Magma Access Gateway

Release Validation Report

Version:1.7_5G-Alpha

Table of Content

1. INTRODUCTION 4
1.1 Purpose of the Document 4
2. ABBREVATIONS 4
3. SETUP 5
3.1 Access Gateway Hardware 5
3.1.1 Physical Gateways 5
3.2 Test tools and Traffic Emulator 5
3.2.1 Test Setup Architecture 5
3.2.2 Test Activity 6
4. Install, Upgrade and Validation 9
4.1 AGW BareMetal Installation 9
4.1.1 Network Type Tested 9
4.2 AGW Upgrade 9
4.2.1 Enable 5G features 10
4.3 ORC8R 11
4.4 Accessing & using Magma nms-UI (User Interface) 11
4.4.1 NMS-UI Validation 14
5. Feature Testing 16
5.1 General Procedures 16
5.1.1 NGAP Connection Establishment 16
5.1.2 Registration 17
5.1.3 Connection Management 18
5.1.4 PDU session management 20
6. Stability and PERFORMANCE Testing 21
6.1 Stability Testing 21
6.1.1 Traffic Emulator 21
6.1.2 Test Activity on Spirent 22
6.2 PERFORMANCE 23
7. Test Report from CI pipeline 24
7.1 Test Activity on Abot 25
7.2 List of Abot TC running in CI 26
7.3 Magma CI dashboard 26
8. Real Equipment Testing-SIT 26
8.1 Test Activity on Real Device (UE) 27
8.2 List of Test Case 29

9. REFERENCES 29

LIST OF FIGURES

Figure 1: Magma 5G SA – Test Topology 6
Figure 2: Basic Call Flow with SUCI 7
Figure 3: Basic Call Flow with GUTI 8
Figure 4: Active/Idle mode tests 9
Figure 5: Curl-API showing 5G Flag Disabled 10
Figure 6: Showing only 4G is UP 10
Figure 7: Curl-API After enabling 5G 10
Figure 8: Showing both 4G & 5G up 10
Figure 9: Adding User 11
Figure 10: Subscribers Overview Page 12
Figure 11: Adding Subscribers 12
Figure 12: Gateway Check-Ins 13
Figure 13: Alert Rules 13
Figure 14: Metrics Grafana Dashboard View 14
Figure 15: Test Activity on Viavi TeraVM 16
Figure 16: High level block diagram for the emulated setup for a NAT setup 21
Figure 17 High level block diagram for the emulated setup for a DHCP setup 22
Figure 18: Test Activity on Spirent 23
Figure 19: Spirent GUI 400Mbps traffic Graph 24
Figure 20: Test Report from CI pipeline 25
Figure 21: Test Activity on Abot 25
Figure 22: Magma CI dashboard 26
Figure 23: Test Activity on Real Device 27
Figure 24: UE in Aeroplan mode 27
Figure 25: UE with 5G Signal Detected 28
Figure 26: Traffic sent by UE after PDU Establishment 28

LIST OF TABLES

Table 1: Physical Gateway Specifications 5
Table 2: AGW Upgrade actions and Commands 9
Table 3: NMS Validation 16
Table 4: NGAP Connection 16
Table 5: Registration 18
Table 6: Service Request Procedure 19
Table 7: Paging Procedure 20
Table 8: PDU Session Management Procedure 21
Table 9: Performance 23
Table 10: Performance with Description & Duration 24
Table 11: List of Abot TC 26
Table 12: Real Equipment Testing 29

PREFACE

This document is the 1.7 release version of Magma core and it is created to examine more about 5G in magma.

Note: *For 5G there is no release version before, but for 4G 1.6 release version is available.*

Version Information

Title	Magma Access Gateway
Document Ver. No.	V 1.7_5G-Alpha
Approved By	
Drafted by	
Doc. Classification	

Version History

Version #	Date	Author(s)	Approved by	Description
1.0	17-Mar-2022	Parthiban Nalliamudali / Neelima K		Initial Report

1. INTRODUCTION

1.1 Purpose of the Document

The purpose of this document is to enable 5G in the magma 5G Core and validate 5G procedures using different testing tools (Rebaca ABot, Viavi Teravm, Spirent, etc.,). It also has the test reports from each tool.

2. ABBREVATIONS

#	Abbreviations	Expansions
1	AGW	Access Gateway
2	TVM	Teravm
3	UE	User Equipment
4	BW	Bandwidth
5	SUCI	Subscription Concealed Identifier
6	GUTI	Globally Unique Temporary ID
7	SCTP	Stream Control Transmission Protocol
8	NGAP	NG Application Protocol
9	NMS	Network Management Station
10	NAS	Non-access stratum
11	AMF	Access and Mobility Management Function
12	AN	Access Network
13	RRC	Radio Resource Control
14	3GPP	3rd Generation Partnership Project
15	CM	Centimeter wave
16	RAN	Radio Access Network
17	NG-RAN	NG Radio Access Network
18	5GMM	5G Mobility Management
19	PDU	Protocol Data Unit
20	TC	Test Cases
21	SMF	Session Management Function
22	APN	Access Point Name
23	DNN	Data Network Name
24	QOS	Quality of Service
25	NAT	Network Address Translation

3. SETUP

Here it shows the Test SETUP for Access Gateway where the main services/procedures are validated are done.

3.1 Access Gateway Hardware

- Below is the list of Access Gateway Hardware.

3.1.1 Physical Gateways

Item	Description
CPU	X86_Intel_4 Cores_Speed 1.91 GHz
RAM	8 GB
Storage	60.00 GB

Table 1: Physical Gateway Specifications

3.2 Test tools and Traffic Emulator

- Viavi Teravm is a UE and Gnb simulators along with automation framework to test functional/features of Magma 5GC.
- Spirent is used as a traffic emulator to do performance testing.
- Abot from Rebaca is used for Functional/features validation by automating testcases and it is used in the CICD daily regression.

3.2.1 Test Setup Architecture

- Below diagram represents the Magma 5G SA test topology. Here Magma AGW is connected with AWS public cloud orchestrator (Hosted by Wavelabs).
- From Orchestrator the information is saved in subscriber DB of Magma 5GC. AMF gets the information from subscriber DB and give to SMF.

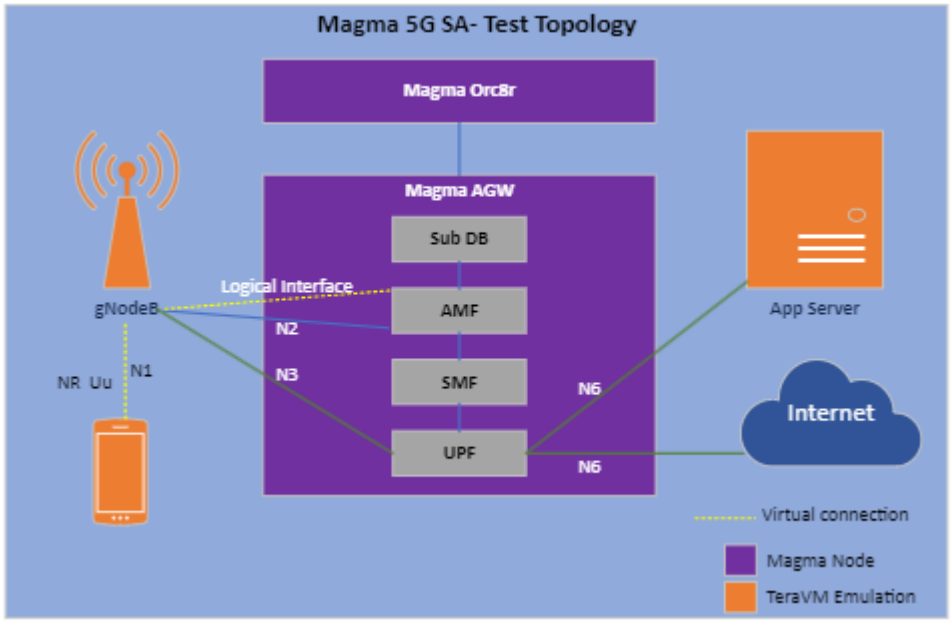

Figure 1: Magma 5G SA – Test Topology

- UPF takes care of all data plane and allows packet processing & traffic aggregation which is to be performed closer to the network edge, increasing bandwidth efficiencies while reducing network load.
- AMF receives all connection and session related information from the UE, but is responsible only for handling connection and mobility management tasks.
- Once the registration is completed, PDU establishment request comes in and internally AMF sends the request to SMF and SMF fetches the APN or Policy information.
- Once the sessions are up or it is successful, SMF sends the session related information to UPF and traffic is triggered over the session.

3.2.2 Test Activity

- Below are the different call flows that are supported in Magma 5GC.
  - Basic Call Flow with **SUCI**
  - Basic Call Flow with **GUTI**
  - Active/Idle mode tests

3.2.2.1 Basic Call Flow with SUCI

- SUCI allows SUPI to be signaled without exposing the identity of the user.
- When the testcase is triggered, it initiates an INITIAL_UE_MESSAGE that is received

from UE to AMF, which is for connection establishment. Now a new registration request comes in and it is processed internally.

- During the registration procedure, internally Authentication and Security mode commands are triggered.
- Once the Authentication Request & Response and Security mode is done, user sends the context request to gNodeB and accept the UE, so that UE moves to registered connected mode. i.e., UE registration is completed.
- After completion of the registration, the PDU-Establishment is triggered.
- PDU-Establishment request comes from UE and PDUSessionResourceSetupRequest, DL NAS transport and PDU session establishment accept messages are sent by AMF. Once this is completed the traffic is triggered.
    - PDUSessionResourceSetupRequest is for gnodeb to allocate the resources for the UE-Context.
    - PDUSessionResourceSetupResponse is the response from gnodeb, with this PDU-Establishment is finished and traffic is started.
- Once the traffic session is completed, the PDU-Release is done.
- After completion of PDU-Release, the De-Registration is done.

