Use Cases in the Lab**
  - 5G Network Testing: Validating RAN performance under various conditions.
  - Application Development: Testing 5G-enabled applications in a controlled environment.
  - Interoperability Testing: Evaluating compatibility with different core network elements.
  - Training and Research: Hands-on experience for engineers and researchers working with 5G technologies.

Implementationof 5G RAN

- **Provisioning of server for installation**
- The RAN-in-a-Box solution proposed for the lab is a fully integrated system that includes preinstalled software for Central Unit (CU), Distributed Unit (DU), and Radio Unit (RU) within a single hardware package. Since this is a self-contained deployment, there is no need for an external server to install or run individual CU/DU functions separately
- **OS and Virtualization software installation**
- The RAN-in-a-Box does not require an external OS or hypervisor installation, as it comes with preloaded firmware and software optimized for 5G RAN functionality.
- No need for VMware, KVM, or other virtualization platforms, as the system operates natively on its own embedded OS.
- .

Configuration of 5G Core

To configure core elements, we need to update the coral configuration file with the required changes. This configuration defines the core and RAN integration settings by specifying IP addresses, mobility parameters, and service components.

In the next slide, we have included coral file screenshots for better understanding.

Here are some key examples:

Mobility Parameters:

MCC: 001, MNC: 001, MME-MNC: 01

TAC: 1, AMF: 8000, SD: 000000

Mode: vonr

CSCF & Node IPs:

CSCF: 192.168.254.30

IP Servicing CSCF: 192.168.8.67

IP Feature Server: 192.168.8.68

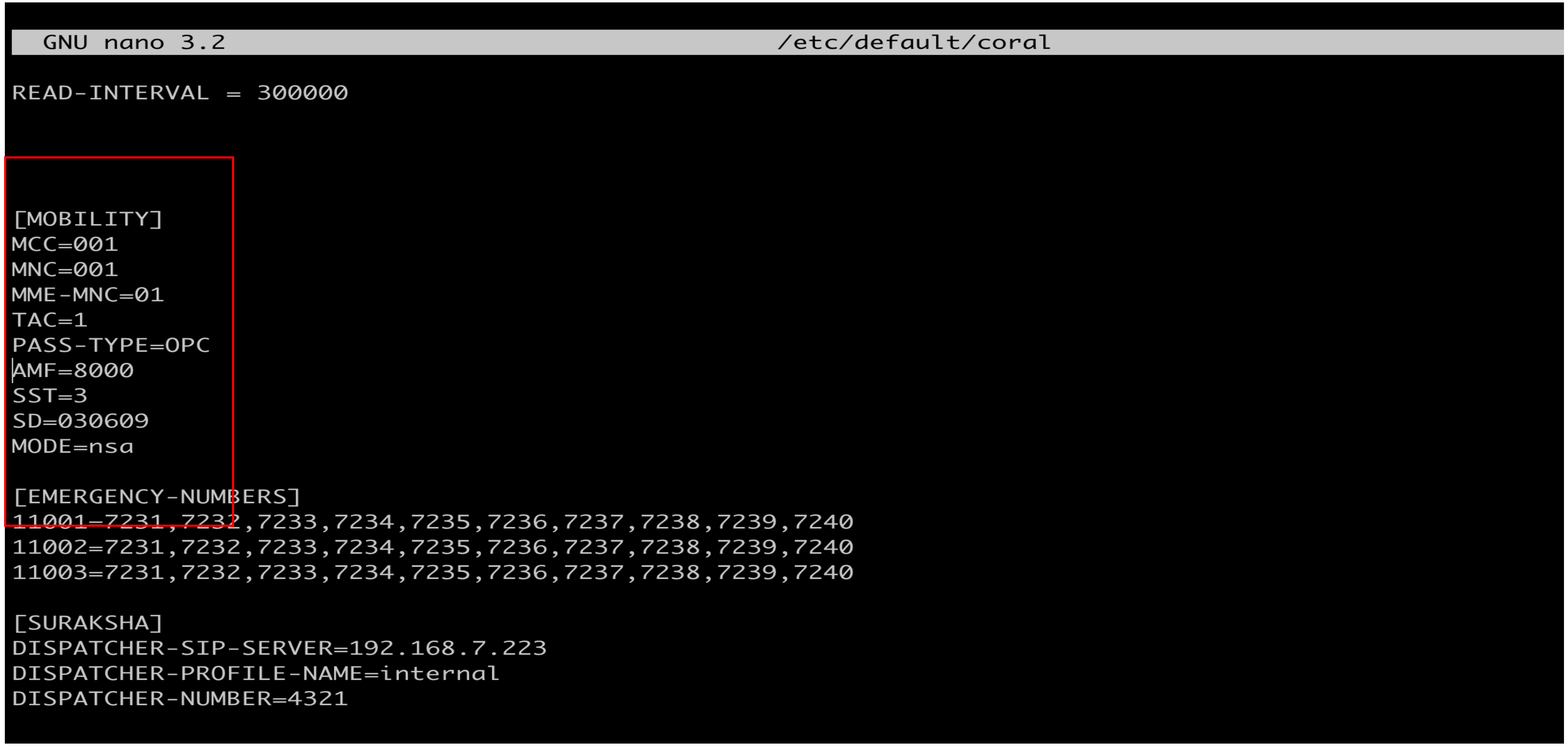
IP Trunk Gateway: 192.168.8.69

IP AMF: 192.168.8.66

Media Proxy: 127.0.0.1

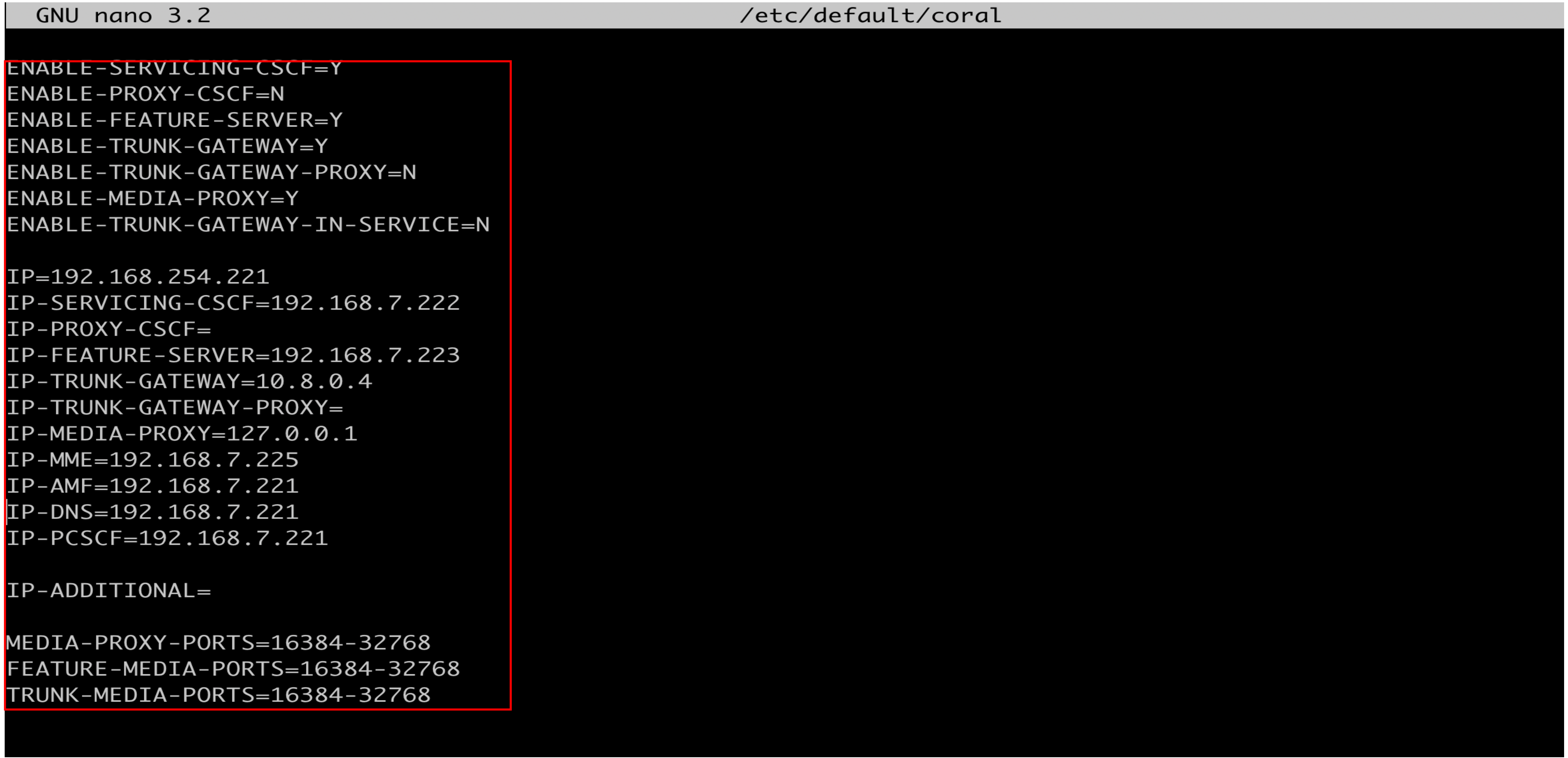
Gateway: 192.168.8.254

Configuration of 5G Core and RAN



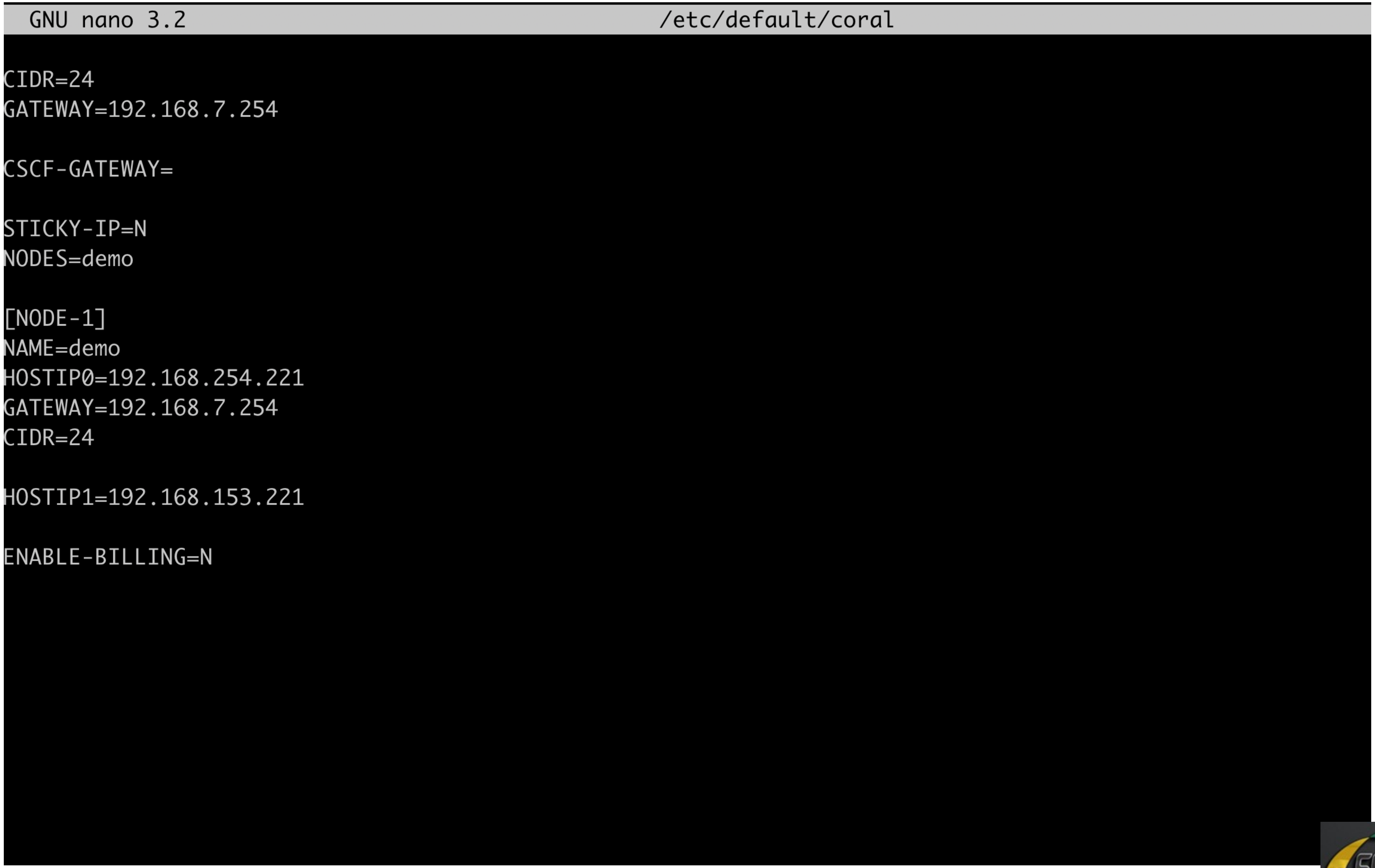
```
  GNU nano 3.2                                          /etc/default/coral

READ-INTERVAL = 300000



[MOBILITY]
MCC=001
MNC=001
MME-MNC=01
TAC=1
PASS-TYPE=OPC
AMF=8000
SST=3
SD=030609
MODE=nsa

[EMERGENCY-NUMBERS]
11001=7231,7232,7233,7234,7235,7236,7237,7238,7239,7240
11002=7231,7232,7233,7234,7235,7236,7237,7238,7239,7240
11003=7231,7232,7233,7234,7235,7236,7237,7238,7239,7240

[SURAKSHA]
DISPATCHER-SIP-SERVER=192.168.7.223
DISPATCHER-PROFILE-NAME=internal
DISPATCHER-NUMBER=4321
```

Configuration of 5G Core and RAN



```
GNU nano 3.2                                    /etc/default/coral

ENABLE-SERVICING-CSCF=Y
ENABLE-PROXY-CSCF=N
ENABLE-FEATURE-SERVER=Y
ENABLE-TRUNK-GATEWAY=Y
ENABLE-TRUNK-GATEWAY-PROXY=N
ENABLE-MEDIA-PROXY=Y
ENABLE-TRUNK-GATEWAY-IN-SERVICE=N

IP=192.168.254.221
IP-SERVICING-CSCF=192.168.7.222
IP-PROXY-CSCF=
IP-FEATURE-SERVER=192.168.7.223
IP-TRUNK-GATEWAY=10.8.0.4
IP-TRUNK-GATEWAY-PROXY=
IP-MEDIA-PROXY=127.0.0.1
IP-MME=192.168.7.225
IP-AMF=192.168.7.221
IP-DNS=192.168.7.221
IP-PCSCF=192.168.7.221

IP-ADDITIONAL=

MEDIA-PROXY-PORTS=16384-32768
FEATURE-MEDIA-PORTS=16384-32768
TRUNK-MEDIA-PORTS=16384-32768
```

Configuration of 5G Core and RAN

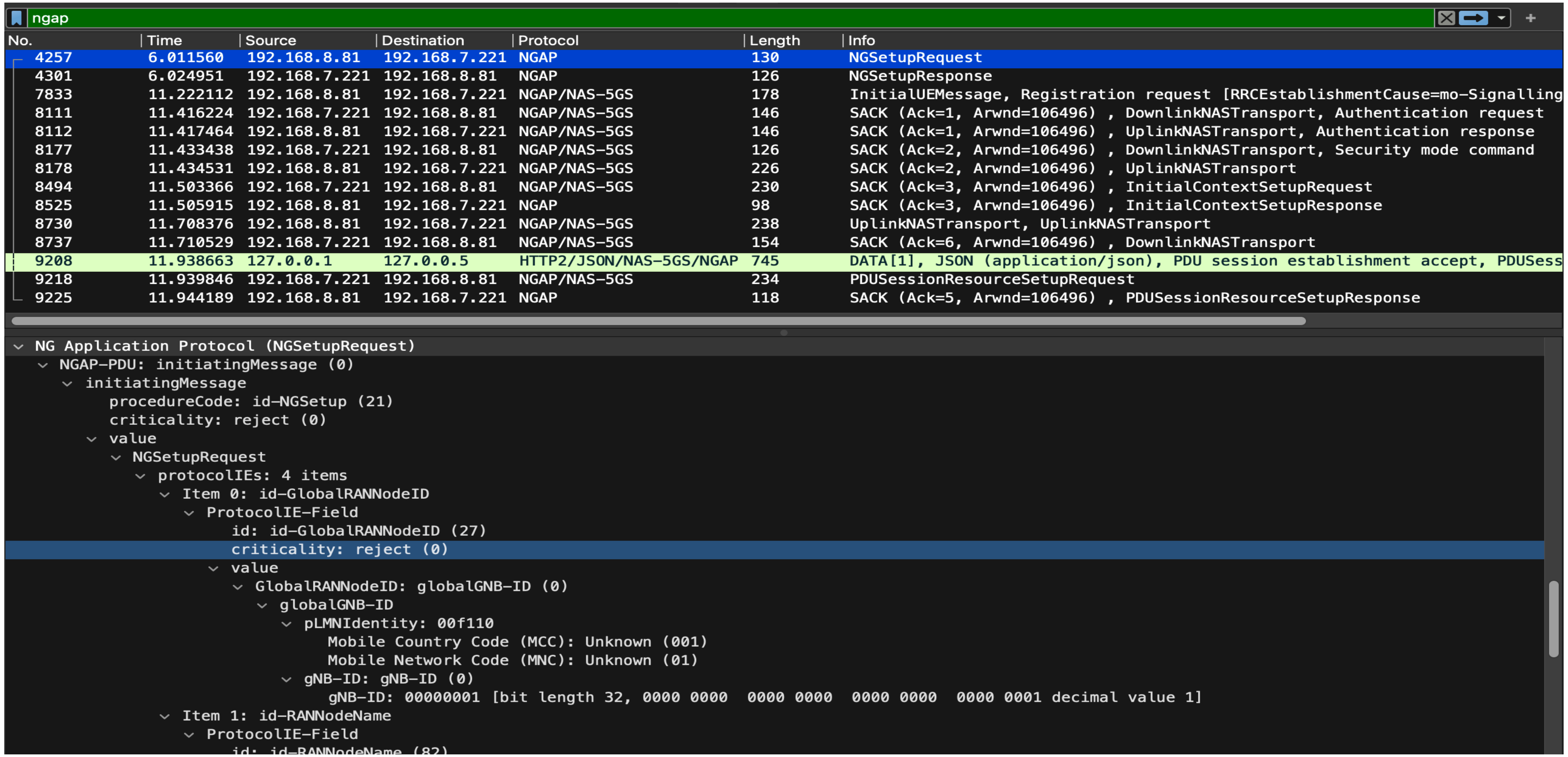


```
  GNU nano 3.2                                 /etc/default/coral

CIDR=24
GATEWAY=192.168.7.254

CSCF-GATEWAY=

STICKY-IP=N
NODES=demo

[NODE-1]
NAME=demo
HOSTIP0=192.168.254.221
GATEWAY=192.168.7.254
CIDR=24

HOSTIP1=192.168.153.221

ENABLE-BILLING=N
```

Research,
Design, Develop &
Manufacturing in India

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

After successful configuration, the connection establishment between the RAN (gNB) and core network elements (AMF) involves signaling. The AMF is responsible for signaling interactions.



ngap

```
No.          Time        Source        Destination   Protocol                 Length  Info
4257         6.011560    192.168.8.81  192.168.7.221 NGAP                     130     NGSetupRequest
4301         6.024951    192.168.7.221 192.168.8.81  NGAP                     126     NGSetupResponse
7833         11.222112   192.168.8.81  192.168.7.221 NGAP/NAS-5GS             178     InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling
8111         11.416224   192.168.7.221 192.168.8.81  NGAP/NAS-5GS             146     SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request
8112         11.417464   192.168.8.81  192.168.7.221 NGAP/NAS-5GS             146     SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response
8177         11.433438   192.168.7.221 192.168.8.81  NGAP/NAS-5GS             126     SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command
8178         11.434531   192.168.8.81  192.168.7.221 NGAP/NAS-5GS             226     SACK (Ack=2, Arwnd=106496) , UplinkNASTransport
8494         11.503366   192.168.7.221 192.168.8.81  NGAP/NAS-5GS             230     SACK (Ack=3, Arwnd=106496) , InitialContextSetupRequest
8525         11.505915   192.168.8.81  192.168.7.221 NGAP                     98      SACK (Ack=3, Arwnd=106496) , InitialContextSetupResponse
8730         11.708376   192.168.8.81  192.168.7.221 NGAP/NAS-5GS             238     UplinkNASTransport, UplinkNASTransport
8737         11.710529   192.168.7.221 192.168.8.81  NGAP/NAS-5GS             154     SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport
9208         11.938663   127.0.0.1     127.0.0.5     HTTP2/JSON/NAS-5GS/NGAP  745     DATA[1], JSON (application/json), PDU session establishment accept, PDUSess
9218         11.939846   192.168.7.221 192.168.8.81  NGAP/NAS-5GS             234     PDUSessionResourceSetupRequest
9225         11.944189   192.168.8.81  192.168.7.221 NGAP                     118     SACK (Ack=5, Arwnd=106496) , PDUSessionResourceSetupResponse
```

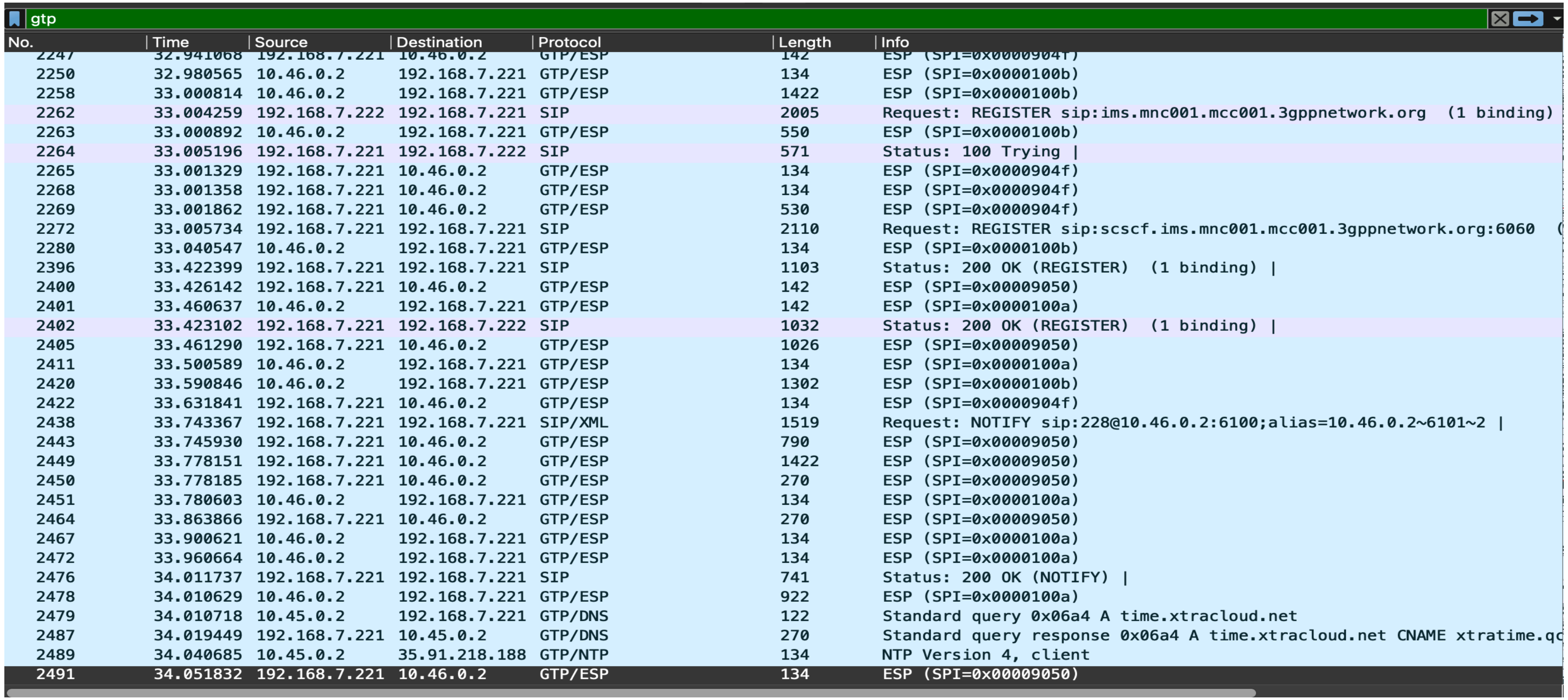
```
NG Application Protocol (NGSetupRequest)
  NGAP-PDU: initiatingMessage (0)
    initiatingMessage
      procedureCode: id-NGSetup (21)
      criticality: reject (0)
      value
        NGSetupRequest
          protocolIEs: 4 items
            Item 0: id-GlobalRANNodeID
              ProtocolIE-Field
                id: id-GlobalRANNodeID (27)
                criticality: reject (0)
                value
                  GlobalRANNodeID: globalGNB-ID (0)
                    globalGNB-ID
                      pLMNIdentity: 00f110
                        Mobile Country Code (MCC): Unknown (001)
                        Mobile Network Code (MNC): Unknown (01)
                      gNB-ID: gNB-ID (0)
                        gNB-ID: 00000001 [bit length 32, 0000 0000  0000 0000  0000 0000  0000 0001 decimal value 1]
            Item 1: id-RANNodeName
              ProtocolIE-Field
                id: id-RANNodeName (82)
```

NGAP messages between AMF and gNB

Research, Design, Develop & Manufacturing in India

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

After successful configuration, the connection establishment between the RAN (gNB) and core network elements (UPF) involves data-plane communication protocol. The UPF manages user-plane data forwarding.

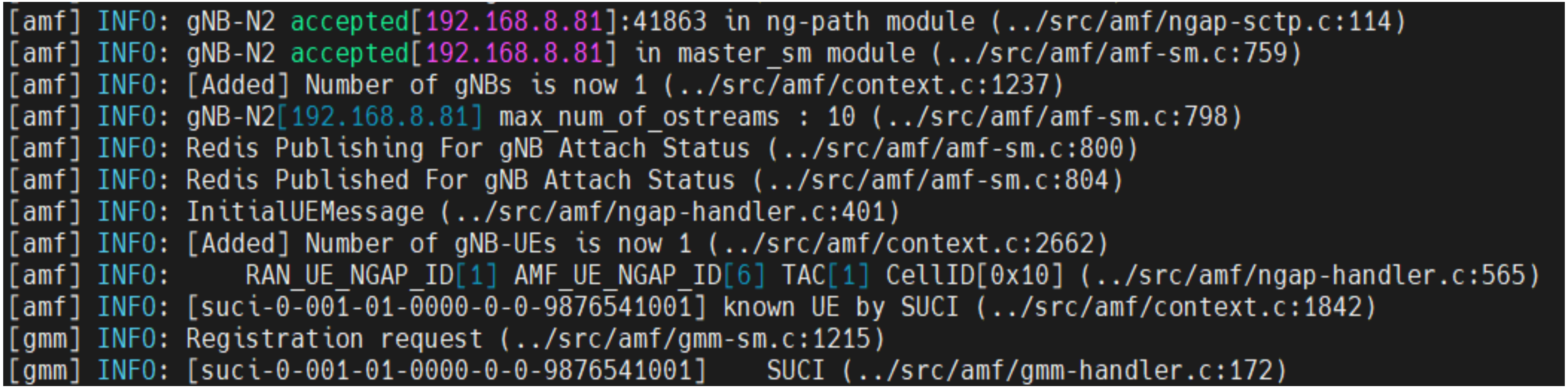


```
gtp
No.     Time       Source        Destination   Protocol   Length  Info
  2247  32.941068  192.168.7.221 10.46.0.2     GTP/ESP    142     ESP (SPI=0x0000904f)
  2250  32.980565  10.46.0.2     192.168.7.221 GTP/ESP    134     ESP (SPI=0x0000100b)
  2258  33.000814  10.46.0.2     192.168.7.221 GTP/ESP    1422    ESP (SPI=0x0000100b)
  2262  33.004259  192.168.7.222 192.168.7.221 SIP        2005    Request: REGISTER sip:ims.mnc001.mcc001.3gppnetwork.org  (1 binding)
  2263  33.000892  10.46.0.2     192.168.7.221 GTP/ESP    550     ESP (SPI=0x0000100b)
  2264  33.005196  192.168.7.221 192.168.7.222 SIP        571     Status: 100 Trying |
  2265  33.001329  192.168.7.221 10.46.0.2     GTP/ESP    134     ESP (SPI=0x0000904f)
  2268  33.001358  192.168.7.221 10.46.0.2     GTP/ESP    134     ESP (SPI=0x0000904f)
  2269  33.001862  192.168.7.221 10.46.0.2     GTP/ESP    530     ESP (SPI=0x0000904f)
  2272  33.005734  192.168.7.221 192.168.7.221 SIP        2110    Request: REGISTER sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:6060  (
  2280  33.040547  10.46.0.2     192.168.7.221 GTP/ESP    134     ESP (SPI=0x0000100b)
  2396  33.422399  192.168.7.221 192.168.7.221 SIP        1103    Status: 200 OK (REGISTER)  (1 binding) |
  2400  33.426142  192.168.7.221 10.46.0.2     GTP/ESP    142     ESP (SPI=0x00009050)
  2401  33.460637  10.46.0.2     192.168.7.221 GTP/ESP    142     ESP (SPI=0x0000100a)
  2402  33.423102  192.168.7.221 192.168.7.222 SIP        1032    Status: 200 OK (REGISTER)  (1 binding) |
  2405  33.461290  192.168.7.221 10.46.0.2     GTP/ESP    1026    ESP (SPI=0x00009050)
  2411  33.500589  10.46.0.2     192.168.7.221 GTP/ESP    134     ESP (SPI=0x0000100a)
  2420  33.590846  10.46.0.2     192.168.7.221 GTP/ESP    1302    ESP (SPI=0x0000100b)
  2422  33.631841  192.168.7.221 10.46.0.2     GTP/ESP    134     ESP (SPI=0x0000904f)
  2438  33.743367  192.168.7.221 192.168.7.221 SIP/XML    1519    Request: NOTIFY sip:228@10.46.0.2:6100;alias=10.46.0.2~6101~2 |
  2443  33.745930  192.168.7.221 10.46.0.2     GTP/ESP    790     ESP (SPI=0x00009050)
  2449  33.778151  192.168.7.221 10.46.0.2     GTP/ESP    1422    ESP (SPI=0x00009050)
  2450  33.778185  192.168.7.221 10.46.0.2     GTP/ESP    270     ESP (SPI=0x00009050)
  2451  33.780603  10.46.0.2     192.168.7.221 GTP/ESP    134     ESP (SPI=0x0000100a)
  2464  33.863866  192.168.7.221 10.46.0.2     GTP/ESP    270     ESP (SPI=0x00009050)
  2467  33.900621  10.46.0.2     192.168.7.221 GTP/ESP    134     ESP (SPI=0x0000100a)
  2472  33.960664  10.46.0.2     192.168.7.221 GTP/ESP    134     ESP (SPI=0x0000100a)
  2476  34.011737  192.168.7.221 192.168.7.221 SIP        741     Status: 200 OK (NOTIFY) |
  2478  34.010629  10.46.0.2     192.168.7.221 GTP/ESP    922     ESP (SPI=0x0000100a)
  2479  34.010718  10.45.0.2     192.168.7.221 GTP/DNS    122     Standard query 0x06a4 A time.xtracloud.net
  2487  34.019449  192.168.7.221 10.45.0.2     GTP/DNS    270     Standard query response 0x06a4 A time.xtracloud.net CNAME xtratime.qc
  2489  34.040685  10.45.0.2     35.91.218.188 GTP/NTP    134     NTP Version 4, client
  2491  34.051832  192.168.7.221 10.46.0.2     GTP/ESP    134     ESP (SPI=0x00009050)
```

NGAP messages between UPF and gNB

Verification of connection establishment between Core and RAN

Verification of Successful connection establishment between Core and RAN

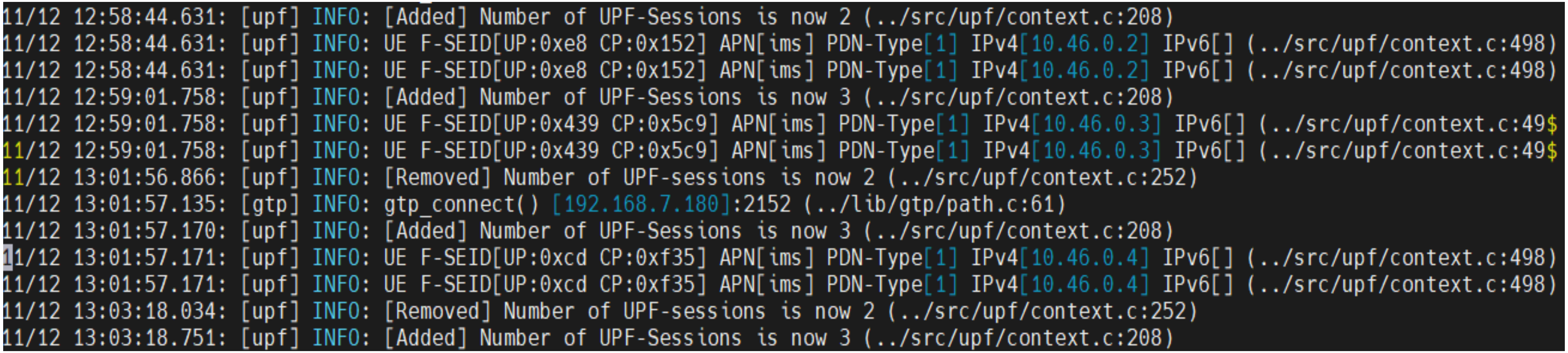


```
[amf] INFO: gNB-N2 accepted[192.168.8.81]:41863 in ng-path module (../src/amf/ngap-sctp.c:114)
[amf] INFO: gNB-N2 accepted[192.168.8.81] in master_sm module (../src/amf/amf-sm.c:759)
[amf] INFO: [Added] Number of gNBs is now 1 (../src/amf/context.c:1237)
[amf] INFO: gNB-N2[192.168.8.81] max_num_of_ostreams : 10 (../src/amf/amf-sm.c:798)
[amf] INFO: Redis Publishing For gNB Attach Status (../src/amf/amf-sm.c:800)
[amf] INFO: Redis Published For gNB Attach Status (../src/amf/amf-sm.c:804)
[amf] INFO: InitialUEMessage (../src/amf/ngap-handler.c:401)
[amf] INFO: [Added] Number of gNB-UEs is now 1 (../src/amf/context.c:2662)
[amf] INFO:     RAN_UE_NGAP_ID[1] AMF_UE_NGAP_ID[6] TAC[1] CellID[0x10] (../src/amf/ngap-handler.c:565)
[amf] INFO: [suci-0-001-01-0000-0-0-9876541001] known UE by SUCI (../src/amf/context.c:1842)
[gmm] INFO: Registration request (../src/amf/gmm-sm.c:1215)
[gmm] INFO: [suci-0-001-01-0000-0-0-9876541001]    SUCI (../src/amf/gmm-handler.c:172)
```

AMF LOGS

Verification of connection establishment between Core and RAN

Verification of Successful connection establishment between Core and RAN



```
11/12 12:58:44.631: [upf] INFO: [Added] Number of UPF-Sessions is now 2 (../src/upf/context.c:208)
11/12 12:58:44.631: [upf] INFO: UE F-SEID[UP:0xe8 CP:0x152] APN[ims] PDN-Type[1] IPv4[10.46.0.2] IPv6[] (../src/upf/context.c:498)
11/12 12:58:44.631: [upf] INFO: UE F-SEID[UP:0xe8 CP:0x152] APN[ims] PDN-Type[1] IPv4[10.46.0.2] IPv6[] (../src/upf/context.c:498)
11/12 12:59:01.758: [upf] INFO: [Added] Number of UPF-Sessions is now 3 (../src/upf/context.c:208)
11/12 12:59:01.758: [upf] INFO: UE F-SEID[UP:0x439 CP:0x5c9] APN[ims] PDN-Type[1] IPv4[10.46.0.3] IPv6[] (../src/upf/context.c:49$
11/12 12:59:01.758: [upf] INFO: UE F-SEID[UP:0x439 CP:0x5c9] APN[ims] PDN-Type[1] IPv4[10.46.0.3] IPv6[] (../src/upf/context.c:49$
11/12 13:01:56.866: [upf] INFO: [Removed] Number of UPF-sessions is now 2 (../src/upf/context.c:252)
11/12 13:01:57.135: [gtp] INFO: gtp_connect() [192.168.7.180]:2152 (../lib/gtp/path.c:61)
11/12 13:01:57.170: [upf] INFO: [Added] Number of UPF-Sessions is now 3 (../src/upf/context.c:208)
11/12 13:01:57.171: [upf] INFO: UE F-SEID[UP:0xcd CP:0xf35] APN[ims] PDN-Type[1] IPv4[10.46.0.4] IPv6[] (../src/upf/context.c:498)
11/12 13:01:57.171: [upf] INFO: UE F-SEID[UP:0xcd CP:0xf35] APN[ims] PDN-Type[1] IPv4[10.46.0.4] IPv6[] (../src/upf/context.c:498)
11/12 13:03:18.034: [upf] INFO: [Removed] Number of UPF-sessions is now 2 (../src/upf/context.c:252)
11/12 13:03:18.751: [upf] INFO: [Added] Number of UPF-Sessions is now 3 (../src/upf/context.c:208)
```

UPF LOGS

IE (Information Elements) Message Tracing

Information Elements (IEs) are structured data units used in 5G signaling messages. Capturing and analyzing these elements with Wireshark/Tshark provides valuable insights into message exchanges.

Common 5G Protocols and Key IEs:

- NGAP (N2 interface): UEContextRelease, InitialUEMessage, PDU Session Resource Setup Request.
- GTPv1-U (N3 interface): Tunnel Endpoint Identifier (TEID), Sequence Number, QoS Flow Identifier.
- PFCP (N4 interface): Session Establishment, FAR, PDR, URR.

Example Tshark command to capture NGAP messages:

```
sudo tshark -i any -f "port 38412" -Y "ngap" -O ngap
```

a. Locating and Viewing Logs

- Tshark can save packet captures for later analysis or display live traces. Here’s how you can capture, save, and view logs:

- Capture packets to a file:

```
sudo tshark -i any -w 5g_core_capture.pcapng
```

- View captured logs:

```
sudo tshark -r 5g_core_capture.pcapng
```

- To extract specific protocol logs:

```
sudo tshark -r 5g_core_capture.pcapng -Y "ngap" -O ngap
```

b. How to Filter Messages

Filtering messages is crucial to focus on relevant traffic. Tshark and Wireshark offer flexible filtering options.

Common 5G Core Filters:

- NGAP messages: ngap
- GTPv1-U packets: gtp
- PFCP messages: pfcp
- NAS signaling: nas-5gs

Example filters:

- Capture only Initial UE messages:

```
sudo tshark -i any -Y "ngap.InitialUEMessage"
```

- Filter PDU Session Setup messages:

```
sudo tshark -i any -Y "ngap.PDUSessionResourceSetupRequest"
```

- Show packets to/from a specific IP:

```
sudo tshark -i any -f "host 192.168.15.10"
```

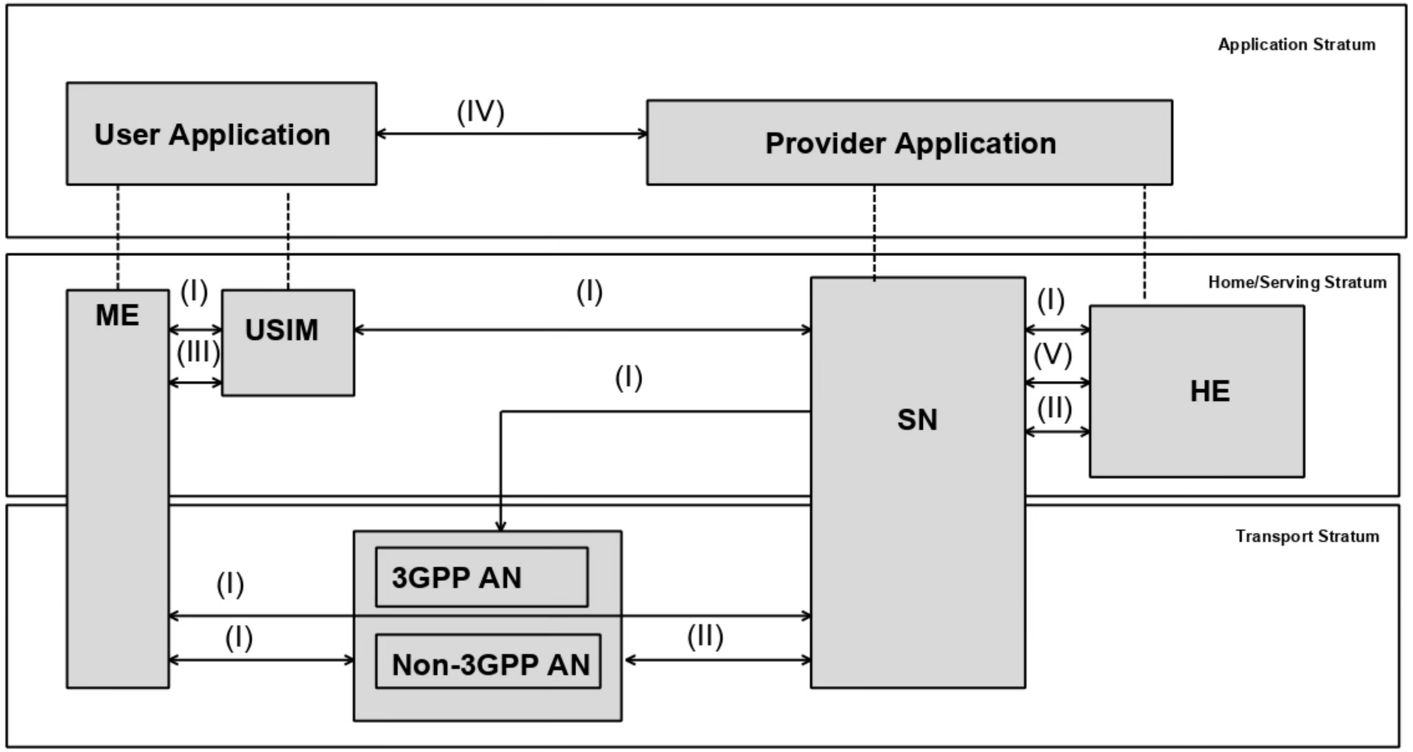
- Filtering in Wireshark GUI:
  - Use the display filter bar to apply filters interactively.
  - Example:

```
pfcp && ip.addr == IP_address_of_machine
```

QoS and Security

5G Core Security

The 5G Core (5GC) network introduces advanced security mechanisms to protect network communication, user authentication, and data exchange across different network domains. The security framework is structured into multiple security domains to ensure comprehensive protection against potential threats.



Security domain architecture

5G Core Security Framework – Key Domains & Features

Security Domains:

- Network Access Security: Secure UE authentication and access for 3GPP & Non-3GPP networks.
- Network Domain Security: Secure signaling and user plane data exchange.
- User Domain Security: Secure UE access control.
- Application Domain Security: Secure message exchange between user and provider apps.
- SBA Domain Security: Protects network element registration, discovery, and authorization.
- Visibility & Configurability: Displays whether security features are active.

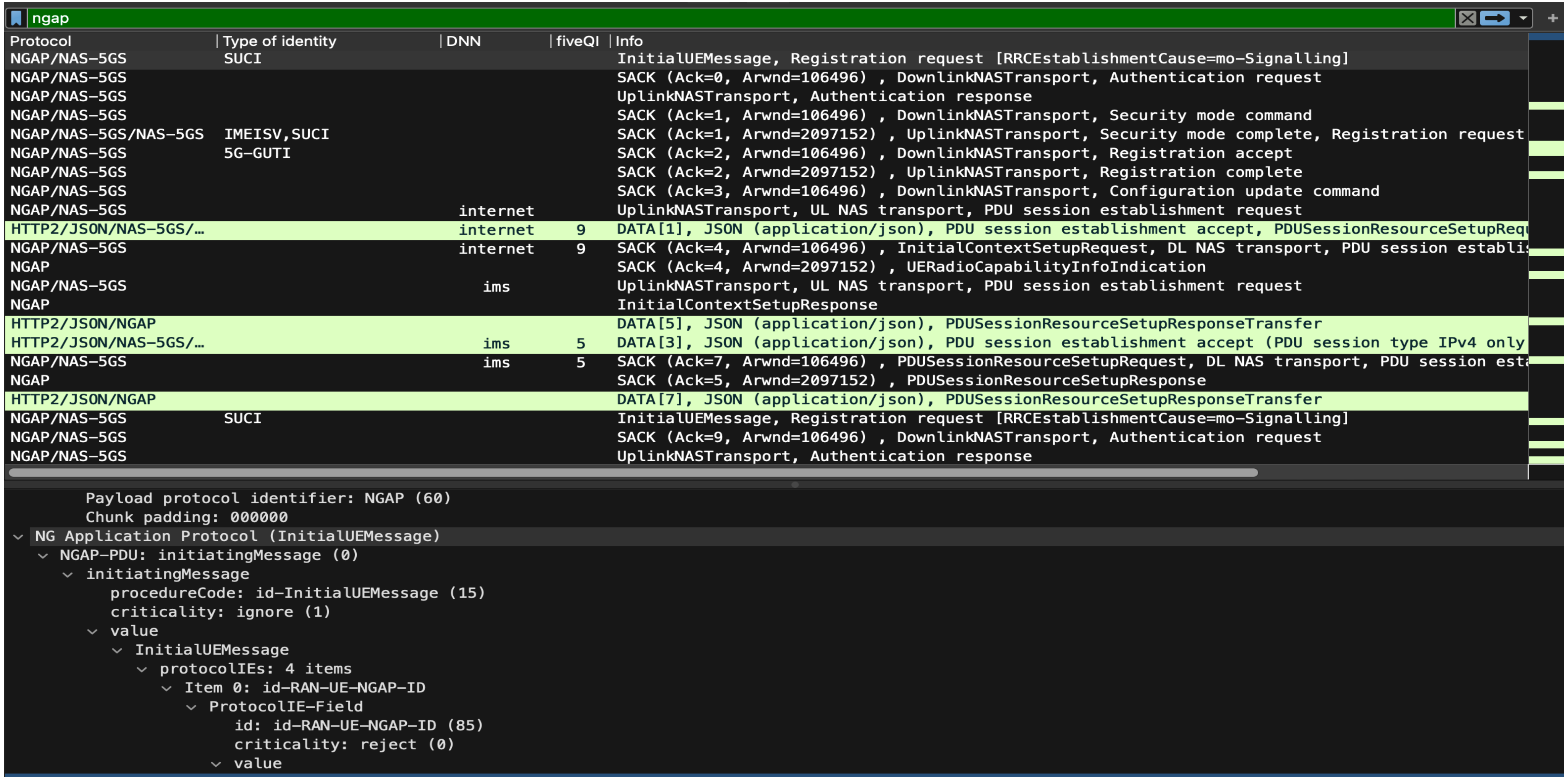
Key 5G Security Features (3GPP):

- Increased Home Control: Prevents IMSI interception by verifying device location during roaming.
- Unified Authentication: Common authentication for 3GPP & non-3GPP access (e.g., Wi-Fi).
- Security Anchor Function (SEAF): Enables re-authentication across networks without full authentication.
- Subscriber Privacy: Uses SUPI (instead of IMSI) concealed with SUCI to prevent identity exposure.

Security Entities in the 5G Core

1. AUSF (Authentication Server Function)
2. ARPF (Authentication Credential Repository and Processing Function)
3. SIDF (Subscription Identifier De-concealing Function)
4. SEAF (Security Anchor Function)

5G Core Security:

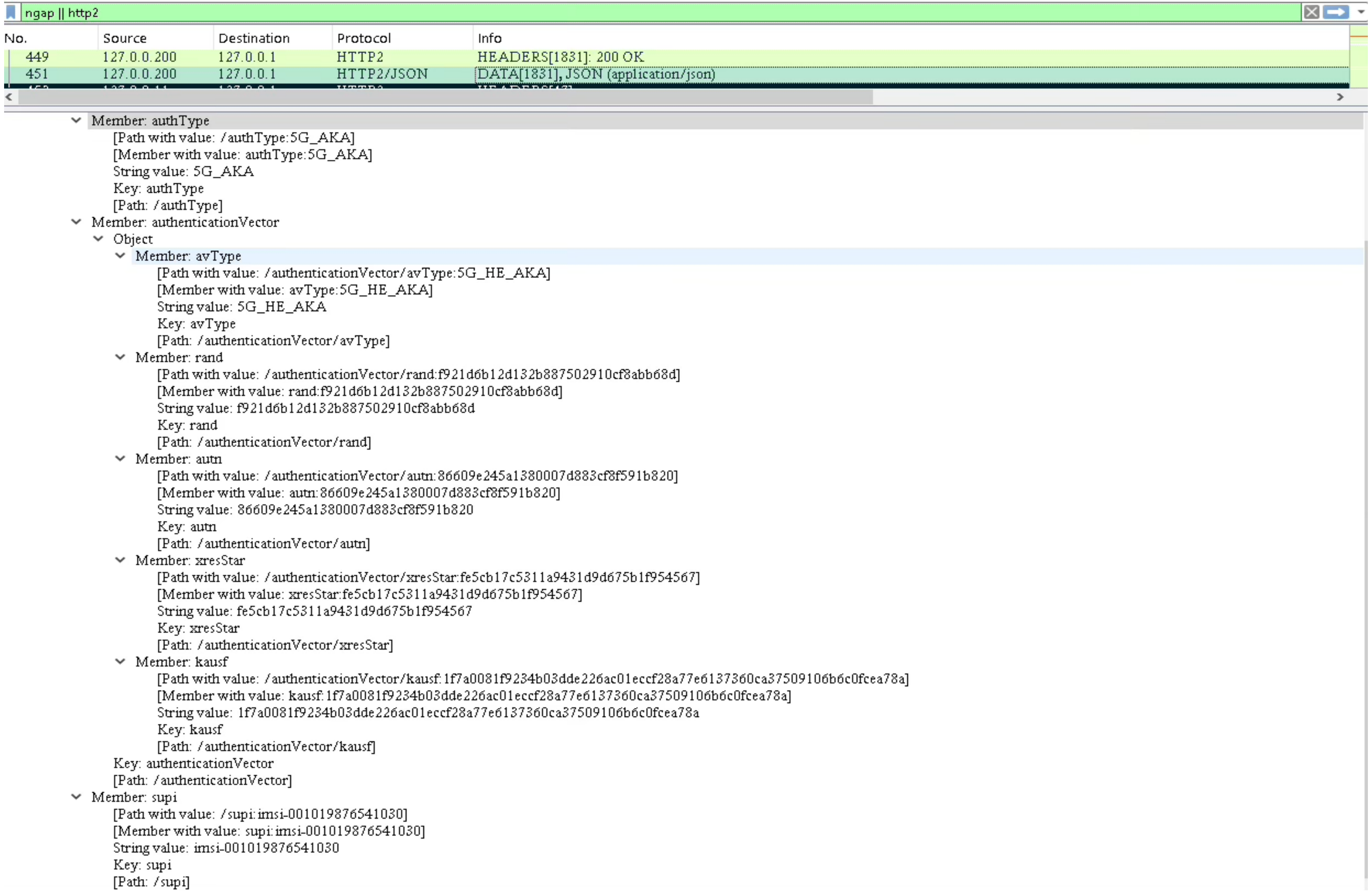


```
Protocol              | Type of identity     | DNN      | fiveQI | Info
NGAP/NAS-5GS            SUCI                                       InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
NGAP/NAS-5GS                                                       SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request
NGAP/NAS-5GS                                                       UplinkNASTransport, Authentication response
NGAP/NAS-5GS                                                       SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command
NGAP/NAS-5GS/NAS-5GS    IMEISV,SUCI                                SACK (Ack=1, Arwnd=2097152) , UplinkNASTransport, Security mode complete, Registration request
NGAP/NAS-5GS            5G-GUTI                                    SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Registration accept
NGAP/NAS-5GS                                                       SACK (Ack=2, Arwnd=2097152) , UplinkNASTransport, Registration complete
NGAP/NAS-5GS                                                       SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Configuration update command
NGAP/NAS-5GS                                   internet            UplinkNASTransport, UL NAS transport, PDU session establishment request
HTTP2/JSON/NAS-5GS/…                           internet     9      DATA[1], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequ
NGAP/NAS-5GS                                   internet     9      SACK (Ack=4, Arwnd=106496) , InitialContextSetupRequest, DL NAS transport, PDU session establi
NGAP                                                               SACK (Ack=4, Arwnd=2097152) , UERadioCapabilityInfoIndication
NGAP/NAS-5GS                                     ims               UplinkNASTransport, UL NAS transport, PDU session establishment request
NGAP                                                               InitialContextSetupResponse
HTTP2/JSON/NGAP                                                    DATA[5], JSON (application/json), PDUSessionResourceSetupResponseTransfer
HTTP2/JSON/NAS-5GS/…                             ims        5      DATA[3], JSON (application/json), PDU session establishment accept (PDU session type IPv4 only
NGAP/NAS-5GS                                     ims        5      SACK (Ack=7, Arwnd=106496) , PDUSessionResourceSetupRequest, DL NAS transport, PDU session esta
NGAP                                                               SACK (Ack=5, Arwnd=2097152) , PDUSessionResourceSetupResponse
HTTP2/JSON/NGAP                                                    DATA[7], JSON (application/json), PDUSessionResourceSetupResponseTransfer
NGAP/NAS-5GS            SUCI                                       InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
NGAP/NAS-5GS                                                       SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Authentication request
NGAP/NAS-5GS                                                       UplinkNASTransport, Authentication response
```

```
      Payload protocol identifier: NGAP (60)
      Chunk padding: 000000
v NG Application Protocol (InitialUEMessage)
  v NGAP-PDU: initiatingMessage (0)
    v initiatingMessage
        procedureCode: id-InitialUEMessage (15)
        criticality: ignore (1)
      v value
        v InitialUEMessage
          v protocolIEs: 4 items
            v Item 0: id-RAN-UE-NGAP-ID
              v ProtocolIE-Field
                  id: id-RAN-UE-NGAP-ID (85)
                  criticality: reject (0)
                v value
```

Initial-UE Message with SUCI

5G Core Security:

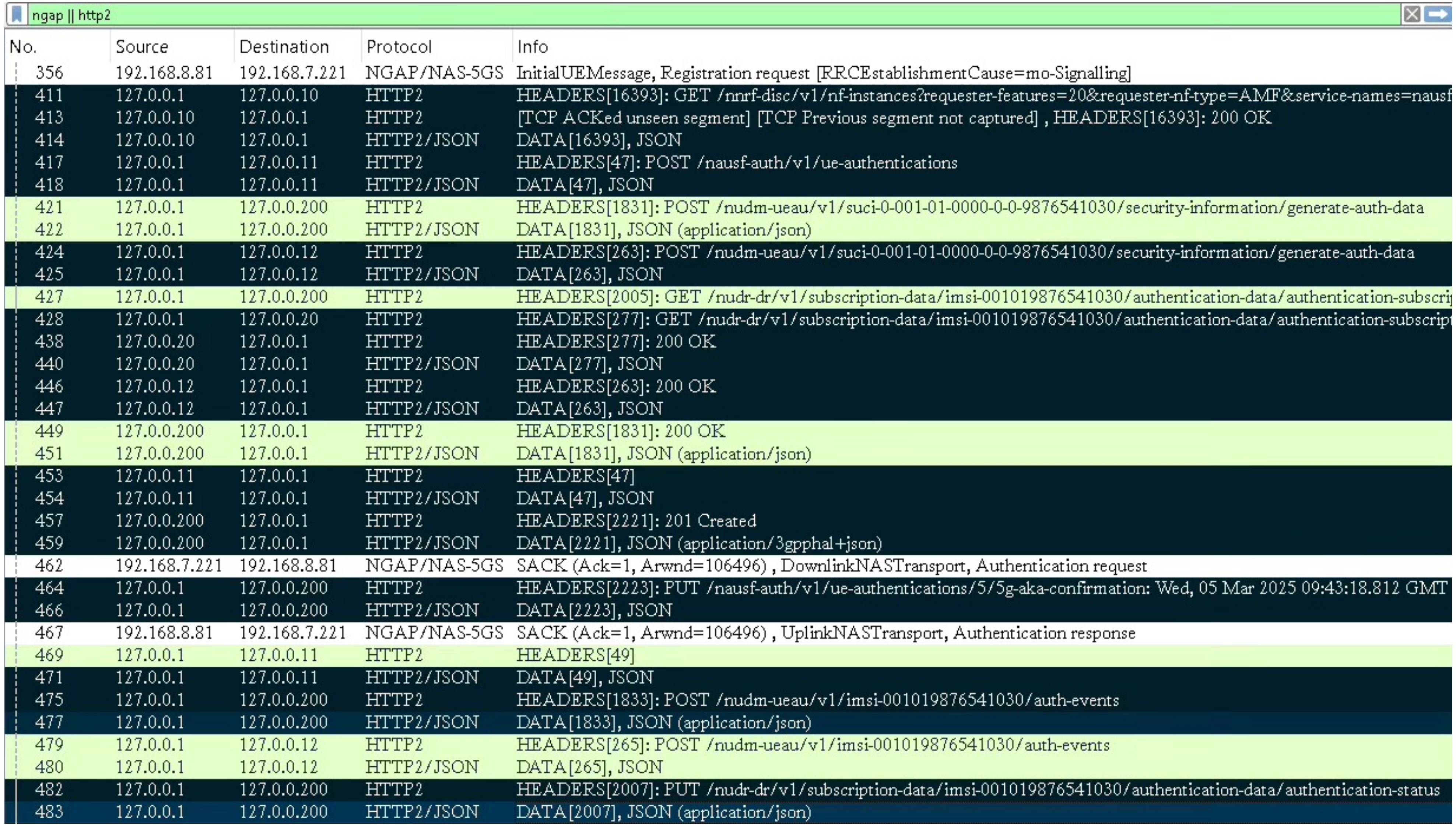


```
ngap || http2

No.    Source        Destination   Protocol      Info
449    127.0.0.200   127.0.0.1     HTTP2         HEADERS[1831]: 200 OK
451    127.0.0.200   127.0.0.1     HTTP2/JSON    DATA[1831], JSON (application/json)
```

```
    Member: authType
        [Path with value: /authType:5G_AKA]
        [Member with value: authType:5G_AKA]
        String value: 5G_AKA
        Key: authType
        [Path: /authType]
    Member: authenticationVector
        Object
            Member: avType
                [Path with value: /authenticationVector/avType:5G_HE_AKA]
                [Member with value: avType:5G_HE_AKA]
                String value: 5G_HE_AKA
                Key: avType
                [Path: /authenticationVector/avType]
            Member: rand
                [Path with value: /authenticationVector/rand:f921d6b12d132b887502910cf8abb68d]
                [Member with value: rand:f921d6b12d132b887502910cf8abb68d]
                String value: f921d6b12d132b887502910cf8abb68d
                Key: rand
                [Path: /authenticationVector/rand]
            Member: autn
                [Path with value: /authenticationVector/autn:86609e245a1380007d883cf8f591b820]
                [Member with value: autn:86609e245a1380007d883cf8f591b820]
                String value: 86609e245a1380007d883cf8f591b820
                Key: autn
                [Path: /authenticationVector/autn]
            Member: xresStar
                [Path with value: /authenticationVector/xresStar:fe5cb17c5311a9431d9d675b1f954567]
                [Member with value: xresStar:fe5cb17c5311a9431d9d675b1f954567]
                String value: fe5cb17c5311a9431d9d675b1f954567
                Key: xresStar
                [Path: /authenticationVector/xresStar]
            Member: kausf
                [Path with value: /authenticationVector/kausf:1f7a0081f9234b03dde226ac01eccf28a77e6137360ca37509106b6c0fcea78a]
                [Member with value: kausf:1f7a0081f9234b03dde226ac01eccf28a77e6137360ca37509106b6c0fcea78a]
                String value: 1f7a0081f9234b03dde226ac01eccf28a77e6137360ca37509106b6c0fcea78a
                Key: kausf
                [Path: /authenticationVector/kausf]
        Key: authenticationVector
        [Path: /authenticationVector]
    Member: supi
        [Path with value: /supi:imsi-001019876541030]
        [Member with value: supi:imsi-001019876541030]
        String value: imsi-001019876541030
        Key: supi
        [Path: /supi]
```

Authentication-vectors in 5G Core

5G Core Security:

