W4S-LAB
UAT Document

Table of Contents

1 Introduction **5**

1.1. Purpose and Scope **5**

2 Testcases 6

2.1 Physical Material Verification 6

2.2 5G Network specs (Core+RAN) 9

2.3 5G SA CN 30

2.4 5G NR Radio 55

NG User Plane 75

NG Control Plane 85

Radio Protocol Architecture 94

4.8 Router Firewall specs 102

Web Filtering 109

Optional: Intrusion Prevention System 115

Secure Remote Access 119

Application Control 126

Intelligent Networking 129

4.9 Server 1 with 5G Core, IMS and NMS software 133

Processors 133

Memory 134

Storage 135

Network Interface 137

PCIe Slots 139

4.10 Server 2 with 5G MEC Platform and Application Server 140

Processors 140

Memory 141

Storage 142

Network 143

PCIe Slots 144

4.11 5G SIM 148

4.12 5G EVALUATION BOARD 154

4.13 IOT Gateway 169

Access Points 177

Networks 180

VLAN 182

Security 185

Management 189

Others 196

4.14 5G Mini Drones 202

Physical Tests 202

Functionality Tests(Indoor Tests) 206
Functionality Tests (Outdoor Tests) 209
4.15 XR Device AR/VR 212
Connectivity / Sensors 215
Input/Output 217
4.16 5G Indoor CPE 220
5G 222
RF 231
Security 235
Interface 238
Management 240
4.17 5G Camera 241
Camera 245
LENS 248
VIDEO 250

1 Introduction

1.1. Purpose and Scope

Purpose

The purpose of this User Acceptance Testing (UAT) document is to validate the performance, functionality, and integration of the 5G products and solutions provided to TCIL (Telecommunications Consultants India Limited). This UAT aims to ensure that all specified equipment and devices meet TCIL's standards and requirements before full deployment.

The products under evaluation include the 5G RAN, CORE, and MEC server (running applications such as idronam, Thingsboard, minicom, and VLC), LPRU, and a Private 5G Network setup. This setup features IoT components such as sensors (Temperature & Humidity, Light, Soil, Water), IoT Gateway RUTX50, Kenstal CPE, Evaluation Board, 5G Mini Drone, and a Sparsh camera. 5G lab setup that integrates various devices and services into a private 5G network, utilizing edge computing and core network capabilities to deliver low-latency and high-performance applications.

Scope

The scope of this UAT encompasses:

- Testing: Verification of functionality, performance, and integration for each piece of equipment and device listed.
- Deliverables: Test plans, execution results, and issue reports detailing performance, functionality, and any issues encountered.

This UAT ensures that the 5G products are fully compliant with TCIL's requirements and ready for operational use.

2 Testcases

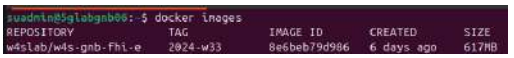
2.1 Physical Material Verification

S. No.	Description	Qty.	Make	Model	Serial Number
1	5G Core	1	W4S	W4S 5G Core	
2	5G Radio (Integrated RAN)	1	W4S	W4S Integrated RAN	
3	IMS solution	1	W4S	W4S IMS	
4	MEC & Application server	1	W4S	W4S MEC & Application	
5	NMS (with Dashboard)	1	W4S	W4S NMS	
6	Router with Firewall	1	Anexgate	AG200	
7	5G SIMs	50	Linking Minds	SIM	
8	5G Evaluation Board / Hardware and Software Development Kit.	1	CORAL TELECOM	NA	
9	IoT Gateway	1	TELETONIKA	RUTX50	

10	IoT sensors with analytics software (Loaded in Application server)	1	W4S	W4S_IOT	
11	Temperature & Humidity sensor	1	Standard COTS Item	NA	
12	Light sensor	1	Standard COTS Item	NA	
13	Soil sensor (NPK)	1	Standard COTS Item	NA	
14	Water (TDS/chlorine) sensor	1	Standard COTS Item	NA	
15	5G XR(AR/VR/MR) headset or Device	1	Ajnalens	AjnaXR	
16	5G Mini Drone	1	Menthosa	5G Drone	
17	5G Indoor CPE	1	Kenstel	KCP-510	
18	5G Camera with AI enabled Video Analytics	1	Samriddhi	SC-IM82NP-I(Z)(S)(H)	
19	5G Handsets	2	One Plus	ONEPLUS NORD CE 3	

20	Adjustable Tripod Pole (3m)	1	Standard COTS Item	NA	
21	24 U Rack	1	President	NA	
22	UPS 5KVA (1hr backup)	1	Uniline	NA	
23	32 inch FHD Display	1	Standard COTS Item	Monitor 32 Inch	
24	L2 Managed Switch (24 port)	1	D-Link	DGS-1510	
25	Testing & Tracing Tools	1	Meritech	Sigma	

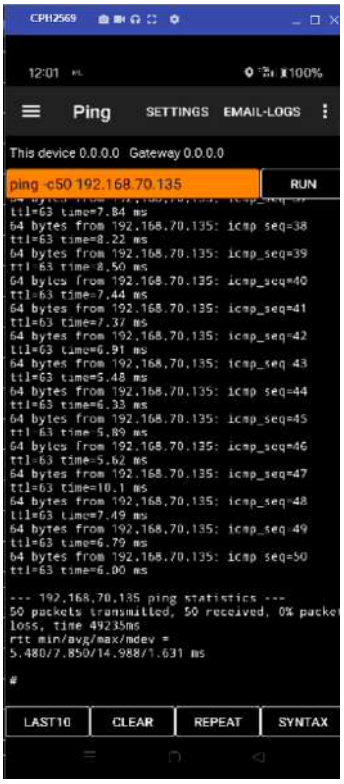
2.2 5G Network specs (Core+RAN)

Test ID	4.2.i		
Requirement	Radio Configuration		
Test Objective	Integrated RAN (CU+DU) or disintegrated RAN		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Physical verification of CU,DU and RU CU+DU software installed on gNB machine (Rack mountable). docker images shows the 5g ran stack	Integrated RAN (CU/DU) 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.2.iii
Requirement	Data Rate (DL+UL) >= 200 Mbps

Test Objective	Verify RAN Supports Data throughput (UL+DL) >=200 Mbps	
Test Description	**Set Steps**	**Acceptance Criteria**
	1) Attach UE in the Private 5G Network Download aruba utilities from play store (if not present in UE) 2) Execute below command to run **iperf server** at Core network *ssh suadmin@192.168.x.20* *Password: Admin@123* docker exec -it oai-ext-dn /bin/bash then type : iperf3 -s 3) Open the aruba utilities app in the mobile phone and navigate to iperf3 and execute the below command to run the iperf client on the mobile application . **THIS COMMAND IS USED TO TEST down link TRAFFIC** -c 192.168.70.135 -t10 -i1 -b250M -u -R **INCASE of upLINK TRAFFIC** -c 192.168.70.135 -t10 -i1 -b100M -u	1) Attached UE should be in private 5G Network Downlink:  Uplink: 
Overall Test Result	Pass:☐	Fail:☐
Comments		

Name	Name of Verifier	Signature	

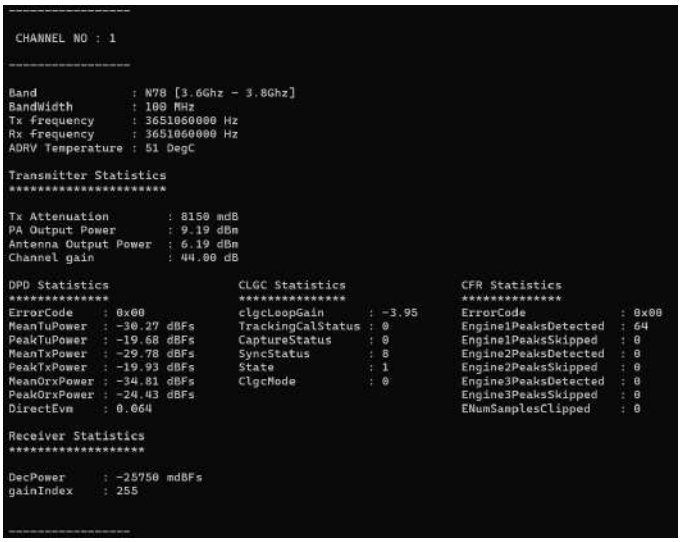
Test ID	4.2.iv	
Requirement	Latency<=15 ms	
Test Objective	Latency Test (Control Plane and User Plane)	
Test Description	**Set Steps**	**Acceptance Criteria**
	A) Open aruba utilities app in mobile phone and navigate to ping and start a 50 ping packets user plane function via pinging to upf command to use in phone :ping -c 50 192.168.70.155	User Plane Latency over 50 ping packets should be <=15 Please refer min/average/max latency after 50 packets ping from UE to Test server  rtt min/avg/max/mdev= 5.480/7.850/14.988/1.631 ms
Overall Test Result	Pass:☐	Fail:☐
Comments		

Name	Name of Verifier	Signature	

Test ID	4.2.v	
Requirement	Max No. of active devices (That network can connect)	
Test Objective	30 UEs should be attached to the network. (Simulation Environment)	
Test Description	**Set Steps**	**Acceptance Criteria**
	In the gNB server start UE Simulator by below commands: start network ./start_network.sh start simulated UE's ./start_32_ue.SH	simulated ue's are attached to the network . The simulated ue's can be seen in the amf logs .
Overall Test Result	Pass:☐	Fail:☐
Comments		

Name	Name of Verifier	Signature	

Test ID	4.2.vi
Requirement	Radio Power

Test Objective	Radiating power of Radio should be Upto 100 mW		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Login to RU console and run below command to get RU power per port: ssh root@192.168.4.50 password: **** tail -f /media/sd-mmcblk0p4/TransceiverStatistics.txt Antenna Output power shall be less than 20dBm	RU output for radiation power details 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.2.vii**	
Requirement	Duplexing Mode	
Test Objective	Need to check system compatibility in TDD mode	
Test Description	**Set Steps**	**Acceptance Criteria**

	login into ru - **ssh root@192.168.4.50** Execute the following command in the ru console **sysrepocfg -X -d running**. Navigate to tx and rx array carrier information in the running configuration file to observe the frequency set for tx and rx Alternately the sigma ml mobile tracing tool shows the arfcn of the centre frequency which can be decoded for the tdd duplex mode on any arfcn calculator .	In TDD ,the same frequency is Configured for Both Uplink and Downlink Path . Verify following under Tx and Rx array carriers **<absolute-frequency-center>643404** **<center-of-channel-bandwidth>3651060000** 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.2.viii**	
Requirement	Channel Bandwidth	
Test Objective	Channel bandwidth should be 100 Mhz	
Test Description	**Set Steps**	**Acceptance Criteria**

	Attach Mobile with Tracing tool on the network. open the sigma ml application	Check NR DL BW on Trace tool in UE:  	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.2.ix**	
Requirement	Band support	
Test Objective	5G Band n78 should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	open the Tracing tool (sigma ml) on the Mobile	Check NR Band on Trace tool: 
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	**4.2.x**
Requirement	MIMO Configuration
Test Objective	Check that RU is supporting 2T2R (min)

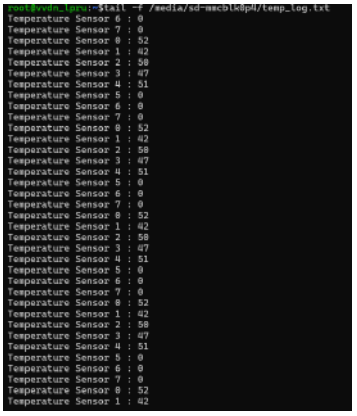
Test Description	**Set Steps**	**Acceptance Criteria**	
	1.Open the tracing tool in the mobile 2.verify the MIMO configuration via sigma ml app on the mobile phone.	Check under NR DL Transmission Info  Open Sigma ML application in UE to check configured configuration	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.2.xi**
Requirement	Synchronization

Test Objective	IEEE 1588 Precision Time Protocol (PTP) in ITU-T Standards		
Test Description	**Set Steps**	**Acceptance Criteria**	
	open the wireshark application and apply **PTP** filter. check the subtree under the message **Precision Time Protocol(IEEE1588)**	**Precision Time Protocol (IEEE1588)** 0000 .... = majorSdoId: Unknown (0x0) .... 0000 = messageType: **Sync Message** (0x0) 0000 .... = minorVersionPTP: 0 .... 0010 = **versionPTP: 2**	
Overall Test Result	Pass:☐	Fail:☐	
Commments			
Name	Name of Verifier	Signature	

Test ID	4.2.xii	
Requirement	Antenna	
Test Objective	To verify antenna type used External or Internal	
Test Description	**Set Steps**	**Acceptance Criteria**

	Visual inspection of radio unit connected with an external antenna.	By observation Antennas are mounted external antennas attached to Radio Unit 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

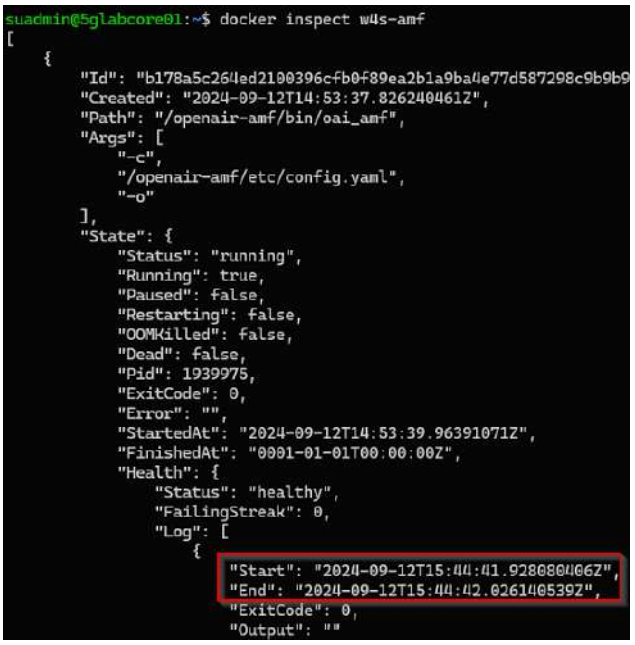
Test ID	4.2.xiii		
Requirement	Mechanical/Environmental		
Test Objective	IP54/QM333 wherever applicable. (Environmental Testing). Temperature and Humidity as per the Indian Geographical conditions for RU		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Operating Temperature: - 40 to 55C IP 65 Login into RU from DU ssh root@192.168.4.50 Pass:- vvdn root@vvdn_lpru: tail -f /media/sdmmcblk0p4/temp_log.txt	Required Factory Test report attached Temperature Sensor 0 : 52 Temperature Sensor 1 : 45 Temperature Sensor 2 : 52 Temperature Sensor 3 : 49 Temperature Sensor 4 : 52 Temperature Sensor 5 : 0 Temperature Sensor 6 : 0 Temperature Sensor 7 : 0 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.2.xiv	
Requirement	MIMO Configuration	
Test Objective	Minimum support is required	
Test Description	**Set Steps**	**Acceptance Criteria**
	Start the sigma ml application measurement . Attach the mobile phone to the network verify the mimo configuration via sigma ml app on the mobile phone	Access the sigma ml tracing tool in the mobile and navigate to 5GNR section to see the mimo information 
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.2.xv	
Requirement	Network Slicing	
Test Objective	Support for slicing, Preconfigured multiple different slices(min).	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verify via Wireshark and apply **ngap** filter NG setup response	**protocolIEs: 4 items** Item 0: id-AMFName Item 1: id-ServedGUAMIList Item 2: id-RelativeAMFCapacity **Item 3: id-PLMNSupportList** value → PLMNSupportList: 1 item → Item 0 → PLMNSupportItem → pLMNIdentity: 00f110 → sliceSupportList: 3 items → Item 0 → SliceSupportItem → s-NSSAI → **sST: 80** **sD: 000080** Item 1 →

		SliceSupportItem → s-NSSAI → **sST: 01** **sD: 000001** Item 2 → SliceSupportItem → s-NSSAI → **sST: 82** **sD: 000082**	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.2.xvi		
Requirement	5G Use case scenario { eMBB(R15), URLLC(R16), MMTC(R16) }		
Test Objective	Verification of eMBB support		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verifiable with the result of test case 4.2.iii		
Overall Test Result	Pass:☐	Fail:☐	
Comments	Verifiable with the result of test case 4.2.iii		
Name	Name of Verifier	Signature	

Test ID	**4.2.xvii**		
Requirement	Uptime (99%)		
Test Objective	Test setup working status with stability		
Test Description	**Set Steps**	**Acceptance Criteria**	
	execute the following command on core network server docker inspect w4s-amf	Verify the result within 2 hours of run time : output example 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.2.xxii**		
Requirement	Security		
Test Objective	Features to ensure system security (security features for Core, RAN and devices, solution for internal and external attack vectors, proactive security monitoring, reporting and alarms, are the security alerts stored including supporting data & logs) Security considerations in deployment of solution – both interface and application level to be considered		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Provided Firewall is configured to take care of any internal and external attack vectors, IT should do the proactive security monitoring, reporting and alarms, which are the security alerts which are stored including the supporting data & logs.	Refer to the Firewall User manual attached in the Appendix to configure the required security policies.	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.2.xxiii	
Requirement	5G Devices	
Test Objective	All 5G devices to support private PLMN IDs	
Test Description	**Set Steps**	**Acceptance Criteria**

	Configured private PLMN(001) should be supported by all delivered 5G devices verify the plmn via sigma ml application in mobile phones	NR Primary Cell Info → NR PLMN 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.2.xxiv	
Requirement	IP communication	
Test Objective	IP assignment of the UE should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**

	mobile settings > about device > status >IP Address as IPV4	Check the assigned ip-address to attached 5G mobile  IP address is 10.0.0.3 which is IPv4	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

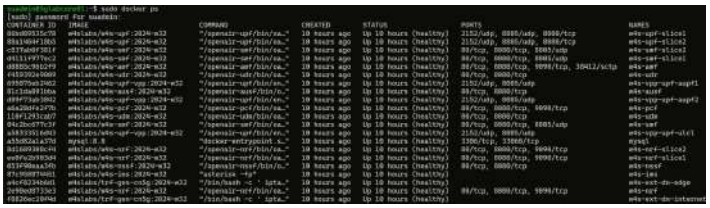
2.3 5G SA CN

Test ID	**4.3.1 a**		
Requirement	Separate the User Plane (UP) functions from the Control Plane (CP) functions, allowing independent scalability		
Test Objective	Show the separation of CP and UP in Core network via N2 and N3 interfaces for control plane and user plane respectively		
Test Description	**Set Steps**	**Acceptance Criteria**	

	attach a ue to the network
	
	UPF and AMF are Connected via N3 and N2 respectively to the RAN separating the CP and UP correct
		Control Plane
		
		N2 interface messages : 3.XII and 3.XIV
		
		User Plane
		
		check the gpt messages from the ue
		
		Check the ip assigned to ue after connecting it to the 5g network by navigating to settings -> about device -> status
		
		execute the traceroute for the ip of ue on the upf container .
		(install traceroute in the container if required)
		
		`traceroute to 12.2.1.3 (12.2.1.3), 30 hops max, 60 byte packets`
		`1 * * 12.2.1.3 (12.2.1.3) 26.984 ms`	

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.3.1.b**

Requirement	Evolution and flexible deployments e.g. centralized location or distributed (remote) location.		
Test Objective	Evolution and flexible deployments of core network		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Core Network Nodes are deployed via Docker Containers docker ps	Dockerized core network is deployed **docker ps** output:  => These containers verify that the Dockerized services are correctly deployed and operational	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.3.1.c**		
Requirement	Modularize the function design, e.g. to enable flexible and efficient network slicing.		
Test Objective	Network slicing should support		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Execute the RAN with different slices configuration that can be defined in the configuration file	Attach the ue with slice specific apn configuration Verify slices via wireshark Messages for session establishment SST:1 SD:1 SST:128 SD:128 SST:130 SD:130 Reference procedures 3.IV , 3.XII	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.3.1.d**		
Requirement	Wherever applicable, define procedures (i.e. the set of interactions between network functions) as services, so that their re-use is possible.		
Test Objective	Core network nodes implementation supports service based communication		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Start wireshark from a system and access the core network server via ssh and select w4s-core interface to capture traffic	Core Network Nodes implementation is via service based architecture where each node has a service based interface which communicates via http Core network Nodes inter communication via typical http and tcp framework .	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.3.1.e**		
Requirement	Enable each Network Function (NF) to interact with other NF directly if required. The architecture does not preclude the use of an intermediate function to help route Control Plane messages (e.g. like a DRA)		
Test Objective	Different Nodes in core network should interact each other directly or via intermediary		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Start wireshark from a system and access the core network server via ssh and select w4s-core interface to capture traffic	Core network Nodes inter communication via typical http framework .	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.3.1.g**		
Requirement	Support a unified authentication framework.		
Test Objective	Authentication framework should be supported		
Test Description	**Set Steps**	**Acceptance Criteria**	
	 Attach UE to the network	Below command the process status of AUSF NODE docker ps to check logs of ausf node type below command **docker logs -f w4s-ausf** 	
Overall Test Result	Pass:☐	Fail:☐	
comments			
Name	Name of Verifier	Signature	

Test ID	**4.3.1.j**	
Requirement	Support concurrent access to local and centralized services. To support low latency services and access to local data networks, UP functions can be deployed close to the Access Network.	
Test Objective	Demonstrate access local and centralized services	
Test Description	**Set Steps**	**Acceptance Criteria**

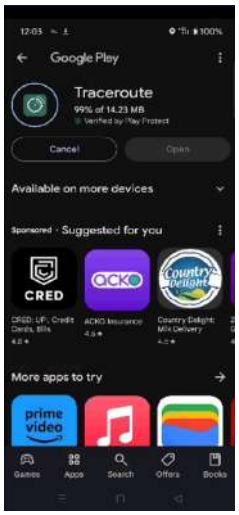
	Steps: 1. Access the internet service such as youtube or google for centralized services access 2.perform iperf3 throughput test from the mec server to show local network access	The ue should be able to reach google /youtube or any other centralized service to show centralized services access The ue should be able to communicate within the local network to show local services	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.3.2.a	
Requirement	Authentication Server Function (AUSF)	
Test Objective	AUSF node should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	ssh suadmin@192.168.x.20 Pass:- Admin@123 goto core directory **docker compose -f docker-compose-w4s.yaml up -d** check docker status by **docker ps** to check ausf logs run **docker logs -f w4s-ausf** UE Auth Request from AMF to AUSF **docker logs -f w4s-amf**	[ausf_nrf] [info] Sending NF registration request [ausf_client] [debug] Send a simple HTTP request [ausf_nrf] [warning] Could not get the response from NRF! [ausf_app] [debug] ausf profile to JSON: {"ausfInfo":{"groupId":"oai-ausf-testgroupid","routingIndicators":["0210","9876"],"supiRanges":[{"end":"","pattern":"209238210938","start":"q0930j0c80283ncjf"}]},"capacity":100,"fqdn":"","heartBeatTimer":50,"ipv4Addresses":["192.168.70.138"],"nfInstanceId":"86c51ed0-7010-4b61-a5b4-b6b7898856d4","nfInstanceName":"OAI-AUSF",**"nfStatus":"REGISTERED"**,"nfType":"AUSF","priority":1,"sNssais":[]} Auth Request Start to generate Authentication Vectors [amf_n1] [debug] Get Authentication Vectors from AUSF [amf_n1] [debug] Promise ID generated 9 [amf_sbi] [info] Receive UE Authentication Request message, handling ... [amf_sbi] [debug] Send UE Authentication Request to AUSF (HTTP version 2) [amf_sbi] [debug] Send UE Authentication Request to AUSF, URL http://w4s-ausf:8080/nausf-auth/v1/ue-authentications

	UE Authentication response from Ausf to AMF	[amf_sbi] [debug] Send UE Authentication Request to AUSF, msg body: {"servingNetworkName":"5G:mnc001.mcc001.3gppnetwork.org","supiOrSuci":"001010000000164"} [amf_sbi] [info] Send HTTP message to http://w4s-ausf:8080/nausf-auth/v1/ue-authentications [amf_sbi] [info] HTTP message Body: {"servingNetworkName":"5G:mnc001.mcc001.3gppnetwork.org","supiOrSuci":"001010000000164"} Auth response: UE Authentication, response from AUSF, HTTP Code: 201 [2024-10-15 08:45:05.569] [amf_sbi] [debug] UE Authentication, response from AUSF , {"5gAuthData":{"autn":"36b5f905c80b800058a2a90518916bea","hxresStar":"88c18c9d94db80c6ac1ba1219abe842c","rand":"06a683230fc8e4a534fbe0505ce1c68d"},"_links":{"5G_AKA":{"href":"http://192.168.70.138:8080/nausf-auth/v1/ue-authentications/36b5f905c80b800058a2a90518916bea/5g-aka-confirmation"}},"authType":"5G_AKA"}
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.3.2.b	
Requirement	Access and Mobility Management Function (AMF)	
Test Objective	AMF node should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	goto core directory **docker compose -f docker-compose-w4s.yaml up -d** check docker status by **docker ps** to check amf logs run **docker logs -f w4s-amf** registration request from AMF to NRF	[amf_sbi] [info] Receive Register NF Instance Request, handling ... [amf_sbi] [debug] Send NF Instance Registration to NRF [amf_app] [debug] AMF profile to json: {"amfInfo":{"amfRegionId":"01","amfSetId":"001","guamiList":[{"amfId":"010041","plmnId":{"mcc":"001","mnc":"01"}}]},"capacity":100,"custom_info":null,"heartBeatTimer":50,"ipv4Addresses":["192.168.70.132"],"nfInstanceId":"c23127fd-ba7d-4602-8761-a713786e6cc9","nfInstanceName":"OAI-AMF","nfServices":[{"ipEndPoints":[{"ipv4Address":"192.168.70.132","port":8080,"transport":"TCP"}],"**nfServiceStatus**":"**REGISTERED**","scheme":"http","serviceInstanceId":"namf_communication","serviceName":"namf_communication","versions":[{"apiFullVersion":"1.0.0","apiVersionInUri":"v1"}]}],"**nfStatus**":"**REGISTERED**","nfType":"AMF","priority":1,"sNssais":[{"sd":"000080","sst":128},{"sd":"000001","sst":1},{"sd":"000082","sst":130}]} [2024-10-15 08:58:37.675] [amf_sbi] [debug] Send NF Instance Registration to NRF, NRF URI (RegisterNFInstance API) [2024-10-15 08:58:37.675] [amf_sbi] [debug] Send NF **Instance Registration to NRF, msg body:** {"amfInfo":{"amfRegionId":"01","amfSetId":"001","guamiList":[{"amfId":"010041","plmnId":{"mcc":"001","mnc":"01"}}]},"capacity":100,"custom_info":null,"heartBeatTimer":50,"**ipv4Addresses**":["**192.168.70.132**"],"nfInstanceId":"c23127fd-ba7d-4602-8761-a713786e6cc9","nfInstanceName":"OAI-AMF","nfServices":[{"ipEndPoints":[{"ipv4Address":"192.168.70.132","port":8080,"transport":"TCP"}],"nfServiceStatus":"REGISTERE

		D","scheme":"http","serviceInstanceId":"namf_communication","serviceName":"namf_communication","versions":[{"apiFullVersion":"1.0.0","apiVersionInUri":"v1"}]}],"nfStatus":"REGISTERED","nfType":"AMF","priority":1,"sNssais":[{"sd":"000080","sst":128},{"sd":"000001","sst":1},{"sd":"000082","sst":130}]}	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.3.2.c	
Requirement	Data Network (DN), e.g. operator services, Internet access or 3rd party services	
Test Objective	Data Network (DN) node should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	Attach UE with the private network Verify internet services via youtube/google/playstore etc.	Attach a 5g ue to the 5g private network and verify internet access via accessing a webpage or downloading an android application as shown in the example below (download an app via play store). 
	Apply gtp filter in wireshark Standard query from UE	GPRS Tunneling Protocol TEID: 0x00000019 (25) Internet Protocol Version 4, Src: 12.0.0.9, Dst: 172.21.3.100
	Standard query response from data network	GPRS Tunneling Protocol TEID: 0x97dab204 (2547692036) Internet Protocol Version 4, Src: 172.21.3.100, Dst: 12.0.0.9

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.3.2.e	
Requirement	Network Repository Function (NRF)	
Test Objective	NRF node should be running in virtualized container	
Test Description	**Set Steps**	**Acceptance Criteria**
	goto core directory **docker compose -f docker-compose-w4s.yaml up -d** check docker status by **docker ps** to check amf logs run **docker logs -f w4s-nrf**	[nrf_app] [debug] NF instance info Instance ID: cac755f2-0686-4b40-a75a-467728b316aa Instance name: OAI-SMF Instance type: SMF Status: REGISTERED HeartBeat timer: 10 Priority: 1 Capacity: 100 NNSSAI(SST, SD): 130, 000082 IPv4 Addr: 192.168.70.133 NF instance info Instance ID: 3799d789-ea3d-4839-83af-0af96b8c7aae

		Instance name: OAI-PCF Instance type: PCF Status: REGISTERED HeartBeat timer: 10 Priority: 1 Capacity: 100 IPv4 Addr: 192.168.70.139 NF instance info Instance ID: 114dd3e9-dcdd-4c2d-a371-4e1217c8d570 Instance name: AUPF1 Instance type: UPF Status: REGISTERED HeartBeat timer: 10 Priority: 1 Capacity: 100 NNSSAI(SST, SD): 130, 000082 FQDN: aupf1.node.5gcn.mnc01.mcc001.5glabindia.in IPv4 Addr: 192.168.70.202	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.3.2.f	
Requirement	Network Slice Selection Function (NSSF)	
Test Objective	NSSF node should be running in virtualized container	
Test Description	**Set Steps**	**Acceptance Criteria**
	goto core directory **docker compose -f docker-compose-w4s.yaml up -d** check docker status by **docker ps** to check nssf logs run **docker logs -f w4s-nssf**	Received request for NS Selection - (HTTP_VERSION 2) [nssf_sbi] [debug] **QueryString**: nf-type=AMF&nf-id=c23127fd-ba7d-4602-8761-a713786e6cc9&slice-info-request-for-pdu-session ={"roamingIndication":"NON_ROAMING",**"sNssai":{"sd":"000080 ","sst":128**}} [nssf_sbi] [info] Query_PARAM::NF_TYPE - AMF [nssf_sbi] [info] Query_PARAM::NF_ID - c23127fd-ba7d-4602-8761-a713786e6cc9 [nssf_sbi] [info] **Query_PARAM** slice-info-request-for-pdu-session - {"roamingIndication":"NON_ROAMING",**"sNssai":{"sd":"000080","sst":128**}} Received request for NS Selection - (HTTP_VERSION 2) [nssf_sbi] [debug] **QueryString**: nf-type=AMF&nf-id=c23127fd-ba7d-4602-8761-a713786e6cc9&slice-info-request-for-pdu-session ={"roamingIndication":"NON_ROAMING","**sNssai":{"sd":"000001 ","sst":1**}} [nssf_sbi] [info] Query_PARAM::NF_TYPE - AMF [nssf_sbi] [info] Query_PARAM::NF_ID - c23127fd-ba7d-4602-8761-a713786e6cc9 [nssf_sbi] [info] **Query_PARAM** slice-info-request-for-pdu-session - {"roamingIndication":"NON_ROAMING","**sNssai":{"sd":"000001","sst":1**}}

		Received request for NS Selection - (HTTP_VERSION 2) [nssf_sbi] [debug] **QueryString**: nf-type=AMF&nf-id=c23127fd-ba7d-4602-8761-a713786e6cc9&slice-info-request-for-pdu-session ={"roamingIndication":"NON_ROAMING","**sNssai":{"sd":"000082 ","sst":130**}} [nssf_sbi] [info] Query_PARAM::NF_TYPE - AMF [nssf_sbi] [info] Query_PARAM::NF_ID - c23127fd-ba7d-4602-8761-a713786e6cc9 [nssf_sbi] [info] **Query_PARAM** slice-info-request-for-pdu-session - {"roamingIndication":"NON_ROAMING","**sNssai" :{"sd":"000082","sst":130**}}	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.3.2.g		
Requirement	Policy Control Function (PCF)		
Test Objective	PCF node should be running in virtualized container		
Test Description	**Set Steps**	**Acceptance Criteria**	
	goto core directory **docker compose -f docker-compose-w4s.yaml up -d** check docker status by **docker ps** to check pcf logs run **docker logs -f w4s-pcf**	[pcf_app] [debug] Policy Storage: - Default Decision: -- PCC Rule IDs: internet-rule - Slice Decisions: -- Slice: Sd: 000082 Sst: 130 -- PCC Rule IDs: internet-rule - DNN Decisions: -- DNN: 5glab -- PCC Rule IDs: internet-rule - SUPI Decisions: -- SUPI: imsi-001010000000164 -- PCC Rule IDs: internet-rule	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.3.2.h	
Requirement	Session Management Function (SMF)	
Test Objective	SMF node should be running in virtualized container	
Test Description	**Set Steps**	**Acceptance Criteria**
	goto core directory **docker compose -f docker-compose-w4s.yaml up -d** check docker status by **docker ps** to check smf logs run **docker logs -f w4s-smf-slice1**	DFS Asynch: Handle UPF 192.168.70.155 [smf_app] [debug] Created PDR ID, rule ID 1 [smf_app] [info] Sending ITTI message 37itti_n4_**session_establishment_request** to task TASK_SMF_N4 [smf_api] [debug] Got result for promise ID 154 [smf_api] [debug] Add location header /nsmf-pdusession/v1/sm-contexts/1 [smf_n4] [info] handle_receive(70 bytes) [smf_n4] [debug] handle_receive_pfcp_msg msg type 51 length 66 [smf_app] [debug] Received N4 Session Establishment Response sender teid 0x1 pfcp_tx_id 9B [smf_app] [debug] Handle N4 Session Establishment Response (PDU Session Id 1) [smf_app] [debug] Successfully associate PDR 1 with F-TEID ID 0x1 - IP: 192.168.70.155 (QFI: 1) [smf_app] [debug] UPF graph in SMF finished [smf_n1] [debug] Created new QoS rule with ID 1 and 1 packet filters [smf_app] [debug] Prepare a **PDU Session Establishment Accept message** and send to UE