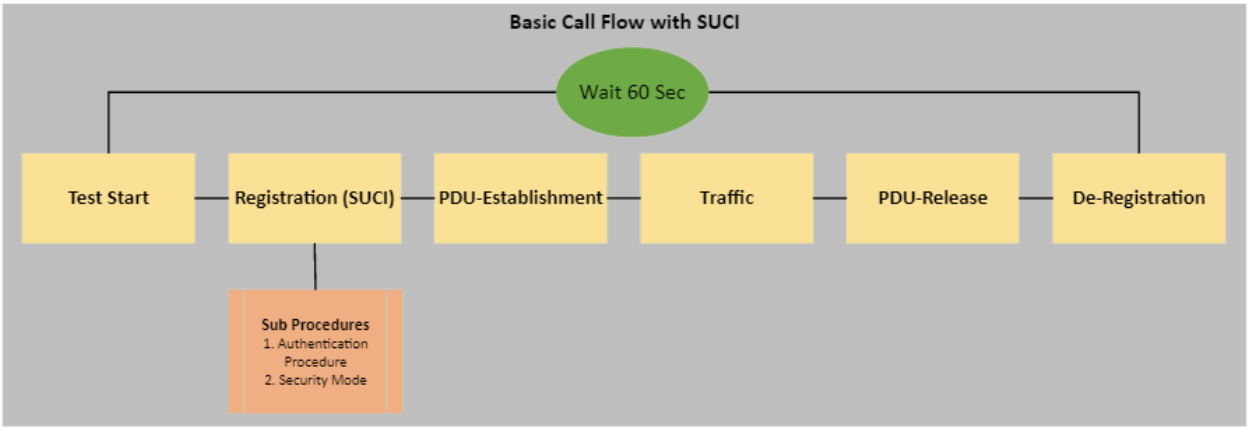

Figure 2: Basic Call Flow with SUCI

3.2.2.2 Basic Call Flow with GUTI

- When the testcase is triggered, it initiates an INITIAL_UE_MESSAGE that is received from UE to AMF, which is for connection establishment. Now a new registration request comes in and it is processed internally.
- Here during the registration procedure, internally Identity mode, Authentication and Security mode commands are triggered.
- Once the Identity Request & Response, Authentication Request & Response and Security mode is done, user sends the context request to gNodeB and accept the UE,

so that UE moves to registered connected mode. i.e., UE registration is completed.

- After completion of the registration, the PDU-Establishment is triggered.
- PDU-Establishment request comes from UE and PDUSessionResourceSetupRequest, DL NAS transport and PDU session establishment accept messages are sent by AMF. Once this is completed the traffic is triggered.
    - PDUSessionResourceSetupRequest is for gnodeb to allocate the resources for the UE-Context.
    - PDUSessionResourceSetupResponse is the response from gnodeb, with this PDU-Establishment is finished and traffic is started.
- Once the traffic session is completed, the PDU-Release is done.
- After completion of PDU-Release, the De-Registration is done.

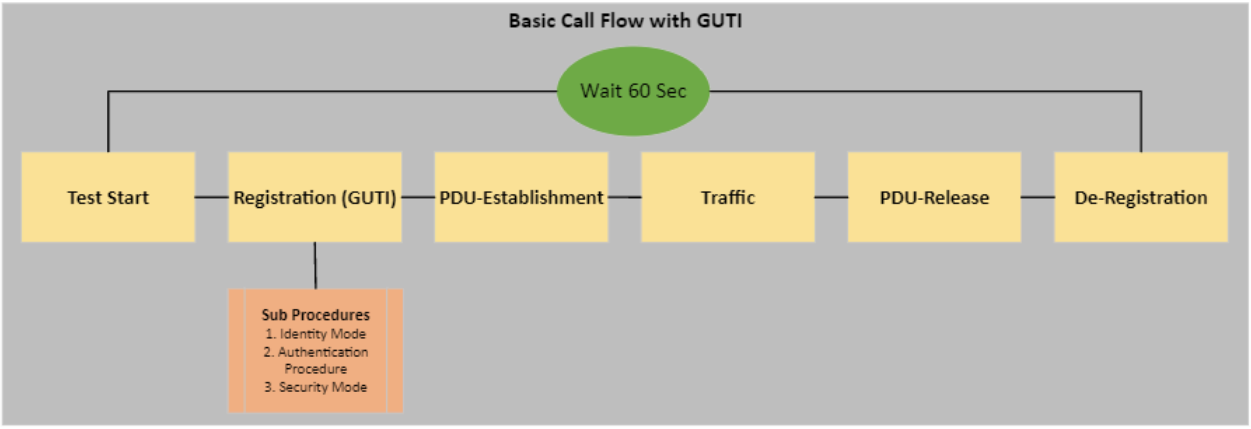

Figure 3: Basic Call Flow with GUTI

3.2.2.3 Active/Idle mode tests

- When the testcase is triggered, it initiates an INITIAL_UE_MESSAGE that is received from UE to AMF, which is for connection establishment. Now a new registration request comes in and it is processed internally.
- During the registration procedure, internally Authentication and Security mode commands are triggered.
- Once the Authentication Request & Response and Security mode is done, user sends the context request to gNodeB and accept the UE, so that UE moves to registered connected mode. i.e., UE registration is completed.
- After completion of the registration, the PDU-Establishment is triggered.
- PDU-Establishment request comes from UE and PDUSessionResourceSetupRequest, DL NAS transport and PDU session establishment accept messages are sent by AMF. Once this is completed the traffic is triggered.
    - PDUSessionResourceSetupRequest is for gnodeb to allocate the resources for

the UE-Context.

- PDUSessionResourceSetupResponse is the response from gnodeb, with this PDU-Establishment is finished and traffic is started.

- If UE does not having any traffic to send over session after inactive timer expiry, then it moves to idle mode, in idle mode if there is uplink traffic, then the service request procedure is triggered and if there is downlink traffic, then paging procedure is triggered and the PDU-Release is done.
- After completion of PDU-Release, the De-Registration is done.

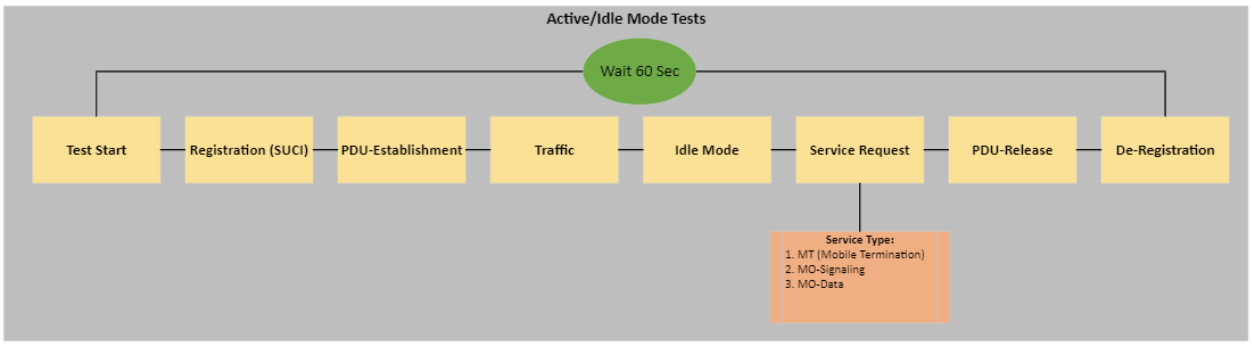

Figure 4: Active/Idle mode tests

4. Install, Upgrade and Validation

4.1 AGW BareMetal Installation

Step.1 Install AGW 1.7.0.

Step.2 Download and run using the below URL.

wget https://raw.githubusercontent.com/magma/magma/master/lte/gateway/deploy/agw_install_ubuntu.sh

4.1.1 Network Type Tested

- NAT (Network Address Translation) is a way to map multiple local private addresses to a public address before transferring the information. Organization which wants multiple devices to employ a single IP address uses the NAT (As like home routers).
- Basic Non-NAT testing is done and extensive testing is in progress.

4.2 AGW Upgrade

- Access Gateway upgrade path is from V1.6 to V1.7.

Actions	Commands Used
To Check the Installed version	apt list –installed | grep magma

To check the latest package in the master-ci	apt-cache madison magma
To Upgrade/Update to the latest Master Build	sudo apt update sudo apt-get install magma
To Update to specific Version in Master-CI	sudo apt-get install magma=Version_Number

Table 2: AGW Upgrade actions and Commands

4.2.1 Enable 5G features

- In below screen shot the Curl API shows, **enable 5G feature flag** as **"False"** and in this API the 5G features can be enabled.

```
{
  "cloud_subscriberdb_enabled": false,
  "congestion_control_enabled": true,
  "default_rule_id": "default_rule_1",
  "enable5g_features": false,
  "gx_gy_relay_enabled": false,
  "hss_relay_enabled": false,
  "lte_auth_amf": "gAA=",
  "lte_auth_op": "EREREREREREREREREREREQ==",
  "mcc": "001",
  "mnc": "01",
  "mobility": {
    "enable_multi_apn_ip_allocation": true,
    "enable_static_ip_assignments": true,
    "ip_allocation_mode": "NAT",
    "nat": {
      "ip_blocks": [
        "192.168.0.0/16"
      ]
```

Figure 5: Curl-API showing 5G Flag Disabled

- Below is the **sctp** port output where it shows only 4G, i.e., only 4G port (36412) is up.

```
ubuntu@rupa-agw:~$ sudo netstat -l | grep sctp
sudo: unable to resolve host rupa-agw: Name or service not known
sctp                172.16.5.150:36412                          LISTEN
unix  2      [ ACC ]     STREAM     LISTENING     23420362 ///tmp/sctpd_downstream.sock
unix  2      [ ACC ]     STREAM     LISTENING     23425258 ///tmp/sctpd_upstream.sock
```