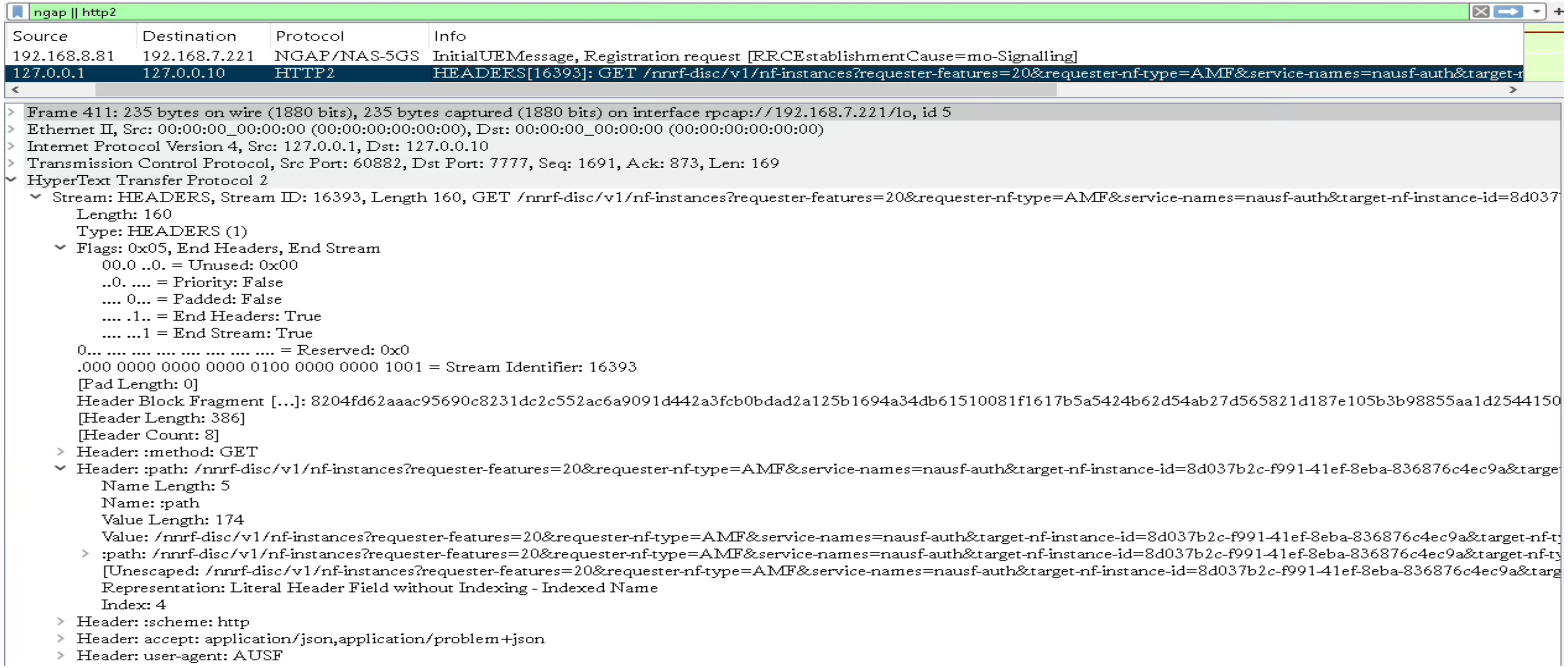


ngap || http2

No.	Source	Destination	Protocol	Info
356	192.168.8.81	192.168.7.221	NGAP/NAS-5GS	InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
411	127.0.0.1	127.0.0.10	HTTP2	HEADERS[16393]: GET /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf
413	127.0.0.10	127.0.0.1	HTTP2	[TCP ACKed unseen segment] [TCP Previous segment not captured] , HEADERS[16393]: 200 OK
414	127.0.0.10	127.0.0.1	HTTP2/JSON	DATA[16393], JSON
417	127.0.0.1	127.0.0.11	HTTP2	HEADERS[47]: POST /nausf-auth/v1/ue-authentications
418	127.0.0.1	127.0.0.11	HTTP2/JSON	DATA[47], JSON
421	127.0.0.1	127.0.0.200	HTTP2	HEADERS[1831]: POST /nudm-ueau/v1/suci-0-001-01-0000-0-0-9876541030/security-information/generate-auth-data
422	127.0.0.1	127.0.0.200	HTTP2/JSON	DATA[1831], JSON (application/json)
424	127.0.0.1	127.0.0.12	HTTP2	HEADERS[263]: POST /nudm-ueau/v1/suci-0-001-01-0000-0-0-9876541030/security-information/generate-auth-data
425	127.0.0.1	127.0.0.12	HTTP2/JSON	DATA[263], JSON
427	127.0.0.1	127.0.0.200	HTTP2	HEADERS[2005]: GET /nudr-dr/v1/subscription-data/imsi-001019876541030/authentication-data/authentication-subscri
428	127.0.0.1	127.0.0.20	HTTP2	HEADERS[277]: GET /nudr-dr/v1/subscription-data/imsi-001019876541030/authentication-data/authentication-subscript
438	127.0.0.20	127.0.0.1	HTTP2	HEADERS[277]: 200 OK
440	127.0.0.20	127.0.0.1	HTTP2/JSON	DATA[277], JSON
446	127.0.0.12	127.0.0.1	HTTP2	HEADERS[263]: 200 OK
447	127.0.0.12	127.0.0.1	HTTP2/JSON	DATA[263], JSON
449	127.0.0.200	127.0.0.1	HTTP2	HEADERS[1831]: 200 OK
451	127.0.0.200	127.0.0.1	HTTP2/JSON	DATA[1831], JSON (application/json)
453	127.0.0.11	127.0.0.1	HTTP2	HEADERS[47]
454	127.0.0.11	127.0.0.1	HTTP2/JSON	DATA[47], JSON
457	127.0.0.200	127.0.0.1	HTTP2	HEADERS[2221]: 201 Created
459	127.0.0.200	127.0.0.1	HTTP2/JSON	DATA[2221], JSON (application/3gpphal+json)
462	192.168.7.221	192.168.8.81	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request
464	127.0.0.1	127.0.0.200	HTTP2	HEADERS[2223]: PUT /nausf-auth/v1/ue-authentications/5/5g-aka-confirmation: Wed, 05 Mar 2025 09:43:18.812 GMT
466	127.0.0.1	127.0.0.200	HTTP2/JSON	DATA[2223], JSON
467	192.168.8.81	192.168.7.221	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response
469	127.0.0.1	127.0.0.11	HTTP2	HEADERS[49]
471	127.0.0.1	127.0.0.11	HTTP2/JSON	DATA[49], JSON
475	127.0.0.1	127.0.0.200	HTTP2	HEADERS[1833]: POST /nudm-ueau/v1/imsi-001019876541030/auth-events
477	127.0.0.1	127.0.0.200	HTTP2/JSON	DATA[1833], JSON (application/json)
479	127.0.0.1	127.0.0.12	HTTP2	HEADERS[265]: POST /nudm-ueau/v1/imsi-001019876541030/auth-events
480	127.0.0.1	127.0.0.12	HTTP2/JSON	DATA[265], JSON
482	127.0.0.1	127.0.0.200	HTTP2	HEADERS[2007]: PUT /nudr-dr/v1/subscription-data/imsi-001019876541030/authentication-data/authentication-status
483	127.0.0.1	127.0.0.200	HTTP2/JSON	DATA[2007], JSON (application/json)

HTTP/2 and NGAP Packets for AKA

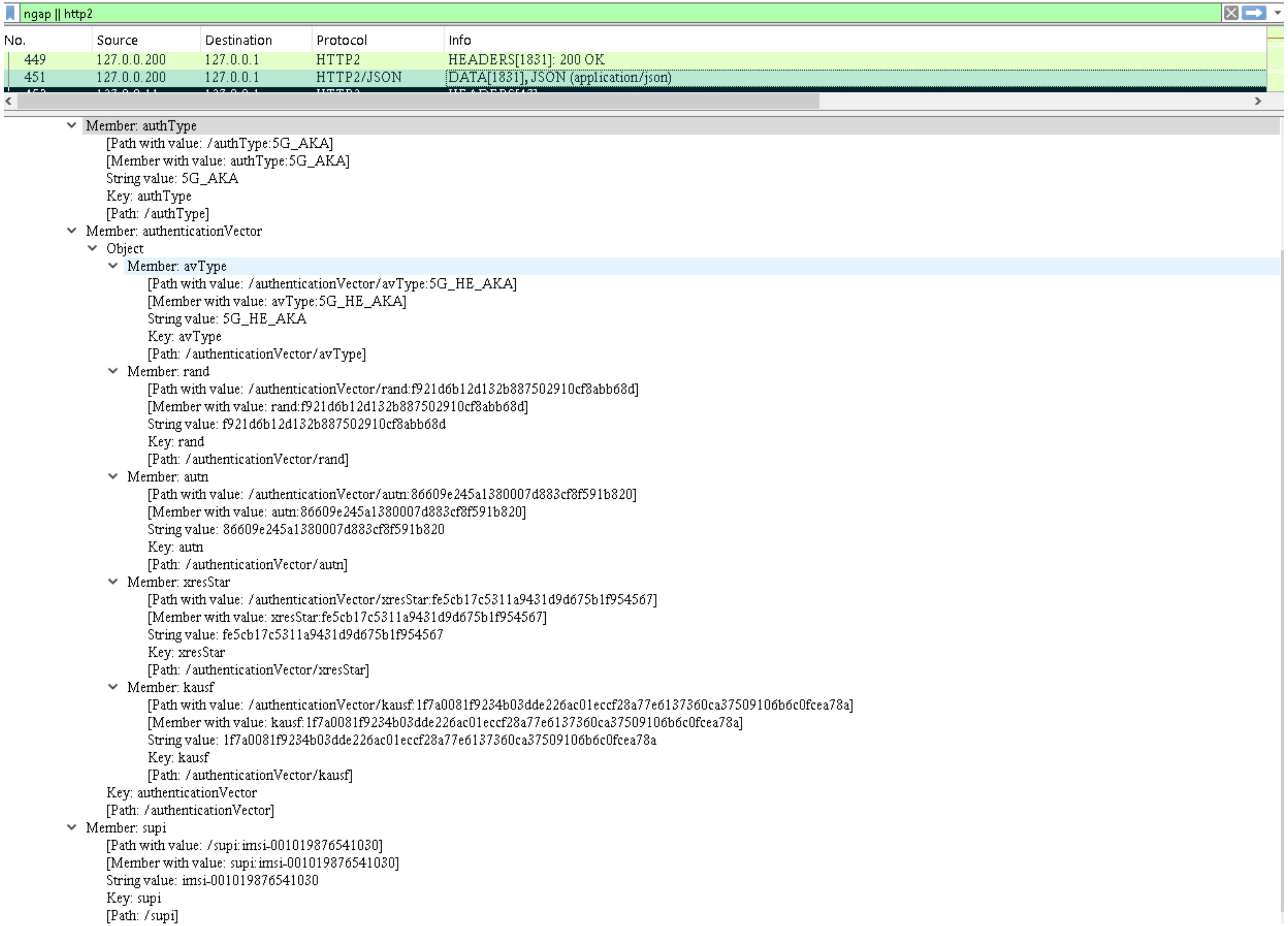
5G Core Security



```
ngap || http2

Source          Destination     Protocol       Info
192.168.8.81    192.168.7.221   NGAP/NAS-5GS   InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
127.0.0.1       127.0.0.10      HTTP2          HEADERS[16393]: GET /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-r

> Frame 411: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits) on interface rpcap://192.168.7.221/lo, id 5
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.10
> Transmission Control Protocol, Src Port: 60882, Dst Port: 7777, Seq: 1691, Ack: 873, Len: 169
v HyperText Transfer Protocol 2
  v Stream: HEADERS, Stream ID: 16393, Length 160, GET /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-nf-instance-id=8d037
      Length: 160
      Type: HEADERS (1)
    v Flags: 0x05, End Headers, End Stream
        00.0 ..0. = Unused: 0x00
        ..0. .... = Priority: False
        .... 0... = Padded: False
        .... .1.. = End Headers: True
        .... ...1 = End Stream: True
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0100 0000 0000 1001 = Stream Identifier: 16393
      [Pad Length: 0]
      Header Block Fragment […]: 8204fd62aaac95690c8231dc2c552ac6a9091d442a3fcb0bdad2a125b1694a34db61510081f1617b5a5424b62d54ab27d565821d187e105b3b98855aa1d2544150
      [Header Length: 386]
      [Header Count: 8]
    > Header: :method: GET
    v Header: :path: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-nf-instance-id=8d037b2c-f991-41ef-8eba-836876c4ec9a&targe
        Name Length: 5
        Name: :path
        Value Length: 174
        Value: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-nf-instance-id=8d037b2c-f991-41ef-8eba-836876c4ec9a&target-nf-ty
      > :path: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-nf-instance-id=8d037b2c-f991-41ef-8eba-836876c4ec9a&target-nf-ty
        [Unescaped: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-nf-instance-id=8d037b2c-f991-41ef-8eba-836876c4ec9a&targ
        Representation: Literal Header Field without Indexing - Indexed Name
        Index: 4
    > Header: :scheme: http
    > Header: accept: application/json,application/problem+json
    > Header: user-agent: AUSF
```

AUSF ue-authentication

5G Core Security



```
ngap || http2

No.    Source        Destination   Protocol      Info
449    127.0.0.200   127.0.0.1     HTTP2         HEADERS[1831]: 200 OK
451    127.0.0.200   127.0.0.1     HTTP2/JSON    DATA[1831], JSON (application/json)
```

```
Member: authType
    [Path with value: /authType:5G_AKA]
    [Member with value: authType:5G_AKA]
    String value: 5G_AKA
    Key: authType
    [Path: /authType]
Member: authenticationVector
    Object
        Member: avType
            [Path with value: /authenticationVector/avType:5G_HE_AKA]
            [Member with value: avType:5G_HE_AKA]
            String value: 5G_HE_AKA
            Key: avType
            [Path: /authenticationVector/avType]
        Member: rand
            [Path with value: /authenticationVector/rand:f921d6b12d132b887502910cf8abb68d]
            [Member with value: rand:f921d6b12d132b887502910cf8abb68d]
            String value: f921d6b12d132b887502910cf8abb68d
            Key: rand
            [Path: /authenticationVector/rand]
        Member: autn
            [Path with value: /authenticationVector/autn:86609e245a1380007d883cf8f591b820]
            [Member with value: autn:86609e245a1380007d883cf8f591b820]
            String value: 86609e245a1380007d883cf8f591b820
            Key: autn
            [Path: /authenticationVector/autn]
        Member: xresStar
            [Path with value: /authenticationVector/xresStar:fe5cb17c5311a9431d9d675b1f954567]
            [Member with value: xresStar:fe5cb17c5311a9431d9d675b1f954567]
            String value: fe5cb17c5311a9431d9d675b1f954567
            Key: xresStar
            [Path: /authenticationVector/xresStar]
        Member: kausf
            [Path with value: /authenticationVector/kausf:1f7a0081f9234b03dde226ac01eccf28a77e6137360ca37509106b6c0fcea78a]
            [Member with value: kausf:1f7a0081f9234b03dde226ac01eccf28a77e6137360ca37509106b6c0fcea78a]
            String value: 1f7a0081f9234b03dde226ac01eccf28a77e6137360ca37509106b6c0fcea78a
            Key: kausf
            [Path: /authenticationVector/kausf]
    Key: authenticationVector
    [Path: /authenticationVector]
Member: supi
    [Path with value: /supi:imsi-001019876541030]
    [Member with value: supi:imsi-001019876541030]
    String value: imsi-001019876541030
    Key: supi
    [Path: /supi]
```

Authentication Vectors in 5G Core

5G RAN Security:

- User Plane Integrity: Ensures both integrity and confidentiality protection.
- DTLS & IPsec: Mandates support for DTLS (Datagram Transport Layer Security) and IPsec for backhaul control (N2) and handover (Xn).
- CU/DU Security: Requires DTLS, IPsec ESP, and IKEv2 certificate-based authentication with confidentiality, integrity, and replay protection for internal RAN (F1 and E1 interfaces).
- Certificate & Software Security: Supports certificate enrollment and software update verification before installation.
- PDCP Counter Check: Detects maliciously inserted packets.
- SCTP Inspections: Implements stateful SCTP inspections (host-based or inline firewall) for Xn-C, E2, and E1 interfaces to prevent vulnerabilities.

References:
5G RAN Security
5G Core security

5G LAB

IMS

IMS (IP Multimedia Subsystem)

IP Multimedia Subsystem (IMS) is a standardized architectural framework that facilitates the delivery of rich multimedia services like voice, video, and messaging over IP networks, including Voice over New Radio (VoNR)

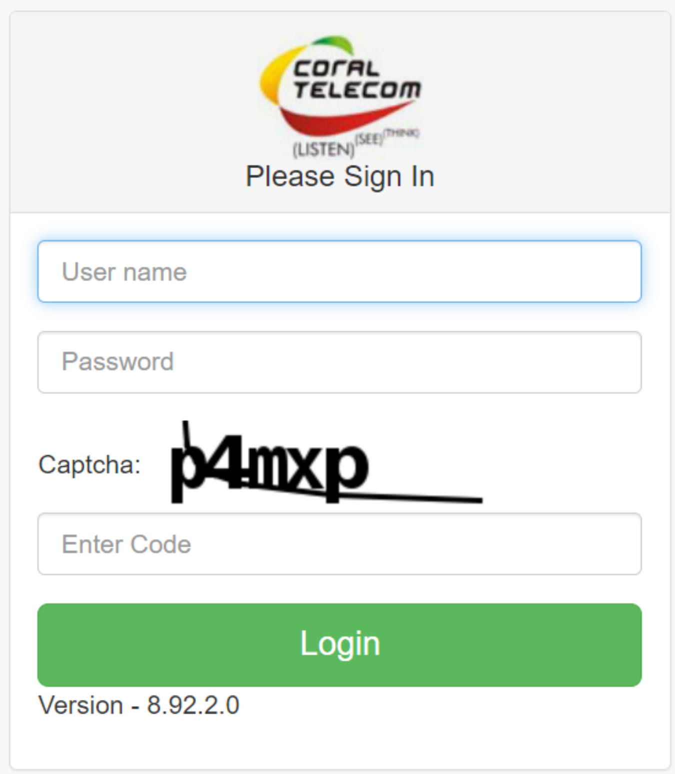
Loggin in to IMS

Step 3: - Enter the credentials

Username: - admin

Password: - admin123

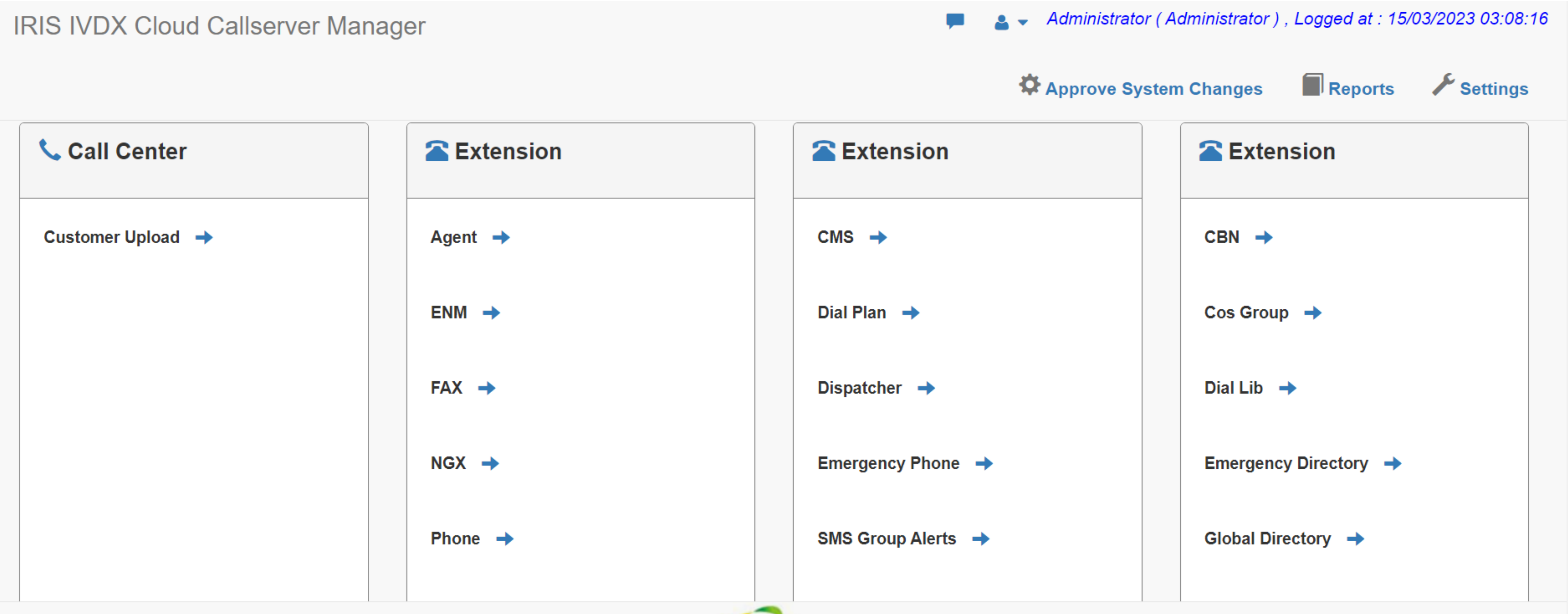
The page will be shown below



NOTE: You can also create/update/delete an extension, Trunks, & different features from GUI.

- **Extension user administration by GUI:**
- **Step 1: -** Go to web browser
- **Browser link: -**
- **https://<ip>/manager/**
- **Step 2: -** A window opens up

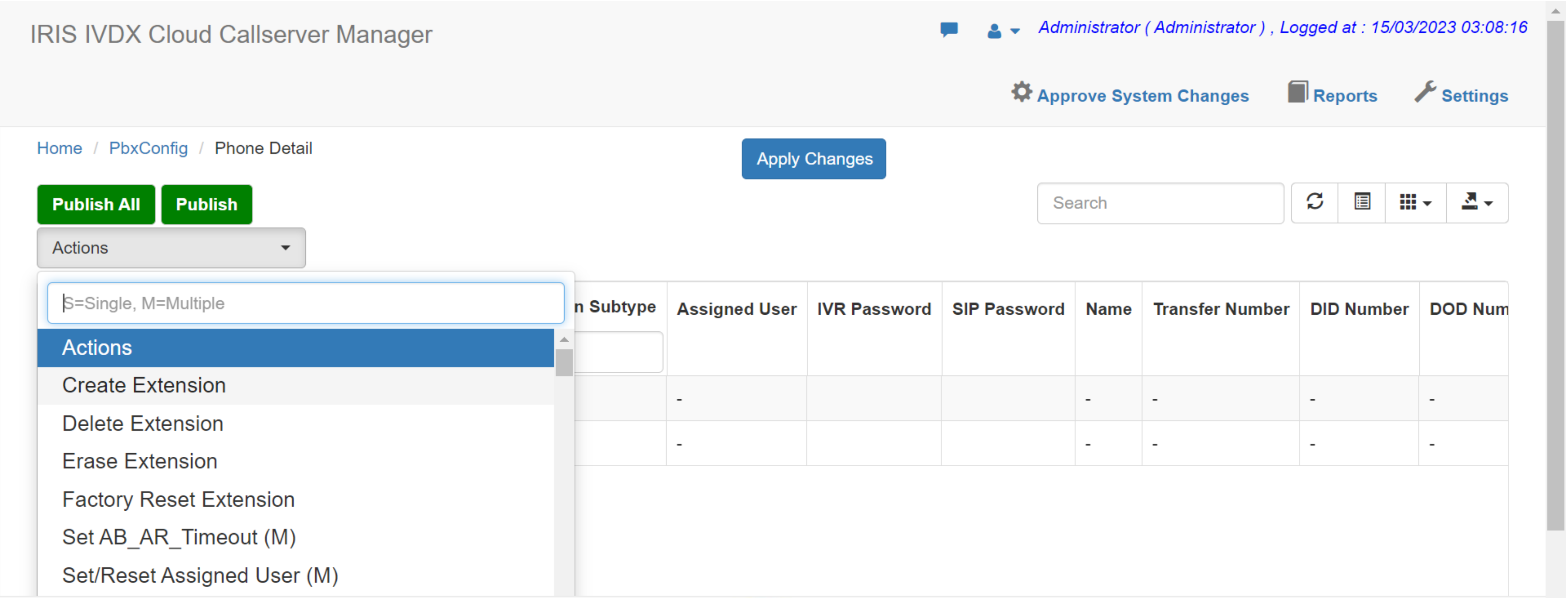
Extension (VoNR) Creation in IMS



IRIS IVDX Cloud Callserver Manager

Administrator (Administrator) , Logged at : 15/03/2023 03:08:16

Extension (VoNR) Creation in IMS



IRIS IVDX Cloud Callserver Manager

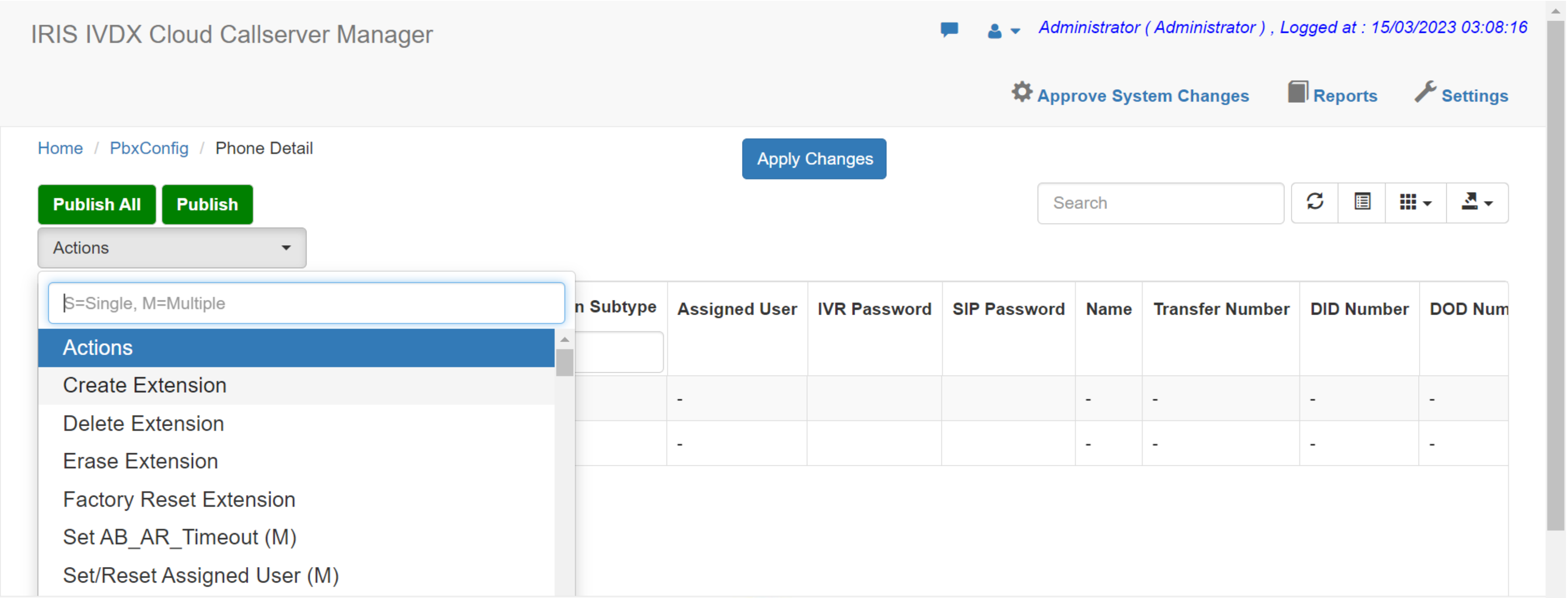
Administrator (Administrator) , Logged at : 15/03/2023 03:08:16

Home / PbxConfig / Phone Detail

S=Single, M=Multiple

n Subtype	Assigned User	IVR Password	SIP Password	Name	Transfer Number	DID Number	DOD Num
	-			-	-	-	-
	-			-	-	-	-

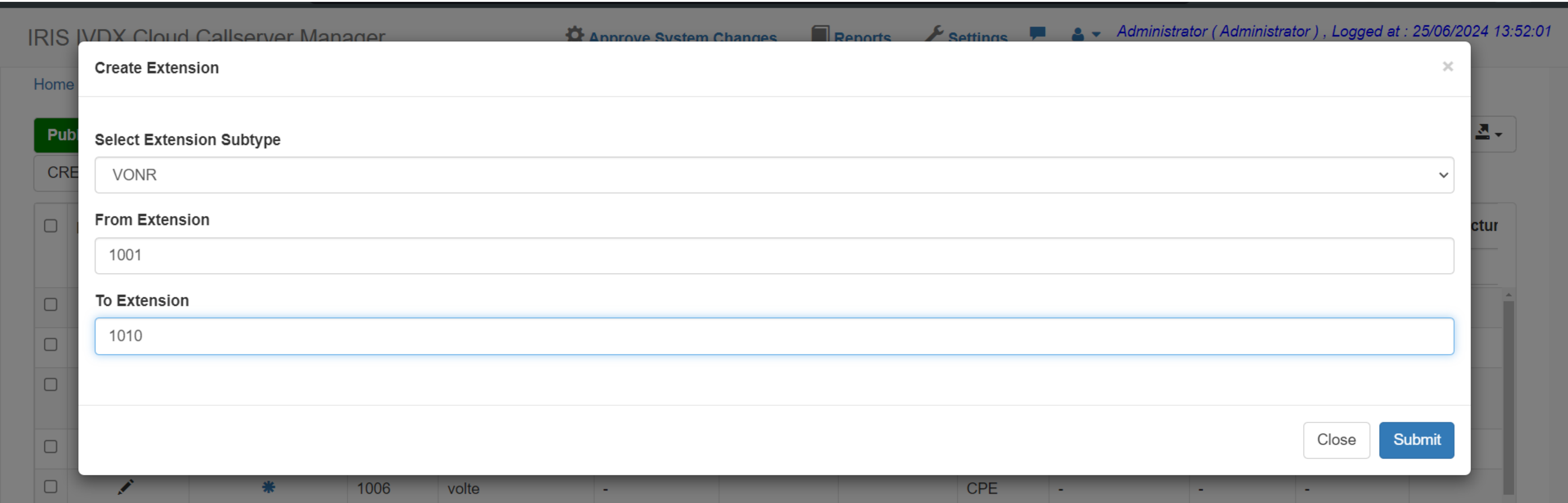
Extension (VoNR) Creation in IMS



From Extension: - <Starting Extension>

To Extension: - <Ending Extension No>

- Enter the credentials as below: -
- **Select extension Subtype: - VONR <default>**



IRIS IVDX Cloud Callserver Manager
Approve System Changes
Reports
Settings
Administrator (Administrator) , Logged at : 25/06/2024 13:52:01
Home
Pub
CRE
ctur
1006
volte
CPE

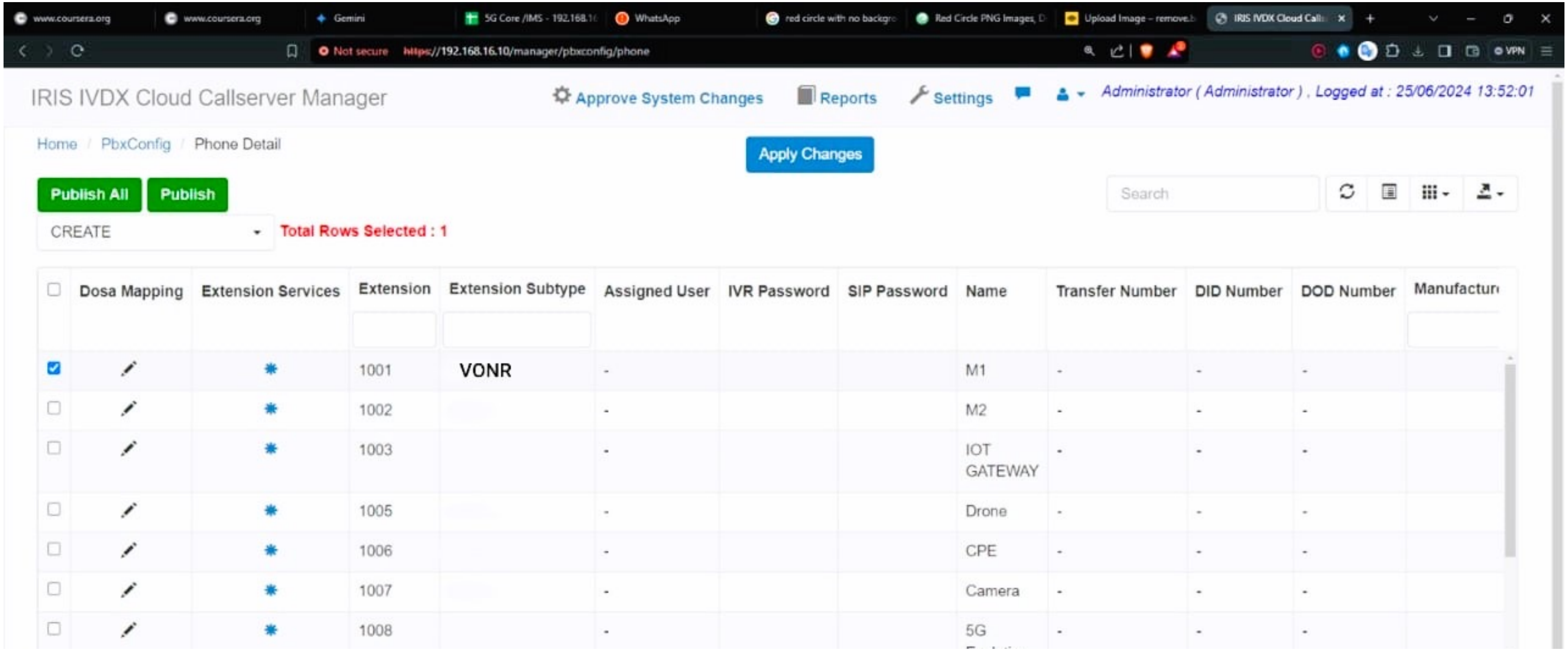
Create Extension

Select Extension Subtype: VONR

From Extension: 1001

To Extension: 1010

Extensions are now created and select the extension by clicking the dialogue box

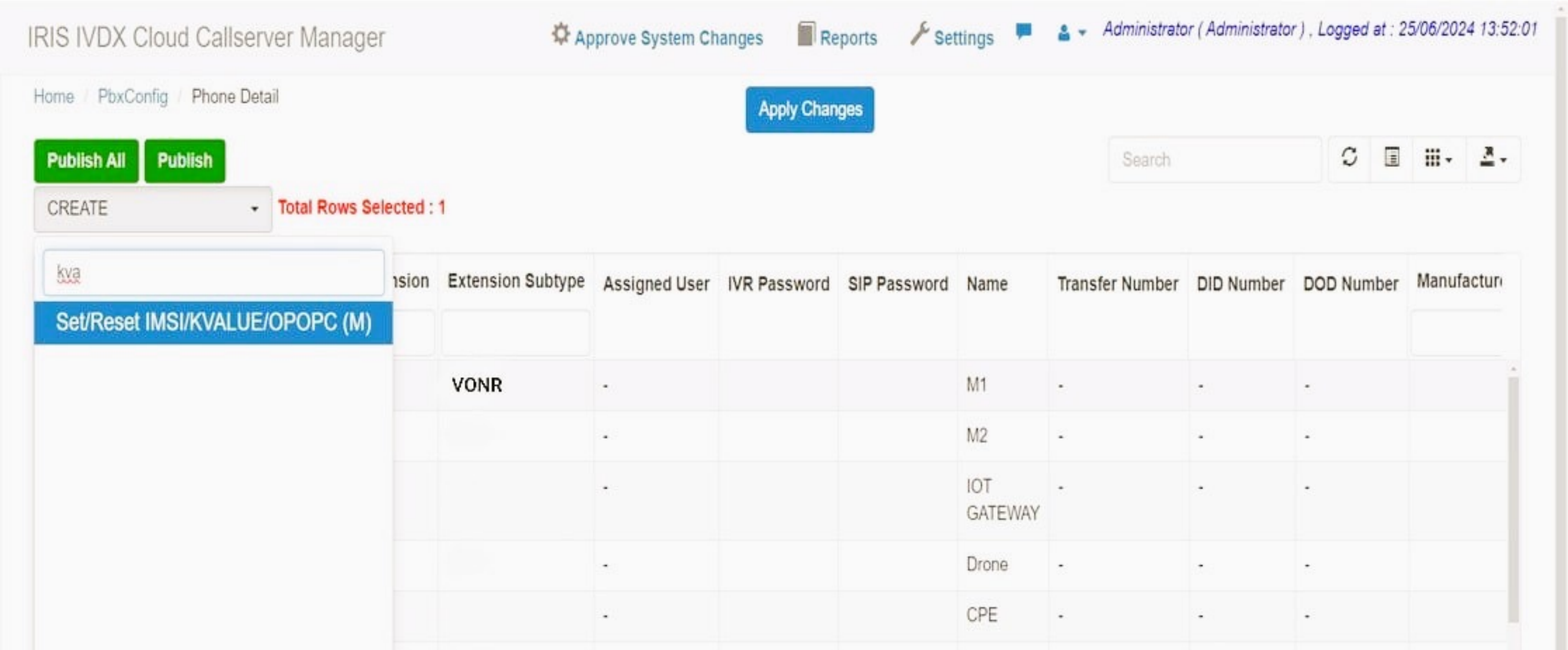


Administrator (Administrator) , Logged at : 25/06/2024 13:52:01

Total Rows Selected : 1

☐	Dosa Mapping	Extension Services	Extension	Extension Subtype	Assigned User	IVR Password	SIP Password	Name	Transfer Number	DID Number	DOD Number	Manufactur
☑	✎	✱	1001	VONR	-			M1	-	-	-	
☐	✎	✱	1002		-			M2	-	-	-	
☐	✎	✱	1003		-			IOT GATEWAY	-	-	-	
☐	✎	✱	1005		-			Drone	-	-	-	
☐	✎	✱	1006		-			CPE	-	-	-	
☐	✎	✱	1007		-			Camera	-	-	-	
☐	✎	✱	1008		-			5G	-	-	-	

Click on the dropdown box and then enter the Kval , opcval , imsival paramters



Administrator (Administrator) , Logged at : 25/06/2024 13:52:01

CREATE

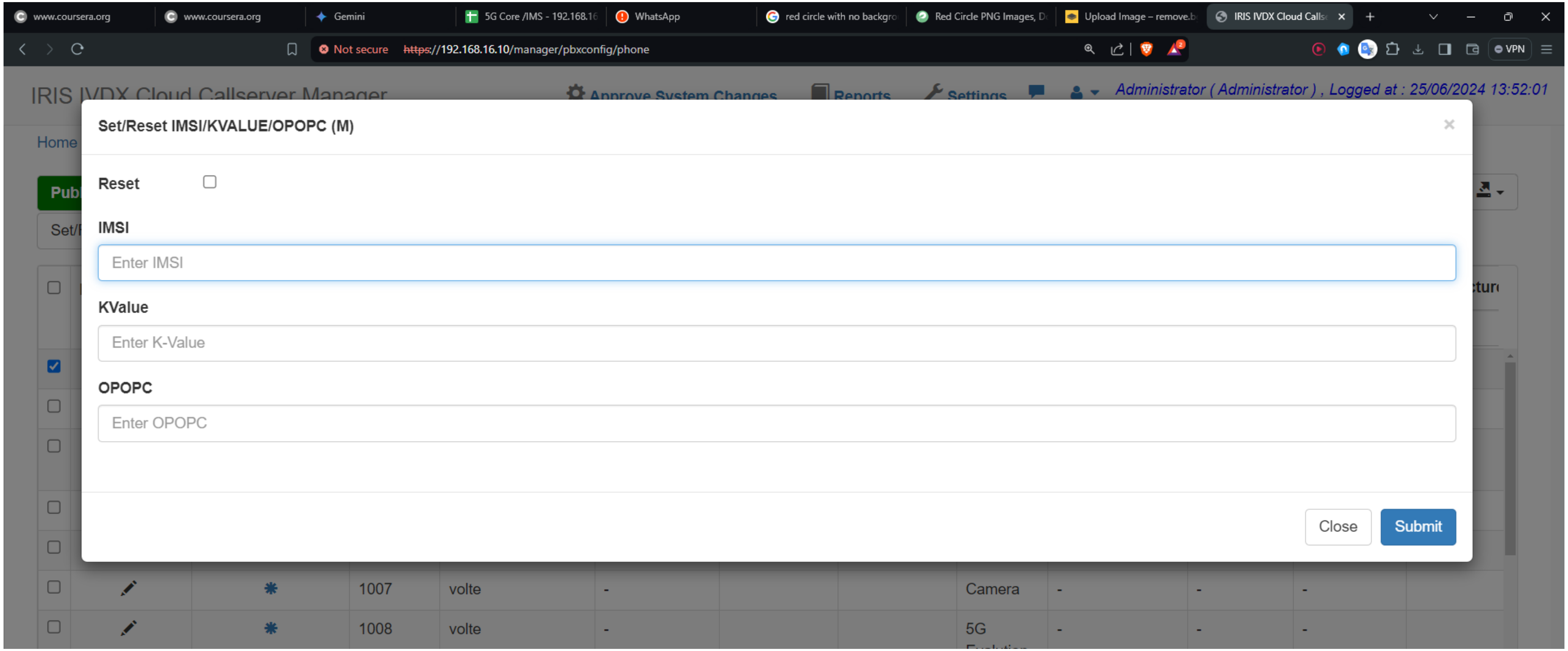
Total Rows Selected : 1

kva

Set/Reset IMSI/KVALUE/OPOPC (M)

nsion	Extension Subtype	Assigned User	IVR Password	SIP Password	Name	Transfer Number	DID Number	DOD Number	Manufactur
	VONR	-			M1	-	-	-	
		-			M2	-	-	-	
		-			IOT GATEWAY	-	-	-	
		-			Drone	-	-	-	
		-			CPE	-	-	-	

The Dialogue box will now be open like this and input the values in it respectively



Administrator (Administrator) , Logged at : 25/06/2024 13:52:01

Set/Reset IMSI/KVALUE/OPOPC (M)

Reset ☐

IMSI

Enter IMSI

KValue

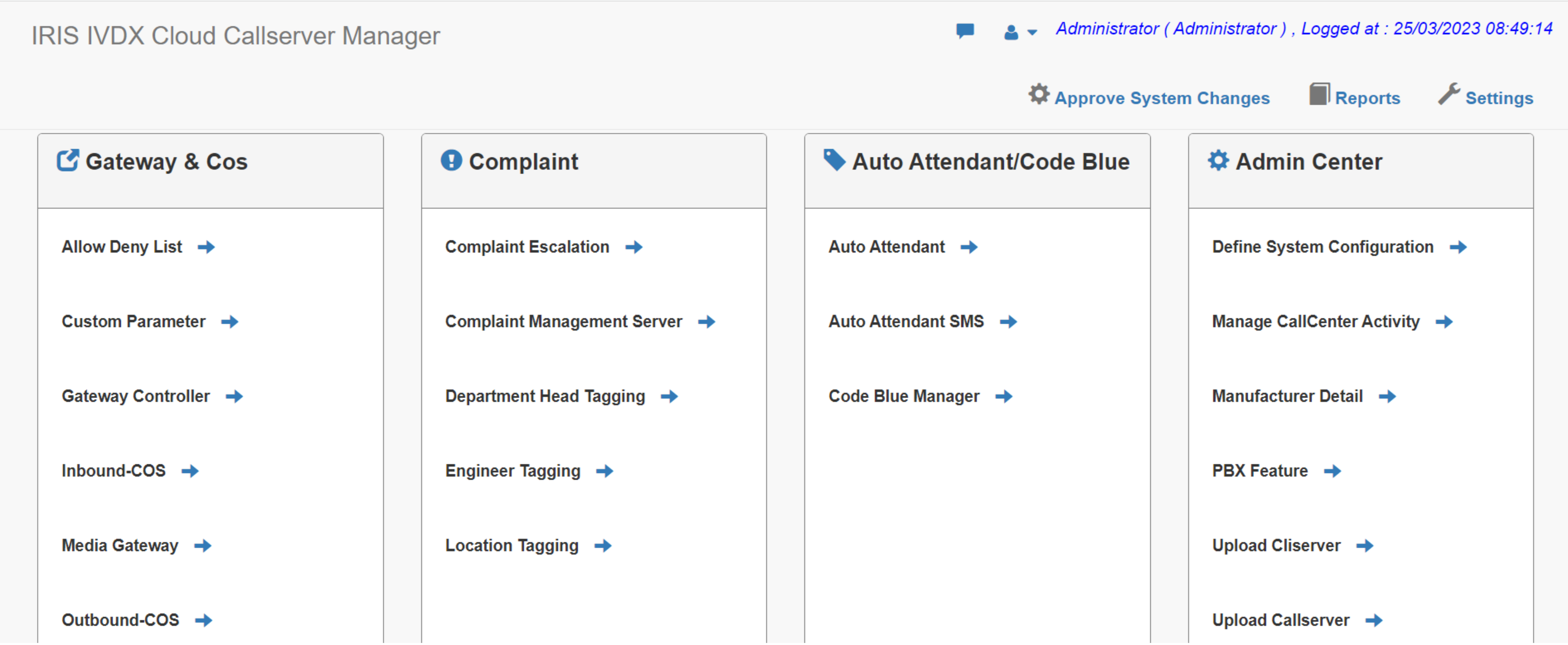
Enter K-Value

OPOPC

Enter OPOPC

☐	✎	✱	1007	volte	-			Camera	-	-	-
☐	✎	✱	1008	volte	-			5G	-	-	-

Step 2 - Configure COS (Class of service)



IRIS IVDX Cloud Callserver Manager

Administrator (Administrator) , Logged at : 25/03/2023 08:49:14

Approve System Changes | Reports | Settings

Gateway & Cos

- Allow Deny List →
- Custom Parameter →
- Gateway Controller →
- Inbound-COS →
- Media Gateway →
- Outbound-COS →

Complaint

- Complaint Escalation →
- Complaint Management Server →
- Department Head Tagging →
- Engineer Tagging →
- Location Tagging →

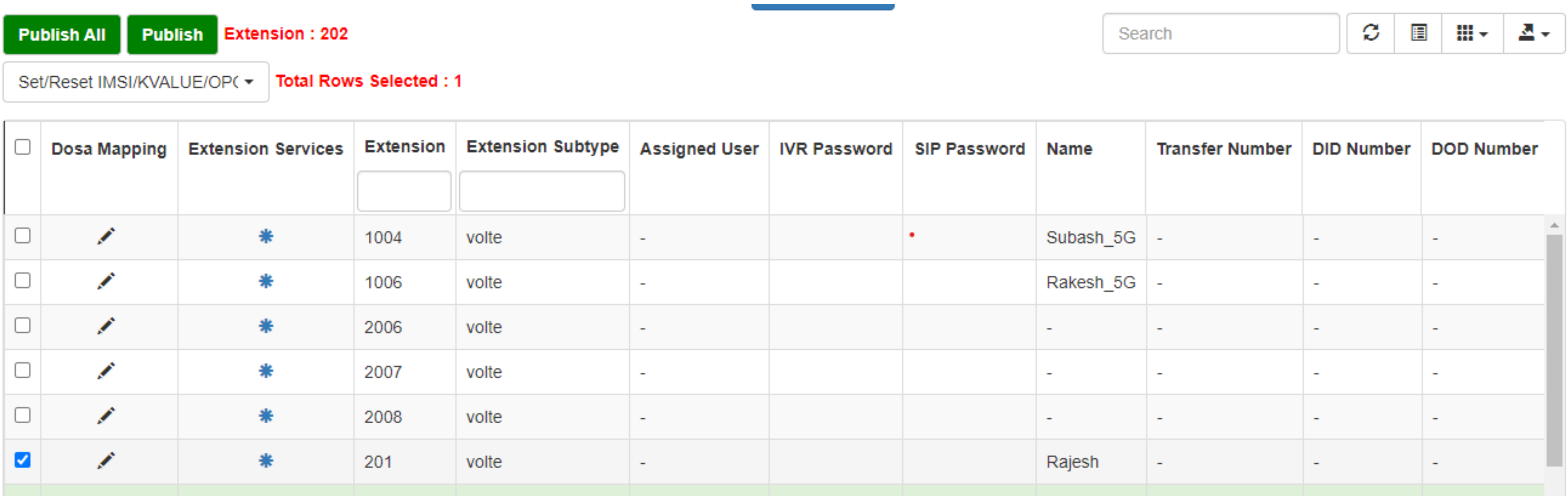
Auto Attendant/Code Blue

- Auto Attendant →
- Auto Attendant SMS →
- Code Blue Manager →

Admin Center

- Define System Configuration →
- Manage CallCenter Activity →
- Manufacturer Detail →
- PBX Feature →
- Upload Cliserver →
- Upload Callserver →

Verify extension parameters



Extension : 202

Total Rows Selected : 1

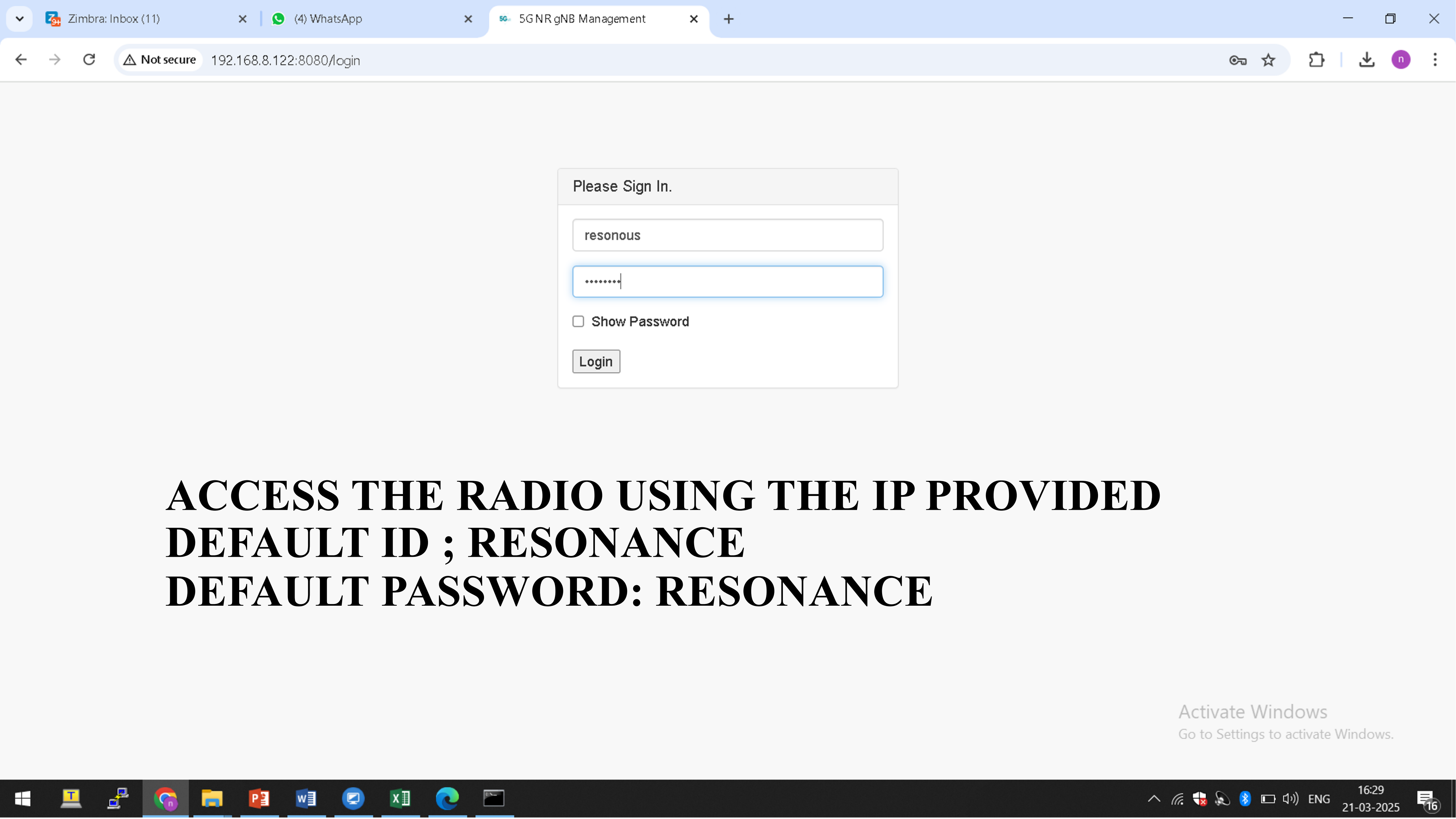
□	Dosa Mapping	Extension Services	Extension	Extension Subtype	Assigned User	IVR Password	SIP Password	Name	Transfer Number	DID Number	DOD Number
□	✎	✱	1004	volte	-		•	Subash_5G	-	-	-
□	✎	✱	1006	volte	-			Rakesh_5G	-	-	-
□	✎	✱	2006	volte	-			-	-	-	-
□	✎	✱	2007	volte	-			-	-	-	-
□	✎	✱	2008	volte	-			-	-	-	-
☑	✎	✱	201	volte	-			Rajesh	-	-	-

Live Training on IMS with user creation and VoNR Calling

5G LAB

Configuration Of 5G Radio (gNodeB)

Accessing The gNodeB Through IP Address



Please Sign In.

resonous

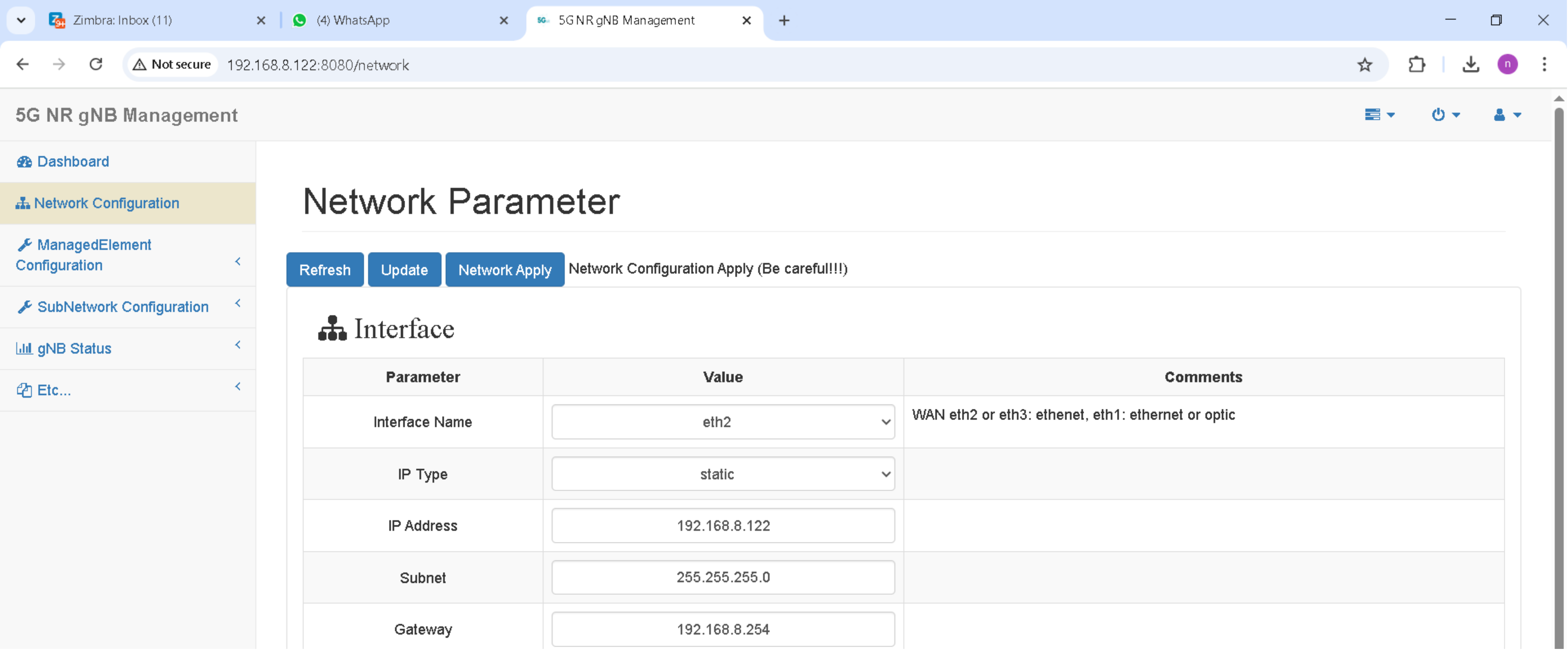
••••••••

□ Show Password

Login

ACCESS THE RADIO USING THE IP PROVIDED
DEFAULT ID ; RESONANCE
DEFAULT PASSWORD: RESONANCE

To change the IP Address of gNodeB:
-Step 1 : Go to Network Parameter and change the IP Address

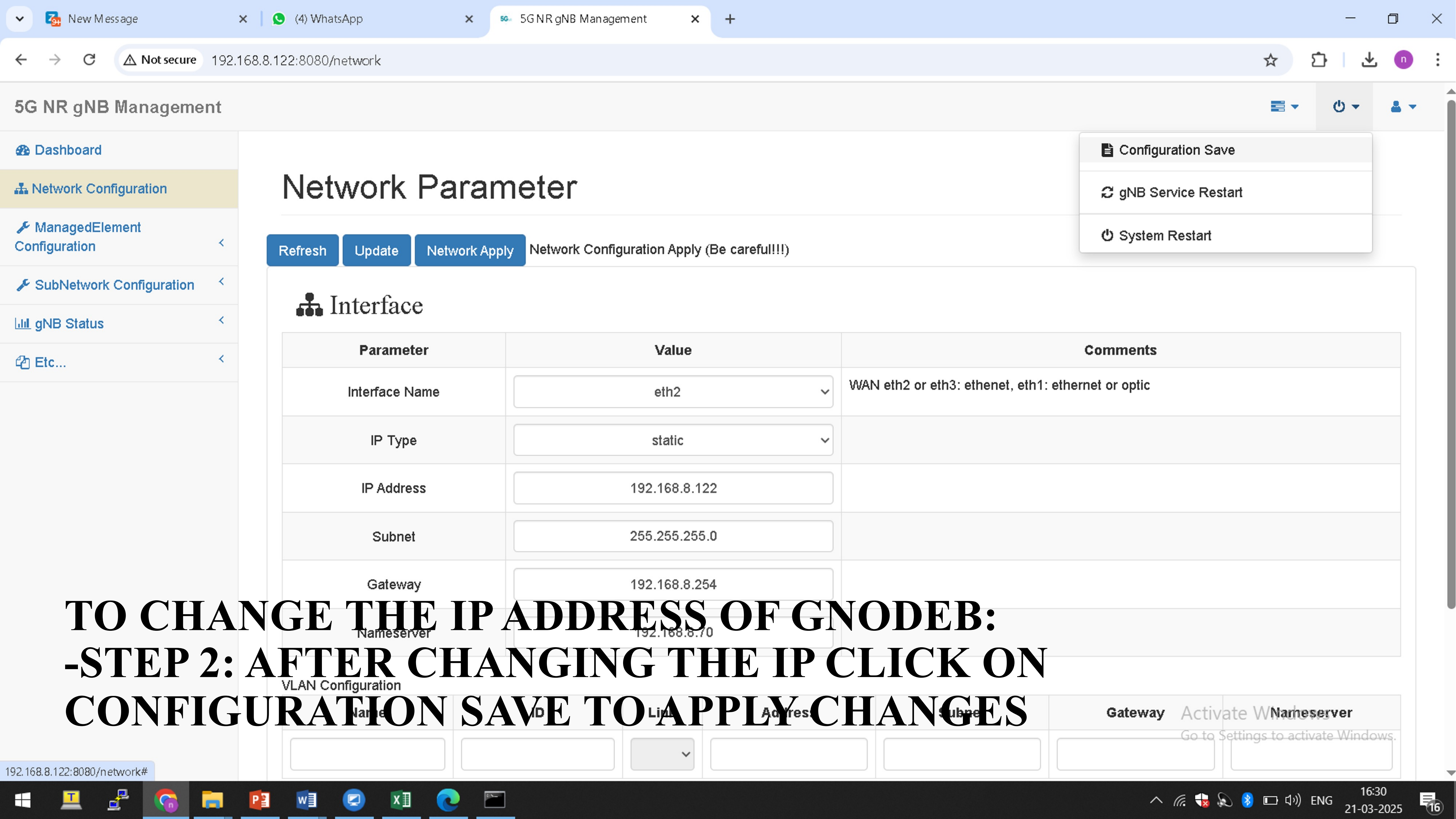


Network Parameter

Network Configuration Apply (Be careful!!!)

Interface

Parameter	Value	Comments
Interface Name	eth2	WAN eth2 or eth3: ethenet, eth1: ethernet or optic
IP Type	static	
IP Address	192.168.8.122	
Subnet	255.255.255.0	
Gateway	192.168.8.254	



5G NR gNB Management

Network Parameter

Network Configuration Apply (Be careful!!!)