		[smf_n1] [info] Create N1 SM Container, PDU Session Establishment Accept [smf_n1] [info] **PDU_SESSION_ESTABLISHMENT_ACCEPT**, encode starting... [smf_n1] [debug] SM header, Extended Protocol Discriminator 0x2e, PDU Session Identity 1, Procedure Transaction Identity: 97, Message Type: 194 [smf_n1] [debug] PDU Session Type: 1 [smf_n1] [debug] Get default values for Session-AMBR [smf_n1] [debug] Get SMF context with SUPI **1010000000164** [smf_app] [debug] Get AMBR info from the subscription information (DNN 5glabs1)	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

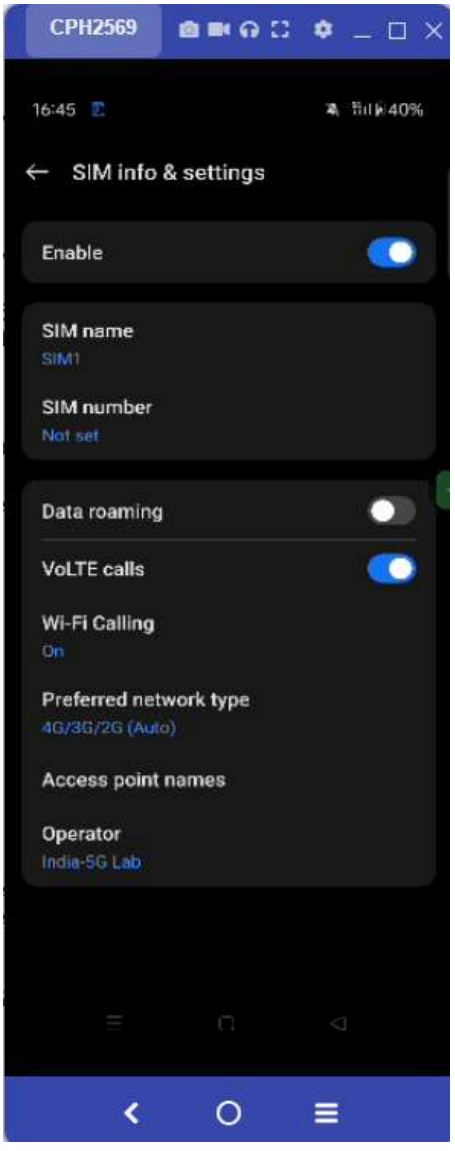
Test ID	4.3.2.i	
Requirement	Unified Data Management (UDM)	
Test Objective	UDM node should be running in virtualized container	
Test Description	**Set Steps**	**Acceptance Criteria**
	goto core directory **docker compose -f docker-compose-w4s.yaml up -d** check docker status by **docker ps** to check udm logs run **docker logs -f w4s-udm**	[udm_ueau] [info] Handle Generate Auth Data Request [udm_ueau] [debug] Remote URI: http://**w4s-udr**:8080/nudr-dr/v1/subscription-data/00101 0000000164/authentication-data/authentication-subscripti on [udm_client] [debug] Send a simple HTTP request New SQN (for next round) = 00000000dee0 [udm_ueau] [debug] Remote URI: http://**w4s-udr**:8080/nudr-dr/v1/subscription-data/**00101 0000000164/**authentication-data/authentication-subscript ion [udm_ueau] [info] **Update UDR with PATCH message**, body: [{"from":"","op":"replace","path":"","value":"{\"lastIndexe s\":{\"ausf\":0},\"sqn\":\"00000000dee0\",\"sqnScheme\" :\"NON_ TIME_BASED\"}"}] [udm_client] [debug] Send a simple HTTP request [udm_ueau] [info] **Send 200 OK response to AUSF** [udm_ueau] [info] **AuthInfoResult** {"authType":"5G_AKA","authenticationVector":{"autn":"36 b5f905c80b800058a2a90518916bea","avType":"5G_HE_A KA","kausf":"ac479b19c2c861c729a7e58ea51 fd0283fa53850ec42d76ac208e6f4a50f4ce7","rand":"06a6 83230fc8e4a534fbe0505ce1c68d","xresStar":"9f443f81d1 b467a2ce5aa9e610ebc87e"}} [udm_ueau] [info] Send response to AUSF [udm_ueau] [info] Update sqn in Database

		[udm_ueau] [info] Handle **Authentication Confirmation**	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.3.2.j		
Requirement	Unified Data Repository (UDR)		
Test Objective	UDR node should be running in virtualized container		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Same as 4.3.2.i		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

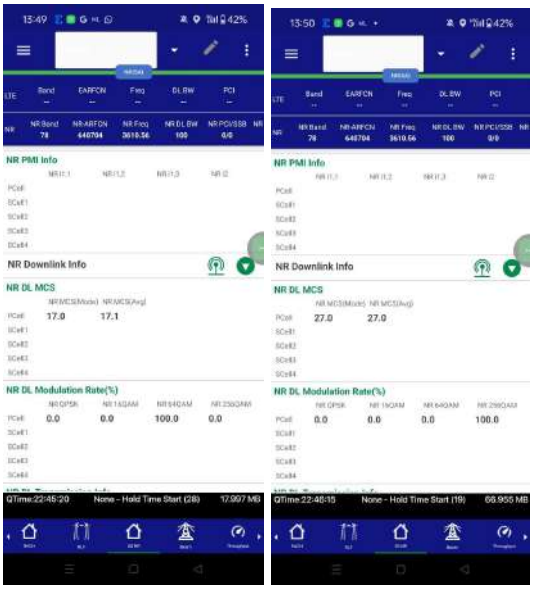
Test ID	4.3.2.k	
Requirement	User Plane Function (UPF)	
Test Objective	UPF node should be running in virtualized container	
Test Description	**Set Steps**	**Acceptance Criteria**
	goto core directory **docker compose -f docker-compose-w4s.yaml up -d** check docker status by **docker ps** to check upf logs run **docker logs -f w4s-upf** **Attach UE with private 5g network**	Received **N4_SESSION_ESTABLISHMENT_REQUEST** seid 0x7 [upf_n4] [info] pfcp_session::add(far) seid 0x7 [upf_n4] [info] pfcp_session::add(pdr) seid 0x7 rmv outer hdr tun id - GTPU_UDP_IPV4:00000007 **UE IPv4 - 12.0.0.2** Received **N4_SESSION_MODIFICATION_REQUEST** seid 0x7 [upf_n4] [info] pfcp_session::add(far) seid 0x7 [upf_n4] [info] pfcp_session::add(pdr) seid 0x7
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	**4.3.2.m**
Requirement	User Equipment (UE)

Test Objective	UE should be registered with the private 5G Network and the UE should show 5G network in the device to confirm.		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Attach the UE to the 5g network		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	**4.3.2.n**		
Requirement	(Radio) Access Network (RAN)		
Test Objective	RAN should be available		
Test Description	**Set Steps**	**Acceptance Criteria**	
	ssh suadmin@192.1688.x.10 Pass:- Admin@123 sudo systemctl startran sudo systemctl stop ran sudo systemctl status ran tail -f gnb.log	Access the RAN server by following 2.2.a the RAN stack is available in the docker image for w4s-gnb-fhi72 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

5G NR Radio

Test ID	4.4.1.a		
Requirement	Functions for Radio Resource Management: Radio bearer Control,Radio Admission Control, Connection Mobility Control, Dynamic allocation to UEs in both uplink and downlink (scheduling)		
Test Objective	Verify UE (User Equipment) can successfully register to a 5G network and browse data by establishing a data session		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Dynamic Allocation: open sigmaML application in the mobile phone to check NR Downlink Info → NR DL MCS		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.1.a	
Requirement	Functions for Radio Resource Management: Radio bearer Control,Radio Admission Control, Connection Mobility Control, Dynamic allocation to UEs in both uplink and downlink (scheduling)	
Test Objective	Verify UE (User Equipment) can successfully register to a 5G network and browse data by establishing a data session	
Test Description	**Set Steps**	**Acceptance Criteria**
	Radio Admission: open wireshark and apply the **nr-rrc** filter.	**NR Radio Resource Control (RRC) protocol** ue-Identity: ng-5G-S-TMSI-Part1 (0) ng-5G-S-TMSI-Part1: establishmentCause: mps-PriorityAccess (8) **NR Radio Resource Control (RRC) protocol** DL-CCCH-Message message: c1 (0) c1: rrcSetup (1) rrcSetup rrc-TransactionIdentifier: 1 criticalExtensions: rrcSetup (0) rrcSetup <NR Radio Resource Control (RRC) protocol> radioBearerConfig masterCellGroup rlc-BearerToAddModList: 1 item mac-CellGroupConfig physicalCellGroupConfig spCellConfig **NR Radio Resource Control (RRC) protocol** c1: rrcSetupComplete (2) rrcSetupComplete rrcSetupComplete selectedPLMN-Identity: 1 dedicatedNAS-Message: Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Plain NAS 5GS Message Extended protocol discriminator: 5G mobility management messages type: Plain NAS message, not security protected (0) Message type: Registration request 5GS registration type NAS key set identifier 5GS mobile identity

		Type of identity: 5G-GUTI (2) Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) AMF Region ID: 1 0000 0000 01.. .... = AMF Set ID: 1 ..00 0001 = AMF Pointer: 1 5G-TMSI: 15 (0x0000000f) TMSI/P-TMSI/M-TMSI/5G-TMSI: 15 UE security capability NAS message container ng-5G-S-TMSI-Value: ng-5G-S-TMSI-Part2 (1)	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.1.b
Requirement	Encryption and integrity protection of data; - Selection of an AMF at UE attachment when no routing to an AMF can be determined from the information provided by the UE

Test Objective	Encryption and integrity protection of data should be available while UE is doing signaling before establishing the data connection		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Attach a UE to the network	The security parameters can be verified via the security command message	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.1.c	
Requirement	Routing of User Plane data towards UPF(s);	
Test Objective	UE data path should establish to/from UPF	
Test Description	**Set Steps**	**Acceptance Criteria**
	open wireshark application and put **gtp** filter	Internet Protocol Version 4, Src: **192.168.2.10,** Dst: **192.168.70.155** Protocol: UDP (17) Source Address: 192.168.2.10 <Source or Destination Address: **192.168.2.10**> <[Source Host: **192.168.2.10**]> <[Source or Destination Host: **192.168.2.10**]> Destination Address: **192.168.70.155** <Source or Destination Address: **192.168.70.155**> <[Destination Host: **192.168.70.155**]> <[Source or Destination Host: **192.168.70.155]**> User Datagram Protocol, GPRS Tunneling Protocol Internet Protocol Version 4, Src: **12.0.0.5**, Dst: 172.21.3.100 in which **gnb ip : 192.168.2.10** **upf: 192.168.70.155** **ue ip : 12.0.0.5**

		User Datagram Protocol, Src Port: 2152, Dst Port: 2152 UDP payload (85 bytes)	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.1.d	
Requirement	Routing of Control Plane information towards AMF	
Test Objective	UE signaling path should connect to AMF	
Test Description	**Set Steps**	**Acceptance Criteria**
	open wireshark application and apply **NGAP** filter	**NG Application Protocol** (InitialUEMessage) → NGAP-PDU: initiatingMessage (0) initiatingMessage → value → InitialUEMessage → protocolIEs: 5 items → Item 0: id-RAN-UE-NGAP-ID Item 1: id-NAS-PDU Item 2: id-UserLocationInformation Item 3: id-RRCEstablishmentCause Item 4: id-UEContextRequest

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.1.e	
Requirement	Connection setup and release;	
Test Objective	UE should attach and release to/from private 5G network	
Test Description	**Set Steps**	**Acceptance Criteria**
	apply **NGAP** filter in wireshark in (UEContextReleaseCommand) message	NGAP-PDU: initiatingMessage --> initiatingMessage --> value --> UEContextReleaseCommand --> protocolIEs: 2 items --> Item 0: id-UE-NGAP-IDs ProtocolIE-Field id: id-UE-NGAP-IDs Item 1: id-Cause ProtocolIE-Field id: id-Cause value → aMF-UE-NGAP-ID: 70 rAN-UE-NGAP-ID: 3 **Cause: nas** **nas: deregister**

	in(UEContextReleaseComplete) message	NG Application Protocol (UEContextReleaseComplete) --> NGAP-PDU: successfulOutcome --> successfulOutcome --> procedureCode: id-UEContextRelease **NG Application Protocol (UEContextReleaseComplete)** NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-UEContextRelease (41) criticality: reject (0) value UEContextReleaseComplete protocolIEs: 2 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: ignore (1) value **AMF-UE-NGAP-ID: 70** Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID criticality: ignore value **RAN-UE-NGAP-ID: 3**

Overall Test Result	Pass: ☐	Fail: ☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.1.g	
Requirement	Scheduling and transmission of system broadcast information (originated from the AMF or OAM);	
Test Objective	gNB should transmit MIB and SIB information	
Test Description	**Set Steps**	**Acceptance Criteria**
	for MIB message- open wireshark application and apply **NR-RRC** filter	MAC-NR BCCH PDU -->\ NR Radio Resource Control (RRC) protocol -->\ message: mib -->\ mib -->\ systemFrameNumber: b0 [bit length 6, 2 LSB pad bits, 1011 00.. decimal value 44]\ subCarrierSpacingCommon: scs30or120 (1)\ ssb-SubcarrierOffset: 0\ dmrs-TypeA-Position: pos2 (0)\ pdcch-ConfigSIB1\ cellBarred: notBarred (1)\ intraFreqReselection: notAllowed (1)\ spare: 00 [bit length 1, 7 LSB pad bits, 0... .... decimal value 0]
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.4.1.g	
Requirement	Scheduling and transmission of system broadcast information (originated from the AMF or OAM);	
Test Objective	gNB should transmit MIB and SIB information	
Test Description	**Set Steps**	**Acceptance Criteria**
	for SIB1 message open the wireshark application and apply **NR-RRC** filter	MAC-NR BCCH PDU (116 bytes, on DL-SCH transport) --> NR Radio Resource Control (RRC) protocol --> BCCH-DL-SCH-Message --> message: c1 (0) --> c1: systemInformationBlockType1 (1) --> systemInformationBlockType1 cellSelectionInfo cellAccessRelatedInfo si-SchedulingInfo servingCellConfigCommon <Enumerated Index: 0> ims-EmergencySupport: true (0) <Enumerated Index: 0> eCallOverIMS-Support: true (0) ue-TimersAndConstants uac-BarringInfo
Overall Test Result	Pass:☐	Fail:☐

Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.1.h	
Requirement	Measurement and measurement reporting configuration for mobility and scheduling;	
Test Objective	gNB should transmit measurement report	
Test Description	**Set Steps**	**Acceptance Criteria**
	Apply the filter in wireshark nr-rrc NR Radio Resource Control (RRC) protocol	c1: measurementReport (0) measResultServingMOList Item 0 MeasResultServMO servCellId: 0 measResultServingCell physCellId: 0 measResult cellResults resultsSSB-Cell rsrp: -74dBm <= SS-RSRP < -73dBm (83) rsrq: -10.5dB <= SS-RSRQ < -10.0dB (66) sinr: 23.0dB <= SS-SINR < 23.5dB (93) rsIndexResults

		resultsSSB-Indexes: 1 item Item 0 ResultsPerSSB-Index ssb-Index: 0 ssb-Results rsrp: -74dBm <= SS-RSRP < -73dBm (83) rsrq: -10.5dB <= SS-RSRQ < -10.0dB (66) sinr: 23.0dB <= SS-SINR < 23.5dB (93)	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.1.j	
Requirement	Session Management	
Test Objective	pdusession management should be present	
Test Description	**Set Steps**	**Acceptance Criteria**

	apply ngap||nas-5gs filter in wireshark NG Application Protocol (PDUSessionResourceSetupRequest)	procedureCode: id-PDUSessionResourceSetup (29) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 1 pDUSessionNAS-PDU [truncated]: xxx s-NSSAI pDUSessionResourceSetupRequestTransfer: Item 3: id-UEAggregateMaximumBitRate
	NG Application Protocol (PDUSessionResourceSetupResponse)	NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupResponse

		protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceSetupListSURes ProtocolIE-Field id: id-PDUSessionResourceSetupListSURes (75) criticality: ignore (1) value PDUSessionResourceSetupListSURes: 1 item Item 0 PDUSessionResourceSetupItemSURes pDUSessionID: 1 pDUSessionResourceSetupResponseTransfer: xxx	
Overall Test Result	Pass:☐	Fail:☐	
Remarks			
Name	Name of Verifier	Signature	

Test ID	4.4.1.k	
Requirement	Support of Network Slicing	
Test Objective	2 Different network slicing should support	
Test Description	**Set Steps**	**Acceptance Criteria**

	Follow procedure 2.1 and 2.2	Refer to section 3.XIII for network slicing related message in 5g network message trace logs **Network Slicing : 3.XIII**	
Overall Test Result	Pass:☐	Fail:☐	
Remarks			
Name	Name of Verifier	Signature	

Test ID	4.4.1.l	
Requirement	QoS Flow management and mapping to data radio bearers	
Test Objective	Configure the supported QFI/5qi in Database	
Test Description	**Set Steps**	**Acceptance Criteria**
	Apply ngap||nas-5gs filter in wireshark NG Application Protocol (PDUSessionResourceSetupRequest)	NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items

		Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 1 pDUSessionNAS-PDU [truncated]: xxx s-NSSAI pDUSessionResourceSetupRequestTransfer: xxx PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate Item 1: id-UL-NGU-UP-TNLInformation Item 2: id-PDUSessionType Item 3: id-QosFlowSetupRequestList ProtocolIE-Field id: id-QosFlowSetupRequestList (136) criticality: reject (0) value

		QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem qosFlowIdentifier: 1 qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) nonDynamic5QI fiveQI: 5 allocationAndRetentionPriority Item 3: id-UEAggregateMaximumBitRate
	NG Application Protocol (PDUSessionResourceSetupResponse)	NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupResponse protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceSetupListSURes ProtocolIE-Field id: id-PDUSessionResourceSetupListSURes (75) criticality: ignore (1) value

		PDUSessionResourceSetupListSURes: 1 item Item 0 PDUSessionResourceSetupItemSURes pDUSessionID: 1 pDUSessionResourceSetupResponseTransfer: 0003e0c0a8020a9b96af310001 PDUSessionResourceSetupResponseTransfer dLQosFlowPerTNLInformation uPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a8020a TransportLayerAddress (IPv4): 192.168.2.10 gTP-TEID: 9b96af31 associatedQosFlowList: 1 item Item 0 AssociatedQosFlowItem qosFlowIdentifier: 1	
Overall Test Result	Pass:☐	Fail:☐	
Remarks			
Name	Name of Verifier	Signature	

Test ID	4.4.1.n
Requirement	Distribution function for NAS messages;

Test Objective	NAS messages for Registration , session management		
Test Description	**Set Steps**	**Acceptance Criteria**	
	apply **nas-5gs filter** on wireshark application .	check for the messages below: InitialUEMessage , Registration Request DownlinkNASTransport, Identity request UplinkNASTransport, Identity response DownlinkNASTransport, Authentication request *- UplinkNASTransport, Authentication response DownlinkNASTransport, Security mode command InitialContextSetupRequest InitialContextSetupResponse, UplinkNASTransport, UplinkNASTransport PDU session establishment request PDU session establishment accept PDUSessionResourceSetupRequestTransfer PDUSessionResourceSetupRequest	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

NG User Plane

Test ID	4.4.3.a

Requirement	The NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.	
Test Objective	gNB should connect to core network-UPF	
Test Description	**Set Steps**	**Acceptance Criteria**
	Apply filter ngap in Wireshark NG Application Protocol (PDUSessionResourceSetupRequest)	NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq PDUSessionID: 7 pDUSessionNAS-PDU [truncated]: xxx

		Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Plain NAS 5GS Message s-NSSAI pDUSessionResourceSetupRequestTransfer: xxx PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a84686 gTP-TEID: 00000041 Item 2: id-PDUSessionType Item 3: id-QosFlowSetupRequestList Item 3: id-UEAggregateMaximumBitRate
	PDUSessionResourceSetupResponse	NG Application Protocol (PDUSessionResourceSetupResponse) NGAP-PDU: successfulOutcome (1)

		successfulOutcome procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupResponse protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field Item 2: id-PDUSessionResourceSetupListSURes ProtocolIE-Field id: id-PDUSessionResourceSetupListSURes (75) criticality: ignore (1) value PDUSessionResourceSetupListSURes: 1 item Item 0 PDUSessionResourceSetupItemSURes pDUSessionID: 1 pDUSessionResourceSetupResponseTransfer: 0003e0c0a8020a521f22c50001

		PDUSessionResourceSetupResponseTransfer dLQosFlowPerTNLInformation uPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a8020a [bit length 32, 1100 0000 1010 1000 0000 0010 0000 1010 decimal value 3232236042] TransportLayerAddress (IPv4): 192.168.2.10 gTP-TEID: 521f22c5 associatedQosFlowList: 1 item	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.4.3.b
Requirement	The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RAN node and the UPF.

Test Objective	A GTP-U tunnel should be establish between gNB and UPF after attaching a UE in the network	
Test Description	**Set Steps**	**Acceptance Criteria**
	Attach UE Apply gtp filter in wireshark	Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.70.155 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 104 Identification: 0x7c97 (31895) 010. .... = Flags: 0x2, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: UDP (17) Header Checksum: 0xf3f7 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.2.10 Destination Address: 192.168.70.155
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.4.3.c	
Requirement	NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF.	
Test Objective	To check 5QI value in QOS Flow	
Test Description	**Set Steps**	**Acceptance Criteria**
	Apply ngap filter in wireshark NG Application Protocol (PDUSessionResourceSetupRequest)	NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 7

		pDUSessionNAS-PDU [truncated]: xxx s-NSSAI pDUSessionResourceSetupRequestTransfer: xxx PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate Item 1: id-UL-NGU-UP-TNLInformation Item 2: id-PDUSessionType Item 3: id-QosFlowSetupRequestList ProtocolIE-Field id: id-QosFlowSetupRequestList (136) criticality: reject (0) value QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem qosFlowIdentifier: 6 qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) nonDynamic5QI fiveQI: 9 allocationAndRetentionPriority Item 3: id-UEAggregateMaximumBitRate
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		

Name	Name of Verifier	Signature	

Test ID	4.4.3.d	
Requirement	Further details of NG-U compliance as per 3GPP standards	
Test Objective	NG-U Compliance as per 3GPP standards should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	Informative	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

NG Control Plane

Test ID	4.4.4.b	
Requirement	NG interface management	
Test Objective	NGSetupReq/Resp message should be captured in wireshark while gNB connect to AMF	
Test Description	**Set Steps**	**Acceptance Criteria**
	Apply ngap filter in wireshark NG Application Protocol (NGSetupRequest)	NGAP-PDU: initiatingMessagNG Application Protocol (NGSetupResponse) 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)

	NG Application Protocol (NGSetupResponse)	gNB-ID: gNB-ID (0) gNB-ID: 0000e000 Item 1: id-RANNodeName Item 2: id-SupportedTAList Item 3: id-DefaultPagingDRX NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-NGSetup (21) criticality: reject (0) value NGSetupResponse protocolIEs: 4 items Item 0: id-AMFName ProtocolIE-Field id: id-AMFName (1) criticality: reject (0) value AMFName: OAI-AMF Item 1: id-ServedGUAMIList ProtocolIE-Field id: id-ServedGUAMIList (96) criticality: reject (0) value ServedGUAMIList: 1 item Item 0 ServedGUAMIItem

		gUAMI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) aMFRegionID: 01 aMFSetID: 0040 aMFPointer: 04 Item 2: id-RelativeAMFCapacity Item 3: id-PLMNSupportList	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.4.4.c	
Requirement	UE context management	
Test Objective	UE Context Release and UE capability message should be captured in gNB wireshark	
Test Description	**Set Steps**	**Acceptance Criteria**
	Apply ngap filter in wireshark NG Application Protocol (InitialContextSetupRequest)	NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-InitialContextSetup (14) criticality: reject (0) value InitialContextSetupRequest protocolIEs: 9 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-GUAMI Item 3: id-AllowedNSSAI Item 4: id-UESecurityCapabilities Item 5: id-SecurityKey Item 6: id-MobilityRestrictionList Item 7: id-MaskedIMEISV Item 8: id-NAS-PDU ProtocolIE-Field

		id: id-NAS-PDU (38) criticality: ignore (1) value NAS-PDU: xxx Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0xbaab6b1f Sequence number: 1
	NG Application Protocol (InitialContextSetupResponse)	NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-InitialContextSetup (14) criticality: reject (0) value InitialContextSetupResponse protocolIEs: 2 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Stream Control Transmission Protocol NG Application Protocol (UplinkNASTransport) NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-UplinkNASTransport (46)

		criticality: ignore (1) value UplinkNASTransport protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-NAS-PDU ProtocolIE-Field id: id-NAS-PDU (38) criticality: reject (0) value NAS-PDU: 7e023851d135018a56b0 Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) Message authentication code: 0x3851d135 Sequence number: 1 Item 3: id-UserLocationInformation	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.4.4.d	
Requirement	UE mobility management	
Test Objective	Check DL/UL NAS message transfer while UE registration	
Test Description	**Set Steps**	**Acceptance Criteria**
	Apply ngap filter in wireshark NG Application Protocol (InitialUEMessage)	NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-InitialUEMessage (15) value InitialUEMessage protocolIEs: 6 items Item 0: id-RAN-UE-NGAP-ID Item 1: id-NAS-PDU ProtocolIE-Field id: id-NAS-PDU (38) criticality: reject (0) value NAS-PDU: xxx Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Plain NAS 5GS Message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0

		.... 0000 = Security header type: Plain NAS message, not security protected (0) Message type: Registration request (0x41) 5GS registration type NAS key set identifier 5GS mobile identity UE security capability NAS message container Item 2: id-UserLocationInformation Item 3: id-RRCEstablishmentCause Item 4: id-FiveG-S-TMSI Item 5: id-UEContextRequest	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.4.4.e	
Requirement	Transport of NAS messages	
Test Objective	NAS signalling should be traceable between gNB and Core	
Test Description	**Set Steps**	**Acceptance Criteria**

		refer test case 4.4.1.n	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.4.g		
Requirement	PDU Session Management		
Test Objective	PDU session Establishment Req/Accept should be captured in wireshark		
Test Description	**Set Steps**	**Acceptance Criteria**	
		refer test case 4.4.3.a	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.4.j	
Requirement	Further details of NG-C compliance as per 3GPP standards	
Test Objective	NG-C Compliance as per 3GPP standards should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	Informative	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Radio Protocol Architecture

Test ID	4.4.7.a	
Requirement	Protocol stack for the user plane, i.e. SDAP, PDCP, RLC and MAC sublayers (terminated in gNB on the network side) should perform the functions as per 3GPP Release 15.	
Test Objective	All 5G Radio protocols should be supported while establishing a connection and data transfer to/from UE	
Test Description	**Set Steps**	**Acceptance Criteria**

	Apply nr-rrc||ngap filter in wireshark RRC Reconfiguration SDAP	cnAssociation: sdap-Config (1) sdap-Config pdu-Session: 1 sdap-HeaderDL: present (0) sdap-HeaderUL: present (0) 1... .... defaultDRB: True mappedQoS-FlowsToAdd: 1 item Item 0 QFI: 1 drb-Identity: 1
	PDCP	pdcp-Config drb discardTimer: infinity (15) pdcp-SN-SizeUL: len18bits (1) pdcp-SN-SizeDL: len18bits (1) headerCompression: notUsed (0) notUsed: NULL t-Reordering: ms100 (14)
	MAC-NR DL-SCH	MAC-NR DL-SCH (LCID:1 385 bytes) (Padding 48 bytes) [Context (RNTI=45799)] Subheader: (LCID:1 385 bytes)

	RLC	RLC-NR UEId=1 [DL] [AM] SRB:1 [DATA] (P) SN=7 [383-bytes] [Context] AM Header (P) SN=7 AM Data [truncated]: xxx	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.4.7.b	
Requirement	The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15 :	
Test Objective	All 5G Radio protocols should be supported while establishing a connection and data transfer to/from UE	
Test Description	**Set Steps**	**Acceptance Criteria**
	As tested in above testcases	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		

Name	Name of Verifier	Signature	

Test ID	4.4.7.c		
Requirement	PDCP, RLC and MAC sublayers (terminated in gNB on the network side) should perform the functions listed in 3GPP Standards.		
Test Objective	All 5G Radio protocols should be supported while establishing a connection and data transfer to/from UE		
Test Description	**Set Steps**	**Acceptance Criteria**	
	same as 4.4.7.a		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.4.7.d
Requirement	RRC (terminated in gNB on the network side) performs the functions listed in 3GPP Standards.
Test Objective	All 5G Radio protocols should be supported while establishing a connection and data transfer to/from UE

Test Description	**Set Steps**	**Acceptance Criteria**	
	Apply nr-rrc||ngap filter in wireshark NR Radio Resource Control (RRC) protocol	DL-CCCH-Message message: c1 (0) c1: rrcSetup (1) rrcSetup rrc-TransactionIdentifier: 1 criticalExtensions: rrcSetup (0) rrcSetup radioBearerConfig masterCellGroup [truncated]: xxx CellGroupConfig cellGroupId: 0 rlc-BearerToAddModList: 1 item mac-CellGroupConfig physicalCellGroupConfig spCellConfig	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.4.7.e

Requirement	NAS control protocol (terminated in AMF on the network side) performs the functions listed in 3GPP Standards.for instance: authentication, mobility management, security control.	
Test Objective	NAS protocols should be supported while establishing a connection to/from UE	
Test Description	**Set Steps**	**Acceptance Criteria**
	Apply nas-5gs||ngap filter in wireshark Authentication Request	initiatingMessage procedureCode: id-DownlinkNASTransport (4) criticality: ignore (1) value DownlinkNASTransport protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-NAS-PDU ProtocolIE-Field id: id-NAS-PDU (38) criticality: reject (0) value NAS-PDU: xxx Non-Access-Stratum 5GS (NAS)PDU Plain NAS 5GS Message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0

	Authentication Response	.... 0000 = Security header type: Plain NAS message, not security protected (0) Message type: Authentication request (0x56) 0000 .... = Spare Half Octet: 0 NAS key set identifier - ngKSI ABBA Authentication Parameter RAND - 5G authentication challenge Element ID: 0x21 RAND value: xxx Authentication Parameter AUTN (UMTS and EPS authentication challenge) - 5G authentication challenge Element ID: 0x20 Length: 16 AUTN value: db78678ffca780009d87cb5802b52456 SQN xor AK: db78678ffca7 AMF: 8000 MAC: 9d87cb5802b52456 NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-UplinkNASTransport (46) criticality: ignore (1) value UplinkNASTransport

		protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 101 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 1 Item 2: id-NAS-PDU ProtocolIE-Field id: id-NAS-PDU (38) criticality: reject (0) value NAS-PDU: xxx Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) .... 0001 = Security header type: Integrity protected (1) Message authentication code: 0x3e8330b2

		Sequence number: 9 Plain NAS 5GS Message Extended protocol discriminator: 5G mobility management messages (126) .... 0000 = Security header type: Plain NAS message, not security protected (0) Message type: Authentication response (0x57) Authentication response parameter Element ID: 0x2d Length: 16 RES: d446904d4e82cc8e2f7a0012128aa9b3 Item 3: id-UserLocationInformation	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

4.8 Router Firewall specs

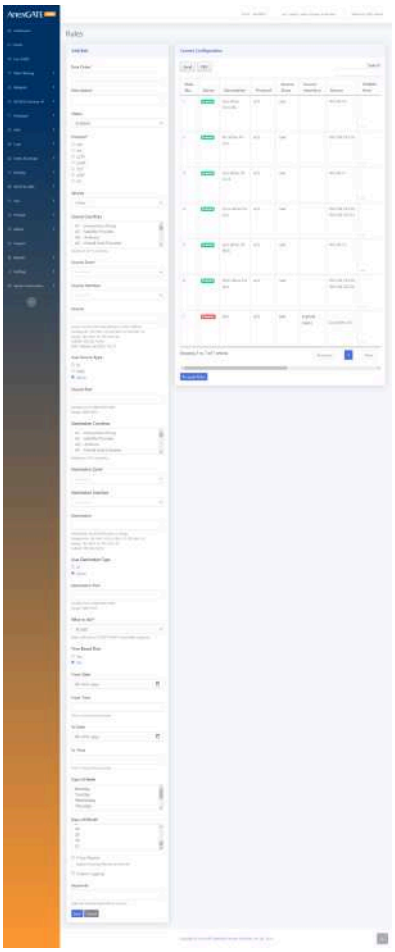
Test ID	4.8.1(a)
Requirement	1 Gigabit Base-T (Cu) = 6 ports or higher(as required)
Test Objective	6*GE copper-LAN/WAN configurable 6*1G SFP LAN/WAN configurable

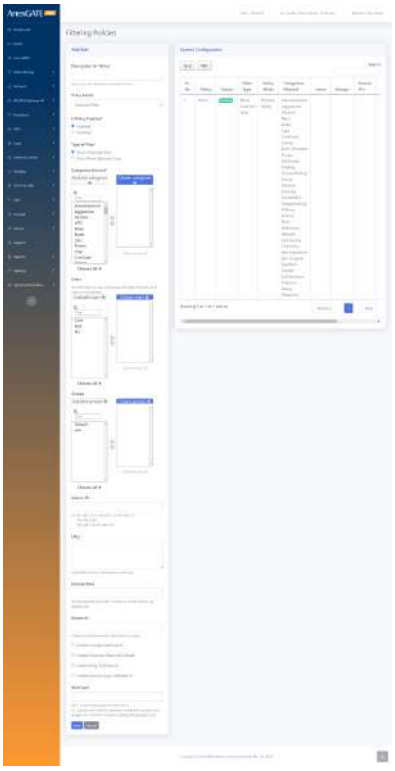
Test Description	**Set Steps**	**Acceptance Criteria**	
	Visual Inspection		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.1(b)		
Requirement	WAN Interface Modified Clause: 2 x 1G Gigabit Ethernet SFP+ports.		
Test Objective	6*1G SFP LAN/WAN configurable		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Visual Inspection		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