Figure 6: Showing only 4G is UP

- To enable 5G features, user must **enable 5G feature flag** as **"True"**, which gets reflected in the config file of AGW via orchestrator (5G AGW comes up with 5G ports).
- In below screen shot the Curl API shows **enable 5G feature flag** as **"True"** and in this API the 5G features are enabled.

```
{
  "cloud_subscriberdb_enabled": false,
  "congestion_control_enabled": true,
  "default_rule_id": "default_rule_1",
  "enable5g_features": true,
  "gx_gy_relay_enabled": false,
  "hss_relay_enabled": false,
  "lte_auth_amf": "gAA=",
  "lte_auth_op": "EREREREREREREREREREREQ==",
  "mcc": "001",
  "mnc": "01",
  "mobility": {
    "enable_multi_apn_ip_allocation": true,
    "enable_static_ip_assignments": true,
    "ip_allocation_mode": "NAT",
    "nat": {
      "ip_blocks": [
        "192.168.0.0/16"
      ]
```

Figure 7: Curl-API After enabling 5G

- Below is the **sctp** ports output which shows both 4G and 5G ports are up. (36412 for 4G and 38412 for 5G)

```
ubuntu@rupa-agw:~$ sudo netstat -l | grep sctp
sudo: unable to resolve host rupa-agw: Name or service not known
sctp                172.16.5.150:38412                                      LISTEN
sctp                172.16.5.150:36412                                      LISTEN
unix  2      [ ACC ]     STREAM     LISTENING     23350954 ///tmp/sctpd_downstream.sock
unix  2      [ ACC ]     STREAM     LISTENING     23353150 ///tmp/sctpd_upstream.sock
```

Figure 8: Showing both 4G & 5G up

4.3 ORC8R

- Magma's Orchestrator is a centralized controller for a set of networks. Orchestrator handles the control plane for various types of gateways in Magma. Orchestrator functionality is composed of two primary components.
    - A standardized, vendor-agnostic northbound REST API which exposes configuration and metrics for network devices
    - A southbound interface which applies device configuration and reports device status
- Click here to know more about Orchestrator.
- Click here for orchestrator installation guide.

4.4 Accessing & using Magma nms-UI (User Interface)

- Magma NMS provides an enterprise grade GUI for provisioning and operating magma based networks. It enables operators to create and manage:
    - Organizations
    - Networks
    - Gateways and eNodeBs
    - Subscribers
    - Policies and APNs

Step.1 Add Users.

- ✔ New users to NMS can be added or edited through the admin page.
- ✔ Users can be configured as a superuser/user/readonly user.

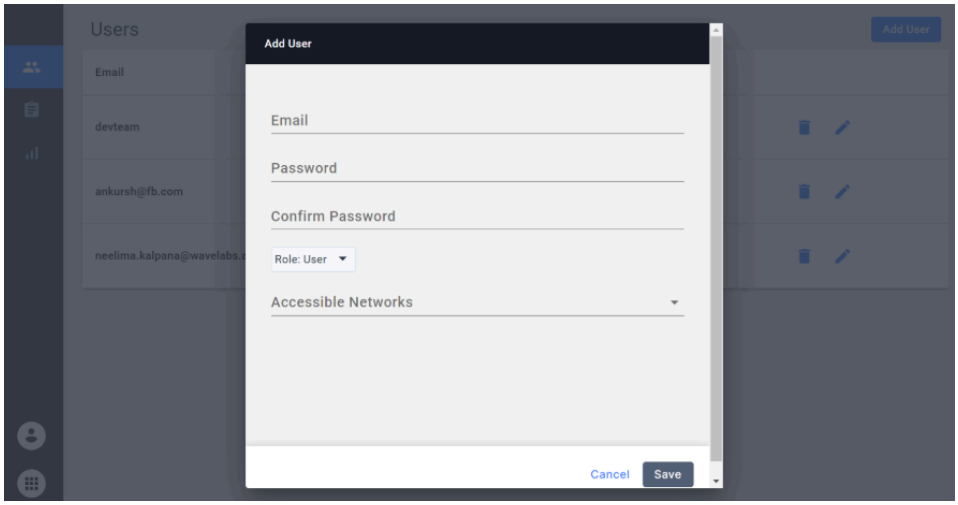

Figure 9: Adding User

Step.2 Subscriber configuration.

- ✔ The Subscriber Overview page contains a table listing all subscribers in the network.
- ✔ Subscriber configuration in the overview page provides the ability to do bulk provisioning of subscribers by either entering the details manually or uploading them through a subscriber .csv file.
- ✔ Clicking on the 'Add subscriber' button in the subscriber overview page opens the bulk subscriber configuration page.

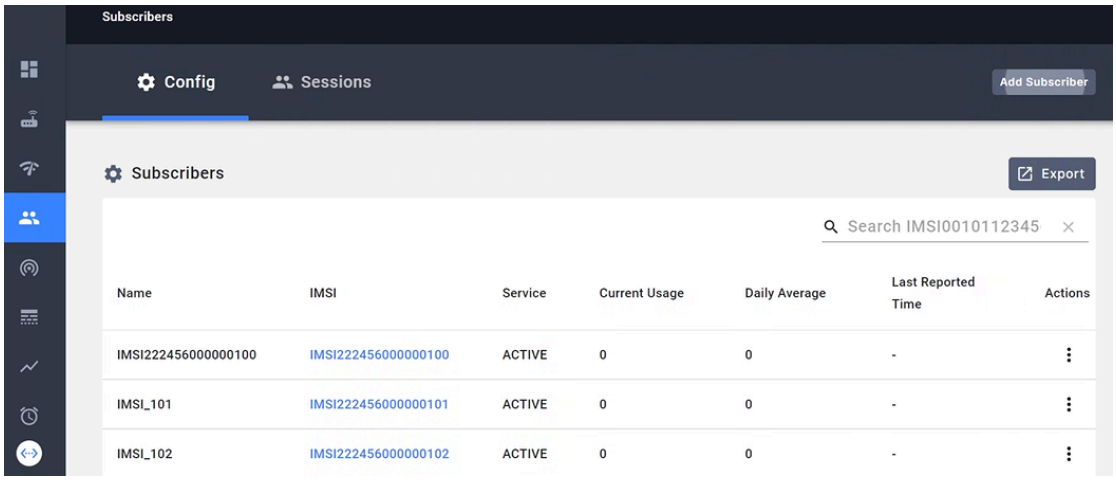

Figure 10: Subscribers Overview Page

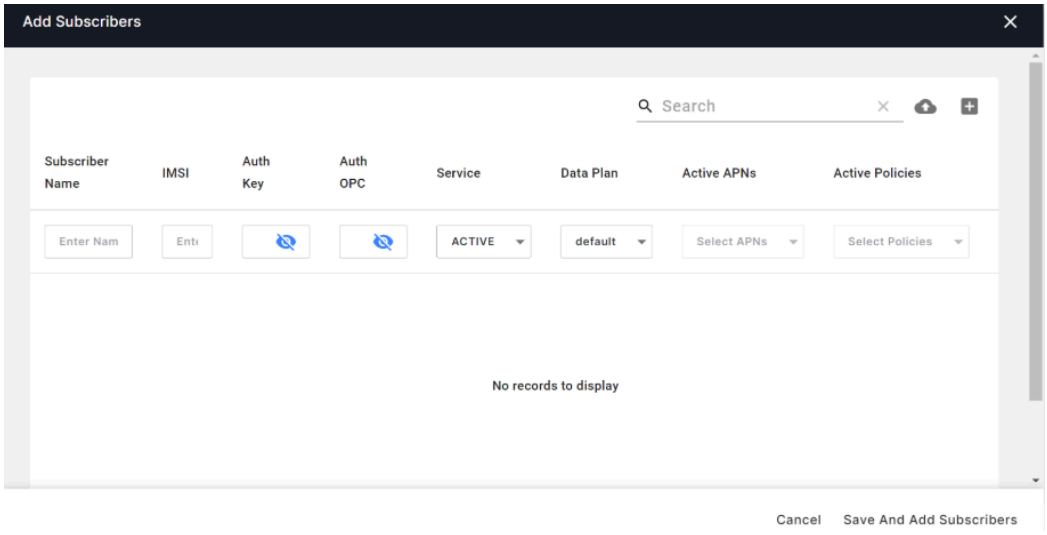

Figure 11: Adding Subscribers

Step.3 Check-in Gateway.

- ✔ Gateway overview table with a selector is to view either **status** or **upgrade** of the gateways in the network.
- ✔ Click on **Add New** button to add a new access gateway in the network.

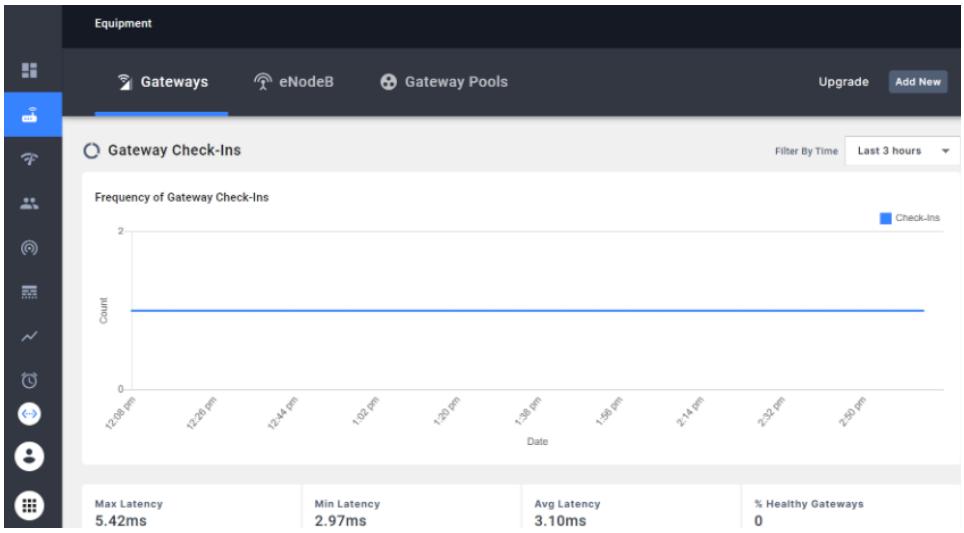

Figure 12: Gateway Check-Ins

Step.4 Sync predefined alerts.