Interface

Parameter	Value	Comments
Interface Name	eth2	WAN eth2 or eth3: ethenet, eth1: ethernet or optic
IP Type	static	
IP Address	192.168.8.122	
Subnet	255.255.255.0	
Gateway	192.168.8.254	
Nameserver	192.168.8.70	

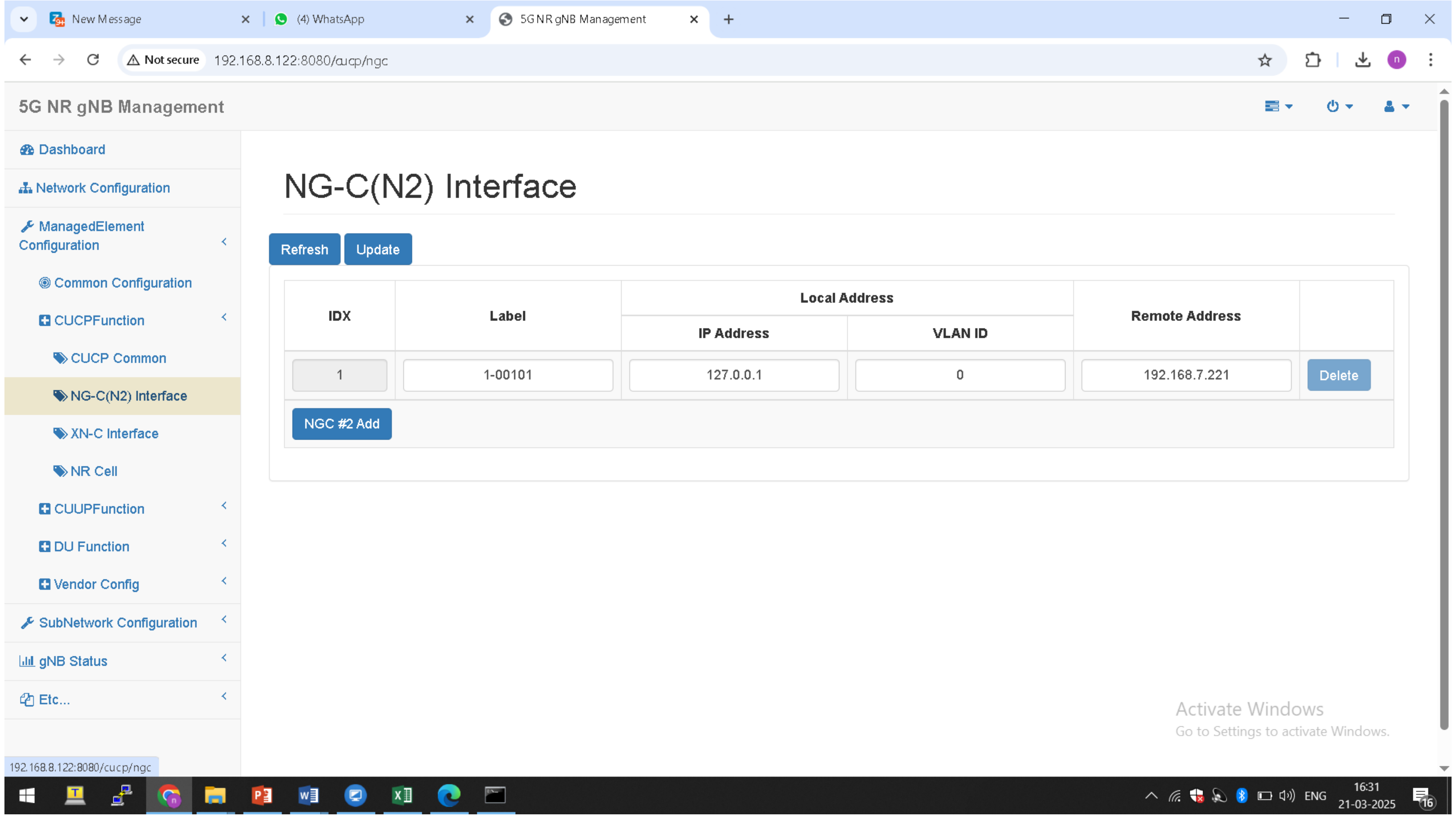
VLAN Configuration

Name	ID	Link	Address	Subnet	Gateway	Nameserver

TO CHANGE THE IP ADDRESS OF GNODEB:
-STEP 2: AFTER CHANGING THE IP CLICK ON CONFIGURATION SAVE TO APPLY CHANGES

Configuration Of NG-C(N2)

Configuration of NG-C(N2):
-Step 1: Go to Managed Element Configuration and then navigate to : CUCP Function - NG-C(N2) Interface

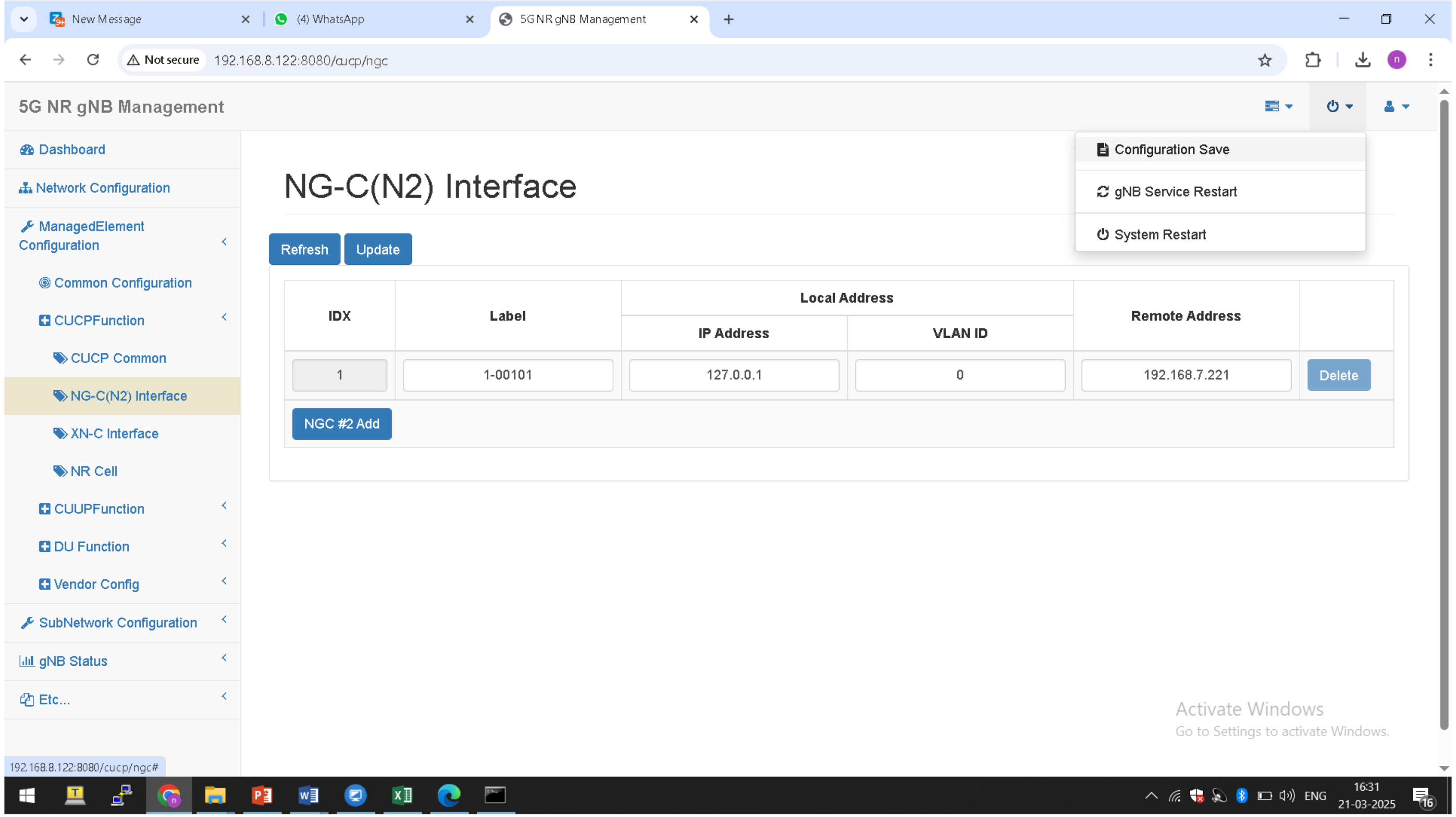


NG-C(N2) Interface

IDX	Label	Local Address		Remote Address	
		IP Address	VLAN ID		
1	1-00101	127.0.0.1	0	192.168.7.221	Delete

Configuration of NG-C(N2):

-Step 2: After making the desired changes. Click on Configuration Save drop down and then save the configurations



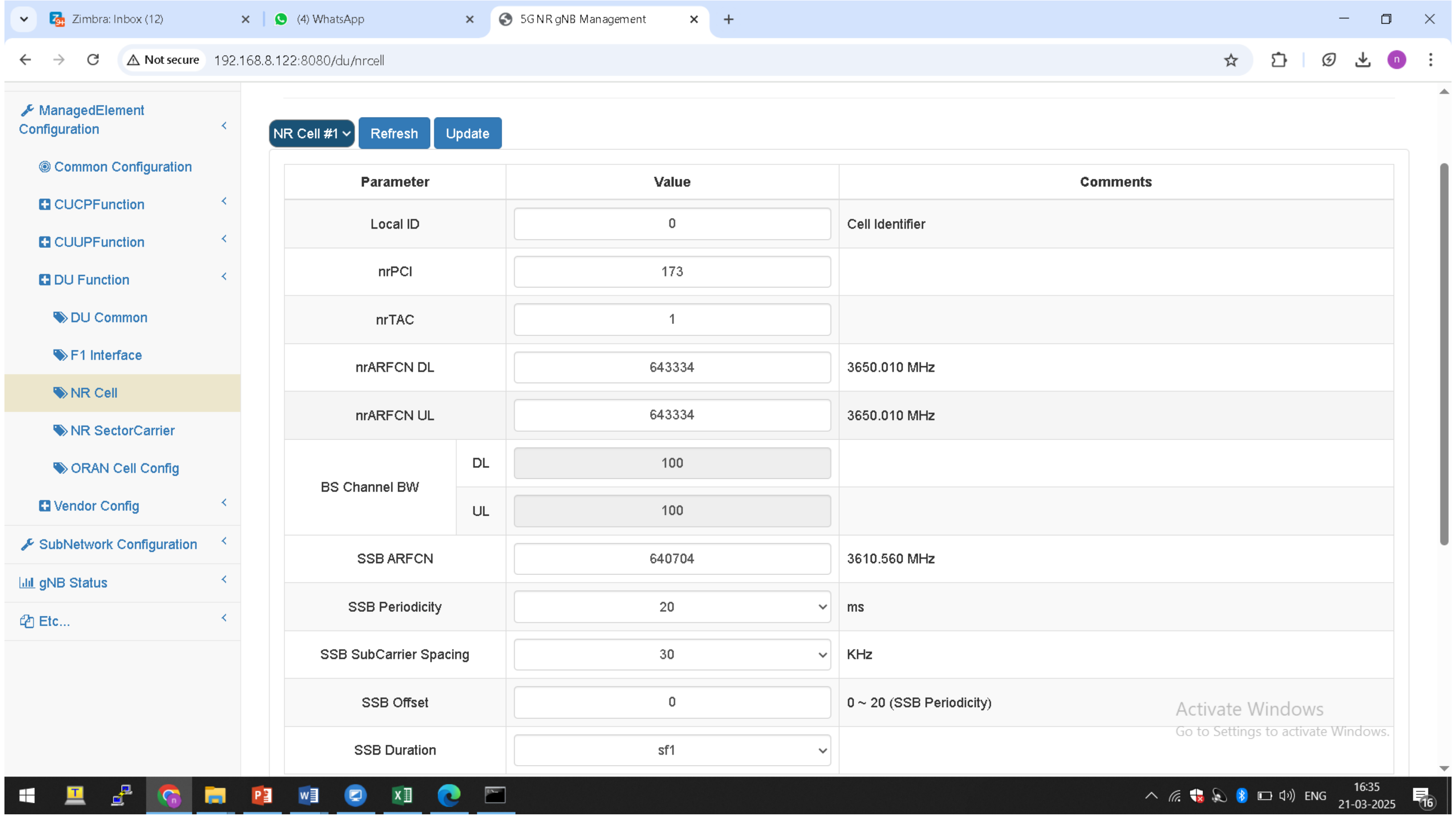
NG-C(N2) Interface

IDX	Label	Local Address		Remote Address	
		IP Address	VLAN ID		
1	1-00101	127.0.0.1	0	192.168.7.221	Delete

Configuration Of NR-Cell

Configuration of NR-Cell:

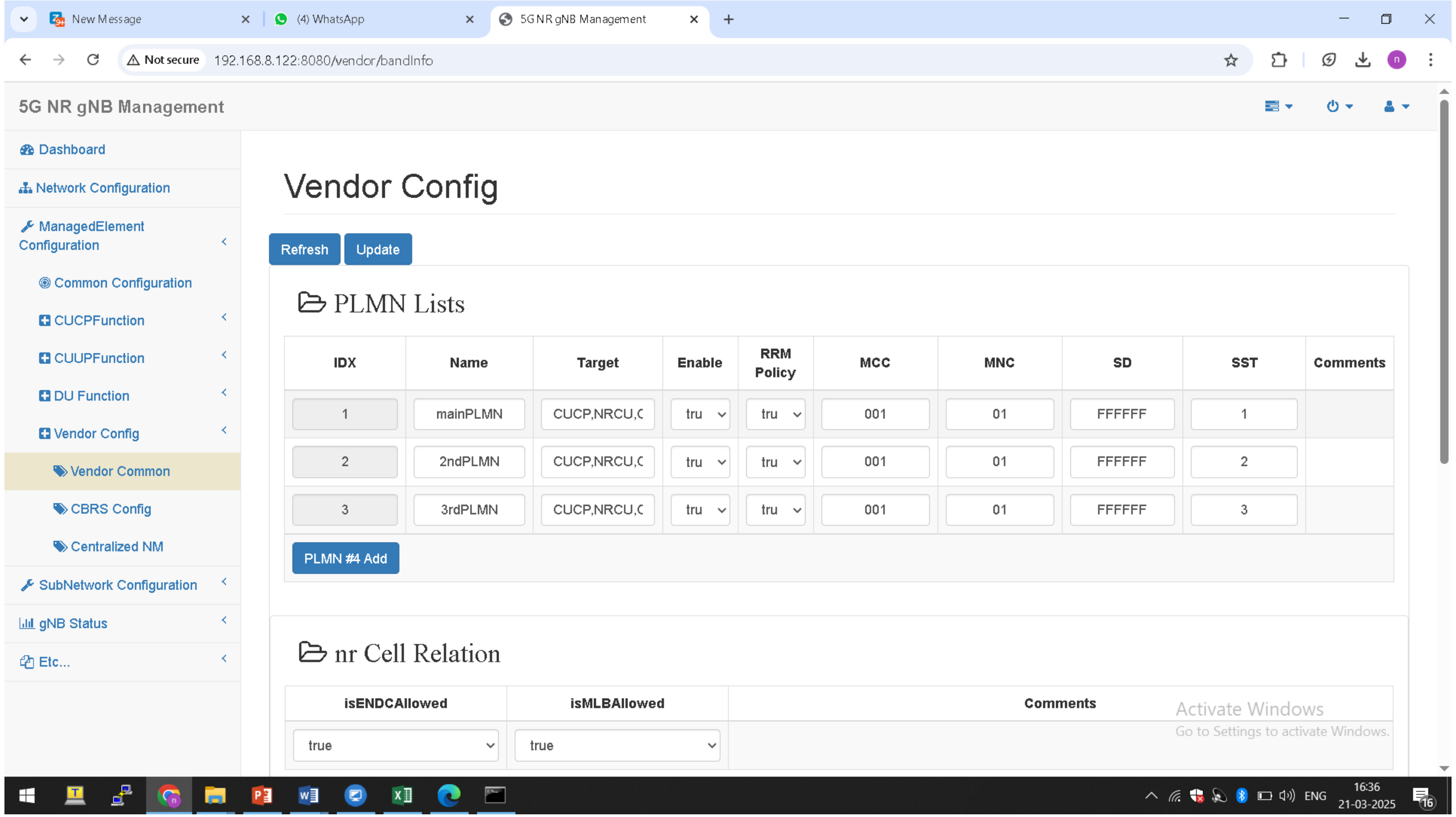
-Navigate to DU Function and then go to NR Cell and then make the desired changes in configuration



Parameter		Value	Comments
Local ID		0	Cell Identifier
nrPCI		173	
nrTAC		1	
nrARFCN DL		643334	3650.010 MHz
nrARFCN UL		643334	3650.010 MHz
BS Channel BW	DL	100	
	UL	100	
SSB ARFCN		640704	3610.560 MHz
SSB Periodicity		20	ms
SSB SubCarrier Spacing		30	KHz
SSB Offset		0	0 ~ 20 (SSB Periodicity)
SSB Duration		sf1	

Configuration
Of
PMLN & Slicing

Configuration of PMLN & nr Cell Relation:
-Navigate to Vendor Config and then go to Vendor Common



Vendor Config

PLMN Lists

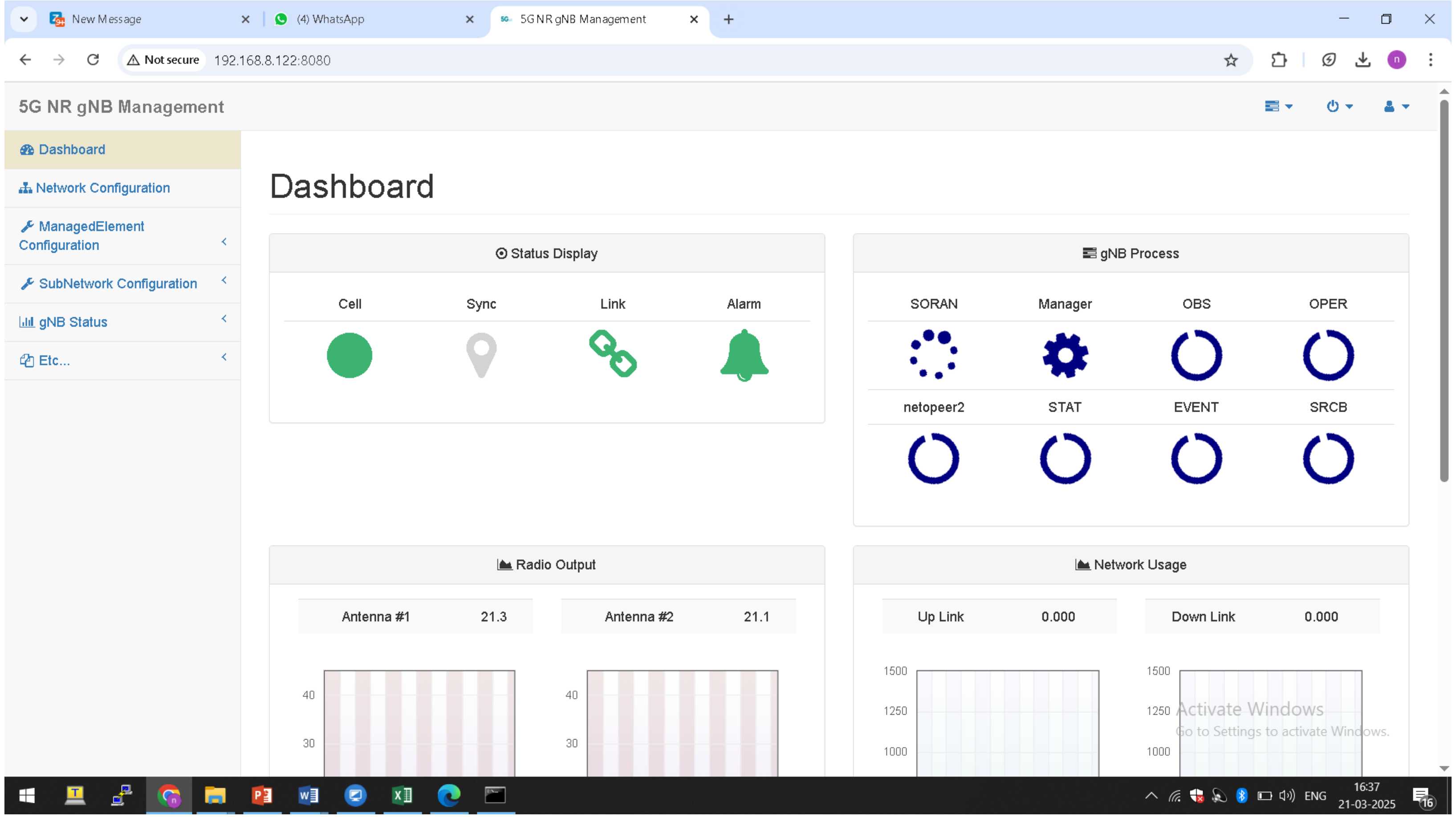
IDX	Name	Target	Enable	RRM Policy	MCC	MNC	SD	SST	Comments
1	mainPLMN	CUCP,NRCU,C	tru	tru	001	01	FFFFFF	1	
2	2ndPLMN	CUCP,NRCU,C	tru	tru	001	01	FFFFFF	2	
3	3rdPLMN	CUCP,NRCU,C	tru	tru	001	01	FFFFFF	3	

nr Cell Relation

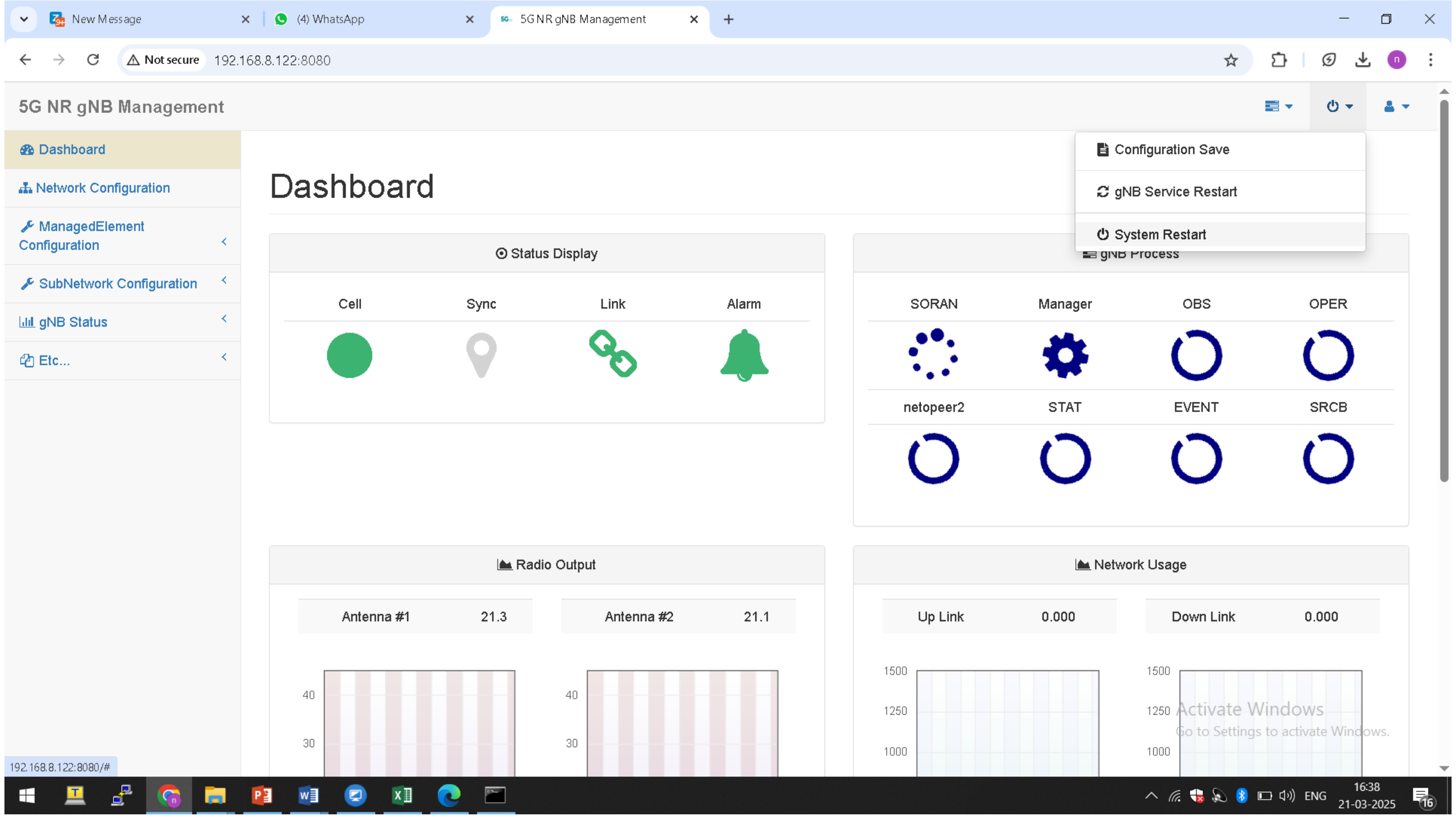
isENDCAllowed	isMLBAllowed	Comments
true	true	

Finalizing The Changes of gNodeB

Finalizing the Changes of gNodeB:
Step 1: To save the mentioned changes click on the power button on the top-right page and
A drop-down menu will appear



Finalizing the Changes of gNodeB:
Step 2: Click on System Restart and your desired changes will now take place on the network.



SETUP

1.Connect the 48V power supply to the gNB

2.Connect the Ethernet cable(CAT-7) from gNB to switch 2.5 Ghz port

3.Connect your core to the switch with a CAT-7 Ethernet and switch it on.

4.Connect the DNN to the switch in similar fashion if want to transfer data on the network.

5.Switch on the gNB and wait for it to come up.

6.ssh to the gNB from DNN using command `*ssh root@gnodeB IP*`.

7.Enter the username and password both as `*root*`.

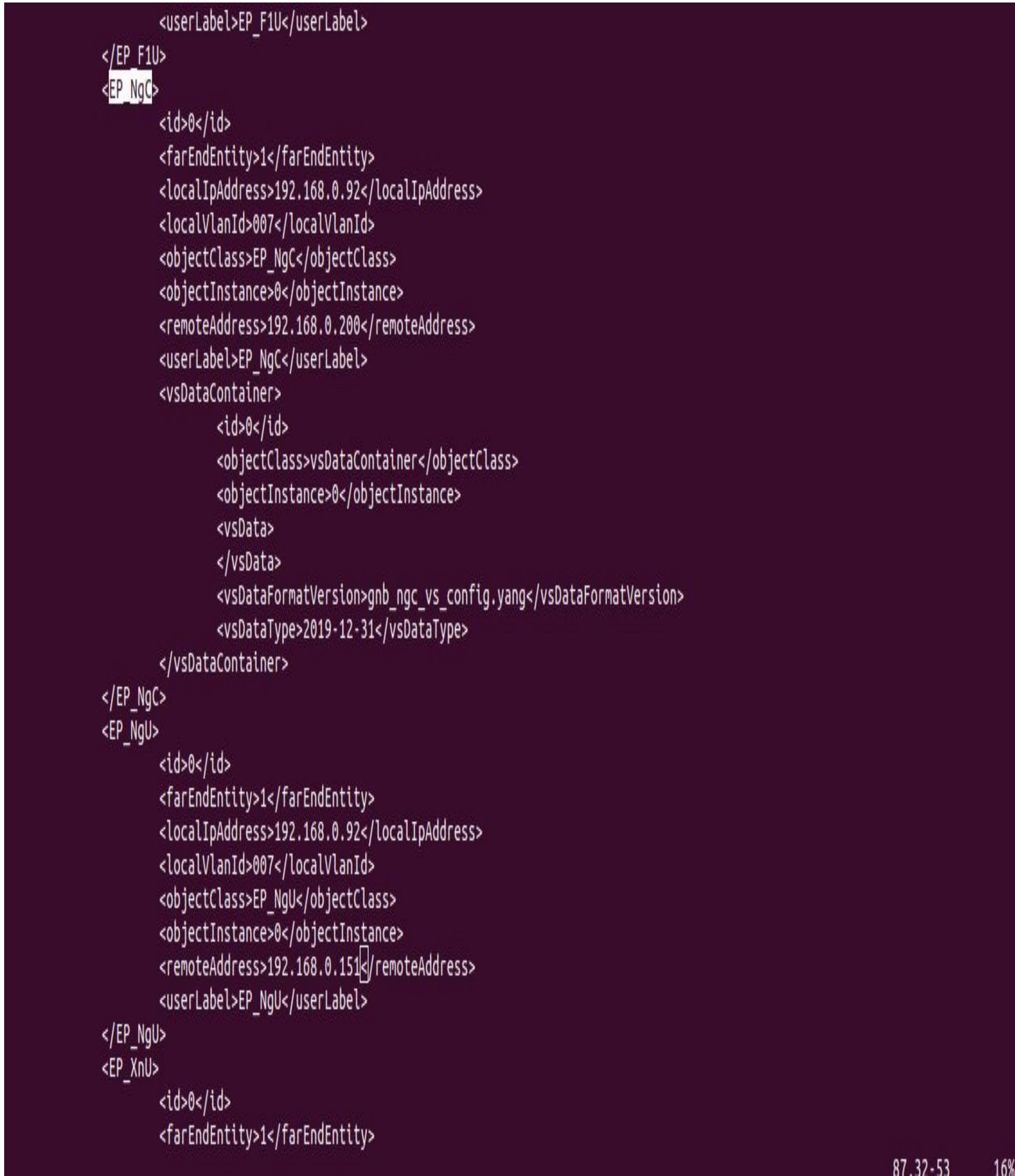
8.Enter `*vi /etc/systemd/network/eth0.network*` and change the board address relevant to your network subnet.

9.Enter vi /cu/config/me_config.xml and set the control plane and user plane ip as shown in the figure below.

10.`<EP_NgC>` is the control plane configuration and `<EP_NgU>` is the user plane configuration.

11.`*localIpAddress*` should be set as the gnb ip and the `*remoteAddress*` should be set according to the core control plane and user plane address.

12.Reboot the gNB with reboot command and wait for the service to come up.



```
                <userLabel>EP_F1U</userLabel>
        </EP_F1U>
        <EP_NgC>
                <id>0</id>
                <farEndEntity>1</farEndEntity>
                <localIpAddress>192.168.0.92</localIpAddress>
                <localVlanId>007</localVlanId>
                <objectClass>EP_NgC</objectClass>
                <objectInstance>0</objectInstance>
                <remoteAddress>192.168.0.200</remoteAddress>
                <userLabel>EP_NgC</userLabel>
                <vsDataContainer>
                        <id>0</id>
                        <objectClass>vsDataContainer</objectClass>
                        <objectInstance>0</objectInstance>
                        <vsData>
                        </vsData>
                        <vsDataFormatVersion>gnb_ngc_vs_config.yang</vsDataFormatVersion>
                        <vsDataType>2019-12-31</vsDataType>
                </vsDataContainer>
        </EP_NgC>
        <EP_NgU>
                <id>0</id>
                <farEndEntity>1</farEndEntity>
                <localIpAddress>192.168.0.92</localIpAddress>
                <localVlanId>007</localVlanId>
                <objectClass>EP_NgU</objectClass>
                <objectInstance>0</objectInstance>
                <remoteAddress>192.168.0.151</remoteAddress>
                <userLabel>EP_NgU</userLabel>
        </EP_NgU>
        <EP_XnU>
                <id>0</id>
                <farEndEntity>1</farEndEntity>
                                                                        87,32-53      16%
```

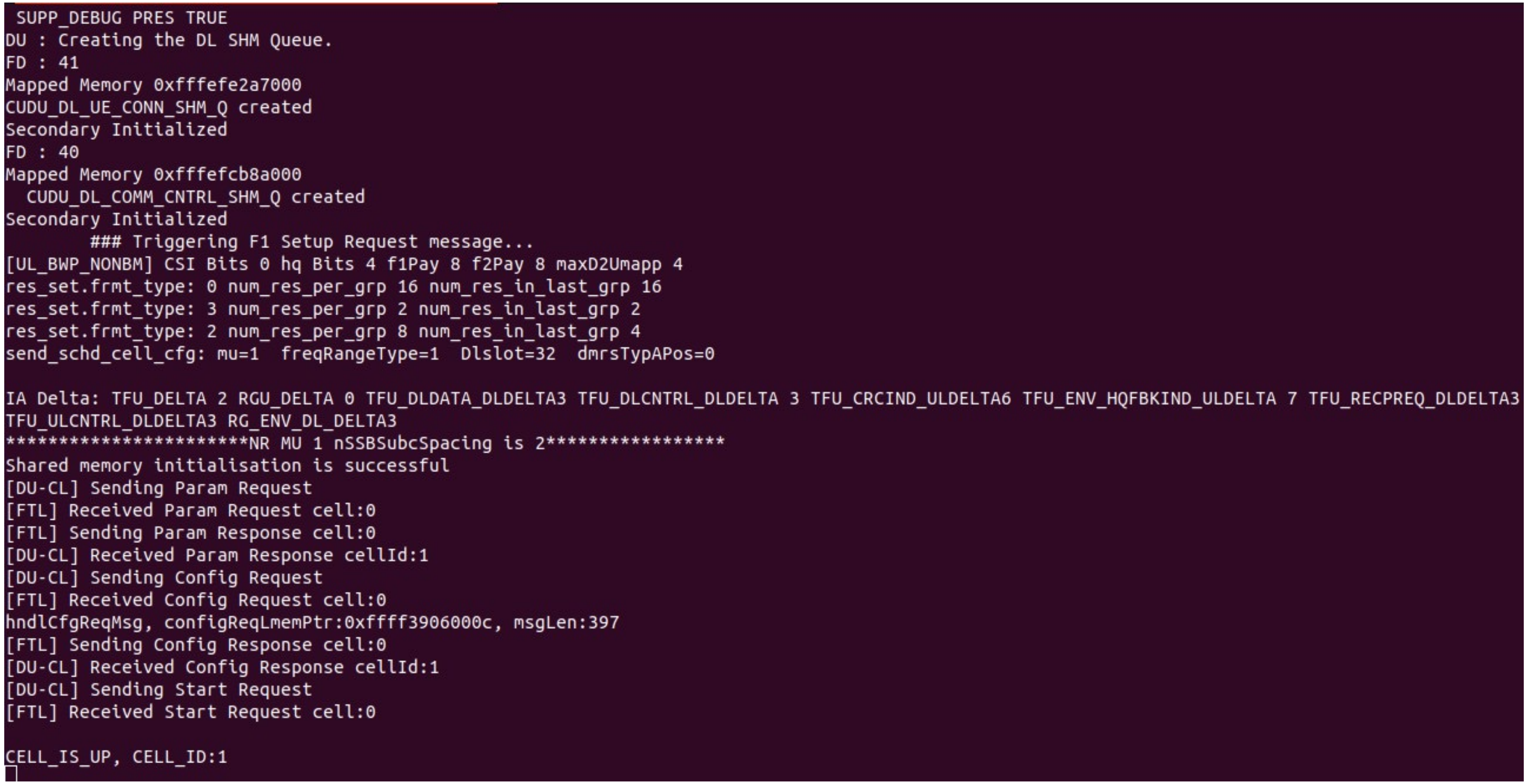
- **Integrated gNodeB Software components**

- It is based on commercial SOC built on ARM and RISC architectures for L2/L2/L1 modules. Following are the major components
  - Platform – U-BOOT, Linux and RFS
  - OAM – Configuration data such YAML, xml files
  - O-CU L2/L3 – software modules to perform NGAP, RRC, PDCP, etc. Communicate over F1AP with O-DU
  - O-DU L1/L2 – software modules to perform RLC, MAC, and PHY
  - RF Mager – Configuration, management of RF Transceiver module and RF front end module to manage the RF power, etc.,
-

CHECKING CELL UP

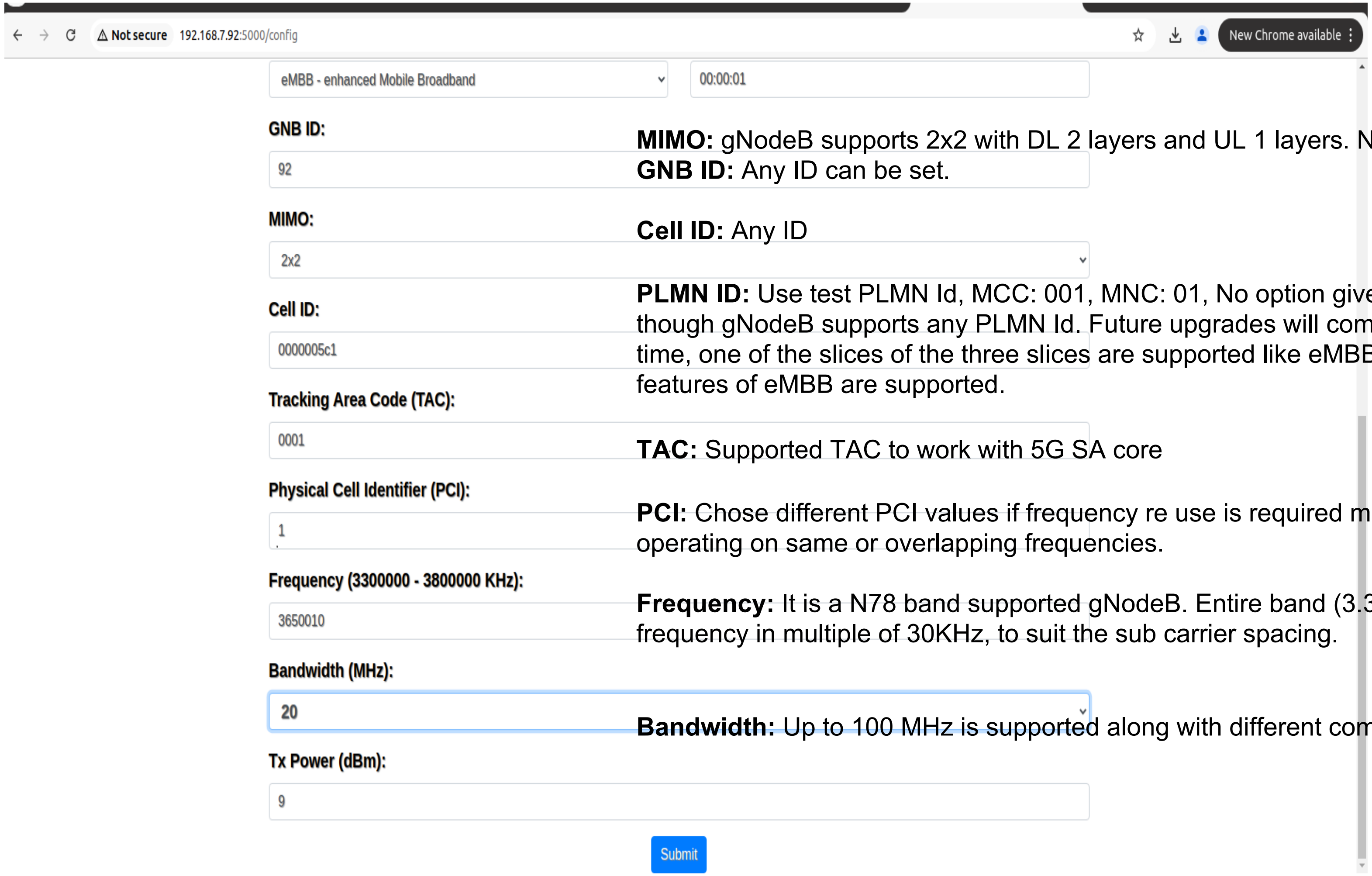
1. Check raptor service status with `*systemctl status raptor2*` command.
2. Check whether the cell is up or not with command `*tail -f /logdump/du_log.txt*`.

Refer to the pic shown below to confirm if Cell is UP.



```
 SUPP_DEBUG PRES TRUE
DU : Creating the DL SHM Queue.
FD : 41
Mapped Memory 0xfffefe2a7000
CUDU_DL_UE_CONN_SHM_Q created
Secondary Initialized
FD : 40
Mapped Memory 0xfffefcb8a000
  CUDU_DL_COMM_CNTRL_SHM_Q created
Secondary Initialized
        ### Triggering F1 Setup Request message...
[UL_BWP_NONBM] CSI Bits 0 hq Bits 4 f1Pay 8 f2Pay 8 maxD2Umapp 4
res_set.frmt_type: 0 num_res_per_grp 16 num_res_in_last_grp 16
res_set.frmt_type: 3 num_res_per_grp 2 num_res_in_last_grp 2
res_set.frmt_type: 2 num_res_per_grp 8 num_res_in_last_grp 4
send_schd_cell_cfg: mu=1  freqRangeType=1  Dlslot=32  dmrsTypAPos=0

IA Delta: TFU_DELTA 2 RGU_DELTA 0 TFU_DLDATA_DLDELTA3 TFU_DLCNTRL_DLDELTA 3 TFU_CRCIND_ULDELTA6 TFU_ENV_HQFBKIND_ULDELTA 7 TFU_RECPREQ_DLDELTA3
TFU_ULCNTRL_DLDELTA3 RG_ENV_DL_DELTA3
**********************NR MU 1 nSSBSubcSpacing is 2****************
Shared memory initialisation is successful
[DU-CL] Sending Param Request
[FTL] Received Param Request cell:0
[FTL] Sending Param Response cell:0
[DU-CL] Received Param Response cellId:1
[DU-CL] Sending Config Request
[FTL] Received Config Request cell:0
hndlCfgReqMsg, configReqLmemPtr:0xffff3906000c, msgLen:397
[FTL] Sending Config Response cell:0
[DU-CL] Received Config Response cellId:1
[DU-CL] Sending Start Request
[FTL] Received Start Request cell:0

CELL_IS_UP, CELL_ID:1
```

Local EMS -http://gNodeB ip:5000/
In Chrome browser- gnodeB IP:5000 for access the 5G NodeB EMS



⚠ Not secure 192.168.7.92:5000/config

eMBB - enhanced Mobile Broadband

00:00:01

GNB ID:

92

MIMO:

2x2

Cell ID:

0000005c1

Tracking Area Code (TAC):

0001

Physical Cell Identifier (PCI):

1

Frequency (3300000 - 3800000 KHz):

3650010

Bandwidth (MHz):

20

Tx Power (dBm):

9

MIMO: gNodeB supports 2x2 with DL 2 layers and UL 1 layers. No other option possible currently.
GNB ID: Any ID can be set.

Cell ID: Any ID

PLMN ID: Use test PLMN Id, MCC: 001, MNC: 01, No option given to modify the same with EMS. Even though gNodeB supports any PLMN Id. Future upgrades will come with this modifications. **Slice:** At a time, one of the slices of the three slices are supported like eMBB, URLCC, mMTC. Note that only real features of eMBB are supported.

TAC: Supported TAC to work with 5G SA core

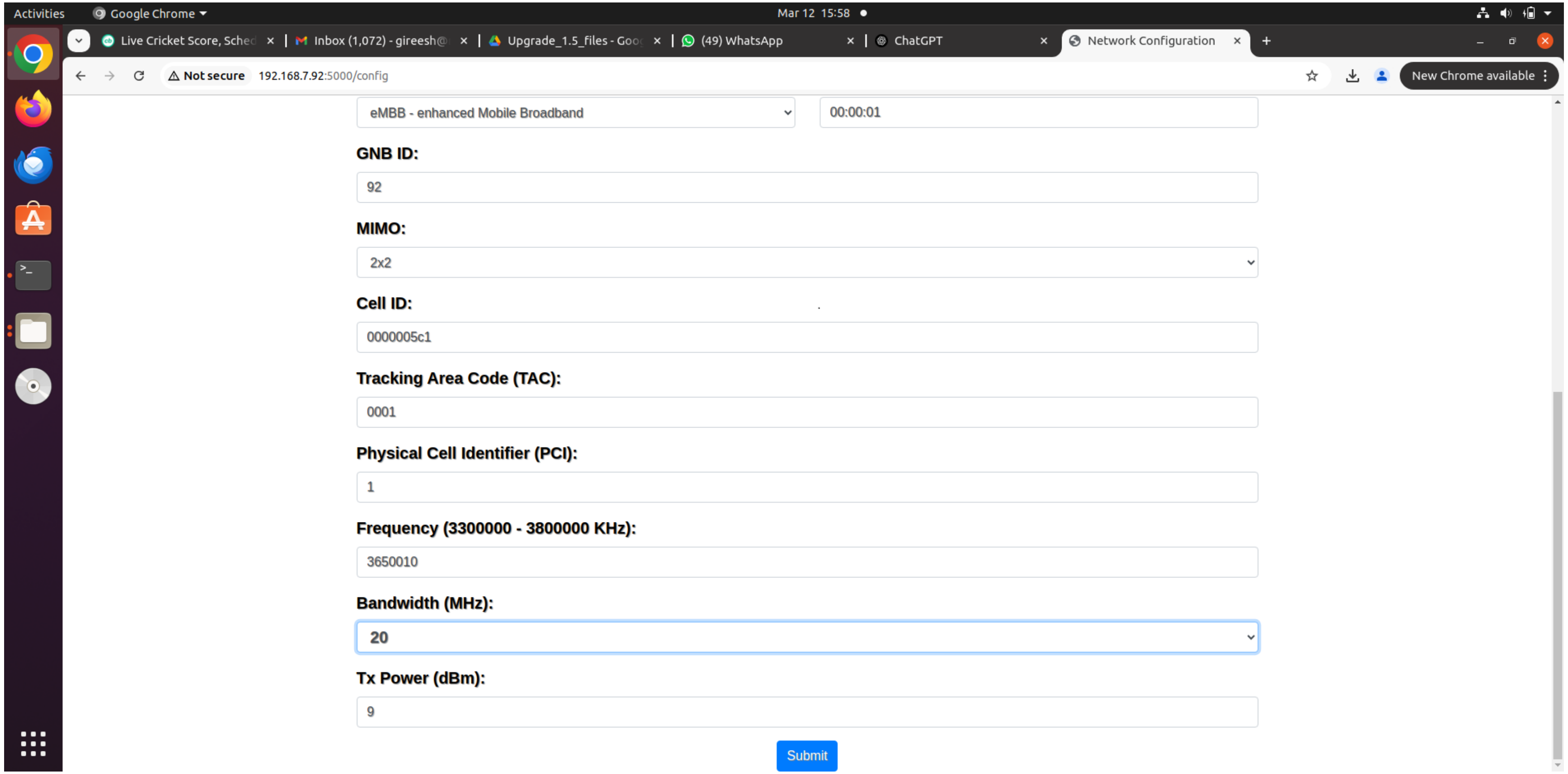
PCI: Chose different PCI values if frequency re use is required means if adjacent gNodeB are operating on same or overlapping frequencies.

Frequency: It is a N78 band supported gNodeB. Entire band (3.3-3.8 GHz) is operational. Chose the frequency in multiple of 30KHz, to suit the sub carrier spacing.

Bandwidth: Up to 100 MHz is supported along with different combinations provide below.

Slice Configuration -SD and SST

Login EMS ->Config ->Change SST & SD Value as per Required configuration



eMBB - enhanced Mobile Broadband | 00:00:01

GNB ID: 92

MIMO: 2x2

Cell ID: 0000005c1

Tracking Area Code (TAC): 0001

Physical Cell Identifier (PCI): 1

Frequency (3300000 - 3800000 KHz): 3650010

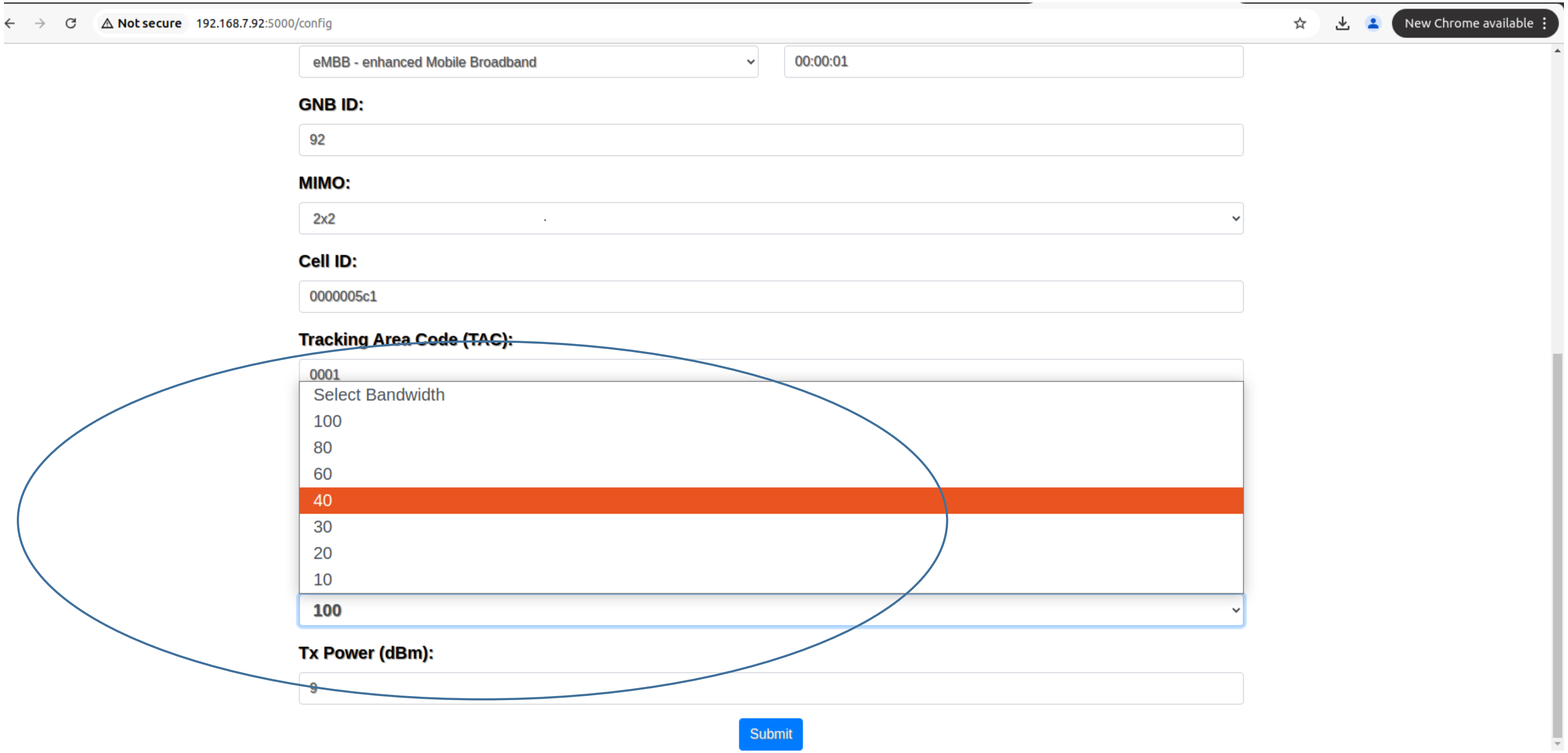
Bandwidth (MHz): 20

Tx Power (dBm): 9

Submit

Different Bandwidth Configuration -100 ,80,60,40 etc

Login EMS ->Config ->Change Bandwidth as per Required configuration
Refer below picture



eMBB - enhanced Mobile Broadband
00:00:01

GNB ID:
92

MIMO:
2x2

Cell ID:
0000005c1

Tracking Area Code (TAC):
0001

Select Bandwidth
100
80
60
40
30
20
10

100

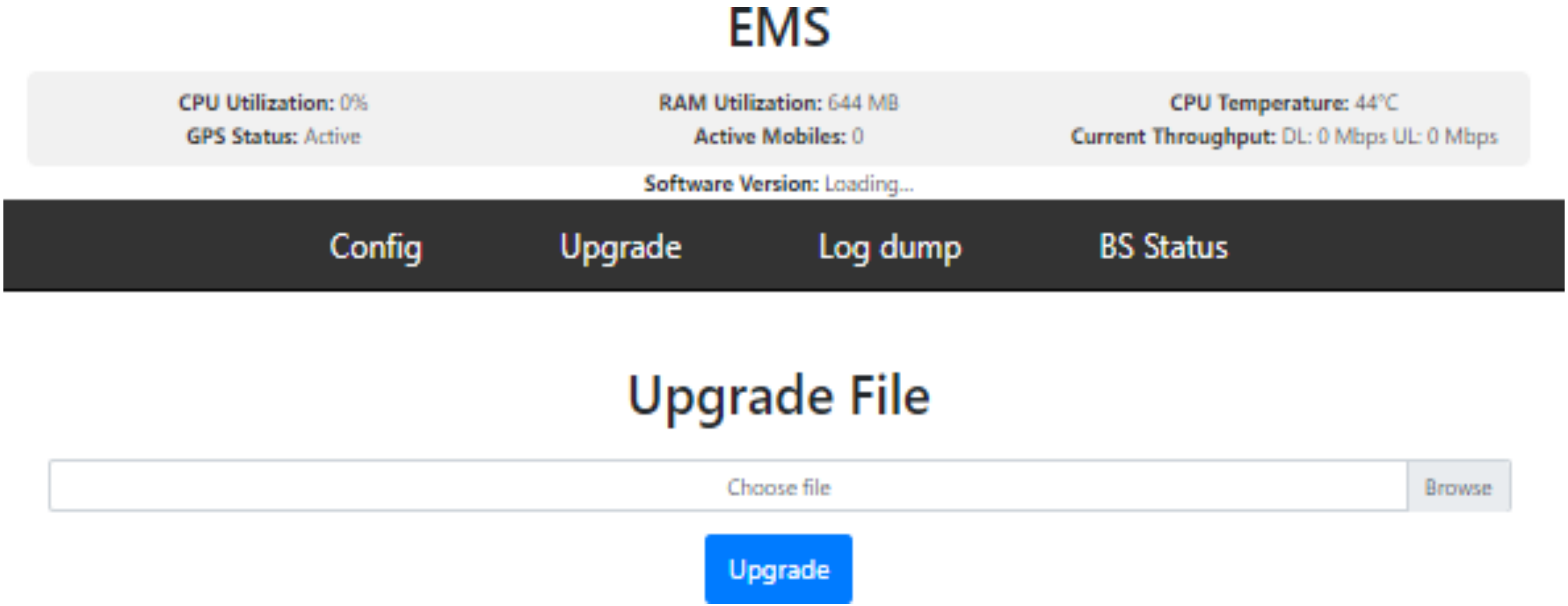
Tx Power (dBm):
9

Submit

Management

Upgrade –Software upgrade as per new release version

gNodeB is upgradable for Platform, and application loads. Respective scrpits, and loads are bundled for seam less upgrade, where user can upgrade or down grade supplied loads.

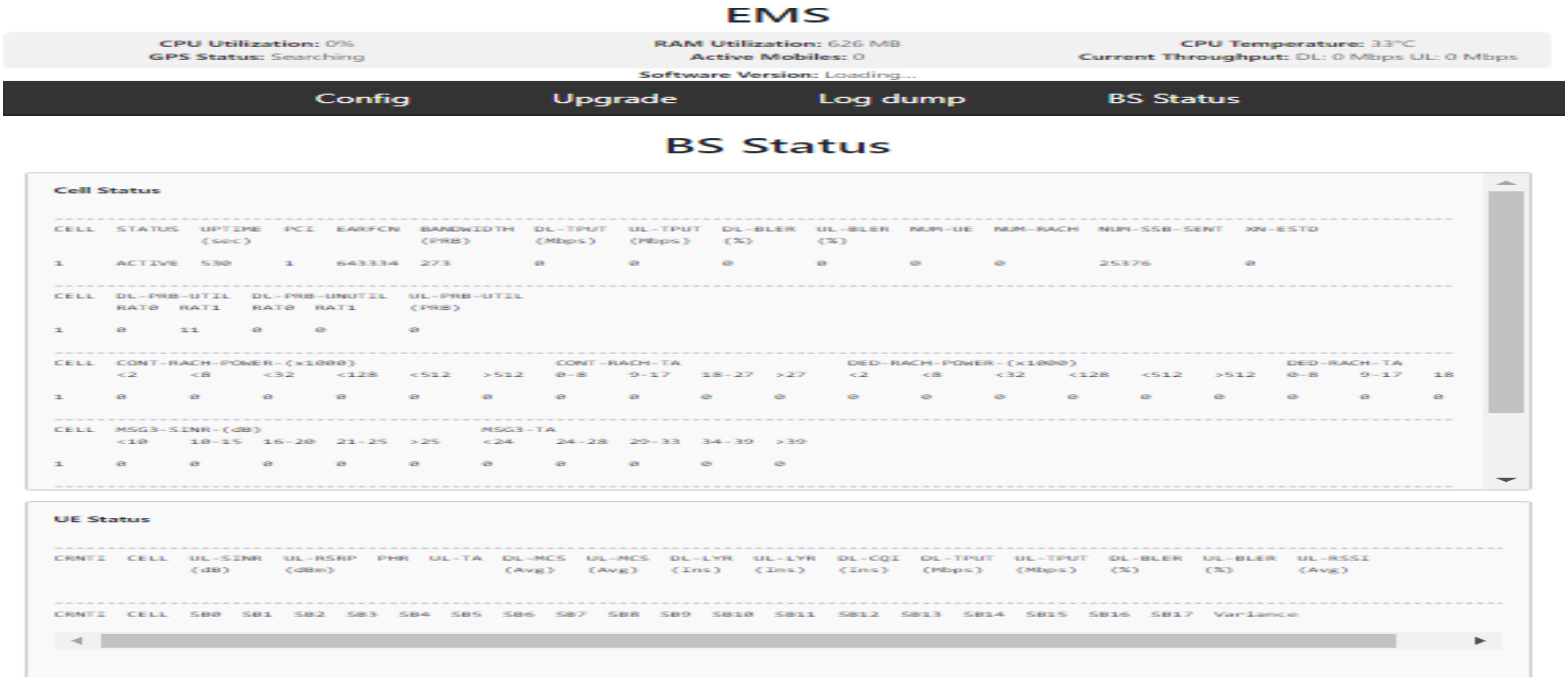


CPU Utilization: 0%
GPS Status: Active
RAM Utilization: 644 MB
Active Mobiles: 0
CPU Temperature: 44°C
Current Throughput: DL: 0 Mbps UL: 0 Mbps
Software Version: Loading...

Statistics

BS status –Cell Status & UE Status

will provide both top level cell and ue specific statistics. In future, more counters will be provided which are getting updated in the gNodeB.



EMS

CPU Utilization: 0% RAM Utilization: 626 MB CPU Temperature: 33°C
GPS Status: Searching Active Mobiles: 0 Current Throughput: DL: 0 Mbps UL: 0 Mbps
Software Version: Loading...