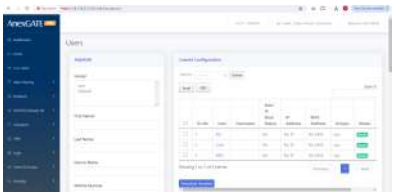
Test ID	4.8.1(c)		
Requirement	Management Port 10/100 Mbps RJ 45 Management port		
Test Objective	Management port should be supported		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Default LAN Interface(On Firewall mentioned as LAN 1) IP Address on Management Port : 192.168.100.1 Management Port Access : https://192.168.100.1:4443	By following IP address we can access Management port of firewall and configure required policies and rules as per requirement	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.2
Requirement	**Firewall Features**
Test Objective	1.Layer 2 and Layer 3 2.Application visibility and control(AVC) 3.User Identity

	4.NAT 5.VPN 6.Next Generation Intrusion prevention system(IPS) 7.Zero day protection / malware protection Bandwidth Aggregation 8.web security essential / URL Filters	
Test Description	**Set Steps**	**Acceptance Criteria**
	1. Firewall --> Rules. Here the forwarding and blocking can be done based on Layer 2 and Layer 3  2. Application Control can be configured under Web Filtering --> Policies and Visibility can be verified under Logs	By following set-steps mentioned we can configure firewall with different features to meet our dependency

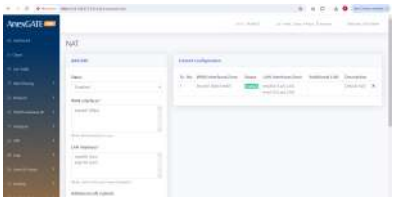


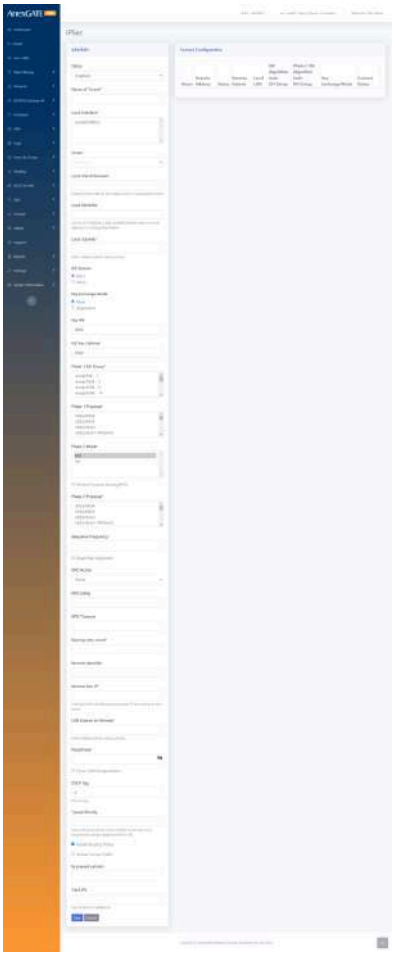
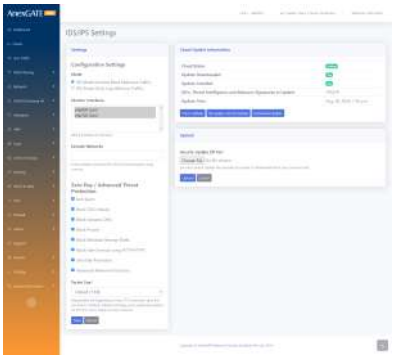
3. User & Groups ---> Users. Here Users can be created and based on that Policies can be applied

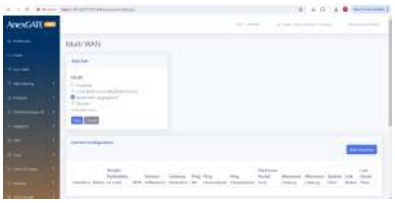




4. Under Network tab. Different types of NAT can be created. Default NAT configuration : Network ---> NAT



	5. Under VPN option. Different options are available under VPN (IPsec, SSL)  6. IDS/IPS/Gateway AV --> IDS/IPS settings  7. In IDS/IPS/Gateway AV --> IDS/IPS settings. Different options are available along with Zero Day Protection/ Malware Protection. Bandwidth Aggregation : Network --> Multi WAN	

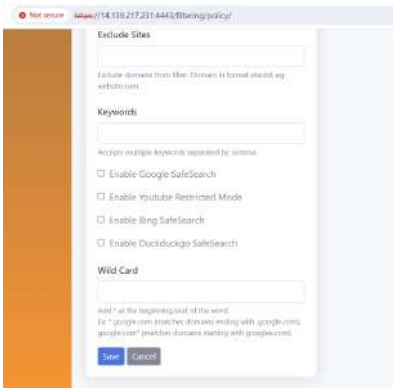
	 8. Under Web Filtering option. Here Policies can be created based on the requirements. Web Filtering --> Policies		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Web Filtering

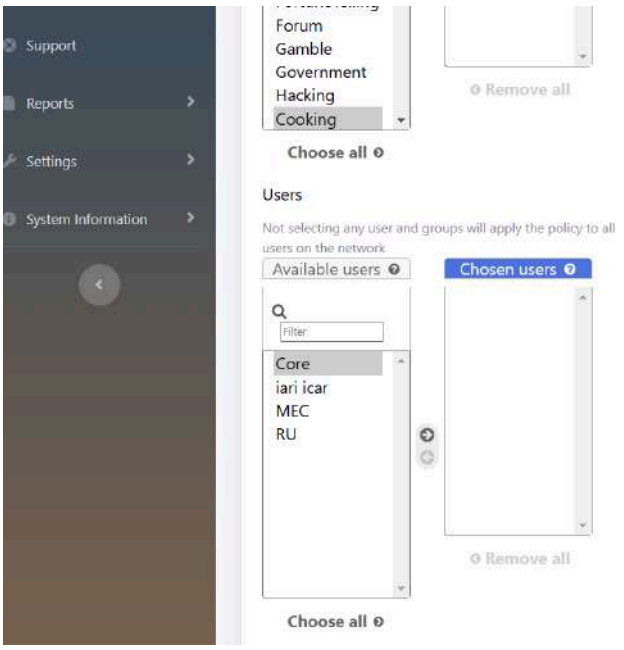
Test ID	4.8.4(a)		
Requirement	Control access to websites and website categories (e.g. business, news, sports, social media)		
Test Objective	Control access to websites and website categories		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Policies will be applied under Web Filtering ---> Policies		
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.8.4(b)	
Requirement	Integrate into Active Directory, applying policies to specific users or user groups.	
Test Objective	Integrate into Active Directory, applying policies to specific users or user groups.	
Test Description	**Set Steps**	**Acceptance Criteria**

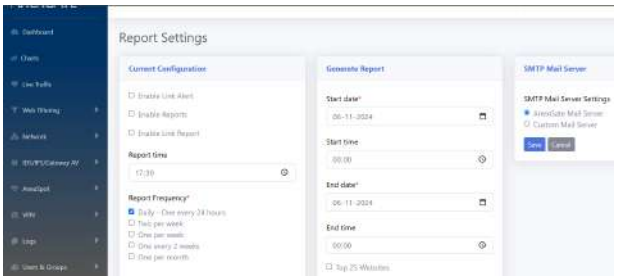
	Integration option is available under Anexspot --> Settings. After the Integration is done we can apply policies to Users and Groups	Input the field for active directory in the firewall 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

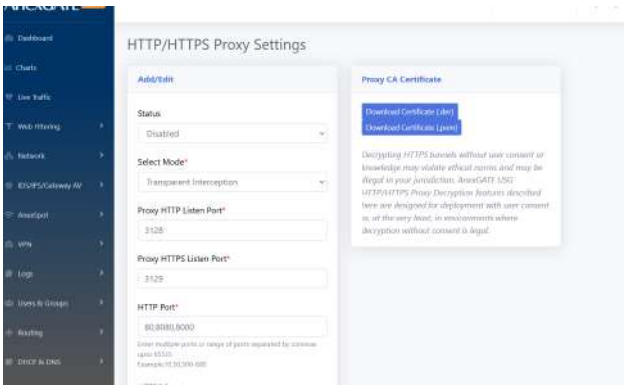
Test ID	4.8.4(c)	
Requirement	Enforce Safe Search	
Test Objective	Enforce Safe search	
Test Description	**Set Steps**	**Acceptance Criteria**
	Present in Web Filtering --> Policies scroll to end of the page to find safe search	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.8.4(d)
Requirement	Block or control access to Cloud services.
Test Objective	Block or control access to Cloud services.

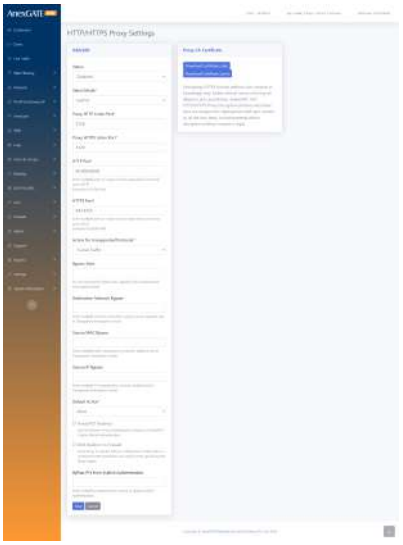
Test Description	**Set Steps**	**Acceptance Criteria**	
	For blocking refer 4.8.4.a For access control Policies will be applied under Web Filtering ---> Policies and navigate to users to apply these policies to specific users for access control		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.4(e)	
Requirement	Detailed web access reports (by user, group, website)	
Test Objective	Detailed web access reports	
Test Description	**Set Steps**	**Acceptance Criteria**

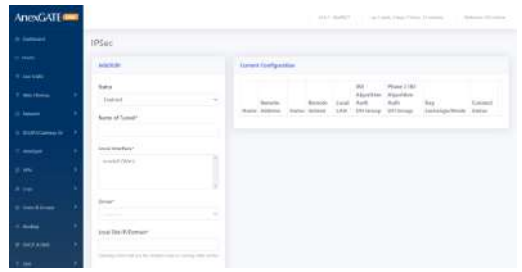
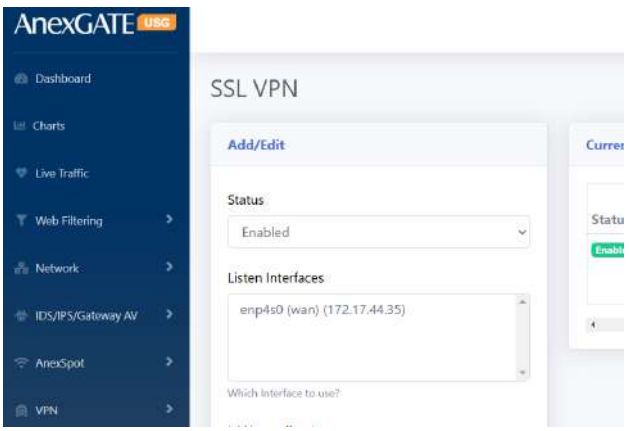
	Can be seen under **Reports section**		
Overall Test Result	Pass:☐	Fail:☐	
Comments	Generate Report from this Section		
Name	Name of Verifier	Signature	

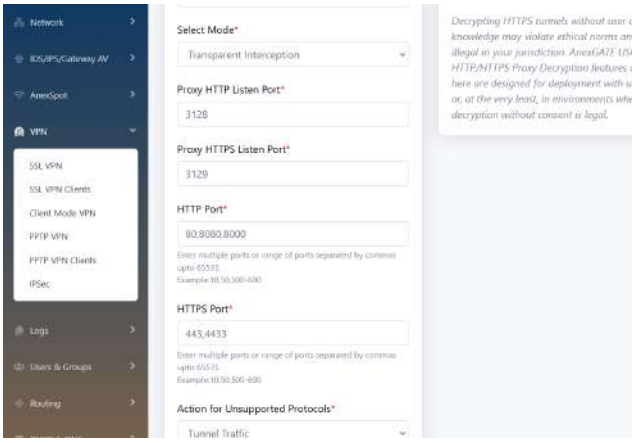
Test ID	4.8.4(f)	
Requirement	Full SSL Inspection support	
Test Objective	Full SSL Inspection support	
Test Description	**Set Steps**	**Acceptance Criteria**
	Configured under **Web Filtering ---> HTTP/HTTPS Proxy**	

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.4(g)	
Requirement	Transparent solution (or explicit proxy support)	
Test Objective	Transparent solution	
Test Description	**Set Steps**	**Acceptance Criteria**
	Configured under **Web Filtering ---> HTTP/HTTPS Proxy**	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Secure Remote Access

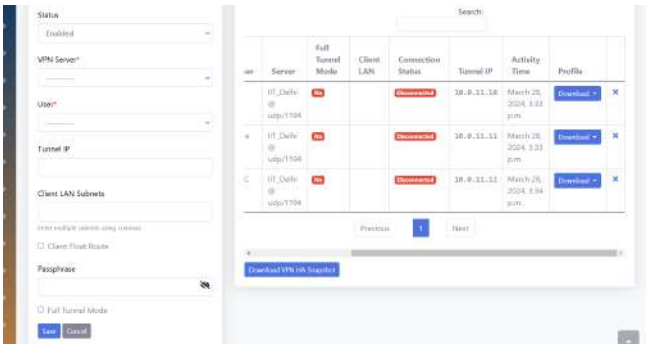
Test ID	4.8.6(a)	
Requirement	SSL and IPSec VPN support	
Test Objective	IPSec VPN Encryption: 3DES,AES 128/192/256-bit, AES GCM, Camellia Hash algorithms: MD5, SHA1, SHA2, 256/384/512-bit, PRFSHA1, PRFSHA256 Diffie Hellman modes: 1, 2, 5, 14, 15, 16, 17, 18, 22, 23, 24, 26, 32, 35 Authentication: pre-shared key (PSK), IKEv1, IKEv2 Dead Peer Detection (DPD) Perfect Forward Secrecy (PFS)	
Test Description	**Set Steps**	**Acceptance Criteria**
	Present under VPN options VPN -> SSL VPN	 
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

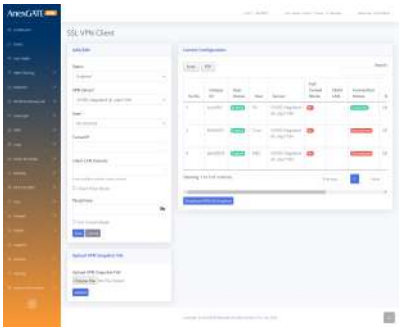
Test ID	4.8.6(b)		
Requirement	Web-Portal and full VPN client application		
Test Objective	IPSec VPN Encryption: 3DES,AES 128/192/256-bit, AES GCM, Camellia Hash algorithms: MD5, SHA1, SHA2, 256/384/512-bit, PRFSHA1, PRFSHA256 Diffie Hellman modes: 1, 2, 5, 14, 15, 16, 17, 18, 22, 23, 24, 26, 32, 35 Authentication: pre-shared key (PSK), IKEv1, IKEv2 Dead Peer Detection (DPD) Perfect Forward Secrecy (PFS)		
Test Description	**Set Steps**	**Acceptance Criteria**	
	The vpn settings can be configured by navigating to vpn section		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.6(c)
Requirement	Site-to-Site IPSec VPN (with Dynamic Routing)

Test Objective	IPSec VPN Encryption: 3DES,AES 128/192/256-bit, AES GCM, Camellia Hash algorithms: MD5, SHA1, SHA2, 256/384/512-bit, PRFSHA1, PRFSHA256 Diffie Hellman modes: 1, 2, 5, 14, 15, 16, 17, 18, 22, 23, 24, 26, 32, 35 Authentication: pre-shared key (PSK), IKEv1, IKEv2 Dead Peer Detection (DPD) Perfect Forward Secrecy (PFS)		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Can be configured under VPN --> Ipsec		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.6(f)	
Requirement	Two-Factor authentication support (e.g. Secure Token)	
Test Objective	IPSec VPN Encryption: 3DES,AES 128/192/256-bit, AES GCM, Camellia Hash algorithms: MD5, SHA1, SHA2, 256/384/512-bit, PRFSHA1, PRFSHA256 Diffie Hellman modes: 1, 2, 5, 14, 15, 16, 17, 18, 22, 23, 24, 26, 32, 35 Authentication: pre-shared key (PSK), IKEv1, IKEv2 Dead Peer Detection (DPD) Perfect Forward Secrecy (PFS)	
Test Description	**Set Steps**	**Acceptance Criteria**

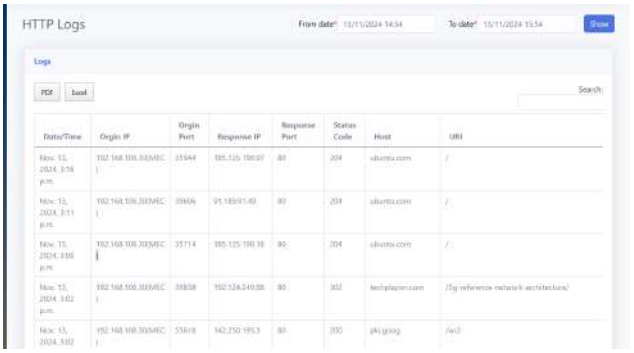
	Two-factor authentication can be done using the cert file and the password authentication in **VPN section→SSL VPN Clients**		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.6(g)	
Requirement	High performance VPN concentrator solution	
Test Objective	Secure SSL VPN Support Encryptions : 3DES,AES (128 & 256),RC2, Blowfish, AES GCM Support Message integrity : MD-5, SHA-1, SHA (256 ,384 ,512) Multi-layered Client Authentication: Certificate & Password Support TCP & UDP Tunnelling Network access - Split and Full Tunnel Mode	
Test Description	**Set Steps**	**Acceptance Criteria**
	VPN Concentrator can be configured under **VPN --> SSL VPN and SSL VPN Clients and IPsec**	

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

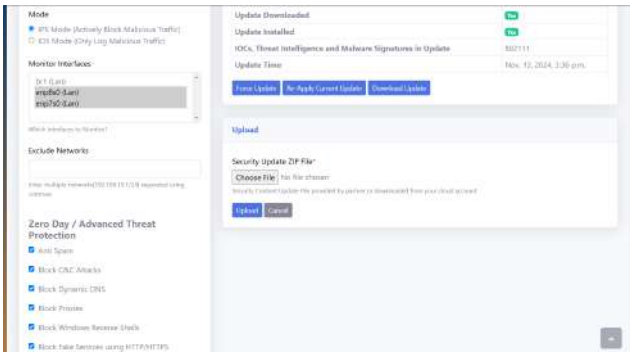
Application Control

Test ID	4.8.7(a)		
Requirement	Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps)		
Test Objective	Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps)		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Using **Web Filtering ---> Policies** **Reference by:-** **4.8.4.a** **4.8.4.d** **4.8.4.e**		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.7(b)		
Requirement	Full network visibility of HTTP and HTTPS traffic		
Test Objective	Should support full network visibility of HTTP and HTTPs Traffic		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check under **Logs→HTTP Logs**		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.7(c)	
Requirement	Control access to specific applications (e.g. Web Games, Video Streaming)	
Test Objective	Control of access to specific application	
Test Description	**Set Steps**	**Acceptance Criteria**

	It can be configured under **Web Filtering --> Policies** **Reference By :-** **4.8.4.d**		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

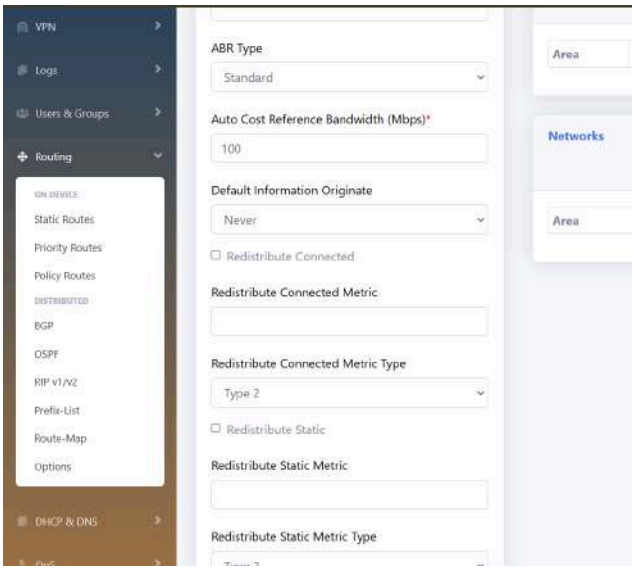
Test ID	4.8.7(d)	
Requirement	Block access to malicious content or websites	
Test Objective	Should block access to malicious content	
Test Description	**Set Steps**	**Acceptance Criteria**
	Present under **IDS/IPS Settings**	
Overall Test Result	Pass:☐	Fail:☐

Remarks	select IPS for blocking IDS is for reporting		
Name	Name of Verifier	Signature	

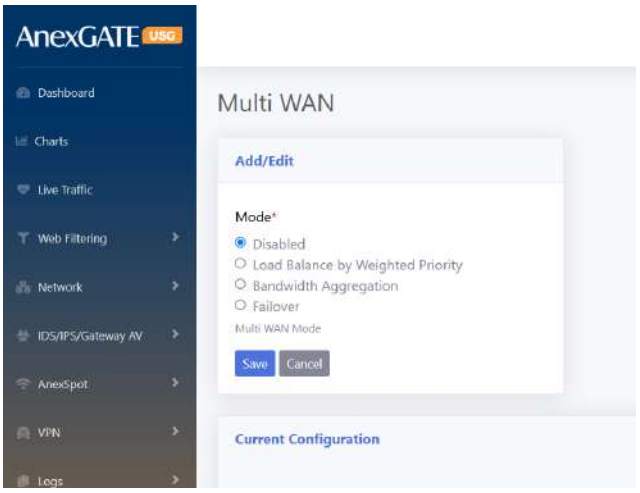
Test ID	4.8.7(e)		
Requirement	Detailed reporting and network visibility		
Test Objective	Should provide detailed reporting and network visibility		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Checked under **Logs optio**n and **Reports option** **Reference By:-** **4.8.4.e** **4.8.7.b**		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Intelligent Networking

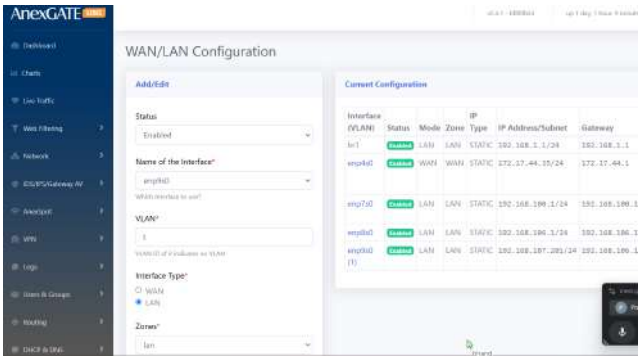
Test ID	4.8.8(a)
Requirement	Dynamic routing (OSPF/BGP/RIP)

Test Objective	Routing configuration support for firewall		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Dynamic Routing can be configured under the **Routing option**. Different options are available for OSPF/BGP/RIP		
Overall Test Result	Pass:☐	Fail:☐	
Comments	These settings can be configured as required		
Name	Name of Verifier	Signature	

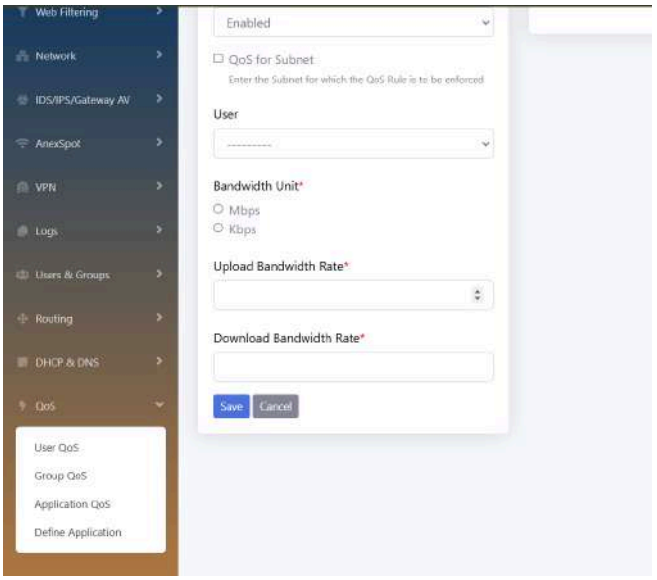
Test ID	4.8.8(b)	
Requirement	Load-Balancing and ECMP	
Test Objective	Multi Link Auto Failover :Tethering Weighted Round Robin & Policy based Load balancing and Bandwidth Aggregation Transparent Mode, Route Mode , L2 Bridge Mode Configurable LAN/WAN/DMZ Ports NAT- DNAT ,SNAT	
Test Description	**Set Steps**	**Acceptance Criteria**

	Present under **Network --> Multi WAN** **Transparent Mode : web filtering ->HTTP/HTTPS Proxy Settings** **routing -> static routes** ECMP through multi wan and routing		
Overall Test Result	Pass:☐	Fail:☐	
Comments	Can be configured as required		
Name	Name of Verifier	Signature	

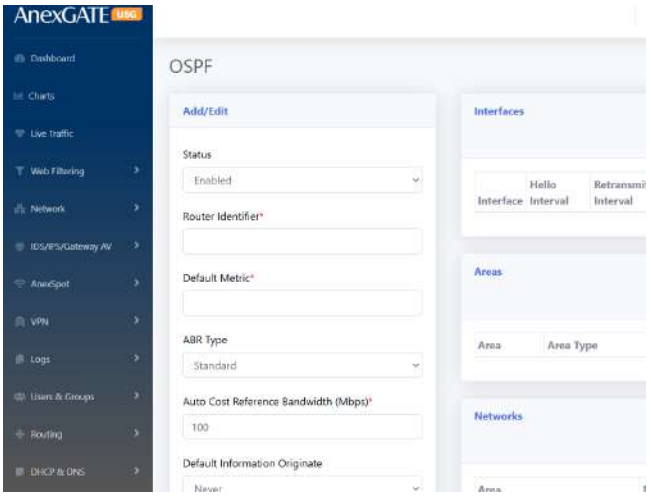
Test ID	4.8.8(c)	
Requirement	802.1Q VLAN and Layer2 switching support	
Test Objective	VLAN and layer 2 switching support	
Test Description	**Set Steps**	**Acceptance Criteria**

	Different VLANs can be configured for interfaces under **Network ---> WAN/LAN**		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.8(d)	
Requirement	Rich traffic/shaping QOS support	
Test Objective	Verify QOS configuration support in Firewall	
Test Description	**Set Steps**	**Acceptance Criteria**

	QOS can be configured under the **QOS option**. Different options are available for **QOS (User QOS, Group QOS and Application QOS)**		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.8.8(e)	
Requirement	Dynamic routing over VPN (e.g. OSPF)	
Test Objective	Verify Dynamic routing over VPN (e.g. OSPF)	
Test Description	**Set Steps**	**Acceptance Criteria**

	Dynamic Routing can be configured over VPN. OSPF and BGP routes will be advertised over the VPN tunnel		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

4.9 Server 1 with 5G Core, IMS and NMS software

Processors

Test ID	4.9.1.a	
Requirement	**Modified Clause:** 3rd Gen Intel Xeon Gold 2.1GHz , 24Cor or equivalent. Each servers with minimum 1 Processors and 2 Socket or higher as required.	
Test Objective	Server should be 3rd Gen Intel Xeon Gold 2.1GHz , 24Cor or equivalent. Each servers with minimum 1 Processors and 2 Socket or higher as required.	
Test Description	**Set Steps**	**Acceptance Criteria**

	Login to Server to check processor details ssh suadmin@192.168.x.20 password: Admin@123 lscpu	Architecture: x86_64 CPU op-mode(s): 32-bit, 64-bit Address sizes: 46 bits physical, 57 bits virtual Byte Order: Little Endian CPU(s): 48 On-line CPU(s) list: 0-47 Vendor ID: GenuineIntel Model name: Intel(R) Xeon(R) Gold 5317 CPU @ 3.00GHz CPU family: 6 Model: 106 Thread(s) per core: 2 Core(s) per socket: 12 Socket(s): 2 Stepping: 6 CPU max MHz: 3600.0000	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Memory

Test ID	4.9.2.a	
Requirement	DDR5-4800 or above 64 GB scalable upto 256 GB or above Modified Clause: DDR4 or above 64 GB scalable upto 256 GB or above	
Test Objective	DDR4 or above 64 GB scalable upto 256 GB or above	
Test Description	**Set Steps**	**Acceptance Criteria**
	sudo dmidecode --type 17	Handle 0x1110, DMI type 17, 92 bytes Memory Device Array Handle: 0x1000 Error Information Handle: Not Provided Total Width: 72 bits Data Width: 64 bits **Size: 32 GB** Form Factor: DIMM

		Set: 3 **Locator: B1** Bank Locator: Not Specified **Type: DDR4** Handle 0x1100, DMI type 17, 92 bytes Memory Device Array Handle: 0x1000 Error Information Handle: Not Provided Total Width: 72 bits Data Width: 64 bits **Size: 32 GB** Form Factor: DIMM Set: 1 **Locator: A1** Bank Locator: Not Specified **Type: DDR4**	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.9.2.b	
Requirement	Advanced memory redundant technologies like Advanced error-correcting code (ECC) and memory mirroring	
Test Objective	Support for advanced memory redundant technologies like Advanced error-correcting code (ECC) and memory mirroring	
Test Description	**Set Steps**	**Acceptance Criteria**

	sudo dmidecode | grep ECC	Error Correction Type: Single-bit ECC
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Storage

Test ID	4.9.3.a	
Requirement	SAS SSD Storage = 1TB Usable expandable to 5 TB	
Test Objective	SAS SSD Storage = 1TB Should be there. Slots for expandable HDD for 5 TB should be there	
Test Description	**Set Steps**	**Acceptance Criteria**
	verified physically df -h	Filesystem Size Used Avail Use% Mounted on tmpfs 6.3G 4.6M 6.3G 1% /run /dev/mapper/ubuntu--vg-ubuntu--lv 98G 81G 13G 87% / tmpfs 32G 0 32G 0% /dev/shm tmpfs 5.0M 0 5.0M 0% /run/lock /dev/sda2 2.0G 254M 1.6G 14% /boot
Overall Test Result	Pass:☐	Fail:☐

Comments			
Name	Name of Verifier	Signature	

Test ID	4.9.3.b	
Requirement	The server should have front accessible, hot swappable. Enterprise class SSD Drives	
Test Objective		
Test Description	**Set Steps**	**Acceptance Criteria**
	Physical Verification	physically verified
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.9.4.a	
Requirement	Virtualization and OS for all environment	
Test Objective	Virtualization and OS for all environment	
Test Description	**Set Steps**	**Acceptance Criteria**
	lscpu	Virtualization features: Virtualization: VT-x Caches (sum of all): L1d: 1.1 MiB (24 instances) L1i: 768 KiB (24 instances)

		L2: 30 MiB (24 instances) L3: 36 MiB (2 instances)
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Network Interface

Test ID	4.9.5.a	
Requirement	Dual port 1G SFP+ card, 4 x 1G BaseT	
Test Objective	Dual port 1G SFP+ card, 4 x 1G BaseT	
Test Description	**Set Steps**	**Acceptance Criteria**
	Physical Inspection or Login to BIOS of Server to check Network details. commands to check check network interfaces lshw -C network lists detailed information about all network interfaces on your system	Each BCM5720 chip supports up to 2 Ethernet ports (interfaces), each capable of 1 Gbit/s : *-network:0 **description: Ethernet interface** product: NetXtreme BCM5720 Gigabit Ethernet PCIe vendor: Broadcom Inc. and subsidiaries physical id: 0 bus info: pci@0000:32:00.0 logical name: eno12399 version: 00 serial: 04:32:01:9e:b4:0e **size: 1Gbit/s** capacity: 1Gbit/s which means for

	and lspci | grep -i ethernet to list PCI devices related to Ethernet controllers	Broadcom NetXtreme BCM5720 Gigabit Ethernet PCIe **4 x 1Gbit/s** interfaces (two sets of two on different PCI buses). and for Broadcom BCM57412 NetXtreme-E 10Gb RDMA Ethernet Controller **2 x 10Gbit/s** interfaces also 10Gbit/s Controllers are there means 2 x Broadcom BCM57412. Here NIC with multiple ports, such as a 4-port NIC, you would have four 1 Gbit/s ports for the active interface, which could be referred to as "4x1Gbit/s
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

PCIe Slots

Test ID	4.9.5	
Requirement	Minimum 4 x PCIe 16x 4.0 slots for I/O Connectivity or higher as required.	
Test Objective	Minimum 4 x PCIe 16x 4.0 slots for I/O Connectivity or higher as required.	
Test Description	**Set Steps**	**Acceptance Criteria**

	lspci -vv |grep -i pci gives detailed info about all PCIe and show connected devices and their interfaces: sudo dmidecode -t slot | grep PCIe gives detailed info about PCIe slots	These are PCI bridges :  above ; the devices attached to these PCIe bridges. For example, Ethernet controllers and RAID controllers connected through PCIe now by other command : Designation: PCIe Slot 2 Type: x16 PCI Express 4 Designation: PCIe Slot 3 Type: x16 PCI Express 4 Designation: PCIe Slot 6 Type: x16 PCI Express 4 Designation: PCIe Slot 4 Type: x8 PCI Express 4 Designation: PCIe Slot 5 Type: x8 PCI Express 4 Designation: PCIe Slot 7 Type: x16 PCI Express 4 => four entries specifying x16 PCI Express 4: ● PCIe Slot 2 ● PCIe Slot 3 ● PCIe Slot 6 ● PCIe Slot 7 
Overall Test Result	Pass:☐	Fail:☐
Comments		

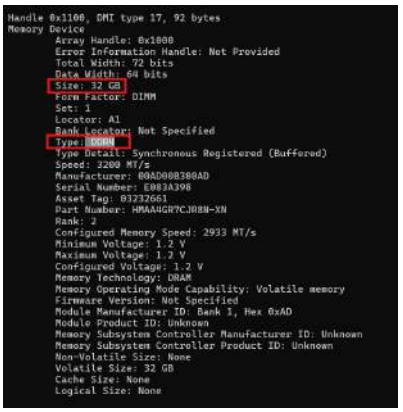
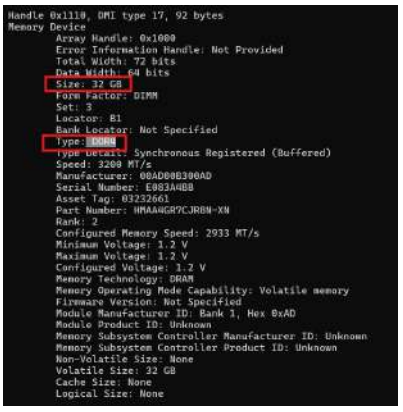
Name	Name of Verifier	Signature	

4.10 Server 2 with 5G MEC Platform and Application Server

Processors

Test ID	4.10.1	
Requirement	Modified Clause: 3rd Gen Intel Xeon Gold 2.1GHz , 24Cor or equivalent. Each servers with minimum 1 Processors and 2 Socket or higher as required	
Test Objective	3rd Gen Intel Xeon Gold 2.1GHz , 24Cor or equivalent. Each servers with minimum 1 Processors and 2 Socket or higher as required	
Test Description	**Set Steps**	**Acceptance Criteria**
	Login to your server, lscpu command displays information about the CPU architecture. /proc/cpuinfo file contains detailed information about the CPU	Intel (R) Xeon(R) Gold 5317 CPU @ 3.00GHz  and for more detailed info : 
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

Memory

Test ID	4.10.2	
Requirement	DDR5-4800 or higher, 128 GB scalable upto 512 GB Modified Clause: DDR4 or above 64 GB scalable upto 256 GB or above	
Test Objective	DDR4 or above 64 GB scalable upto 256 GB or above	
Test Description	**Set Steps**	**Acceptance Criteria**
	Access the server and use the below command to see memory related details sudo dmidecode -t memory	In one location (A1) ;  and in other location (B1) ; 
Overall Test Result	Pass:☐	Fail:☐

Comments			
Name	Name of Verifier	Signature	

Storage

Test ID	4.10.3	
Requirement	SAS SSD Storage = 4TB Usable expandable to 8 TB or above HDD Storage = 4TB Usable expandable to 8 TB or above	
Test Objective	SAS SSD Storage = 4TB Usable expandable to 8 TB or above HDD Storage = 4TB Usable expandable to 8 TB or above	
Test Description	**Set Steps**	**Acceptance Criteria**
	Continue login to same server , command to check storage lsblk -o NAME,SIZE,TYPE,MOUNTPOINT This also can use sudo fdisk -l	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

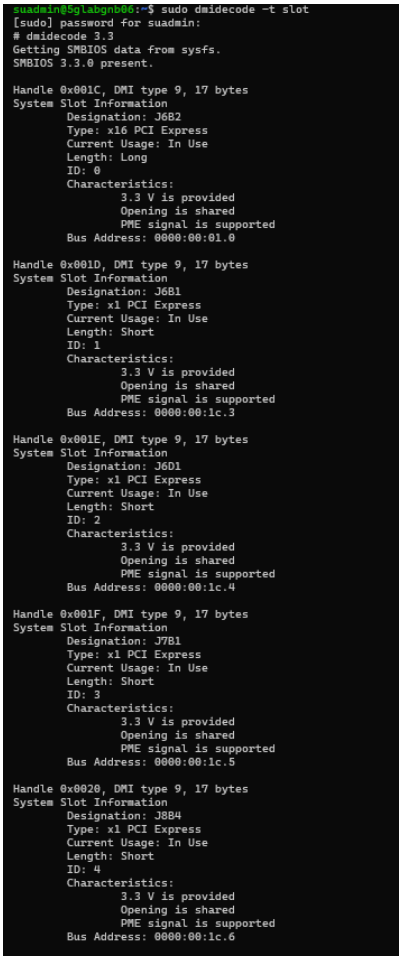
Network

Test ID	4.10.4

Requirement	Single port 1G SFP+ card, 2 x 1G BaseT		
Test Objective	Single port 1G SFP+ card, 2 x 1G BaseT		
Test Description	**Set Steps**	**Acceptance Criteria**	
	In same server ; Execute these commands : sudo apt-get install ethtool or lspci Sudo ethtool eno8303 (this port u can get from ip a command) Here u can see BaseT info and ethernet using twisted pair which typically indicates an SFP+ interface.If you don't see "fibre" or "SFP" and only see "twisted pair," your network interfaces are likely BaseT		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

PCIe Slots

Test ID	4.10.5
Requirement	Minimum 8 x PCIe 16x 4.0 slots for I/O Connectivity or higher as required. Modified Clause: Minimum 4 x PCIe 16x 4.0 slots for I/O Connectivity or higher" as required
Test Objective	Minimum 8 x PCIe 16x 4.0 slots for I/O Connectivity or higher as required.