- ✔ Magma NMS comes loaded with some default set of alert rules. These default rules are not configured automatically. If an operator chooses to use these default rules, then they can do it by clicking on “Sync Predefined Alerts” button in Alert rule configuration tab.

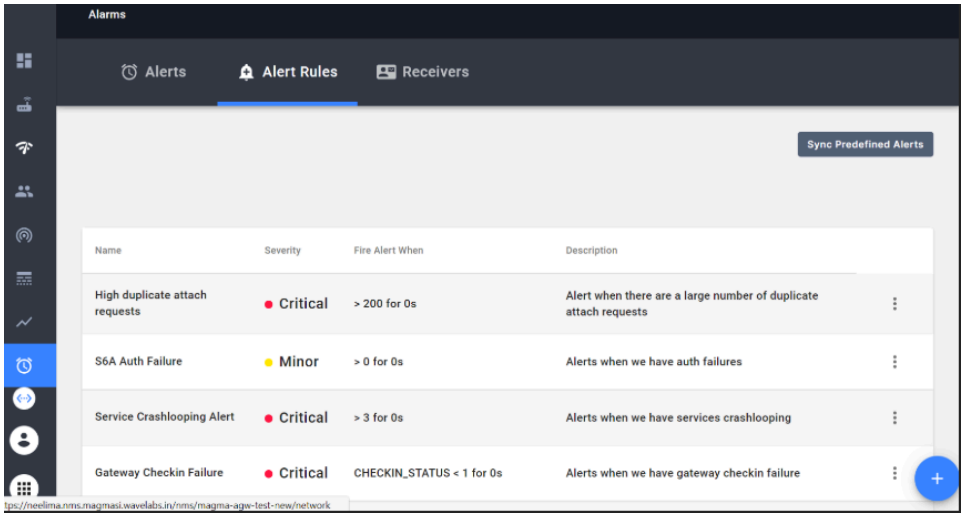

Figure 13: Alert Rules

Step.5 Metrics-Grafana dashboard.

- ✔ Metrics Grafana dashboards contain dropdown selectors to choose which network(s) and gateway(s) user wants to look at.
- ✔ In Grafana, user can look at any collection of networks or gateways which their organization has access to it.

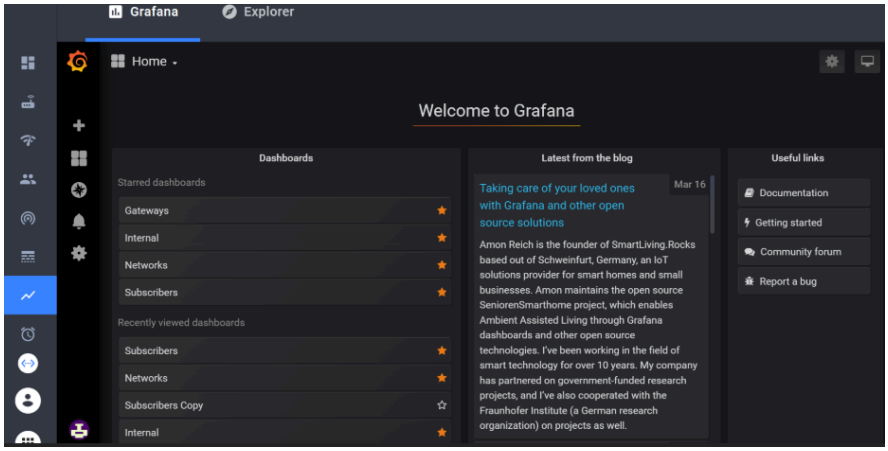

Figure 14: Metrics Grafana Dashboard View

4.4.1 NMS-UI Validation

- NMS (Network Management Station) is a part of Orchestrator and it is a multitenancy where user can add organization and the network.

Testcase ID	Test Scenario	Result
TC1	NMS - Create an organization	Pass
TC2	NMS - Administrative tools -Create a user	Pass
TC3	NMS - Administrative tools -Audit log	Pass

TC4	NMS - Administrative tools -Create a network	Pass
TC5	NMS - Network -Create a network	Pass
TC6	NMS - Network -Edit network	Pass
TC7	NMS - Network -Edit Epc	Pass
TC8	NMS - Network -Edit Ran	Pass
TC9	NMS - Equipment - Gateway -Create a gateway	Pass
TC10	NMS - Equipment – Gateway-Create an eNodeB	Pass
TC11	NMS - Equipment – Gateway-Create a gatewaypool	Pass
TC12	NMS - Subscriber -Create a subscriber	Pass
TC13	NMS - Subscriber -Configure subscriber	Pass
TC14	NMS - Subscriber -Session subscriber	Pass
TC15	NMS - Subscriber -Edit a subscriber	Pass
TC16	NMS - Subscriber -Edit a traffic policy	Pass
TC17	NMS - Subscriber -Edit an APN static IPs	Pass
TC18	NMS - Subscriber-Overview-Overview of subscribers,Status, Datausage	Pass
TC19	NMS - Subscriber-Overview-Overview of subscribers	Pass
TC20	NMS - Subscriber-Overview-Status	Pass
TC21	NMS - Subscriber-Overview-Datausage	Pass
TC22	NMS - Subscriber-Event-Create an Event	Pass
TC23	NMS - Traffic – Policies-Create a profile	Pass
TC24	NMS - Traffic - Policies -Create a policy	Pass
TC25	NMS - Traffic - Policies -Create a Rating group	Pass
TC26	NMS - Traffic – APNs-Create an APN	Pass
TC27	NMS - Traffic – APNs-Modify an APN	Pass
TC28	NMS - Network -Modify a network	Pass
TC29	NMS - Network -Enable NAT	Pass
TC30	NMS - Network -Enable DHCP	Pass
TC31	NMS - Network -Enable Static IP	NA
TC32	NMS - Network -Enable policy Enforcement	NA
TC33	NMS - Equipment - Gateway -Modify a gateway	Pass

TC34	NMS - Equipment -Gateway overview-Overview of Gateway	Pass
TC35	NMS - Equipment -Gateway status-Enable event aggregation	Pass
TC36	NMS - Equipment -Gateway status-Enable log aggregation	Pass
TC37	NMS - Equipment – eNodeB-Add a managed eNodeB	Pass
TC38	NMS - Equipment - Gateway Configure-Edit Aggregation	Pass
TC39	NMS - Equipment - Gateway Configure-Edit EPC	Pass
TC40	NMS - Equipment - Gateway Configure-Edit RAN	Pass
TC41	NMS - Equipment - Gateway Configure-Edit Header Enrichment	Pass
TC42	NMS - Equipment - Gateway Configure-Edit Dynamic services	Pass
TC43	NMS - Call Tracing -Create call trace	Pass
TC44	NMS - Call Tracing -Download call trace	Pass
TC45	NMS - Metrics -Check Metrics	Pass
TC46	NMS - Metrics -Check Grafana	Pass
TC47	NMS – Metrics-Configure Metric Explorer	Pass
TC48	NMS - Alerts -Configure Alerts	Pass
TC49	NMS - Alerts -View Alerts	Pass
TC50	NMS - Alerts Rules-Add Alert rules	Pass
TC51	NMS - Alerts - receivers -Configure Alert receivers	Pass
TC52	NMS - Alerts -Sync Predefined Alerts	Pass

Table 3: NMS Validation

5. Feature Testing

- Feature Testing is to explain all procedures and sub procedures that are tested as part of Magma 5G SA Alpha- V1.7 release.

Test Activity on Viavi TeraVM

- Have Access Gateway installed with V1.7 or upgrade it from the older version to V1.7 (Refer section 4.2 for AGW Upgrade)
- Configure both UE and AMF. From UE perspective user must change the IMSI value and the authentication keys.
- Once the Test is started, all procedures are triggered inside the testcase and cleanup happens.
- When the TC execution is done, it will either be pass or fail and user collects all logs and finish the process. If it is not done, then it goes to inconclusive mode.

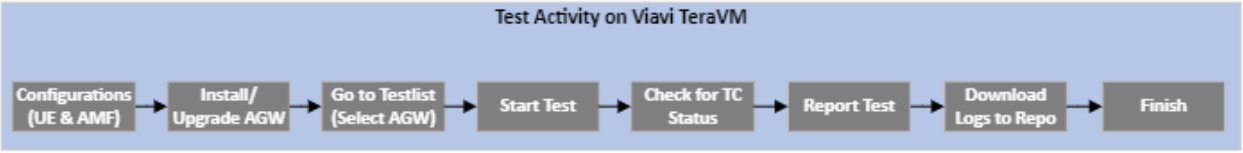

Figure 15: Test Activity on Viavi TeraVM

5.1 General Procedures

5.1.1 NGAP Connection Establishment

- Below table gives the list of test cases that are tested using Viavi Teravm test tool.
- NGAP connection between the Network entities.