BS Status

Cell Status

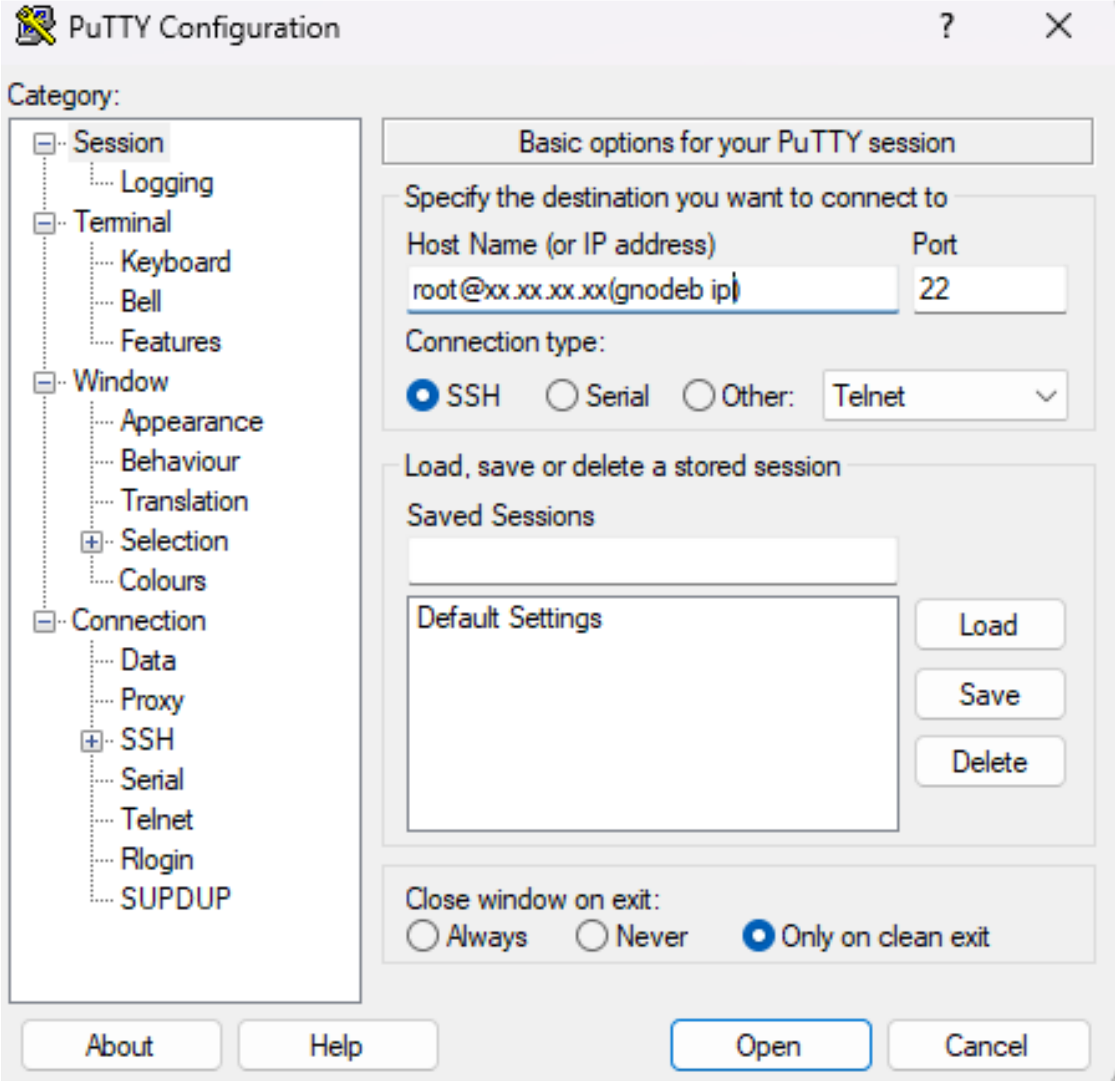
```
----------------------------------------------------------------------------------------------------------------------------------------------------
CELL   STATUS   UPTIME   PCI   EARFCN   BANDWIDTH   DL-TPUT   UL-TPUT   DL-BLER   UL-BLER   NUM-UE   NUM-RACH   NUM-SSB-SENT   XN-ESTD
                (sec)                   (PRB)       (Mbps)    (Mbps)    (%)       (%)

1      ACTIVE   530      1     643334   273         0         0         0         0         0        0          25376          0
----------------------------------------------------------------------------------------------------------------------------------------------------
CELL   DL-PRB-UTIL    DL-PRB-UNUTIL   UL-PRB-UTIL
       RAT0   RAT1    RAT0   RAT1     (PRB)

1      0      11      0      0        0
----------------------------------------------------------------------------------------------------------------------------------------------------
CELL   CONT-RACH-POWER-(x1000)                     CONT-RACH-TA                 DED-RACH-POWER-(x1000)                      DED-RACH-TA
       <2     <8     <32    <128   <512   >512   0-8    9-17   18-27   >27     <2     <8     <32    <128   <512   >512    0-8    9-17   18

1      0      0      0      0      0      0      0      0      0       0       0      0      0      0      0      0       0      0      0
----------------------------------------------------------------------------------------------------------------------------------------------------
CELL   MSG3-SINR-(dB)                      MSG3-TA
       <10    10-15   16-20   21-25   >25  <24    24-28   29-33   34-39   >39

1      0      0       0       0       0    0      0       0       0       0
----------------------------------------------------------------------------------------------------------------------------------------------------
```

UE Status

```
--------------------------------------------------------------------------------------------------------------------------------------------------------------
CRNTI   CELL   UL-SINR   UL-RSRP   PHR   UL-TA   DL-MCS   UL-MCS   DL-LYR   UL-LYR   DL-CQI   DL-TPUT   UL-TPUT   DL-BLER   UL-BLER   UL-RSSI
               (dB)      (dBm)                  (Avg)    (Avg)    (Ins)    (Ins)    (Ins)    (Mbps)    (Mbps)    (%)       (%)       (Avg)

--------------------------------------------------------------------------------------------------------------------------------------------------------------
CRNTI   CELL   SB0   SB1   SB2   SB3   SB4   SB5   SB6   SB7   SB8   SB9   SB10   SB11   SB12   SB13   SB14   SB15   SB16   SB17   Variance
```

Log Collection

- Login gNodeB through Putty ssh
- User name –root
- Password -*****
- After login through SSH
- Run below comment
- tcpdump -i any -w /tmp/filename .pcap
- Once log collected
- Terminate the log collection by press (ctrl+c)
- And can be downloaded from temp folder by using the WINSCP application



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): root@xx.xx.xx.xx(gnodeb ip)

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

5G LAB

Lunch Break

5G LAB

MEC
(Multi-access Edge Computing)

What is MEC

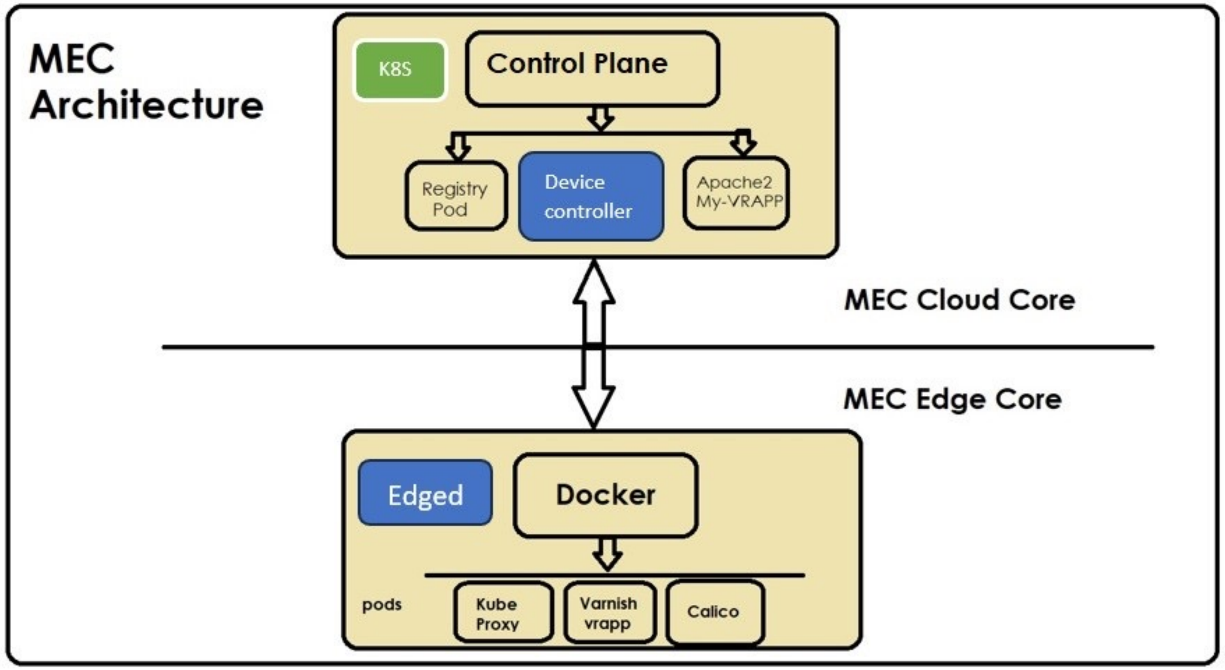
- Multi-access Edge Computing (MEC) refers to a network architecture that brings computational resources closer to the end user, specifically to the edge of the mobile network, such as base stations or even local routers. This minimizes latency by processing data near its source.

Why MEC Matters

- **Latency reduction**: MEC reduces delays by processing data at the edge, close to where it’s needed, which is essential for applications like autonomous vehicles or gaming.
- **Bandwidth optimization**: By offloading data processing to the edge, MEC reduces the traffic sent to the cloud, making more bandwidth available for other uses.

Continue …

- **Enhanced user experience**: With faster data processing, users experience quicker responses, which is critical for real-time applications.
- **Supporting IoT, 5G, and AI at the edge**: MEC facilitates processing for the massive amounts of data generated by IoT devices, enabling the smooth functioning of 5G networks and artificial intelligence (AI) applications.



MEC Architecture

MEC Cloud Core components

CONTROL PLANE: AN EXTENDED KUBERNETES CONTROLLER WHICH MANAGES EDGE NODES AND PODS METADATA SO THAT THE DATA CAN BE TARGETED TO A SPECIFIC EDGE NODE.

DEVICE CONTROLLER: AN EXTENDED KUBERNETES CONTROLLER WHICH MANAGES DEVICES SO THAT THE DEVICE METADATA/STATUS DATA CAN BE SYNCED BETWEEN EDGE AND CLOUD.

Continue…

- **Registry Pod:** A web socket client responsible for interacting with Cloud Service for edge computing (like Edge Controller as in the Kube Edge Architecture). This includes syncing cloud-side resource updates to the edge and reporting edge-side host and device status changes to the cloud.
- **Apche2-My-VRapp :** A cloud core side pod that is running and contains the VR application that will push to edge core.

MEC Cloud Edge components

- **Edged:** an agent that runs on Cloud edge core and manages containerized applications.
- **Kube-proxy :** Network proxy that runs on each node within the cluster, responsible for managing network rules and routing traffic between services and their underlying pods.

Continue…

- **Calico :** Containerized process running on a node within a cluster that acts as the primary agent for Calico, a network plugin used to manage pod-to-pod communication by assigning IP addresses, routing traffic, and enforcing network security policies across the cluster.
- **Varnish-VR-app**: Edge side pod that contains the VR application using caching application named Varnish, where the content has been pushed by MEC Cloud Core pod.

Key MEC Technologies

- **Containers (e.g., Docker)**: Containers allow applications to be packaged with all their dependencies and deployed on any system, making it easier to manage and scale MEC applications.

- **KubeEdge** is an open source system extending native containerized application orchestration and device management to hosts at the Edge. It is built upon Kubernetes and provides core infrastructure support for networking, application deployment and metadata synchronization between cloud and edge.

Components of MEC

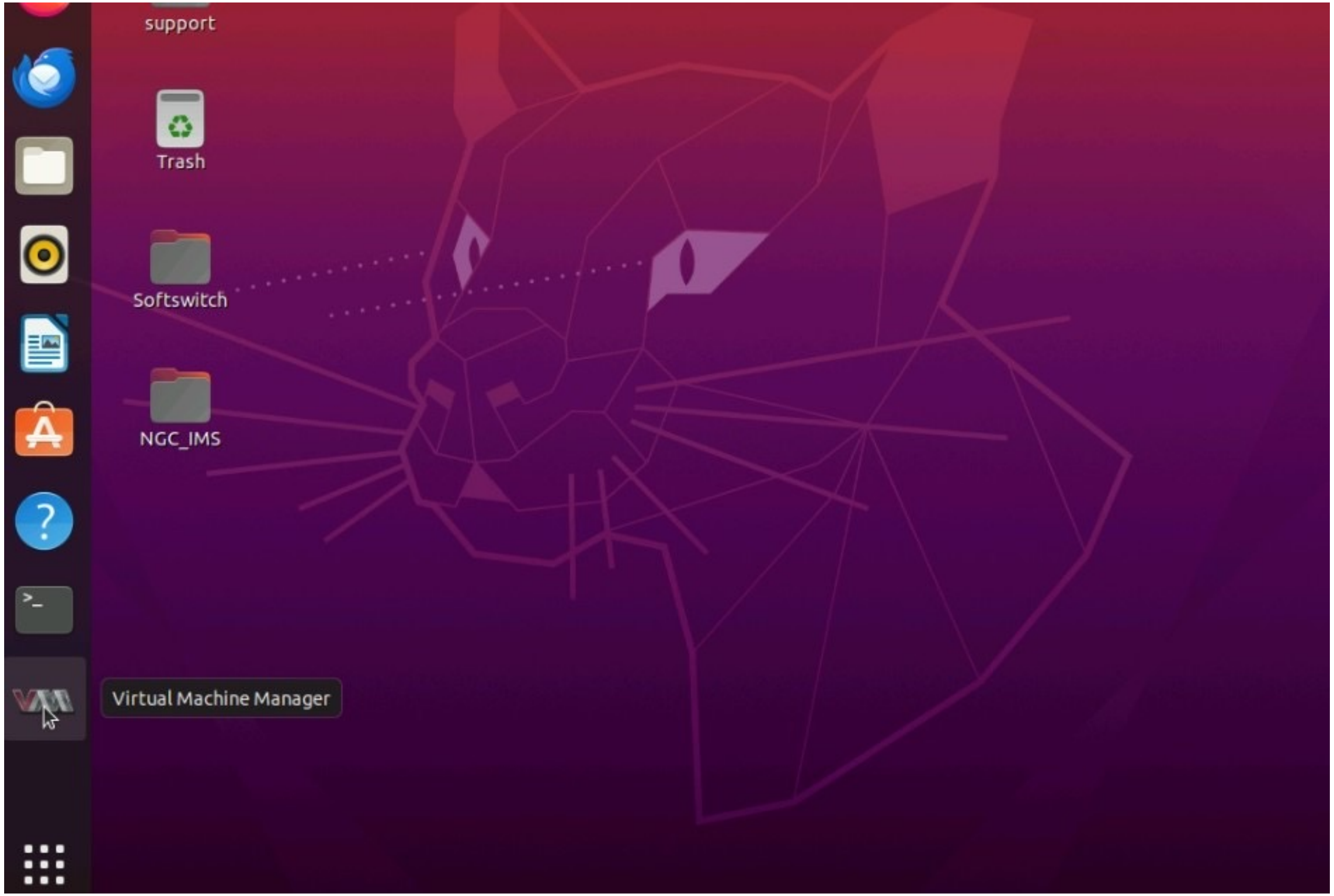
- MEC Cloud Core: These servers provide the computational resources at the edge of the network, enabling local data processing, storage, and analytics.
- MEC Edge Core: These are distributed computing units that process data locally instead of sending it to the cloud. They are deployed close to the users or devices to reduce latency.

- **Communication Networks (5G core, RAN)**: These networks facilitate data transfer between the edge nodes, servers, and end devices.
- **End Devices (smartphones, IoT devices, VR Set)**: These devices generate data and often require fast processing, which MEC helps to handle by moving the computational tasks closer to them.

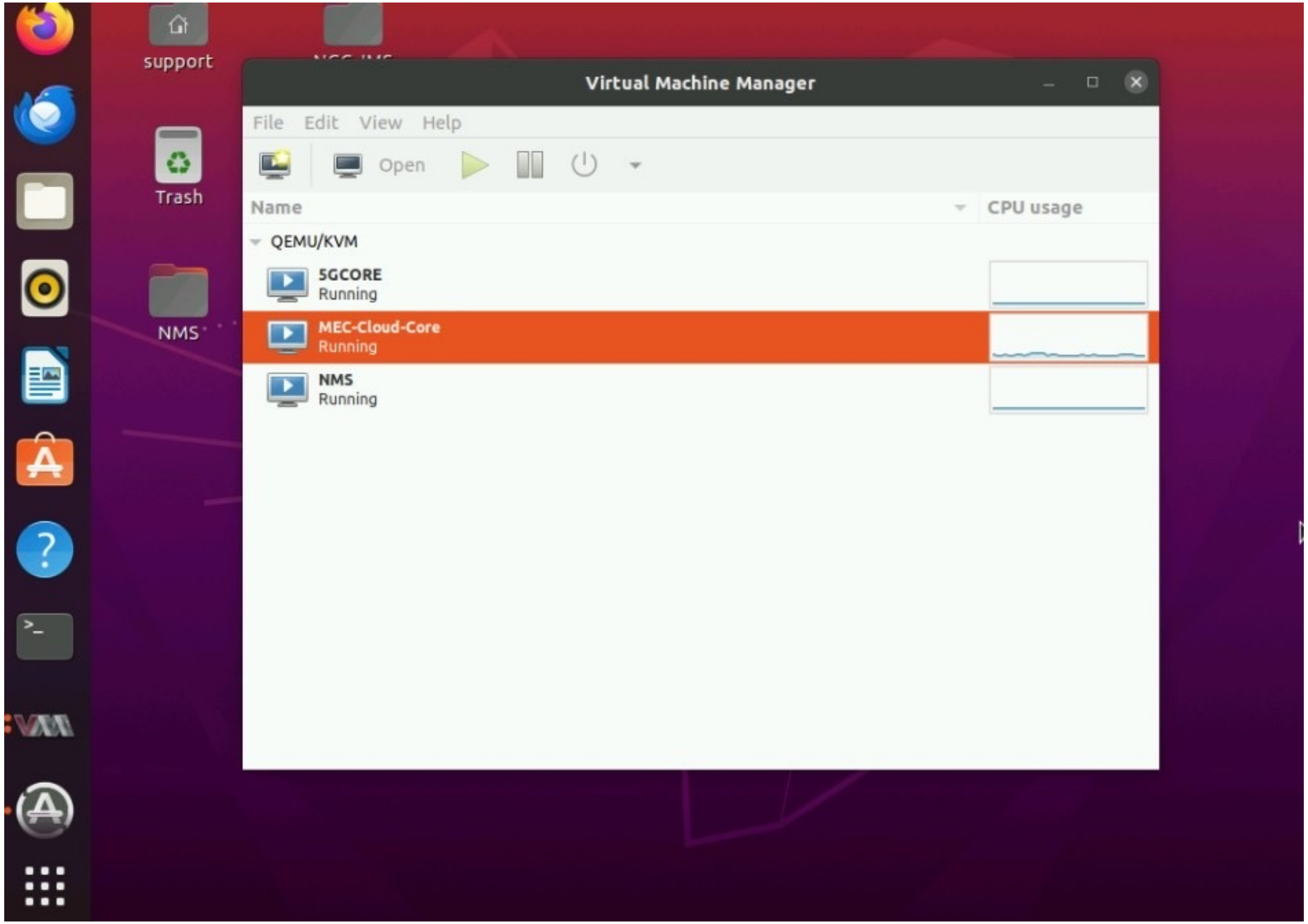
MEC with Virtualization

- **KVM** (Kernel-based Virtual Machine) is a virtualization technology built into the Linux kernel. It allows you to run virtual machines (VMs) on a Linux system, turning it into a hypervisor. With KVM, you can run multiple isolated environments on a single physical machine, each with its own operating system and applications, essentially enabling hardware virtualization.

- **Virtual Machine Management**: Both MEC Cloud Core and MEC Edge Core uses KVM virtualization platform itself is just a core part of the virtualization process. Guest machines that are running on both MEC servers are like 5G Cloud Core, NMS and MEC Cloud Core where on other server’s guest machines are running MEC edge Core.



KVM manager



QEMU/KVM

Name	CPU usage
5GCORE Running	
MEC-Cloud-Core Running	
NMS Running	

Guest Machines running on KVM

Guest Operating Systems:

- KVM supports a wide range of guest operating systems, including various versions of Linux, Windows, and other UNIX-like operating systems.

Application installation procedure

All applications files have standard design in yaml format. Upload the installation files from the system to MEC Cloud Core server under /home/support using WinSCP application

Now go to /home/support/

There will be two files for MEC installation:

1. mec-core-server_1.0.0_amd64.deb

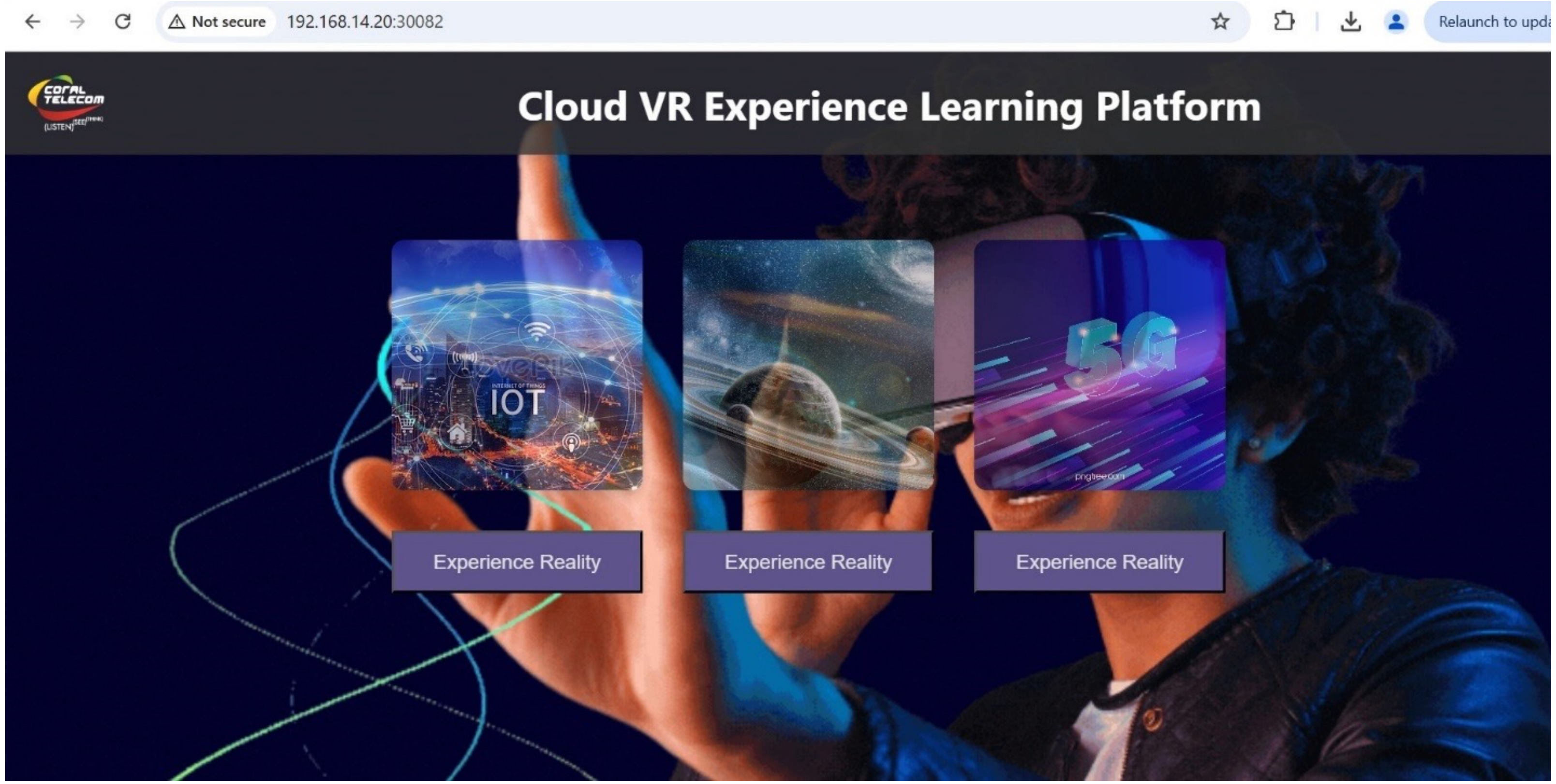
2.mec-deployments.tar

MEC Use Cases

Virtual Reality (VR) Application:

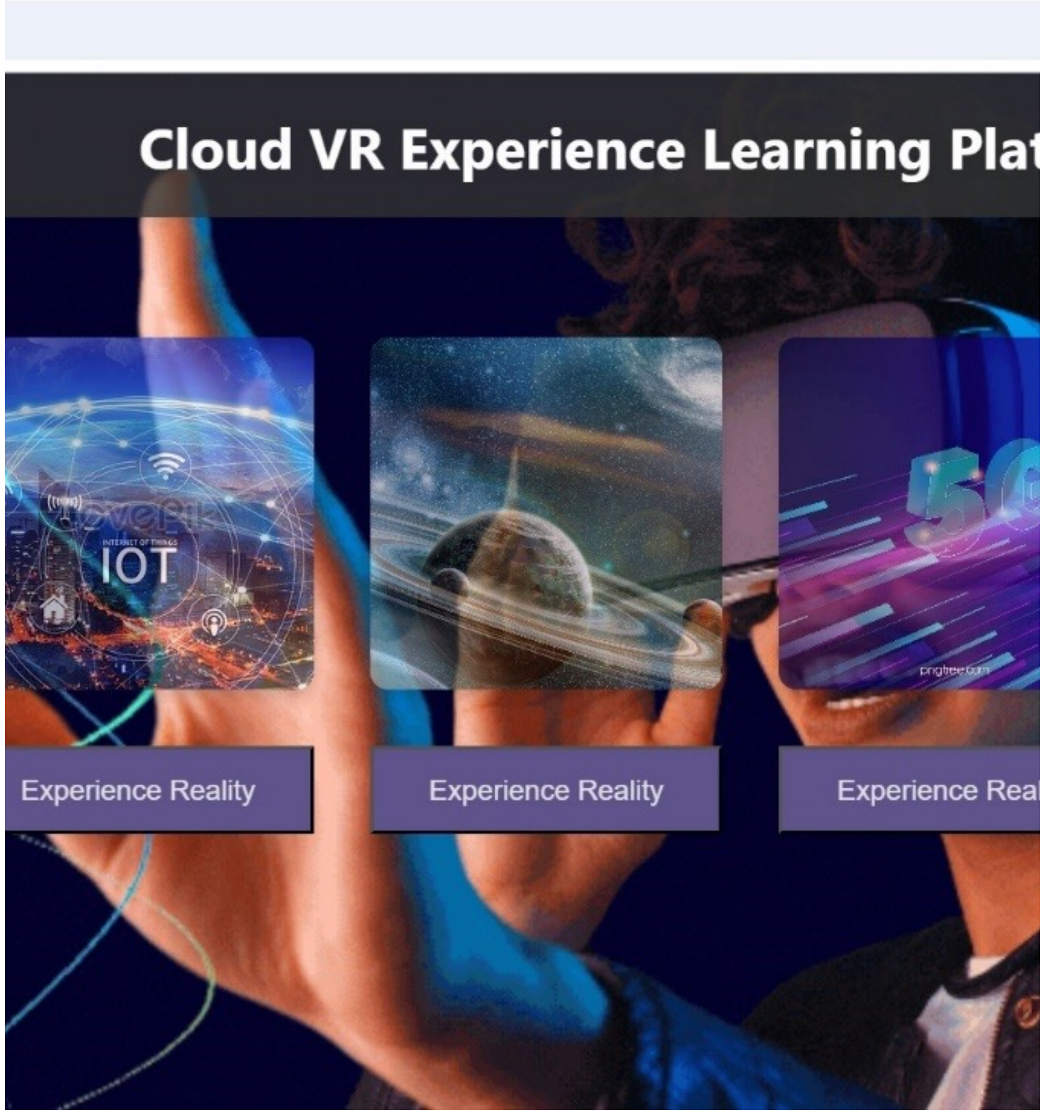
- **Reducing latency for immersive experiences**: AR/VR applications require extremely low latency to provide immersive user experiences. MEC enables this by processing data close to the user.
- **Cloud rendering at the edge**: MEC can support AR/VR applications by offloading graphics rendering tasks from core to the edge, ensuring faster and more responsive experiences.

- **Caching:** Varnish caching is a high-performance HTTP accelerator commonly used to speed up web applications by caching HTTP responses. It is often deployed in front of web servers (like Apache or Nginx) to reduce latency and decrease load on backend servers. Integrating Varnish with containers can enhance scalability and performance. Here’s an overview of how you can use Varnish caching in a containerized environment.



Cloud VR Experience Learning Platform

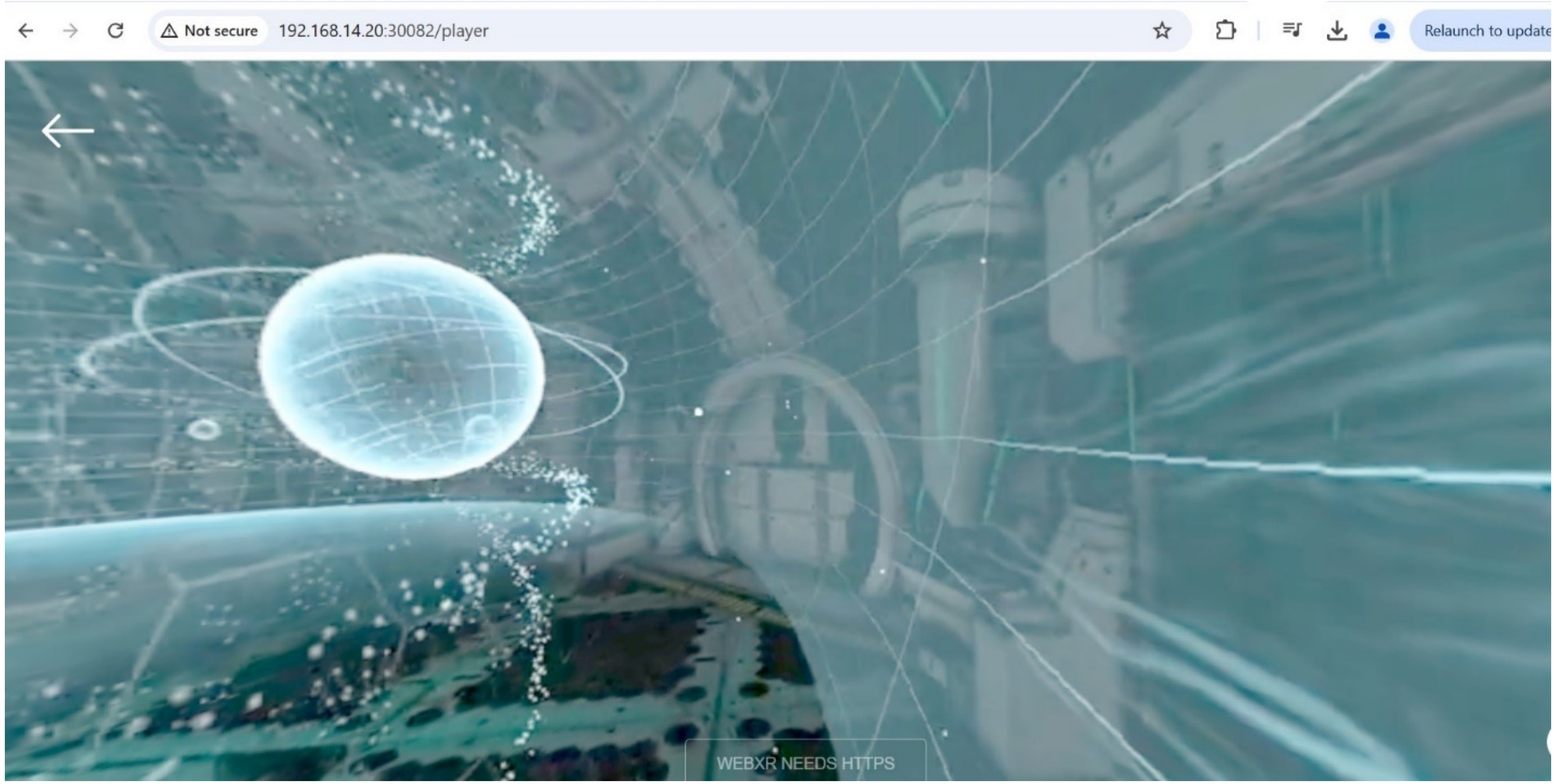
Cloud core IP:
192.168.x.x:30082



Cloud VR Experience Learning Plat

Application will be pushed to Edge Core using deployment files. Once application will be deployed go to edge core and application will be accessible using below URL.

- **http://ip-of-mec-edge-core**



Application running inside VR set

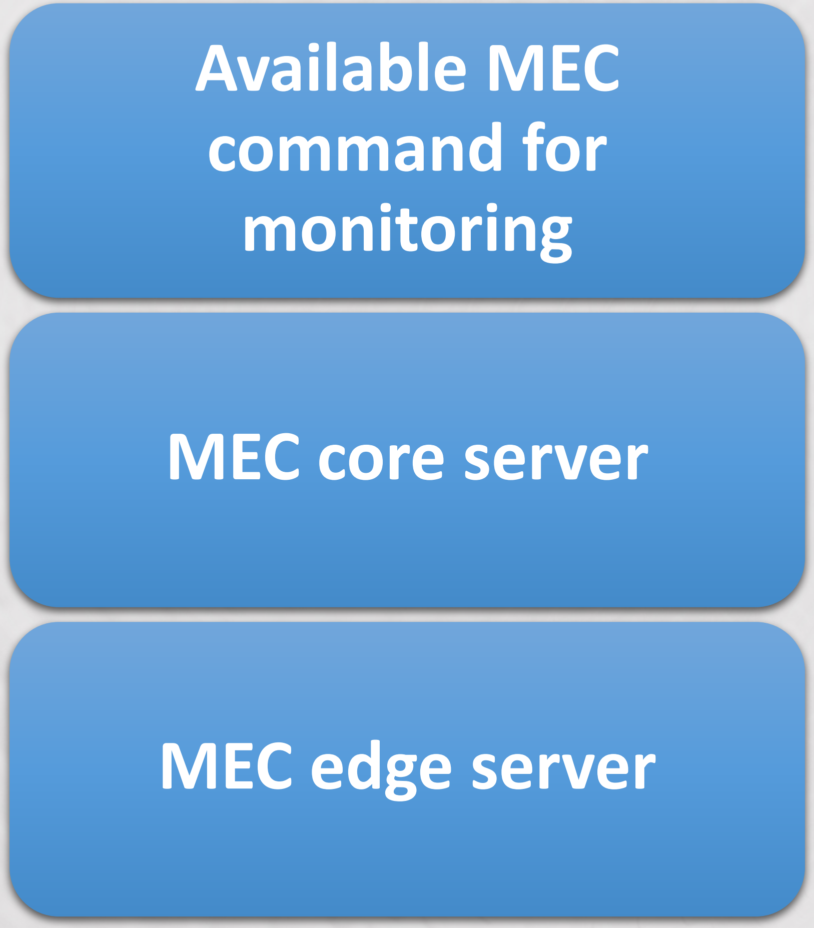
Use case objective

Latency and Bandwidth Optimization

- **Content delivery networks (CDNs) in MEC**: MEC can act as a localized CDN, reducing latency for content delivery and improving user experiences.

  - **Edge computing in ultra-low-latency applications**: 5G networks require ultra-low latency for applications such as telemedicine, VR, and AR. MEC is key to enabling these applications by processing data at the edge.

Monitoring of services in MEC

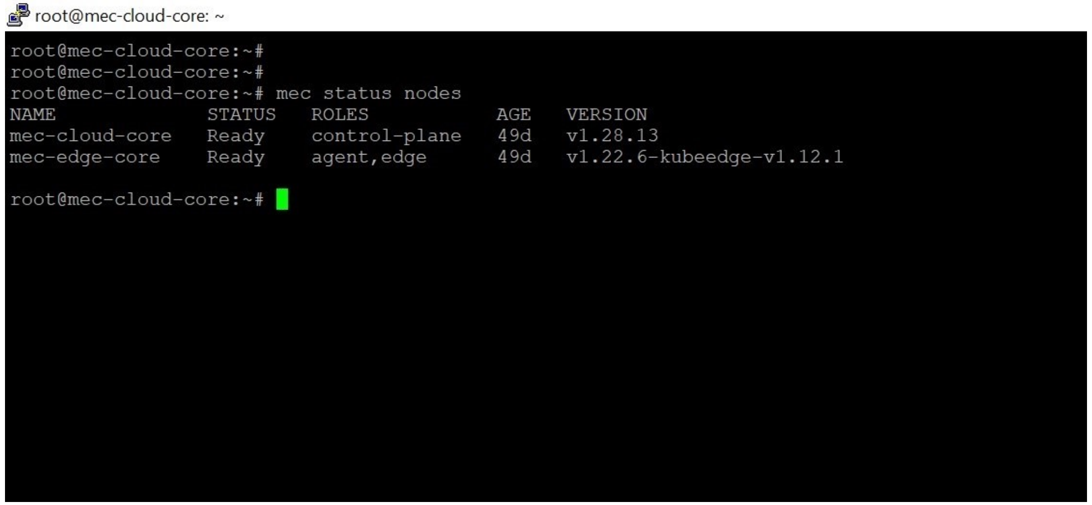


Available MEC command for monitoring

MEC core server

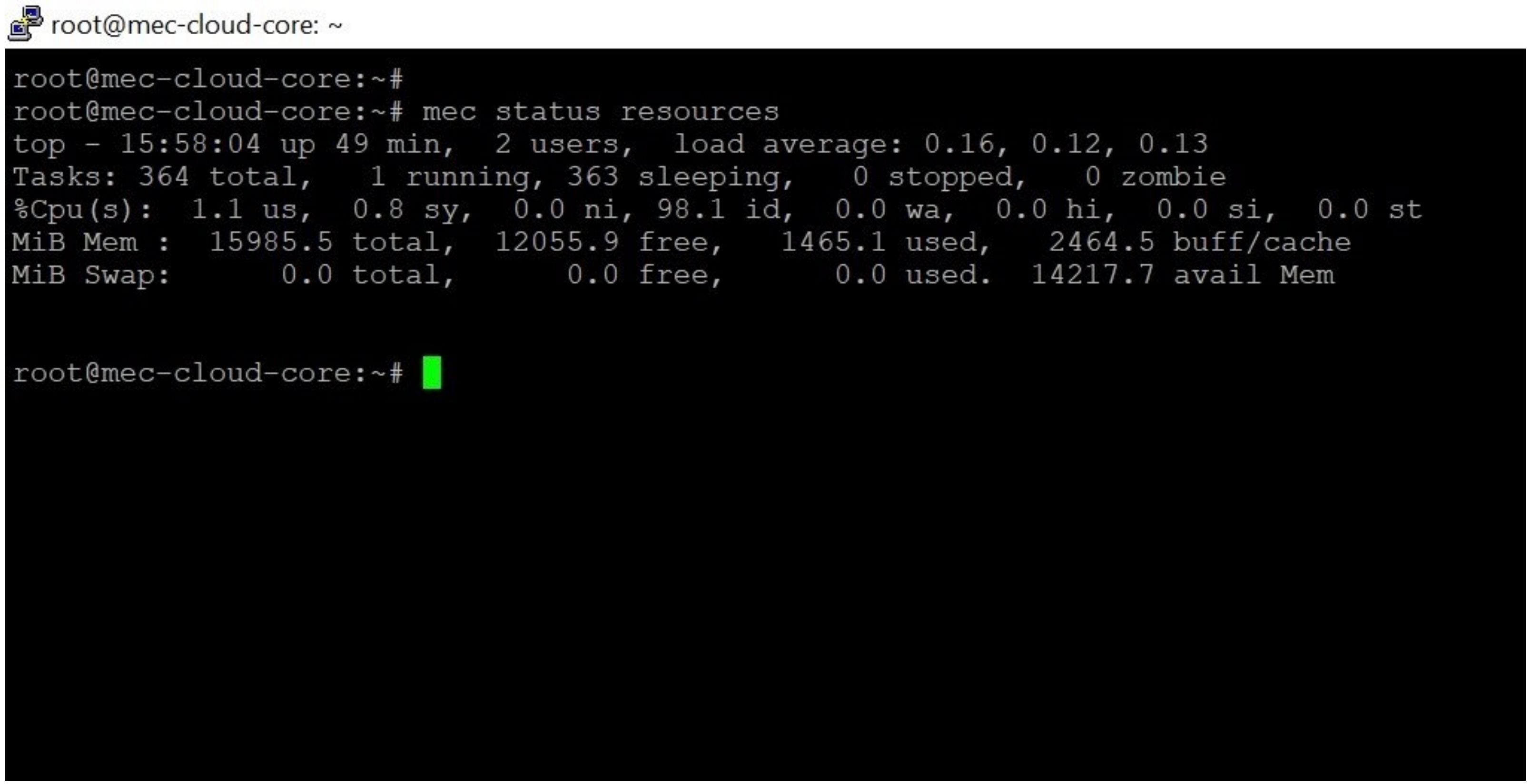
MEC edge server

All edge servers will connect with cloud core. To verify this run the above command on MEC Cloud Core
#mec status nodes



root@mec-cloud-core: ~

```
root@mec-cloud-core:~#
root@mec-cloud-core:~#
root@mec-cloud-core:~# mec status nodes
NAME             STATUS   ROLES           AGE   VERSION
mec-cloud-core   Ready    control-plane   49d   v1.28.13
mec-edge-core    Ready    agent,edge      49d   v1.22.6-kubeedge-v1.12.1

root@mec-cloud-core:~#
```

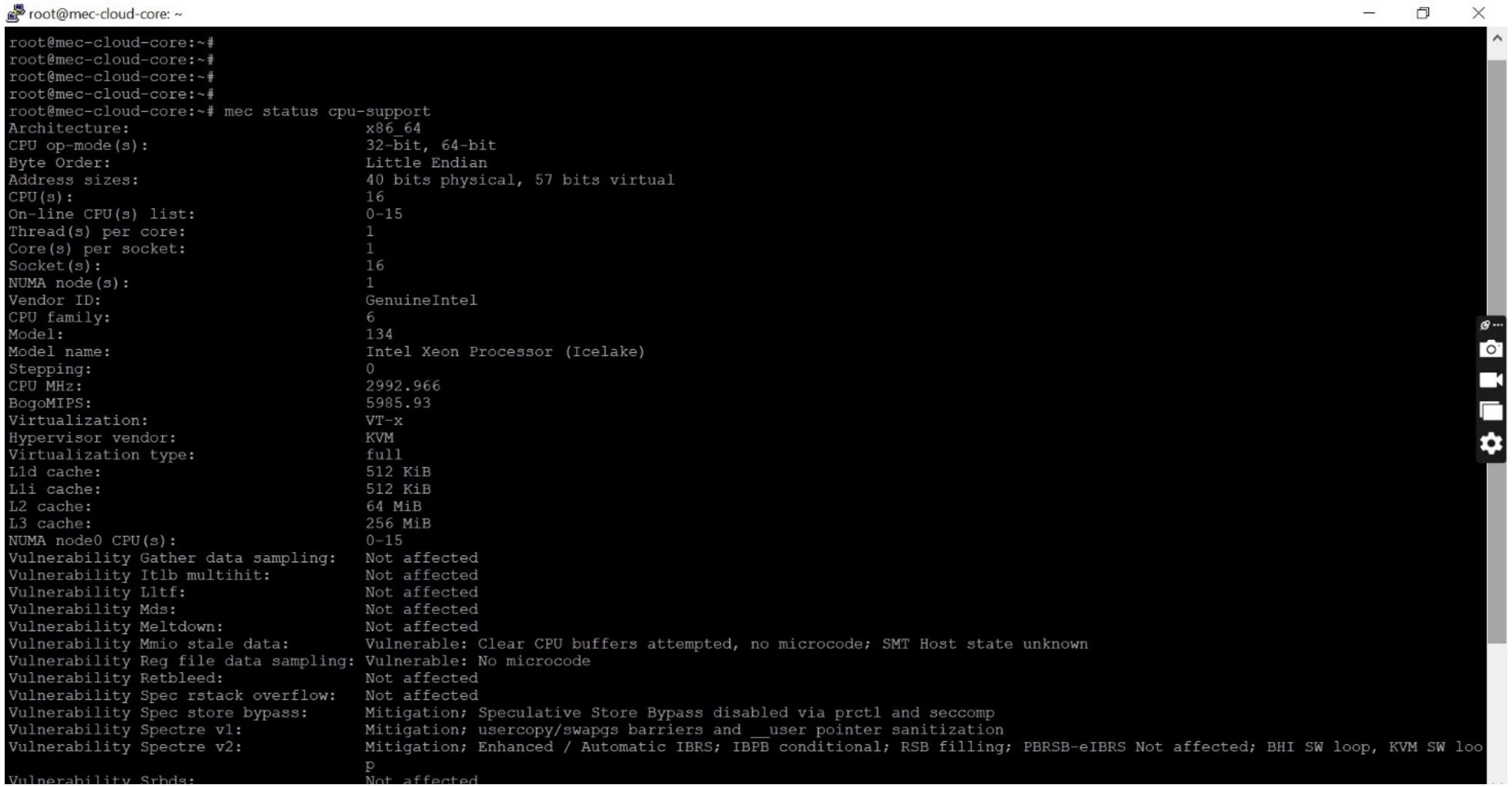


root@mec-cloud-core: ~

```
root@mec-cloud-core:~#
root@mec-cloud-core:~# mec status resources
top - 15:58:04 up 49 min,  2 users,  load average: 0.16, 0.12, 0.13
Tasks: 364 total,   1 running, 363 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.1 us,  0.8 sy,  0.0 ni, 98.1 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  15985.5 total,  12055.9 free,   1465.1 used,   2464.5 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.  14217.7 avail Mem


root@mec-cloud-core:~# █
```

Command result will display the cpu utilization, load average , tasks running , memory utilization etc.

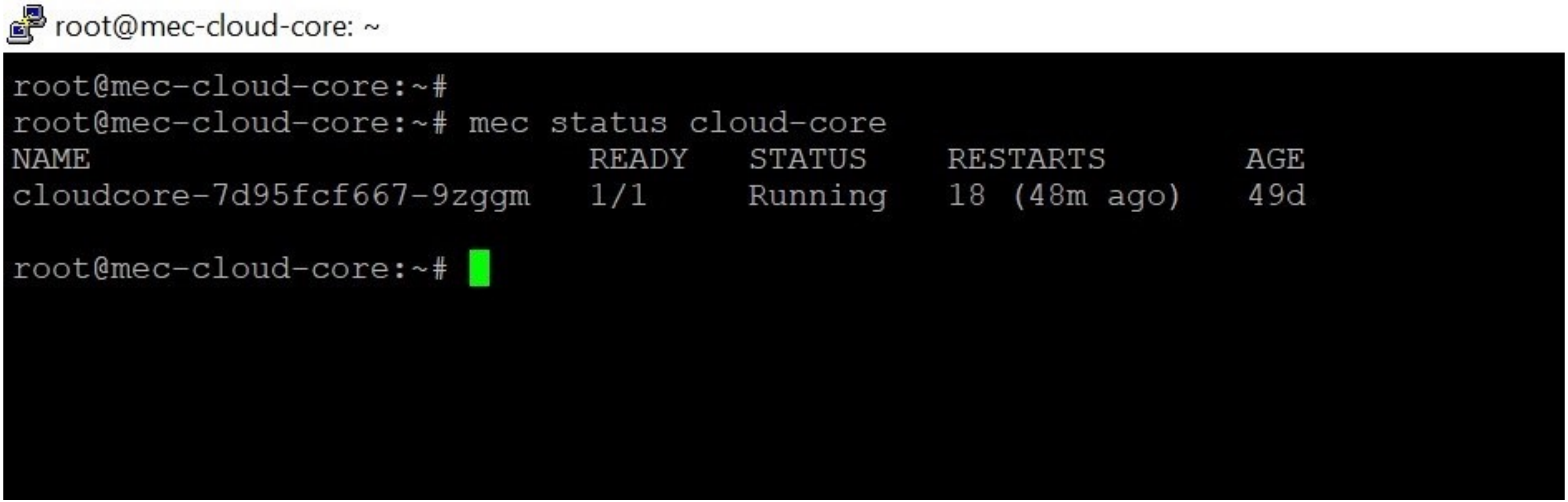
#mec status resources



```
root@mec-cloud-core:~#
root@mec-cloud-core:~#
root@mec-cloud-core:~#
root@mec-cloud-core:~#
root@mec-cloud-core:~# mec status cpu-support
Architecture:                         x86_64
CPU op-mode(s):                       32-bit, 64-bit
Byte Order:                           Little Endian
Address sizes:                        40 bits physical, 57 bits virtual
CPU(s):                               16
On-line CPU(s) list:                  0-15
Thread(s) per core:                   1
Core(s) per socket:                   1
Socket(s):                            16
NUMA node(s):                         1
Vendor ID:                            GenuineIntel
CPU family:                           6
Model:                                134
Model name:                           Intel Xeon Processor (Icelake)
Stepping:                             0
CPU MHz:                              2992.966
BogoMIPS:                             5985.93
Virtualization:                       VT-x
Hypervisor vendor:                    KVM
Virtualization type:                  full
L1d cache:                            512 KiB
L1i cache:                            512 KiB
L2 cache:                             64 MiB
L3 cache:                             256 MiB
NUMA node0 CPU(s):                    0-15
Vulnerability Gather data sampling:   Not affected
Vulnerability Itlb multihit:          Not affected
Vulnerability L1tf:                   Not affected
Vulnerability Mds:                    Not affected
Vulnerability Meltdown:               Not affected
Vulnerability Mmio stale data:        Vulnerable: Clear CPU buffers attempted, no microcode; SMT Host state unknown
Vulnerability Reg file data sampling: Vulnerable: No microcode
Vulnerability Retbleed:               Not affected
Vulnerability Spec rstack overflow:   Not affected
Vulnerability Spec store bypass:      Mitigation; Speculative Store Bypass disabled via prctl and seccomp
Vulnerability Spectre v1:             Mitigation; usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2:             Mitigation; Enhanced / Automatic IBRS; IBPB conditional; RSB filling; PBRSB-eIBRS Not affected; BHI SW loop, KVM SW loo
                                      p
Vulnerability Srbds:                  Not affected
```

This command will display all the cpu related information. #mec status cpu-support

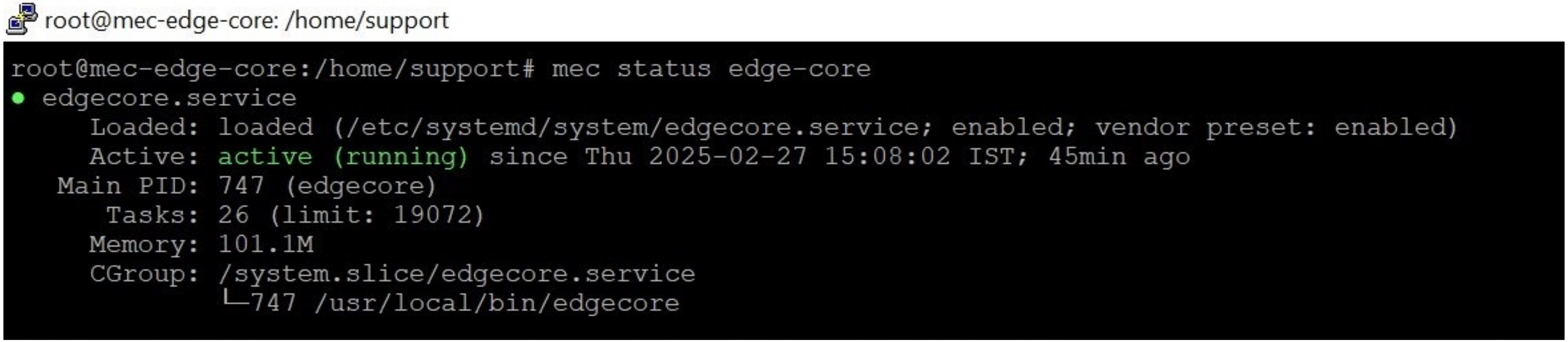
It will print the status of cloudcore on MEC Cloud Core server
#mec status cloud-core



root@mec-cloud-core: ~

```
root@mec-cloud-core:~#
root@mec-cloud-core:~# mec status cloud-core
NAME                         READY   STATUS     RESTARTS       AGE
cloudcore-7d95fcf667-9zggm   1/1     Running    18 (48m ago)   49d

root@mec-cloud-core:~# 
```

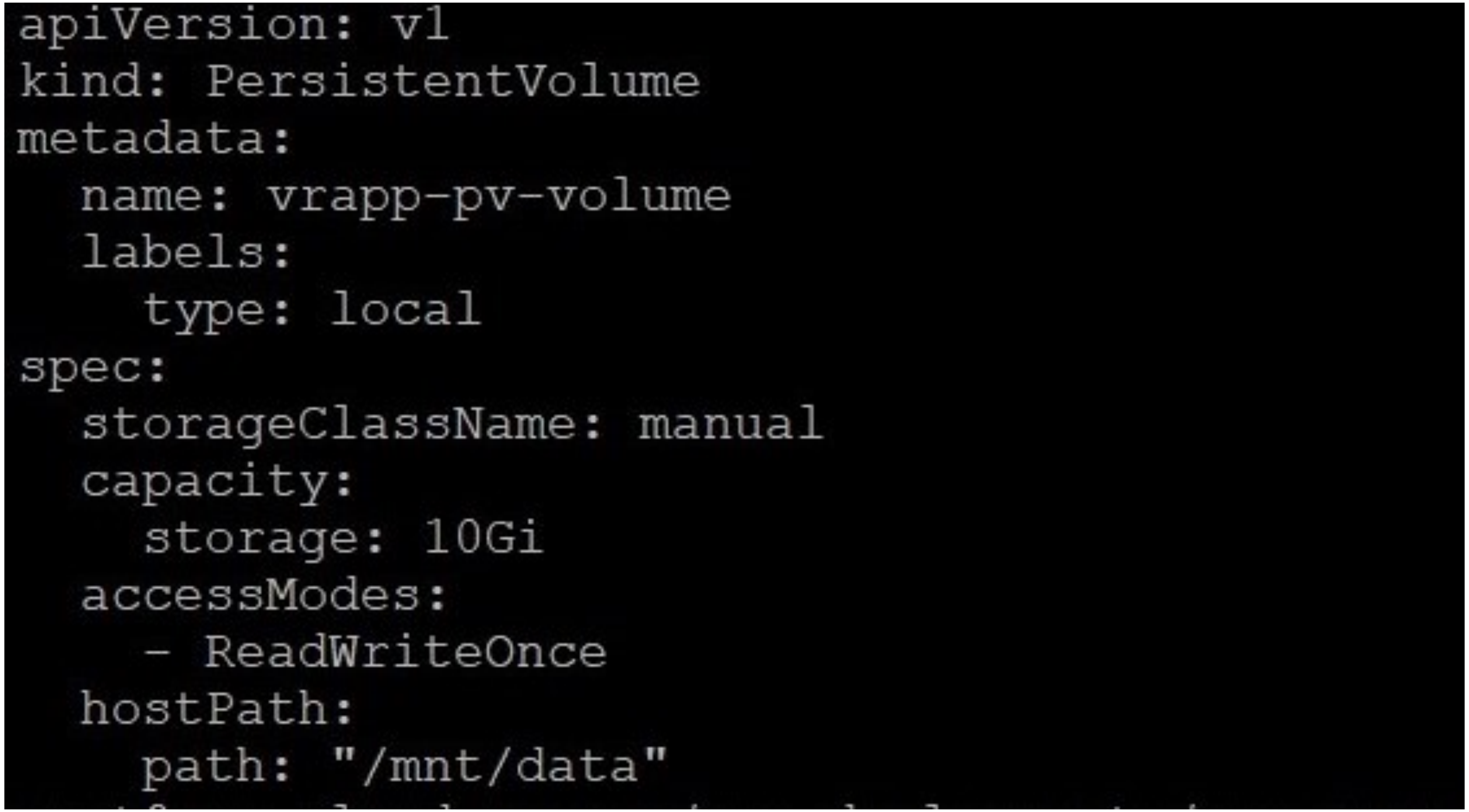
It will print the current status of the daemon MEC Edge Core server
#mec status edge-core



root@mec-edge-core: /home/support

```
root@mec-edge-core:/home/support# mec status edge-core
● edgecore.service
     Loaded: loaded (/etc/systemd/system/edgecore.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-02-27 15:08:02 IST; 45min ago
   Main PID: 747 (edgecore)
      Tasks: 26 (limit: 19072)
     Memory: 101.1M
     CGroup: /system.slice/edgecore.service
             └─747 /usr/local/bin/edgecore
```

It will print the current volume attached to MEC Cloud Core server
#mec status persistent-storage



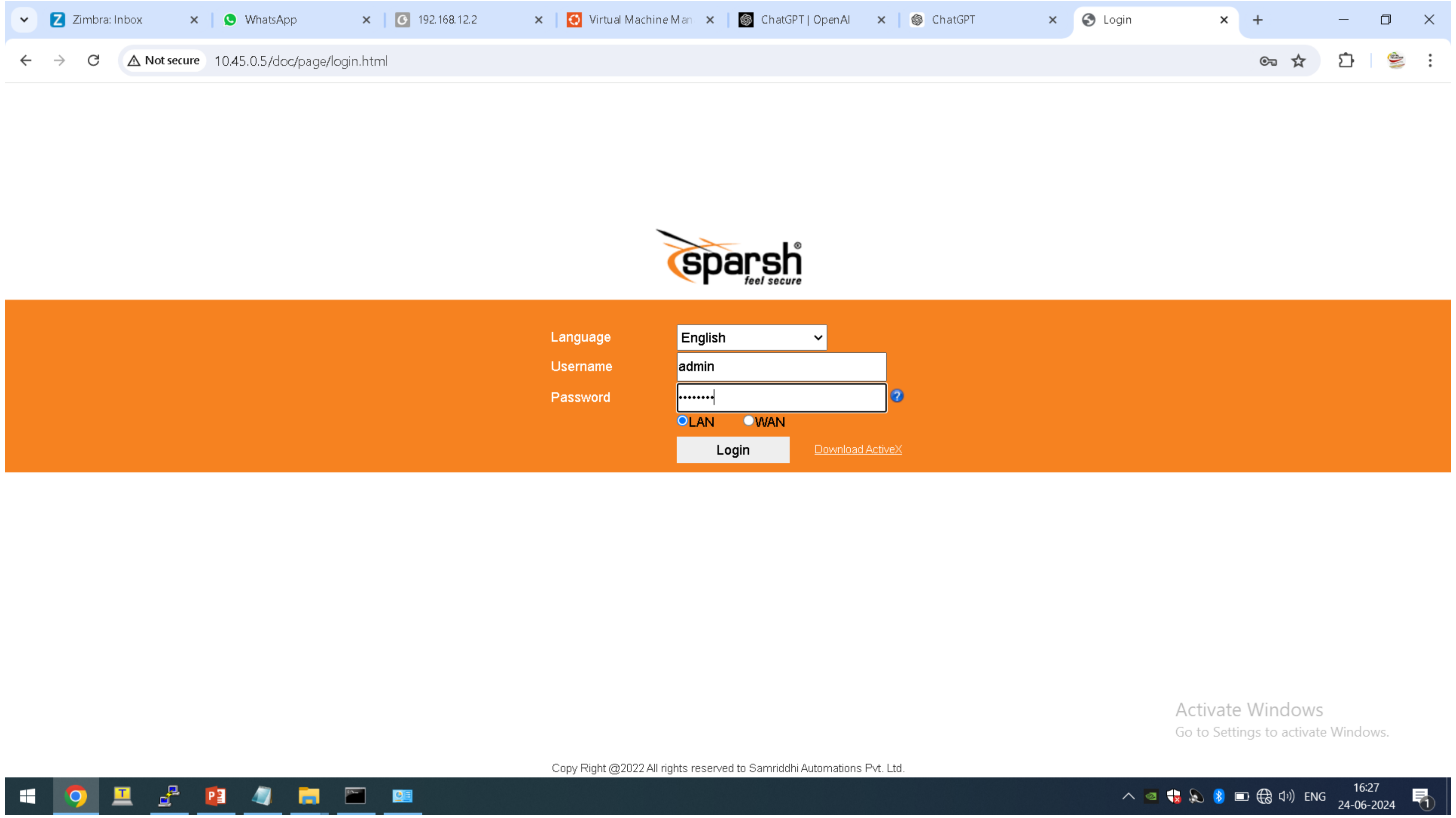
```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: vrapp-pv-volume
  labels:
    type: local
spec:
  storageClassName: manual
  capacity:
    storage: 10Gi
  accessModes:
    - ReadWriteOnce
  hostPath:
    path: "/mnt/data"
```

5G AI Camera

- Features:
- • 5MP 1/2.7" CMOS image sensor, low luminance, and high-definition image.
- • Intelligent Analytics Supported: Human Detection, Intrusion Detection, Audio Detection, Object Left, Object Lost, Line crossing, Scene Change
- • SD card supported up to 512GB.
- • Wide Dynamic Range up to 120dB
- • Digital Alarm 1 Ch In/ 1 Ch Out

5G AI Camera

- LOGIN Credentials;
- Username: admin
- Password: admin123



10.45.0.5/doc/page/login.html

Language: English

Username: admin

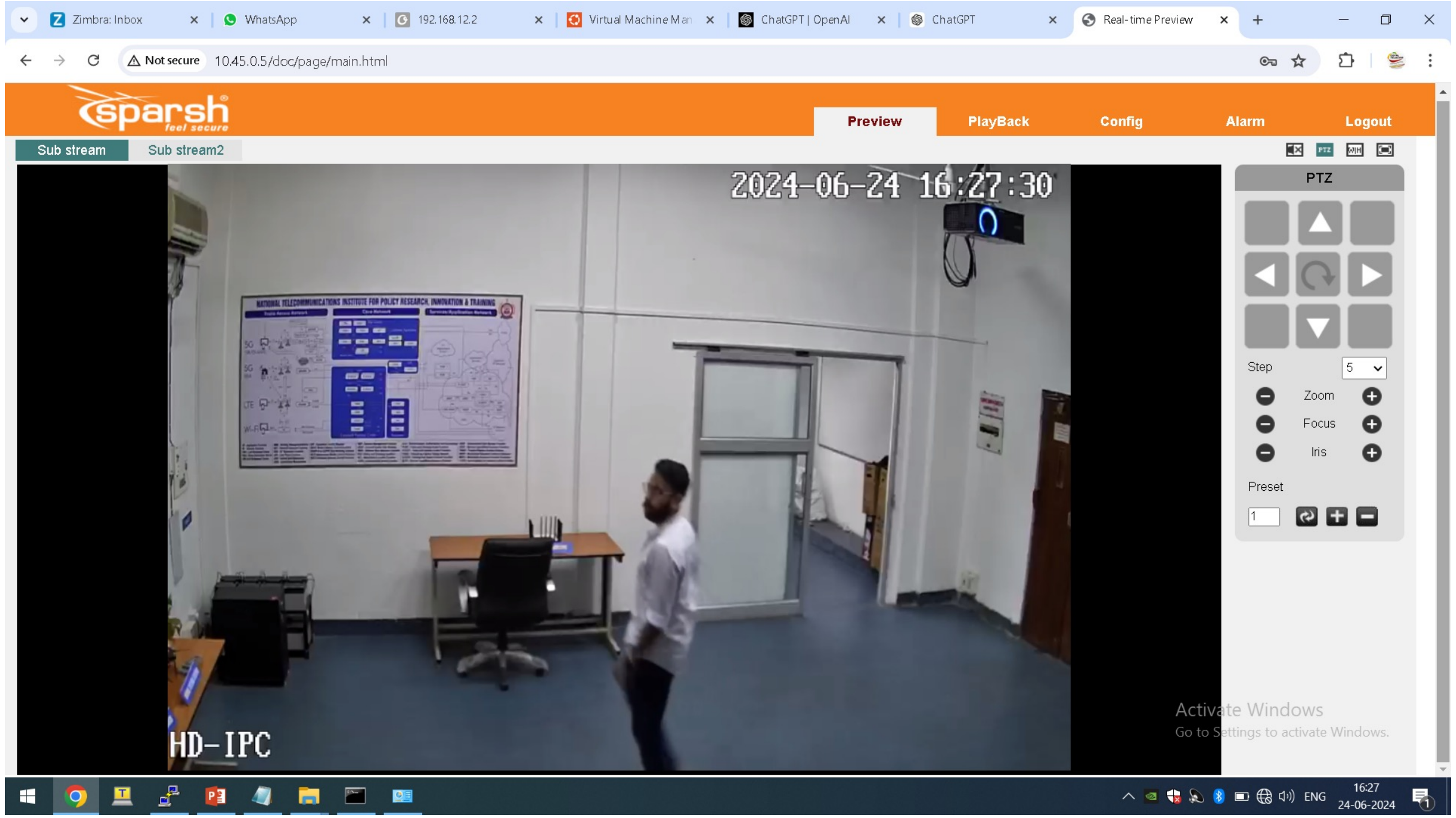
Password: ••••••••

● LAN ○ WAN

Copy Right @2022 All rights reserved to Samriddhi Automations Pvt. Ltd.