	Modified Clause: Minimum 4 x PCIe 16x 4.0 slots for I/O Connectivity or higher" as required	
Test Description	**Set Steps**	**Acceptance Criteria**
	In same server ; Execute these commands : sudo dmidecode -t slot | grep PCIe	

		 suadmin@5glabcore01:~$ sudo dmidecode -t slot [sudo] password for suadmin: # dmidecode 3.3 Getting SMBIOS data from sysfs. SMBIOS 3.3.0 present. Handle 0x0900, DMI type 9, 24 bytes System Slot Information Designation: PCIe Slot 2 Type: x16 PCI Express 4 Current Usage: Available Length: Long ID: 2 Characteristics: 3.3 V is provided PME signal is supported Data Bus Width: 0 Peer Devices: 0 Height: Not applicable Handle 0x0901, DMI type 9, 24 bytes System Slot Information Designation: PCIe Slot 3 Type: x16 PCI Express 4 Current Usage: Available Length: Long ID: 3 Characteristics: 3.3 V is provided PME signal is supported Data Bus Width: 0 Peer Devices: 0 Height: Not applicable Handle 0x0902, DMI type 9, 24 bytes System Slot Information Designation: PCIe Slot 6 Type: x16 PCI Express 4 Current Usage: In Use Length: Long ID: 6 Characteristics: 3.3 V is provided PME signal is supported Bus Address: 0000:98:00.0 Data Bus Width: 0 Peer Devices: 0 Height: Not applicable Handle 0x0903, DMI type 9, 24 bytes System Slot Information Designation: PCIe Slot 4 Type: x8 PCI Express 4 Current Usage: Available Length: Long ID: 4 Characteristics: 3.3 V is provided PME signal is supported Data Bus Width: 0 Peer Devices: 0 Height: Not applicable Handle 0x0904, DMI type 9, 24 bytes System Slot Information Designation: PCIe Slot 5 Type: x8 PCI Express 4 Current Usage: Available Length: Long ID: 5 Characteristics: 3.3 V is provided PME signal is supported Data Bus Width: 0 Peer Devices: 0 Height: Not applicable Handle 0x0905, DMI type 9, 24 bytes System Slot Information Designation: PCIe Slot 7 Type: x16 PCI Express 4 Current Usage: Available Length: Long ID: 7 Characteristics: 3.3 V is provided PME signal is supported Data Bus Width: 0 Peer Devices: 0 Height: Not applicable

		
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

4.11 5G SIM

Test ID	4.11.a		
Requirement	Network Supported : 5G SA		
Test Objective	SIM should be attached in private 5G Network		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Follow procedure 2.1 and 2.2 Attach a UE(mobile) in private 5G Network	Navigate to Settings-> Mobile Networks -> sim1/2-> operator field to see the mobile attached to the private network	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.11.b	
Requirement	File Structure : 3GPP Compliant	
Test Objective	SIM File structure should be 3gpp compliant	
Test Description	**Set Steps**	**Acceptance Criteria**

	SIM file structure via sim reader		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.11.c	
Requirement	Data Security : Secure channel	
Test Objective	Data Security features such as Integrity and encryption algorithms should be implemented	
Test Description	**Set Steps**	**Acceptance Criteria**
	Follow procedure 2.1 and 2.2 and attach a ue (mobile) to the netwotk	The security mode command message indicates the data security features used for that mobile Reference Procedure 4.21

Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.11.d		
Requirement	Authentication : 3GPP Compliant		
Test Objective	Sim should support 5G_AKA algorithm		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Follow the procedure 1.1 and 1.2 Attach a ue to the network	The RAND and AUTN parameters sent from amf to ue (mobile) in the authentication request message indicates the 5G_AKA algorithm used in authentication Reference Procedure 4.22	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.11.e
Requirement	Should be Vibration, shock, impact and chemical resistance

Test Objective	SIM card holder should have all type of sizes e.g nano,micro		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Visual inspection		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.11.f	
Requirement	Material : PVC	
Test Objective	Material type should be PVC	
Test Description	**Set Steps**	**Acceptance Criteria**
	Visual Inpection	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.11.g	
Requirement	Card Characteristics : as per ISO/IEC 7810	
Test Objective	Card characteristics	
Test Description	**Set Steps**	**Acceptance Criteria**
	physically inspect the dimensions of the sim card	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.11.h	
Requirement	Any future upgrade should be supported through SIM upgrade or replacement or through OTA	
Test Objective	Any future upgrade should be supported through SIM upgrade or replacement or through OTA	
Test Description	**Set Steps**	**Acceptance Criteria**
	Can not be demonstrated	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

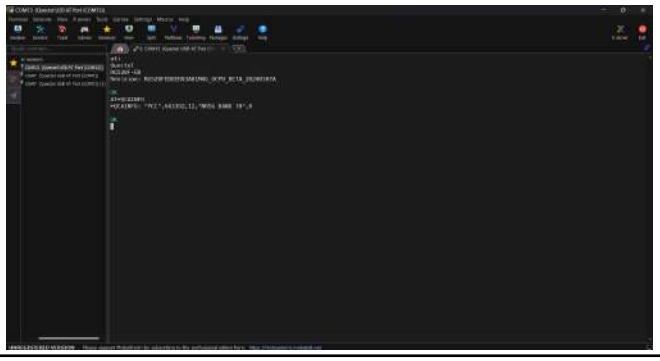
Test ID	4.11.i	
Requirement	SIM card programmer/writer or support to provision SIMs in agreed response time throughout the project period	
Test Objective		
Test Description	**Set Steps**	**Acceptance Criteria**
	Support provided for for sim card changes as per the tender	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

Test ID	4.11.j	
Requirement	SIM cards to support all sizes	
Test Objective	Supported sim size	
Test Description	**Set Steps**	**Acceptance Criteria**
	visual inspection Supports 2ff(),3ff(),4ff()	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

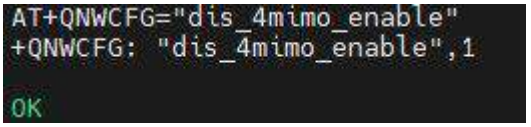
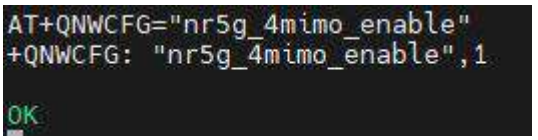
4.12 5G EVALUATION BOARD

Test ID	4.12.a	
Requirement	5G Qualcomm Snapdragon™ X62/X65 or higher 5G Modem-RF system Supported	
Test Objective	5G Qualcomm Snapdragon™ X62/X65 or higher 5G Modem-RF system Supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	1.Power up the board and connect it with a pc using type c cable . 2.Use any standard at command tester for see details of modem using (**ATI**) command. .	 OUTPUT WITH COMMAND ATI Quectel RG520F-EB Revision: RG520FEBDER03A01M4G_ OCPU_BETA_20240307A OK
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

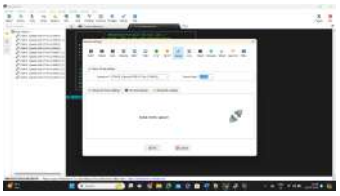
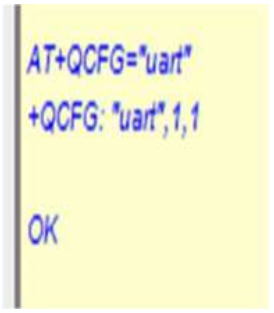
Test ID	4.12.b
Requirement	**Cellular Modem-RF Specs:** 5x20 MHz carrier aggregation (DL) and above, 100/200 MHz bandwidth (sub-6 GHz),

	Optional: 8 carriers (mmWave), 3x20 MHz carrier aggregation (UL), 800 MHz bandwidth (mmWave).	
Test Objective	**Cellular Modem-RF Specs:** 5x20 MHz carrier aggregation (DL) and above, 100/200 MHz bandwidth (sub-6 GHz), Optional: 8 carriers (mmWave), 3x20 MHz carrier aggregation (UL), 800 MHz bandwidth (mmWave).	
Test Description	**Set Steps**	**Acceptance Criteria**
	1. Carrier aggregation and bandwidth verified from the data sheet. 2. Cellular Modem-RF RG520F. 3. Use AT Command :- **AT+QCAINFO**	 
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

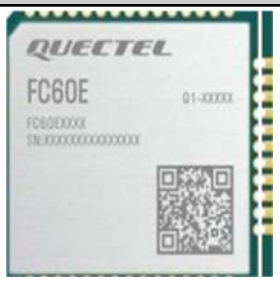
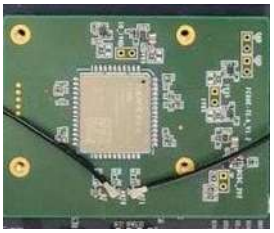
Test ID	4.12.c
Requirement	**Performance Enhancement Technologies:** 100 MHz envelope tracking, Adaptive antenna tuning, Uplink Data Compression (UDC), 5G envelope tracking.

Test Objective	To verify 100 MHz envelope tracking	
Test Description	**Set Steps**	**Acceptance Criteria**
	AT Commands :- **AT+QNWCFG="dis_4mimo_enable"** +QNWCFG: "dis_4mimo_enable",1 OK **AT+QNWCFG="nr5g_4mimo_enable"** +QNWCFG: "nr5g_4mimo_enable",1 OK	 
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

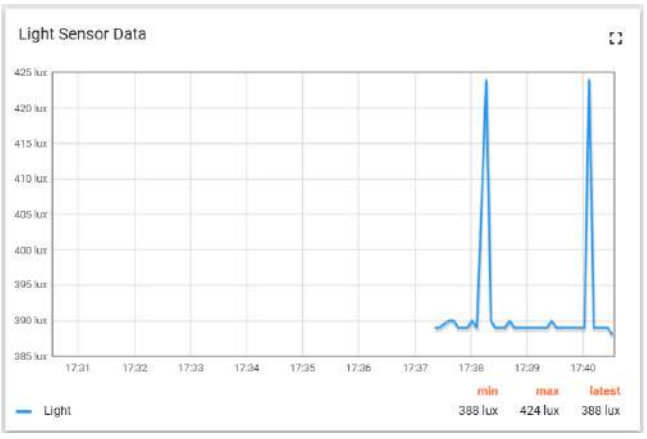
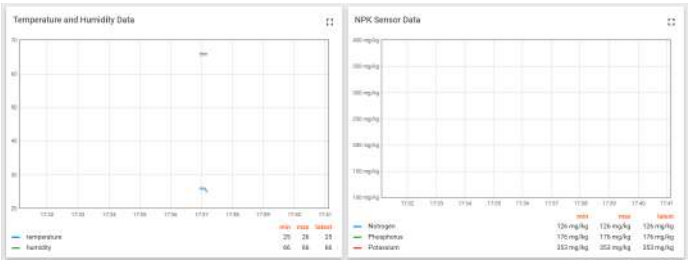
Test ID	4.12.e

Requirement	Peripheral connectors on the platform support UART, SPI, I2C and GPIO	
Test Objective	Peripheral connectors on the platform support UART, SPI, I2C and GPIO	
Test Description	**Set Steps**	**Acceptance Criteria**
	1. GPIO 2. I2C 3. SPI 4. UART Open the 5G eval up plates Functional verification 1.Baud rate 115200 is used and transmit and receive large amount of data.  2.Configure CPOL and CPHA settings, communicate with SPI devices. 3. Set 2 master on the bus & perform read write operation 4.Configured 1 GPIO as input & 1 GPIO as output results verified at ground 5. power up the board and connect with your pc using type c data cable. 6. Check the interfaces by below AT commands : AT+CREG AT+CREG? AT+QCFG=”uart” Check Supported Configurations: **AT+QCFG=?** List supported configurations and options	    

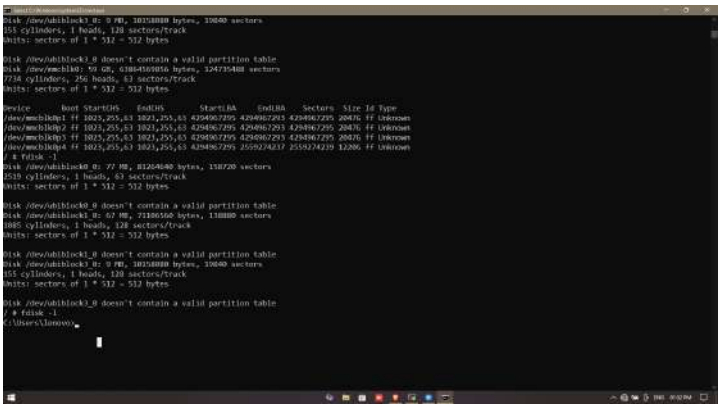
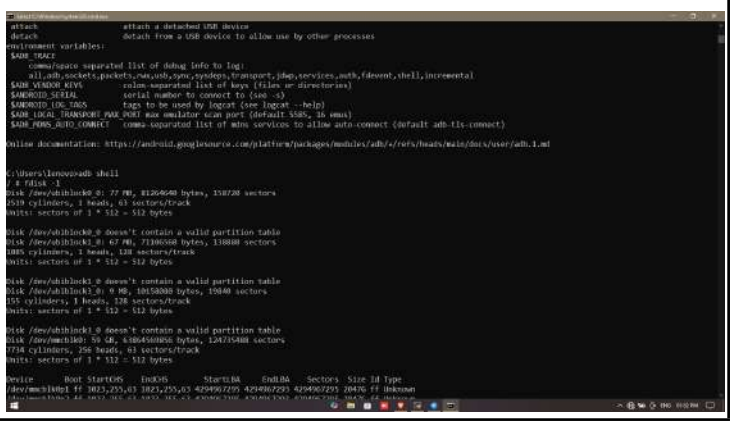
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

Test ID	4.12.d	
Requirement	Physical and Wi-Fi Interface Modules	
Test Objective	Physical and Wi-Fi Interface Module	
Test Description	**Set Steps**	**Acceptance Criteria**
	1. Insert the sim and power up the board . 2. Search the WiFi from your PC/UE to connect with the ssid of 5G Evb. 3. Connect it to verify	  

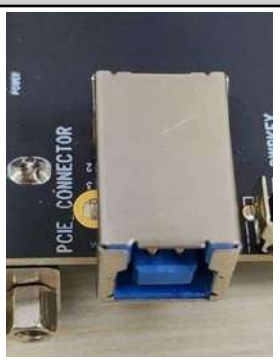
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)	QSoftAP is the network ssid of 5G Eval Board.	
Name	Name of Verifier	Signature

Test ID	4.12.f	
Requirement	Sensor interfaces for medical devices, smart-home appliances and smart-city applications	
Test Objective	Sensor interfaces for medical devices, smart-home appliances and smart-city applications	
Test Description	**Set Steps**	**Acceptance Criteria**
	The sensor can connect with the Wi-Fi or Cellular of Evb and it can monitor & manage with help of 5G Evb. 1. Power up the board 2. Connect coral gyan with a hotspot of 5G Evb. 3. You can send the data to your desired API or Connect raspberry pi with the wifi of 5G Eval and send sensor data through it	 
Overall Test Result	Pass:☐	Fail:☐

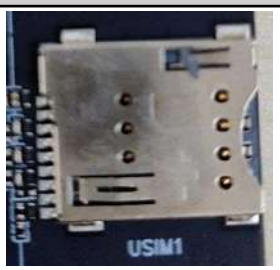
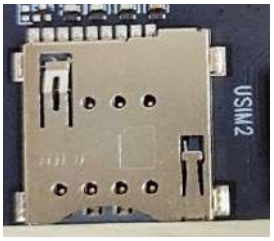
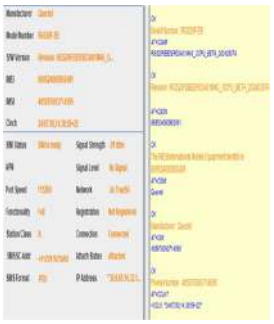
Comments	Variable data for sensors can be seen with changing environment conditions	
Name	Name of Verifier	Signature

Test ID	4.12.g	
Requirement	SD Card Connector	
Test Objective	SD Card Connector	
Test Description	**Set Steps**	**Acceptance Criteria**
	The SD card can see on the right side of 5G Evb. 1. Install ADB in your system 2. After that connect your PC with the 5G Evaluation Board (Coral Anubhav) 3. Access command prompt and launch adb and enter the command to show all devices(adb devices). 4.After that in command prompt type adb shell. You will access 5G EvB board 5. And then enter **fdisk -l** on command prompt to see the SD Card details.	  

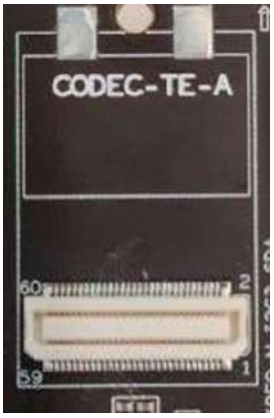
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)	Using **fdisk -l** command in ADB to see storage.	
Name	Name of Verifier	Signature

Test ID	4.12.h	
Requirement	PCI to USB Connector	
Test Objective	PCI to USB Connector	
Test Description	**Set Steps**	**Acceptance Criteria**
	The PCIE to the USB connector is on the front side of the 5G Evb.	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

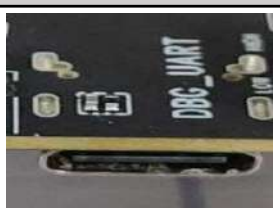
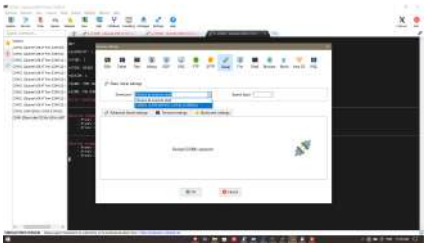
Test ID	4.12.i
Requirement	Dual (U)SIM card supported: 1.8 V and 2.95 V

Test Objective	Dual (U)SIM card supported: 1.8 V and 2.95 V	
Test Description	**Set Steps**	**Acceptance Criteria**
	The sim card slot are on the left side USIM card 1 USIM card 2 Check the sim status using standard AT command tester Application on "**sim status**". FUNCTIONAL VERIFICATION 1.Power up the board and connect the type c data cable between your pc and EV board. 2 use the AT command tester to see the details of sim like SIM/IMSI no. AT Commands:- **AT+QUIMSLOT?** +QUIMSLOT: 1 OK **AT+CIMI** 001010000000130 OK **AT+QUIMSLOT=2** OK **AT+QUIMSLOT?** +QUIMSLOT: 2 OK **AT+CIMI** 001010000000101 OK	  
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		

Name	Name of Verifier	Signature

Test ID	4.12.j	
Requirement	1 digital audio codec board interface	
Test Objective	1 digital audio codec board interface	
Test Description	**Set Steps**	**Acceptance Criteria**
	Open the top plate of 5G Evb and see the left side of the board. **Functional Verification** 1. Insert the sim and power up the board . 2 Using AT command tester call to a number like this "**ATD1234567890;**" Now you can talk above numbers by using Audio earphones.	 
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

Test ID	4.12.k

Requirement	COM1 and COM2. Also support Main UART, Debug UART	
Test Objective	COM1 and COM2. Also support Main UART, Debug UART	
Test Description	**Set Steps**	**Acceptance Criteria**
	Both debug ports are on the front side of the 5G Eval Board 1. Power up the board and connect the type c data cable between your pc and EV board. 2. connect the cable. 3. Boot up the system 4. COM1 and COM2 should be detected and listed in the system	   
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)	Debug and Main UART are visible in the above attached snaps	
Name	Name of Verifier	Signature

Test ID	4.12.I

Requirement	USB Type C Interface, USB 3.0 & USD 2.0 supported	
Test Objective	USB Type C Interface, USB 3.0 & USD 2.0 supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	1.The USB type **C** interface is on the right side of 5G Evb 2. Connect the type **C** Data cable to use the 5G Evb with your PC.	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

Test ID	4.12.m	
Requirement	LEDs indication	
Test Objective	LEDs indication	
Test Description	**Set Steps**	**Acceptance Criteria**

	1. LEDs are top on the board 2. open Top plate of 5G Evb box the LEDs are below the Wi-Fi card . 3. when the board is powered up the power LED(Red light) on. And other LEDs are on when the corresponding work is done. SWITCH ON Board check for below listed LEDs details a) red led for power up indication b) yellow for debug mode c) blue light for registration status 2nd blue led show connectivity	 
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

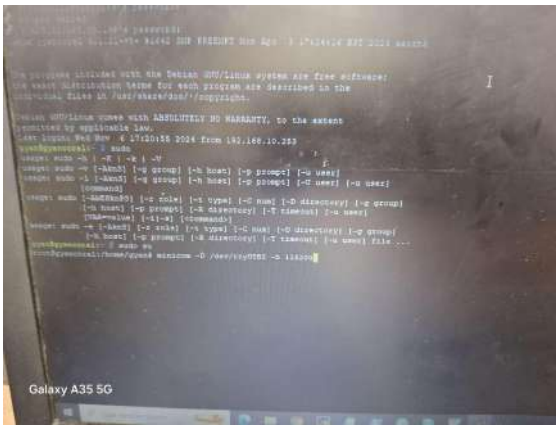
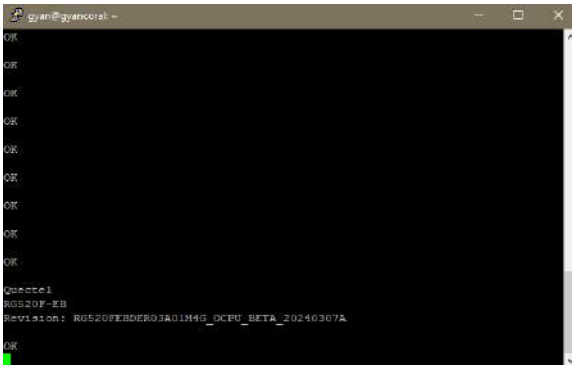
Test ID	4.12.n	
Requirement	Power key, Reset key, USB Boot, Power Switch, etc	
Test Objective	Power key, Reset key, USB Boot, Power Switch	
Test Description	**Set Steps**	**Acceptance Criteria**

	1.All the keys are on the board 2.To confirm open the top plate of 5G Evb 3.The functionality of each can be checked by using them KEYS:- POWER, RESET, USB BOOT AND POWER SWITCH	   
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

Test ID	4.12.o	
Requirement	12 Antenna Interfaces	
Test Objective	12 Antenna Interfaces(8 cellular, 2 wifi, 2 gps)	
Test Description	**Set Steps**	**Acceptance Criteria**
	Open the top plate of 5G Evb and check for antennas are mounted on the board with written frequency on it 1.ANT0, ANT1 700 MHz–6 GHz	

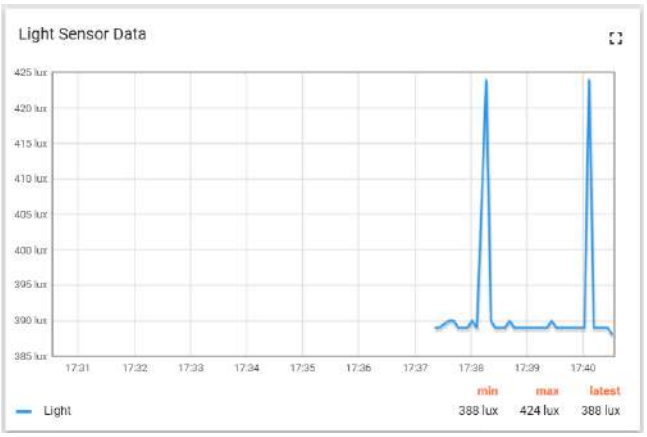
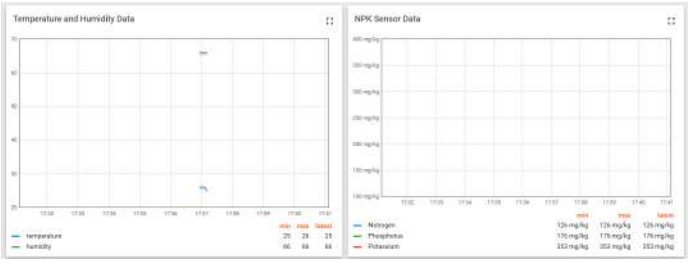
	2.ANT2 ANT7 1.7 GHz–6 GHz	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.12.p	
Requirement	Should include minimum Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors	
Test Objective	Verification of cables	
Test Description	**Set Steps**	**Acceptance Criteria**
	Visual Inspection of below listed cables 1.Cables 2.Antenna 3.Power adaptors 4.Wi-Fi Ethernet 5.PCI TO USB Audio earphone	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.12.q	
Requirement	AT command (external MCU integration) and SDK support (within the module)	
Test Objective	AT command (external MCU integration) and SDK support (within the module)	
Test Description	**Set Steps**	**Acceptance Criteria**
	1. Turn on your 5G Evb Board using the power adapter and make sure your Raspberry Pi(MCU) is on the same network. 2. Connect your Raspberry Pi with 5G Evb Board via USB 3. Take access of RaspberryPi using Putty and then switch to superuser using the command : sudo su 4. After switching to super user run the minicom command to take access which is : minicom -D /dev/ttyUSB2 -b 115200 5. Now you will be able to operate your 5G Evb Board using the Raspberry Pi	MCU Integration:  

	6. Now you will be able to operate a 5G Evb Board using Raspberry Pi. All the supported AT Commands will be functional.	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.12.r	
Requirement	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc. 32bit 400MHz Dual Core or higher Interface. I2C, SPI, UART, GPIO, ADC, Timer, EEPROM, Flash/NVS, etc RTOS Support for Real-Time Application MCU Development Board Should able to integrate with the 5G Development Board via Wi-Fi / Ethernet / USB	
Test Objective	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc. 32bit 400MHz Dual Core or higher Interface. I2C, SPI, UART, GPIO, ADC, Timer, EEPROM, Flash/NVS, etc RTOS Support for Real-Time Application MCU Development Board Should able to integrate with the 5G Development Board via Wi-Fi / Ethernet / USB	
Test Description	**Set Steps**	**Acceptance Criteria**

	1.You can configure a mcu for smart city or medical devices . 2. Connect raspberry pi with the wifi of 5G eval and send sensor data through it	 
Overall Test Result	Pass:☐	Fail:☐
Comments	Variable data for sensors can be seen with changing environment conditions	
Name	Name of Verifier	Signature

4.13 IOT Gateway

Test ID	4.13.1.a	
Requirement	CPU : Qualcomm or equivalent, Dual core or Higher	
Test Objective	CPU : Qualcomm or equivalent, Dual core or Higher	
Test Description	**Set Steps**	**Acceptance Criteria**

	Steps : 1.Power On the RUTX 50 2.Connect the RUTX 50 to the MEC Server via lan 3. Access the RUTX web configuration page by inputting the ip address : 192.168.1.1 in a web browser. The login credentials for RUTX are Username : admin Password : Admin@123 System>maintenance>CLI *CLI Command : cat /proc/cpuinfo*	processor : 0 model name : ARMv7 Processor rev 5 (v7l) BogoMIPS : 96.00 Features : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm CPU implementer : 0x41 CPU architecture: 7 CPU variant : 0x0 CPU part : 0xc07 CPU revision : 5 processor : 1 model name : ARMv7 Processor rev 5 (v7l) BogoMIPS : 96.00 Features : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm CPU implementer : 0x41 CPU architecture: 7 CPU variant : 0x0 CPU part : 0xc07 CPU revision : 5 processor : 2 model name : ARMv7 Processor rev 5 (v7l) BogoMIPS : 96.00 Features : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm CPU implementer : 0x41 CPU architecture: 7 CPU variant : 0x0 CPU part : 0xc07 CPU revision : 5 processor : 3 model name : ARMv7 Processor rev 5 (v7l) BogoMIPS : 96.00 Features : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm CPU implementer : 0x41 CPU architecture: 7 CPU variant : 0x0 CPU part : 0xc07 CPU revision : 5
Overall Test Result	Pass:☐	Fail:☐

Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.1.b	
Requirement	RAM: 256 MB	
Test Objective	RAM: 256 MB	
Test Description	**Set Steps**	**Acceptance Criteria**
	CLI Command : free -h	root@RUIX50:~# free -h total used free shared buff/cache available Mem: 248616 66704 136220 232 45692 134376 Swap: 0 0 0
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

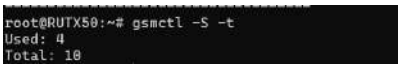
Test ID	4.13.1.c
Requirement	Module: 5G Sub-6Ghz SA 1/2 Gbps DL (4x4 MIMO) or higher , 900/600 Mbps UL (2x2)

Test Objective	Module: 5G Sub-6Ghz SA 1/2 Gbps DL (4x4 MIMO) or higher , 900/600 Mbps UL (2x2)		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from Datasheet		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.1.d	
Requirement	Status: Signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP Bytes sent/received, connected band, IMSI, ICCID.	
Test Objective	Status: Signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP Bytes sent/received, connected band, IMSI, ICCID.	
Test Description	**Set Steps**	**Acceptance Criteria**

	Steps : Gsmctl AT commands- *RSSI, RSRP, SINR, RSRQ- gsmctl -q, --signal* *EC/IO- gsmctl -E, --ecio* *RSCP- gsmctl -X, --rscp* *IMSI- gsmctl -x, --imsi* *ICCID- gsmctl -J, --iccid* Mobile details can be seen in : RUTX50 WebUI > RUTX50 Status section > RUTX50 Network> Mobile	Go to System->CLI username:- root password:- Admin@123 then follow the commands written in Set steps one by one (then we can get following screenshot) : RSSI: -61 RSRP: -91 SINR: 15 RSRQ: -12 Steps : Go to Status ->Network -> Mobile Then we can see the below screenshot 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.1.e
Requirement	SMS/Call status

Test Objective	SMS/Call status	
Test Description	**Set Steps**	**Acceptance Criteria**
	Steps : gsmctl -S -r, --sms --read gsmctl -S -l, --sms --list <TYPE> gsmctl -S -t, --sms --total gsmctl -S -d, --sms --delete <INDEX>	Go to System->CLI Use the same commands to capture the following screenshots    root@RUTX50:~# gsmctl -S -t Used: 4 Total: 10 
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.13.1.f		
Requirement	Supports sending and reading Unstructured Supplementary Service Data messages		
Test Objective	Supports sending and reading Unstructured Supplementary Service Data messages		
Test Description	**Set Steps**	**Acceptance Criteria**	
	gsmctl -S -s, --sms --send "<NUMBER> <TEXT>" gsmctl -S -r, --sms --read	do ssh root@192.168.1.1 [password : Admin@123] and Use the same commands to capture the following screenshots 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