Software Build info		1.7.0-1647047113-6937a1c1
NGAP Connection		
Test Case ID	**Test Scenario**	**Result**
TC53	Verify SST = 01 in Ngap Setup	Pass
TC53a	Verify SST by setting non "01" in NgAP Setup Request	Pass

Table 4: NGAP Connection

5.1.2 Registration

- A UE must register with the network to get authorized to Receive services, to enable mobility tracking and reachability.
- The scenarios tested as part of Registration are as follows.
  - Initial Registration to the 5GC
    - ✔ Initial Registration type is supported in Magma: SUCI, GUTI and SUPI.
  - Periodic Registration Update (Due to a predefined period of inactivity)
    - ✔ Perform Periodic Registration Update procedure is triggered by expiration of the periodic update and timer to notify the network whether the UE is still active or not.
    - ✔ Periodic Registration can be triggered either in UE-Idle Mode or UE-Connected Mode.
  - Registration failure scenarios
    - ✔ Registration Rejection
    - ✔ Authentication Rejection
    - ✔ Security mode Rejection

Software Build info		1.7.0-1647047113-6937a1c1
Scenarios Related to Registration		
Test Case ID	**Test Scenario**	**Result**
TC1	UE Initiated Registration Procedures - SUCI as id (UE and AMF	Pass

	Interactions- NAS) - Single gNB	
TC1a	Loop SUCI Registration with Single UE	Pass
TC1b	UE Initiated Registration Procedures - SUCI as id (UE and AMF Interactions- NAS) - Multiple gNB(upto 12 2) & Multiple UE (2 n)	Pass
TC6	Hyper Guti No PDU	Pass
TC6a	Loop Subsequent GUTI Registration with Single UE	Pass
TC6b	Concurrent GUTI Registration with 2 UE	Pass
TC6c	Concurrent GUTI Registration with 2 UE (Mix of Valid + Invalid UE Reg - no subdb)	Pass
TC1d	Concurrent SUCI Registration with 2 UE (Mix of Valid + Invalid UE Reg)	Pass
TC8	UE initiated Periodic Registration	Pass
TC8b	UE initiated Periodic Registration - Idle Mode	Pass
TC13	Verify T3550 Expiry Reg Complete Accept Failure	Pass
TC14	Verify T3560 expiry and Retransmission of AUTHENTICATION REQUEST	Pass
TC14b	Verify T3560 expiry and Retransmission of Security Mode cmd	Pass
TC15	Verify *T3570* expiry and Retransmission of IDENTITY REQUEST message	Pass
TC18a	Registration-Reject - Cause #6 – Illegal UE	Pass
TC18c1	Registration-Reject - Cause #23 - UE Security Capability Mismatch	Pass
TC18c2	With out ue security capabilities IE in initial registration request	Pass
TC18c3	With UE security capabilities IE, but all bits are Zero, means ue don’t support any algorithm	Pass
TC18d	Periodic Registration Reject - Cause #23 - UE Security Capability Mismatch	Pass
TC18g	Authentication Failure on Resync with cause 21	Pass
TC43a	Verify Authentication Reject with "Cause #20 – MAC failure"	Pass
TC43c	Verify Authentication Reject with Cause #26 – Non-5G authentication unacceptable	Pass
TC43d	Verify Authentication Reject with "Cause #24 – Security mode rejected, unspecified"	Pass
TC43e	Verify Authentication Reject with "Cause #23 – UE security capabilities mismatch"	Pass
TC43f	Verify Successfull Authentication After Resync	Pass
TC43g	Verify Security Mode Reject with Cause 24 Security mode rejected	Pass

	unspecified	
TC43h	Verify Security Mode Reject with Cause 23 UE security capabilities mismatch	Pass

Table 5: Registration

5.1.3 Connection Management

- Connection management contains the function of establishing and releasing a NAS signaling connection between a UE and the AMF over N1.
- The NAS signaling connection is used to enable NAS signaling exchange between the UE and the core network and it also includes;
  - The AN signaling connection between the UE and the AN (RRC Connection over 3GPP access or UE-N3IWF connection over N3GPP access)
  - The N2 connection for the UE between the AN and the AMF.

5.1.4.1 CM-IDLE Mode

- Below are two CM states used to reflect the NAS signaling Connection of the UE with the AMF.
  - ❖ CM-IDLE
    - ✔ A UE in CM-IDLE state has no NAS signaling connection established with the AMF over N1.
    - ✔ There are no AN signaling connection, N2 connection and N3 connections for the UE in the CM-IDLE state.
  - ❖ CM-CONNECTED
    - ✔ UE in CM-CONNECTED state has a NAS signaling connection with the AMF over N1.
    - ✔ NAS signaling connection uses a RRC Connection between the UE & the NG-RAN.
    - ✔ NGAP UE associates between the AN and the AMF for 3GPP access.
  - ❖ Service Request procedure
    - ✔ The purpose of the service request procedure is to change the 5GMM mode from 5GMM-IDLE to 5GMMCONNECTED, and/or to request the establishment of user-plane resources for PDU sessions which are established without user-plane resources.

Software Build info	1.7.0-1647047113-6937a1c1
Service Request Scenarios	
Test Case ID	**Test Scenario**	**Result**
TC7	UE Idle Mode Support (Service Request- Mo Signaling)	Pass
TC7a	Verify “PDU session establishment” after Service Request – Signaling & Service Accept	Pass

TC7b	UE Idle Mode Support (Service Request - MO Data) + PDU session	Pass
TC7c	Verify Service Reject for SReq-MO Signaling	Pass
TC7c2	Verify Service Request - Mo Signaling without UE context release - Change the RAN-UE-NGAP-ID in Service Req	Pass
TC7d	Verify Service Reject for SReq-MO Data	Pass
TC7e	Verify Service Reject cause-#9 after max retry of Registration accept	Pass
TC7f	Verify Service Reject when wrong TMSI is used in Service Request	Pass

Table 6: Service Request Procedure

- ❖ Paging procedure
  - ✔ The network initiates the paging procedure for 5GS services when NAS signaling messages or user data is pending to send to the UE in 5GMM-IDLE mode over 3GPP access.

Software Build info	1.7.0-1647047113-6937a1c1
Paging Procedures	
Test Case ID	**Test Scenario**	**Result**
TC9	AMF Initiated Paging	Pass
TC9a	Verify T3513 and Max Paging retry	Pass
TC9b	Verify_Paging_reponse_in_last_paging_Retry	Pass

Table 7: Paging Procedure

5.1.4 PDU SESSION MANAGEMENT

- The SMF is responsible for the session management functions to provide the PDU connectivity service to the UE by the SM signaling between UE and SMF.
- The session management procedures include;
  - The UE-requested PDU session establishment procedure;(Supported)
  - The PDU session authentication and authorization procedure;(Supported)
  - The UE-requested PDU session modification procedure; (Can be supported in upcoming release))
  - The network requested PDU session modification procedure;(Can be supported in upcoming release)
  - The UE-requested PDU session release procedure; (Supported)
  - The network requested PDU session release procedure (Can be supported in upcoming release)

Software Build info	1.7.0-1647047113-6937a1c1

5G End-to-End basic call flow		
Test Case ID	**Test Scenario**	**Result**
TC1d	Concurrent SUCI Registration with 2 UE (Mix of Valid + Invalid UE Reg)	Pass
TC6a	Loop Subsequent GUTI Registration with Single UE	Pass
TC6b	Concurrent GUTI Registration with 2 UE	Pass
TC6c	Concurrent GUTI Registration with 2 UE (Mix of Valid + Invalid UE Reg - no subdb)	Pass
TC7a	Verify "PDU session establishment" after Service Request – Signaling & Service Accept	Pass
TC7b	UE Idle Mode Support (Service Request - MO Data) + PDU session	Pass
TC9	AMF Initiated Paging	Pass
TC9a	Verify T3513 and Max Paging retry	Pass
TC9b	Verify_Paging_reponse_in_last_paging_Retry	Pass
TC33	Attempt UE Registration when initial context response was not sent to AMF on the previous registration request	Pass
TC34	Attempt UE Registration when security mode completion was not sent to AMF in the previous registration attempt	Pass
TC35	Attempt UE registration. Before UE registration is complete, Send periodic registration update request to AMF	Pass
TC36	Attempt UE registration. Before UE registration is complete, Send Deregistration request to AMF	Pass
TC66	Skip UeContextRequest in InitialUE and verify UE Inactivity flow	Pass
TC67	Skip UeContextRequest in InitialUE and verify PDU est flow	Pass

Table 8: PDU Session Management Procedure

Note: *Click here to find the test results and the debug logs of the above test cases.*

6. Stability and PERFORMANCE Testing

6.1 Stability Testing

- Stability Testing is a type of Software Testing to check the quality and behavior of the software in different environmental parameters. It is defined as the ability of the product to continue to function over time without failure. Here, the test runs with maximum number of UEs, with

maximum session and supported throughput for long duration.

6.1.1 Traffic Emulator

- Traffic Emulator is a tool where stress data is validated and reported with server functionalities.
- Below diagram is Spirent setup where scale test is performed. Here the Emulated UEs, Emulated server and Emulated gNodeBs are the Spirent Landslide 5G which is connected with the lab network, and the lab network is connected with Magma Access Gateway.
- Eth1 interface is connected with AGW and Eth0 is connected with Orchestrator.
- From Eth0 to lab network traffic signals are sent, this interface is used for GTP interface. (GTP is the UPF path)
- Eth0 is connected with lab node, where GTP interface gets created and PDU session is established and traffic flows via this interface (Eth0 to Lab Network).