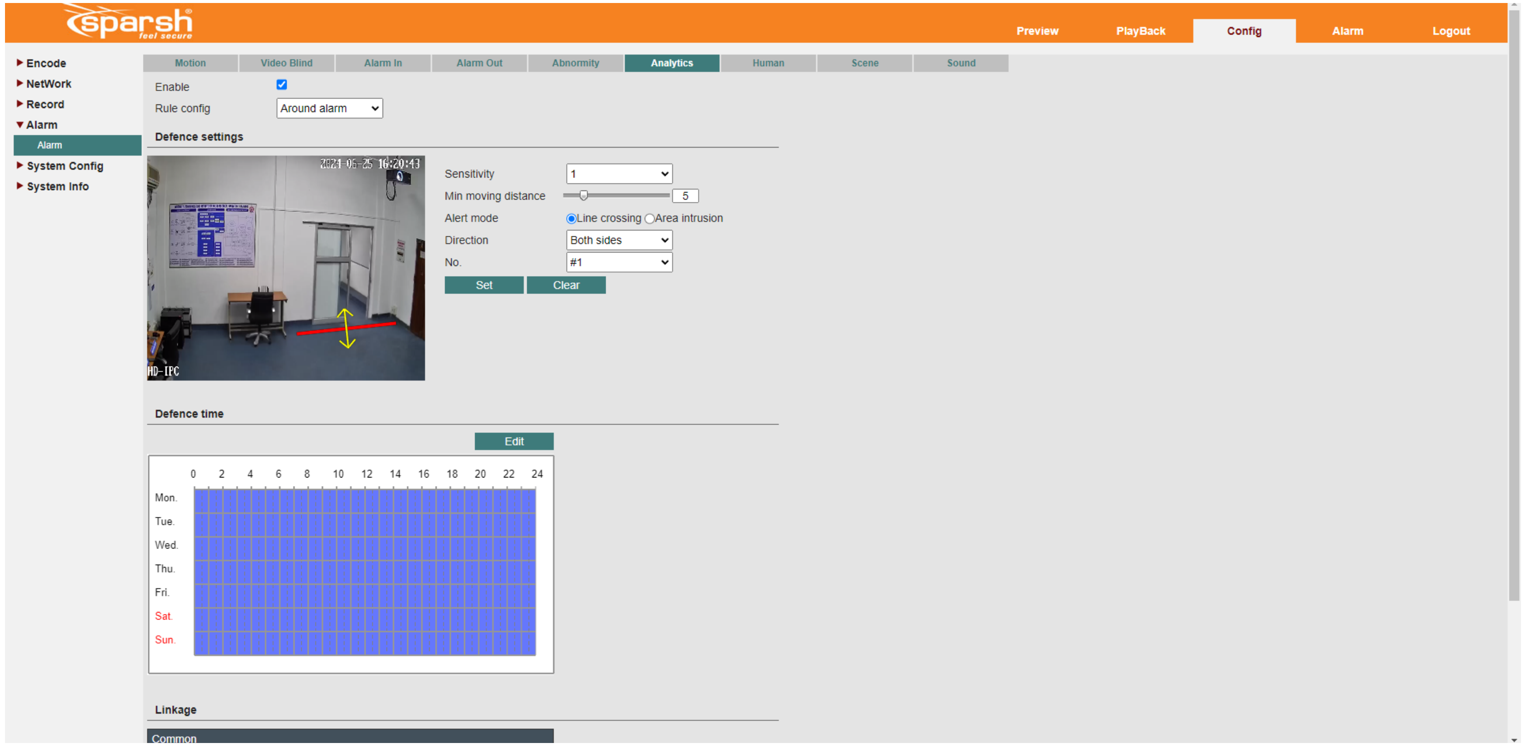
5G AI Camera

- **Live streaming of the camera**



5G AI Camera

Live alarm in case of crossing



Enable ☑

Rule config: Around alarm

Defence settings

Sensitivity: 1

Min moving distance: 5

Alert mode: ● Line crossing ○ Area intrusion

Direction: Both sides

No.: #1

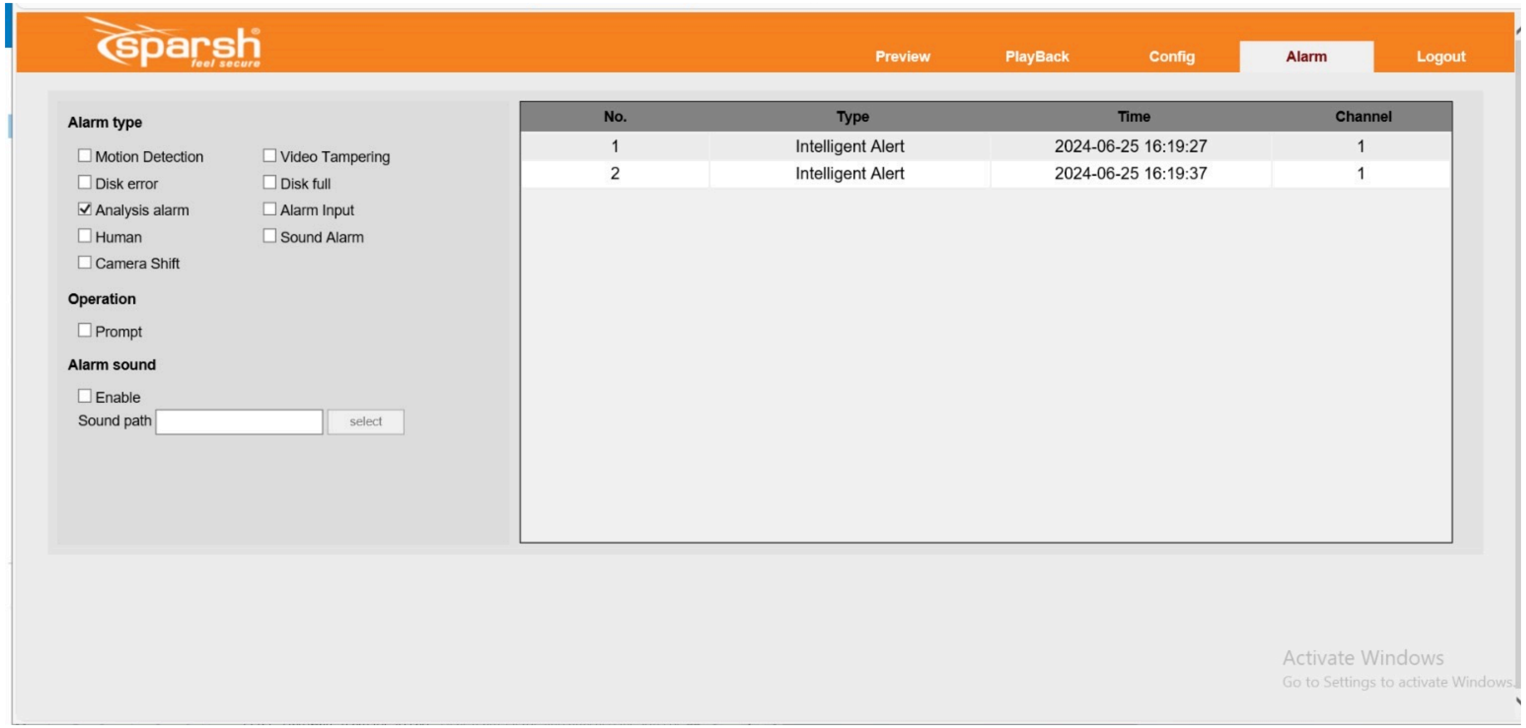
Defence time

Linkage

Common

5G AI Camera

check the alarm logs by checking the analysis alarm in Alarm section in the upper tab section



Alarm type

☐ Motion Detection
☐ Disk error
☑ Analysis alarm
☐ Human
☐ Camera Shift
☐ Video Tampering
☐ Disk full
☐ Alarm Input
☐ Sound Alarm

Operation

☐ Prompt

Alarm sound

☐ Enable

Sound path

No.	Type	Time	Channel
1	Intelligent Alert	2024-06-25 16:19:27	1
2	Intelligent Alert	2024-06-25 16:19:37	1

IoT Gateway

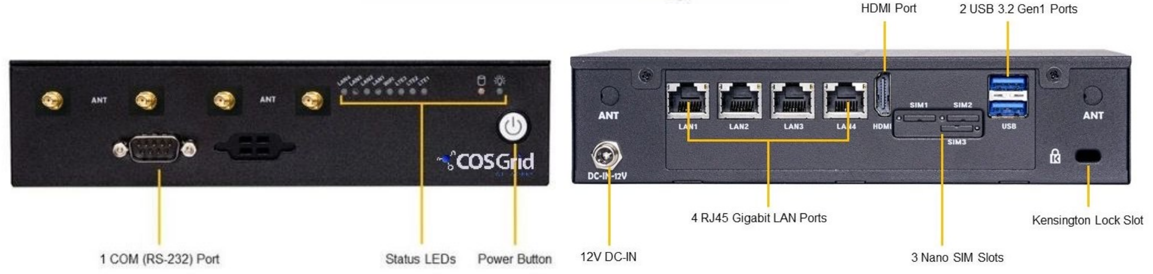
COSGrid IoT Gateway- IG4XG - Hardware Overview

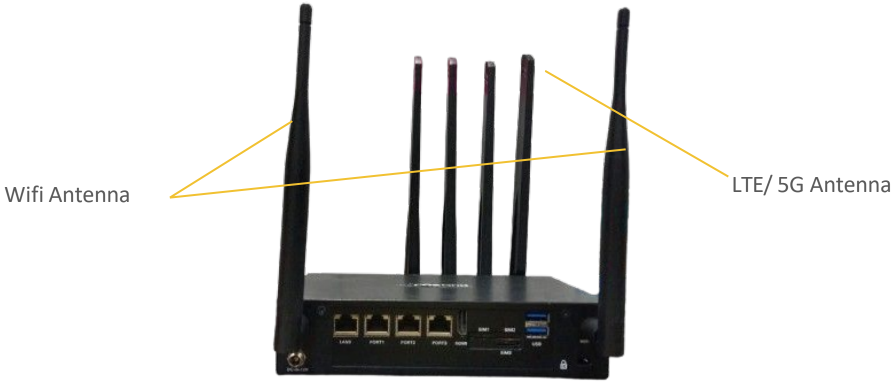
Intel Celeron J3455 and supports 4x GbE LAN ports, 1 HDMI port, and 3 M.2 B key wireless modules

Key Highlights

- Intel® Celeron J3455 4C/4T Processor with up to 8GB DDR3L 1866MHz SODIMM
- Intel® HD Graphics
- 4x Gigabit LAN Ports (C: Intel® I211 AT)
- 3x M.2 B Key (USB) 2242/3042 with 3x Nano SIM Slot
- 1x M.2 E Key 2230 1x 2.5” 7mm Storage Drive
- 2x USB 3.2 Ports Gen1
- 1 HDMI Port, 1 COM Port;

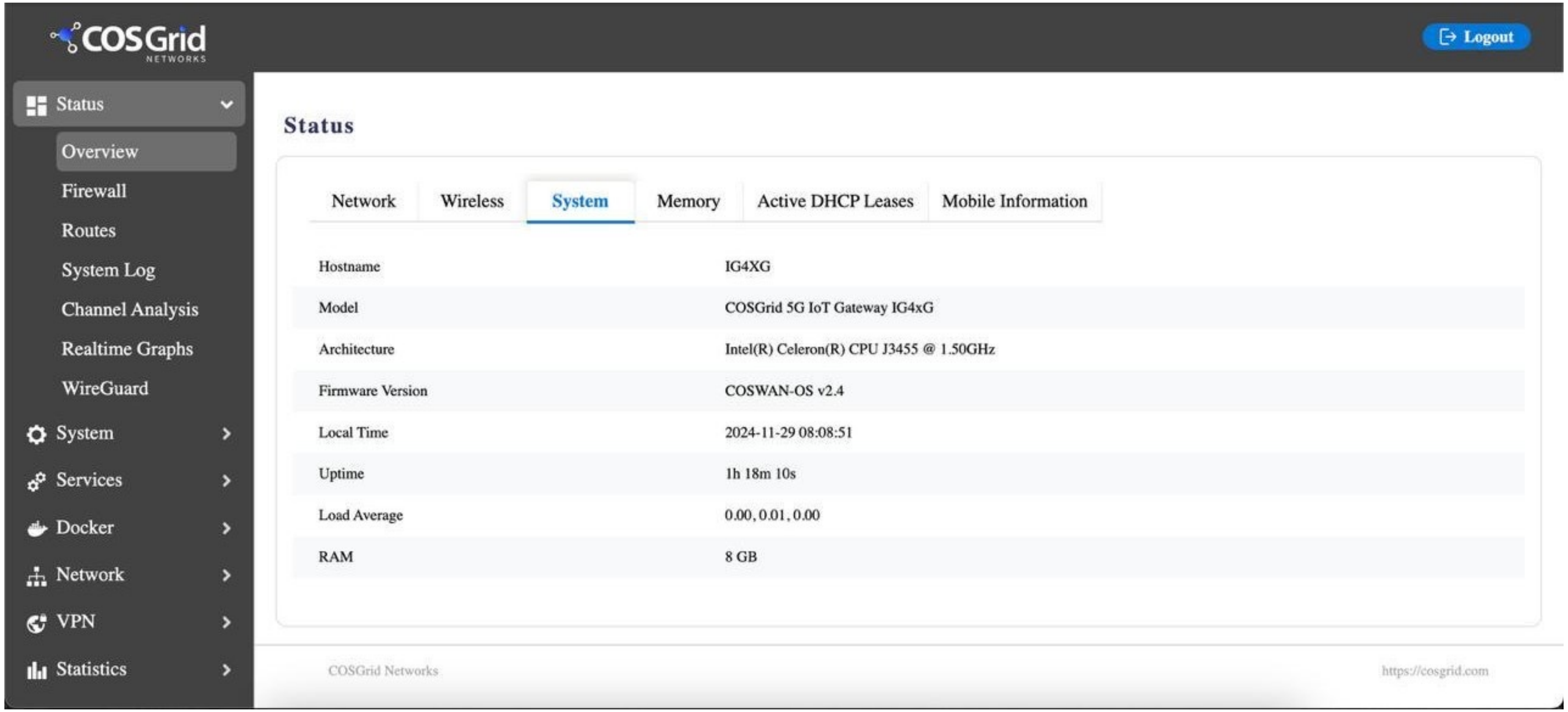
Features	Description
Form Factor	Fan-based Embedded Rackmount | Enclosure: 190 x 44 x 120mm (7.48" x 1.72" x 4.72") Package: 300 x 130 x 279mm (11.81" x 5.12" x 11.02")
Processor	Intel® Celeron® J3455 processor Up to 4C/4T; Up to 2MB Cache
System Memory	Slot Count: 1 DIMM slots Max Memory (2DPC): Up to 8GB 1866MT/s non-ECC UDIMM
Input/Output	LAN: 4 RJ45 1 GbE LAN port(s) Video: 1 HDMI 1.4 port(s)
System Cooling	Fans: 1x 40mmcm heavy duty fans with optimal fan speed control
Wi-Fi	Wi-Fi 802.11n/ac with 2 X Modules
Antenna	4 X LTE/5G + 2 X Wifi Antenna,
Power Supply	1x 60W power supply
Expansion Slots	1 M.2 NVMe slot(s) (E-key 2230) 2 M.2 NVMe slot(s) (B-key 2242/3042) 1 M.2 NVMe/SATA slot(s) (B-key 2242/3042)
Operating Environment	Operating Temperature: °C ~ °C (°F ~ °F) Non-operating Temperature: °C to °C (°F to °F) Operating Relative Humidity: % to % () Non-operating Relative Humidity: % to % ()





Gateway Configuration

Set Steps	Acceptance Criteria
In GUI Navigate ***Status - > Overview - > Systems***	CPU : Qualcomm or equivalent, Dual core or Higher **RAM: 256 MB**

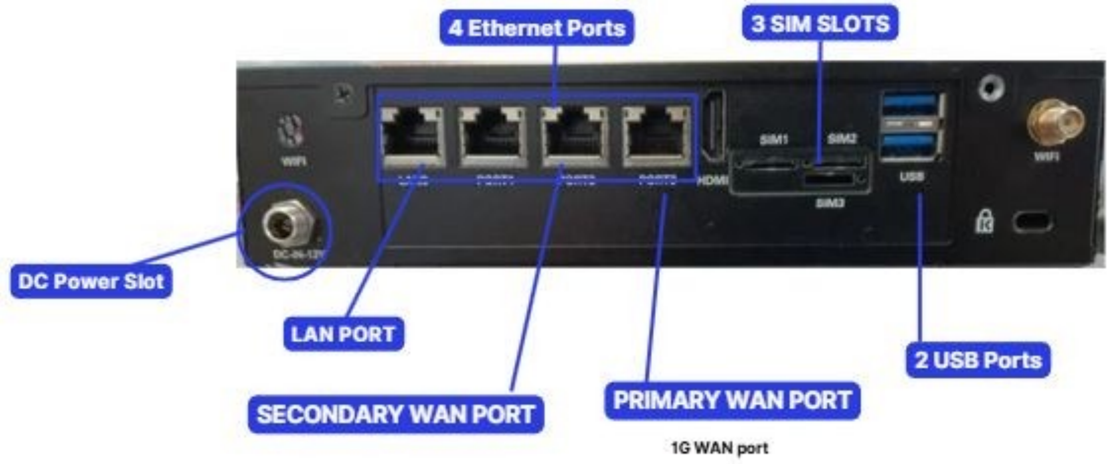


Status

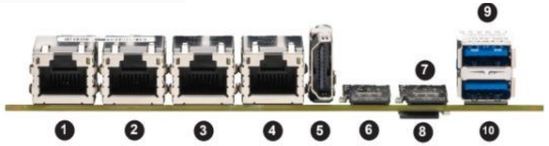
Hostname	IG4XG
Model	COSGrid 5G IoT Gateway IG4xG
Architecture	Intel(R) Celeron(R) CPU J3455 @ 1.50GHz
Firmware Version	COSWAN-OS v2.4
Local Time	2024-11-29 08:08:51
Uptime	1h 18m 10s
Load Average	0.00, 0.01, 0.00
RAM	8 GB

Verify Input /Output Configuration Support

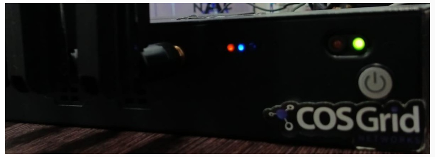
Set Steps	Acceptance Criteria
Take the Hardware & Check Manually	Supports USB Supports minimum 4 nos 10/100/1000 Ethernet ports Supports 1G WAN port . Supports status LED Supports PoE and DC power socket. Supports 1 or more SIMs

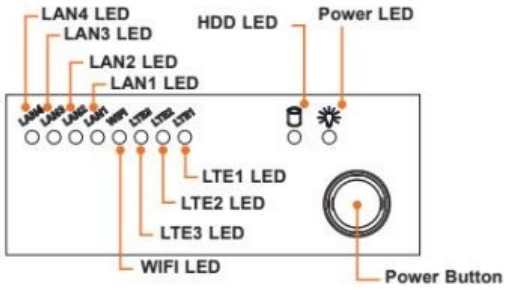


1G WAN port



1 LAN1	6 SIM Slot 1 (JMD1)
2 LAN2	7 SIM Slot 2 (JMD2)
3 WAN2	8 SIM Slot 3 (JMD3)
4 WAN1	**9** USB1
5 HDMI Port	**10** USB0

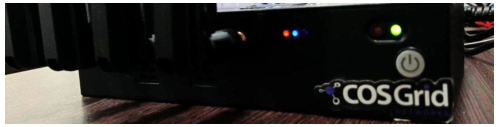


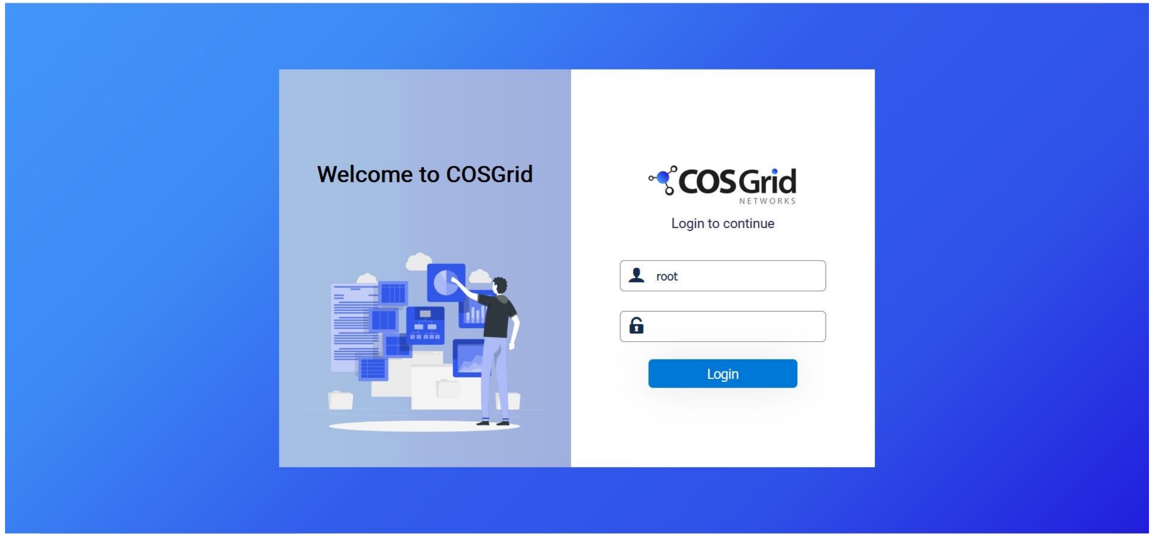


Click Here - For Hardware Setup Overview

Hardware & GUI Connectivity

Set Steps	Acceptance Criteria
Turn on the device after plugging in the power. Connect the ethernet cable to the LAN port and your laptop.	The LED in the device should blink.
Then you can go to the **IP Address provided by the provider** in your browser. Figure:1	The login window to access COSGrid IoT Gateway should be visible.
Enter the credential provided by the provider.	You should be able to login and see the functionalities. Figure:2




Welcome to COSGrid

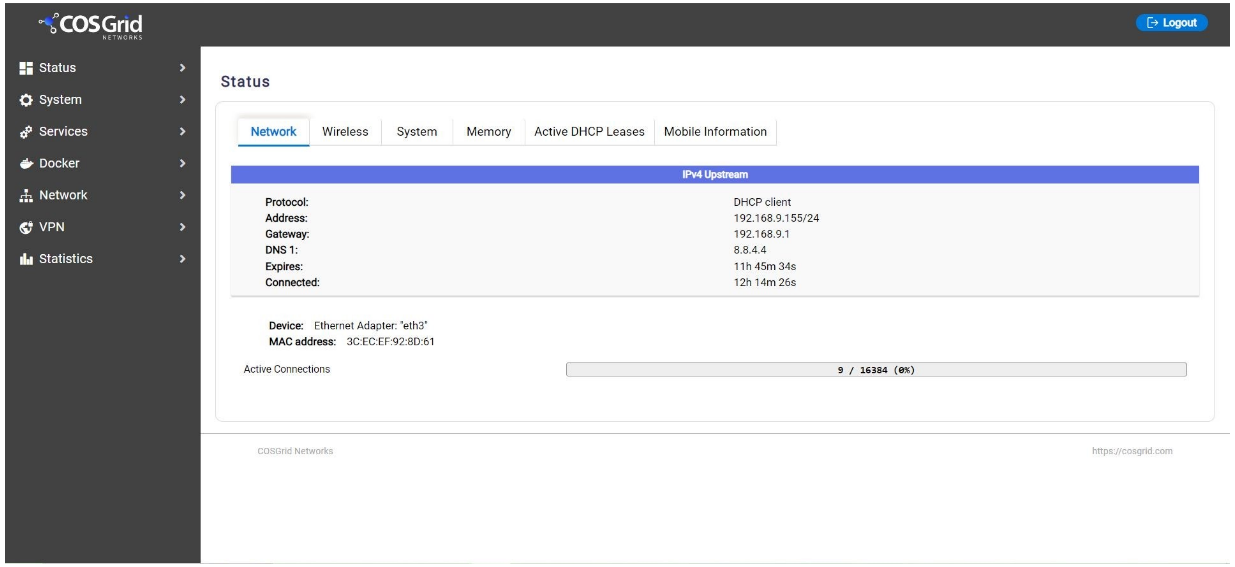
COSGrid NETWORKS

Login to continue

root

Login

Figure1



Status

Network | Wireless | System | Memory | Active DHCP Leases | Mobile Information

IPv4 Upstream

Protocol:	DHCP client
Address:	192.168.9.155/24
Gateway:	192.168.9.1
DNS 1:	8.8.4.4
Expires:	11h 45m 34s
Connected:	12h 14m 26s

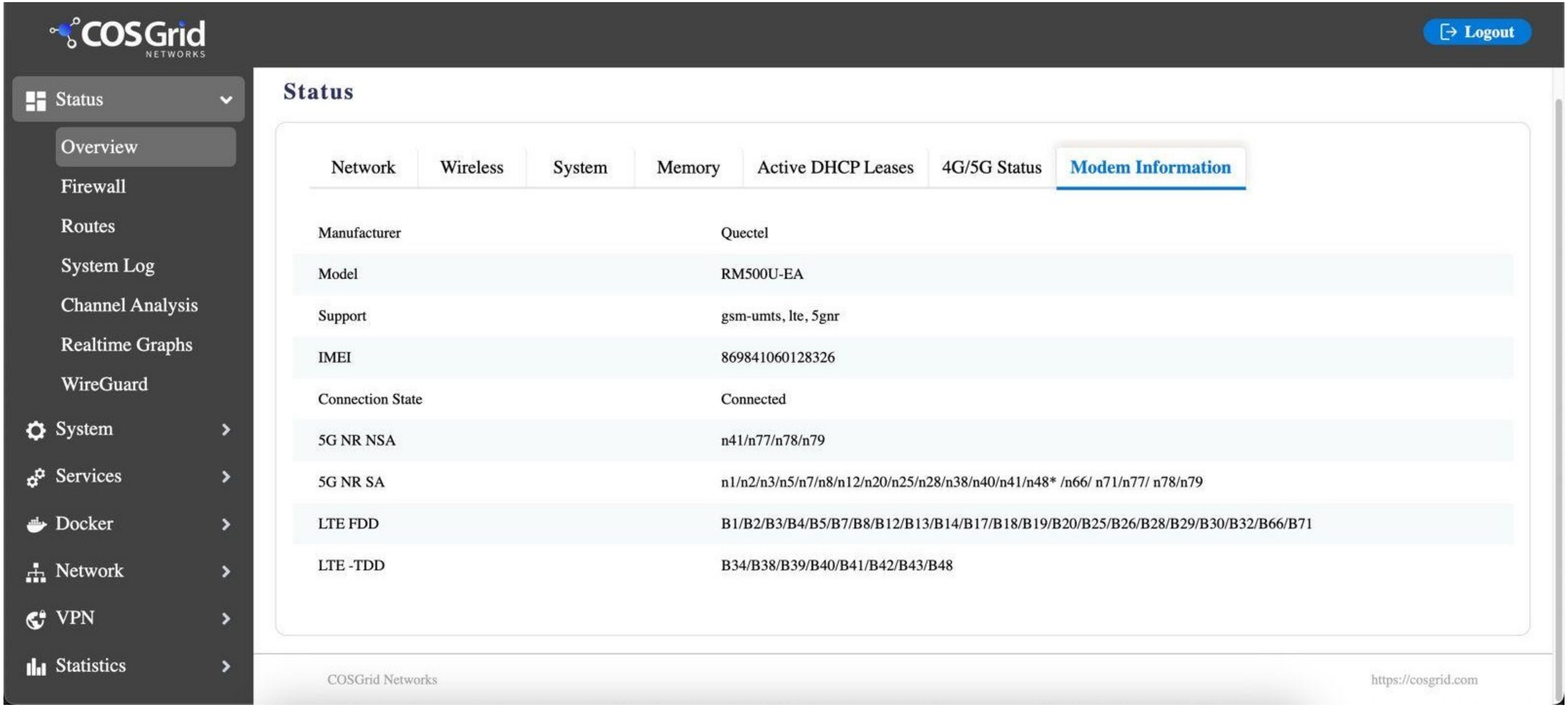
Device: Ethernet Adapter: "eth3"
MAC address: 3C:EC:EF:92:8D:61

Active Connections 9 / 16384 (0%)

COSGrid Networks https://cosgrid.com

Figure:2

Modem & cellular Bands Status

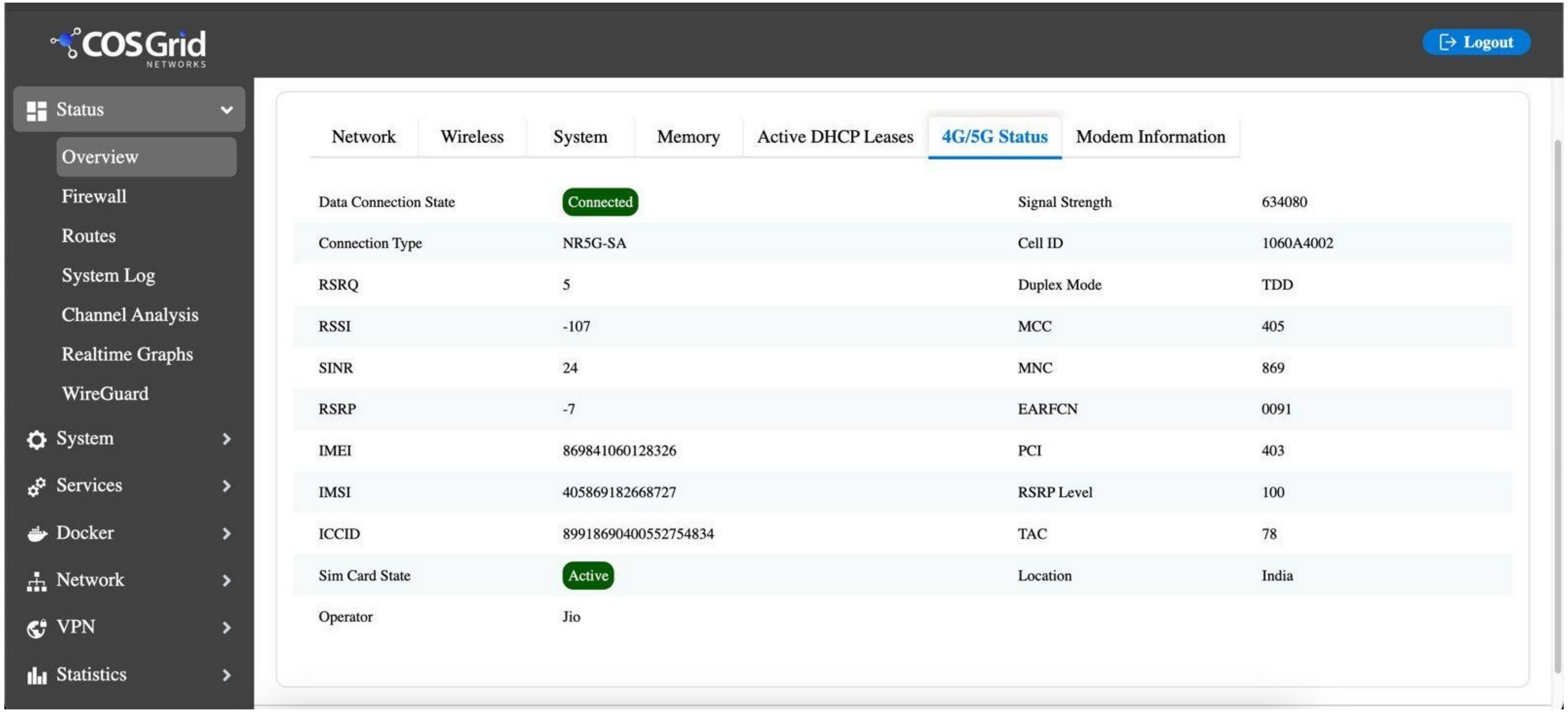


Status

Manufacturer	Quectel
Model	RM500U-EA
Support	gsm-umts, lte, 5gnr
IMEI	869841060128326
Connection State	Connected
5G NR NSA	n41/n77/n78/n79
5G NR SA	n1/n2/n3/n5/n7/n8/n12/n20/n25/n28/n38/n40/n41/n48* /n66/ n71/n77/ n78/n79
LTE FDD	B1/B2/B3/B4/B5/B7/B8/B12/B13/B14/B17/B18/B19/B20/B25/B26/B28/B29/B30/B32/B66/B71
LTE -TDD	B34/B38/B39/B40/B41/B42/B43/B48

Device, WAN status & Mobile Signal Quality

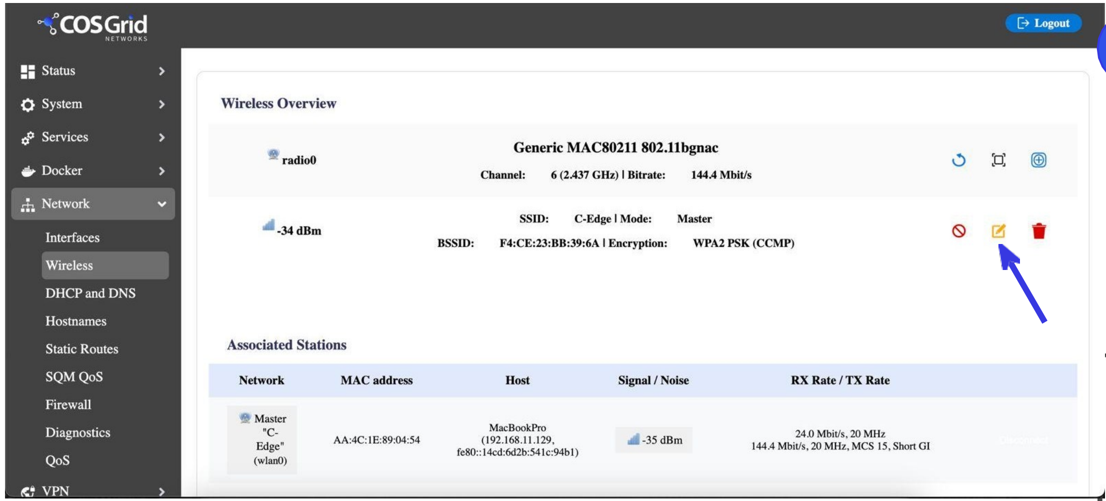
Set Steps	Acceptance Criteria
Go to ***Status > Overview. Under the 4G/5G Status*** Verify the capability of the IoT gateway to monitor Mobile Cell ID. Figure:27	Allows monitoring of: Device Model, Revision and Serial Number, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP, WAN Type, WAN IP, Mobile Operator Name, Mobile Signal Strength, Mobile Network Type.



Data Connection State	Connected	Signal Strength	634080
Connection Type	NR5G-SA	Cell ID	1060A4002
RSRQ	5	Duplex Mode	TDD
RSSI	-107	MCC	405
SINR	24	MNC	869
RSRP	-7	EARFCN	0091
IMEI	869841060128326	PCI	403
IMSI	405869182668727	RSRP Level	100
ICCID	89918690400552754834	TAC	78
Sim Card State	Active	Location	India
Operator	Jio		

WiFi Access points & Security

Set Steps	Acceptance Criteria
Navigate ***Network > Wireless.*** Click the Edit button, Configuration window Popup Scroll down the pop up You will see the General Setup tab ***Select Access Point Mode.*** Confirm the settings for **SSID, security protocols (WPA2, WPA3).**	Both options for configuring a network manually and scanning networks should be there. WiFi Security : WPA X /WEP/ TKIP variants as per the latest version.
Ensure that devices can connect to the network seamlessly, and there are no connectivity issues. Test the compatibility of various devices (laptops, smartphones, IoT devices) with the Access Point.	Support minimum 30 simultaneous WiFi users connections. The network should work seamlessly on every device.



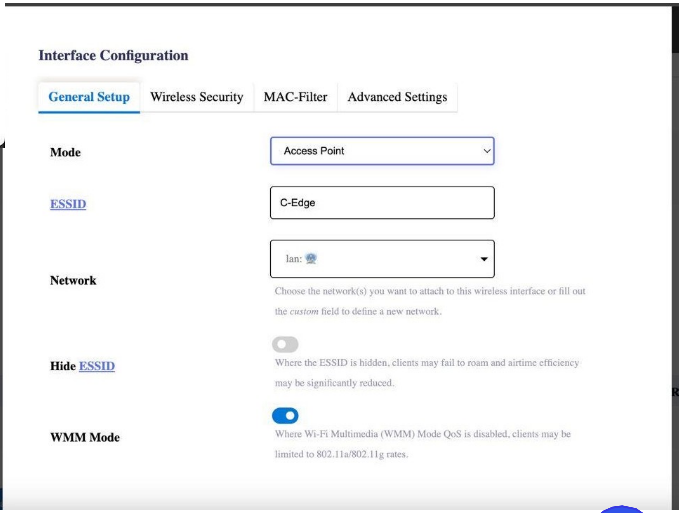
Wireless Overview

radio0 — Generic MAC80211 802.11bgnac
Channel: 6 (2.437 GHz) | Bitrate: 144.4 Mbit/s

-34 dBm — SSID: C-Edge | Mode: Master
BSSID: F4:CE:23:BB:39:6A | Encryption: WPA2 PSK (CCMP)

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate
Master "C-Edge" (wlan0)	AA:4C:1E:89:04:54	MacBookPro (192.168.11.129, fe80::14cd:6d2b:541c:94b1)	-35 dBm	24.0 Mbit/s, 20 MHz 144.4 Mbit/s, 20 MHz, MCS 15, Short GI



Interface Configuration

General Setup | Wireless Security | MAC-Filter | Advanced Settings

Mode: Access Point

ESSID: C-Edge

Network: lan:

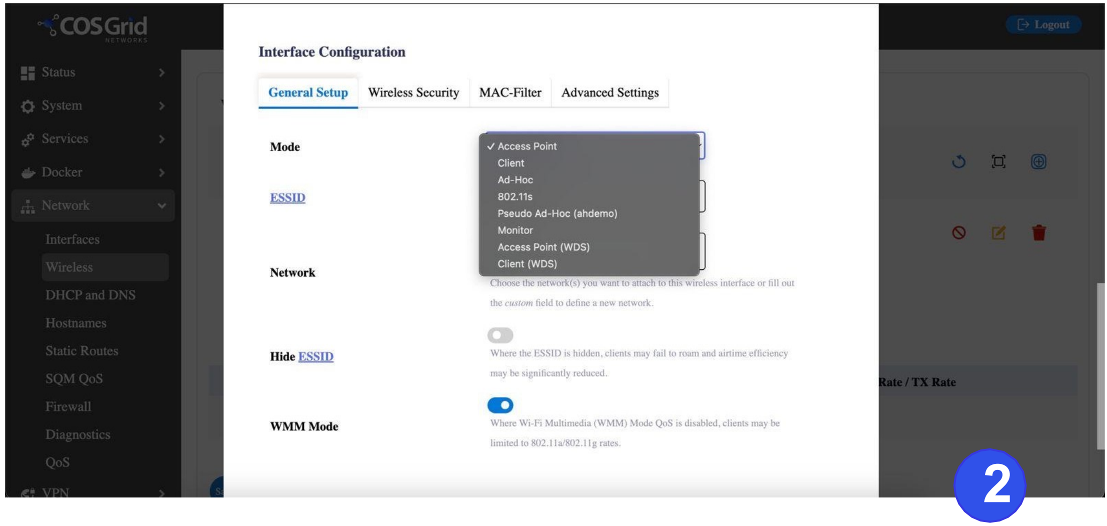
Choose the network(s) you want to attach to this wireless interface or fill out the *custom* field to define a new network.

Hide ESSID

Where the ESSID is hidden, clients may fail to roam and airtime efficiency may be significantly reduced.

WMM Mode

Where Wi-Fi Multimedia (WMM) Mode QoS is disabled, clients may be limited to 802.11a/802.11g rates.



Interface Configuration

General Setup | Wireless Security | MAC-Filter | Advanced Settings

Mode

ESSID

Network

Choose the network(s) you want to attach to this wireless interface or fill out the *custom* field to define a new network.

Hide ESSID

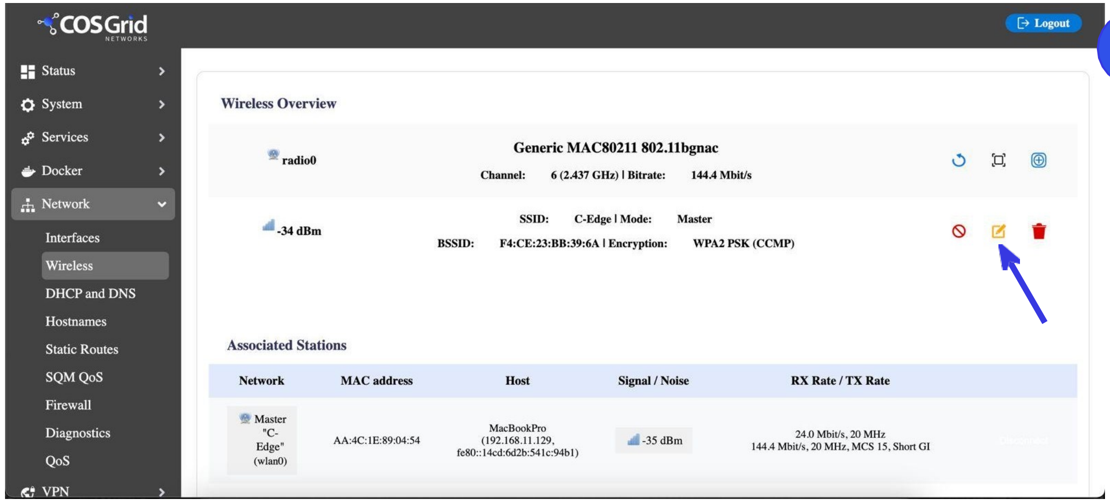
Where the ESSID is hidden, clients may fail to roam and airtime efficiency may be significantly reduced.

WMM Mode

Where Wi-Fi Multimedia (WMM) Mode QoS is disabled, clients may be limited to 802.11a/802.11g rates.

WiFi Client & Security

Set Steps	Acceptance Criteria
In Side Bar ***Network > Wireless.***	Both options for configuring a network manually and scanning networks should be there.
Select Client Mode. Confirm the settings for **SSID, security protocols (WPA2, WPA3).**	WiFi Security : WPA X /WEP/ TKIP variants as per the latest version.
Check the Internet Connection. **You can do a ping test**. Go to ***Network > Diagnostics.***	You should be able to ping any running website.



Wireless Overview

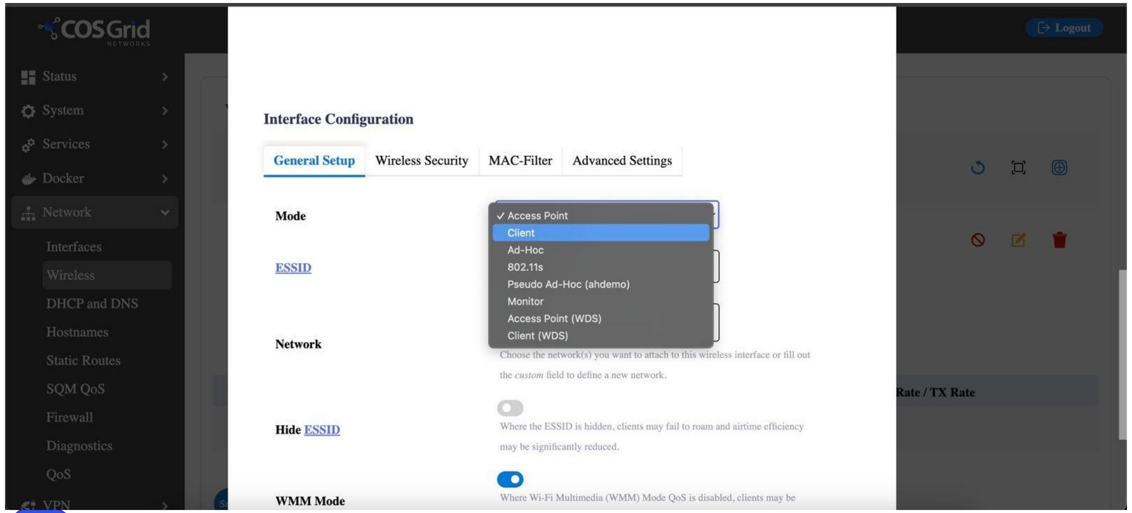
radio0 Generic MAC80211 802.11bgnac
Channel: 6 (2.437 GHz) | Bitrate: 144.4 Mbit/s

-34 dBm SSID: C-Edge | Mode: Master
BSSID: F4:CE:23:BB:39:6A | Encryption: WPA2 PSK (CCMP)

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate
Master "C-Edge" (wlan0)	AA:4C:1E:89:04:54	MacBookPro (192.168.11.129, fe80::14cd:6d2b:541c:94b1)	-35 dBm	24.0 Mbit/s, 20 MHz 144.4 Mbit/s, 20 MHz, MCS 15, Short GI

1



Interface Configuration

General Setup | Wireless Security | MAC-Filter | Advanced Settings

Mode: ✓ Access Point / Client / Ad-Hoc / 802.11s / Pseudo Ad-Hoc (ahdemo) / Monitor / Access Point (WDS) / Client (WDS)

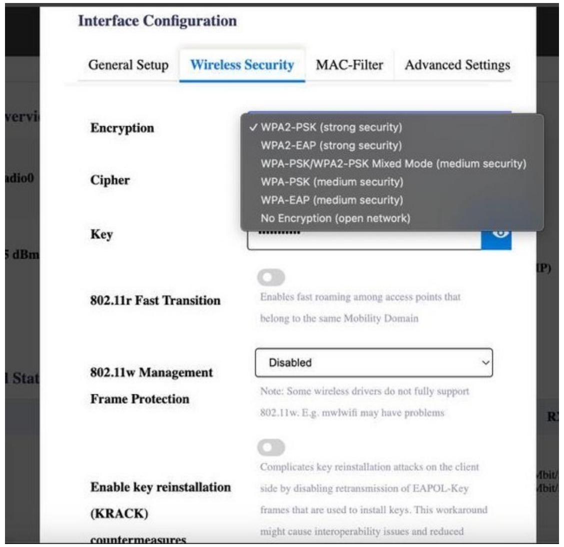
ESSID

Network: Choose the network(s) you want to attach to this wireless interface or fill out the *custom* field to define a new network.

Hide ESSID: Where the ESSID is hidden, clients may fail to roam and airtime efficiency may be significantly reduced.

WMM Mode: Where Wi-Fi Multimedia (WMM) Mode QoS is disabled, clients may be

2



Interface Configuration

General Setup | Wireless Security | MAC-Filter | Advanced Settings

Encryption: ✓ WPA2-PSK (strong security) / WPA2-EAP (strong security) / WPA-PSK/WPA2-PSK Mixed Mode (medium security) / WPA-PSK (medium security) / WPA-EAP (medium security) / No Encryption (open network)

Cipher

Key: ....

802.11r Fast Transition: Enables fast roaming among access points that belong to the same Mobility Domain

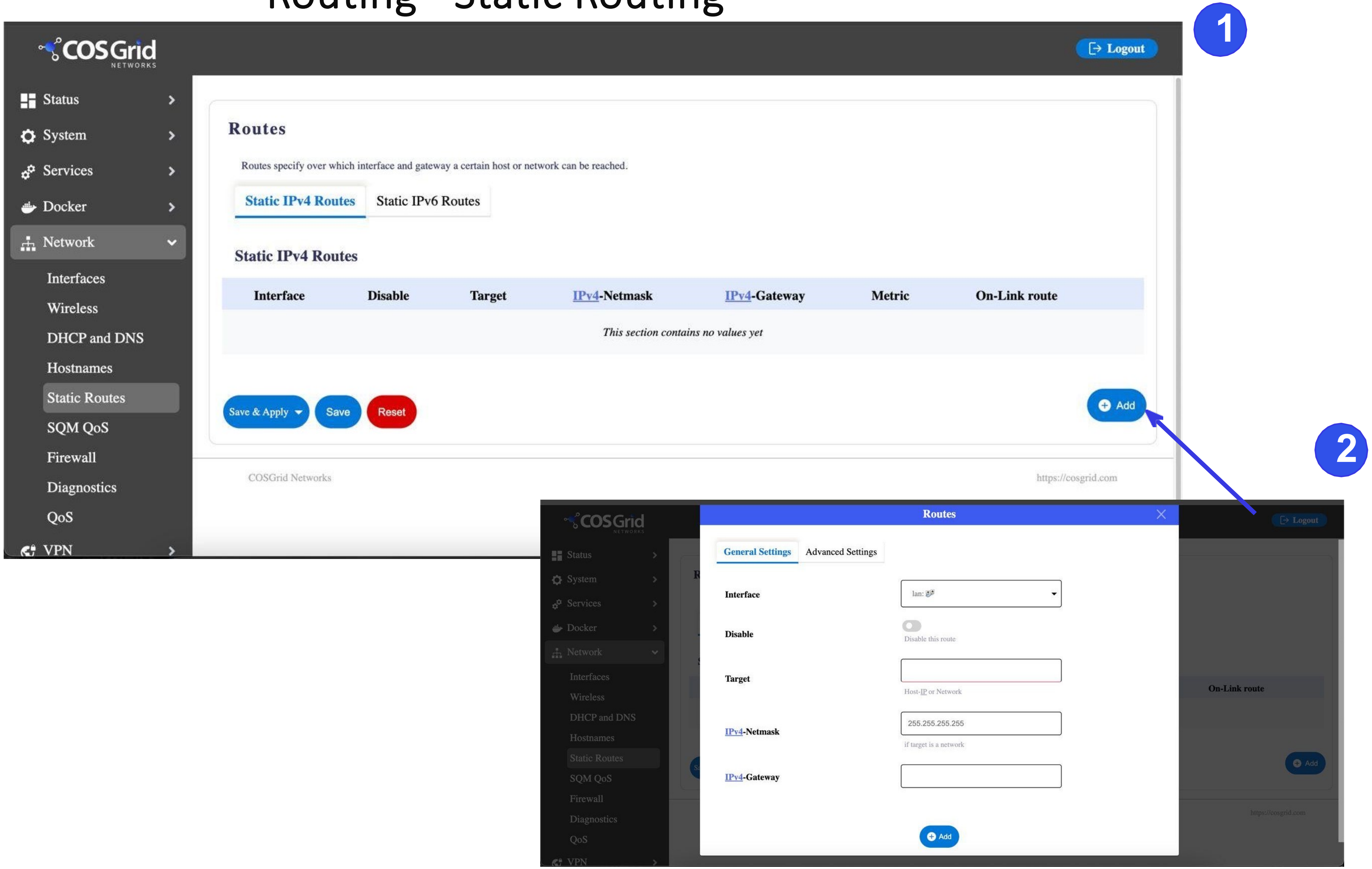
802.11w Management Frame Protection: Disabled
Note: Some wireless drivers do not fully support 802.11w. E.g. mwlwifi may have problems

Enable key reinstallation (KRACK) countermeasures: Complicates key reinstallation attacks on the client side by disabling retransmission of EAPOL-Key frames that are used to install keys. This workaround might cause interoperability issues and reduced

3

Routing - Static Routing

Set Steps	Acceptance Criteria
Go to ***Network > Static Routes.*** Test the implementation of static routing. Figure:7	Options to add **Target, Netmask** etc. should be there.
Configure a Route by adding your desired Target and Gateway.	Should be able to see the route configuration in the table. **Note** : *Rouīe will work or noī will depend on your configuraīion.*

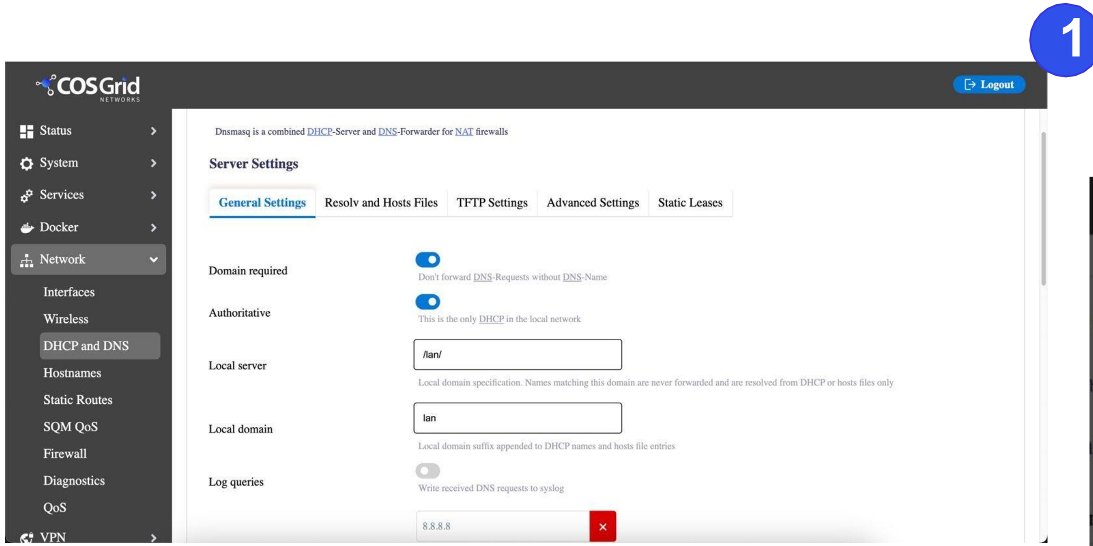


Routes specify over which interface and gateway a certain host or network can be reached.

This section contains no values yet

DHCP - Static and dynamic IP allocation

Set Steps	Acceptance Criteria
Go to ***Network > DHCP and DNS.*** Test the ability to define DHCP and DNS parameters. Figure:8	The configuration should work for all the devices connected.
Go to ***Network > DHCP and DNS. Under the Static Leases Tab,*** Verify leases creation. Figure:9	A lease should be assigned to every device that is connected.
Under the Static Leases Tab. Verify that devices successfully renew their IP addresses as leases expire.	After the mentioned Lease time the device lease should be renewed.



Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

Domain required: on — Don't forward DNS-Requests without DNS-Name

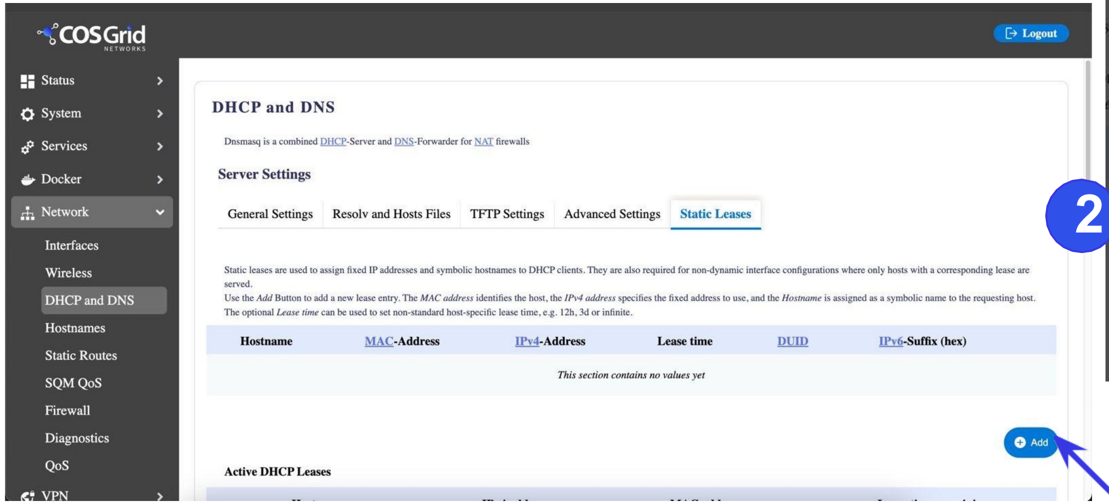
Authoritative: on — This is the only DHCP in the local network

Local server: /lan/ — Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only

Local domain: lan — Local domain suffix appended to DHCP names and hosts file entries

Log queries: off — Write received DNS requests to syslog

8.8.8.8



DHCP and DNS

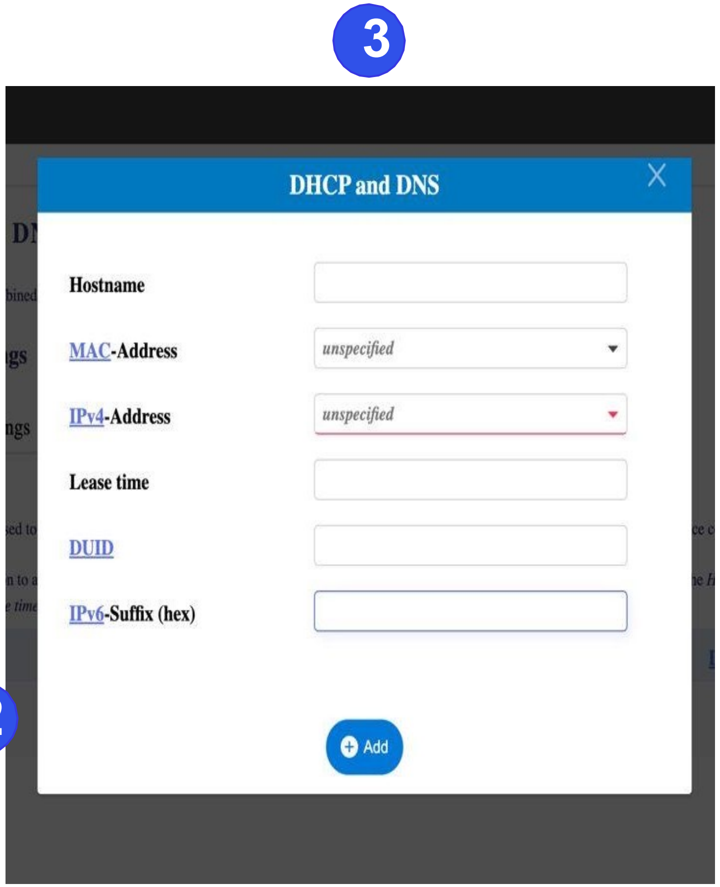
Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the *Add* Button to add a new lease entry. The *MAC address* identifies the host, the *IPv4 address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	DUID	IPv6-Suffix (hex)
This section contains no values yet					

Active DHCP Leases

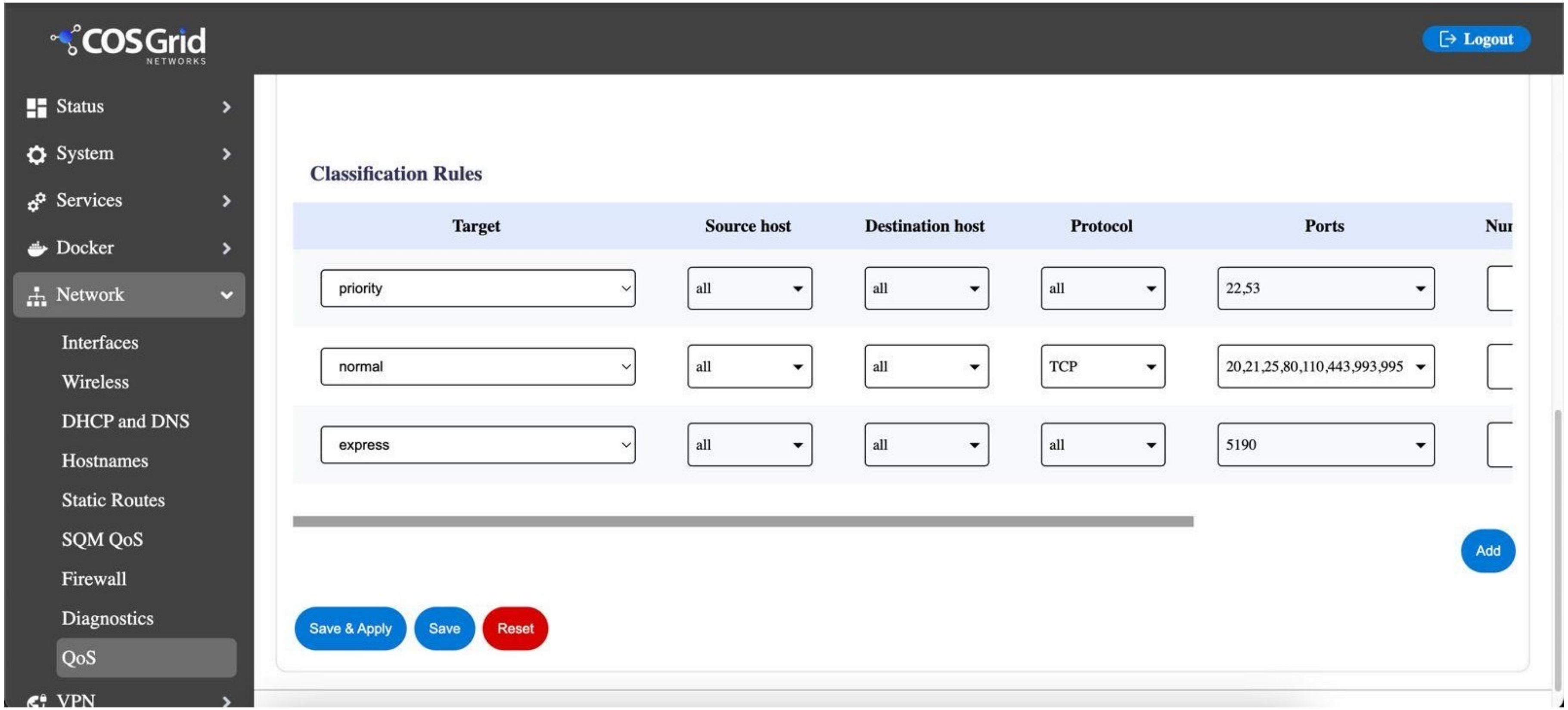


DHCP and DNS

Hostname	
MAC-Address	unspecified
IPv4-Address	unspecified
Lease time	
DUID	
IPv6-Suffix (hex)	

Qos Policies

Set Steps	Acceptance Criteria
Go to ***Network > QoS.*** Test the ability to define and modify QoS policies.	You should be able to add a rule.
Test the allocation of bandwidth to different classes of traffic.	After refreshing the bandwidth configuration should be shown.