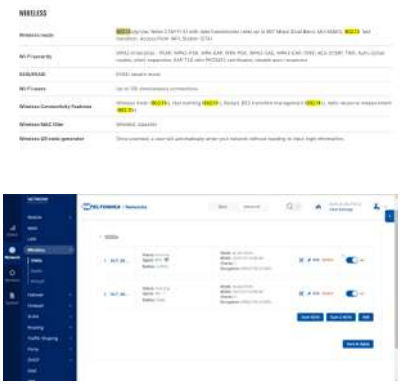
Test ID	4.13.1.g
Requirement	APN

Test Objective	APN		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Access the RUTX web configuration page by inputting the ip address : 192.168.1.1 in a web browser. Go to :- System>Setup Wizard> Mobile> Custom APN	See APN document  	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.1.h	
Requirement	Possibility to use different PDNs for multiple network access and services	
Test Objective	Possibility to use different PDNs for multiple network access and services	
Test Description	**Set Steps**	**Acceptance Criteria**

		# Interface mob1s2a1_4 nameserver xx.xx.x.x # Interface mob1s2a1_6 nameserver xxxx:xxx:xxx::x	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Access Points

Test ID	4.13.2.a	
Requirement	Supports 802.11b/g/n/ac	
Test Objective	Supports 802.11b/g/n/ac	
Test Description	**Set Steps**	**Acceptance Criteria**
	Network> Wireless 2.4 GHz 802.11bgn 5 GHz 802.11ac	

			
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.2.b	
Requirement	WiFi Security : WPA X /WEP/ TKIP variants as per the latest version.	
Test Objective	WiFi Security : WPA X /WEP/ TKIP variants as per the latest version.	
Test Description	**Set Steps**	**Acceptance Criteria**
	Network>Wireless>edit >Wireless Security	 
Overall Test Result	Pass:☐	Fail:☐

Comments			
Name	Name of Verifier	Signature	

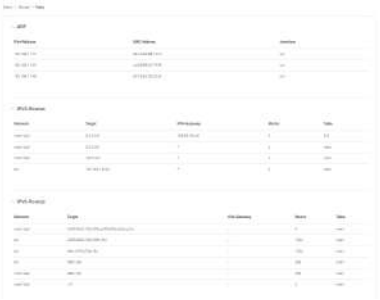
Test ID	4.13.2.c	
Requirement	Support minimum 30 simultaneous WiFi users connections	
Test Objective	Support minimum 30 simultaneous WiFi users connections	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verify in Datasheet	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Networks

Test ID	4.13.3.a

Requirement	Supports all required network protocols	
Test Objective	Supports all required network protocols	
Test Description	**Set Steps**	**Acceptance Criteria**
	Attach a UE to the network and collect the logs	The Protocol messages for NGAP , NAS , RRC , MAC , RLC , PDCP ,gtp are present in the traced log file
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.13.3.b	
Requirement	Supports Static and dynamic routing	
Test Objective	Supports Static and dynamic routing	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Status -> Routes -> General/Dynamic routing	

			
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

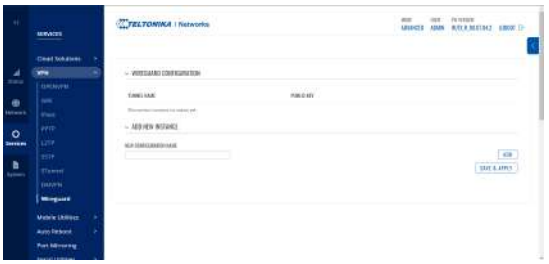
Test ID	4.13.3.c	
Requirement	Supports static and dynamic IP allocation	
Test Objective	Supports static and dynamic IP allocation	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Network->Interfaces->General->dhcp, static lease->static ip allocation	
Overall Test Result	Pass:☐	Fail:☐

Comments (if any)			
Name	Name of Verifier	Signature	

VLAN

Test ID	4.13.4.a	
Requirement	Multiple clients and a server can run simultaneously	
Test Objective	Multiple clients and a server can run simultaneously	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Services->VPN->OPENVPN->Add new instance and define role as server or client as per requirement.	 
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

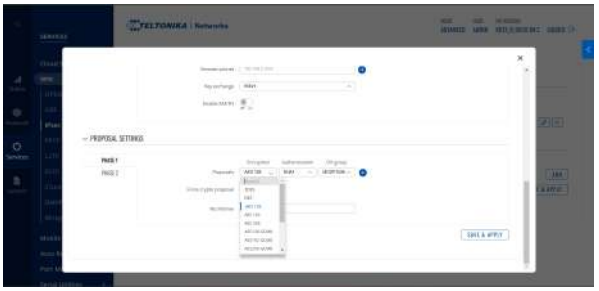
Test ID	4.13.4.b

Requirement	WireGuard VPN client and server support		
Test Objective	WireGuard VPN client and server support		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to : Services> VPN> Wireguard>Configuration	 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.4.c
Requirement	Port and tag-based VLAN separation
Test Objective	Port and tag-based VLAN separation

Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Network>VLAN> Port and interface based tag	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

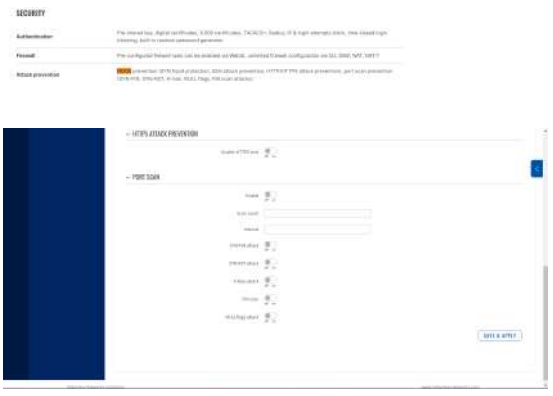
Test ID	4.13.4.d	
Requirement	Supports up to 5 x VPN IPsec tunnels with different AES/DES encryption methods.	
Test Objective	Supports up to 5 x VPN IPsec tunnels with different AES/DES encryption methods	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Services> VPN> IPSEC > Configuration --aes/des	

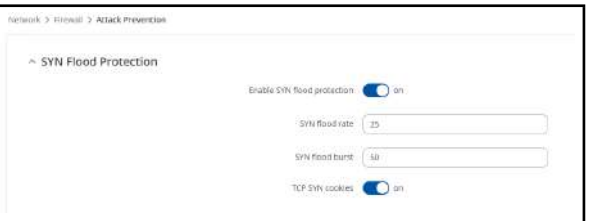
			
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Security

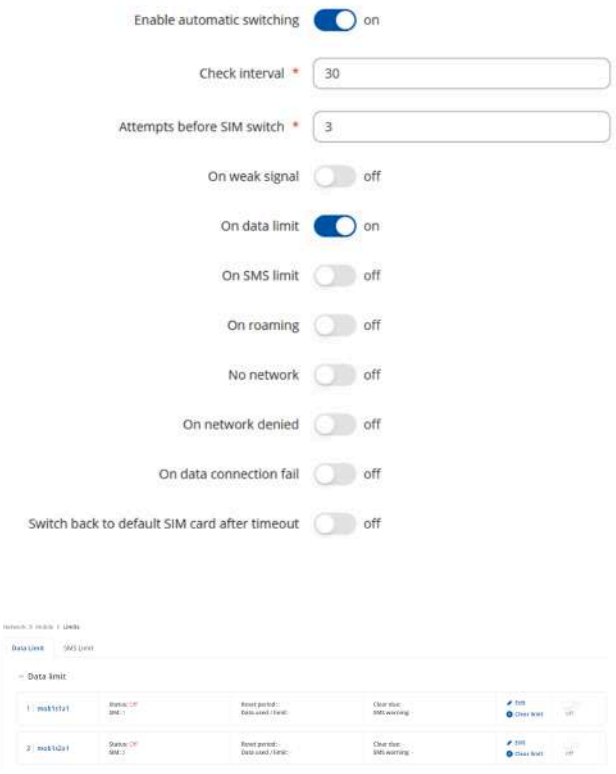
Test ID	4.13.5.a	
Requirement	Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI; NAT; NAT-T	
Test Objective	Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI; NAT; NAT-T	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Network> Firewall For CLI go to : System->Maintenance->CLI CLI Command : vi /etc/config/firewall	config rule '32' list dest_port '4500' list dest_port '4500' option src 'wan' option name 'Allow-IPsec-NAT-T' option target 'ACCEPT' option vpn_type 'IPsec' option proto 'udp'

		config redirect '35' option proto 'any' option name 'Exclude-IPsec-from-NAT' option extra '-m policy --dir out --pol ipsec' option vpn_type 'IPsec' option target 'ACCEPT' option dest 'wan'
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature	

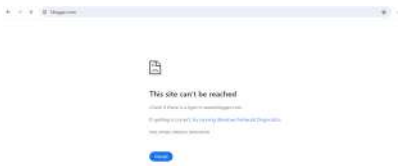
Test ID	4.13.5.b	
Requirement	DDOS prevention (port scan prevention)	
Test Objective	DDOS prevention (port scan prevention)	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Network>Firewall>Attack Prevention>Port Scan SYN Flood Protection can be set ON	

			
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

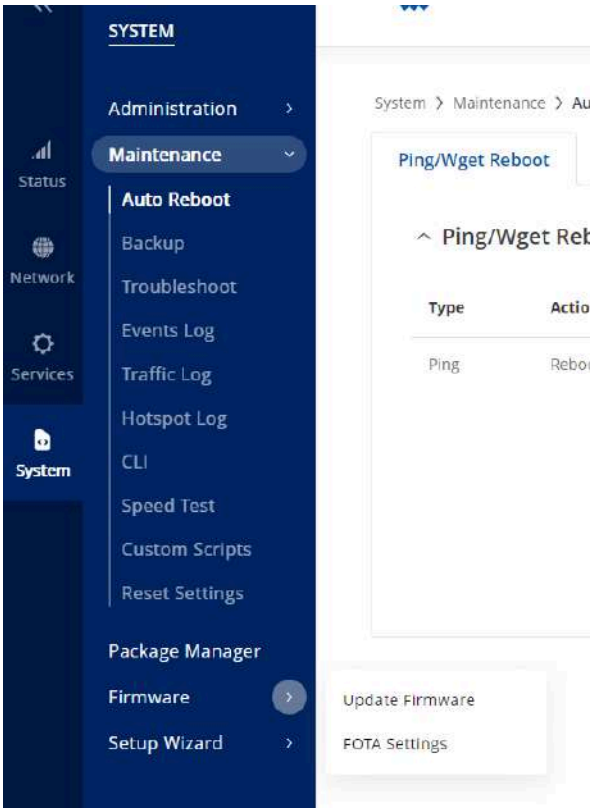
Test ID	4.13.5.c	
Requirement	Sets up custom data limits for SIM card	
Test Objective	Sets up custom data limits for SIM card	
Test Description	**Set Steps**	**Acceptance Criteria**

	Go to :- Network >Mobile >SIM Switch>Data Limit		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

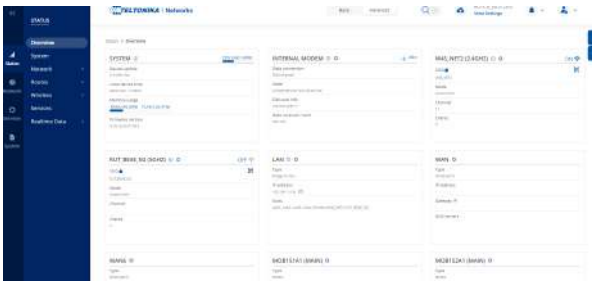
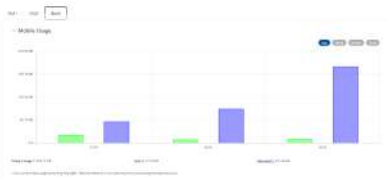
Test ID	4.13.5.d
Requirement	Blacklist for blocking out unwanted websites, Whitelist for specifying allowed sites only
Test Objective	Blacklist for blocking out unwanted websites, Whitelist for specifying allowed sites only

Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to :- Services->Web filter->Site Blocking	 Enable and click on apply and save like shown in fig  Before Blacklisting  After blacklist  	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Management

Test ID	4.13.6.a	
Requirement	Status, configuration, FW update, CLI, troubleshoot, event log, system log.	
Test Objective	Allows monitoring of: Device data, Mobile data, Network info, Availability	
Test Description	**Set Steps**	**Acceptance Criteria**
	Available on System Page.	 Monitoring (on document): 

		Realtime Connection status: Status->Realtime data->Connection  =>The graph shows the number of active connections over time, with the y-axis representing the number of connections and the x-axis representing time. Connections across three different protocols: UDP(58 connections), TCP(4 active connections) shaded area in blue indicates the total number of connections across all protocols. Realtime LAN traffic:  Realtime ipv4 and ipv6 traffic status: 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

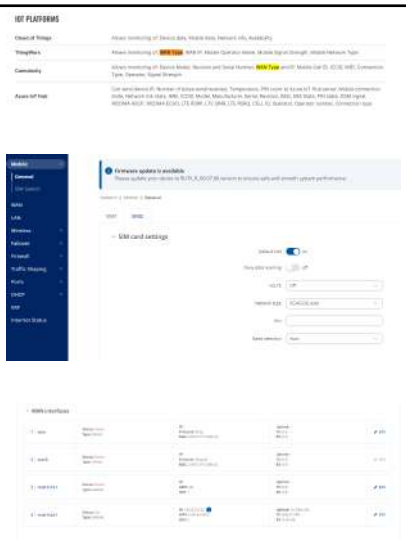
Test ID	4.13.6.b	
Requirement	Allows monitoring of: Device data, Mobile data, Network info, Availability	
Test Objective	Allows monitoring of: Device data, Mobile data, Network info, Availability	
Test Description	**Set Steps**	**Acceptance Criteria**
	Can be Seen at Web GUI on Overview	   
Overall Test Result	Can be seen	Fail:☐

Comments			
Name	Name of Verifier	Signature	

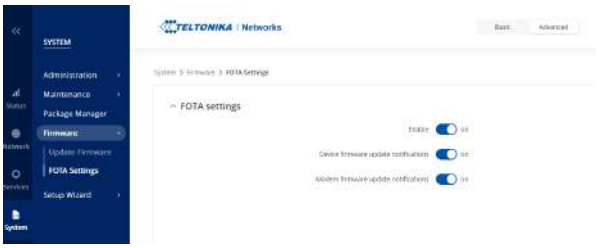
Test ID	4.13.6.c	
Requirement	Allows monitoring of: Device Model, Revision and Serial Number, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP	
Test Objective	Allows monitoring of: Device Model, Revision and Serial Number, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP	
Test Description	**Set Steps**	**Acceptance Criteria**
	Can be verified on GUI pages: Status > System and Status > Network > Mobile	  

			
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.6.d	
Requirement	Allows monitoring of: WAN Type, WAN IP, Mobile Operator Name, Mobile Signal Strength, Mobile Network Type.	
Test Objective	Allows monitoring of: WAN Type, WAN IP, Mobile Operator Name, Mobile Signal Strength, Mobile Network Type.	
Test Description	**Set Steps**	**Acceptance Criteria**
	Status > Network > Mobile Status >Network >Topology	

	Please see below link https://wiki.teltonika-networks.com/view/RUTX50_Network_section		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.6.e	
Requirement	Firmware update from server, automatic notification	
Test Objective	Firmware update from server, automatic notification	
Test Description	**Set Steps**	**Acceptance Criteria**

	Please see below link https://wiki.teltonika-networks.com/view/RUTX50_Firmware#Update_Firmware		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.6.f	
Requirement	Management API over HTTP/HTTPS	
Test Objective		
Test Description	**Set Steps**	**Acceptance Criteria**
	The Management webpage is available at http://192.168.1.1	Verify the management meny via accessing the mentioned url
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Others

Test ID	4.13.7.a	
Requirement	Supports 1 or more SIMs	
Test Objective	Supports 1 or more SIMs	
Test Description	**Set Steps**	**Acceptance Criteria**
	2 SIM card can be inserted, and any one can be active at a time	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.13.7.b	
Requirement	Supports location tracking	
Test Objective	Supports location tracking	
Test Description	**Set Steps**	**Acceptance Criteria**

	Please see below link https://wiki.teltonika-networks.com/view/RUTX50_GPS		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

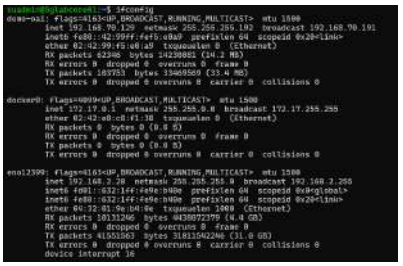
Test ID	4.13.7.c	
Requirement	Supports USB.	
Test Objective	Supports USB	
Test Description	**Set Steps**	**Acceptance Criteria**
	Please see below link https://wiki.teltonika-networks.com/view/RUTX50_USB_Tools	
Overall Test Result	Pass:☐	Fail:☐
Comments		

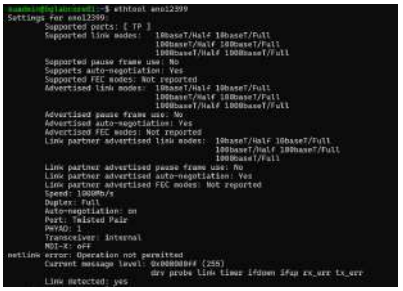
Name	Name of Verifier	Signature	

Test ID	4.13.7.d	
Requirement	Supports digital input/output	
Test Objective	Supports digital input/output	
Test Description	**Set Steps**	**Acceptance Criteria**
	Input -1 x Digital Input, 0 - 6 V detected as logic low, 8 - 30 V detected as logic high Output - 1 x Digital Output, Open collector output, max output 30 V, 300 mA	
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.13.7.e	
Requirement	Supports minimum 4 nos 10/100/1000 Ethernet ports.	
Test Objective	Supports minimum 4 nos 10/100/1000 Ethernet ports	
Test Description	**Set Steps**	**Acceptance Criteria**

	WAN - 1 x WAN port 10/100/1000 Mbps LAN - 4 x LAN ports, 10/100/1000 Mbps		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.7.f	
Requirement	Supports 1G WAN port.	
Test Objective	Supports 1G WAN port	
Test Description	**Set Steps**	**Acceptance Criteria**
	WAN - 1 x WAN port 10/100/1000 Mbps	Firstly we have to see the network interface for core ip address 192.168.xx.20 by command ifconfig  now to check speed and duplex we use command ethtool eno12399

		 we can see here that the interface is operating at 1G (1000 Mbps) which confirms that the interface supports the 1G WAN port requirement . The duplex mode is”FULL”, which is expected for a Gigabit Ethernet interface . The interface supports various link modes including 1000baseT/Full, which is essential for 1G operation.
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.13.7.g	
Requirement	Supports status LED	
Test Objective	Status LED should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**

	Can be verified physically on device		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.13.7.h		
Requirement	Supports PoE and DC power socket.		
Test Objective	Supports PoE and DC power socket.		
Test Description	**Set Steps**	**Acceptance Criteria**	
	PoE (passive) - possibility to power up through LAN1 port, not compatible with IEEE802.3af, 802.3at and 802.3bt standards, Mode B, 9 - 30 VDC		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

4.14 5G Mini Drones

Test ID	4.14	
Requirement	Verification of Physical Structure and Sensors of drone.	
Test Objective	To Check the Physical Structure and Sensors of drone.	
Test Description	**Set Steps**	**Acceptance Criteria**
	●Check the drone cover. ●Check the drone motors. ●Check the drone propellers. ●Check the Time of flight sensor. ●Check the VIO sensor. ●Check the image sensor. ●Check the VOA sensor. ●Check the drone battery. ●Check the tracking sensor. ●Check the Nano SIM slot.	● The drone cover should be intact. ● The drone should have 4 motors. ● The drone should have 4 propellers. ● The Time of flight sensor should be present at the back of the drone ● A VIO sensor should be present at the bottom of the drone. ● Image sensor should be in front of the drone. ● A VOA sensor should be mounted on the top of the drone. ● Battery should be present with the drone. ● The tracking sensor should be mounted on the drone arm. ● At the back of the drone there should be a Nano SIM slot. 

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.14 (a) 5G enabled and controlled drone (m) 5G Modem (n78 band)	
Requirement	To Check Drone is integrated into the System and supports 5G Modem (n78 band)	
Test Objective	To Check Drone is integrated into the System and supports 5G Modem (n78 band)	
Test Description	**Set Steps**	**Acceptance Criteria**
	Step-1: Verify the 5G network is on N78 band only. Step-2: Insert the 5G SIM into the drone and Power ON the drone by inserting the battery. Step-3: The drone will automatically send the UE-attach message to the 5G network. After successful attach and IP assignment, the drone can be connected via the GCS.	All the drone data - 1. 3D Map Data. 2. Video data. 3. Drone Telemetry data should be available on the GCS - ‘ iDronam Enterprise ’ via 5G.

	Step-3: Open the GCS - ‘iDronam Enterprise’. Connect to the drone. Step-4: Check if all the drone data are coming - ○ 3D Map data. ○ Video data. ○ Drone Telemetry data.		
Overall Test Result	Pass:☐	Fail:☐	
Comments	It is verified Drone is integrated and supporting n78 Band		
Name	Name of Verifier	Signature	

Test ID	4.14.(b) Supports 5G nano SIM	
Requirement	Supports 5G Nano Sim	
Test Objective	To verify support of 5G Nano Sim	
Test Description	**Set Steps**	**Acceptance Criteria**
	Step-1 : Take a 5G Nano SIM and Insert into the drone SIM card slot. Step-2: Connect the GCS to the 5G network. Step-3: Connect the GCS to the drone. Step-4: Check for the drone connection and information	Successful insertion of 5G Nano SIM in SIM Slot of 5G Communication Module of Drone. 

	being displayed on the GCS screen. Inspection of drone communication module.		
Overall Test Result	Pass:☐	Fail:☐	
Comments	Successful insertion of 5G Nano SIM in SIM Slot of 5G		
Name	Name of Verifier	Signature	

Test ID	4.14.(c) Connectivity Options: Cellular (5G) and WiFi	
Requirement	Connectivity Options: Cellular (5G) and WiFi	
Test Objective	To Verify Connectivity Options	
Test Description	**Set Steps**	**Acceptance Criteria**
	For 5G Connectivity : Insert the SIM in the nano sim slot and Power ON the drone. Check for the drone connection and information being displayed on the GCS screen. For WiFi :Turn ON the Drone Connect the GCS to Drone Wifi and then Open iDronam and connect to the drone.	For 5G Connectivity: Check the 5G Core for UE attach and IP assignment. For Wifi : GCS successfully connects to the drone.
Overall Test Result	Pass:☐	Fail:☐

Comments	Successful insertion of 5G Nano SIM in SIM Slot. Wi Fi is supported.		
Name	Name of Verifier	Signature	

Test ID	4.14.(d) Qualcomm or equivalent onboard processing engine for AI/ML analytics	
Requirement	Onboard processing engine for AI/ML analytics and MEC application support.	
Test Objective	To Check drone capabilities for AI/ML and MEC.	
Test Description	**Set Steps**	**Acceptance Criteria**
	Step-1: Connect to the drone. A web page is hosted inside the drone. Open the webpage by going to the drone's IP - 10.42.0.1:5000 using a browser. Step-2: The page will open and the user can upload an image to the drone. Step-3: After processing, the drone will return the results of object detection in image and JSON formats. These can be downloaded for further use. Should support MEC applications The webpage should successfully be opened. Using this drone's AI/ML capabilities can be seen. Page 144 of 153 The drone is ME UE which is offloading the drone video stream. Step-1: Connect the MEC Server to the drone.	The webpage should successfully be opened. Using this drone's AI/ML capabilities can be seen.

	Step-2: An MEC application will be running on the MEC server which will receive the incoming video stream. Step-3: After processing the output can be viewed on the web page hosted in MEC.		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.14.(e) Autonomy: Visual Inertial Odometry (VIO), path planning, PX4, GPS-denied navigation, BVLOS, follow me.	
Requirement	Verify To Check Drone Autonomy	
Test Objective	To Check Drone Autonomy	
Test Description	**Set Steps**	**Acceptance Criteria**
	1: Connect the drone to MAVLink Packet Decoder (e.g, Mission Planner) 2: Start Capturing the MAVLink Data Stream. 3: Look for the“VISION_POSITION_ESTIMATE”“LOCAL_POSITION_NED” ,“OBSTACLE_DISTANCE” data packets for Visual inertial Odometry, GPS Denied Navigation, path planning	For PX4 a Valid MAVLink stream. “VISION_POSITION_ESTIMATE”, “LOCAL_POSITION_NED”, “OBSTACLE_DISTANCE” msg should be present and changed as the drone moves.

	respectively. for BVLOS connect the GCS to drone and subscribe to “/map” for 3d map. PX4 uses MAVLink Protocol for Drone Communication.		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.14.(f) 360 obstacle avoidance: Depth estimation, obstacle detection, mapping and VOA	
Requirement	360 obstacle avoidance, Depth estimation, obstacle detection, mapping and VOA	
Test Objective	To Verify Drone Obstacle Avoidance and Mapping	
Test Description	**Set Steps**	**Acceptance Criteria**
	1: Connect the drone to any MAVLink Decoder(Mission Planner/QGC) and look for “OBSTACLE_DISTAN CE”, “RANGEFINDER” messages for obstacle and depth estimation respectively. **For Mapping and VOA:** 1: The ‘iDronam Enterprise’ Software to drone and subscribe to “/map” for 3d	360 obstacle avoidance, Depth Estimation and obstacle detection: Before arming the drone a test object can be placed within a distance of ~20cm at 45 degree intervals around the drone. The drone will detect it and give a pre-arm warning giving the details of angle and distance of the object. 

	map and Dynamic Obstacle plotter.	Mapping and VOA: Take off the drone to 1-1.2 m altitude. The mapping algorithm will map the surroundings of the drone as it takes off. A test object can be brought close to the drone from the front face and the drone will back off once a threshold of 1.5m is crossed by the object. “OBSTACLE_DISTANCE”, “RANGEFINDER” messages should be defined and changed as you increase drone height and environment change. The map should be visible and updated with every obstacle.	
Overall Test Result	Pass:☐	Fail:☐	
Comments	1.5m is crossed by the object. “OBSTACLE_DISTANCE”,“RANGEFINDER” messages as you increase drone height and environment change. The map should be visible on the GCS.		
Name	Name of Verifier	Signature	

Test ID	4.14.(g) Payload Capacity – 500g/1 Kg or above	
Requirement	Payload Capacity – 500g or above	
Test Objective	To Check Payload Capacity	
Test Description	**Set Steps**	**Acceptance Criteria**
	Step-1: Take the drone outdoors. Step-2: Attach the 500gm Payload using hooks and Turn on the Drone Step-3: Takeoff the Drone.(Read Proper Manual Before Flying)	Drone Takes off up to a height of 1.2m and hovers in its place for a duration as per requirement.

	Step-4: Land the Drone		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.14.(h) GPS or NAVIC enabled	
Requirement	To Check GPS	
Test Objective	To verify GNSS Capabilities	
Test Description	**Set Steps**	**Acceptance Criteria**
	Step-1: Connect the drone to GCS and read the sensor status for GPS/Navic at Serial4/UART8. Drone should be placed in an outdoor environment under clear skies and location should not be near buildings of height greater than 20m. Step-2: Turn on the drone and connect to GCS.	The drone should have a GPS lock which will be indicated in GCS. An accuracy of 3m is expected. It should return “3D FIX” AND “3D DGPS” or relevant status depending upon the GPS Locking.
Overall Test Result	Pass:☐	Fail:☐

Comments	GPS is for Outdoor		
Name	Name of Verifier	Signature	

Test ID	4.14.(i) Geo Fencing		
Requirement	To Check Geo Fencing		
Test Objective	To Check Geo Fencing		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Turn ON the Drone. Step-2: Connect the drone to GCS and in the plan section create a fence plan.	After Uploading the Fence. Click on the Read Fence Button to read to fence Drone stored.	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.14.(k) Tracking Sensor
Requirement	To Check Tracking Sensor
Test Objective	To Check Tracking Sensor

Test Description	**Set Steps**	**Acceptance Criteria**	
	● Drone should be placed in an outdoor environment where GPS Signals are uninterrupted. ● Once 3D Fix has come the GPS will have a good lock of Drone Position. ● The Drone can be tracked.	After GPS Fix, the drone is successfully tracked via the GCS.	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.14.(I) Image Sensor	
Requirement	To Check Image Sensor	
Test Objective	To Check Image Sensor	
Test Description	**Set Steps**	**Acceptance Criteria**
	Turn ON the drone. Connect to it using the GCS.	The Live Stream of the drone camera will be displayed in iDronam. 

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.14.(n) Ethernet / management port	
Requirement	Ethernet / management port	
Test Objective	To Check Drone Ethernet / management port	
Test Description	**Set Steps**	**Acceptance Criteria**
	Connect to the drone via wifi. A web page is hosted inside the drone. Open the webpage by going to the drone's IP - 10.42.0.1 using a browser.	The webpage should successfully be opened. Using this drone's network modes can be managed. 
Overall Test Result	Pass:☐	Fail:☐
Comments		

Name	Name of Verifier	Signature	

Test ID	4.14.(o) Wi-Fi (2.4/5 GHz)		
Requirement	Wi-Fi (2.4/5 GHz)		
Test Objective	To Check drone Wi-Fi (2.4/5 GHz)		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Turn ON the Drone and wait for the drone to initialize. Step-1: Open GCS. Step-2: Connect the GCS WiFi to Drone's WiFi. Step-3: Open iDronam and connect to the drone.	GCS and drone must be on the same wifi network and the drone should successfully connect to the drone over WiFi.	
Overall Test Result	Pass:☐	Fail:☐	
Comments	Wi Fi Supported		
Name	Name of Verifier	Signature	

4.15 XR Device AR/VR

Test ID	4.15.1.a		
Requirement	Chipset : 2.0 GHz 8-core Qualcomm		
Test Objective	Qualcomm XR2 Gen 1		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Available processor detail ● Qualcomm XR 2 + Gen 1 chip ● - ● GPU Adreno 650	Check via datasheet	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.15.1.b		
Requirement	Memory : 64GB internal storage / 4GB RAM / MicroSD slot		
Test Objective	64GB Internal Storage, RAM 4GB/MicroSD slot		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Refer to attach datasheet 1. Power On the Device 2. Go to Device Settings 3. Go to Storage		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.15.1.d	
Requirement	Port : USB type C and Audio	
Test Objective	Type C port and audio	
Test Description	**Set Steps**	**Acceptance Criteria**

	Visual inspection Type C - located on the left panel of the Device		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Connectivity / Sensors

Test ID	4.15.2.a	
Requirement	Bluetooth 5.0	
Test Objective	Bluetooth 5.0 should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**
	Refer to datasheet	
Overall Test Result	Pass:☐	Fail:☐

Comments			
Name	Name of Verifier	Signature	

Test ID	4.15.2.b	
Requirement	802.11 a/b/g/n/ac - 2.4 GHz and 5GHz	
Test Objective	Wifi Range - ~25 meters	
Test Description	**Set Steps**	**Acceptance Criteria**
	refer to the datasheet	**Connectivity** Ports : USB-C PC-VR cable Support : yes Wireless Streaming Support : yes Wi-Fi : 6
Overall Test Result	Pass:☐	Fail:☐
Comments		
Name	Name of Verifier	Signature

Test ID	4.15.2(d)	REMOVE /REVIEW

Requirement	3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass)		
Test Objective	Inside-out 6DOF Tracking 4X IR Cameras		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Visual Inspection		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Input/Output

Test ID	4.15.3.a
Requirement	Display: 24° field-of-view, 24-bit color LCD, outdoor visible, HD resolution

Test Objective	Dual 2.1 inch F-LCD Resolution 3200 x 1600 Refresh Rate 90Hz FoV 95 - 105 PPI 1058 Foveated Rendering Support		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Refer to attached datasheet		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.15.3.b	
Requirement	Microphone	
Test Objective	USB-C Earphone Microphone Support	
Test Description	**Set Steps**	**Acceptance Criteria**

	Refer to attached datasheet Visual Inspection		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.15.3.c	
Requirement	Speaker : Internal 94 dBA loudspeaker	
Test Objective	Audio in DB 93±3db at 2kHz,0.3W/5cm	
Test Description	**Set Steps**	**Acceptance Criteria**
	Visual Inspection	
Overall Test Result	Pass:☐	Fail:☐

Comments			
Name	Name of Verifier	Signature	

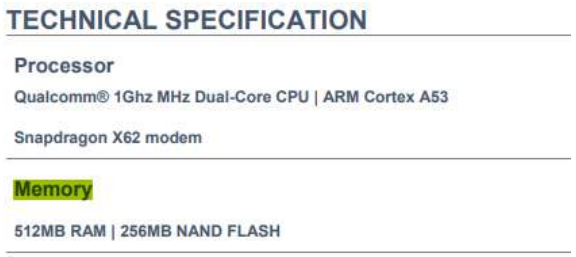
4.16 5G Indoor CPE

Test ID	4.16.1.a	
Requirement	CPU Clock Speed 1.0GHz or higher	
Test Objective	CPU Clock Speed 1.0GHz or higher	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verification via the CPE document	**TECHNICAL SPECIFICATION** **Processor** Qualcomm® 1Ghz MHz Dual-Core CPU | ARM Cortex A53 Snapdragon X62 modem **Memory** 512MB RAM | 256MB NAND FLASH