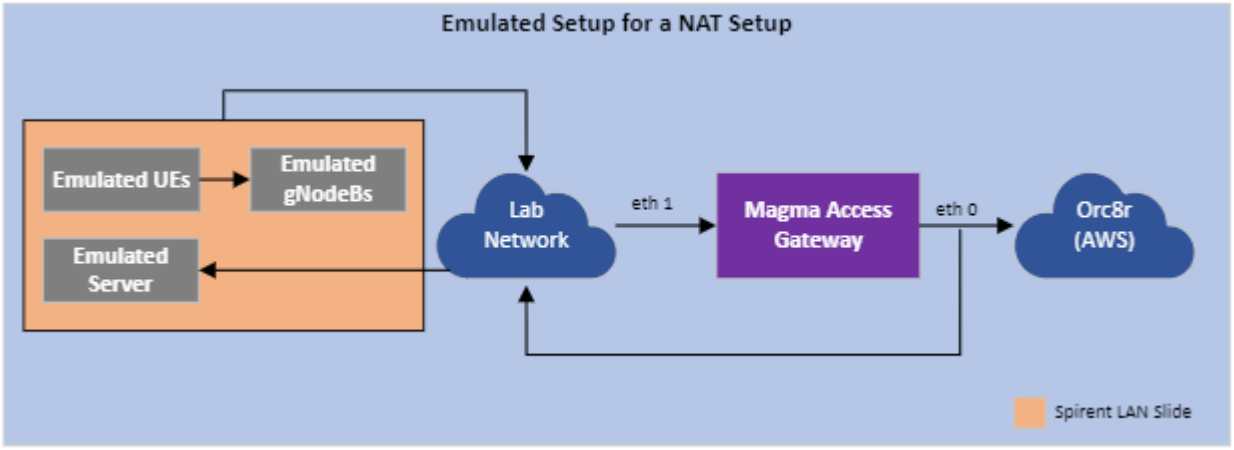

Figure 16: High level block diagram for the emulated setup for a NAT setup

- Below diagram is with DHCP server and it is with NAT disabled.
- Here when a user wants to communicate with any entity which is out of his/her domine or Network, there will be a router which sits before the main router.
- Based on the destination IP address, the NAT reads it and translates the source to the particular destination network IP address where the two source and destination are reachable.

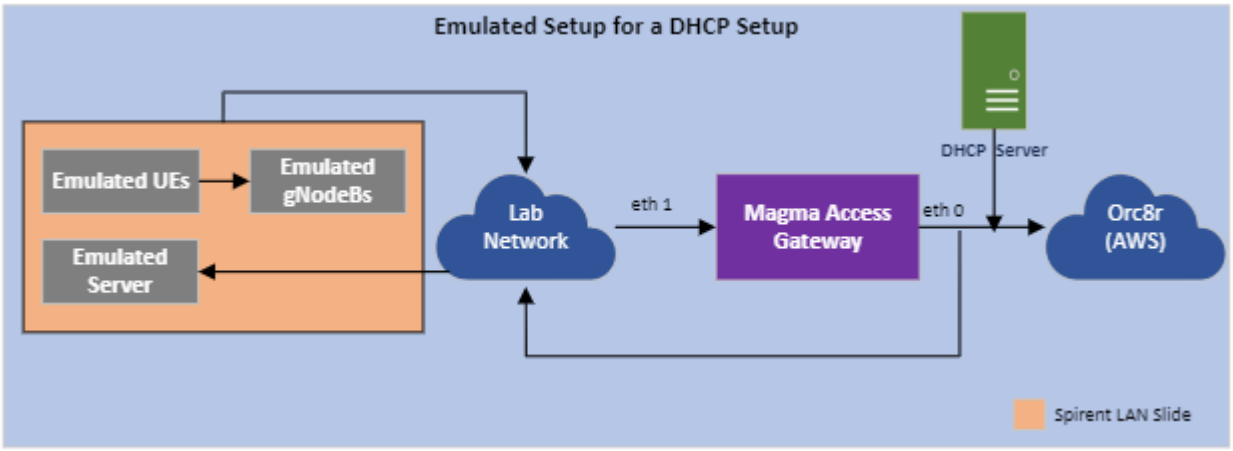

Figure 17 High level block diagram for the emulated setup for a DHCP setup

6.1.2 Test Activity on Spirent

- Have Access Gateway installed with V1.7 or upgrade it from the older version to V1.7 (Refer Section 4.2 for AGW Upgrade)
- Verify whether all the 5G ports and the magma services are running successfully.
- Below are the commands used to verify all magma services and SCTP ports status are active or not.
  - Magma services: *sudo service magma@* status*
  - 5G Port:
    - *sudo netstat -a | grep sctp*
    - *cat /proc/net/sctp/eps*
- When the test case runs, all required procedures (Registration, PDU-Establishment, Traffic, PDU-Cleanup or Release and De-Registration) are triggered.
- Once the De-Registration is done i.e., cleanup is done, then the test case is stopped and all the logs and PCAPs (Packet Captures) are collected and stored in the scenarios page, where user can download it and analyze.

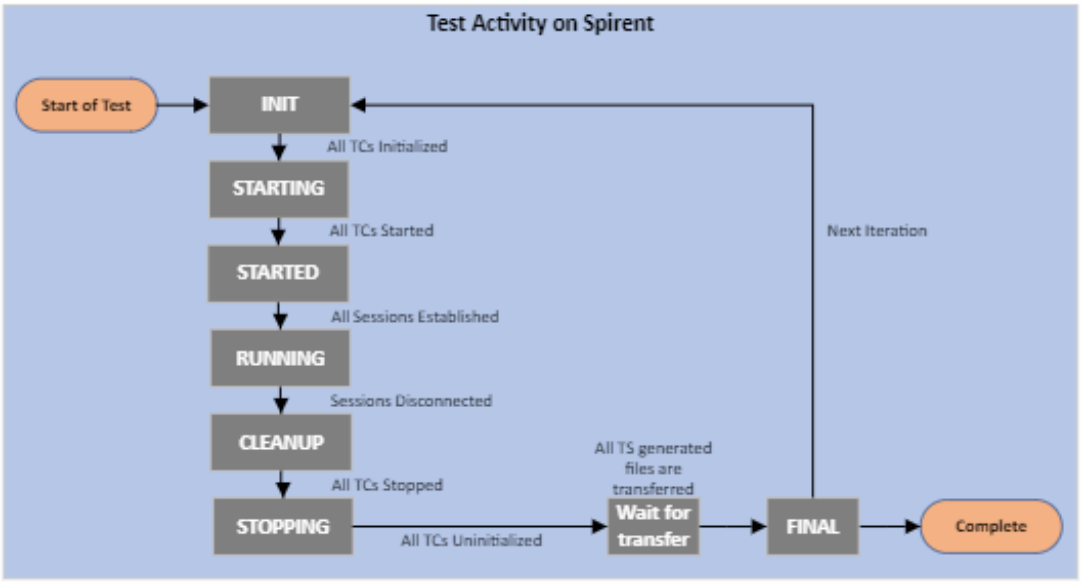

Figure 18: Test Activity on Spirent

6.2 PERFORMANCE

- Performance Testing is done on Spirent test setup to verify and confirm the stability of AGW with increasing load and for longer duration.

Testcase ID	Testcase Name	Result
TC001	200UE_5rate_Registration_Deregistration	Pass
TC002	200UE_5rate_2Mbps_ Registration_Deregistration	Pass
TC003	200UE_5rate_5Mbps_ Registration_Deregistration	Pass
TC004	200UE_5rate_50Mbps_Registration_Deregistration	Pass
TC005	200UE_5rate_Active_Idle_Service Request_Service_Accept_DeRegistration	In progress
TC006	600UE_5rate_Registration_DeRegistration	In progress
TC007	200UE_5rate_Active_Idle_Paging_Registration_ DeRegistration	In progress
TC008	200UE_5AttachRate_350K_UDP_DL_Traffic_Registration_Deregistration	Pass
TC009	200UE_5AttachRate_400Mbps_UDP_DL_Traffic_Registration_Deregistration	Pass

Table 9: Performance

Testcase ID	Testcase Name	Test Description	Duration	Result
TC001	TC001_Perormance_data_200 UE_350K_UDP	200UE register at 5UE/sec, push 350K UDP traffic for 10 mins then deregister. Continue the cycle for 15 loops	8hrs	Pass
TC002	TC001_Performance_data_200 UE_350K_UDP	200UE Register at 5UE/sec, push 350K per UE of traffic then deregister at 5UE/sec. Trigger traffic for 8hrs per UE.	8hrs	Pass
TC003	TC002_Performance_data_200 UE_400M_UDP	200UE Register at 5UE/sec, push 400Mbps of traffic then deregister at 5UE/sec. Trigger traffic for 8hrs per UE.	8hrs	Pass

Table 10: Performance with Description & Duration

Note: *Click here to find the test results and the debug logs of the above test cases.*

- Testing is done through Spirent tool. Below is the screen shot of traffic graph from Spirent.

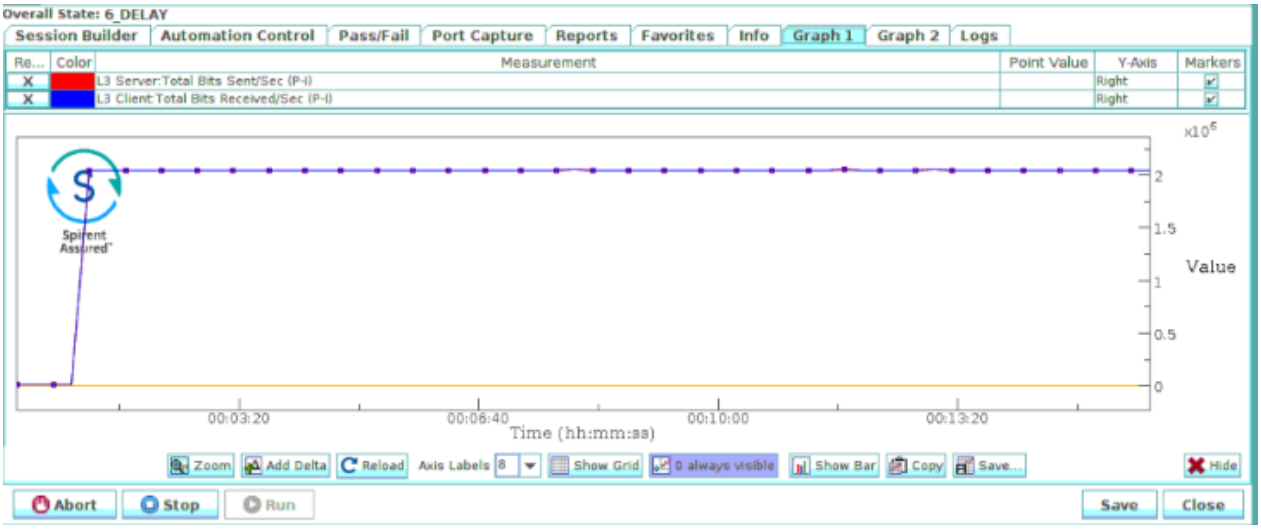

Figure 19: Spirent GUI 400Mbps traffic Graph

7. Test Report from CI pipeline

- Wavelabs CI/CD pipeline trigger happens on every build generated from CI-Master.
- Below are the steps involved in Pipeline trigger.
  - Step.1 Check for checkout from repo.
  - Step.2 Deploy and upgrade AGW.
  - Step.3 Trigger TC from Abot framework.
  - Step.4 Get test results information and download it.