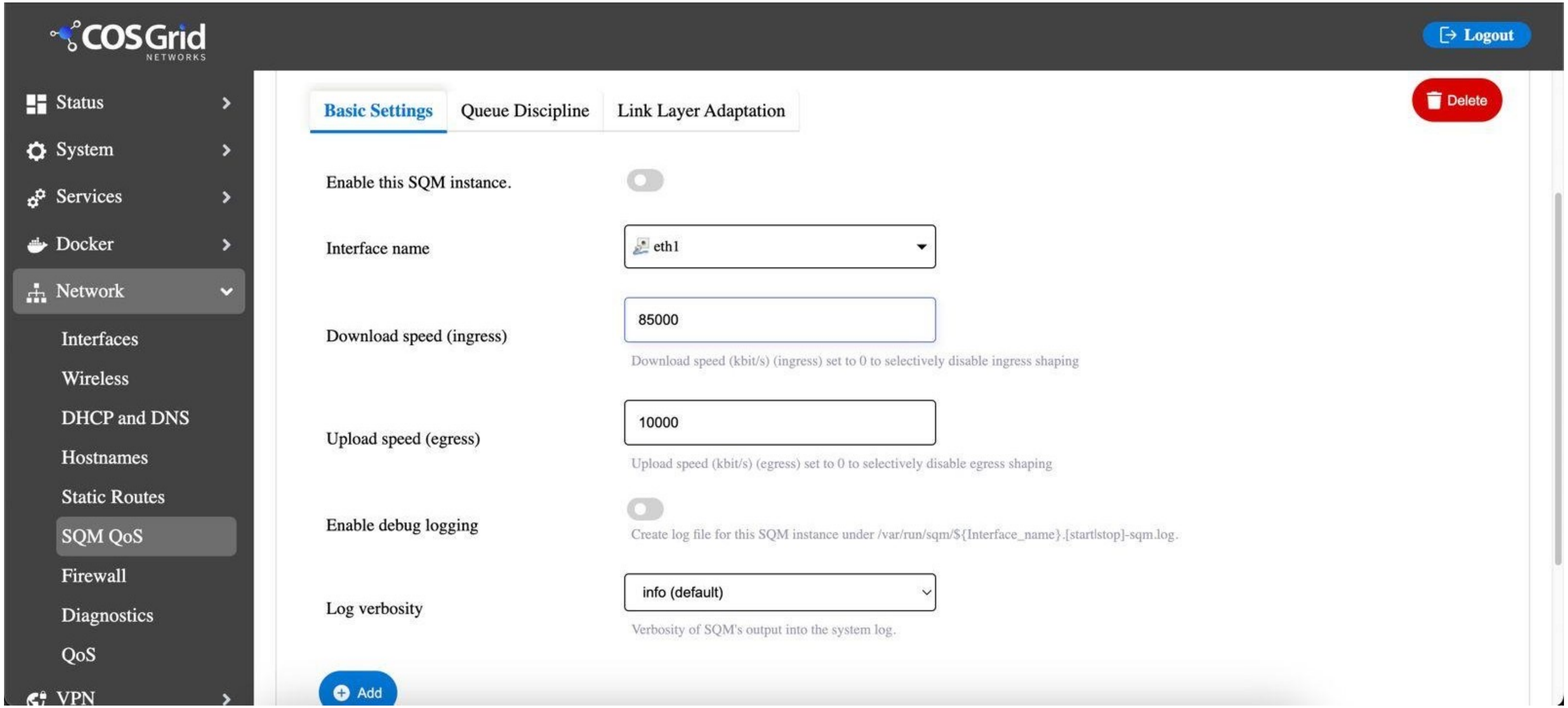


Classification Rules

Target	Source host	Destination host	Protocol	Ports	Nur
priority	all	all	all	22,53	
normal	all	all	TCP	20,21,25,80,110,443,993,995	
express	all	all	all	5190	

Custom Limit for SIM Card

Set Steps	Acceptance Criteria
Go to ***Network > SQM QoS.*** Test the ability to define and modify Queues.	Options of Download and Upload Speed should be mentioned.
Test the allocation of bandwidth to different classes of traffic.	After refreshing the bandwidth configuration should be shown.



Enable this SQM instance.

Interface name: eth1

Download speed (ingress): 85000

Download speed (kbit/s) (ingress) set to 0 to selectively disable ingress shaping

Upload speed (egress): 10000

Upload speed (kbit/s) (egress) set to 0 to selectively disable egress shaping

Enable debug logging

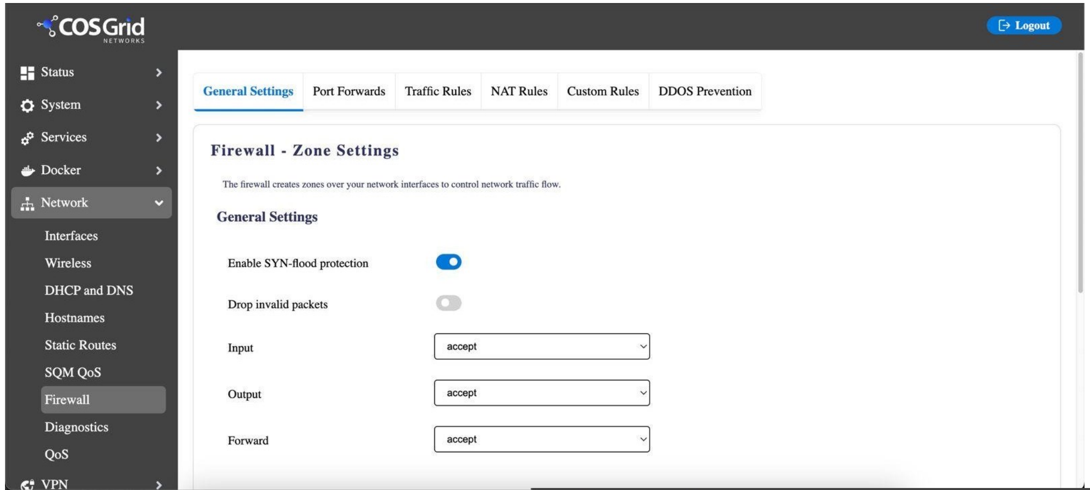
Create log file for this SQM instance under /var/run/sqm/${Interface_name}.[start|stop]-sqm.log.

Log verbosity: info (default)

Verbosity of SQM's output into the system log.

Firewall

Set Steps	Acceptance Criteria
Go to ***Network > Firewall.*** Test the ability of the firewall to filter incoming and outgoing traffic **based on zone**.	After saving a zone configuration, it should be shown in the table.

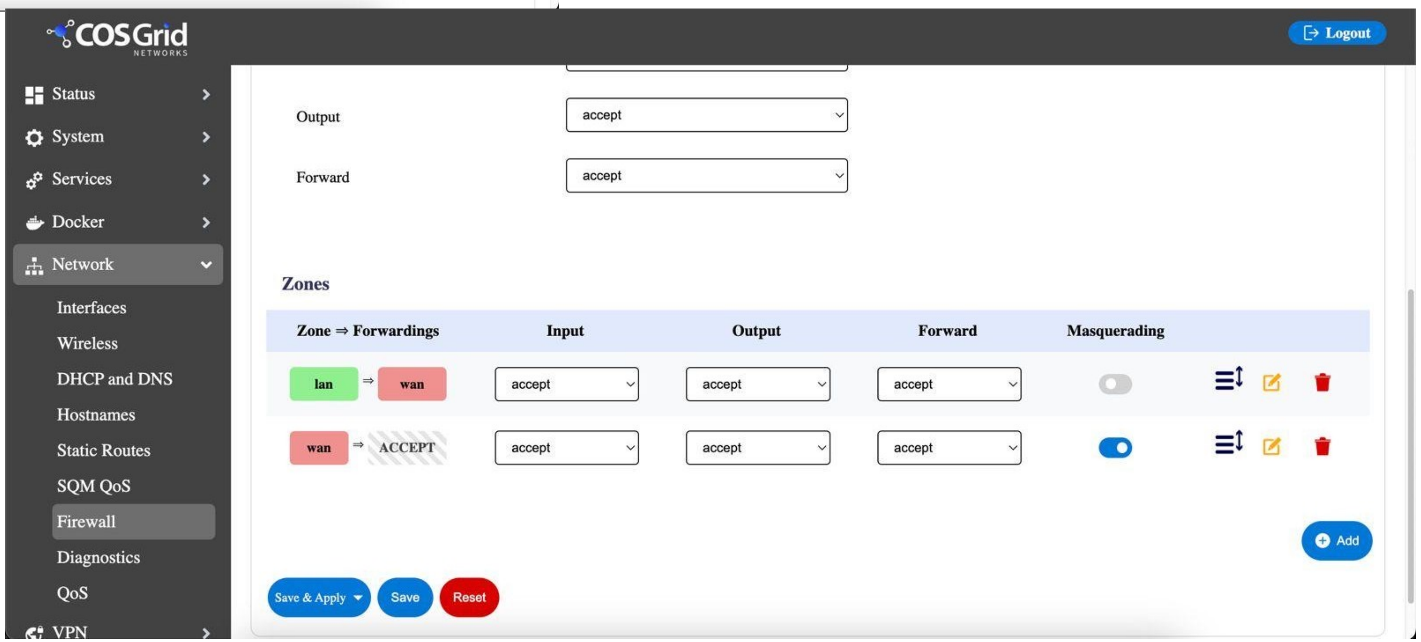


Firewall - Zone Settings

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
Forward	accept



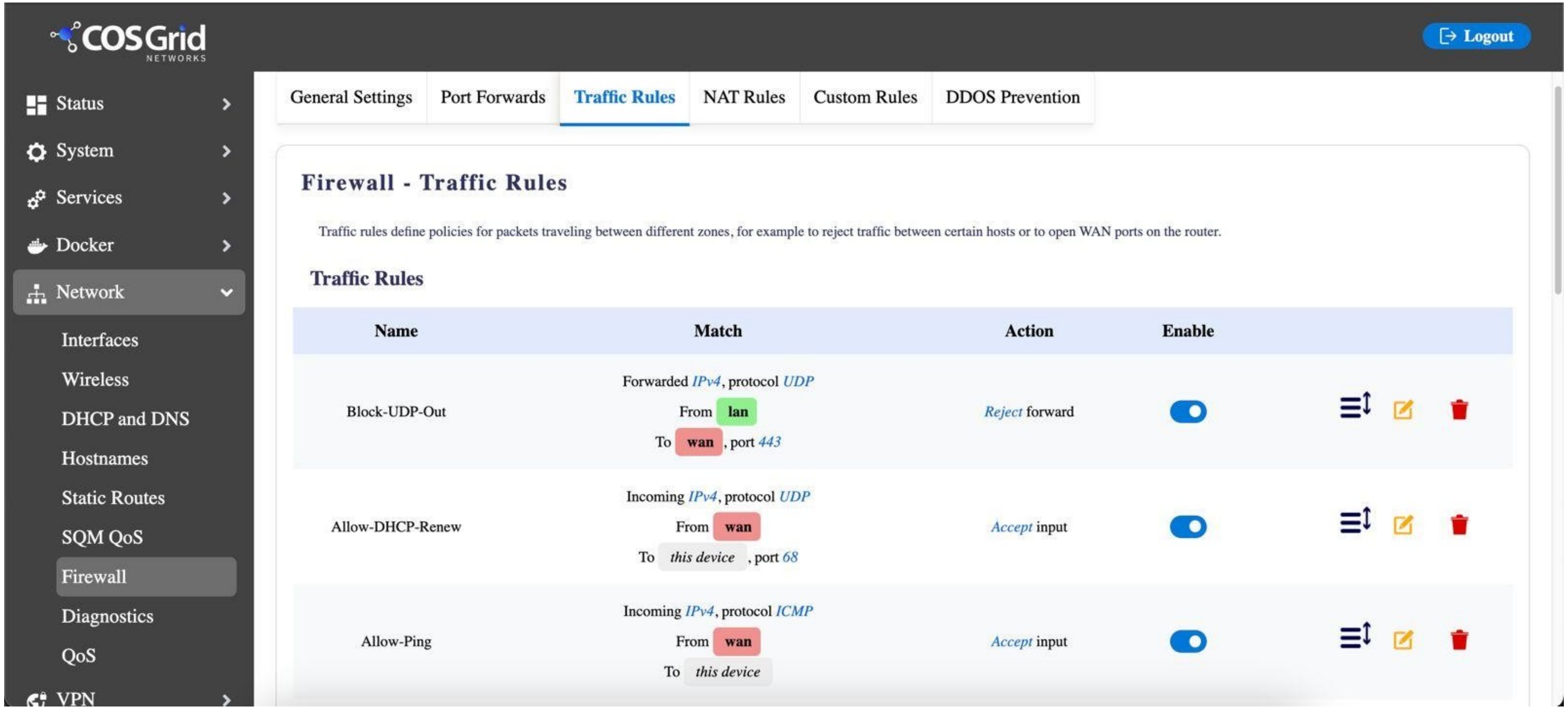
Output	accept
Forward	accept

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading
lan ⇒ wan	accept	accept	accept	○
wan ⇒ ACCEPT	accept	accept	accept	●

Firewall - Traffic Rules

Set Steps	Acceptance Criteria
Go to ***Network > Firewall, Under Traffic Rules tab.*** You should be able to add a traffic rule using below Add button based on **source address and destination address**.	Now the rule should be displayed in the table also.



Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

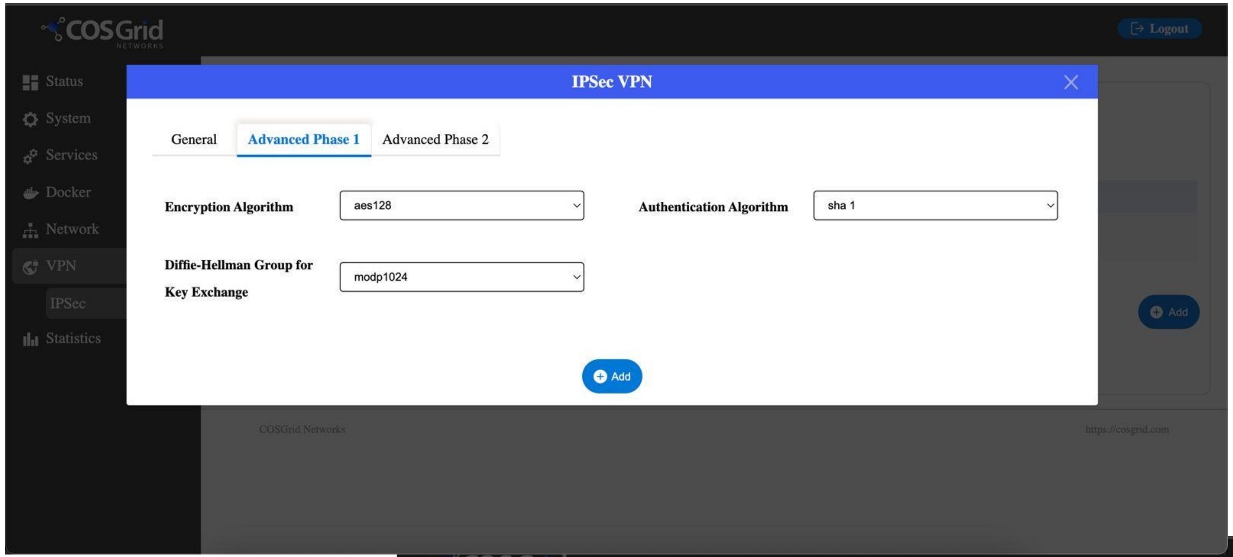
Traffic Rules

Name	Match	Action	Enable
Block-UDP-Out	Forwarded *IPv4*, protocol *UDP* From lan To wan, port *443*	*Reject* forward	●
Allow-DHCP-Renew	Incoming *IPv4*, protocol *UDP* From wan To *this device*, port *68*	*Accept* input	●
Allow-Ping	Incoming *IPv4*, protocol *ICMP* From wan To *this device*	*Accept* input	●

IPSec

Set Steps	Acceptance Criteria
Go to ***VPN > IPsec.*** Try to add a tunnel with customized encryption algorithms under ***Advanced Phase 1/2 tab***.	Supports different AES/DES encryption methods.

3

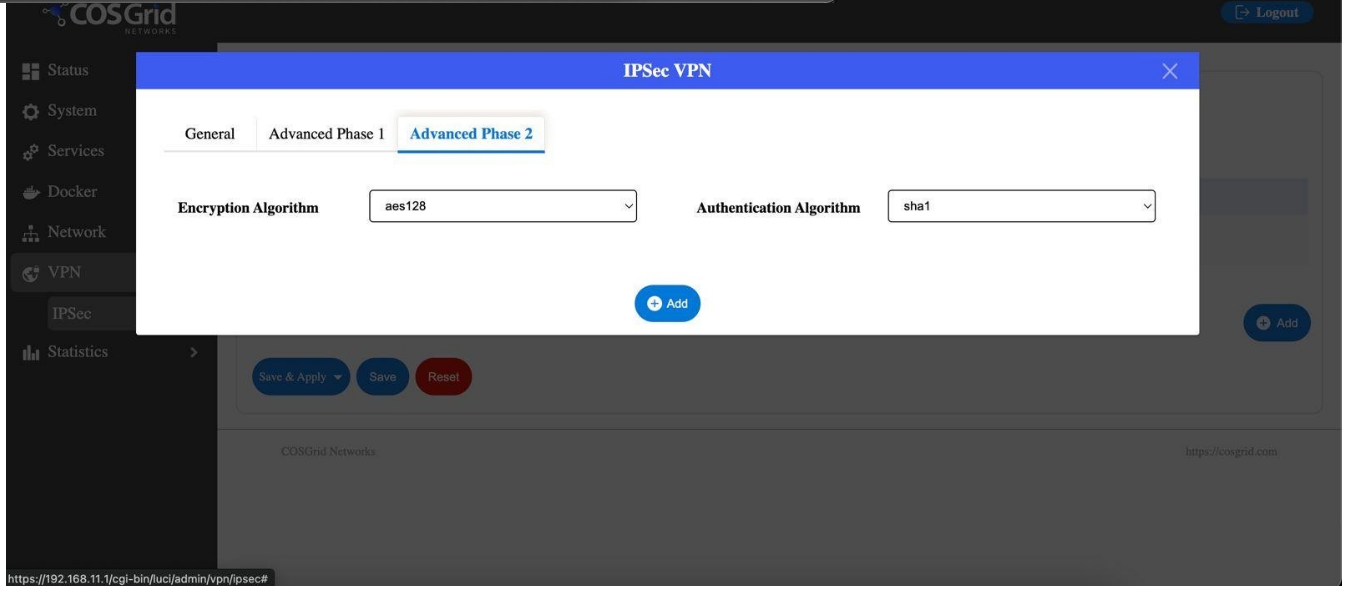


Encryption Algorithm: aes128

Authentication Algorithm: sha 1

Diffie-Hellman Group for Key Exchange: modp1024

4

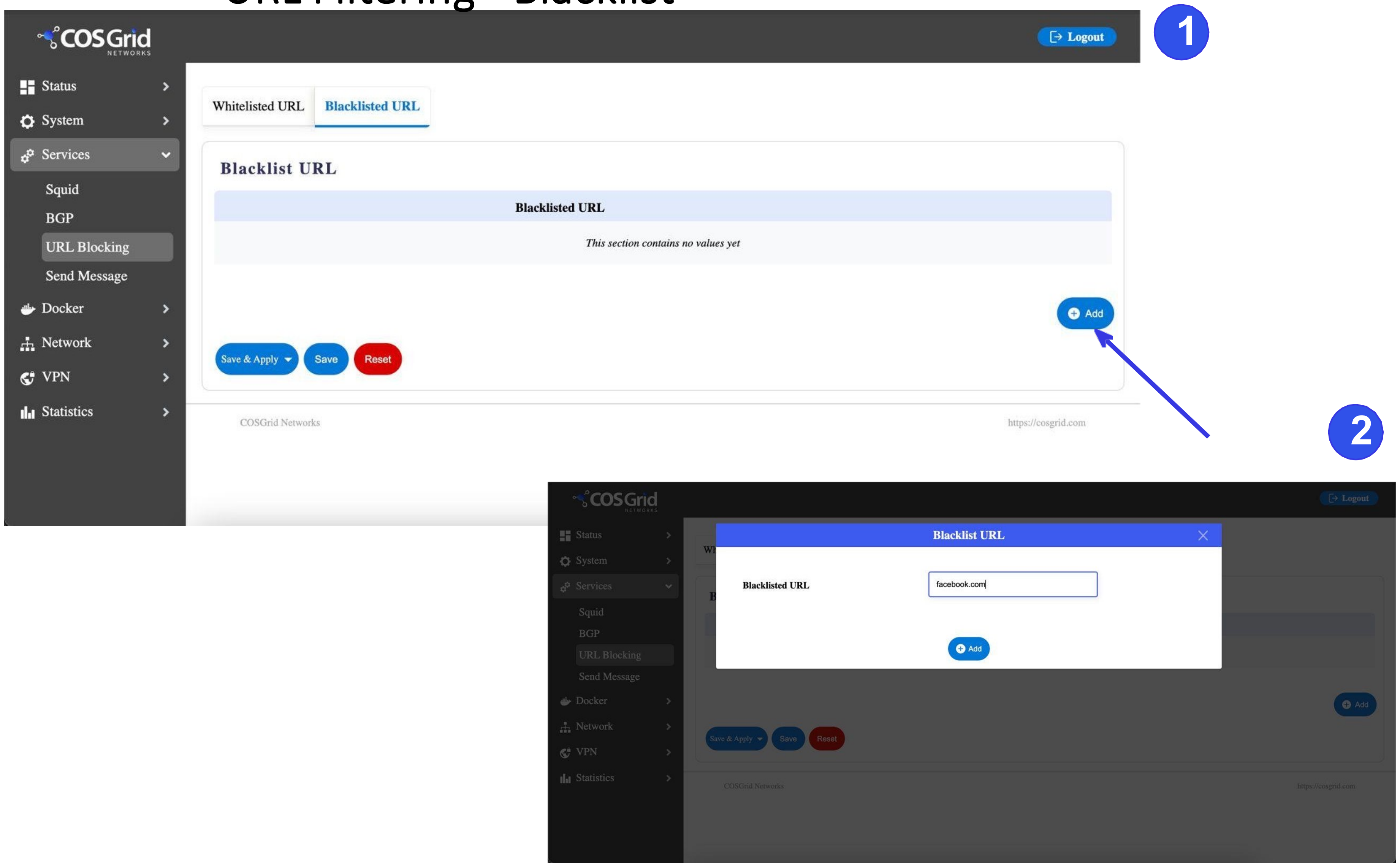


Encryption Algorithm: aes128

Authentication Algorithm: sha1

URL Filtering - Blacklist

Set Steps	Acceptance Criteria
Go to ***Services > URL Blocking. Under the Blacklist Url tab,*** Test the ability to configure blacklist websites.	Blacklist for specifying blocked sites only



Blacklist URL

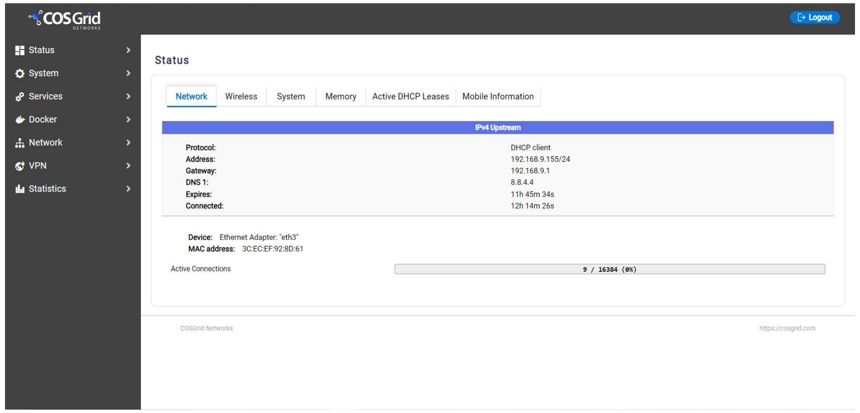
Blacklisted URL
This section contains no values yet

Blacklist URL

Blacklisted URL: facebook.com

Status Overview & Diagnostics

Set Steps	Acceptance Criteria
Go to ***Status > Overview. Under the Network tab,*** Verify that network interfaces are correctly identified and displayed in the status overview. Figure:24	Status should contain proper parameters to define it.
Go to ***Status > Overview. Under the Memory,*** Verify the memory status. Figure:25	Visibility of critical system parameters such as CPU usage, memory utilization, and storage capacity.
Go to ***Network > Diagnostics*** Test tools such as ping, traceroute. Figure:26	Ensure they provide meaningful result



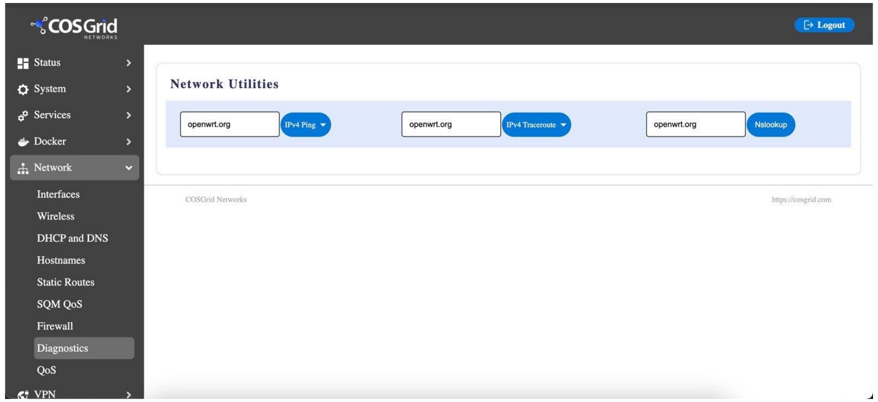
Status

Protocol:	DHCP client
Address:	192.168.9.155/24
Gateway:	192.168.9.1
DNS 1:	8.8.4.4
Expires:	11h 45m 34s
Connected:	12h 14m 26s

Device: Ethernet Adapter: "eth3"
MAC address: 3C:EC:EF:92:8D:61

Active Connections 9 / 16384 (0%)

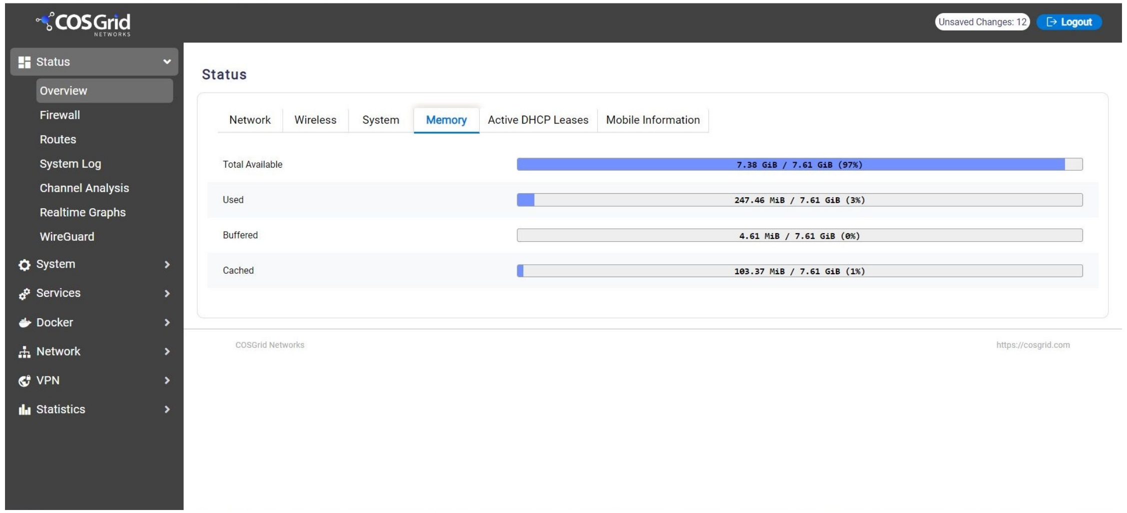
COSGrid Networks https://cosgrid.com



Network Utilities

openwrt.org IPv4 Ping openwrt.org IPv4 Traceroute openwrt.org Nslookup

COSGrid Networks https://cosgrid.com



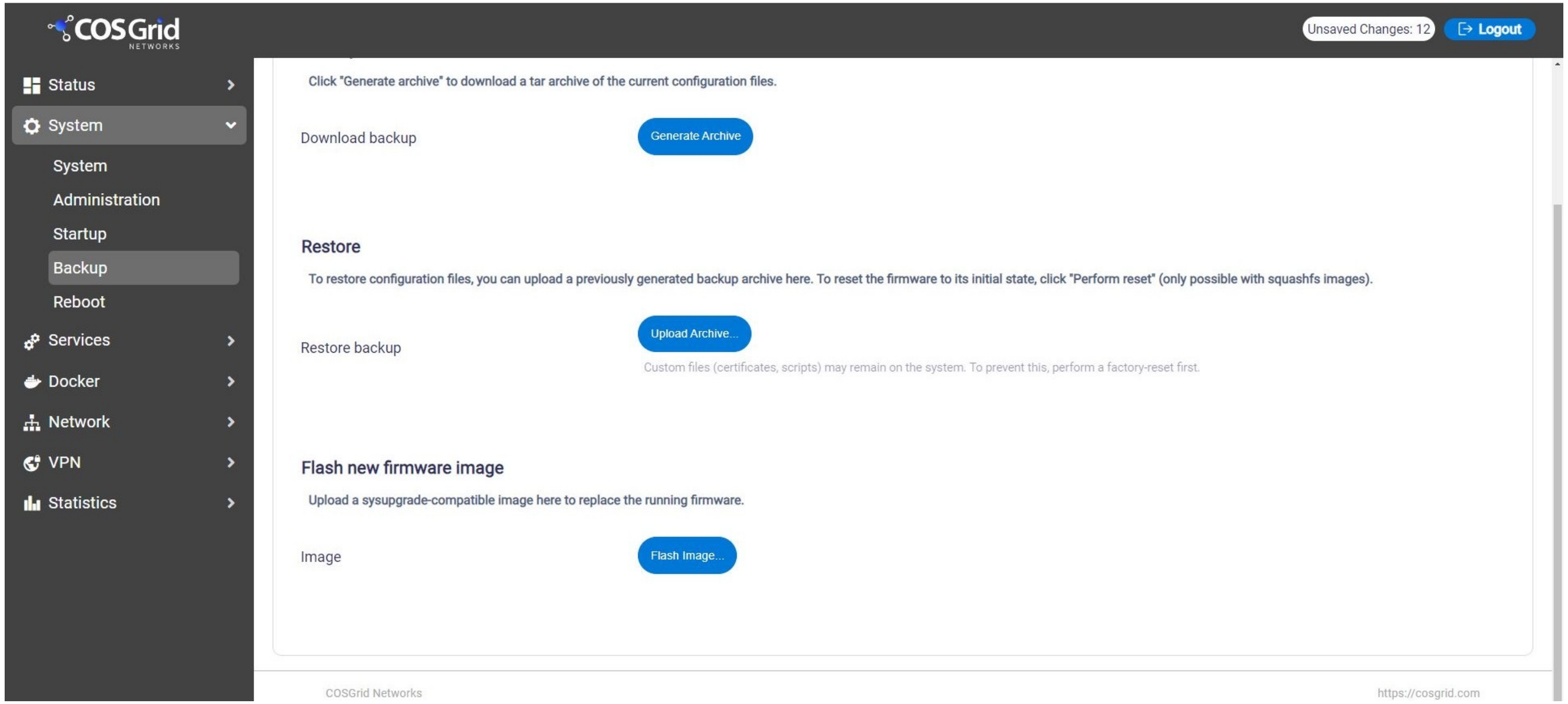
Status

Total Available	7.38 GiB / 7.61 GiB (97%)
Used	247.46 MiB / 7.61 GiB (3%)
Buffered	4.61 MiB / 7.61 GiB (0%)
Cached	103.37 MiB / 7.61 GiB (1%)

COSGrid Networks https://cosgrid.com

Firmware

Set Steps	Acceptance Criteria
Go to ***System > Backup*** Verify that the IoT gateway provides functions to add a firmware image available.	Options to add the firmware image should be there. Note : Image should be **sysupgrade-compatible**



Click "Generate archive" to download a tar archive of the current configuration files.

Download backup — Generate Archive

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Restore backup — Upload Archive...

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware.

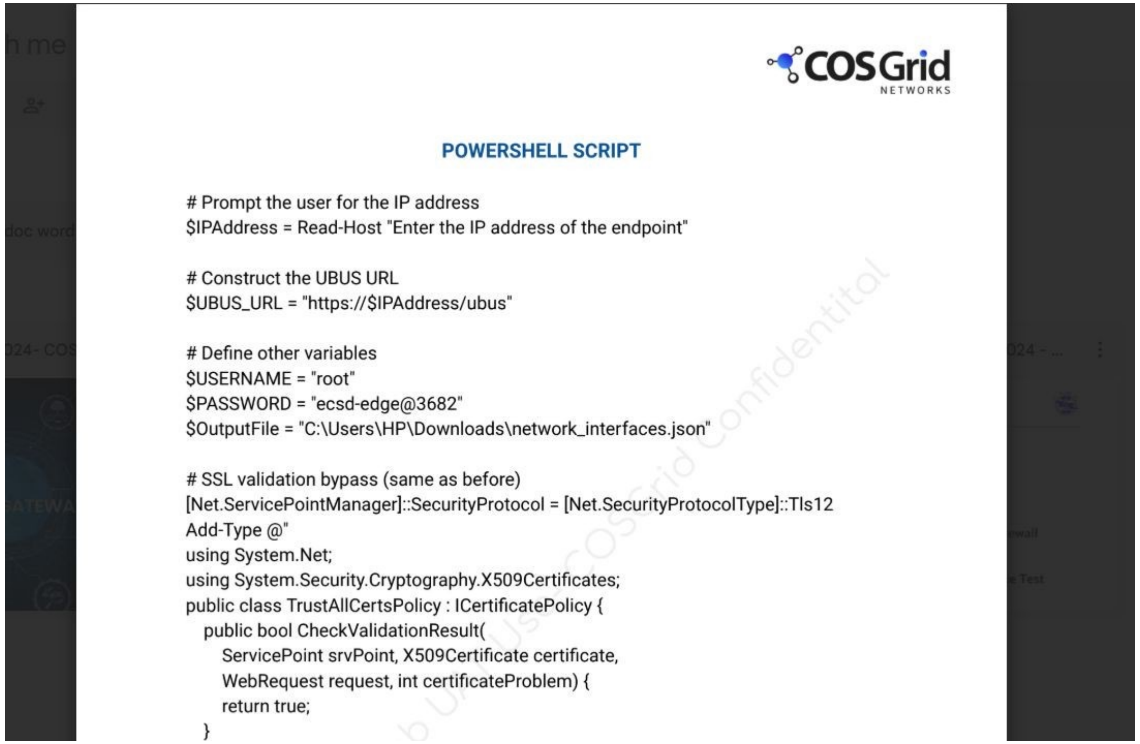
Image — Flash Image...

COSGrid Networks https://cosgrid.com

Management API using HTTP/HTTPS

- Open Powershell & Type the Script given in this document

https://drive.google.com/file/d/1zRWBkswGVhkkIZGlUSO_KeKpbAGaLFOG/view?usp=drive_link



POWERSHELL SCRIPT

```
# Prompt the user for the IP address
$IPAddress = Read-Host "Enter the IP address of the endpoint"

# Construct the UBUS URL
$UBUS_URL = "https://$IPAddress/ubus"

# Define other variables
$USERNAME = "root"
$PASSWORD = "ecsd-edge@3682"
$OutputFile = "C:\Users\HP\Downloads\network_interfaces.json"

# SSL validation bypass (same as before)
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Add-Type @"
using System.Net;
using System.Security.Cryptography.X509Certificates;
public class TrustAllCertsPolicy : ICertificatePolicy {
  public bool CheckValidationResult(
    ServicePoint srvPoint, X509Certificate certificate,
    WebRequest request, int certificateProblem) {
    return true;
  }
```

AI/ML & IoT in 5G:

Applications & Integration

Contents

- Overview Of AI/ML Techniques
- AI/ML Applications For 5G
- IoT Technology Overview
- IoT Use-Cases & Deployment Scenarios
    - Coral Gyan Data on NMS:
- Integration Of IoT in 3GPP Standards Framework
- 5G Labs & Emerging Technology

Overview of AI/ML Techniques

- Artificial Intelligence (AI) and Machine Learning (ML) have revolutionized various industries by enabling machines to learn from data, recognize patterns, and make intelligent decisions. These technologies are extensively used to enhance automation, optimize decision-making, and drive innovation. Key AI/ML techniques include:

Overview of AI/ML Techniques

- **Supervised Learning**: A technique where a model learns from a dataset containing input-output pairs. The algorithm uses labeled examples to learn the mapping function between inputs (features) and outputs (labels). It is widely used in classification (e.g., spam detection, image recognition) and regression tasks (e.g., predicting house prices, stock prices). Popular algorithms include Decision Trees, Support Vector Machines (SVMs), and Neural Networks.

- **Unsupervised Learning**: Works with unlabeled data, meaning the algorithm tries to find hidden patterns, relationships, or structures without predefined categories. Clustering techniques such as **K-Means, DBSCAN, and Hierarchical Clustering** group similar data points, while **dimensionality reduction techniques like PCA (Principal Component Analysis) and t-SNE** help in feature extraction and visualization of high-dimensional data. Applications include customer segmentation, anomaly detection, and recommendation systems.

Overview of AI/ML Techniques

- **Reinforcement Learning (RL)**: A decision-making framework where an agent interacts with an environment and learns by receiving rewards or penalties. The agent takes actions to maximize cumulative rewards over time. RL algorithms like **Q-Learning, Deep Q Networks (DQN), and Proximal Policy Optimization (PPO)** are widely used in **robotic control (robotic arms, drones), autonomous navigation (self-driving cars), gaming (AlphaGo, Dota 2 AI), and finance (automated trading strategies).**
- **Deep Learning**: A subset of ML that leverages **artificial neural networks (ANNs)**, particularly **deep neural networks (DNNs)** with multiple layers. These models can automatically extract features from raw data, making them highly effective for **image processing (CNNs - Convolutional Neural Networks), speech recognition (WaveNet, DeepSpeech), and natural language processing (RNNs, Transformers like GPT and BERT).** Deep learning powers applications such as **self-driving cars, facial recognition, voice assistants (Siri, Alexa), and automated translation (Google Translate).**

Overview of AI/ML Techniques

- **Federated Learning**: A privacy-focused machine learning technique where models are trained across multiple devices (e.g., smartphones, edge devices) without transferring raw data to a central server. Instead, the model is updated locally and only sends learned insights back to the global model. This approach enhances **data privacy, reduces bandwidth usage, and allows AI models to be trained across decentralized networks**. It is widely used in **healthcare (collaborative medical research), finance (fraud detection), and mobile applications (personalized keyboards, predictive text on smartphones).**

AI/ML Applications for 5G

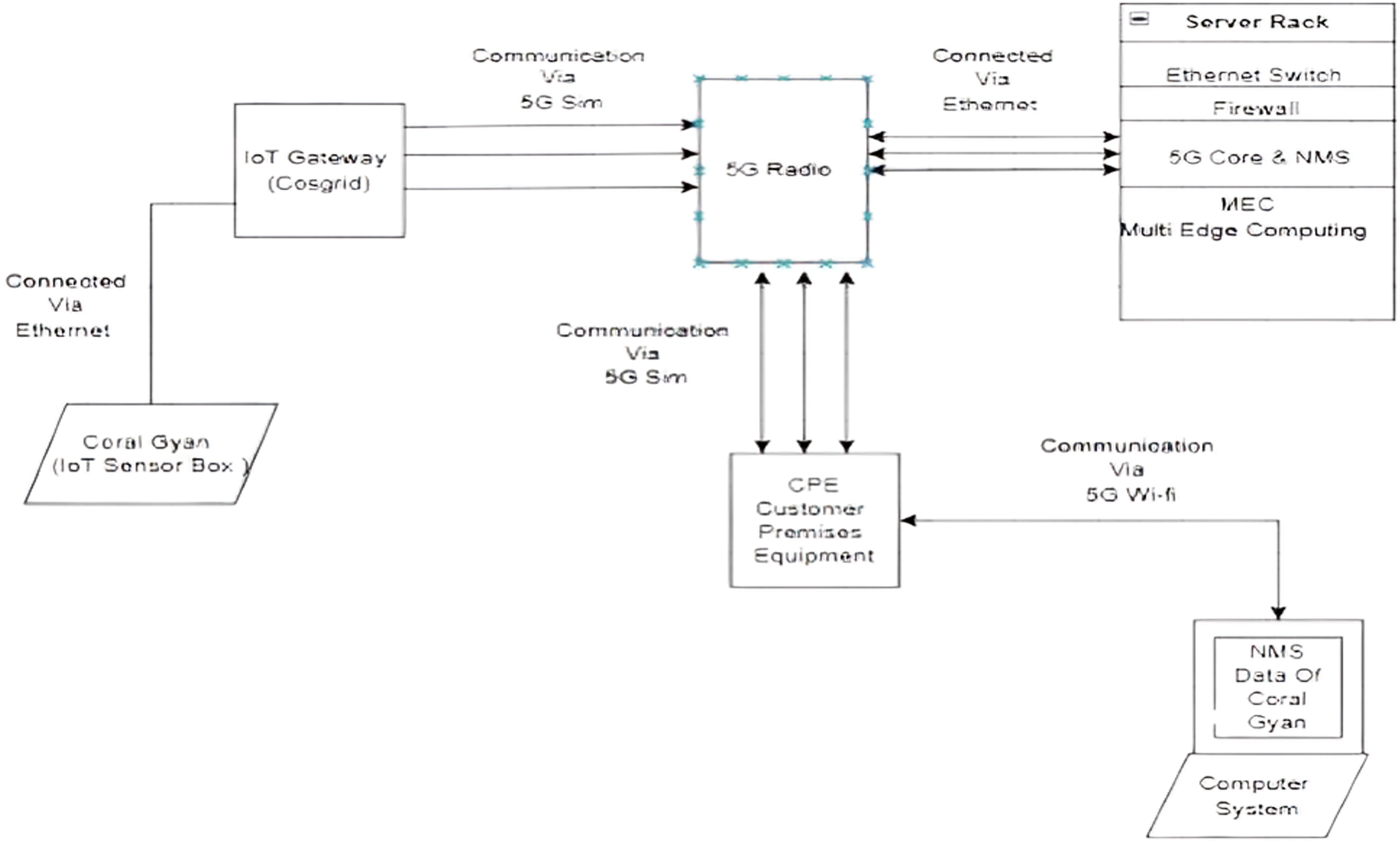
- The integration of AI/ML in 5G networks enhances performance, efficiency, and automation. Some key applications include:
  - **Network Optimization:** AI-powered algorithms optimize network resources, reduce latency, and improve bandwidth utilization by analyzing real-time traffic patterns.
  - **Predictive Maintenance:** ML models predict hardware failures and network outages, ensuring proactive maintenance and reducing downtime.
  - **Dynamic Spectrum Allocation:** AI optimizes frequency spectrum usage based on demand and interference conditions, enhancing spectrum efficiency.
  - **Autonomous Network Management:** AI-driven self-organizing networks (SONs) dynamically adjust network configurations to optimize coverage and capacity.
  - **Security Enhancements:** AI detects and mitigates cyber threats, unauthorized access, and anomalous network behaviors, strengthening network security.
  - **5G Edge Computing/MEC:** AI/ML enhances edge computing by processing data closer to the source, reducing latency for applications like autonomous vehicles and smart factories.
  - **AR/VR and 5G Camera:** In the 5G Lab, AI-driven AR/VR applications and 5G-enabled cameras with face and fire detection utilize Multi-Access Edge Computing (MEC) for low-latency processing and real-time analytics.

IoT Technology Overview

- The Internet of Things (IoT) refers to a network of interconnected devices that collect, analyze, and exchange data. IoT technology enables smart automation and real-time decision-making across various industries. Key components of IoT include:
  - Sensors and Actuators: Devices that collect real-world data (e.g., temperature, motion) and perform actions based on analysis. The Coral Gyan IoT Sensor Box, used in the 5G Lab, includes sensors like NPK, LDR, Temperature & Humidity, and Soil Monitoring for environmental analysis.
  - Connectivity Protocols: IoT devices use protocols such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and 5G for seamless communication.
  - Edge Computing & MEC: Processes data closer to the source, reducing latency and enhancing efficiency. MEC in the 5G Lab supports real-time data analysis from IoT sensors, AR/VR applications, and 5G cameras.
  - AI and Big Data Analytics: Extracts insights from IoT-generated data, enabling predictive analytics and automation.

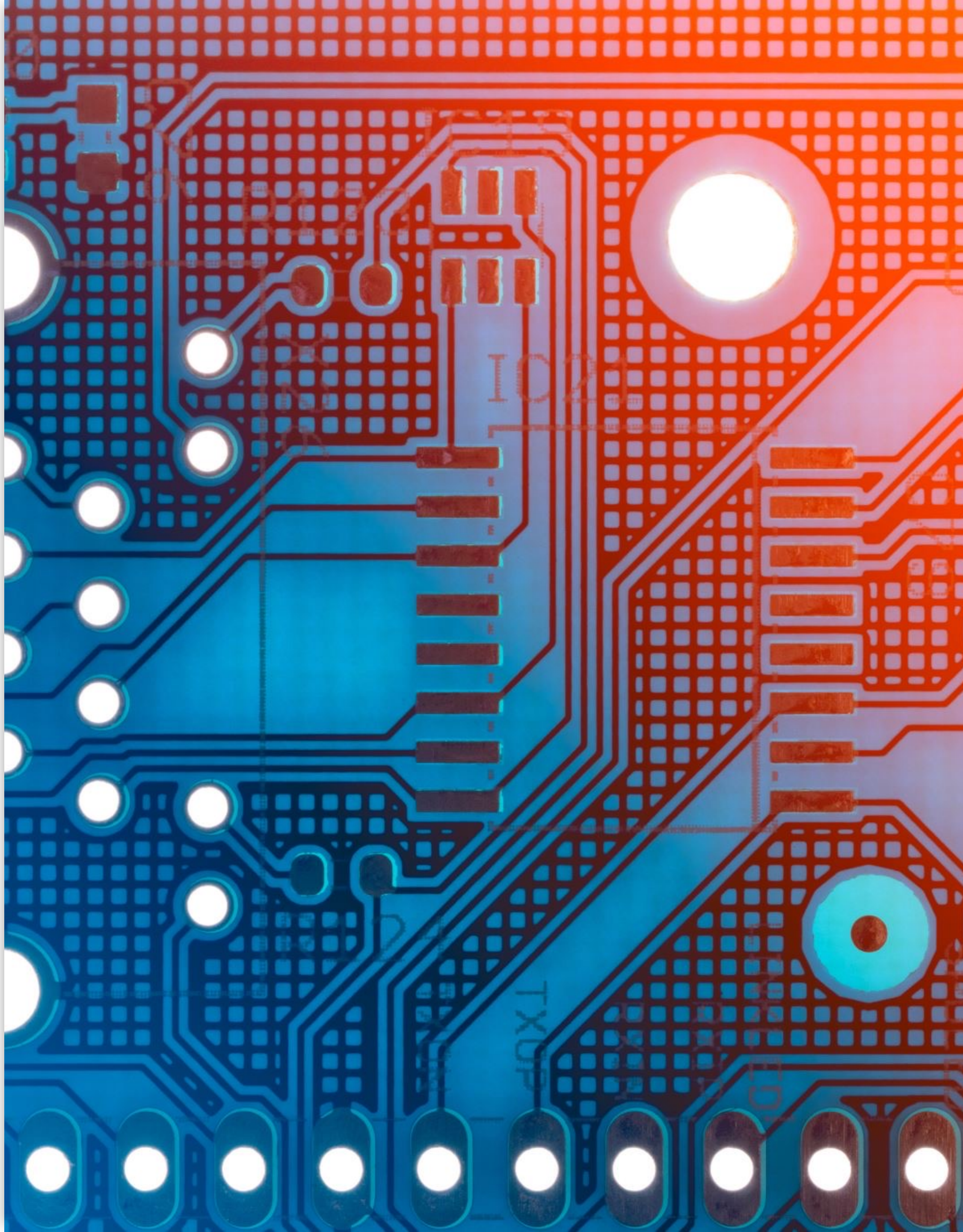
IoT Use-Cases and Deployment Scenarios

- IoT is widely adopted across various sectors with multiple deployment scenarios, including:
  - **Smart Cities:** IoT enables smart lighting, traffic management, waste management, and surveillance systems to improve urban living conditions. **5G-enabled smart cameras and IoT sensor boxes** enhance security and environmental monitoring.
  - **Agriculture:** IoT-driven precision farming optimizes irrigation, soil monitoring, and livestock tracking, leading to higher crop yields. **The IoT Sensor Box (Coral Gyan) plays a crucial role in monitoring soil quality and environmental factors.**
  - **Smart Homes:** Home automation systems manage lighting, security, and appliances, improving convenience and energy efficiency. AI-powered 5G cameras ensure real-time security monitoring.
  - **Automotive and Transportation:** IoT powers connected vehicles, fleet management, and real-time navigation, enhancing road safety and logistics.
  - **Industrial IoT (IIoT):** IoT-enabled manufacturing plants use smart sensors and real-time analytics for predictive maintenance and automated operations.
  - **Healthcare:** IoT devices enable remote patient monitoring, AI-driven diagnostics, and real-time emergency alerts, improving healthcare accessibility and efficiency.


Server Rack
Ethernet Switch
Firewall
5G Core & NMS
MEC
Multi Edge Computing
Communication
Via
5G Sim
Connected
Via
Ethernet
IoT Gateway
(Cosgrid)
5G Radio
Connected
Via
Ethernet
Communication
Via
5G Sim
Coral Gyan
(IoT Sensor Box)
Communication
Via
5G Wi-fi
CPE
Customer
Premises
Equipment
NMS
Data Of
Coral
Gyan
Computer
System

Coral Gyan Data On NMS :Communication Flow

- Step-by-Step Communication Flow:
- i.) Coral Gyan (IoT Sensor Box) Data Collection & Transmission
  - The Coral Gyan IoT Sensor Box collects sensor data
  - It sends this data to the IoT Gateway over Ethernet.
- ii.) IoT Gateway to 5G Radio Transmission
  - The IoT Gateway acts as an intermediary between the sensor box and the 5G network.
  - It aggregates the sensor data and forwards it to the 5G Radio when it detects an active 5G connection via 5G SIM.
- iii.) 5G Radio to 5G Core Transmission
  - The 5G Radio (gNodeB) receives the IoT data from the IoT Gateway.
  - It then transmits the data to the 5G Core.
  - The 5G Core handles authentication, routing.
- iv.) 5G Core to NMS Data Forwarding
  - The 5G Core forwards the received sensor data to the NMS (Network Management System).
  - The NMS is hosted on a cloud or an on-premises server and processes, stores, and visualizes the data.
  - The data can now be monitored through an NMS Dashboard.



Coral Gyan Data On NMS :
Reverse Communication Flow
(From NMS to a Computer via 5G CPE)

- i.) 5G Radio Connection to 5G CPE
  - When a 5G CPE (Customer Premises Equipment) device is connected to the 5G Radio via a 5G SIM, it acts as a bridge between the 5G network and local devices (PCs, IoT devices, etc.).
  - The 5G CPE receives data from the 5G Radio and establishes an IP network for connected devices.
- ii.) 5G CPE to Computer System Transmission
  - Any computer system, IoT device, or local network connected to the 5G CPE can now access the data from the NMS Dashboard.
  - The data can be accessed via a web interface.
- NOTE: By Default the IP of the Coral Gyan is set to 192.168.11.35 but for using it for other devices you can use by setting it and DHCP or Static

Integration of IoT in 3GPP Standards Framework

- The 3rd Generation Partnership Project (3GPP) plays a critical role in defining standards for cellular IoT integration within 5G networks. Key aspects include:
  - **Massive Machine-Type Communication (mMTC)**: Supports large-scale IoT device connectivity with minimal power consumption, essential for smart city applications.
  - **Ultra-Reliable Low Latency Communication (URLLC)**: Ensures real-time data transmission for mission-critical applications like autonomous vehicles and industrial automation.
  - **NB-IoT (Narrowband IoT) and LTE-M**: Provides low-power, wide-area connectivity for IoT devices, improving battery life and coverage.
  - **Network Slicing**: Allocates dedicated network resources to different IoT applications based on priority and requirements, ensuring optimized performance.
  - **Security Frameworks**: Implements end-to-end encryption, authentication, and secure provisioning for IoT devices in 5G networks, ensuring data integrity.

5G Labs and Emerging Technologies

- Leading technology firms and research institutions are establishing **5G Labs** to explore and test AI, IoT, and 5G synergies. These labs focus on:
    - **5G-Enabled Smart Cameras**: AI-powered surveillance cameras leverage 5G for real-time video analytics and security monitoring.
    - **Remote Healthcare**: AI-driven telemedicine solutions powered by 5G enable real-time remote diagnostics and robotic-assisted surgeries.
    - **AR/VR in 5G**: 5G Labs integrate AR/VR applications, enabling immersive experiences for remote training, industrial maintenance, and interactive education.
    - **IoT Sensor Networks**: Research in 5G Labs involves deploying IoT sensor boxes like **Coral Gyan**, which monitor environmental conditions through advanced sensors.
    - **Massive Device Connectivity**: 5G networks can support up to **1 million devices per square kilometer**, enabling large-scale IoT deployments for smart cities and industrial automation.
    - **AI-Driven Network Optimization**: 5G Labs leverage AI to enhance real-time network management, predictive maintenance, and dynamic spectrum allocation.
- These advancements highlight how AI, IoT, and 5G will continue to shape the future of connectivity and automation.

Thank You
For
Your
Time & Patience

5G LAB

Day 3

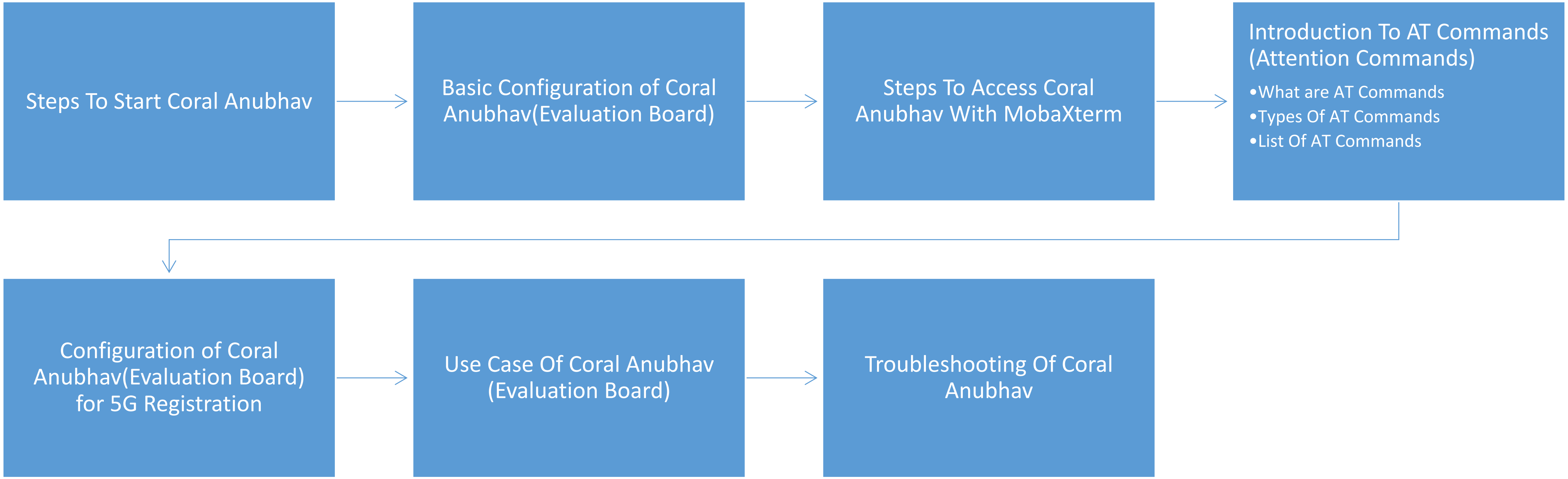
Training

5G Evaluation Board

Coral Anubhav

TRAINING MANUAL

Index



Steps To Start Coral Anubhav

Basic Configuration of Coral Anubhav(Evaluation Board)

Steps To Access Coral Anubhav With MobaXterm

Introduction To AT Commands (Attention Commands)

- What are AT Commands
- Types Of AT Commands
- List Of AT Commands

Configuration of Coral Anubhav(Evaluation Board) for 5G Registration

Use Case Of Coral Anubhav (Evaluation Board)

Troubleshooting Of Coral Anubhav

Steps To Start With Evaluation Board

Step 1: -Insert the Private 5G SIM in the Evaluation Board

Step 2: - Power on the Board using 5V Power Adapter

Step 3: - Press the Reset Button for 3-5 Seconds

Step 4: - Wait for 15 seconds for the Board to Boot Up

Step 5: - Install the appropriate drivers on the computer.

Recommended: Use Driver Booster: Driver Booster   .