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

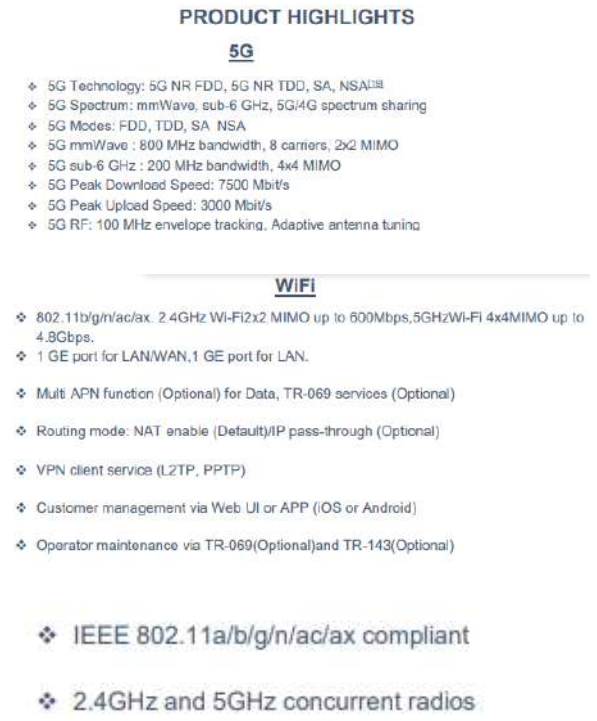
Test ID	4.16.1.b		
Requirement	CPU Cores Dual-core Cortex-A53 Arm or equivalent		
Test Objective	CPU Cores Dual-core Cortex-A53 Arm or equivalent		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verification via the CPE document		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.2
Requirement	Memory : 512 MB RAM or higher

Test Objective	Memory : 512 MB RAM or higher		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verification via the CPE document		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

5G

Test ID	4.16.3.a	
Requirement	3GPP Release 15 or above support	
Test Objective	3GPP Release 15 or above support	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verification via the CPE document	3GPP Release Compatibility:

		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.3.b	
Requirement	5G Sub 6 Band: n78 TDD	
Test Objective	n78 band should be supported	
Test Description	**Set Steps**	**Acceptance Criteria**

	Verification via the CPE document		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

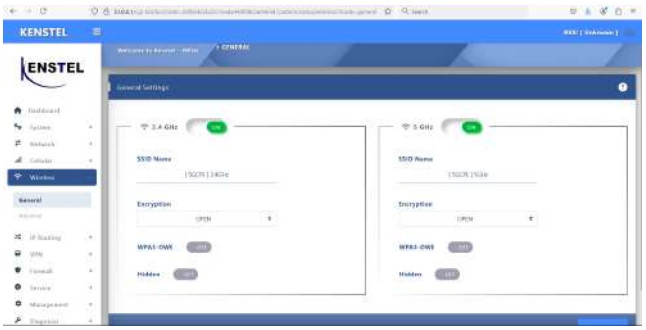
Test ID	4.16.3.c		
Requirement	5G Modem : Snapdragon X62/X65 or equivalent		
Test Objective	5G Modem : Snapdragon X62/X65 or equivalent		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verification via the CPE document		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.3.d		
Requirement	Bandwidth Support : 20/40/60/80/100 MHz		
Test Objective	Bandwidth Support : 20/40/60/80/100 MHz		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verification via the CPE document		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.3.d	
Requirement	MIMO : 4 x 4 or higher	
Test Objective	MIMO : 4 x 4 or higher	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verification via the CPE document	

			
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.3.f		
Requirement	**Download Speed:** Up to 1000 mbps		
Test Objective	**Download Speed:** Up to 1000 mbps		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verification via the CPE document		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.5.a		
Requirement	AP type: Indoor, dual radio, 2.4, 5-GHz		
Test Objective	AP type: Indoor, dual radio, 2.4, 5-GHz		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to : Wireless -> General Set both 2.4GHz and 5GHz in ON mode	**WLAN SPECIFICATIONS** **Operating Frequency** **Dual-Radio Concurrent 2.4GHz & 5 GHz** 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.5.b

Requirement	Dynamic frequency selection (DFS]		
Test Objective	Dynamic frequency selection (DFS]		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verification via the CPE document Wireless>Advance	**802.11ac (Wi-Fi 5)** and **802.11ax (Wi-Fi 6)** both operate in the 5 GHz band and can utilize DFS channels. **Channelization** 802.11ax supports very high throughput (VHT)—VHT 20/40/80/160 MHz 802.11n supports high throughput (HT)—HT 20/40 MHz 802.11n supports very high throughput (VHT) under the 2.4 GHz radio—VHT (1024-QAM) 802.11n/ac packet aggregation: AMPDU, ASPDU	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.5.c	
Requirement	Standards: IEEE 802.11 a/b/g/n/ac wave 2	
Test Objective	Standards: IEEE 802.11 a/b/g/n/ac wave 2	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verification via the CPE document	❖ IEEE 802.11a/b/g/n/ac/ax compliant

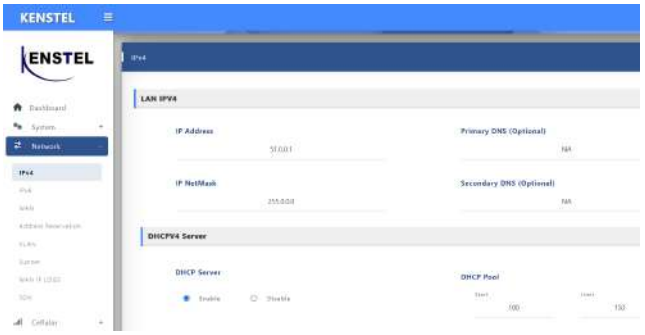
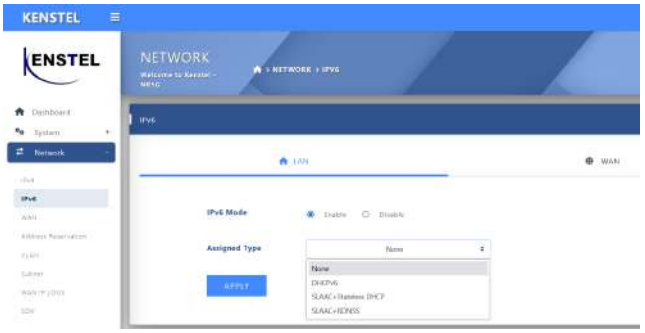
		Power Source Power-over-Ethernet: 802.3af/at or Proprietary 48V |IEEE 802.11e Compliant Source| Active Ethernet (PoE) QoS (Quality of Service) Compliant with IEEE 802.11e Standard | WMM	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.5.d		
Requirement	2x2 MU-MIMO with 2 spatial streams		
Test Objective	2x2 MU-MIMO with 2 spatial streams		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verification via the CPE document	Supported Radio Technologies 802.11b: Direct-Sequence Spread Spectrum (DSSS) 802.11a/g/n/ac/ax: Orthogonal Frequency-Division Multiplexing (OFDM) 802.11n/ac/ax: 4x4 MIMO with 4 Streams	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.5.e

Requirement	PHY rate: 500 Mbps (2.4 GHz) 2048 Mbps (5GHz)		
Test Objective	PHY rate: 500 Mbps (2.4 GHz) 2048 Mbps (5GHz)		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify via the CPE document	**WiFi** ❖ 802.11b/g/n/ac/ax: 2.4GHz Wi-Fi2x2 MIMO up to 600Mbps,5GHzWi-Fi 4x4MIMO up to 4.8Gbps. ❖ 1 GE port for LAN/WAN,1 GE port for LAN. ❖ Multi APN function (Optional) for Data, TR-069 services (Optional) ❖ Routing mode: NAT enable (Default)/IP pass-through (Optional) ❖ VPN client service (L2TP, PPTP)	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.5.f	
Requirement	IPv4 and IPv6 dual stack support	
Test Objective	IPv4 and IPv6 dual stack support	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Network -> IPv4 for ipv4 , IP address is available ; through which we can check in traceroute (in Diagnosis) also	❖ IPv4 and IPv6 dual stack support

	IPv6 can be found just below it . Put IPV4 in enable mode	 	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

RF

Test ID	4.16.6.a	
Requirement	Integrated Omni-directional Antenna	
Test Objective	Integrated Omni-directional Antenna	
Test Description	**Set Steps**	**Acceptance Criteria**

	Verification via the CPE document	Antenna WLAN :Four (4) Internal 3/5 dBi Dual-Concurrent Omni-Directional Antenna| N-Type WWAN: Four (4) Internal 5dBi dBi Wide BAnd Omni-Directional Antenna WWAN MMWAVE: QTM527 with 64 dual polarization antenna elements capable of transmitting power of more than 40dBm (Power Class 1)	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.6.b	
Requirement	Transmit Power : · 25 dBm on 2.4 GHz; · 25 dBm on 5 GHz	
Test Objective	Transmit Power : · 25 dBm on 2.4 GHz; · 25 dBm on 5 GHz	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verification via the CPE document	

Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

Test ID	4.16.6.c		
Requirement	Supports -95 dBm or better Receiver Sensitivity		
Test Objective	Supports -95 dBm or better Receiver Sensitivity		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Connect UE to CPE wifi and check required value in Net Monitor application		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

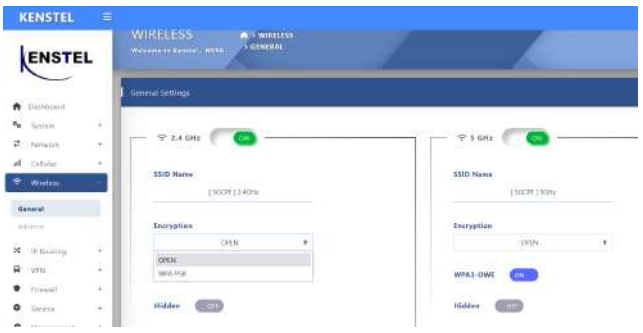
Test ID	4.16.6.d	
Requirement	Supports RF management	
Test Objective	Supports RF management	
Test Description	**Set Steps**	**Acceptance Criteria**

	Verify via the CPE Document		
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

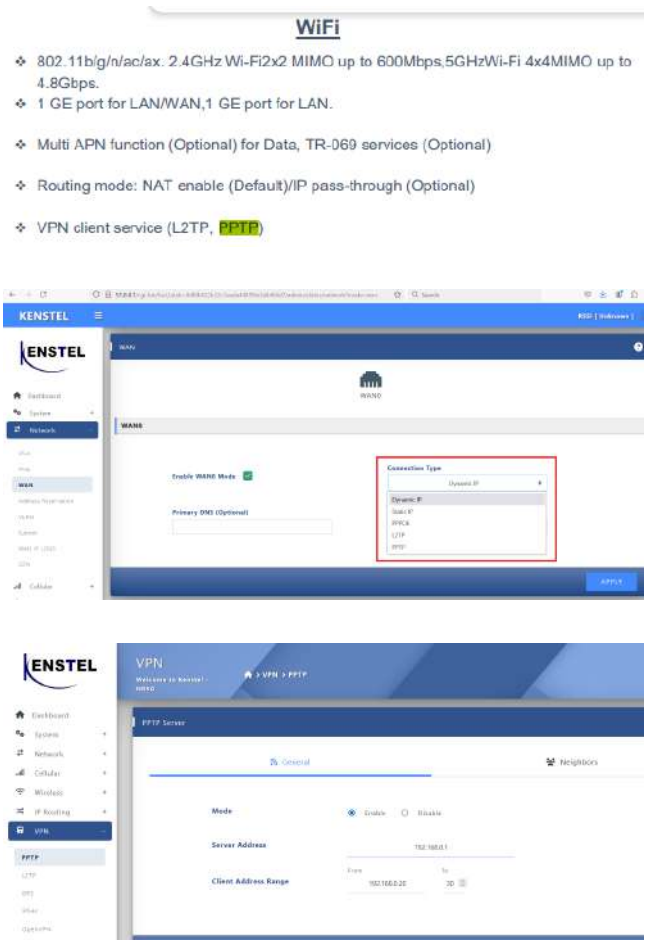
Test ID	4.16.6.e	
Requirement	Intelligent RF control plane for self-healing and self-optimization	
Test Objective	Intelligent RF control plane for self-healing and self-optimization	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verification via the CPE document	
Overall Test Result	Pass:☐	Fail:☐
Comments		

Name	Name of Verifier	Signature	

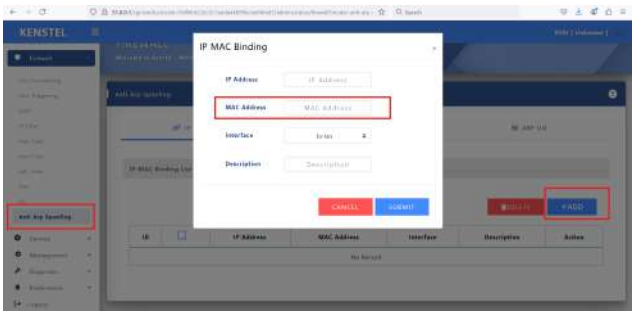
Security

Test ID	4.16.7.c	
Requirement	All version and Latest WPA support	
Test Objective	All version and Latest WPA support	
Test Description	**Set Steps**	**Acceptance Criteria**
	Wireless -> General	**Wireless Security** **WPA2** AES-PSK/**WPA2** Enterprise Hide SSID in Beacons MAC Address Filtering, Up to 32 MACs per SSID Wireless STA (Client) Connected List Https SSH Client Isolation 
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		

Name	Name of Verifier	Signature	

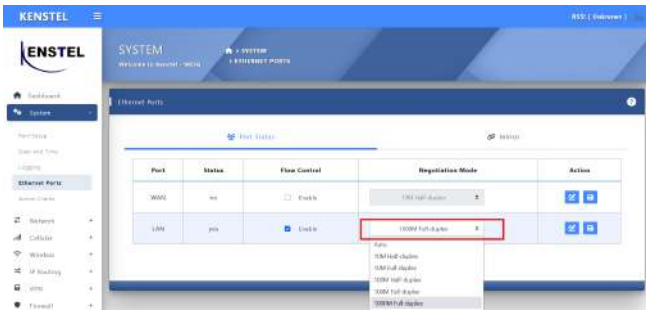
Test ID	4.16.7.e	
Requirement	IP Security (IPSec), PPTP, IP-Filtering	
Test Objective	IP Security (IPSec), PPTP, IP-Filtering	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Network -> WAN VPN -> PPTP	
Overall Test Result	Pass:☐	Fail:☐

Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.16.7.g	
Requirement	MAC address authentication	
Test Objective	MAC address authentication	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : Firewall -> Anti Arp Spoofing here we can enter desired mac address	Here we used **Anti-ARP Spoofing** which is a router feature that prevents attackers from linking their MAC address to another device's IP address through deceptive ARP messages. **Wireless Security** WPA2 AES-PSK/WPA2 Enterprise Hide SSID in Beacons MAC Address Filtering, Up to 32 MACs per SSID Wireless STA (Client) Connected List Https SSH Client Isolation 
Overall Test Result	Pass:☐	Fail:☐

Comments (if any)			
Name	Name of Verifier	Signature	

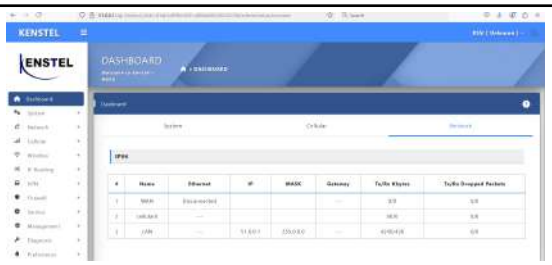
Interface

Test ID	4.16.8.a	
Requirement	2 X 1000 Base-T Ethernet	
Test Objective	2 X 1000 Base-T Ethernet	
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to : System -> Ethernet ports	**Physical Interface** 1x 10/100/1000/2500 BASE-T, RJ-45 Ethernet Port 1x 10/100/1000 BASE-T, RJ-45 Ethernet Port 
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		

Name	Name of Verifier	Signature	

Test ID	4.16.8.a	
Requirement	1 X SIM card slot (Nano-SIM)	
Test Objective	1 X SIM card slot (Nano-SIM)	
Test Description	**Set Steps**	**Acceptance Criteria**
	Physical Verification	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

Test ID	4.16.8.b	
Requirement	Power-over-Ethernet or DC Power	
Test Objective	Power-over-Ethernet or DC Power	
Test Description	**Set Steps**	**Acceptance Criteria**
	In the Dashboard , we can see the connection : connected or disconnected	

			
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Management

Test ID	4.16.9.a		
Requirement	Management: Standalone (via GUI) or through on premise based solution or cloud-based		
Test Objective	Management: Standalone (via GUI) or through on premise based solution or cloud-based		
Test Description	**Set Steps**	**Acceptance Criteria**	
	The management web page is accessible via the gateway ip of the CPE either via the ethernet or wifi connectivity .		
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.16.9.c		
Requirement	Compliant with IEEE 802.11e Standard		
Test Objective	Compliant with IEEE 802.11e Standard		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verification via the CPE document	**Power Source** **Power-over-Ethernet: 802.3af/at or Proprietary 48V |IEEE 802.11e Compliant Source| Active Ethernet (PoE)** **QoS (Quality of Service)** **Compliant with IEEE 802.11e Standard | WMM**	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

4.17 5G Camera

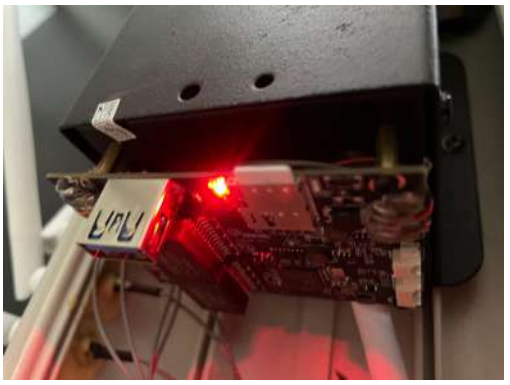
Test ID	4.17.1

Requirement	The camera shall supports advanced AI/ML video analytics Applications on MEC platform: Face Detection/ Recognition, People Counting, LPR(License Plate Recognition), Object Detection/Classification, and object pattern recognition models Etc.		
Test Objective			
Test Description	**Set Steps**	**Acceptance Criteria**	
	Open the application and add the facial information to the application for the ai and ml application demonstration.		
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

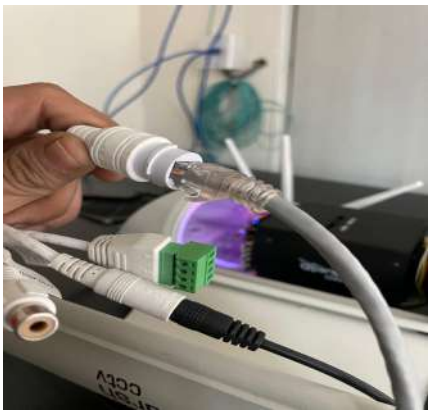
Test ID	4.17.2	
Requirement	5G enabled for Private Network. Supports Sub-6G bands: FR-1, N78	
Test Objective	Supports Sub-6G bands: FR-I, N78	
Test Description	**Set Steps**	**Acceptance Criteria**

	Camera support N78 band, it can be verified by attaching camera over N78 band frequency Open WEBUI verify by login also by https://192.168.128.1 Pass: xyz 	Connected cell info 
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		
Name	Name of Verifier	Signature

Test ID	4.17.3	
Requirement	SIM Card Supported : Nano SIM	
Test Objective	SIM Card Supported	
Test Description	**Set Steps**	**Acceptance Criteria**

	Nano sim card supported it can be verified on hardware		
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)	SIM card slot present in device		
Name	Name of Verifier	Signature	

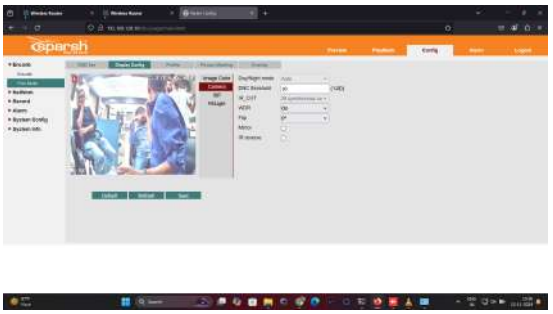
Test ID	4.17.4	
Requirement	Interface · 10/100/1000 Ethernet port – 1 nos · Audio · Alarm	
Test Objective	Interface · 10/100/1000 Ethernet port – 1 nos · Audio · Alarm	
Test Description	**Set Steps**	**Acceptance Criteria**

	All these options can be verified on hardware		
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)	The interfaces are available on the camera		
Name	Name of Verifier	Signature	

Camera

Test ID	4.17.5.a
Requirement	Sensor :5M / 8M effective resolution
Test Objective	Sensor resolution verification

Test Description	**Set Steps**	**Acceptance Criteria**	
	Image sensor is available with resolution upto 8MP, it can be verified by opening camera on web 192.168.128.10 Username :- admin Pass:- admin123 (default) 	Config->Encode settings 	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

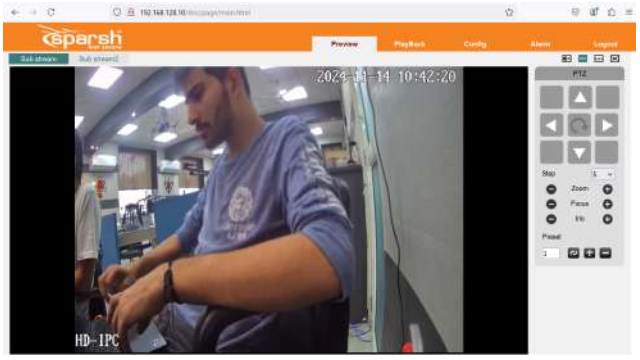
Test ID	4.17.5.b		
Requirement	Wide Dynamic Range (WDR) = 120dB to improves a camera's image quality under high-contrast lighting conditions where both dimly and brightly lit areas are present in the field of view		
Test Objective	Wide Dynamic Range		
Test Description	**Set Steps**	**Acceptance Criteria**	
	log in to the camera management url : 192.168.128.10 on the web browser. admin - username admin123- password. Config → Prev Mode → Display Config → Camera		
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)	Wide Dynamic Range (WDR) Option is present in the given snap.		
Name	Name of Verifier	Signature	

Test ID	4.17.5.c
Requirement	IR distance supported = 30 meter
Test Objective	IR distance verification

Test Description	**Set Steps**	**Acceptance Criteria**	
	supported and can be verified on ground	Verify by taking the image capture. verified by the Datasheet.	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)	Verified by the Datasheet.		
Name	Name of Verifier	Signature	

Test ID	4.17.5.d		
Requirement	Memory : Micro SD & SDXC slot up to 256GB		
Test Objective	Memory : Micro SD & SDXC slot up to 256GB		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Micro SD card support, it can be verified on hardware.	Verify Micro SD Card slot in Camera	
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)			
Name	Name of Verifier	Signature	

LENS

Test ID	4.17.6.a	
Requirement	Lens: Motorized, vary focal (2.7mm-13.5mm)	
Test Objective	zoom and focus	
Test Description	**Set Steps**	**Acceptance Criteria**
	Verification via the camera GUI	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)	toggle option for zoom , Focus and Iris present under the Preview option in the management console.	
Name	Name of Verifier	Signature

Test ID	4.17.6.b
Requirement	Field of View(FOV) : Horizontal – 98 Deg wide. Vertical – 50 Deg wide
Test Objective	Field of View (FOV) : Horizontal — 98 Deg wide. Vertical- 50 Deg wide.

Test Description	**Set Steps**	**Acceptance Criteria**	
	Complied reference in camera document		
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)	refer to the datasheet		
Name	Name of Verifier	Signature	

Test ID	4.17.6.c		
Requirement	Focus and IRIS Control : Auto		
Test Objective	Verify the IRIS control features of the camera		
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Compiled, it can be tested on ground by varying the lighting conditions of the camera .		
Overall Test Result	Pass:☐	Fail:☐	
Comments (if any)	can be verified via datasheet		
Name	Name of Verifier	Signature	

VIDEO

Test ID	4.17.7.a

Requirement	Video Compression : H.265 / H.264 / MJPEG or equivalent		
Test Objective	Video Compression: H.265 1--1.264 MJPEG or equivalent		
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. H.265 Supported, it can be verified via camera web interface.		
Overall Test Result	Pass:☐		
Comments (if any)			
Name	Name of Verifier	Signature	

Test ID	4.17.7.b	
Requirement	High speed live Streaming Capability	
Test Objective	Live streaming of camera feed	
Test Description	**Set Steps**	**Acceptance Criteria**

	Connect the camera to the 5g network link the mobile application to the camera start the live streaming of the camera feed		
Overall Test Result	Pass:☐	Fail:☐	
Comments	Verify the camera feed through rtsp over any streaming application like realtime video,vlc media player		
Name	Name of Verifier	Signature	

Test ID	4.17.7.c	
Requirement	Frame Rate = 1 – 30/60 fps	
Test Objective	Frame Rate = 1 – 30/60 fps	
Test Description	**Set Steps**	**Acceptance Criteria**
	Supported, it can be verified via camera web interface	
Overall Test Result	Pass:☐	Fail:☐
Comments (if any)		

Name	Name of Verifier	Signature	

Test ID	4.17.8		
Requirement	Power : PoE (802.3at)		
Test Objective	Power : PoE (802.3at)		
Test Description	**Set Steps**	**Acceptance Criteria**	
	Supported, it can be tested by using POE switch	Verify Physically	
Overall Test Result	Pass:☐	Fail:☐	
Comments			
Name	Name of Verifier	Signature	

4.18 Other Accessories for Installation

S.No	Equipment/Devices	Compliance
i.	Antennas & Passive components such as cables, connectors, mounting brackets, etc.; Power/OFC cables, AC-DC convertors, GPS antenna with accessories etc.	PHYSICAL INSPECTION

4.19 Technical Specification for Rack and other accessories

SN	Rack Technical Specifications	Compliance
4.19.1	Standard Intelligent racks to host 5G SA equipment.	PHYSICAL INSPECTION
4.19.2	Each cabinet should include 2 nos of Rack PDUs come with up to 16 outlets per strip or more.	PHYSICAL INSPECTION
4.19.3	Shall consist of 24U heights of Steel material to accommodate supplied Servers (3 or more), Routers, UPS, Battery, Monitor etc.	PHYSICAL INSPECTION
4.19.4	should have an open perforation area (more than 75%) on the door to help better cool servers.	PHYSICAL INSPECTION
4.19.5	The cabinet shall be comprised of modular cable management panels or finger sections.	PHYSICAL INSPECTION
4.19.6	32 inch FHD Display screen.(Wall/Tabletop)	PHYSICAL INSPECTION
4.19.7	UPS 5KVA with Battery for 1 hour backup on full load (whole Lab setup)	PHYSICAL INSPECTION
4.19.8	L2 Managed Switch 24x 1G ports +2 x 10G (fiber) with standard security, management, protocol, VLAN and IPV6 support	PHYSICAL INSPECTION
4.19.9	Optional: 1 U sliding rack optimized keyboard, mouse with KVM switch to monitor 3 servers and networking routers/switches.	PHYSICAL INSPECTION

5G LAB

User Acceptance Test

Document history

Version	Date	Author	Changed Sections	Change Description / reference
1.01	30/7/2024	Navin Gupta		5G core commands

Table of Content

1.1 Introduction 12
1.2 Purpose and Scope 12
1.3 Terms and Abbreviations 12
1.4 Physical Material Verification 13
Section 4.2 5G Network specs (Core + RAN) 15
4.2 (i) Radio Configuration 16
4.2 (ii) 3GPP Release 17
4.2 (iii) Data Rate (UL + DL) 18
4.2 (iv) Latency 19
4.2(v) Max No of Active Devices(That network can connect) 20
4.2 (vi) Radio Power 21
4.2 (vii) Duplexing Mode 22
4.2 (viii) Channel Bandwidth 23
4.2 (ix) Radio Band Support 25
4.2 (x)MIMO Configuration 26
4.2(xi) Synchronization 27
4.2(xii) Antenna 28
4.2(xiii) Mechaniacal/Environmental 29
4.2(xiv) MIMO 30
4.2(xv) Network Slicing 31
4.2(xvi) Uptime 33
4.2(xviii) MEC 34
4.2(xix) VoNR Support 36
4.2(xx) API's 38
4.2(xxi) NMS with Dashboards 40
4.2(xxii) Security 41
4.2(xxiii) 5G Devices 42
4.2(xxiv) IP Communication 44
Section 4.3 Funcitional Specification 5G SA Core Network 45
4.3.2(a) AUSF 46
4.3.2(b) AMF 51
4.3.2(c) Data Network (DN), e.g. operator services, Internet access or 3rd Party Service 55
4.3.2(e) NRF 56
4.3.2(f) NSSF 57
4.3.2(g) PCF 58
4.3.2(h) SMF 62
4.3.2(i) UDM 64
4.3.2(j) UDR 67
4.3.2(k) UPF 70
4.3.2(m) UE 72
4.3.2(n) RAN 73
4.3.2(p) NWDAF 74
4.3.4 Network Segmentation/Slicing for Customer QoS for Data Connectivity 75
4.3.6 VoNR 76
4.3.7 Should support open AP-s - for example any O & M (OSS/BSS integration) 77
4.3.7 MEC platform integration 79

4.3.10 uRLLC 79
4.3.11 mMTC 80
Section 4.4: 5G NR Radio 81
4.4.1(a) Funcition for Radio Resource Management :Radio Bearer Control, Radio Admission Control , Connectiln Mobility Control. Dynamic allocation of resources to UEs in voth uplink and Downlinj(Scheduling) 82
4.4.1(c) Routing of User Plane Data towards UPF(s); 84
4.4.1(d) Routing of Control Plane information towards AMF; 87
4.4.1(e) Connection setup and release; 89
4.4.1(f) Scheduling and transmission of paging messages; 91
4.4.1(g) Scheduling and transmission of system broadcast information (originated from the AMF or OAM); 93
4.4.1(h) Measurment and measurement reporting configuration for mobility and scheduling; 96
4.4.1(i) Transport level packet marking in the uplink 98
4.4.1(j) Session Management; 101
4.4.1(k) Support of Network Slicing; 103
4.4.1(l) QoS flow management and mapping to data radio bearers; 104
4.4.1(n) Distribution function for NAS message ; 106
4.4.3(a) Distribution function for NAS message ; 107
4.4.3(b) The transport network layer is built on IP Transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RANnode and the UPF ; 108
4.4.3(c) NG-U Provide non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF ; 109
4.4.3(d) Futher details of NG-U compliances as per 3GPP standards ; 111
4.4.4(a) NG-C provides the following funcition 113
4.4.4(b) NG interface management 114
4.4.4(c) UE context management 116
4.4.4(e) Transport of NAS message 117
4.4.4(f) Paging 118
4.4.4(g) PDU Session management 119
4.4.4(j) Further details of NG-C compliance as per 3GPP standards 120
4.4.5(c) Flow control. 121
4.4.7(a) Protocol stack for the user plane, i.e. SDAP, PDCP, RLC andMAC sublayers (terminated in gNB on the network side) should perform the functions as per 3GPP Release 15. 122
4.4.7(b) The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15 126
4.4.7(c) PDCP, RLC and MAC sublayers (terminated in gNB on thenetwork side) should perform the functions listed in 3GPP Standards 127
4.4.7(d) RRC (terminated in gNB on the network side) performs the functions listed in 3GPP Standards. 128
4.4.7(e) NAS control protocol (terminated in AMF on the network side) performs the functions listed in 3GPP Standards.for instance:authentication, mobility management, security control 130
Section 4.5 Multi-access Edge Computing framework 132
4.5 Check Virtualisation Support 133
4.5 Verify KVM Installation 133
4.5 Verify Dockers Installation 134
4.5 Check Mec Nodes 134

4.5 Check Mec Cloud status 135
4.5.5 Deploy Sample Mec Application 136
4.5 Check Mec Edge Status 137
4.5 Access the Mec Application 138
4.5 Check Resource allocation 139
4.5 Validate Network Configuration 139
4.5 Validate Storage 140
4.5 Deploy & Validate 140
Section 4.6 Support for Tracing & Testing 141
4.6.3 Configure Trace Requirement for UE in subscription Data 142
4.6.4 AMF Propagates trace Requirements to Network Entities 142
4.6.4 AUSF has received Trace Requirement 143
4.6.7 SMF has received trace requirement 143
4.6.7 PCF has received trace requirements 144
4.6.7 UPF has received trace requirement 144
4.6.7 Disable Trace 145
4.6.7 Review trace events 146
Section 4.8 Firewall with Router / SD-WAN Functional / Technical Specification 148
Basic Hardware Setup 149
Accessing Web GUI / Management Console 150
4.8.1.1 Gigabit Base-T (Cu) = 6 ports or higher(as required) | 1 Gs Fiber (SFP) = 4 ports 151
4.8.1.1 Gigabit Base-T (Cu) = 6 ports or higher(as required) | 1 Gs Fiber (SFP) = 4 ports 151
4.8.1.2 WAN Interfaces 152
4.8.1.3 Management Port 152
4.8.2 Firewall Features 153
4.8.3 Performance Requirement 154
4.8.3.1 Firewall throughput of 1 Gbps 155
4.8.3.2 Threat Protection – 500 Mbps 156
Application Specific Throughput (optional) 157
4.8.4 Web Filtering 158
4.8.4.1 Control access to websites and website categories(e.g. business, news, sports, social media) 160
4.8.4.2 Integrate into Active Directory, applying policies to specific users or user groups 162
4.8.4.3 Enforce Safe Search 163
4.8.4.4 Block or control access to Cloud services. 165
4.8.4.5 Detailed web access reports (by user, group, website) 166
4.8.4.6 Full SSL Inspection support 167
4.8.4.7 Transparent solution (or explicit proxy support) 168
4.8.5 Optional: Intrusion Prevention System 169
DDoS Attack Protection 170
4.8.5.1 Detect and block network borne attacks 171
4.8.5.2 Protect mail, web and remote-access servers fromattacks (IIS, Exchange, Citrix) 172
4.8.5.3 Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat) 173
4.8.5.4 Common web platform protection (e.g. .NET, PHP,WordPress, CRM) 174
4.8.5.5 Customizable rule-set and signatures 175
4.8.6.1 SSL and IPSec VPN support 176
4.8.6.2 Web-Portal and full VPN client application 178
4.8.6.2 Web-Portal and full VPN client application 179