Step.5 Sync of Abot test reports into test agent.

- Below is the test report screen shot of the "**Firebase Test Report**" script.

Figure 20: Test Report from CI pipeline

7.1 Test Activity on Abot

- After installing Abot core, user must configure the Gnb, AGW IP ports and Abot Analytic IP.
- Have Access Gateway installed with V1.7 or upgrade it from the older version to V1.7 (Refer section 4.2 for AGW Upgrade)
- Rebaca's Abot is integrated with the magma CICD which automatically triggers the test run for every single built that coming in and V1.7 is exclusively tested using the Abot test tool.
- The feature files are executed as per below steps.
  - Step.1 Test bed comes up.
  - Step.2 Feature file execution is started
  - Step.3 Test bed comes down
  - Step.4 Feature file execution is completed. (All the feature files execution are completed)
- After executing the feature file, in few seconds logs and PCAPS are generated in the artefacts.
- User can download PCAPS and the Logs from the Artefacts.

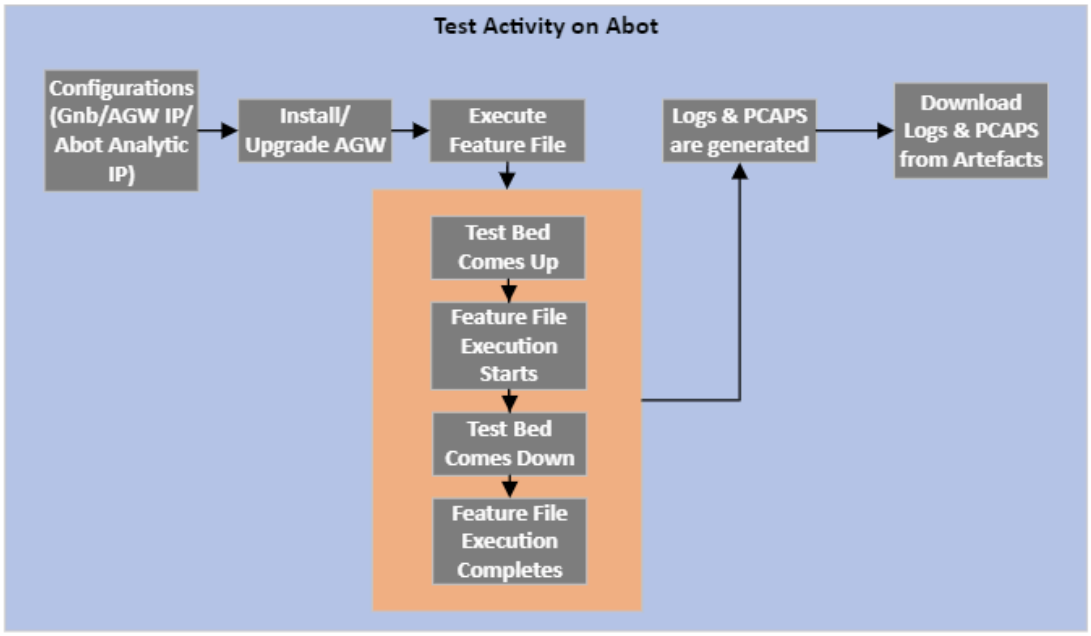

Figure 21: Test Activity on Abot

7.2 List of Abot TC running in CI

- The purpose of running the test case in CI pipeline is to show that the test cases are Pass. It also shows whether all the systems are working correctly or not and no issues found.

Test Case ID	Test Case Title	Execution Status (Pass/Fail/NA)
1	Simple_subcriber_mgmt	Pass
2	Initial_Registration_with_GUTI	Pass
3	OCN_supports_basic_control_functions	Pass
4	OCN_access_service_predefined_loc	Pass
5	CPE_Relocated_One_Location_To_Another	Pass
6	PDU_Session_Release	Pass
7	5G_Registration_PDU_Session_Establishment	Pass
8	NG_Setup_Request_Magma	Pass
9	Dereg_switchOff_suci	Pass

Table 11: List of Abot TC

Note: *Click here to find the test results and the debug logs of the above test cases.*

7.3 Magma CI dashboard

- Magma CI dashboard has results for regression runs using different Automation tools, on every single build that is generated.

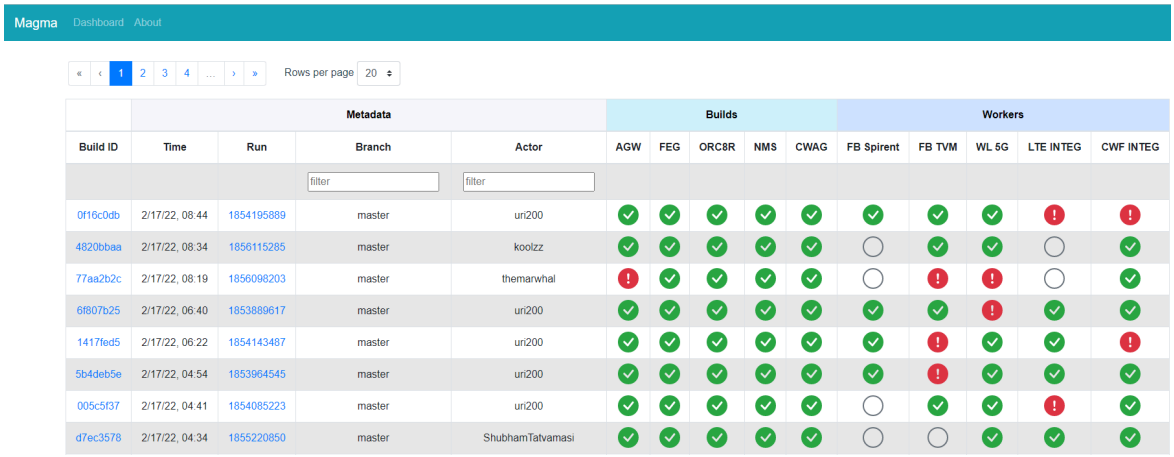

Figure 22: Magma CI dashboard

8. Real Equipment Testing-SIT

- Test activity is done on real device UE-SIT (Huawei), Baicells eNB and magma 5G SA AGW.

  Note: *Mobile device should be 5G enabled*

8.1 Test Activity on Real Device (UE)

- Configure the Baicells Gnb, AGW and UE.
- Have Access Gateway installed with V1.7 or upgrade it from the older version to V1.7 (Refer section 4.2 for AGW Upgrade)
- Switch-on the mobile (Huawei mate UE) and turn-on Wi-Fi or Mobile date.
- Check for the 5G symbol in the network selection.
- Check whether the NGAP setup is established between the devices and all the 5G calls are triggered from the device.
- To validate all the above steps, enable the PCAPs from AGW.

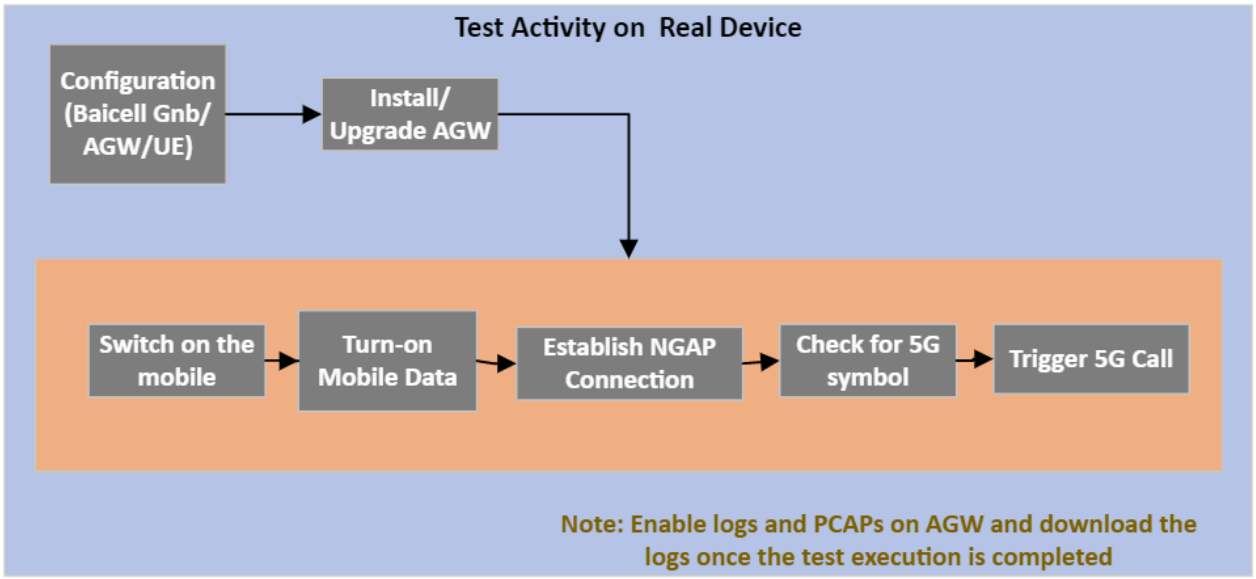

Figure 23: Test Activity on Real Device

- In below screen shot user could find the UE in Aeroplan mode, where the mobile data is turned-off.