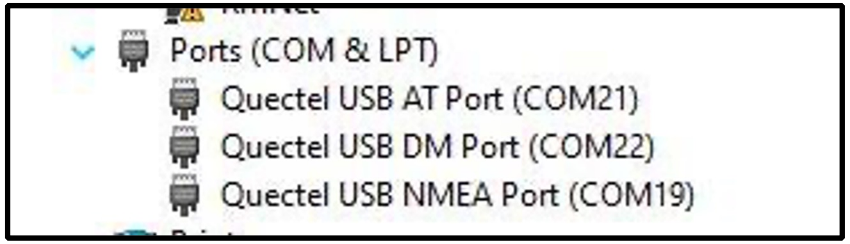
- Install the RG520F Drivers (Must Needed)
- Install the PORT Driver (Must Needed)

You are now ready to take the access of the evaluation board

Basic Configuration Of Evaluation Board

Step 1: - Press Windows + X on your Windows Computer Home screen and navigate to Device Manager

Step 2: - When you will open the Device Manager you see a list of **Ports(COM & LPT)**



Ports (COM & LPT)

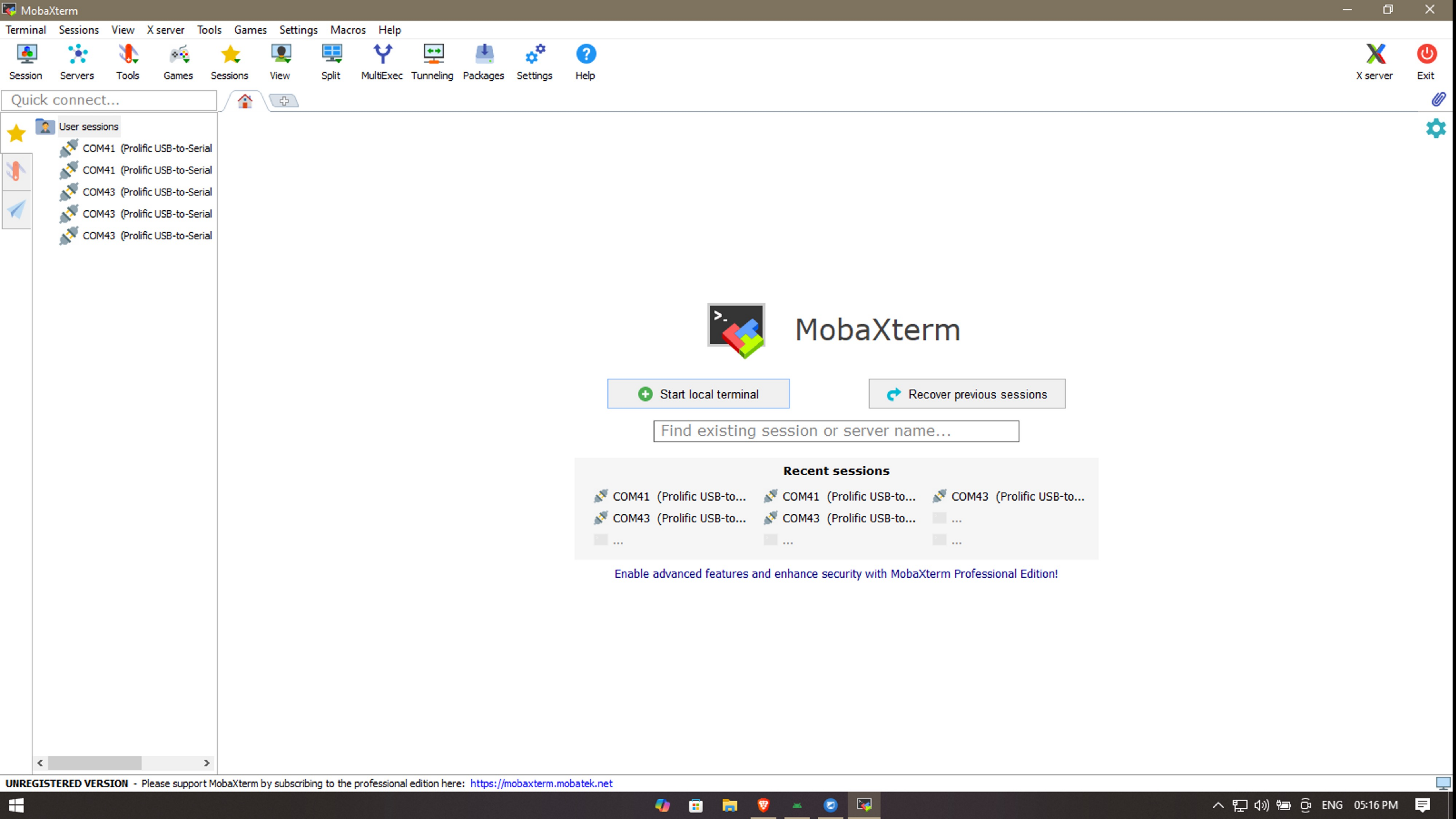
- Quectel USB AT Port (COM21)
- Quectel USB DM Port (COM22)
- Quectel USB NMEA Port (COM19)

Step 3: - After that install MobaXterm from the internet - MobaXterm : - MobaXterm

Step 4: - MobaXterm is an advanced terminal emulator and remote desktop application designed for Windows. It provides a powerful set of tools for developers, system administrators, and IT professionals who work with remote systems.

Steps To Access Coral Anubhav With MobaXterm

- Once When You Will Open MobaXterm you will be welcomed with this screen
- Select the option of Session on the Top-Right Corner of the Screen
- Once you will click on that you will see another window
- Once you get to this screen go for serial connection which have the logo of plug connector
- In This Screen you will Select the AT Port and will enter the BAUD Rate as 115200
- After all this you will be able to access the Coral Anubhav
- Type ATI to see the Basic Details :



User sessions

- COM41 (Prolific USB-to-Serial
- COM41 (Prolific USB-to-Serial
- COM43 (Prolific USB-to-Serial
- COM43 (Prolific USB-to-Serial
- COM43 (Prolific USB-to-Serial

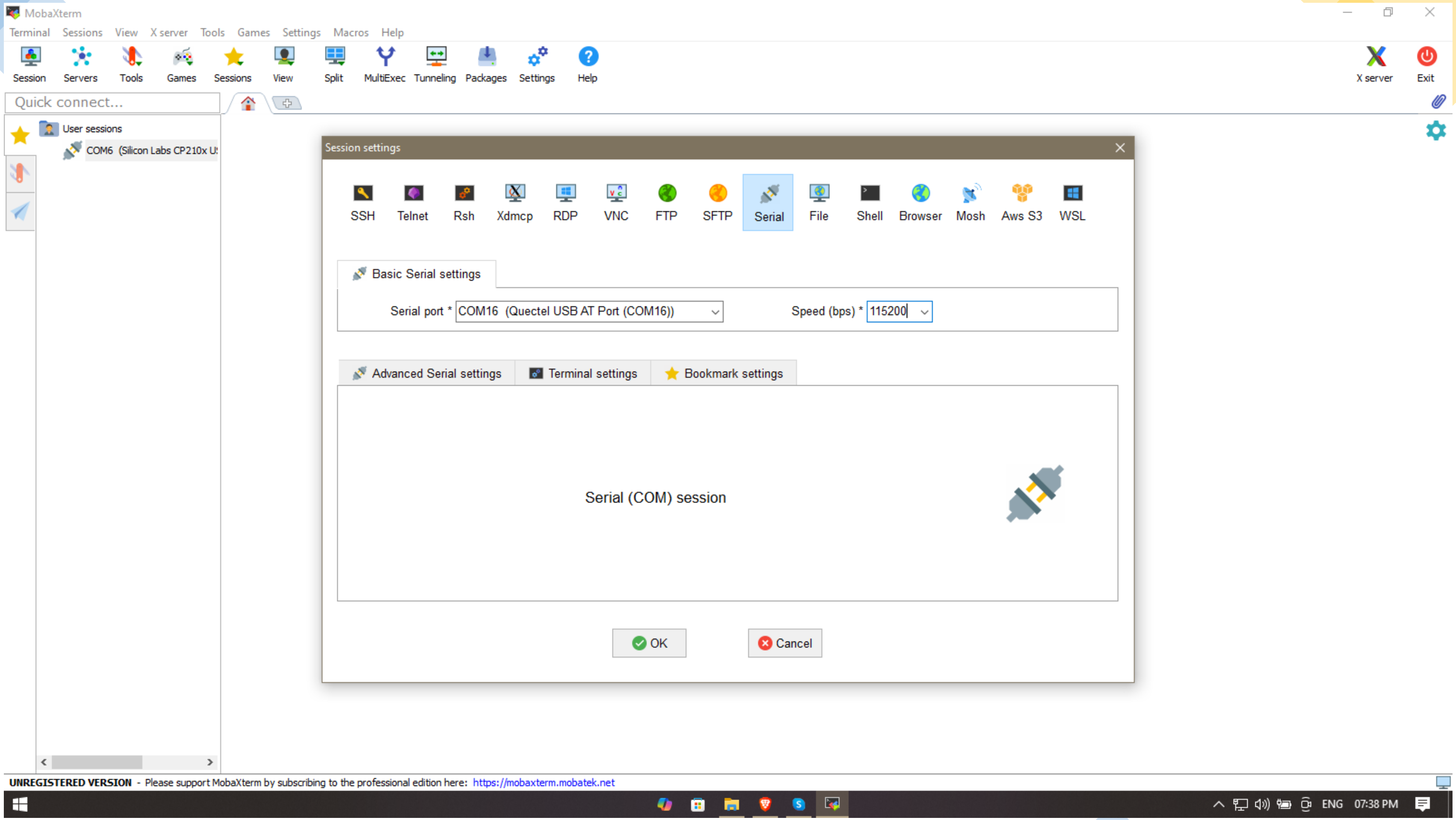
MobaXterm

Recent sessions

COM41 (Prolific USB-to...	COM41 (Prolific USB-to...	COM43 (Prolific USB-to...
COM43 (Prolific USB-to...	COM43 (Prolific USB-to...	...
...	...	...

Enable advanced features and enhance security with MobaXterm Professional Edition!

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net



Session settings

Basic Serial settings

Serial port * COM16 (Quectel USB AT Port (COM16))

Speed (bps) * 115200

Serial (COM) session

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Introduction To Attention Commands (AT Commands)

AT commands (Attention commands) are used to communicate with modems or modules via serial communication. They help configure settings, retrieve information, or control device functionalities.

Types of AT Commands

- **Test Command (=?) -** The command returns the list of parameters and value ranges set by the corresponding Write Command or internal processes.
  - Syntax: AT+COMMAND=?
  - Purpose: Lists all possible values a command supports.
  - Example Response: +CONFIG: (0,1,2,3), indicating valid options.
- **Read Command (?) -** The command returns the currently set value of the parameter or parameters.
  - Syntax: AT+COMMAND?
  - Purpose: Queries the current value of a setting.
  - Example Response: +CONFIG: 2, meaning the current setting is 2.
- **Write Command (=<parameters>) -** The command sets the user-definable parameter values.
  - Syntax: AT+COMMAND=<value>
  - Purpose: Sets a new value for the configuration.
  - Example Response: OK, confirming the update.

AT Command	Functionality
ATI	Returns model number and firmware version.
AT+CIMI	Returns IMSI number.
AT+COPS=?	Displays list of available networks; check if network "00101" is available.
AT+CFUN=0	Switches UE to minimum functionality (returns OK).
AT+CFUN=1	Switches UE to full functionality (returns OK).
AT+CGDCONT?	Displays list of APNs; check APN configuration as per network slice.
AT+CGDCONT=1,"IP","APN-Name"	Set APN to "APN-Name".

Configuration Of Coral Anubhav (5G Evaluation Board) For 5G Registration

Now, we will look at how to connect your 5G Evaluation board with the radio and establish 5G Registration.

Entire registration part is divided into 4 Steps

Step 1: Set network mode preference to NR5G

- Set Network Preferences: **AT+QNWPREFCFG="mode_pref",NR5G**

Step 2: Set APN to 'APNname' for data connection.

- Set APN: **AT+CGDCONT=1,"IP","APNname"**

Step 3: Set the operator selection on Automatic mode

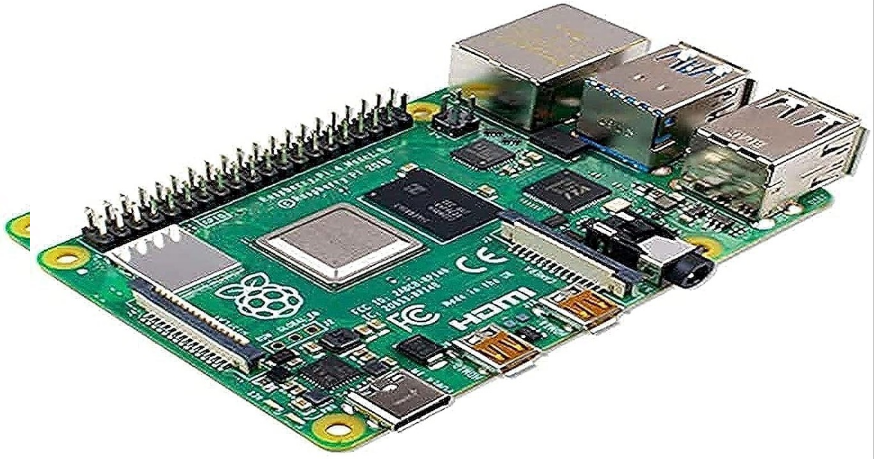
- Set operator selection on automatic mode: **AT+COPS=0**

Step 4: Reload The 5G Evaluation Board (Set UE Functionality)

➔ **AT +CFUN=0**

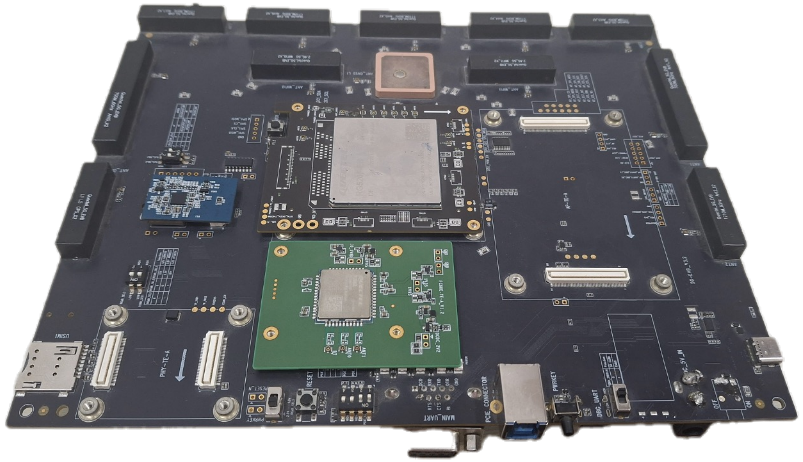
➔ **AT+CFUN=1**

Raspberry Pi Use Case With Coral Anubhav



Introduction

This use case explores the practical applications of automating the configuration of the 5G evaluation(Coral Anubhav) using Bash scripts on a Raspberry Pi. By leveraging predefined commands, users can efficiently manage network registration, modem setup, and configuration changes without manual intervention. This automation enhances reliability, speeds up deployment, and reduces human errors in 5G connectivity setups, making it ideal for IoT applications, industrial automation, and research projects. The guide provides a step-by-step approach to executing AT commands via Bash, ensuring seamless interaction between the Raspberry Pi and the 5G modem.



Prerequisites

- Raspberry Pi (any model with USB support)
- 5G Evaluation Board (Coral Anubhav)
- SIM Card
- Minicom or another serial communication tool
- USB-to-Serial driver installed (if necessary)

Setup Instructions

Run as Root:

```
sudo -i
```

Check Device Path:

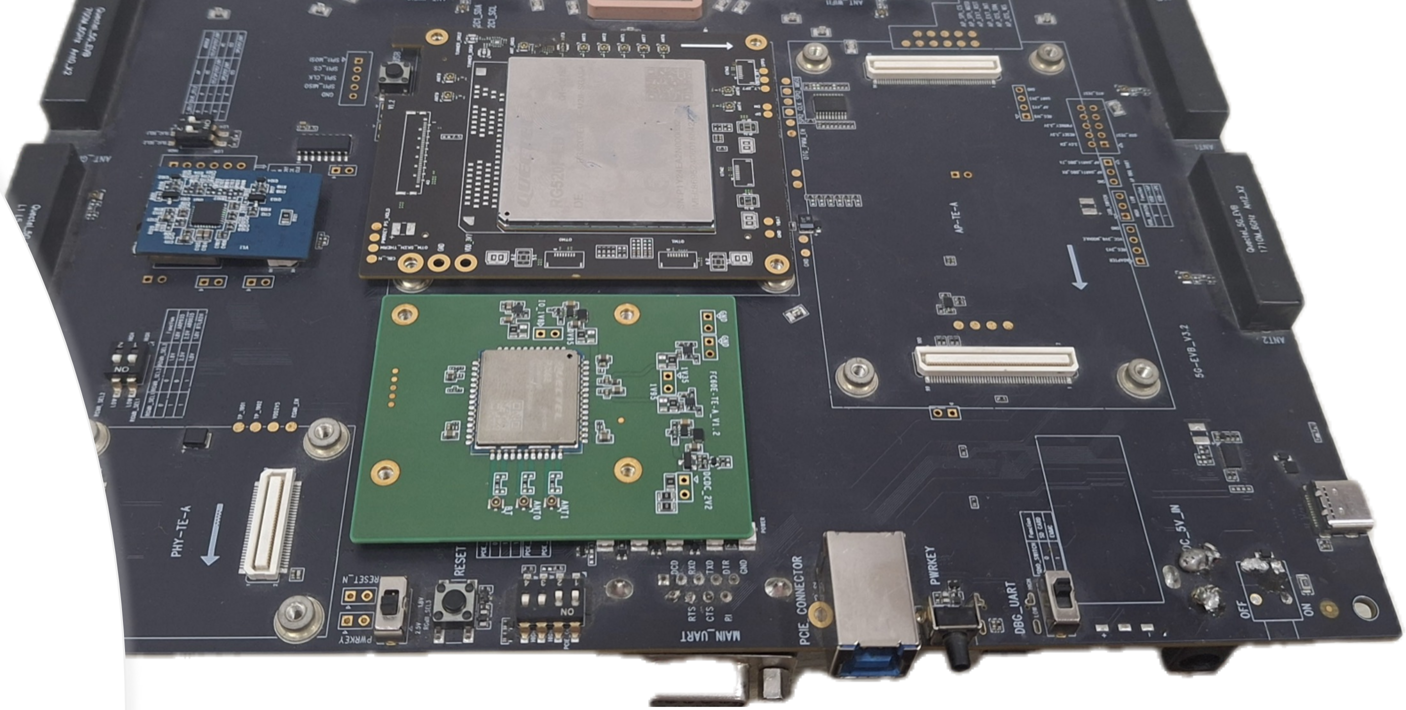
```
ls /dev/ttyUSB*
```

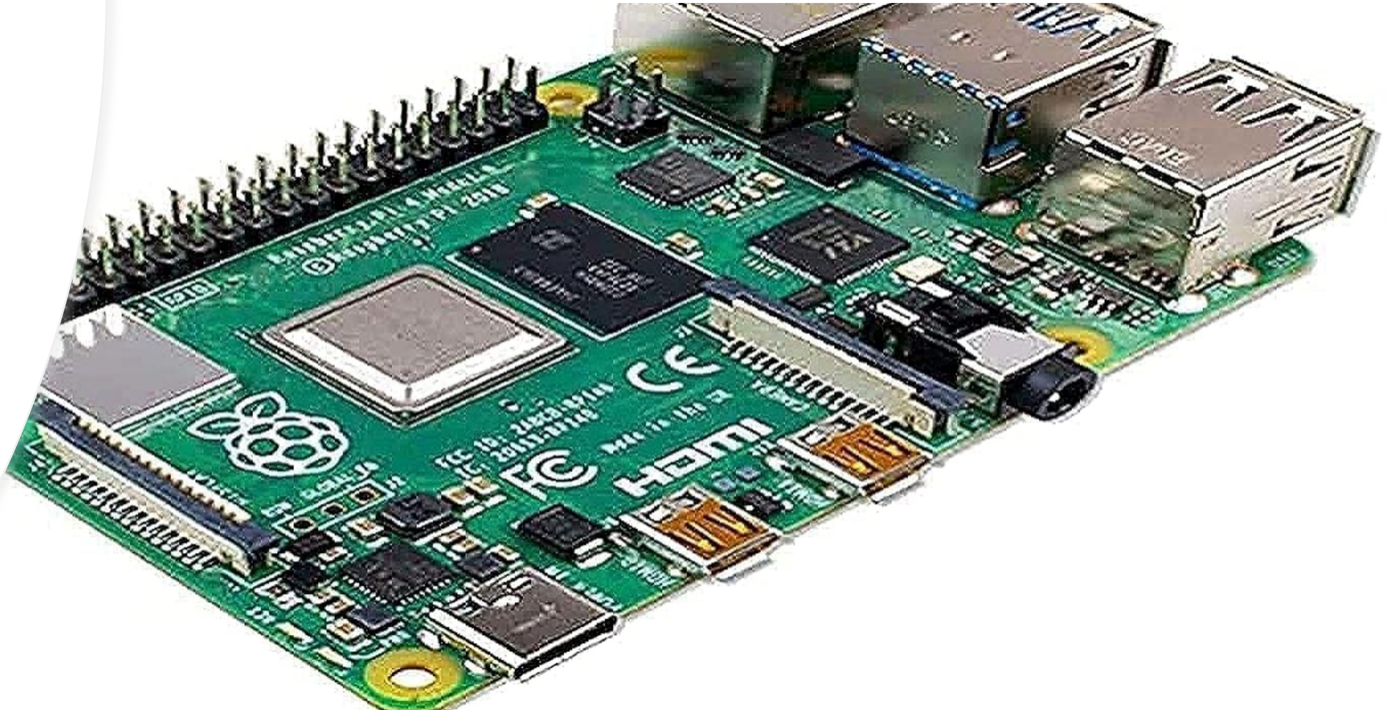
Install Required Packages:

```
sudo apt update && sudo apt install -y socat;
```

Grant USB Permissions:

```
sudo chmod 777 /dev/ttyUSB*
```

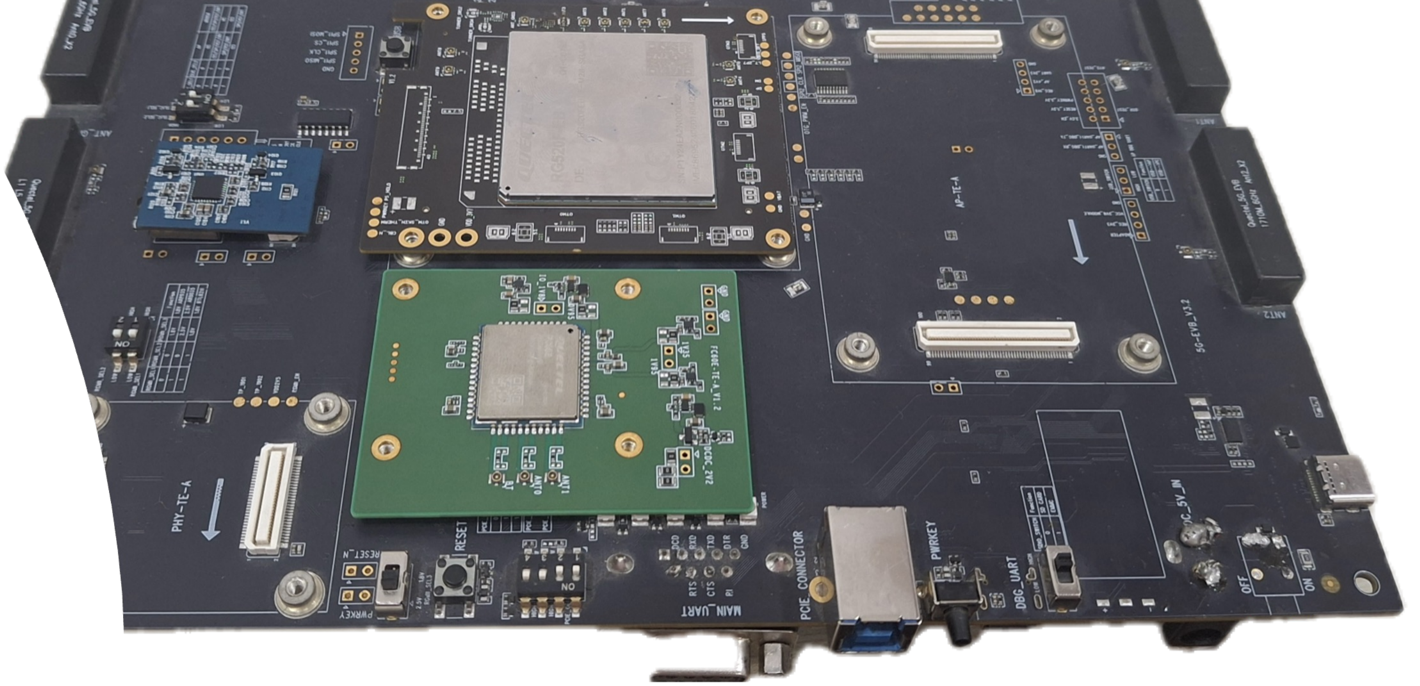


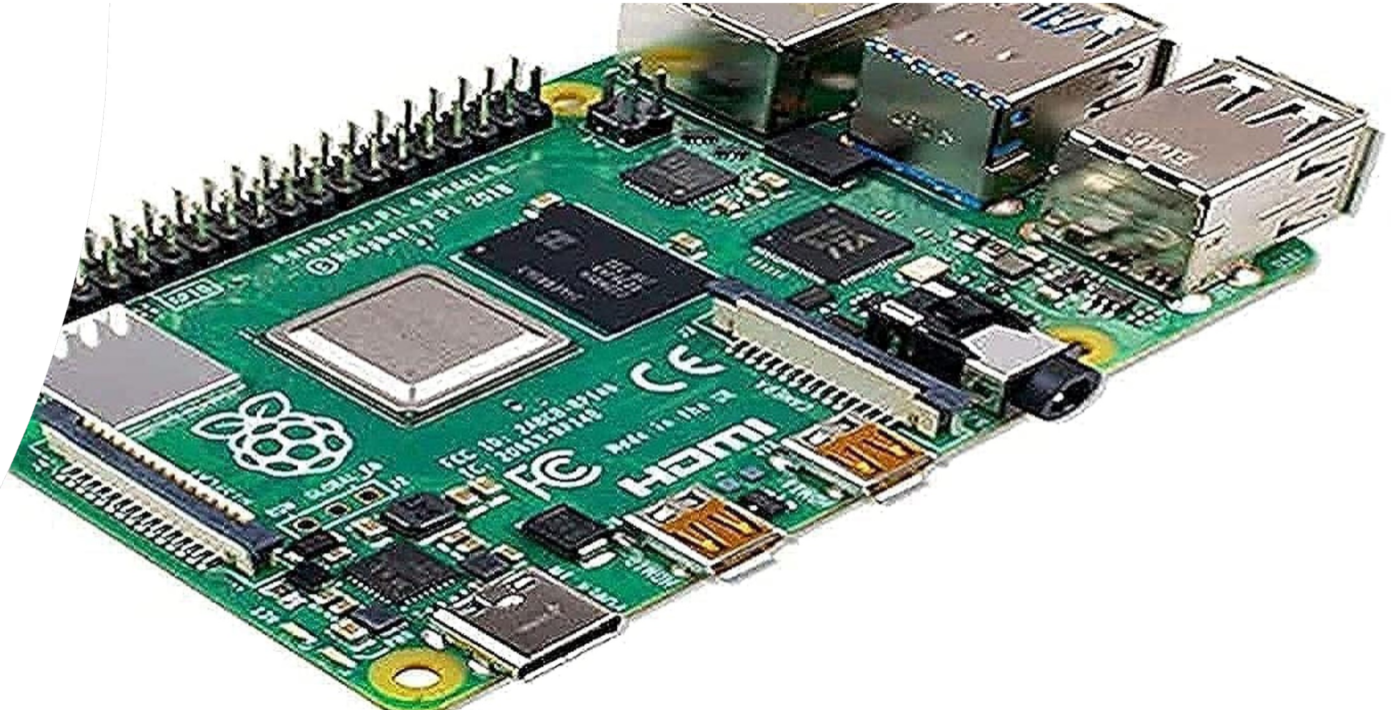


Bash Script for Modem Configuration

Create a script `modem_config.sh` to execute AT commands using `socat`.

```
#!/bin/bash

# Check if minicom is installed

if ! command -v socat &> /dev/null; then

    echo "socat is not installed. Installing..."

    sudo apt update

    sudo apt install -y socat

else

    echo "script is started."

fi

# the command run and output show in file

echo ATI | socat - /dev/ttyUSB2,crnl > /tmp/hello;

echo AT+cimi | socat - /dev/ttyUSB2,crnl > /tmp/hello;

echo AT+QNWCFG=? | socat - /dev/ttyUSB2,crnl >/tmp/hello;

#when you want to append the output

#echo AT+QNWCFG=? | socat - /dev/ttyUSB2,crnl >>/tmp/output.txt;

# for print on file and terminal

#echo ATI | socat - /dev/ttyUSB2,crnl | tee /tmp/hello;

#    read command thru file and output both to terminal and file

#cat commands.txt | socat - /dev/ttyUSB2,crnl | tee /tmp/hello
```





Running the Script

Make the script executable and run it:

```
chmod +x modem_config.sh

sudo ./modem_config.sh
```

Creating a Systemd Service for Automation

To automate the execution of the script, create a systemd service.

```
[Unit]
Description=5G Modem Configuration Service
After=network.target

[Service]
ExecStart=/bin/bash /path/to/modem_config.sh
Restart=always
User=root

[Install]
WantedBy=multi-user.target
```

Save the file as `/etc/systemd/system/modem_config.service` and run the following commands to enable it:

```
sudo systemctl daemon-reload
```

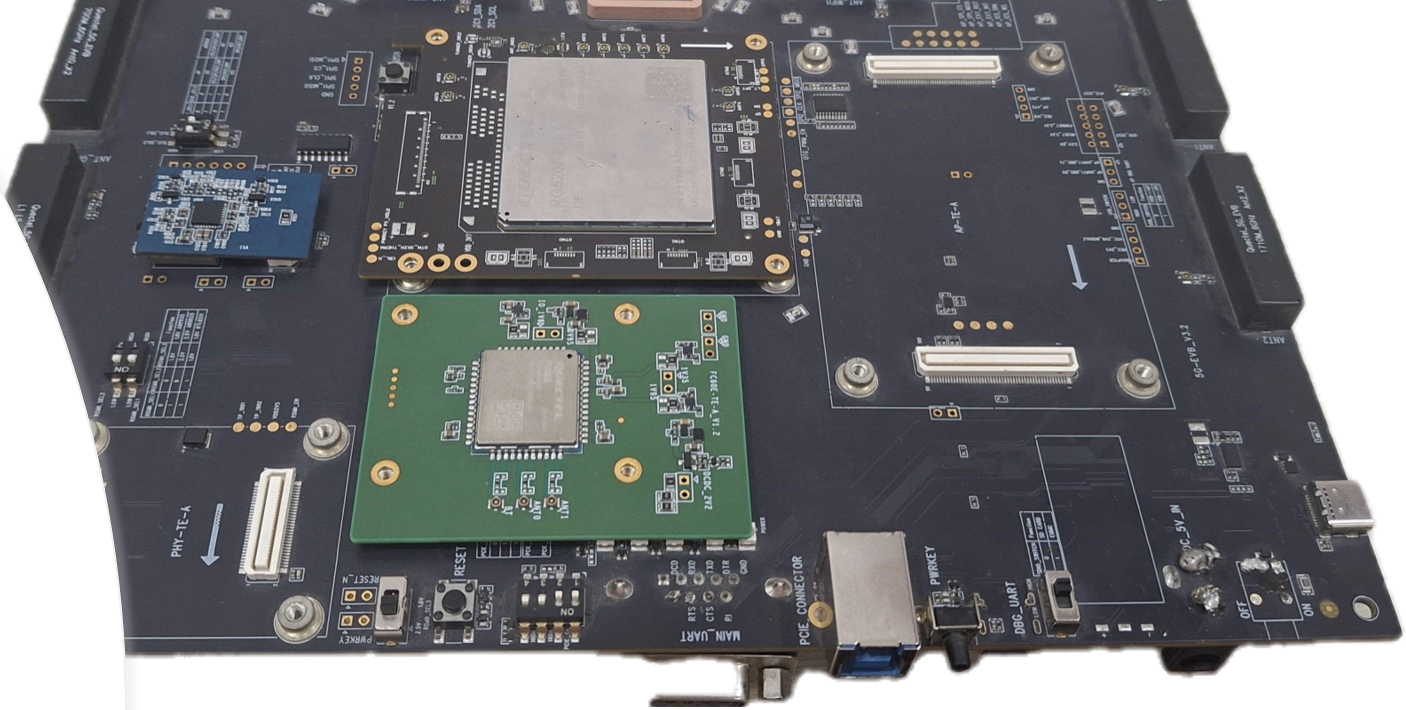
Reloads systemd to recognize new or modified service files.

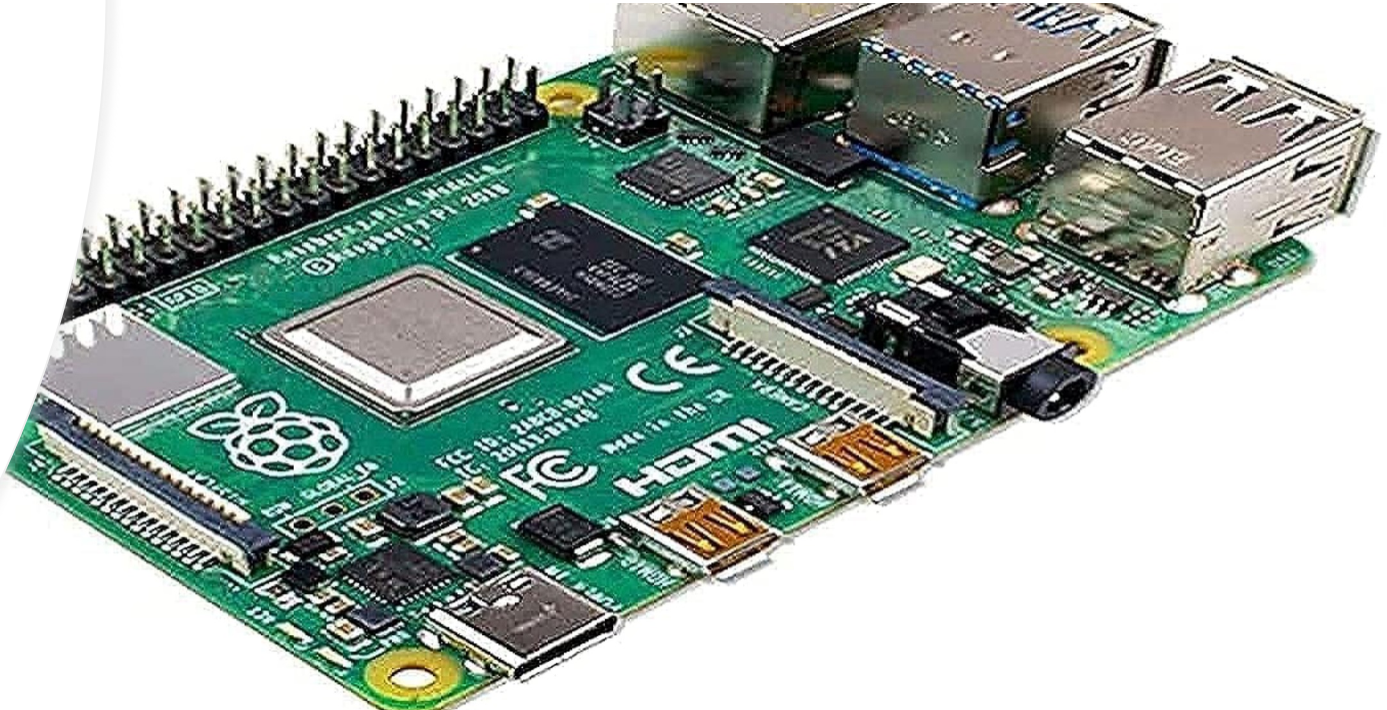
```
sudo systemctl enable modem_config.service
```

Enables the service to start automatically on boot.

```
sudo systemctl start modem_config.service
```

Starts the service immediately without rebooting.





TroubleShooting Of Coral Anubhav

Basic Checks

A. **Power & Hardware Connections**

- Ensure the module is properly powered
- Check if the antennas are connected (for optimal signal reception)
- Verify the SIM card is inserted correctly

A. **Driver & Firmware Verification**

- Check if the necessary drivers are installed (Linux/Windows)
- Ensure firmware is up-to-date
- Default Baud Rate as 115200. Evaluation Board will communicate with devices on this BAUD Rate

A. **AT Command Interface Check**

Use AT commands to verify basic functionality

- `AT` → Check if the module responds
- `ATI` → Get manufacturer info
- `AT+CGMR` → Get firmware version

TroubleShooting Of Coral Anubhav

Debugging Logs

- Insert a USB Type-C connection with Debug UART and then switch to the **Silicon Labs CP210x USB-to-UART Bridge**. Set the BAUD Rate as 115200.This will provide access to hardware-level logs and detailed diagnostic information for all modules and features.

Device and Module Info

➔ Get Firmware and Device Information:

AT+CGMR - Display firmware version.

➔ Check 5G MIMO Status:

AT+QNWCFG="nr5g_mimo" -Check if 5G MIMO is enabled.

➔ Enable 5G MIMO:

AT+QNWCFG="nr5g_mimo",1-Enable 5G MIMO.

TroubleShooting Of Coral Anubhav

ADB(Android Debugging Bridge) Access

- To check about the Coral Anubhav services we can access it by taking adb access to the Coral Anubhav Board.
- Take access by adb shell after connecting it via USB 3.0 provided
- Enter the command - **systemctl status *.service**

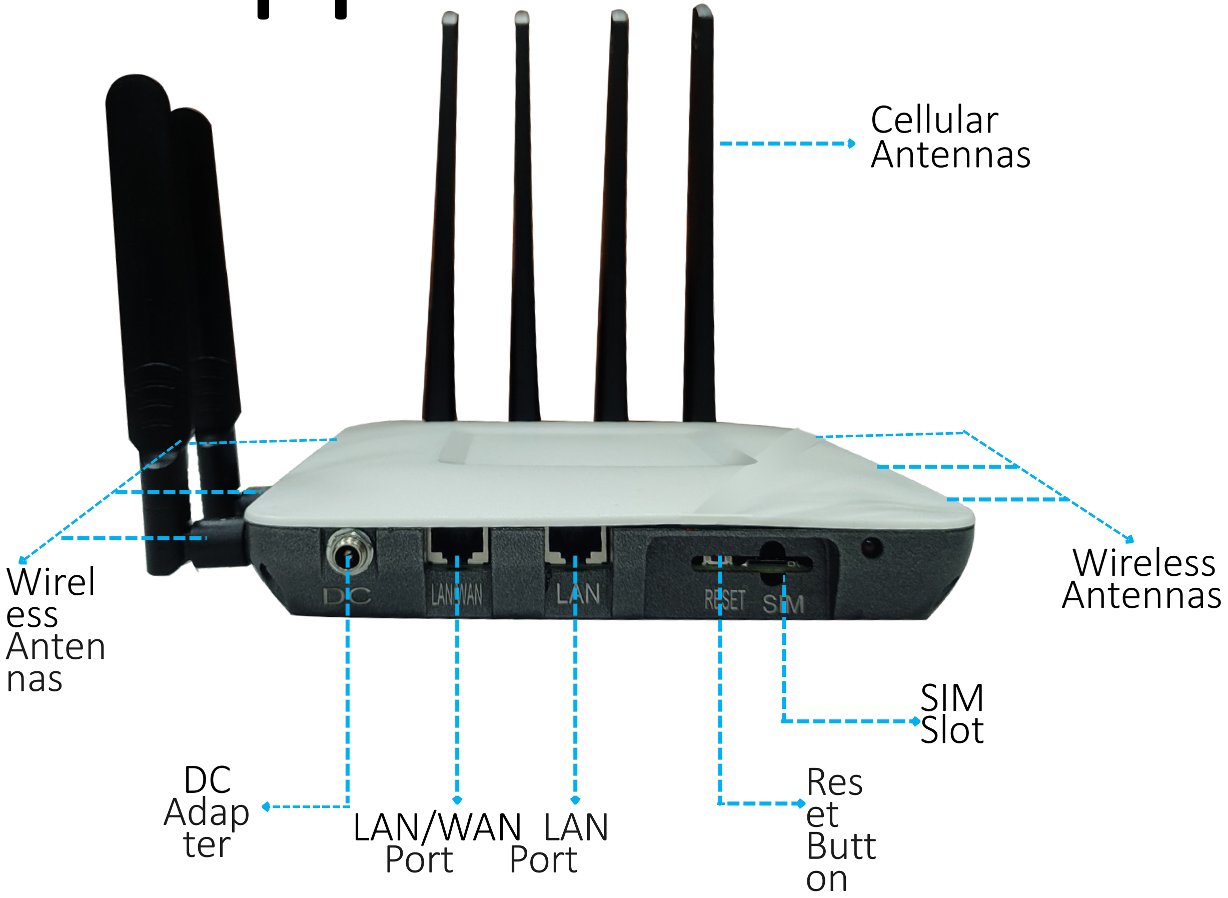
5G CPE

5G LAB

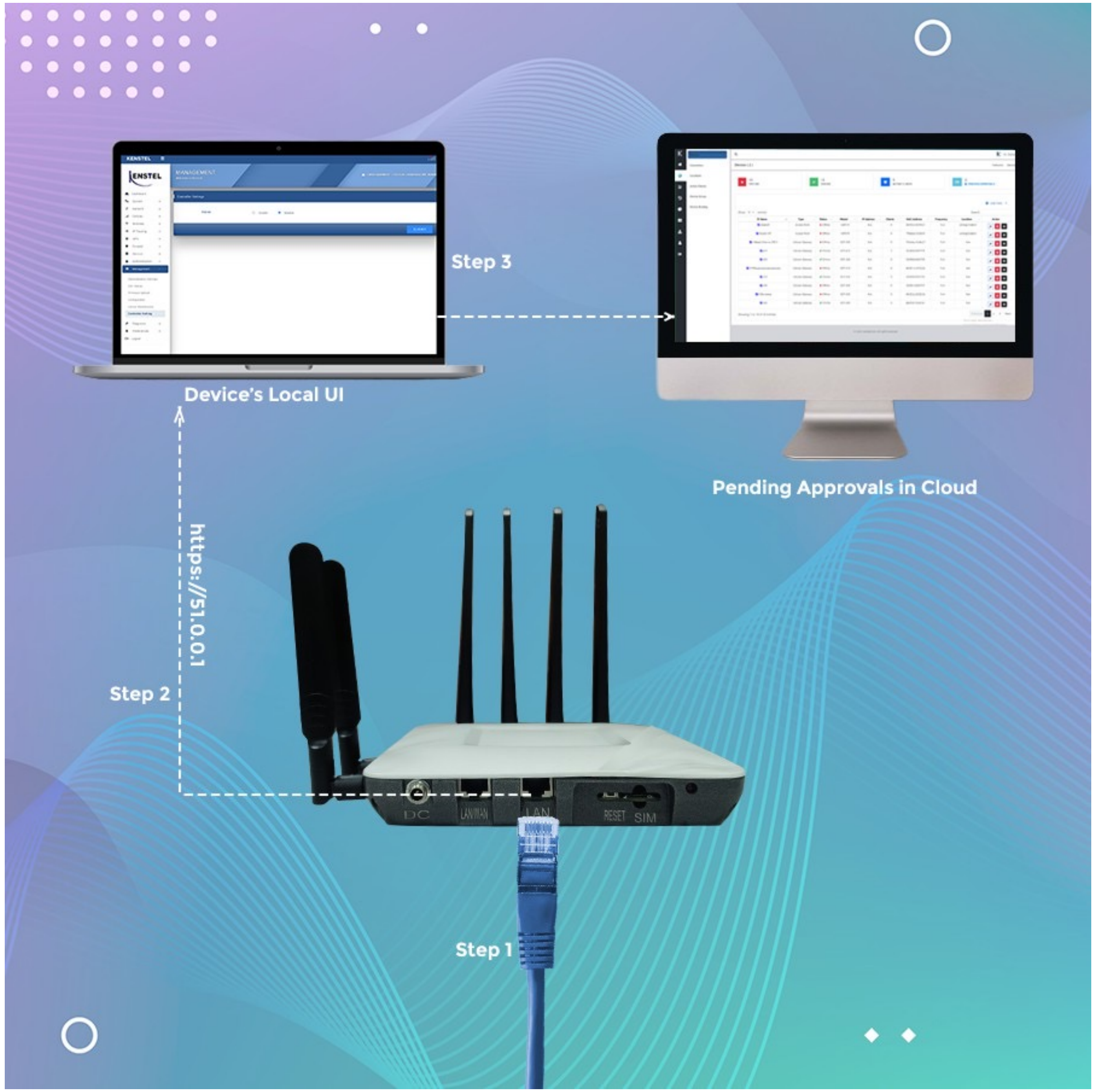
5G CPE

A 5G CPE (Customer Premise Equipment) is a device that connects to a 5G network, converting the 5G signal into Wi-Fi or wired connections, enabling multiple devices (like phones, tablets, IoT GW, and computers) to access the 5G Network.

Appearance


Cellular Antennas
Wireless Antennas
Wireless Antennas
DC
LAN/WAN
LAN
RESET
SIM
SIM Slot
DC Adapter
LAN/WAN Port
LAN Port
Reset Button

Connectivity



Device can run on two modes one is Local and another is Cloud.

If you want to run the Device with local mode you just simply Connect your Device via LAN Port

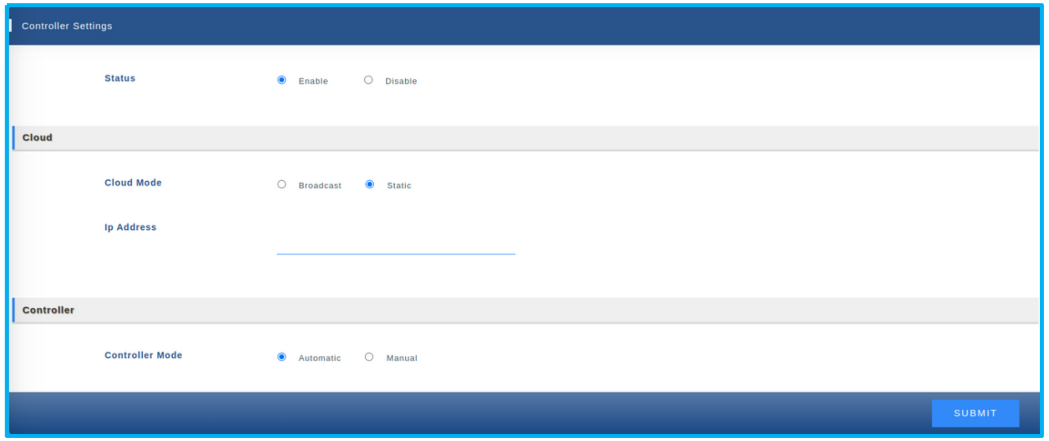
Then open with the IP, https://51.0.0.1 → Signup and Sign in

And if you want to run the Device with Cloud mode you just simply Connect your Device via LAN Port ,Then open with the IP, https://51.0.0.1 → Signup and Sign in , And then go to Management, Controller Setting

Status: Enable the Status.

Cloud Mode: There are two cloud modes one is Broadcast and another one is Static. If you enable Static mode then input the ip address.

Controller Mode: There are two controller modes one is Automatic and another one is Manual. In Automatic mode device will get the IP automatically from cloud while in manual you have to input the IP manually.



Controller Settings

Status ● Enable ○ Disable

Cloud

Cloud Mode ○ Broadcast ● Static

Ip Address

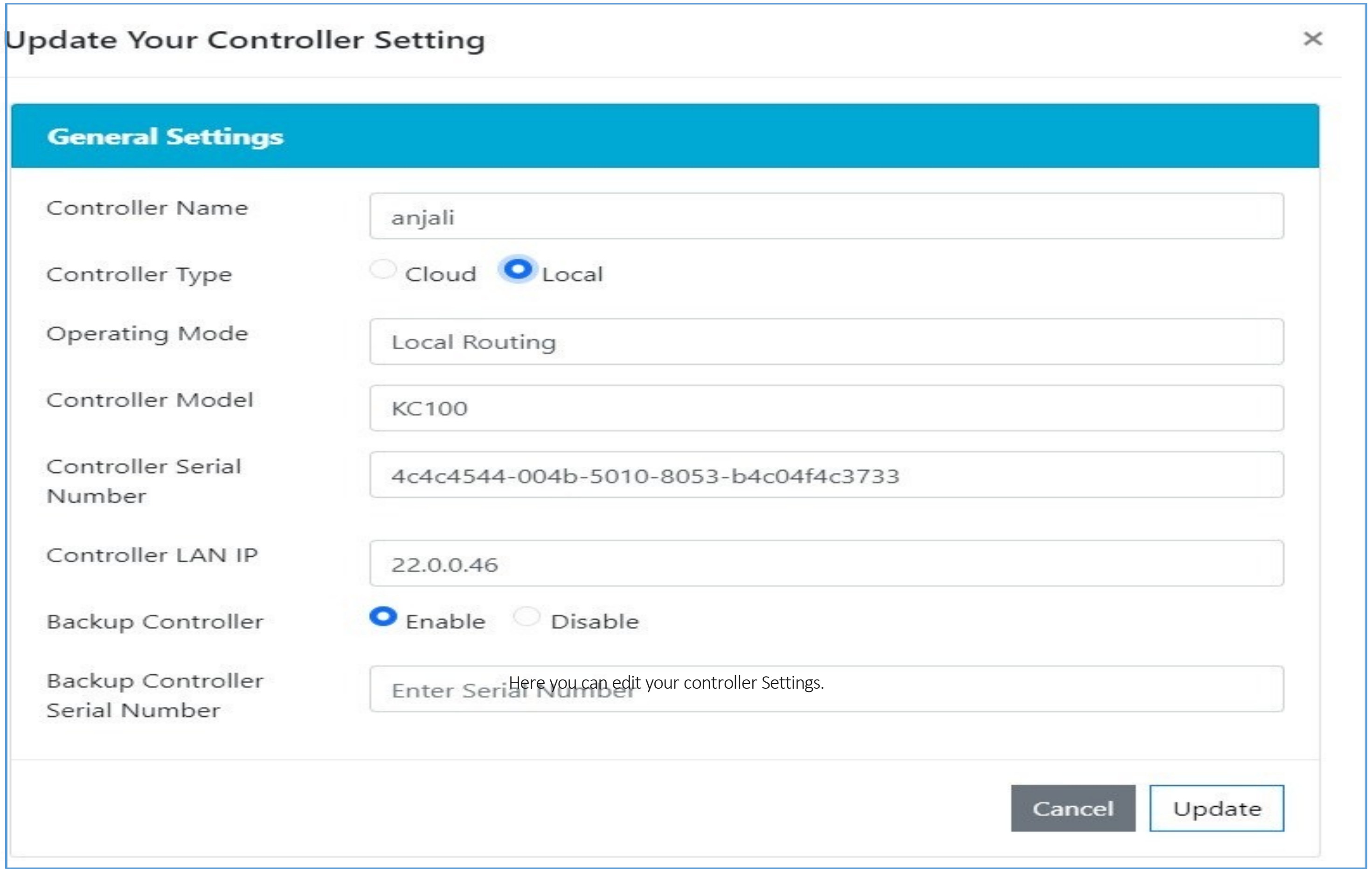
Controller

Controller Mode ● Automatic ○ Manual

Controller

Controller can operate on Local Routing, Centralized forwarding and Bridging.
Local routing: In the case of Local routing, Captive Portal, Network rate limit and user by the rate limit are all features operated on Access Point itself.
Centralized forwarding: But, in the case of Centralized forwarding, all the above features are implemented on controller.

Edit Controller page when controller type is in Local.



Update Your Controller Setting

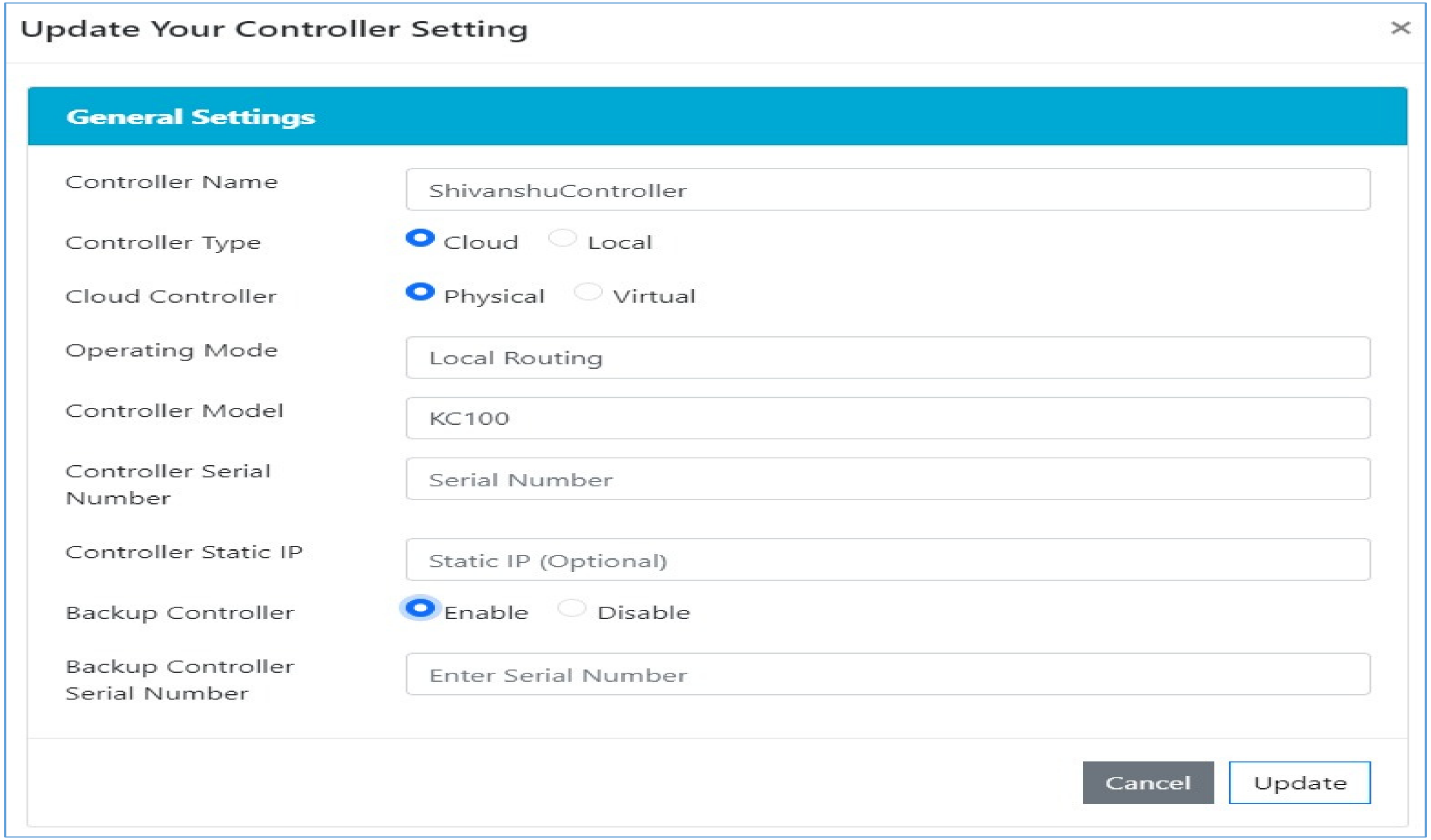
General Settings

Controller Name	anjali
Controller Type	○ Cloud ● Local
Operating Mode	Local Routing
Controller Model	KC100
Controller Serial Number	4c4c4544-004b-5010-8053-b4c04f4c3733
Controller LAN IP	22.0.0.46
Backup Controller	● Enable ○ Disable
Backup Controller Serial Number	Enter Serial Number

Here you can edit your controller Settings.

Controller

Edit Controller page controller type is in Cloud.



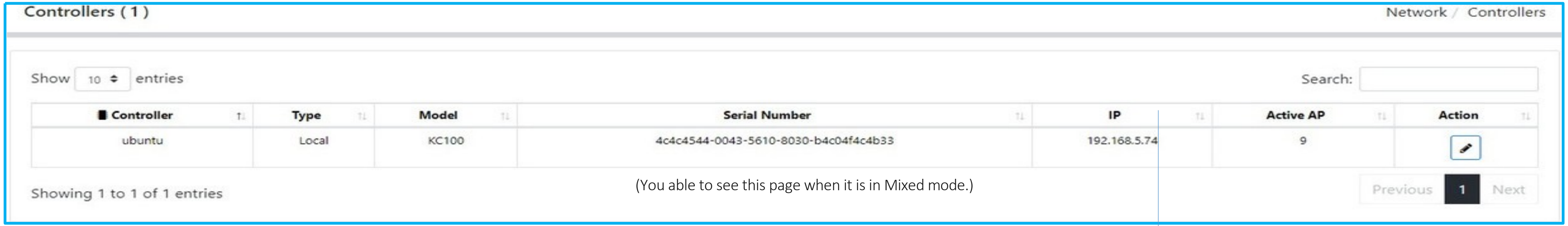
Update Your Controller Setting

General Settings

Controller Name	ShivanshuController
Controller Type	● Cloud ○ Local
Cloud Controller	● Physical ○ Virtual
Operating Mode	Local Routing
Controller Model	KC100
Controller Serial Number	Serial Number
Controller Static IP	Static IP (Optional)
Backup Controller	● Enable ○ Disable
Backup Controller Serial Number	Enter Serial Number

Here you can edit your controller Settings.

Controller



Controllers (1)

Network / Controllers

Show 10 entries

Search:

Controller	Type	Model	Serial Number	IP	Active AP	Action
ubuntu	Local	KC100	4c4c4544-0043-5610-8030-b4c04f4c4b33	192.168.5.74	9	✎

Showing 1 to 1 of 1 entries

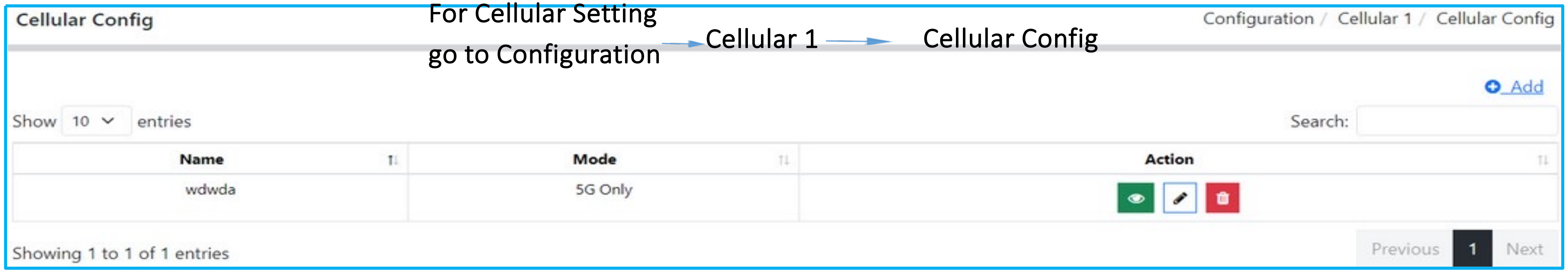
Previous 1 Next

(You able to see this page when it is in Mixed mode.)

Mixed Mode: Mixed mode is a more complex approach that combines both basic and advanced features in the control interface. This mode is designed for users or organizations with diverse needs and provides access to a wide range of capabilities, from basic provisioning and monitoring to more complex features such as advanced automation, policy enforcement, and hybrid cloud management.

Click here to open the edit controller page.

Cellular Setting - Cellular Config



Cellular Config

Configuration / Cellular 1 / Cellular Config

For Cellular Setting go to Configuration → Cellular 1 → Cellular Config

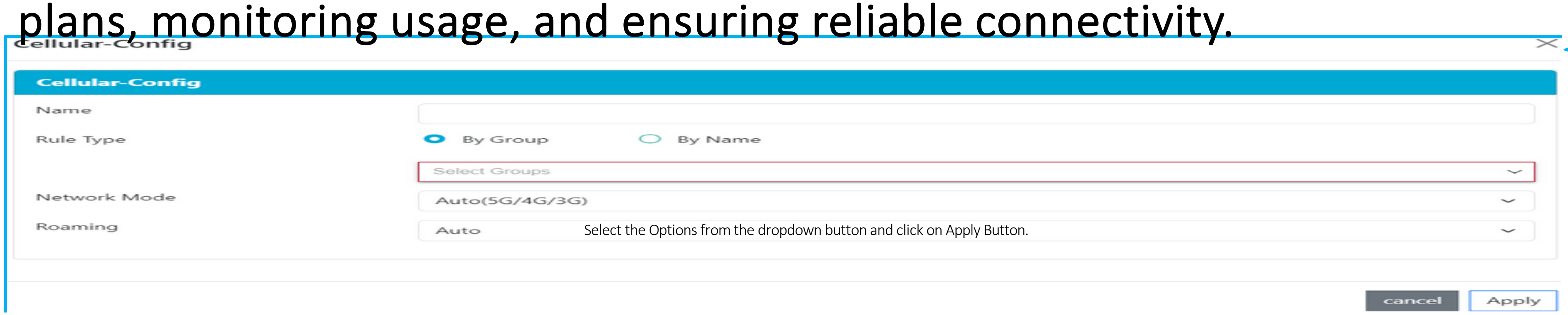
Show 10 entries

Search:

Name	Mode	Action
wdwda	5G Only	👁 ✎ 🗑

Showing 1 to 1 of 1 entries

Cellular configuration typically refers to the setup and management of cellular connectivity for devices within the cloud environment. This could include configuring devices to connect to cellular networks, managing data plans, monitoring usage, and ensuring reliable connectivity.



Cellular-Config

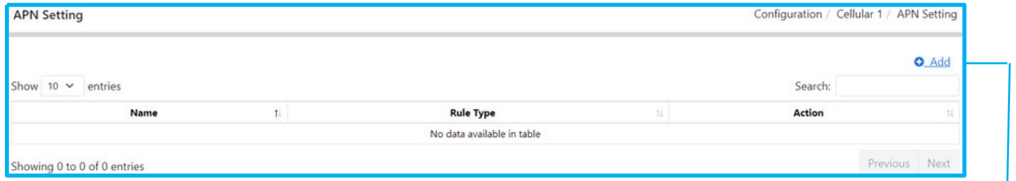
Cellular-Config

Name	
Rule Type	● By Group ○ By Name
	Select Groups
Network Mode	Auto(5G/4G/3G)
Roaming	Auto

Select the Options from the dropdown button and click on Apply Button.

Cellular Setting - APN Setting

For Cellular Setting go to Configuration → Cellular → APN Setting



APN Setting

Configuration / Cellular 1 / APN Setting

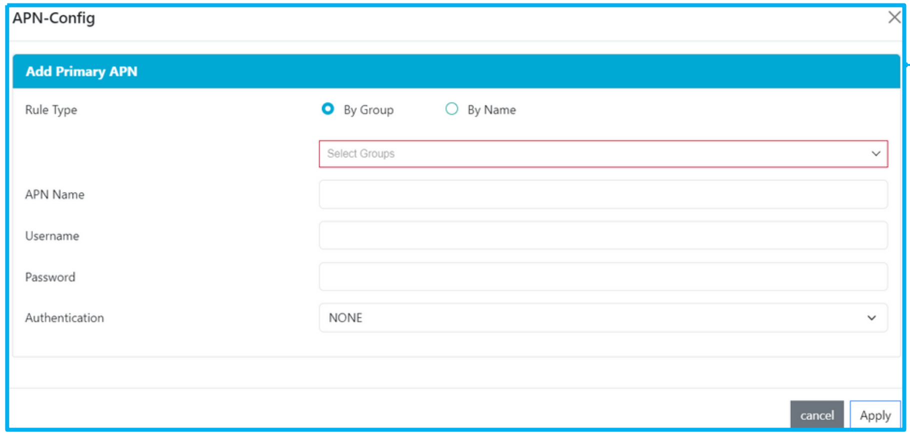
Show 10 entries

Search:

Name	Rule Type	Action
No data available in table		

Showing 0 to 0 of 0 entries

Configuring the Access Point Name (APN) settings is crucial for establishing the connection between the device and the cellular network. The APN acts as a gateway between the mobile network and the internet or a private network, depending on the specific requirements of the application.