4.8.6.3 Site-to-Site IPSec VPN (with Dynamic Routing) 180
4.8.6.4 Optional: RADIUS/Active-Directory integration 181
4.8.6.5 Optional: Granular network access policies 182
4.8.6.6 Two-Factor authentication support (e.g. Secure Token) 183
4.8.6.7 High performance VPN concentrator Solution 186
4.8.7.1 Control and monitor cloud application usage (e.g.Dropbox, Box, Google Apps) 187
4.8.7.2 Full network visibility of HTTP and HTTPS traffic 189
4.8.7.3 Control access to specific applications (e.g. WebGames, Video Streaming) 191
4.8.7.4 Block access to malicious content or websites 192
4.8.7.5 Detailed reporting and network visibility 194
4.8.7.5 Detailed reporting and network visibility 195
4.8.8.1 Dynamic routing (OSPF/BGP/RIP) 196
4.8.8.2 Load-Balancing and ECMP 198
4.8.8.3 802.1Q VLAN and Layer2 switching support 200
4.8.8.4 Rich traffic/shaping QOS support 201
4.8.8.5 Dynamic routing over VPN (e.g. OSPF) 204
Section 4.9 Server 1 with 5G Core, IMS and NMS software 205
4.9.1 Processor 206
4.9.2 Memory 207
4.9.3 Storage 207
4.9.4 Operating System And Virtualization Software 208
4.9.5 Network Interface 209
4.9.6 PCIe Slots 209
4.9.7.1Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control. 210
4.9.7.2 The servershould support industry standard management protocols i.e. IPMI, Red Fish API etc 211
4.9.7.3 One 1-Gbps RJ-45 management port 212
4.9.7.4 One 1-Gbps RJ-45 management port Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc 213
4.9.7.5 Auto generated technical support logs and forwarding to technical support for faster resolution. 214
4.9.7.6 Automated hardware configuration and Operating System deployment to multiple servers .215
4.9.7.7 The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues 216
4.9.7.8 The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility 217
4.9.7.9 The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status 218
4.9.7.10 The server should support multiple management interfaces including web user interface and command line interface. 219
4.9.8.1 The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 104-2 validated) or equivalent. 220
4.9.8.2 Se rver management system should provide anti counter feit 221

4.9.8.3 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent. 222
4.9.8.4 The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head) 223
4.9.8.5 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent. 224
Section 4.10 Server 2 with 5G MEC Platform and Application Server 225
4.10.1 Processor 226
4.10.2 Memory 226
4.10.3 Storage 227
4.10.4 Operating System And Virtualization Software 227
4.10.5 Network Interface 228
4.10.6 PCIe Slots 228
4.10.8.1Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control. 229
4.10.8.2 The server should support industry standard management protocols i.e. IPMI, Red Fish API etc 230
4.10.8.3 One 1-Gbps RJ-45 management port 231
4.10.8.4 One 1-Gbps RJ-45 management port Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc 232
4.10.8.5 Auto generated technical support logs and forwarding to technical support for faster resolution. 233
4.10.8.6 Automated hardware configuration and Operating System deployment to multiple servers 234
4.10.8.7 The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues 235
4.10.8.8 The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility 236
4.10.8.9 The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status 237
4.10.8.10 The server should support multiple management interfaces including web user interface and command line interface. 238
4.10.9.1 The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 104-2 validated) or equivalent. 239
4.10.9.2 Server management system should provide anti counter feit 240
4.10.9.3 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent. 241
4.10.9.4 The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head) 242
4.10.9.5 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent. 243
Section 4.11 5G rewriteable SIM (programmable) 243
Section 4.12 5G Evaluation Board 244
4.12.a RG520F 5G Module 245
4.12.b Cellular Modem-RF 246
4.12.c Performance Enhancement Technologies 246

4.12. d Physical and Wi-Fi Interface Modules. 247
4.12.e UART, SPI, I2C and GPIO Interface 247
4.12 f Sensor interfaces for medical devices, smart-home appliances and 248
smart-cityapplications 248
4.12.g SD Card Connector 249
4.12.h PCIe to USB Connector 249
4.12.i Dual (U)SIM card supported 250
4.12j Digital audio codec board interface 250
4.12.k Debug URAT 251
4.12.l USB Type C Interface 252
4.12.m LEDs indication 252
4.12.n Power key, Reset key, USB Boot, Power Switch 253
4.12.o 12 Antenna Interfaces 253
4.12.p Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi,Ethernet, Audio,
PCI TO USB, Power Adaptors 255
4.12.q AT command (external MCU integration) and SDK support (within the module 256
4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical
Devices, Agritech 256
4.12.a Quectel RG520F 5G Module 257
4.12.b Cellular Modem-RF 258
4.12.c Performance Enhancement Technologies 259
4.12.d Physical and Wi-Fi Interface Modules 260
4.12.e UART, SPI, I2C and GPIO Interface 260
4.12.f Sensor interfaces for medical devices, smart-home appliances and smart-city applications ... 261
4.12.g SD Card Connector 261
4.12.h PCI to USB Connector 262
4.12.i Dual (U)SIM card supported 263
4.12.j 1 digital audio codec board interface 264
4.12.k COM1 and COM2. Also support Main URAT, Debug URAT 264
4.12.l USB Type C 265
4.12.m LEDs indication 265
4.12.n Power key, Reset key, USB Boot, Power Switch 266
4.12.o 12 Antenna Interface 266
4.12.p Minimum Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi,
Ethernet, Audio, PCI TO USB, Power Adaptors 267
4.12.q AT command (external MCU integration) and SDK support (within the module) 267
4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical
Devices, Agritech etc. 268
4.12.e UART, SPI, I2C and GPIO Interface 271
4.12.n Power key, Reset key, USB Boot, Power Switch 274
Section 4.13 IOT Gateway 277
Basic Hardware Setup 278
4.13.1.1 CPU : Qualcomm or equivalent, Dual core or Higher 279
4.13.1.2 RAM -256 Mb 279
4.13.1.3 Module: 5G Sub-6Ghz SA 1/2 Gbps DL (4x4 MIMO) or higher , 900/600 Mbps UL (2x2) 280
4.13.1.4 Status: Signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP Bytes sent/received,
connected band, IMSI, ICCID 281

4.13.1.5 SMS/ Call Status 281
4.3.1.6 Supports sending and reading Unstructured Supplementary Service Data messages 282
4.3.1.7 APN 283
4.13.1.8 Possibility to use different PDNs for multiple network access and services 284
4.13.2.1 Supports 802.11b/g/n/ac 284
4.13.2.2 WiFi Security : WPA X /WEP/ TKIP variants as per the latest version 286
4.13.2.3 Support minimum 30 simultaneous WiFi User connections 287
4.13.2.4 Optional: Support LoRa, Sigfox any of the LPWAN 288
4.13.3.1 Supports all required Network Protocols 289
4.13.3.2 Supports Static and dynamic routing 290
4.13.3.3 Supports static and dynamic IP allocation 291
4.13.4.1 Multiple clients and a server can run simultaneously 292
4.13.4.2 WireGuard VPN client and server support 293
4.13.4.3 Port and tag-based VLAN separation 294
4.13.4.4 Supports up to 5 x VPn IPsec tunnels with differentAES/DES encryption 295
4.13.5.1 Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI; NAT; NAT-T 296
4.13.5.2 DDOS prevention (port scan prevention 298
4.13.5.3 Sets up custom data limits for SIM card 299
4.13.5.4 Blacklist for blocking out unwanted websites, Whitelistfor specifying allowed sites only 300
4.13.6.1 Status, configuration, FW update, CLI, troubleshoot,event log, system log. 302
4.13.6.2 Allows monitoring of: Device data, Mobile data,Network info, Availability 304
4.13.6.3 Allows monitoring of: Device Model, Revision and Serial Number, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP 305
4.13.6.4 Allows monitoring of: WAN Type, WAN IP, Mobile Operator Name, Mobile Signal Strength, Mobile Network Type 306
4.13.6.5 Firmware update from server, automatic notification 307
4.13.6.6 Management API over HTTP/HTTPS 308
4.13.7.1 Supports 1 or more SIMs 309
4.13.7.2 Supports Location Tracking 309
4.13.7.3 Supports USB 310
4.13.7.4 Supports Digital I/O Support 311
4.13.7.5 Supports minimum 4 nos 10/100/1000 Ethernet ports 311
4.13.7.6 Supports 1G WAN port. 312
4.13.7.7 Supports status LED 312
4.13.7.8 Supports PoE and DC power socket. 313
Section 4.14 5G Mini Drones 314
4.14.1.1,4.14.1.13(a) 5G enabled and controlled drone (m) 5G Modem (n78 band) 315
4.14.1.2 TSupports 5G nano SIM 316
4.14.1.3 Connectivity Options: Cellular (5G) and Wi-Fi for ubiquitous and long-range connectivity 316
4.14.1.15 Wi-Fi (2.4/5 GHz) 316
4.14.1.4 Qualcomm or equivalent onboard processing engine for AI/ML analytics Should support MEC applications 317
4.14.1.5 Autonomy: Visual Inertial Odometry (VIO), path planning, PX4, GPS-denied navigation, BVLOS, follow me 318
4.14.1.6 360 obstacle avoidance: Depth estimation, obstacle detection, map60ping and VOA 319
4.14.1.7 Payload Capacity – 500g/1 Kg or above 320

4.14.1.8 GPS or NAVIC enabled 320
4.14.1.9 Geo Fencing 321
4.14.1.10 Tracking sensor 321
4.14.1.11 Image Sensor 321
Section 4.15 XR (AR/VR) Device 322
4.15.1.1 XR(AR/VR) Device Specifications 323
4.15.1.2 XR(AR/VR) Device Specifications 323
4.15.1.3 XR(AR/VR) Device Specifications 323
4.15.2.1 Bluetooth 324
4.15.2.2 Wi-fi 324
4.15.2.4 3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass) 324
4.15.3.1 Display:24°field-of-view, 24-bitcolor LCD ,outdoor visible ,HD resolution 325
4.15.3.2 Microphone 325
4.15.3.3 Speaker 325
Section 4.16 5G Indoor CPE 326
4.16.1 Processor - Qualcomm or equivalent 327
4.16.1.1 CPU Clock Speed 1.0GHz or higher 327
4.16.1.2 CPU Cores Dual-core Cortex-A53 Arm or equivalent 327
4.16.2 Memory: 512 MB RAM or higher 327
4.16.3.1 3GPP Release 328
4.16.3.2 Sub-6 Band n78:TDD 328
4.16.3.3 5G Modem 329
4.16.3.4 Bandwidth Support 329
4.16.3.5 MIMO 330
4.16.3.6 Download speed 330
4.16.5.1 Wireless 330
4.16.5.2 Dynamic Frequency Selection 331
4.16.5.3 Standards: IEEE802.11a/b/g/n/acwave2 331
4.16.5.4: Wireless MIMO Support 332
4.16.5.5: Wireless PHY rate 332
4.16.5.6: IPv4/IPv6 support 333
4.16.6.a: Wireless Antenna 333
4.16.6.b: Transmit power 334
4.16.6.c: Receiver Sensitivity 334
4.16.6.d: RF Management 335
4.16.6.e: RF Control Plane 335
4.16.7.c Security: All version and latest WPA Support 336
4.16.7 e Security: IPSec,PPTP,IP-Filtering 336
4.16.7g MAC address authentication 337
4.16.8 a Interface 337
4.16.8 b SIM Slot 337
4.16.8 c POE 338
4.16.9.1 Management 338
4.16.9.3 IEEE 802.11e Standard 338
4.16.9.4 Intelligent RF Control Plane for self-healing and Self-Optimization 339
Section 4.17 5G Camera 340
4.17.1 Advanced AI/ML video analytics 341

4.17.2 Supports Sub-6G bands: FR-1, N78 341
4.17.3 SIM Card Supported 342
4.17.4 Interfaces 342
10/100/1000 Ethernet port. 342
Audio Port 342
Alarm Port 342
4.17.5 (a) 5M / 8M effective resolution 343
4.17.5 (b) Wide Dynamic Range (WDR)=120dB 343
4.17.5 (c) IR distance 343
4.17.5 (d) Memory: Micro SD & SDXC slot up to 256GB 344
4.17.6 (a) Lens: Motorized, vary focal (2.7mm-13.5mm). 344
4.17.6 (b)Field of View (FOV): 345
Horizontal – 98 Deg wide. 345
Vertical – 50 Deg wide. 345
4.17.6 (c) Focus and IRIS Control: Auto 345
4.17.7 (a) Video Compression: H.265 / H.264 / MJPEG or equivalent 346
4.17.7 (a) Frame Rate = 1 -30/60 346
4.17.8 Power: PoE (802.3at) 346

1.1 Introduction

1.2 Purpose and Scope

1.3 Terms and Abbreviations

The following table contains terms and abbreviations used in this project either directly explained or translated accordingly:

Term / abbreviation	Explanation

Table 1 Terms & Abbrevation

1.4 Physical Material Verification

Equipment/Device Check List/Spec verification				
S.no	**Equipment/Devices**	**Quantity**	**Make/Model**	**Sr. No.**
1.	5G Core	1	Coral Telecom	
2.	5G Radio	1		
3.	IMS solution	1		
4.	MEC & Application server	1		
5.	NMS (with Dashboard)	1		
6.	Router with Firewall	1		
7.	5G SIMs	50		
8.	5G Evaluation Board / Hardware and Software Development Kit.	1		
9.	IoT Gateway	1		
10	IoT sensors with analytics software (Loaded in Application server	1		
11	5G Mini Drone	1		
12	5G XR(AR/VR/MR) headset or Device (with loaded application such as remote maintenance / training/skill development/ education etc.)	1		
13	5G Indoor CPE	1		
14	5G Camera with AI enabled Video Analytics (Face/Object/Motion detection, people counting etc.)	1		
15	5G Handsets	2		
16	Adjustable Tripod Pole (3m)	1		
17	24 U Rack	1		
18	UPS 5KVA (1hr backup)	1		
19	32 inch FHD Display	1		
20	L2 Managed Switch (24 port)	1		
21	Testing & Tracing Tools	1		
22	Installation, Testing and Commissioning	LS		

Section 4.1 Physical Material Verification

Test ID	**Physical Material Verification**				
Requirement	Physical Material Verification				
Test Objective	To Check all physical material as per PO		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• To check the physical aspects of gNB such as Ethernet ports, optical ports, console ports, RF ports power ports, POE adaptor, GPS ports (if applicable). • To check the physical aspects of gNB antennas, fiber, SFP module & Ethernet cables. • Connect gNB with 5G NG (coral) Core using Switch and Ethernet/Optic cables.	1. No physical damage to 5G NR Radio. 2. Power on the 5G NR Radio. Check the current flow & voltage reading using clamp meter & multi meter. 3. Checked current and voltage in compliance within the limits 5G NR Radio as mentioned by Vendor rating. (40V-58V gnb operational voltage checked) 4. LEDs provided on the 5G NR Radio should be operational (Eg. LEDs for module Operational, Fault, Maintenance etc.)	OK OK OK OK		All Physical Materials status are verified and working Fine
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Physical material is checked and found ok				
Name & Signature	**NAME OF VERIFIER**				

Section 4.2 5G Network specs (Core + RAN)

S.no	Description
4.2.(i)	Radio Configurations
4.2 (ii)	3GPP Release
4.2 (iii)	Data Rate (UL + DL)
4.2(iv)	Latency
4.2 (v)	Max No. of active devices (That network can connect
4.2 (vi)	Radio Power
4.2(vii)	Duplexing
4.2 (viii)	Channel Bandwidth
4.2(ix)	Radio Band Support
4.2(x)	MIMO
4.2(xi)	Synchronization
4.2(xii)	Antenna
4.2(xiii)	Mechanical Environment
4.2(xiv)	MIMO Configuration
4.2(xv)	Network Slicing
4.2(xvi)	5G Use Case Scenarios
4.2(xvii)	Uptime
4.2(xviii)	MEC
4.2(xix)	VoNR Support
4.2(xx)	API
4.2(xxi)	NMS with Dashboard
4.2(xxii)	Security
4.2(xxiii)	5G Devices
4.2(xxiv)	IP Communicaton

4.2 (i) Radio Configuration

Test ID	**4.2 (i)Radio Configurations**				
Requirement	To Verify Radio Configurations of gNB				
Test Objective	To Check Radio Configuration of Integrated gNB should be as Per RFP submitted		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Physical verification of Integrated gNB Login gNB in Mobaxterm Tools ssh root@00.00.00.00 user name : root Password : Go to root directory Verify gnb config (CU,DU & RU)	Radio is configured integrated with RU, DU & CU	OK		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified all Radio Configurations of gNB.				
Name & Signature	**NAME OF VERIFIER**				

4.2 (ii) 3GPP Release

Test ID	**4.2 (ii) 3GPP Release**				
Requirement	To verify gNB compliance 3GPP release 15 as per RFP submitted				
Test Objective	Verify that gNB compliance 3GPP release		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Verify gNB compliance 3GPP release 15 & upgradable to Rel 16 in roadmap (	Verified that all functional and conformance testing are done during AT	OK		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	3GPP Release 15 and above supported after upgrade.				
Name & Signature	**NAME OF VERIFIER**				

4.2 (iii) Data Rate (UL + DL)

Test ID	**4.2 (iii) Data Rate (UL+DL)**				
Requirement	To verify gNB supports Data Rate (UL+DL) >=200 Mbps				
Test Objective	Verify that gNB supports Data Rate (UL+DL) >=200 Mbps		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the 5G gNB is brought up. • Install IPERF tool on 5G NGC and UE and Attach UE. • **For Downlink Test:** **On the UE side:** Open the iperf application in UE, Run **iperf –s –u –i1** **On the NGC side:** Open the terminal in NGC, Run **iperf –c [Ue IP] –u –i1 –b200M –t 60** • **For Uplink Test:** **On the UE side:** Open the iperf application in UE, Run **iperf –c [Ue IP] –u –i1 –b200M –t 60** **On the NGC side:** Open the terminal in NGC, Run **iperf –s –u –i1** • Verify that the data transfer is successful between the Server and the Client & vice versa.	1. To verify End to End systems are configured & gNB is radiating. 2. To verify the data rate, IPERF tool installed on 5G NGC & UE. **Testing methodologies:** 3.**For Downlink Result:** UE received DL data via iperf application from NGC. **Result:** DL Data Rate:340Mbps 4.**For Uplink Result:** UE send UL data to NGC via iperf application **Result:** UL Data Rate:40Mbps (OR) **Testing methodology:** To verify the DL & UL throughput in gNB Open mobaxtrem in laptop, Type, root@ [gNB IP] PW: Run, “watch cat gnb_du_cell_stats.txt” **Result:** DL Data Rate:340Mbps UL Data Rate:40Mbps	Ok OK Ok Ok Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that Data Rate of (UL+DL)>=200 Mbps DL Data Rate: 340mbps UL Data rate: 40mbps				
Name & Signature	**NAME OF VERIFIER**				

4.2 (iv) Latency

Test ID	**4.2 (iv) Latency**				
Requirement	To verify gNB compliance Latency <= 15ms as per Rel 16 3GPP standards.				
Test Objective	Verify that gNB supports Latency <= 15ms		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• gNB should be configured as per RFP& it is connected with 5G NGC.UE should register with NGC & data working. **Testing methodology:** • To use iperf tool to verify the latency between UE and 5G NGC. **Downlink Test:** **On the UE side:** Open the iperf application in UE, Run iperf –s –u –i1 **On the NGC side**: Open the terminal in NGC, Run iperf –c [Ue IP] –u –i1 –b200M –t 60 **Uplink Test:** **On the UE side:** Open the iperf application in UE, Run iperf –c [Ue IP] –u –i1 –b200M –t 60 **On the NGC side:** Open the terminal in NGC, Run iperf –s –u –i1	1. To verify End to End systems are configured & gNB is radiating. **For Downlink Result:** UE received DL data successfully via iperf application from NGC. **Result:** RTT iteration is < = 15ms **For Uplink Result:** UE send UL data successfully via iperf application to NGC. **Result:** RTT iteration is < = 15ms	Ok OK OK		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified Data transfer is successful & its latency is always less than 15ms.				
Name & Signature	**NAME OF VERIFIER**				

4.2(v) Max No of Active Devices(That network can connect)

Test ID	4.2 (v) Max No. of active devices (That network can connect)				
Requirement	To verify gNB supports Max No. of active devices (That network can connect)				
Test Objective	Verify that gNB supports Max No. of active devices		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Configure Max Bandwidth, PRB, SCS, OFDM symbols Duplex Mode, Band, maxNumUEs in gNB & maxNumUEs, maxPduSessions in NGC. • Max No of UE should successfully register with NGC.	1. To verify that End to End systems are configured & gNB is radiating. **2.Testing methodology:** To Login gNB via mobaxtrem. Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark >click File > open pcap log (filename. pcap) > Apply nas-5gs filter to verify max no. of PDU session **Result:** Verified up to 64 nos of active PDU session. 3.To verify Max no of active UE in gNB, Open mobaxtrem in laptop Type, root@ [gNB IP] Run,"watch cat gnb_du_cell_stats.txt" Command to check no of UE & RNTI values **Result:** Verified up to 64 no's of Active Users.	Ok OK OK		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified up to 64 numbers of Active Users				
Name & Signature	**NAME OF VERIFIER**				

4.2 (vi) Radio Power

Test ID	**4.2 (vi) Radio Power**				
Requirement	To verify gNB supports Radio Power upto 100mW				
Test Objective	Verify that gNB supports Radio Power upto 100mW		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Configure Nominal Tx Power, ss-PBCH-Block Power in gNB. • Set center freq, offset freq, adjacent ch power, offset ch power, Bandwidth in Spectrum Analyzer to measure gNB power.	1. To verify End to End systems are configured & gNB is radiating. **<u>Testing methodology:</u>** 2.To verify the configuration in gNB, Open mobaxtrem in laptop Type, root@ [gNB IP] PW: root Type path: /du/config/ Open me_config.xml file then check configuredMaxTxPower **Result:** Verified the gNB Radio power is 100 mW. 3. To verify calibration done in Spectrum Analyzer &measure the gNB power in Watt using Spectrum Analyzer.	Ok OK OK		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified Radio power output is 100mW via configuredMaxTxPower.				
Name & Signature	**NAME OF VERIFIER**				

4.2 (vii) Duplexing Mode

Test ID	**4.2 (vii) Duplexing Mode**				
Requirement	To verify gNB supports TDD Duplexing Mode				
Test Objective	Verify that gNB supports TDD Duplexing Mode		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• Integrated 5G NR Radio should be configured with TDD duplexing mode& it's connected with 5G NGC. • Configured Uplink & Downlink frequencies (should be same) in gnb_config.xml of gNB. • UE should successfully register with NGC.	1. To verify End to End systems are configured & gNB is radiating. **<u>Testing methodology:</u>** 2.Open the "Network Signal Guru" application in Android UE and see the "Mode" in which the UE is registered Result: Mode: TDD **3.**To verify the configuration in gNB Open mobaxtrem in laptop, Type, root@ [gNB IP] PW: Type path: /du/config/ Open gnb_config.xml file then check the Mode type Result: Mode Type: TDD	Ok OK OK		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified Duplex Mode: TDD in Network Signal guru application				
Name & Signature	**NAME OF VERIFIER**				

4.2 (viii) Channel Bandwidth

Test ID	**4.2 (viii) Channel Bandwidth**				
Requirement	To verify gNB supports 20MHz, 40MHz, 60MHz, 80MHz, 100MHz bandwidths				
Test Objective	Verify that gNB supports 20MHz, 40MHz, 60MHz, 80MHz, 100MHz bandwidths		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	

	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB.
	• Configure different bandwidths 20MHz, 40MHz, 60MHz, 80MHz, 100MHz in gNB.
		1. To verify End to End systems are configured & gNB is radiating.
		Gnb Config File :
		<bSChannelBwDL>100MHZ</bSChannelBwDL>
		<dlEarfcn>623333</dlEarfcn>
		<nrFreqBand>78</nrFreqBand>
		<subCarrierCfg>
		<offsetToCarrier>0</offsetToCarrier>
		<carrierBw>273</carrierBw>
		<subCarrierSpacing>KHz30</subCarrierSpacing>
		Ue Logs:
		servingCellConfigCommon
		{
		downlinkConfigCommon
		{
		frequencyInfoDL
		{
		frequencyBandList
		{
		{
		freqBandIndicatorNR 78
		}
		},
		offsetToPointA 0,
		scs-SpecificCarrierList
		{
		{
		offsetToCarrier 0,
		subcarrierSpacing kHz30,
		carrierBandwidth 273
			OK		

Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified 100MHZ bandwidth in Netmonster android application				
Name &	**NAME OF VERIFIER**				

Test ID	**4.2 (viii) Channel Bandwidth**
Signature	

4.2 (ix) Radio Band Support

Test ID	**4.2 (ix) Radio Band Support**				
Requirement	To verify gNB supports N78 Band				
Test Objective	Verify that gNB supports N78 Band		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • gNB configured with Freq Band Indicator= 78 in gnb_config.xml	1. To verify End to End systems are configured & gNB is radiating. **<u>Testing methodology:</u>** Check the gnb config file <nrFreqBand>78</nrFreqBand>	Ok Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified Band 78 through Network Gur application in UE				
Name & Signature	**NAME OF VERIFIER**				

4.2 (x)MIMO Configuration

Test ID	**4.2 (x) MIMO Configuration**				
Requirement	To verify gNB supports 2T2R MIMO configuration				
Test Objective	Verify that gNB supports 2T2R MIMO configuration		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and gNB is brought up and attach UE with gNB. • 2.Configure 2T2R MIMO configuration in gnb_config.xml of gNB.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 1.Verified Gnb Config file <dlNumAntPorts>2</dlNumAntPorts> <ulNumOfAntPorts>2</ulNumOfAntPorts> 2.Verified at RRC Reconfiguration message in pcab file pdsch-ServingCellConfig setup: { nrofHARQ-ProcessesForPDSCH n16, **maxMIMO-Layers 2**	Ok Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified 2T2R MIMO configuration in gnb_config.xml of gNB				
Name & Signature	**NAME OF VERIFIER**				

4.2(xi) Synchronization

Test ID	4.2 (xi) Synchronization				
Requirement	To verify gNB supports Synchronization IEEE 1588 standard				
Test Objective	Verify that gNB supports Synchronization IEEE 1588 standard		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Configure PTP port roles, Clock Identity, Sync Interval, Multicast/Unicast Mode in PTP Grandmaster Clock & gnb_config.xml of gNB. UE should successfully register with NGC.	1. To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify the configuration in gNB Open putty in laptop, Type ssh root@ [gNB IP], PW: root Run below commands, show ptp status show sync status show clock sync status Result: PTP: Locked State: Synchronized Synchronization source: PTP	Ok OK		
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)	Verified gNB supports Synchronization IEEE 1588 standard.				
Name & Signature	**NAME OF VERIFIER**				

4.2(xii) Antenna

Test ID	**4.2 (xii) Antenna**				
Requirement	To verify gNB supports External Antenna				
Test Objective	Verify that gNB supports External Antenna		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • gNB connect with SMA connector type Omni External antenna. • UE should successfully register with NGC.	1. To verify End to End systems are installed and configured & gNB is radiating. 2. Physically Verified the External antenna connected to gNB. **<u>Testing methodology:</u>** 3.Access the gNB in chrome browser, Type gNB IP to check gNB config in EMS (http://xx.xx.xx.xx:8080/) can verify, Steps: **Login EMS→ click gNB → click Cell→** **No of Antenna Ports:** 2x2 Result: 2X2	Ok OK		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Physically Verified the External antenna connected to gNB and checked 2x2 configuration via EMS				
Name & Signature	**NAME OF VERIFIER**				

4.2(xiii) Mechaniacal/Environmental

Test ID	**4.2 (xiii) Mechanical/Environmental**				
Requirement	To verify gNB supports Mechanical/Environmental standard IP54/QM333				
Test Objective	Verify that gNB supports Mechanical/Environmental standard IP54/QM333		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Perform environmental test on gNB such as temperature, humidity as per QM333 standard. • Perform dust and water spray test on gNB as per IP54 standard.	1.To verify End to End systems are configured & gNB is radiating 2.To verify that gNB working reliably during environmental testing 3.To verify that gNB working reliably during water& spray testing	Ok OK		
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)	Verified gNB compliance Mechanical/Environmental standard IP54/QM333				
Name & Signature	**NAME OF VERIFIER**				

4.2(xiv) MIMO

Test ID	4.2 (xiv) MIMO Configuration				
Requirement	To verify gNB supports 2T2R MIMO configuration				
Test Objective	Verify that gNB supports 2T2R MIMO configuration		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and gNB is brought up and attach UE with gNB. • Configure 2T2R MIMO configuration in gnb_config.xml of gNB	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify MIMO configuration in gNB, Open mobaxtrem in laptop, Type, root@ [gNB IP] PW: root Type path: /du/config/ Open gnb_config.xml file then check MIMO configuration Result: 2T2R MIMO	Ok Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified 2T2R MIMO configuration in gnb_config.xml of gNB				
Name & Signature	**NAME OF VERIFIER**				

4.2(xv) Network Slicing

Test ID	4.2 (xv) Network Slicing				
Requirement	To verify gNB supports Network Slicing				
Test Objective	Verify that gNB supports Network Slicing		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Configure Network slicing parameters in gnb_config.xml of gNB. • UE should successfully register with NGC.	1. To verify End to End systems are configured & gNB is radiating. Testing methodology: 1.verify supported NSSAI in NGsetup Response NGSetupResponse protocolIEs: 4 items Item 0: id-AMFName Item 1: id-ServedGUAMIList Item 2: id-RelativeAMFCapacity Item 3: id-PLMNSupportList ProtocolIE-Field id: id-PLMNSupportList (80) criticality: reject (0) value PLMNSupportList: 1 item Item 0: PLMNSupportItem pLMNIdentity:00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) sliceSupportList: 4 items Item 0: SliceSupportItem s-NSSAI sST: 01 Item 1: SliceSupportItem s-NSSAI sST: 02 Item 2: SliceSupportItem s-NSSAI sST: 03 Item 3: SliceSupportItem s-NSSAI sST: 03 sD: 030609	OK OK		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified configured Slice value in EMS Slice (NSSAI): SST: X, SD: XXX				
Name &	**NAME OF VERIFIER**				

Signature	

4.2(xvi) Uptime

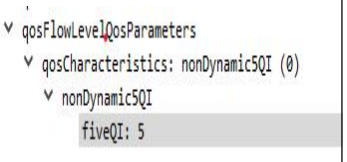
Test ID	4.2 (xvii) Uptime				
Requirement	To verify gNB provides 99% of uptime.				
Test Objective	Verify that gNB supports 99% of uptime.		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • To Verify gNB provides uptime 99%.	1.To verify End to End systems are configured & gNB is radiating & its synched with EMS. **<u>Testing methodology:</u>** 2.To check gNB uptime, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, "watch cat gnb_du_cell_stats.txt" **Result:** gNB uptime: 99%	Ok Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified gNB supports 99% of uptime by checking the cell status timing in gNB logs				
Name & Signature	**NAME OF VERIFIER**				

4.2(xviii) MEC

Test ID	4.2 (xviii) MEC				
Requirement	To verify gNB supports MEC				
Test Objective	Verify that gNB supports MEC		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Configure gNB with MEC API orchestrator platform. • UE should successfully register with NGC.	1.To verify End to End systems are configured & gNB is radiating **Testing methodology:** 2.To verify that gNB is integrated with MEC API orchestrator, Open putty in laptop,Type, ssh root@ gNB IP , Run below commands, show mec configuration show mec api-status show mec services **Result**: API Name: MEC Status: Active, Latency: 10ms 3.To verify that UE send & receive data from gNB via MEC platform, To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap Validation: Open Wireshark app in laptop. Open Wireshark >click File > open pcap log (filename. pcap) > Apply ip. addr ==<MEC_IP_address> http || sctp || udp filter Result: Verified gNB routes UDP packets using MEC platform.	Ok Ok OK		
Overall Test Result	Pass: □	Fail: □			

Remarks / Comments (If Any)	Verified that gNB routes traffic using MEC platform
Name & Signature	**NAME OF VERIFIER**

4.2(xix) VoNR Support

Test ID	4.2 (xix) VoNR Support				
Requirement	To verify gNB supports VoNR				
Test Objective	Verify that gNB supports VoNR		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• gNB should be configured as per RFP& its connected with NGC with Sngrep IMS node. • Perform UE registration. The UE shall also register with Sngrep IMS node. • Initiate VoNR call. The 5G NR Radio shall create dedicated bearer with QFI-1.	1.To verify gNB is configured as per RFP& its connected with NGC with Sngrep IMS node. **Testing methodology:** 2.Verify that UE registration successful & QFI-5 is established for IMS via pcap log, **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] PW: root Run, tcpdump -i [Ethernet/optical interface of gNB] -w [filename].pcap **Validation:** Open Wireshark app in laptop. Open Wireshark >click File > open pcap log (filename. pcap) > Apply nas-5gs || sip|| gtp Filter in pcap log. **Result:** QFI-5 is established.  3.Verify that VoNR call is successful &QFI-1 is established in pcap log. qos_rule_precedence = 255 (0xff) qfi_present = 1 (0x1) segregation = 0 (0x0)	Ok OK Ok		

		qfi = 1 (0x1) Open Wireshark >click File > open pcap log (filename. pcap) > Apply gtp || gtpu, rtp, sip, UDP filters in pcap log Result: OFI-1 Is established.			
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)	Verified gNB supports VoNR via Wireshark logs.				
Name & Signature	**NAME OF VERIFIER**				

4.2(xx) API's

Test ID	4.2 (xx) API's				
Requirement	To verify gNB supports APIs for NMS, MEC platform integration,OT/IT integrations.				
Test Objective	Verify that gNB supports APIs for NMS, MEC platform integration,OT/IT integrations.		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Configure API endpoints in gNB for NMS. • Configure API endpoints in gNB for MEC platform integration. • Configure API endpoints in gNB cli for OT/IT integrations.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify that fault, performance, configuration management& software upgrade menu in NMS dashboard. **Steps:** Login NMS→ click gNB→ Performance Report. Login NMS→ click gNB→ Cell→ configuration. Login NMS→ click gNB→ Maintenance→ Software Upgrade/Downgrade. **Result:** Software upgradation &downgrade are done. 3.To verify that gNB is integrated with MEC API, **Steps**: Open putty in laptop, Type, ssh root@ gNB IP PW: root Run below commands, show mec configuration show mec api-status show mec services **Result:** API Name: MEC Status: Active Latency: 10ms 4.To verify gNB that supports smart village IoT applications using OT/IT integration.	Ok OK Ok Ok		
Overall Test Result	Pass: □	Fail: □			