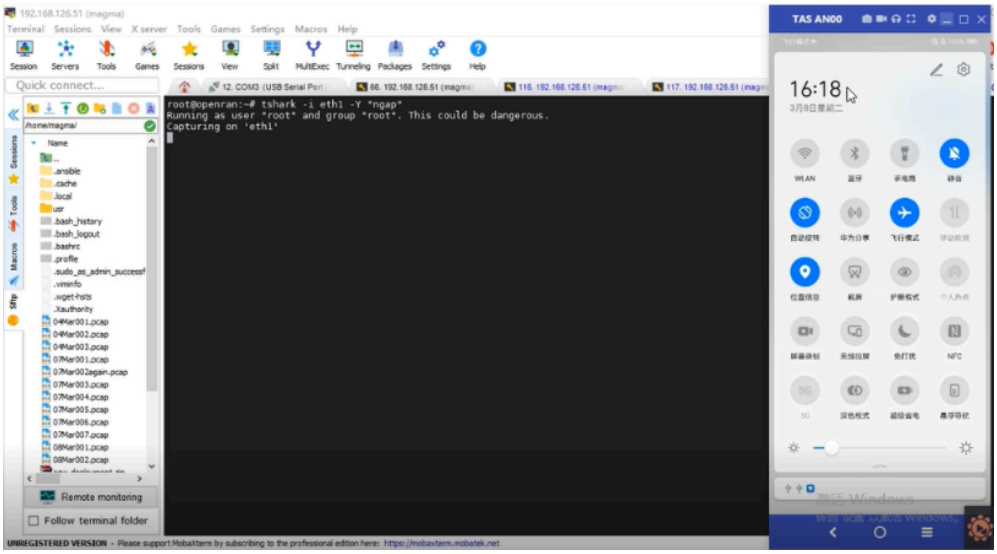

Figure 24: UE in Aeroplan mode

- Once the mobile data is turned-on in UE, 5G signal is detected and it registers with the network (AGW) and the PDU session is successfully established.

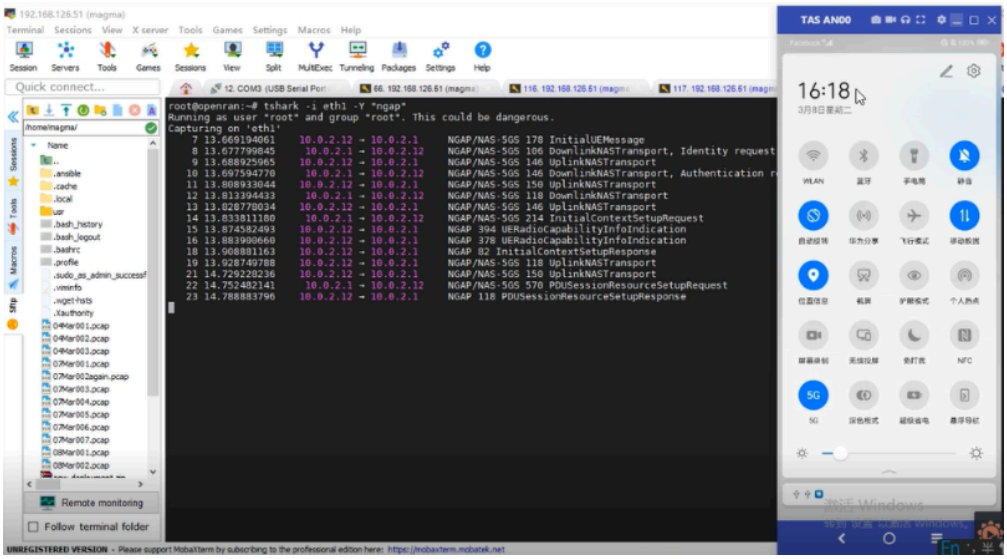

Figure 25: UE with 5G Signal Detected

- Once the PDU session is established, UE sends the traffic over the session.

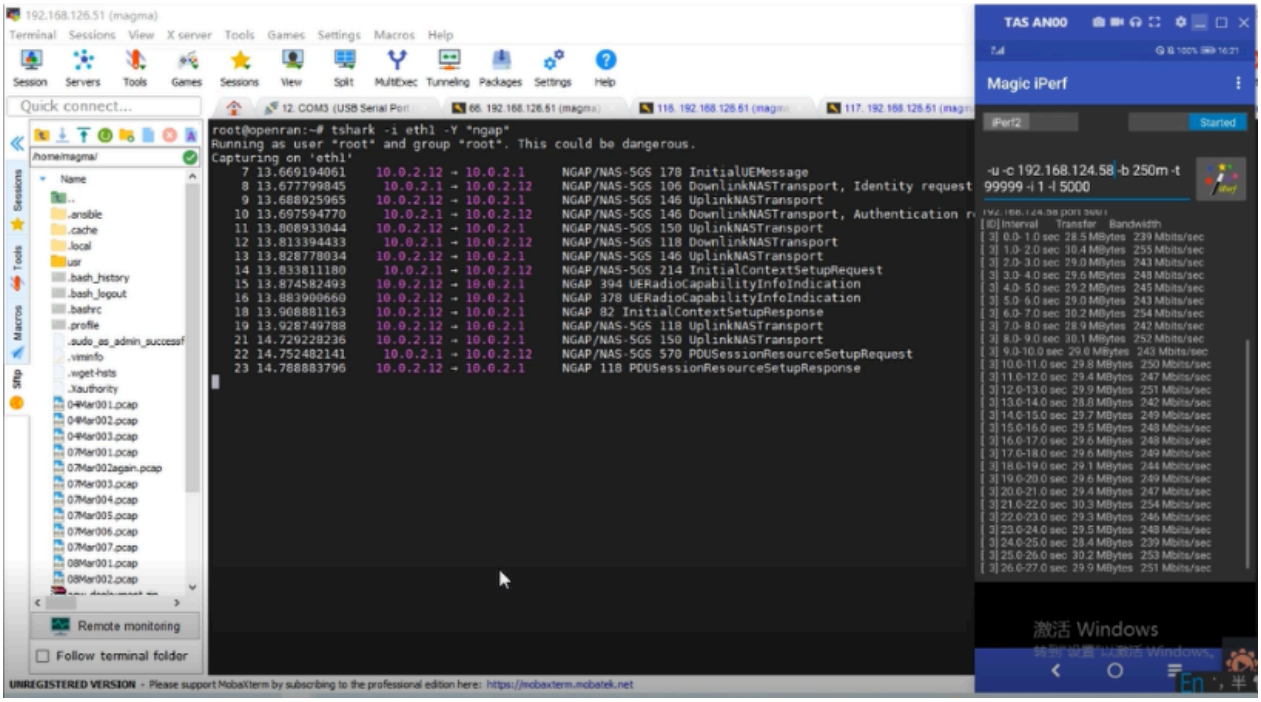

Figure 26: Traffic sent by UE after PDU Establishment

8.2 List of Test Case

- Below are the list of test cases that are executed on the real mobile device.

Software Build info		1.7.0-1647047113-6937a1c1
Real Equipment Testing		
Test Case ID	**Test Scenario**	**Result**
TC1	NGSetup	Pass
TC2	Initial Registration	Pass
TC3	PDU Session Establishment Procedure (IPv4)	Pass
TC4	UE requested PDU session establishment after Initial Registration request	Pass
TC5	UE Triggered Service Request	Pass

Table 12: Real Equipment Testing

Note:

- *Click here to find the test results and the debug logs of the above test cases in **Baicell Lab.***
- *Click here to find the test results and the debug logs of the above test cases in **CpqD Lab.***

9. References

- 3GPP TS 33.501 version 15.4.0 Release 15||Requirements on the UDM: Section # 5.8
- 3GPP TS 33.501 version 15.4.0 Release 15||Subscription identifier privacy: Section # 6.12
- 3GPP TS 33.501 version 15.4.0 Release 15||Subscription identifier de-concealing function (SIDF): Section # 6.12.5
- 3GPP TS 33.501 version 15.4.0 Release 15||Elliptic Curve Integrated Encryption Scheme (ECIES): Section # C.3
- 3GPP TS 24.501 version 15.6.0 Release 15||5GS mobility management messages: Section # 8.2
- 3GPP TS 24.501 version 15.6.0 Release 15||5GS session management messages: Section # 8.3
- 3GPP TS 24.501 version 15.6.0 Release 15||Timers of 5GS mobility management: Section # 10.2
- 3GPP TS 24.501 version 15.6.0 Release 15||Timers of 5GS session management: Section # 10.3
- 3GPP TS 29.281 version 15.7.0 Release 15||Echo Request: Section # 7.2.1
- 3GPP TS 29.281 version 15.7.0 Release 15||Echo Response: Section # 7.2.2
- 3GPP TS 29.281 version 15.7.0 Release 15||End Marker: Section # 7.3.2
- 3GPP TS 38.413 version 16.2.0 Release 16||PDU Session Management Messages: Section # 9.2.1
- 3GPP TS 38.413 version 16.2.0 Release 16||UE Context Management Messages: Section # 9.2.2
- 3GPP TS 38.413 version 16.2.0 Release 16||Paging Messages: Section # 9.2.4
- 3GPP TS 38.413 version 16.2.0 Release 16||NAS Transport Messages: Section # 9.2.5
- 3GPP TS 38.413 version 16.2.0 Release 16||Interface Management Messages: Section # 9.2.6
- TS 124 501 - V15.3.0 - 5G; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (3GPP TS 24.501 version 15.3.0 Release 15) (etsi.org)
- MM-Cause.xlsx (sharepoint.com)

- AGW installation Guide