APN-Config

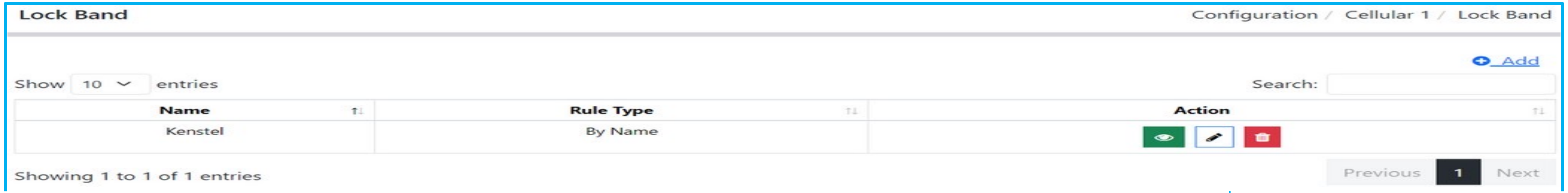
Add Primary APN

Rule Type	● By Group ○ By Name
	Select Groups
APN Name	
Username	
Password	
Authentication	NONE

Fill the credential and Select the authentication mode from the dropdown button and click on Apply Button.

Cellular Setting - Lock Band

For Cellular Setting go to Configuration → Cellular → **Lock** Band



Lock Band

Configuration / Cellular 1 / Lock Band

⊕ Add

Show 10 entries

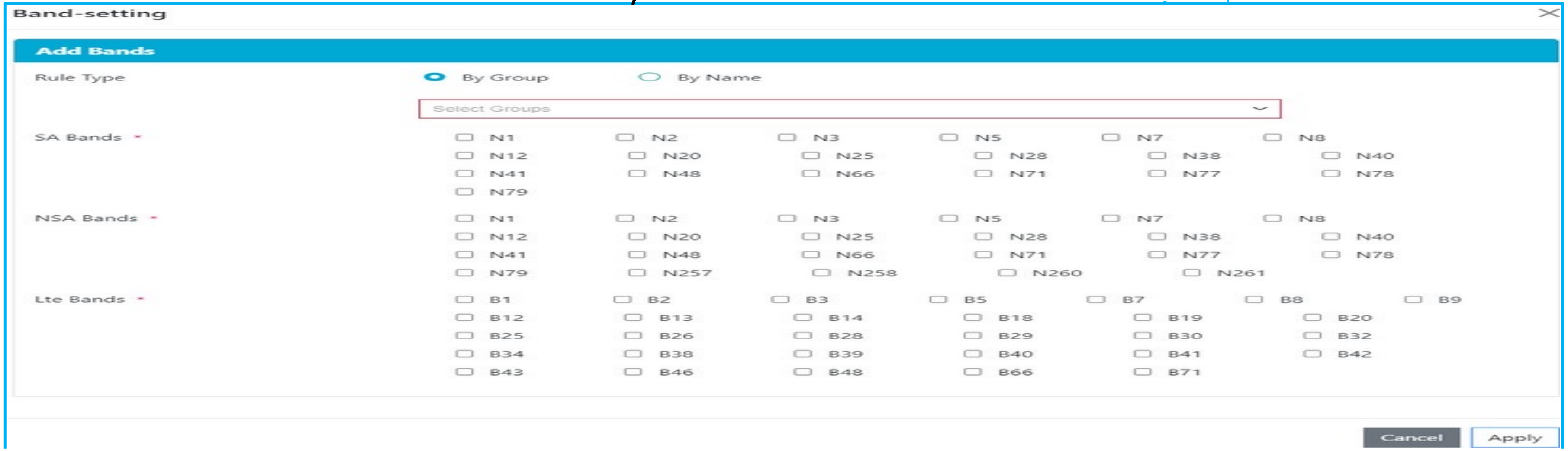
Search:

Name	Rule Type	Action
Kenstel	By Name	👁 ✎ 🗑

Showing 1 to 1 of 1 entries

Previous 1 Next

By locking bands in cellular configurations managed by a cloud controller, organizations can optimize the performance, reliability, and regulatory compliance of their cellular deployments, ensuring seamless communication and connectivity for their devices.



Band-setting ×

Add Bands

Rule Type ● By Group ○ By Name

Select Groups

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

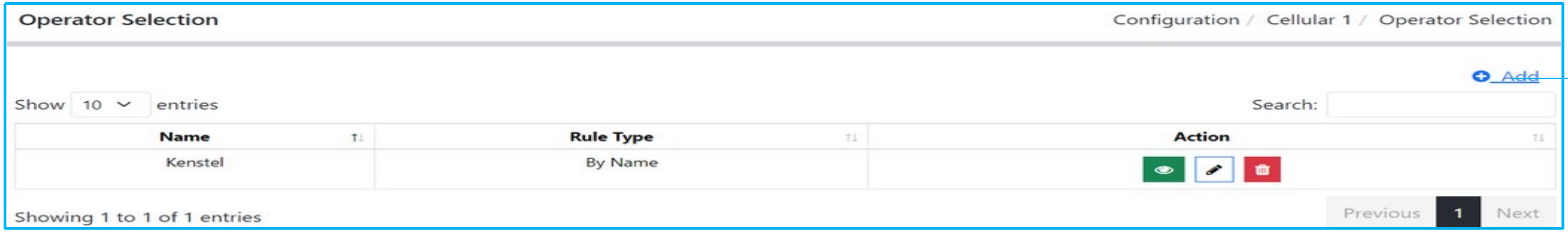
NSA Bands *
□ N1 □ N2 □ N3 □ N5 □ N7 □ N8
□ N12 □ N20 □ N25 □ N28 □ N38 □ N40
□ N41 □ N48 □ N66 □ N71 □ N77 □ N78
□ N79 □ N257 □ N258 □ N260 □ N261

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

Cancel Apply

Cellular Setting - Operator Selection

For Cellular Setting go to Configuration → Cellular → Operator Selection

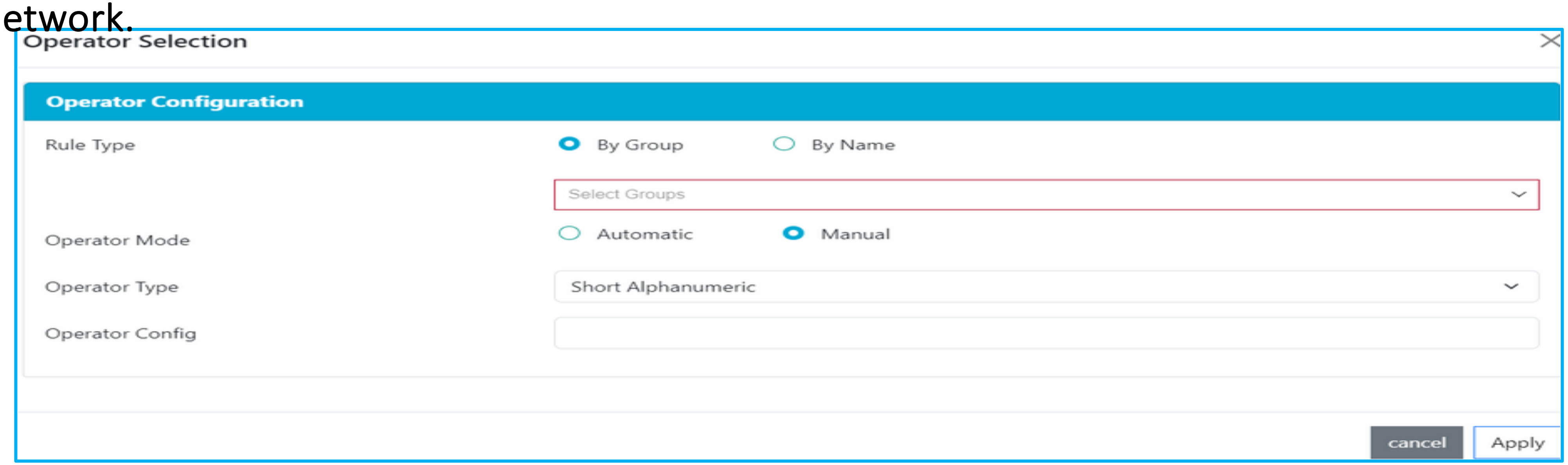


Operator Selection

Name	Rule Type	Action
Kenstel	By Name	

Showing 1 to 1 of 1 entries

A network operator is responsible for the implementation, configuration, and management of TCP/IP protocols across a Cellular network infrastructure. They also ensure reliable data transmission by establishing and maintaining TCP connections between CPE devices and Network.



Operator Selection

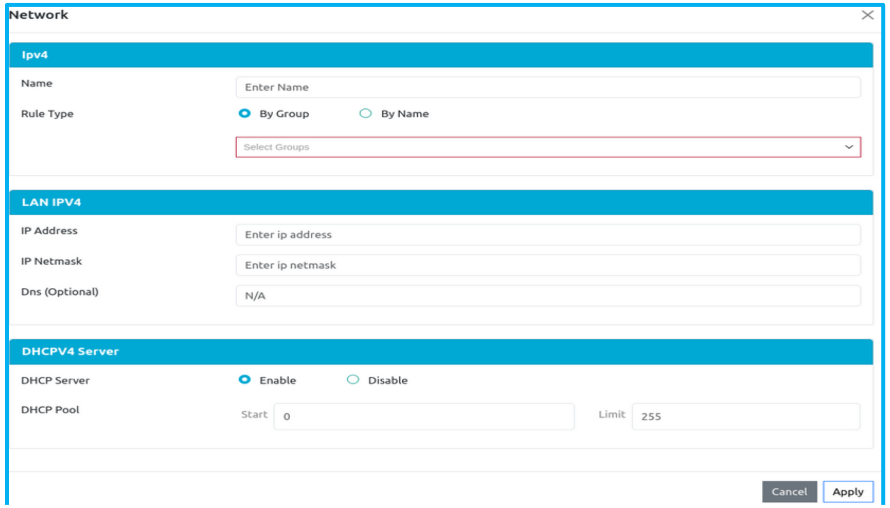
Operator Configuration

Rule Type	● By Group	○ By Name
	Select Groups	
Operator Mode	○ Automatic	● Manual
Operator Type	Short Alphanumeric	
Operator Config		

Network - IPv4

Configuration → Networks → IPv4 → Add

IPv4 is a connectionless protocol, and operates on a best-effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).



Network

Ipv4

Name	Enter Name
Rule Type	● By Group ○ By Name
	Select Groups

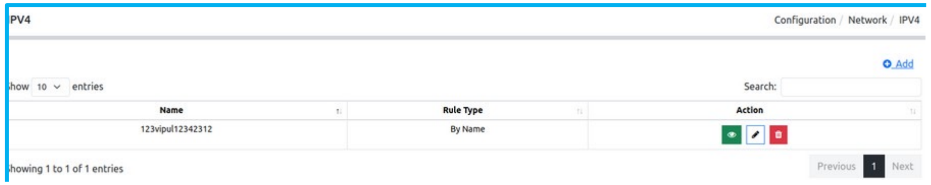
LAN IPV4

IP Address	Enter ip address
IP Netmask	Enter ip netmask
Dns (Optional)	N/A

DHCPV4 Server

DHCP Server	● Enable ○ Disable
DHCP Pool	Start 0 Limit 255

Fill the details and click on Apply button



PV4

Configuration / Network / IPV4

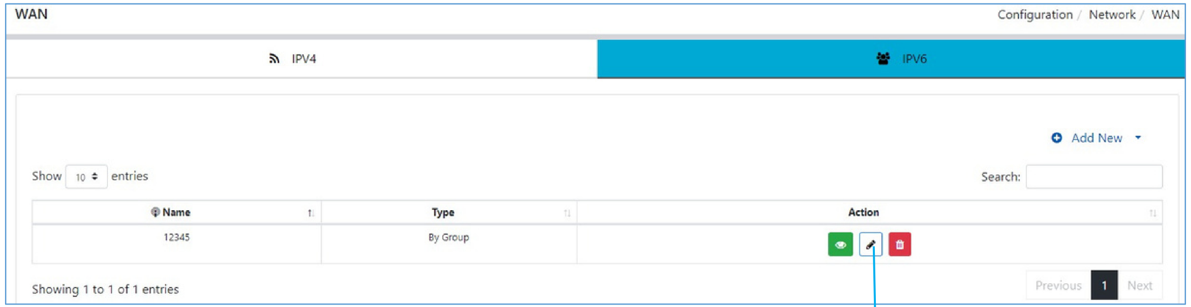
Name	Rule Type	Action
123vipul12342312	By Name	👁 ✎ 🗑

howing 1 to 1 of 1 entries

👁	Click to view the settings.
✎	Click to edit the settings.
🗑	Click to delete the settings.

Network - WAN

Configuration → Network → WAN → IPv6

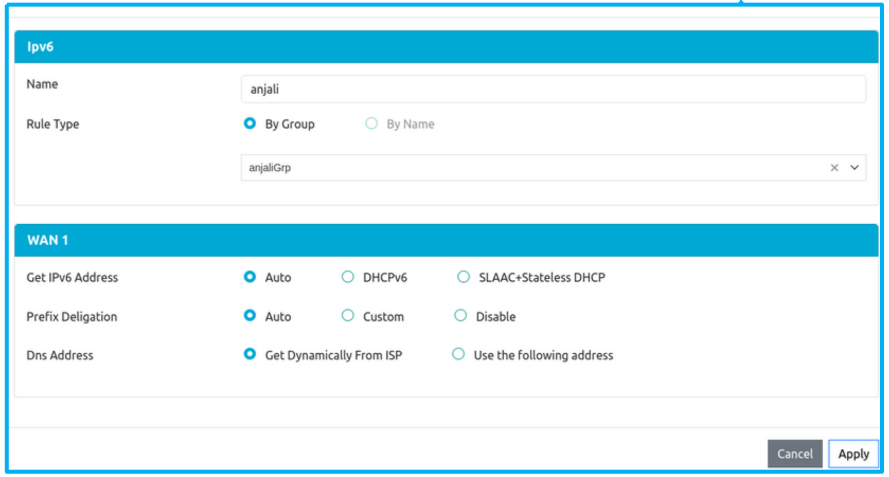


Show 10 entries

Search:

Name	Type	Action
12345	By Group	

Showing 1 to 1 of 1 entries



Name: anjali

Rule Type: ● By Group ○ By Name

anjaliGrp

Get IPv6 Address: ● Auto ○ DHCPv6 ○ SLAAC+Stateless DHCP

Prefix Deligation: ● Auto ○ Custom ○ Disable

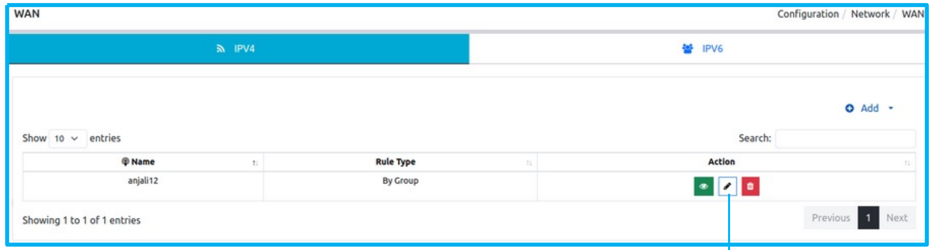
Dns Address: ● Get Dynamically From ISP ○ Use the following address

Name: Enter a specific name for identification.

Rule type: Select either By Group or By Name. And choose Device group if you selected rule type as By Group or Device name if you selected rule type as By Name.

Note: For rest of the fields refer to page no. 50 and 51.

Configuration → Network → WAN → IPv4



WAN

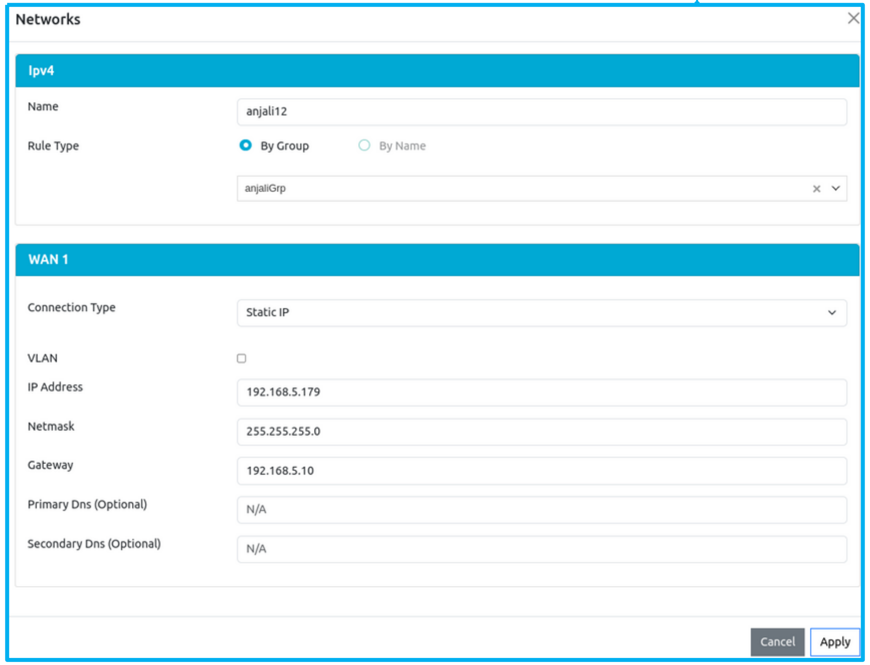
Configuration / Network / WAN

Show 10 entries

Search:

Name	Rule Type	Action
anjali12	By Group	

Showing 1 to 1 of 1 entries



Networks

Ipv4

Name: anjali12

Rule Type: ● By Group ○ By Name

anjaliGrp

WAN 1

Connection Type: Static IP

VLAN: □

IP Address: 192.168.5.179

Netmask: 255.255.255.0

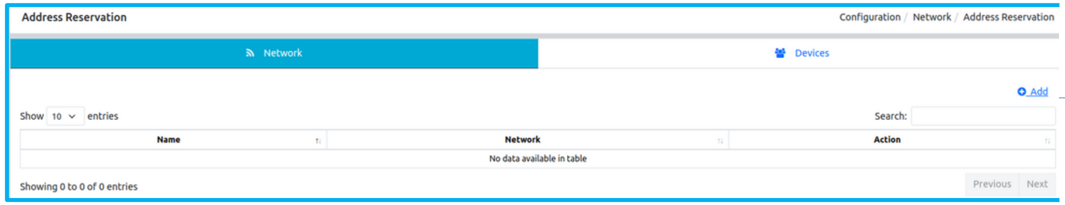
Gateway: 192.168.5.10

Primary Dns (Optional): N/A

Secondary Dns (Optional): N/A

Network - Address Reservation

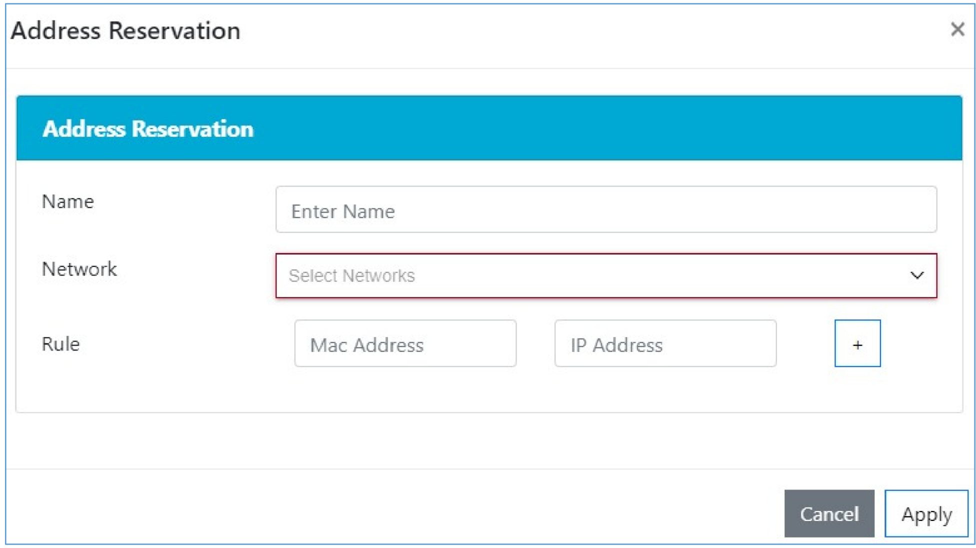
Configuration → Network → Address Reservation → Network



Name	Network	Action
No data available in table		

Showing 0 to 0 of 0 entries

Address Reservation: Address reservation, also known as DHCP reservation, is a feature in DHCP (Dynamic Host Configuration Protocol) where the DHCP server allocates a specific IP address to a device based on its MAC (Media Access Control) address. This ensures that the device consistently receives the same IP address whenever it connects to the network.

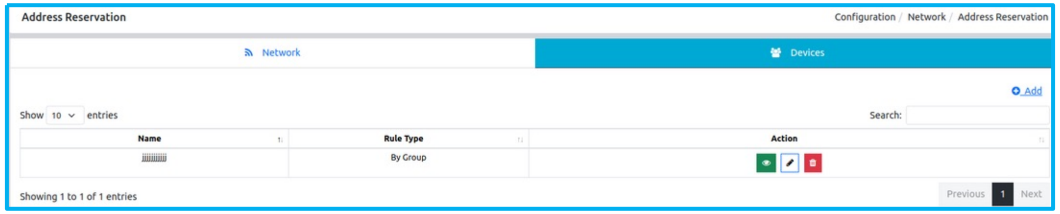


Name: Enter a specific name for identification.

Network: Select network from the dropdown button.

Rule: Input your MAC Address and IP Address. Here you can input multiple MAC and IP Addresses by clicking on +

Configuration → Network → Address Reservation → Devices



Address Reservation

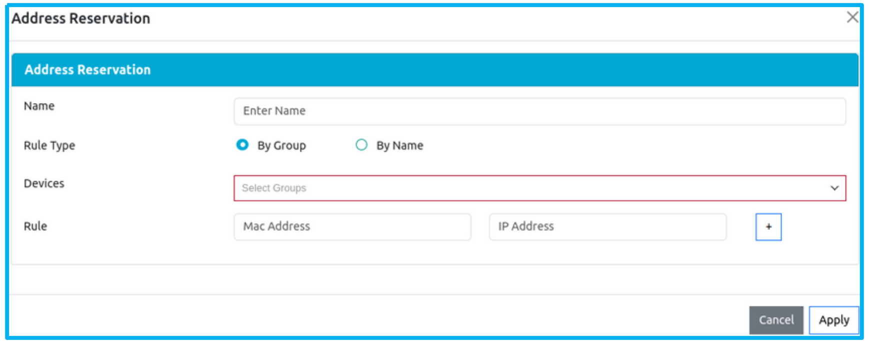
Configuration / Network / Address Reservation

Show 10 entries

Search:

Name	Rule Type	Action
jjjjjjjjjj	By Group	

Showing 1 to 1 of 1 entries



Address Reservation

Address Reservation

Name: Enter Name

Rule Type: ● By Group ○ By Name

Devices: Select Groups

Rule: Mac Address IP Address +

Name: Enter a specific name for identification.

Rule Type: Set Rule type as per your requirement.

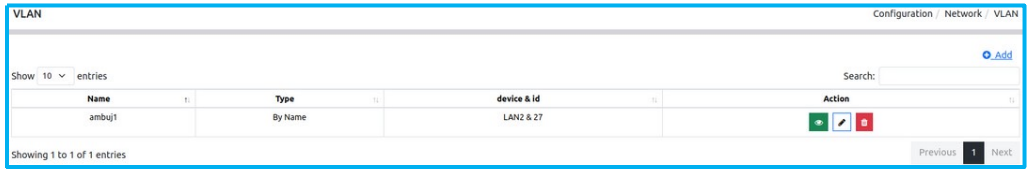
Devices: Select device group if you set the rule type as By Group or device

name if yor set the rule type as By Name from the dropdown button.

Rule: Input your MAC Address and IP Address. Here you can input multiple MAC and IP Addresses by clicking on

Network - VLAN

Configuration → Network → VLAN



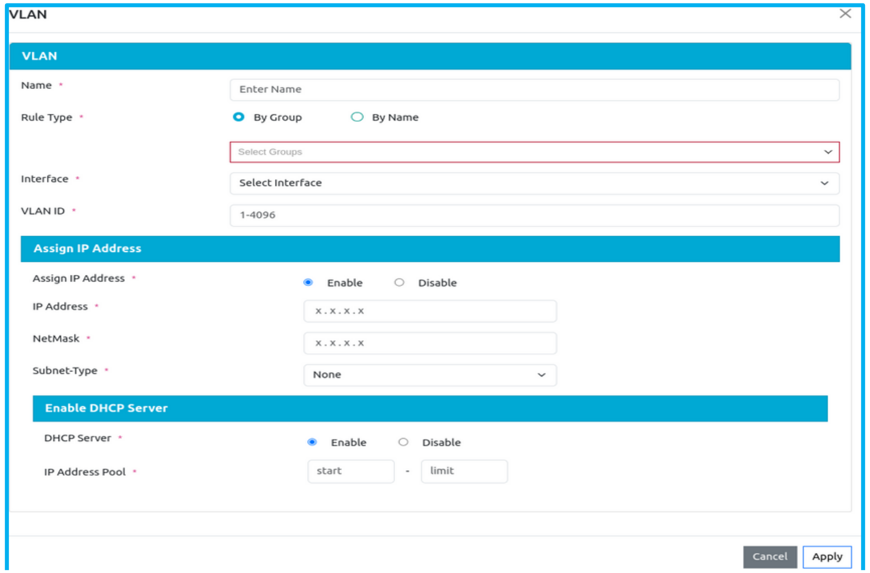
VLAN

Configuration / Network / VLAN

Name	Type	device & id	Action
ambuj1	By Name	LAN2 & 27	

Showing 1 to 1 of 1 entries

VLANs allow you to segment a network into smaller, virtual sub-networks, which can be used to isolate traffic and improve network performance. VLANs are often used in enterprise networks to separate different departments or groups, or to segment different types of traffic (such as voice, data, and video).



VLAN

VLAN

Name * Enter Name

Rule Type * ● By Group ○ By Name

Select Groups

Interface * Select Interface

VLAN ID * 1-4096

Assign IP Address

Assign IP Address * ● Enable ○ Disable

IP Address * x.x.x.x

NetMask * x.x.x.x

Subnet-Type * None

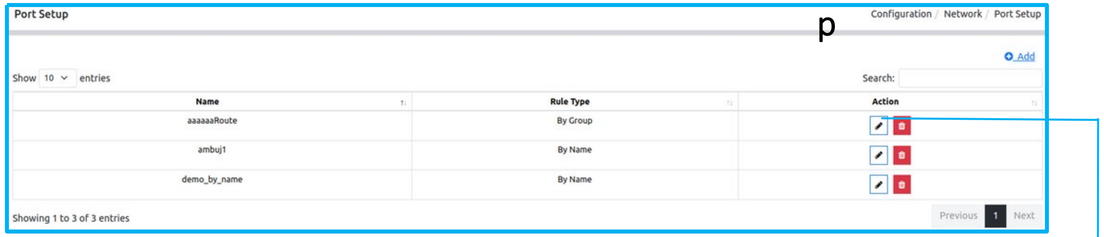
Enable DHCP Server

DHCP Server * ● Enable ○ Disable

IP Address Pool * start - limit

Network - Port Setup

Configuration → Network → Port Setup



Port Setup

Configuration / Network / Port Setup

Add

Show 10 entries

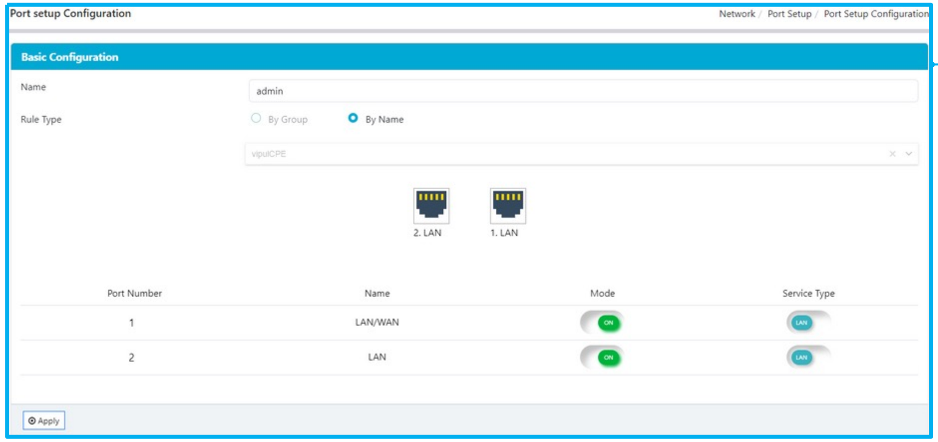
Search:

Name	Rule Type	Action
aaaaaaRoute	By Group	
ambuj1	By Name	
demo_by_name	By Name	

Showing 1 to 3 of 3 entries

Previous 1 Next

By default KCP- 510 device has two port one is LAN and another one is WAN. You can switch one port from LAN to WAN or WAN to LAN. Here you can do the same in Port Setup.



Port setup Configuration

Network / Port Setup / Port Setup Configuration

Basic Configuration

Name: admin

Rule Type: ○ By Group ● By Name

vipulCPE

Port Number	Name	Mode	Service Type
1	LAN/WAN	ON	LAN
2	LAN	ON	LAN

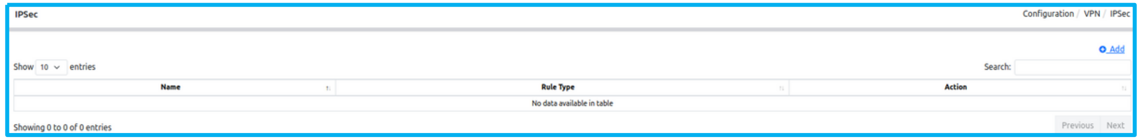
Apply

Here you can set the mode of port whether it is on or off and also can set the service type of LAN and WAN by clicking on the buttons.

VPN - IPSec

Configuration → VPN → IPSec

IPsec (Internet Protocol Security) is a suite of protocols and standards that provide security services for communication at the network layer of the
OSI model. It's widely used to secure communication over IP networks, including the internet. IPsec operates by encrypting and authenticating data to ensure confidentiality, integrity, and authenticity. IPsec provides a robust framework for securing data communication, making it a fundamental tool for network security in the modern digital landscape.



IPSec

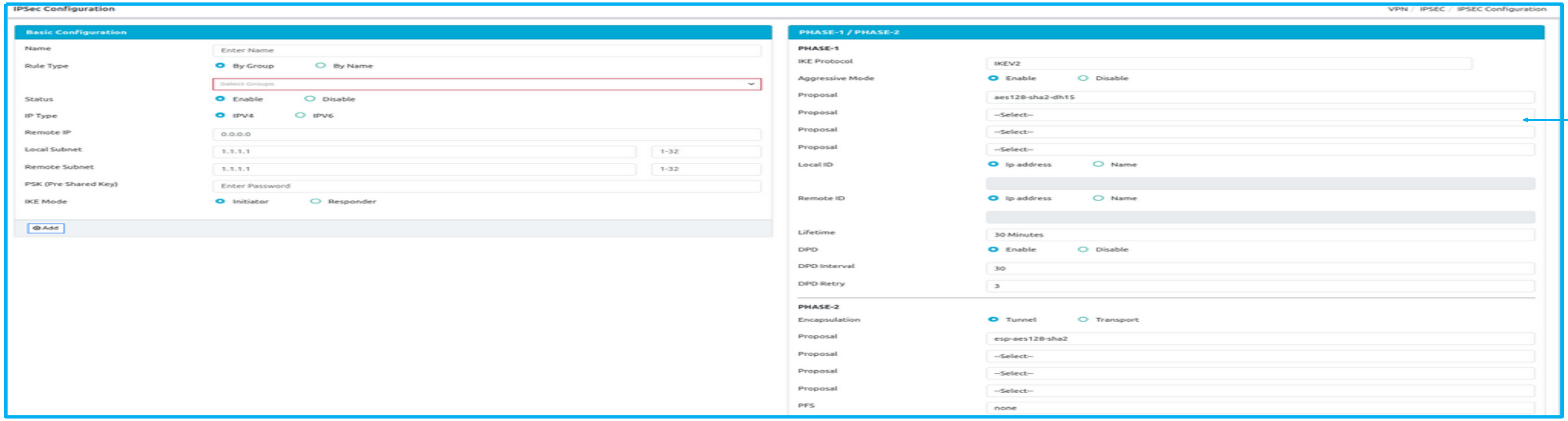
Configuration / VPN / IPSec

Show 10 entries

Search:

Name	Rule Type	Action
No data available in table		

Showing 0 to 0 of 0 entries



IPSec Configuration

VPN / IPSEC / IPSEC Configuration

Basic Configuration

Name: Enter Name

Rule Type: ● By Group ○ By Name

Select Groups

Status: ● Enable ○ Disable

IP Type: ● IPV4 ○ IPV6

Remote IP: 0.0.0.0

Local Subnet: 1.1.1.1 1-32

Remote Subnet: 1.1.1.1 1-32

PSK (Pre Shared Key): Enter Password

IKE Mode: ● Initiator ○ Responder

PHASE-1 / PHASE-2

PHASE-1

IKE Protocol: IKEV2

Aggressive Mode: ● Enable ○ Disable

Proposal: aes128-sha2-dh15

Proposal: --Select--

Proposal: --Select--

Proposal: --Select--

Local ID: ● Ip address ○ Name

Remote ID: ● Ip address ○ Name

Lifetime: 30 Minutes

DPD: ● Enable ○ Disable

DPD Interval: 30

DPD Retry: 3

PHASE-2

Encapsulation: ● Tunnel ○ Transport

Proposal: esp-aes128-sha2

Proposal: --Select--

Proposal: --Select--

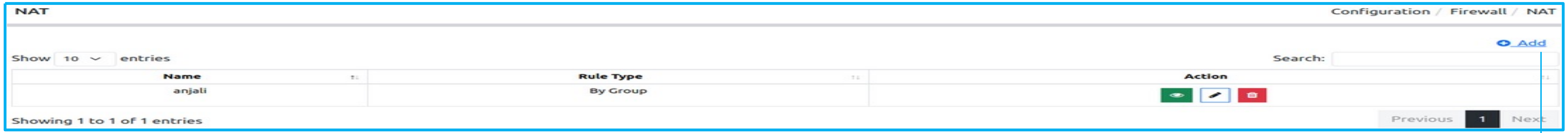
Proposal: --Select--

PFS: none

IKE(Internet Key Exchange): IKE establishes a secure, authenticated communication channel between two parties. IKE negotiates security associations (SAs), which are a set of mutually agreed-upon keys and algorithms used by both parties trying to establish a VPN connection. Here you can select proposals from the drop down. You can select upto four proposals at a time

Firewall - NAT

Configuration → Firewall → NAT



NAT

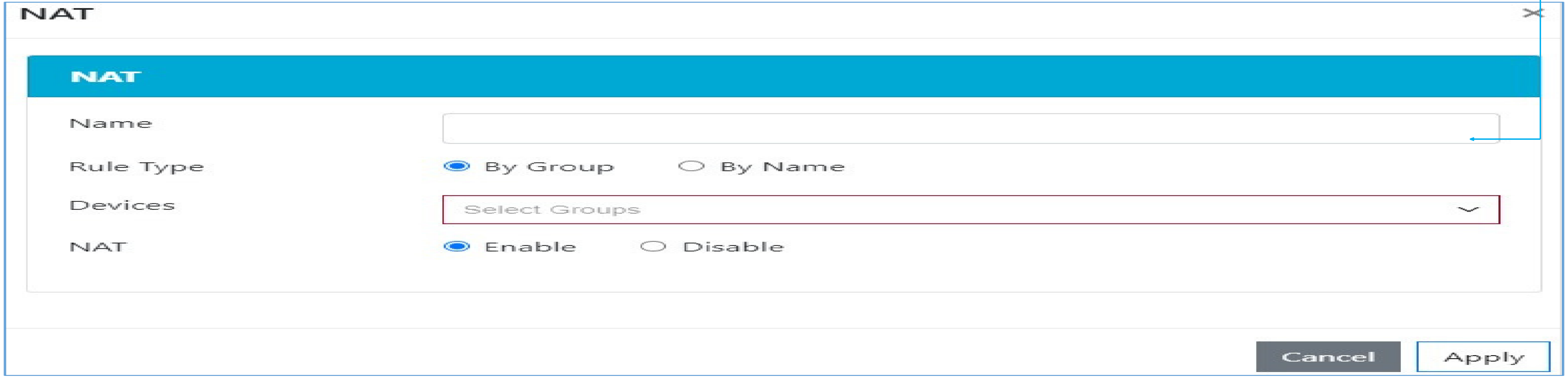
Show 10 entries

Search:

Name	Rule Type	Action
anjali	By Group	

Showing 1 to 1 of 1 entries

NAT, or Network Address Translation, is a crucial component of firewalls and network security. NAT operates at the network layer(Layer 3) of the OSI model and is primarily used to map private IP addresses to public IP addresses. NAT in a firewall is a fundamental tool used to manage and secure communication between a private network and the internet by translating private IP addresses to public IP addresses, thus ensuring efficient and secure data transfer.



NAT

NAT

Name

Rule Type ● By Group ○ By Name

Devices Select Groups

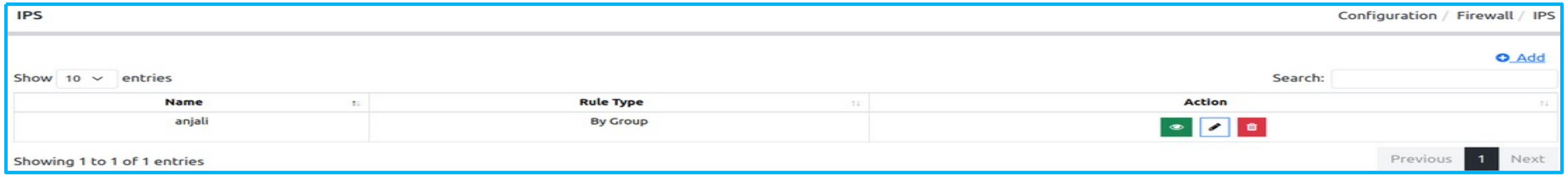
NAT ● Enable ○ Disable

Devices: Select the device group if you selected the Rule type as By Group or select a device name if you selected the Rule type as By Name in which you want add Web GroupFilter.

NAT: Enable NAT if you want to apply NAT service to the selected Devices or Disable it if don’t .

Firewall - IPS

Configuration → Firewall → IPS



IPS

Configuration / Firewall / IPS

Add

Show 10 entries

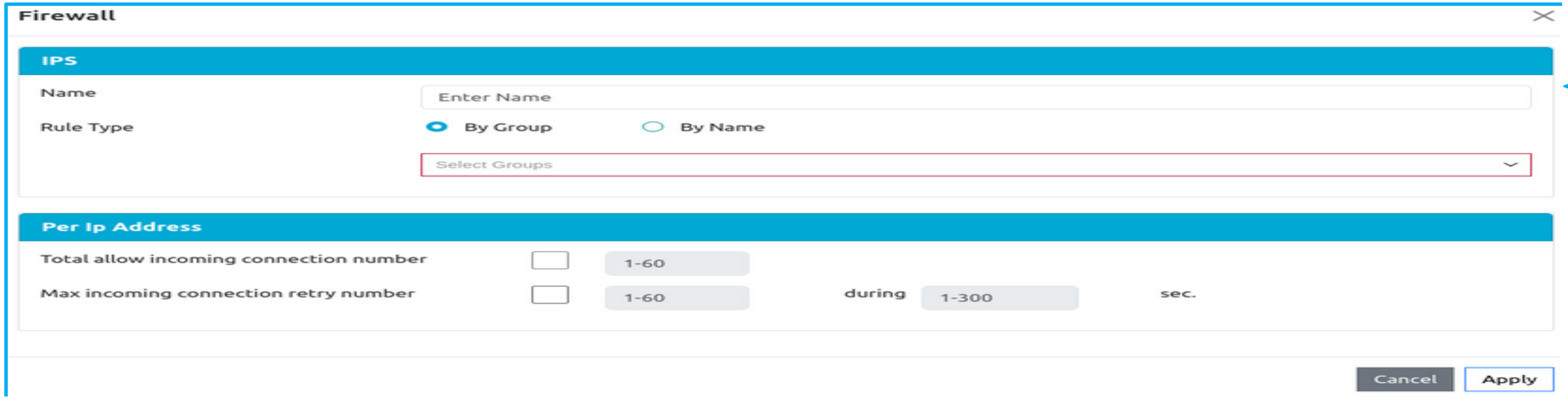
Search:

Name	Rule Type	Action
anjali	By Group	👁 ✎ 🗑

Showing 1 to 1 of 1 entries

Previous 1 Next

IPS, or Intrusion Prevention System, is an advanced security technology commonly integrated into firewalls. It's designed to detect and prevent malicious activities and attacks in a network. It is like having a security guard at the entrance of your network. It constantly checks who's coming in, verifies their credentials (the network packets), and takes action if it detects anything suspicious or malicious, providingan additional level of security and threat prevention.



Firewall

IPS

Name: Enter Name

Rule Type: ● By Group ○ By Name

Select Groups

Per Ip Address

Total allow incoming connection number □ 1-60

Max incoming connection retry number □ 1-60 during 1-300 sec.

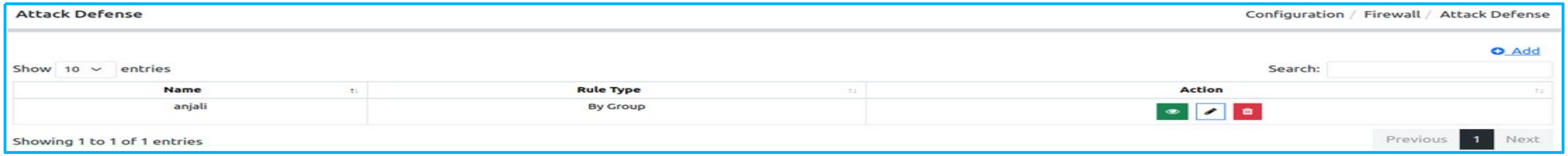
Cancel Apply

Total Allow incoming connection number: The "Total Allow Incoming Connection Number" refers to the maximum permitted number of incoming connections that are considered safe or allowed based on the security policies and configurations set within the IPS.Enable the check box and input your number between 1 to 60.

Max incoming connection retry number: The "Max Incoming Connection Retry Number" typically refers to the maximum number of attempts allowed for establishing a connection with a specific service or resource. When a connection attempt fails, the system or application may retry a certain number of times before considering the connection unsuccessful. Enable the check box and input the number and time. The number should be within 1 to 60 and time should be within 1 to 300 Sec.

Firewall - Attack Defense

Configuration → Firewall → Attack Defense



Attack Defense

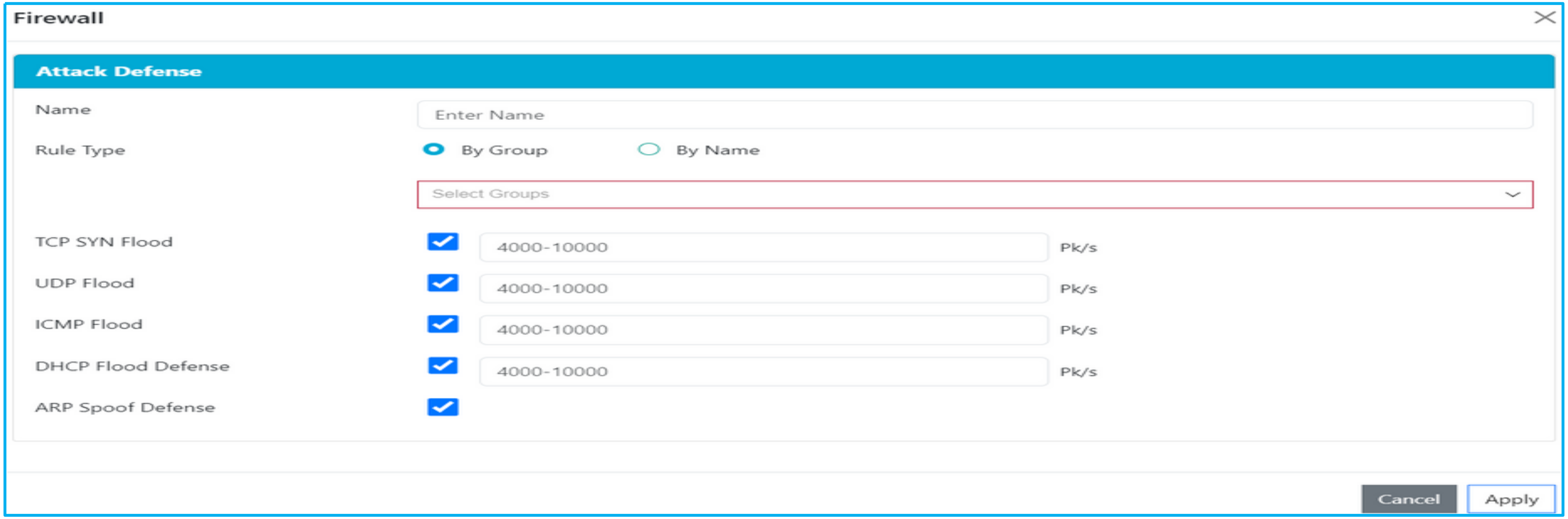
Show 10 entries

Search:

Name	Rule Type	Action
anjali	By Group	👁 ✎ 🗑

Showing 1 to 1 of 1 entries

Attack defense refers to strategies, measures, or mechanisms put in place to protect computer systems, networks, and data from various forms of cyber-attacks. It involves safeguarding against unauthorized access, malicious software, data breaches, and other security threats that could compromise the confidentiality, integrity, or availability of digital assets.



Firewall

Attack Defense

Name	Enter Name	
Rule Type	● By Group ○ By Name	
	Select Groups	
TCP SYN Flood	☑ 4000-10000	Pk/s
UDP Flood	☑ 4000-10000	Pk/s
ICMP Flood	☑ 4000-10000	Pk/s
DHCP Flood Defense	☑ 4000-10000	Pk/s
ARP Spoof Defense	☑	

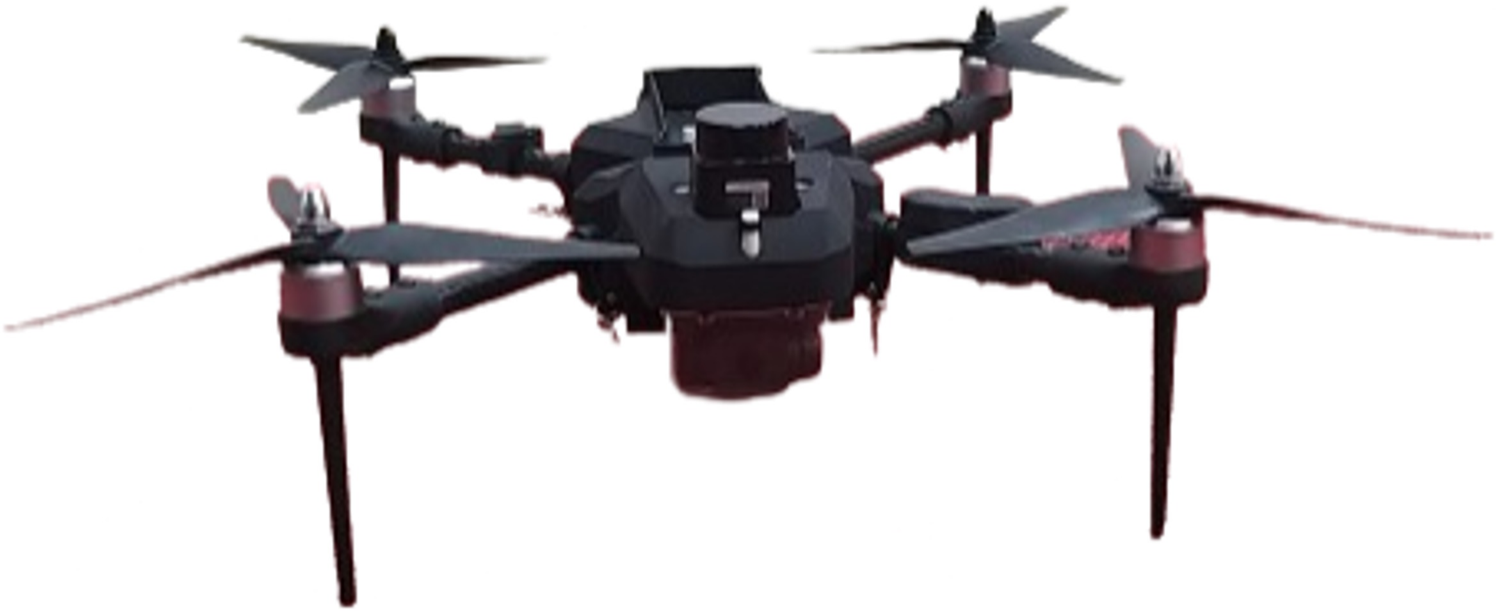
Live Training on 5G CPE

5G LAB

5G LAB

Lunch Break

5G Mini Drone



1. Overview

Suparna control stack runs on autopilot hardware to control drones, UAVs, and other unmanned vehicles. It offers robust capabilities for controlling a wide range of vehicles like multi-copters, fixed-wing, VTOLs, and ground vehicles. Here a quadcopter with autonomous capabilities is presented

2. System Components

The system is composed of several key components that work together to ensure smooth flight operations and management of the vehicle. These components include the Flight Stack, Middleware, Hardware Abstraction, and the Operating System.

3. Flight Stack

The Flight Stack includes the navigation, position estimation, and attitude controllers. It is responsible for ensuring the vehicle follows flight paths, maintains stability, and reaches its intended destination.

4. Middleware

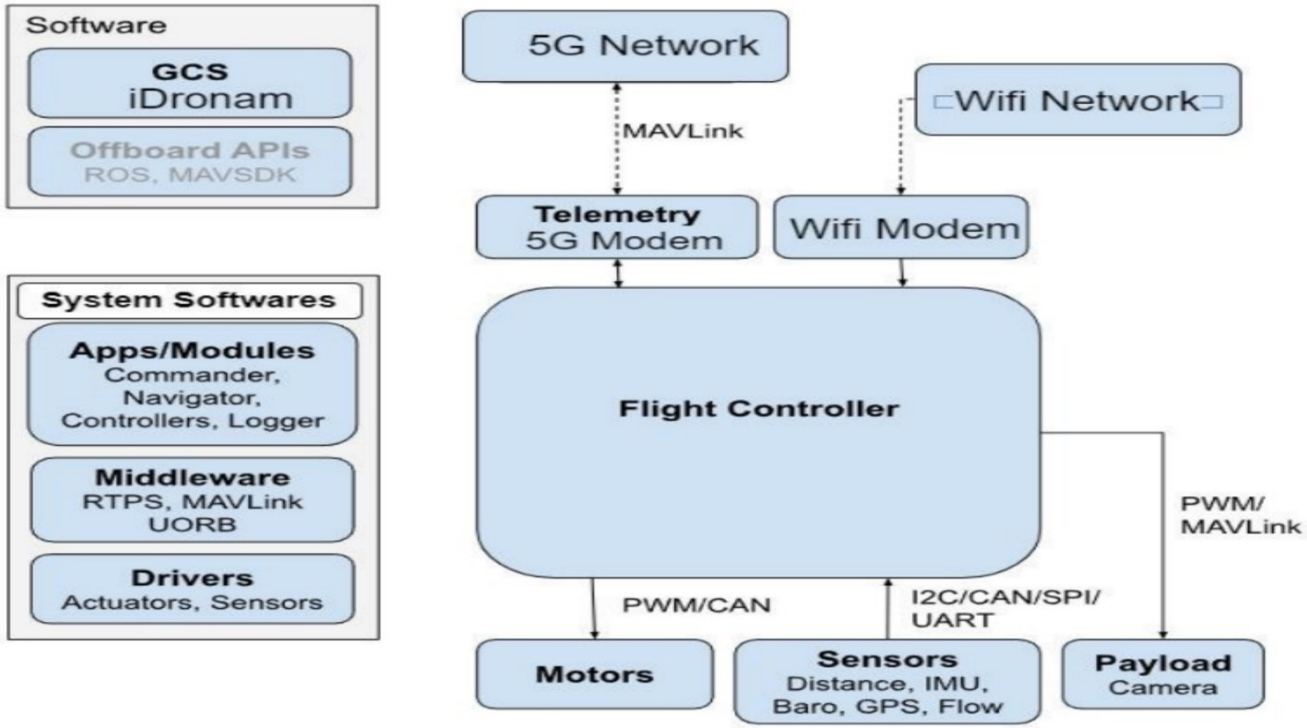
PX4's Middleware facilitates communication between different parts of the system, such as the flight control and sensors. It provides standard interfaces for vehicle components, making the system more modular and extensible.

5. Hardware Abstraction Layer (HAL)

The Hardware Abstraction Layer separates the operating system and hardware-specific implementations from the higher-level flight logic. This ensures that PX4 can run on various autopilot hardware with minimal changes to the software

6. Operating System

The controller is designed to run on top of a real-time operating system, providing low-latency, predictable scheduling required for flight control applications.



Software

GCS
iDronam

Offboard APIs
ROS, MAVSDK

System Softwares

Apps/Modules
Commander,
Navigator,
Controllers, Logger

Middleware
RTPS, MAVLink
UORB

Drivers
Actuators, Sensors

5G Network

MAVLink

□Wifi Network□

Telemetry
5G Modem

Wifi Modem

Flight Controller

PWM/
MAVLink

PWM/CAN

I2C/CAN/SPI/
UART

Motors

Sensors
Distance, IMU,
Baro, GPS, Flow

Payload
Camera

Mission Protocol

The mission sub-protocol allows a GCS or developer API to exchange mission (flight plan), geofence and safe point information with a drone/component.

The protocol covers:

Operations to upload, download and clear missions, set/get the current mission item number, and get notification when the current mission item has changed.

Message type(s) and enumerations for exchanging mission items.

Mission Items ("MAVLink commands") that are common to most systems.

The protocol supports re-request of messages that have not arrived, which allows missions to be reliably transferred over a lossy link.

.

Mission Types

MAVLink 2 supports three types of "missions": flight plans, geofences and rally/safe points. The protocol uses the same sequence of operations for all types (albeit with different types of Mission Items). The mission types must be stored and handled separately/independently.

Mission protocol messages include the type of associated mission in the mission_type field (a MAVLink 2 message extension). The field takes one of the MAV_MISSION_TYPE enum values: MAV_MISSION_TYPE_MISSION, MAV_MISSION_TYPE_FENCE, MAV_MISSION_TYPE_RALLY

Mission Items (MAVLink Commands)

Mission items for all the mission types are defined in the MAV_CMD enum.

MAV_CMD is used to define commands that can be used in missions ("mission items") and commands that can be sent outside of a mission context (using the Command Protocol). Some MAV_CMD can be used with both mission and command protocols. Not all commands/mission items are supported on all systems (or for all flight modes).

The items for the different types of mission are identified using a simple name prefix convention:

Flight plans:

NAV commands (MAV_CMD_NAV_*) for navigation/movement (e.g. MAV_CMD_NAV_WAYPOINT, MAV_CMD_NAV_LAND)

DO commands (MAV_CMD_DO_*) for immediate actions like changing speed or activating a servo (e.g. MAV_CMD_DO_CHANGE_SPEED).

CONDITION commands (MAV_CMD_CONDITION_*) for changing the execution of the mission based on a condition - e.g. pausing the mission for a time before executing next command (MAV_CMD_CONDITION_DELAY).

Geofence mission items:

Prefixed with MAV_CMD_NAV_FENCE_ (e.g. MAV_CMD_NAV_FENCE_RETURN_POINT).

Rally point mission items:

There is just one rally point MAV_CMD: MAV_CMD_NAV_RALLY_POINT.

The commands are transmitted/encoded in MISSION_ITEM or MISSION_ITEM_INT messages. These messages include fields to identify the particular mission item (command id) and up to 7 command-specific optional parameters.

Field Name	Type	Values	Description
commanduint16_t	MAV_CMD		Command id, as defined in MAV_CMD.
param1	float	Param #1.	
param2	float	Param #2.	
param3	float	Param #3.	
param4	float	Param #4.	

param5 (x)	float / int32_t	X coordinate (local frame) or latitude (global frame) for navigation commands (otherwise Param #5).
param6 (y)	float / int32_t	Y coordinate (local frame) or longitude (global frame) for navigation commands (otherwise Param #6).
param7 (z)	float	Z coordinate (local frame) or altitude (global - relative or absolute, depending on frame) (otherwise Param #7).

The first four parameters (shown above) can be used for any purpose - this depends on the particular command. The last three parameters (x, y, z) are used for positional information in MAV_CMD_NAV_* commands, but can be used for any purpose in other commands.

The remaining message fields are used for addressing, defining the mission type, specifying the reference frame used for x, y, z in MAV_CMD_NAV_* messages, etc.:

Field Name	Type	Values	Description
target_system	uint8_t		System ID
target_component	uint8_t		Component ID

seq	uint16_t		Sequence number for item within mission (indexed from 0).
frame	uint8_t	MAV_FRAME	The coordinate system of the waypoint. PX4 support global frames in MAVLink commands (local frames may be supported if the same command is sent via the command protocol).
mission_type	uint8_t	MAV_MISSION_TYPE	Mission type.
current	uint8_t	false:0, true:1	When downloading, whether the item is the current mission item.
autocontinue	uint8_t		Autocontinue to next waypoint when the command completes.

MISSION_ITEM_INT vs MISSION_ITEM

MISSION_ITEM and MISSION_ITEM_INT are used to exchange individual mission items between systems. MISSION_ITEM messages encode all mission item parameters into float parameters fields (single precision IEEE754) for transmission. MISSION_ITEM_INT is exactly the same except that param5 and param6 are Int32 fields.

Protocol implementations must allow both message types in supported operations (along with the corresponding MISSION_REQUEST and MISSION_REQUEST_INT message types).

AR/VR DEVICE

- XR Foundation Features for design and development

- Wireless Connectivity: ADH facilitates establishing a wireless connection between the computer and the AjnaXR headset, eliminating the necessity for cumbersome wired connections.

- • Uninterrupted Testing: Temporarily disabling the proximity sensor and guardian system ensures uninterrupted testing, enabling developers to focus on refining their creations.

- • Visual Debugging: The ADH enables the capturing of screenshots and recording of videos from the headset's perspective, an invaluable aid for debugging purposes.

- • Effortless Deployment: Developers can directly deploy applications from the ADH (PC) to the headset, streamlining the deployment process.

- • Shared Experience: Casting the headset's display to the computer empowers others to partake in the XR experience, fostering collaboration and understanding.

- • Essential Resources: The hub offers the convenience of downloading the latest AjnaVidya Tools and SDKs necessary for XR app development, ensuring developers have the most up-to-date resources. 5

- • Debugging Insights: Creating device logs offers valuable insights for debugging and examination, aiding developers in identifying and addressing issues effectively. In essence, the Ajna Developer Hub (ADH) enriches XR development by providing a centralised platform that enhances efficiency, collaboration, and the overall quality of XR applications.

Benefits of AR/VR for institute

- **1. Immersive Learning & Skill Development**
- Provides hands-on experience in a virtual environment, enhancing understanding.
- Allows students to interact with complex concepts (e.g., medical simulations, engineering designs).
- Enhances soft skills like teamwork and problem-solving through collaborative VR experiences.
- **2. Enhanced Research & Innovation**
- Supports research in AR/VR applications across industries like healthcare, engineering, and gaming.
- Enables real-time data visualization for AI, robotics, and IoT research.
- Facilitates testing and prototyping of new AR/VR applications.
- **3. Safe & Cost-Effective Training**
- Reduces the need for expensive physical equipment by simulating real-world scenarios.
- Provides a safe space for learning hazardous or complex tasks (e.g., surgery, industrial machinery operation).
- Minimizes material wastage in labs (e.g., chemistry experiments in VR).
- **4. Remote Learning & Virtual Collaboration**
- Enables remote access to lab resources through virtual simulations.
- Supports virtual field trips, allowing students to explore historical sites, space, or deep-sea environments.
- Enhances collaboration between students, faculty, and researchers across different locations.
- **5. Industry Readiness & Job Opportunities**
- Prepares students for careers in gaming, architecture, healthcare, and industrial training.
- Helps in developing AR/VR-based solutions for businesses and startups.
- Encourages entrepreneurship and innovation in extended reality (XR) applications.

Live Training With AR/VR Device

5G LAB

Queries ?