Remarks / Comments (If Any)	Verified that gNB supports APIs for NMS, MEC platform integration,OT/IT integrations
Name & Signature	**NAME OF VERIFIER**

4.2(xxi) NMS with Dashboards

Test ID	4.2 (xxi) NMS with dashboards				
Requirement	To verify gNB supports NMS with dashboards				
Test Objective	Verify that gNB supports NMS with dashboards		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Configure API endpoints in gNB cli for NMS • Integrate gNB with NMS using API platform.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify that fault, performance, configuration management& software upgrade menu in NMS dashboard. Login the chrome browser with gNB ip (http://xx.xx.xx.xx:8080/). **Steps:** Login NMS→ click gNB→ Performance Report. Login NMS→ click gNB→ click Cell→ configuration. Login NMS→ click gNB→ click Maintenance→ Software Upgrade/Downgrade. Login NMS→ click gNB→ click Cell→ Power Monitoring. Login NMS→ click gNB→ click Dashboard→ Alarms & Inventory. **Result:** gNB shall be able to successfully upgrade or downgrade the software and the configuration update via NMS	Ok OK Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports NMS with dashboards via Login NMS→ click gNB→ Performance Report. Login NMS→ click gNB→ click Cell→ configuration. Login NMS→ click gNB→ click Maintenance→ Software Upgrade/Downgrade.				
Name & Signature	**NAME OF VERIFIER**				

4.2(xxii) Security

Test ID	4.2 (xxii) Security				
Requirement	To verify gNB supports Security				
Test Objective	Verify that gNB supports Security		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Configure gNB with Network slicing. • Configure Ipsec in gNB with NGC.	1.To verify End to End systems are configured &gNB is radiating. **Testing methodology:** 2.To verify that each slice security policies & data encryption, **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] PW: root Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark > File > open pcap log > Apply filter, ip. addr == <Slice_1_IP_address> || ip. addr == <Slice_2_IP_address> tls || ssl || ipsec **Result:** Control plane&User plane packets are encrypted.	Ok OK Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports slicing & Ipsec Security functionalities				
Name & Signature	**NAME OF VERIFIER**				

4.2(xxiii) 5G Devices

Test ID	4.2 (xxiii) 5G Devices				
Requirement	To verify 5G Devices support private PLMN IDs				
Test Objective	Verify that 5G Devices support private PLMN IDs		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	

	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB.
	• Configure gNB with private PLMN IDs.
	• Ensure 5G devices private PLMN ID is available in the network selection list.
		1.To verify that End to End systems are configured &gNB is radiating.
		Testing methodology:
		2.To verify that gNB supports private PLMN IDs via Wireshark log,
		Steps:
		To Login gNB via mobaxtrem,
		Open mobaxtrem in laptop,
		Type, root@ [gNB IP]
		Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap
		Validation:
		Open Wireshark app in laptop.
		Open Wireshark > File > open pcap log > Apply nas-5gs && plmn-id filters.
		4.verify gnb config file for PLMN as below,
		<pLMNIdList>
		<MCC>001</MCC>
		<MNC>01</MNC>
		5.verify ue log :
		systemInformationBlockType1
		plmn-IdentityList
		{
		{
		mcc
		{
		0,
		0,
		1
		},
		mnc
		{
		0,
		1
		}
		Result:
		Private PLMN-ID: 001 01
			Ok
			
			OK
			
			Ok		

Overall Test Result	Pass: □	Fail: □
Remarks / Comments (If Any)	Verified by configuring the PLMN MCC-001 & MNC-01 with available test mobiles via Open Wireshark > File > open pcap log > Apply > nas-5gs && plmn-id filters.	
Name & Signature	**NAME OF VERIFIER**	

4.2(xxiv) IP Communication

Test ID	4.2 (xxiv) IP communication				
Requirement	To verify gNB supports IPv4 and IPv6				
Test Objective	Verify that gNB supports IPv4 and IPv6		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Perform UE registration with APN protocol IPv4/IPv6 configuration. • Perform UE registration with APN protocol IPv4/IPv6 configuration.	1. To verify End to End systems are configured &gNB is radiating. **Testing methodology:** 2.To verify that IPv4/IPv6 in PDU in Wireshark log, **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark > File > open pcap log > Apply nas-5gs> PDU session establishment accept>IPv4/IPv6 **TransportLayerAddress (IPv4):** 192.168.15.10 session **Result:** IPv4:192.168.11.9 IPv6:2001:4490:c1c:f8b1:25a7:eb80:2bfb:fca5	Ok OK Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

Section 4.3 Funcitional Specification 5G SA Core Network

S.no	Description
4.3.2(a)	AUSF
4.3.2(b)	AMF
4.3.2 (c)	Data Rate (UL + DL)
4.3.2(e)	NRF
4.3.2 (f)	NSSF
4.3.2 (g)	PCF
4.3.2(h)	SMF
4.3.2(i)	UDM
4.3.3(j)	UDR
4.3.2(k)	UPF
4.3.2(m)	UE
4.3.2(n)	RAN
4.3.2(p)	NWDAF
4.3.4	Network Segmentation / Slicing for Customer QoS for Data Connectivity
4.3.6	VoNR
4.3.7	Should support open AP-S for example any O & M (OSS/BSS Integration)
4.3.10	uRLLC
4.3.11	mMTC

4.3.2(a) AUSF

Test ID	4.3.2 (a) AUSF		
Requirement	Ensure AUSF functionality.		
Test Objective	Check Service Status of AUSF.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command systemctl restart coral5gs-ausfd.service OR by Wireshark **AUSF registration with NRF** **AUSF request to NRF:** HEADERS [4747]: PUT ***/nnrf-nfm/v1/nf-instances/b9f1a6ac-9ff7-41ef-b9b5-c12304175775*** Header: ***user-agent: AUSF*** Header: 3gpp-sbi-sendertimestamp: Mon, 11 Nov 202410:24:43.073 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **NRF response to AUSF:** **HEADERS[4747]: 201 Created** Header: :status: 201 Created **Json Body:** **DATA[4747], JSON (application/j son) Object** Member: nfInstanceId Member: nfType Member: nfStatus	**Expected Output:** Active: active (running) Service ID: f069e640-304a-41e9-8bce-f30e3795f078 Value: AUSF user-agent: AUSF Value: NRF Value: 201 : status: 201 Member: nfType [Path with value: /nfType:AUSF] [Member with value: nfType:AUSF] String value: AUSF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED]	

Test ID	4.3.2 (a) AUSF		
		[Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	
	Member: nfProfileChangesSupportInd	Value: nausf-auth	
	APIs 1. **Service provide by AUSF** **url :*POST /nausf-auth/v1/ue-authentic ations*** **SBI Interface Refrence Point - N12(Between AUSF and AMF)** Header: 3gpp-sbi-sender-timestamp Header: 3gpp-sbi-max-rsp-time: 10000 **Json body:** **DATA[3], JSON (application/json) Object**		
	Member: supiOrSuci	Member : supiOrSuci [Path with value: /supiOrSuci:suci-0-001-01-0-0-0-0123456902] [Member with value: supiOrSuci:suci-0-001-01-0-0-0-0123456902] String value: suci-0-001-01-0-0-0-0123456902 Key: supiOrSuci [Path: /supiOrSuci] [Path with value: /servingNetworkName:5G:mnc001.mcc001.3gppnetwork.org]	
	Member: servingNetworkName	[Member with value: servingNetworkName:5G:mnc001.mcc001.3gppnetwork.org] String value: 5G:mnc001.mcc001.3gppnetwork.org	

Test ID	4.3.2 (a) AUSF		
	2.SBI Interface Refrence APIs **API -** ***POST /nudm-ueau/v1/suci-0-001-01-0-0-0-0123456902/security-information/generate-auth-data*** **(Between AUSF and UDM)** Method-POST Interface Refrence Point - N13 Header: 3gpp-sbi-sender-timestamp: Mon, 11 Nov 2024 10:24:43.073 GMT Header: user-agent: AUSF Header: 3gpp-sbi-max-rsp-time: 10000 **Response from UDM to AUSF** HEADERS[707]: 200 OK Header: :status: 200 OK **DATA[13], JSON DOT (application/j son)** **Object** **Member:** authType Member: authenticationVector	Value: nudm-ueau Value: AUSF user-agent: AUSF Value: UDM Value: 200 :status: 200 String value: 5G_AKA Key: authTyp Member: rand [Path with value: /authenticationVector/rand:a141508579f08b5c4d9d76681490cdf7] [Member with value: rand:a141508579f08b5c4d9d76681490cdf7]String value: a141508579f08b5c4d9d76681490cdf7 Key: rand [Path: /authenticationVector/rand]	

Test ID	4.3.2 (a) AUSF		
	Member: supi	Member: autn [Path with value: /authenticationVector/autn:062409cf9e1e8000c55bff42880e2351][Member with value autn:062409cf9e1e8000c55bff42880e2351]String value: 062409cf9e1e8000c55bff42880e2351 Key: autn [Path: /authenticationVector/autn] Member: kausf [Path with value: /authenticationVector/kausf:93718cc4d195c9ee5c8ad05ee89cfd9af03c35830ef9193008aa1515e21482da] [Member with value: kausf:93718cc4d195c9ee5c8ad05ee89cfd9af03c35830ef9193008aa1515e21482da] String value: 93718cc4d195c9ee5c8ad05ee89cfd9af03c35830ef9193008aa1515e21482da Key: kausf [Path: /authenticationVector/kausf] Member: supi [Path with value: /supi:imsi-001010123456902] [Member with value: supi:imsi-001010123456902] String value: imsi-001010123456902 Key: supi [Path: /supi]	
	Response from AUSF to AMF **HEADERS[3]: 201 Created Header: :status: 201 Created** **DATA[23], JSON (application/3 gpphal+json)** **Object** Member: authType	Value: 201 :	

Test ID	**4.3.2 (a) AUSF**		
		status: 201	
	Member:5gAuthData	Member: authType [Path with value: /authType:5G_AKA] [Member with value: authType:5G_AKA]String value: 5G_AKAKey: authType[Path: /authType] Member: rand [Path with value: /5gAuthData/rand:d7d85f51c96c020757841fcfe20d3006] [Member with value: rand:d7d85f51c96c020757841fcfe20d3006]String value: d7d85f51c96c020757841fcfe20d3006Key: rand[Path: /5gAuthData/rand]	
	Member:_links	Member: autn [Path with value: /5gAuthData/autn:c804de5f61568000988457d7a9740ff0 [Member with value:autn:c804de5f61568000988457d7a9740ff0]String value: c804de5f61568000988457d7a9740ff0Key: autn[Path: /5gAuthData/autn]	
Overall Test Result	Pass: □	Fail: □	
Remarks /Comments (If Any)			
Name & Signature	**NAME OF VERIFIER**		

4.3.2(b) AMF

Test ID	**4.3.2(b) AMF**		
Requirement	Ensure AMF functionality.		
Test Objective	Check Service Status of AMF.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Restarting AMF for registration *systemctl restart coral5gs-amd.service* **AMF registration with NRF:** **1.1 AMF request to NRF** **HEADERS[1]: *PUT /nnrf-nfm/v1/nf-instances/ 2a92ad60-a017-41ef-96bd-15f0b46f6729*** Header: 3gpp-sbi-sender-timestamp: Mon, 11 Nov 2024 10:24:43.073 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **1.2 NRF response to AMF** HEADERS[19]: 201 Created Header: :status: 201 Created **Json body:** **DATA[305], JSON (application/json-p atch+json)** Object Member: nfInstanceId	**Expected Output:** Active: active (running) Service ID: 1b87483a-305b-41e9-b670-2985996f8551 Value: 201 : status: 201 Member: nfInstanceId [Path with value: /nfInstanceId:2a92ad60-a017-41ef-96bd-15f0b46f6729]	

Test ID	4.3.2(b) AMF		
		[Member with value: nfInstanceId:2a92ad60-a017-41ef-96bd-15f0b46f6729] String value: 2a92ad60-a017-41ef-96bd-15f0b46f6729 Key: nfInstanceId [Path: /nfInstanceId]	
	Member: nfType	Member: nfType [Path with value: /nfType:AMF] [Member with value: nfType:AMF] String value: AMF Key: nfType [Path: /nfType]	
	Member: nfStatus	Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	
	Member: nfProfileChangesInd		
	Verification of Communication service API: - **UE Registration** **Registration request from UE to AMF on N1 Interface:** **InitialUEMessage, Registration request,** **[RRCEstablishmentCause=mo-Signalling]** protocolIEs: 5 items Item 0: id-RAN-UE-NGAP-ID Item 1: id-NAS-PDU	RAN-UE-NGAP-ID 85 nR-CGI	

Test ID	4.3.2(b) AMF		
	Item 2: id-UserLocationInformation	pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) 0000 0000 0000 0000 0000 0000 0000 1111.... = nRCellIdentity: 0x00000000f tAI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01)	
	Item 3: id-RRCEstablishmentCause	tAC: 1 (0x000001)	
	Item 4: id-UEContextRequest **Registration accept from AMF to UE** **initialContextSetupRequest, Registration accept** protocolIEs: 8 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-GUAMI Item 3: id-AllowedNSSAI Item 4: id-UESecurityCapabilities Item 5: id-SecurityKey Item 6: id-MaskedIMEISV Item 7: id-NAS-PDU	AMF-UE-NGAP-ID: 1 RAN-UE-NGAP-ID: 41 s-NSSAI sST: 01 sD: 030609 SecurityKey: a81a1340f7ff77 cb880f3872527536c515fe4fc1f91f27 eea6f45729bb02ccb4 [bit length	

Test ID	**4.3.2(b) AMF**		
		256] .... .001 = 5GS registration result: 3GPP access (1)	
	Registration complete from UE to AMF **UplinkNASTransport,Registration complete protocolIEs: 4 items** Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-NAS-PDU Item 3: id-UserLocationInformation	AMF-UE-NGAP-ID: 1 RAN-UE-NGAP-ID: 41 Message type: Registration complete (0x43) tAC: 1 (0x000001)	
Overall Test Result	Pass: □	Fail: □	

4.3.2(c) Data Network (DN), e.g. operator services, Internet access or 3rd Party Service

Test ID	4.3.2 (c) Data Network (DN), e.g. operator services, Internet access or 3rd party services		
Requirement	Data Network(DN)		
Test Objective	Verify the Data Network -Internet access by 3rd party service.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Ping request from UE to DN: **Echo (ping) request id=0x002a, seq=2/512, ttl=64 (reply in 11)** GPRS Tunneling Protocol TEID: 0x00002f82 (12162) Internet Protocol Version 4, Src: 10.101.0.x (10.101.0.x), Dst: dns.google (8.8.8.8) Source Address: 10.101.0.x (10.101.0.x) Destination Address: dns.google (8.8.8.8) [Stream index: 0] **Ping reply from DN to UE:** **Echo (ping) reply id=0x002a, seq=2/512, ttl=55 (request in 6)** GPRS Tunneling Protocol Flags: 0x34 Message Type: T-PDU (0xff) Length: 92 TEID: 0x00000001 (1) Source Address: dns.google (8.8.8.8) Destination Address: 10.101.0.x (10.101.0.x) [Stream index: 0]	TEID: 0x00002f82 (12162) Source Address: 10.101.0.x Destination Address: dns.google (8.8.8.8) TEID: 0x00000001 (1) Source Address: dns.google (8.8.8.8) Destination Address: 10.101.0.x (101.202.0.2)	
Overall Test Result	Pass: □	Fail: □	

4.3.2(e) NRF

Test ID	**4.3.2(e)NRF**		
Requirement	Ensure NRF Is Available		
Test Objective	Check Service Status of NRF		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command Systemctl restart coral5gs-nrfd.service NF discovery service triggering by AMF for AUSF to NRF: HEADERS[105]: GET ***/nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-nf-type=AUSF*** Header: :path: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-**nf-type=AUSF** **Response from NRF** HEADERS[105]: 200 OK **Json body:** **DATA[471], JSON (application/json)** Object Member: validityPeriod Member: nfInstances Array Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: ipv4Addresses Member: nfServiceList	**Expected Output:** Service: coral5gs-nrfd.service Active: active (running) Value: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=AMF&service-names=nausf-auth&target-nf-type=AUS HEADERS[105]: 200 OK Member: serviceName [Path with value: /nfInstances/[]/nfServiceList/33ff5732-a00c-41ef-b14f-f5dec28a6926/serviceName:nausf-auth] [Member with value: serviceName:nausf-auth] String value: nausf-auth Key: serviceName [Path: /nfInstances/[]/nfServiceList/33ff5732-a00c-41ef-b14f-f5dec28a6926/serviceName]	
Overall Test Result	Pass: □	Fail: □	

4.3.2(f) NSSF

Test ID	**4.3.2 (f) NSSF**		
Requirement	Ensure NSSF Is Available		
Test Objective	Check Service Status of NSSF		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Restart NSSF for registration Systemctl restart coral5gs-nssfd.service **1. NSSF to NRF register:** URL: ***/nnrf-nfm/v1/nf-instances/74e5e806-a020-41ef-b2dd-0f1785063434*** Header: user-agent: NSSF Header: 3gpp-sbi-sender-timestamp: Mon, 11 Nov 2024 11:31:13.239 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **Response from NRF to NSSF** HEADERS[1]: 201 Created **Json body:** **DATA[1], JSON (application/j son)** Object Member: nfInstanceId Member: nfTyp Member: nfStatus Member: nfProfileChangesSupportInd	**Expected Output:** Service: coral5gs-nssfd.service Active: active (running) Service ID: 1b87483a-305b-41e9-b670-2985996f8551 path: /nnrf-nfm/v1/nf-instances/74e5e806-a020-41ef-b2dd-0f1785063434 Value: /nnrf-nfm/v1/nf-instances/74e5e806-a020-41ef-b2dd-0f1785063434 Value: 201 :status: 201 Member: nfType [Path with value: /nfType:NSSF] [Member with value: nfType:NSSF] String value: NSSF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	
Overall Test Result	Pass: □	Fail: □	

4.3.2(g) PCF

Test ID	4.3.2(g) PCF		
Requirement	Ensure PCF Is Available		
Test Objective	Check Service Status of PCF		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Restart pcf for registration Systemctl restart coral5gs-pcfd.service PCF registration with NRF: PCF To NRF: ***PUT /nnrf-nfm/v1/nf-instances/20e3f556-a0be-41ef-ae1a-114b0ba2858c*** Header: user-agent: PCF Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 06:19:52.783 GMT Header: accept: application/json,application/problem+json **Response: From NRF To PCF** HEADERS[1]: 201 Created **DATA[1], JSON (application/json)** Object Member: nfInstanceId Member: nfType Member: nfStatus Member: nfProfileChangesSupportInd **Interface:** **SBI interface reference point N15 Between PCF and AMF** **Communication service API:**	**Expected Output:** Active: active (running) Service ID: 1b87483a-305b-41e9-b670-2985996f8551 value: 201 status:201 Member: nfType [Path with value: /nfType:PCF] [Member with value: nfType:PCF] String value: PCF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	

Test ID	4.3.2(g) PCF		
	HEADERS[1]*POST /npcf-am-policy-control/v1/policies* **Header: user-agent: AMF** Header: accept: application/json,application/problem+json Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 06:49:52.837 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **DATA[1], JSON (application/json)** JavaScript Object Notation: application/json Object Member: request Object Member: notificationUri Member: supi Member: accessType allowedSnssais Member: ueAmbr Object Member: uplink Member: downlink	Member: supi [Path with value: /supi:imsi-001010123456902] [Member with value: supi:imsi-001010123456902] String value: imsi-001010123456902 Key: supi [Path: /supi] Member: accessType [Path with value: /accessType:3GPP_ACCESS] [Member with value: accessType:3GPP_ACCESS] String value: 3GPP_ACCESS Key: accessType [Path: /accessType] Member: uplink [Path with value: /ueAmbr/uplink:1000000 Kbps] [Member with value: uplink:1000000 Kbps] String value: 1000000 Kbps Key: uplink [Path: /ueAmbr/uplink] Member: downlink	

Test ID	4.3.2(g) PCF		
	Between PCF and SMF on interface N7 to show session related parameter 5QI value: **HEADERS[1]** ***POST /npcf-smpolicycontrol/v1/sm-policies*** Header: user-agent: SMF Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 06:49:53.362 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **Response:** **Json body:** **DATA[55], JSON (application/json)** Object Member: sessRules Member: 5qi Member: suppFeat	[Path with value: /ueAmbr/downlink:1000000 Kbps] [Member with value: downlink:1000000 Kbps] String value: 1000000 Kbps Key: downlink [Path: /ueAmbr/downlink] **Number value: 9** **Key: 5qi** Member: uplink [Path with value: /subsSessAmbr/uplink:1000000 Kbps] [Member with value: uplink:1000000 Kbps] String value: 1000000 Kbps Key: uplink [Path: /subsSessAmbr/uplink] Member: downlink [Path with value: /subsSessAmbr/downlink:1000000 Kbps] [Member with value: downlink:1000000 Kbps] String value: 1000000 Kbps Key: downlink [Path: /subsSessAmbr/downlink]	

Test ID	**4.3.2(g) PCF**		
		Supported Features: 4000000 ...0 = TSC: False ..0. = ResShare: False .0.. = 3GPP-PS-Data-Off: False 0... = ADC: False ...0 = UMC: False ..0. = NetLoc: False .0.. = RAN-NAS-Cause: False 0... = ProvAFsignalFlow: False ...0 = PCSCF-Restoration-Enhancement: False ..0. = PRA: False .0.. = RuleVersioning: False 0... = SponsoredConnectivity: False ...0 = RAN-Support-Info: False ..0. = PolicyUpdateWhenUESuspends: False .0.. = AccessTypeCondition: False 0... = MultiIpv6AddrPrefix: False ...0 = SessionRuleErrorHandling: False ..0. = AF_Charging_Identifier: False .0.. = ATSSS: False 0... = PendingTransaction: False ...0 = URLLC: False ..0. = MacAddressRange: False .0.. = WWC: False 0... = QosMonitoring: False ...0 = AuthorizationWithRequiredQoS: False ..0. = EnhancedBackgroundDataTransfer: False .1.. = DN-Authorization: True 0... = PDUSessionRelCause: False	
Overall Test Result	Pass: □	Fail: □	

4.3.2(h) SMF

Test ID	4.3.2 (h) SMF		
Requirement	Ensure SMF Is Available		
Test Objective			**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Restart SMF for registration Systemctl restart coral5gs-smfd.service **SMF registration with NRF:** **SMF To NRF:** **HEADERS[1]:PUT** ***/nnrf-nfm/v1/nf-instances/25565e0a-a0d5-41ef-911b-095b3d943b36*** Header: user-agent: SMF Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 09:04:38.727 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **Response from NRF to SMF** **Json body:** **HEADERS[1]: 201 Created** Object Member: nfInstanceId Member: nfType Member: nfStatus Member: nfProfileChangesSupportInd **Service provide by SMF to PCF over N7 interface** **HEADERS[1] POST /*npcf-smpolicycontrol/v1/sm-policies*** Header: user-agent: SMF Header: 3gpp-sbi-sender-timestamp: Tue,	**Expected Output:** Service: coral5gs-smfd.service Active: active (running) value: 201 :status:201 Member: nfType [Path with value: /nfType:SMF] [Member with value: nfType:SMF] String value: SMF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	

Test ID	**4.3.2 (h) SMF**		
	12 Nov 2024 09:47:00.968 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **Response:** **Json body:** **DATA[55], JSON (application/json)** Object Member: sessRules Member: 5qi Member: suppFeat **Interface between AMF to SMF on N11** **Request from AMF to SMF For Session context after PDU Session Request Message** **POST /nsmf-pdusession/v1/sm-contexts** **Header: user-agent: AMF** Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 09:47:01.073 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **Response from SMF to AMF** /namf-comm/v1/ue-contexts/imsi-001010123456902/n1-n2-messages **DATA[1], JSON (application/json),**PDU session establishment accept (PDU session type IPv4 only allowed), PDUSessionResourceSetupRequestTransfer Non-Access-Stratum 5GS (NAS)PDU	**Number value: 9** **Key: 5qi** ..00 0001 = Qos flow identifier: 1 Session-AMBR for downlink: 3850 Kbps (3850) Session-AMBR for uplink: 1530 Kbps (1530) DNN: internet.	
Overall Test Result	Pass: □	Fail: □	

4.3.2(i) UDM

Test ID	**4.3.2(i)UDM**		
Requirement	Ensure UDM Is Available		
Test Objective	Check Service Status of UDM		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Restart UDM for registration Systemctl restart coral5gs-udmd.service **UDM** **1.UDM registration with NRF:** **1.1UDM To NRF:** **URL:** ***/nnrf-nfm/v1/nf-instances/b60e4de0-a0e4-41ef-8d5f-6f64befd3fc7*** Header: user-agent: UDM Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 10:56:03.915 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **1.2 Response from NRF to UDM** **Stream: HEADERS[1], Stream ID: 1, Length 108, 201 Created** **DATA[1], JSON (application/json)** Object Member: nfInstanceId Member: nfType Member: nfStatus Member: nfProfileChangesSupportInd	**Expected Output:** Active: active (running) Service ID: 1b87483a-305b-41e9-b670-2985996f8551 **value: 201:** **status: 201** Member: nfType [Path with value: /nfType:UDM] [Member with value: nfType:UDM] String value: UDM Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	

Test ID	4.3.2(i)UDM		
	2.Service provided by UDM: **2.1.SBI interface reference point N13: Between AUSF and UDM for authentication related parameters before Authentication request message** **Service : nudm-ueau AUSF TO UDM:** **Stream: HEADERS, Stream ID: 3, Length 75, POST** ***/nudmueau/v1/imsi-001010123456901/auth-events*** Header: user-agent: AUSF Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 11:02:42.393 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **UDM RESPONSES TO AUSF:** **Stream: HEADERS, Stream ID: 3, Length 66, 201 Created** **JSON body:** Object Member: nfInstanceId Member: success Member: timeStamp Member: authType Member: servingNetworkName **2.2.SBI interface reference point N8: Between AMF and UDM for access related parameters after security mode complete** **Service:nudm-uecm**	**Value: 201** **:status:201** Member: success [Path with value: /success:true] [Member with value: success:true] True value Key: success [Path: /success] Member: authType [Path with value: /authType:5G_AKA] [Member with value: authType:5G_AKA] String value: 5G_AKA Key: authType [Path: /authType]	

Test ID	4.3.2(i)UDM		
	AMF to UDM: **Stream: HEADERS, Stream ID: 5, Length 134, PUT** ***/nudm-uecm/v1/imsi-001010123456902/registrations/amf-3gpp-access*** Header: user-agent: AMF Header: 3gpp-sbi-sender-timestamp: Mon, 11 Nov 2024 10:32:09.013 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **UDM responses to AMF:** **Stream: HEADERS, Stream ID: 1, Length 123, 201 Created** **JSON body:** Member: mcc Member: mnc Member: amfId	**Value: 201** **:status:201** Member: mcc [Path with value: /guami/plmnId/mcc:001] [Member with value: mcc:001] String value: 001 Key: mcc [Path: /guami/plmnId/mcc] Member: mnc [Path with value: /guami/plmnId/mnc:01] [Member with value: mnc:01] String value: 01 Key: mnc [Path: /guami/plmnId/mnc] Member: amfId [Path with value: /guami/amfId:020040] [Member with value: amfId:020040] String value: 020040 Key: amfId [Path: /guami/amfId]	
Overall Test Result	Pass: □	Fail: □	

4.3.2(j) UDR

Test ID	**4.3.2(j) UDR**		
Requirement	Ensure UDR Is Available		
Test Objective	Check Service Status of UDR		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Restart UDR for registration Systemctl restart coral5gs-udrd.service **1.UDR registration with NRF** **1.1 UDR To NRF:** **Stream: HEADERS, Stream ID: 1, Length 188, PUT *<nnrf-nfm/v1/nf-instances/5efce888-a1af-41ef-bff2-91ecfa52ba77>*** Header: user-agent: UDR Header: 3gpp-sbi-sender-timestamp: Wed, 13 Nov 2024 11:06:45.677 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **1.2 Response from NRF to UDR** **Stream: HEADERS, Stream ID: 1, Length 107, 201 Created** **JSON body: JavaScript Object Notation: application/jso** Object Member:nfInstanceId Member: nfTyp Member: nfStatus Member: nfProfileChangesSupportInd **2.Service provided by UDR:** **2.1.SBI interface reference point N35:** **Between UDM and UDR for subscription related parameters**	**Expected Output:** Service: coral5gs-udrd.service Active: active (running) Service ID: 1b87483a-305b-41e9-b670-2985996f8551 **value:201** **:status:201** Member: nfType [Path with value: /nfType:UDR] [Member with value: nfType:UDR] String value: UDR Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	

Test ID	4.3.2(j) UDR		
	Stream: HEADERS, Stream ID: 45, Length 102, GET * dr/v1/subscription-data/imsi- 001010123456902/authentication- data/authentication-subscription* Header: user-agent: UDM Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 11:02:42.087 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **UDR responses to UDM: HEADERS[1]: 200 OK** **JSON BODY:** **JavaScript Object Notation: application/json** Object Member:authenticationMethod Member: encPermanentKey Member: sequenceNumber Member: encOpcKey	**Value: 200** **:status: 200** Member: authenticationMethod [Path with value: /authenticationMethod:5G_AKA] [Member with value: authenticationMethod:5G_AKA] String value: 5G_AKA Key: authenticationMethod [Path: /authenticationMethod] Member: encPermanentKey [Path with value: /encPermanentKey:11111111111111111111111111111111] [Member with value: encPermanentKey:11111111111111111111111111111111] String value: 11111111111111111111111111111111 Key: encPermanentKey [Path: /encPermanentKey] Member: sequenceNumber Object	

Test ID	**4.3.2(j) UDR**		
		Member: sqn [Path with value: /sequenceNumber/sqn:000000000841] [Member with value: sqn:000000000841] String value: 000000000841 Key: sqn [Path: /sequenceNumber/sqn] Key: sequenceNumber [Path: /sequenceNumber] Member: encOpcKey [Path with value: /encOpcKey:11111111111111111111111111111111] [Member with value: encOpcKey:11111111111111111111111111111111] String value: 11111111111111111111111111111111 Key: encOpcKey [Path: /encOpcKey]	
Overall Test Result	Pass: □	Fail: □	

4.3.2(k) UPF

Test ID	**4.3.2(k)UPF**		
Requirement	Ensure UPF Is Available		
Test Objective	Check Service Status of UPF		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Restart UPF for registration Systctemctl restart coral5gs-upfd.service **Registration with SMF:** **Request from SMF side** **PFCP Association Setup Request over N4 interface** Packet Forwarding Control Protocol Message Type: PFCP Association Setup Request (5) Node ID : IPv4 address: 127.0.0.4 **Response from UPF side:** **PFCP Association Setup Response over N4** Packet Forwarding Control Protocol Message Type: PFCP Association Setup Response (6) Node ID : IPv4 address: 127.0.0.7 Cause : Request accepted(success) **Service API:** **Session Connection From SMF side to UPF** **PFCP Session Establishment Request on N4** Packet Forwarding Control Protocol Message Type: PFCP	**Expected Output:** Active: active (running) Service ID: 1b87483a-305b-41e9-b670-2985996f8551 IPv4: smf(127.0.0.4) IPv4: upf(127.0.0.7) accepted(success) (1) .... .001 = PDN Type: IPv4 (1)	

	Session Establishment Request (50) PDN Type : IPv4 User ID : APN/DNN : internet **Response from UPF PFCP Session Establishment Response on N4** Packet Forwarding Control Protocol Message Type: PFCP Session Establishment Response (51) Node ID : IPv4 address: 127.0.0.7 Cause : Request accepted(success) F-SEID : SEID: 0x0000000000000fc5, IPv4 127.0.0.7 **From SMF to UPF over N4 interface PFCP Session Modification Request** Message Type: PFCP Session Modification Request (52) SEID: 0x0000000000000fc5 **PFCP Session Modification Response from UPF to SMF over N4 interface** Message Type: PFCP Session Modification Response (53) Cause : Request accepted(success) **PING service: UL packet from UE to DN**	IMSI: 001010123456902 APN/DNN: internet Request accepted(success) (1) SEID: 0x0000000000000fc5 Cause: Request accepted(success) (1)	
Overall Test Result	Pass: □	Fail: □	

4.3.2(m) UE

Test ID	**4.3.2(m)UE**		
Requirement	Check UE Support		
Test Objective	Able to Support UE for data browse and calls		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Interface between AMF to SMF on N11 **Request from AMF to SMF For Session context after PDU Session Request Message** **POST /nsmf-pdusession/v1/sm-contexts** Header: user-agent: AMF Header: 3gpp-sbi-sender-timestamp: Tue, 12 Nov 2024 09:47:01.073 GMT Header: 3gpp-sbi-max-rsp-time: 10000 **Response from SMF to AMF** /namf-comm/v1/ue-contexts/imsi-001010123456902/n1-n2-messages **DATA[1], JSON (application/json),** PDU session establishment accept, PDUSessionResourceSetupRequestTransfer	**Number value: 9** **Key: 5qi** PDU address Element ID: 0x29 Length: 5 .... 0... = SMF's IPv6 link local address (SI6LLA): Absent .... .001 = PDU session type: IPv4 (1) PDU address information: 10.45.0.4**(UE IP)** DNN: internet.	
Overall Test Result	Pass: □	Fail: □	

4.3.2(n) RAN

Test ID	**4.3.2(n) RAN**		
Requirement	Check for Network Availability		
Test Objective	Check Local 5G Network is available		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	UE Test Go to Network Selection Option Select Manual	Coral 5GS should be displayed in network list	
Overall Test Result	Pass: □	Fail: □	

4.3.2(p) NWDAF

Test ID	**4.3.2(p) NWDAF**		
Requirement	MEC platform integration		
Test Objective	Check for MEC service		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ core-network status nwdaf	**Expected Output:** Service: coral5gs-nwdafd.service Active: active (running) Service ID: 1b87483a-305b-41e9-b670-2985996f8551 The service ID in the example provided is `*1b87483a-305b-41e9-b670-2985996f8551*`. Your specific service ID may vary depending on your system or setup.	**Explanation:** • **Service**: Displays the service name of the service for UPF the service name is: coral5gs-nwdafd.service • **Active**: Indicates the status as active (running). • **Service ID**: Shows the specific Service ID 1b87483a-305b-41e9-b670-2985996f8551. **You can find more details by searching for the Service ID within the captured packets.**
Overall Test Result	Pass: □	Fail: □	

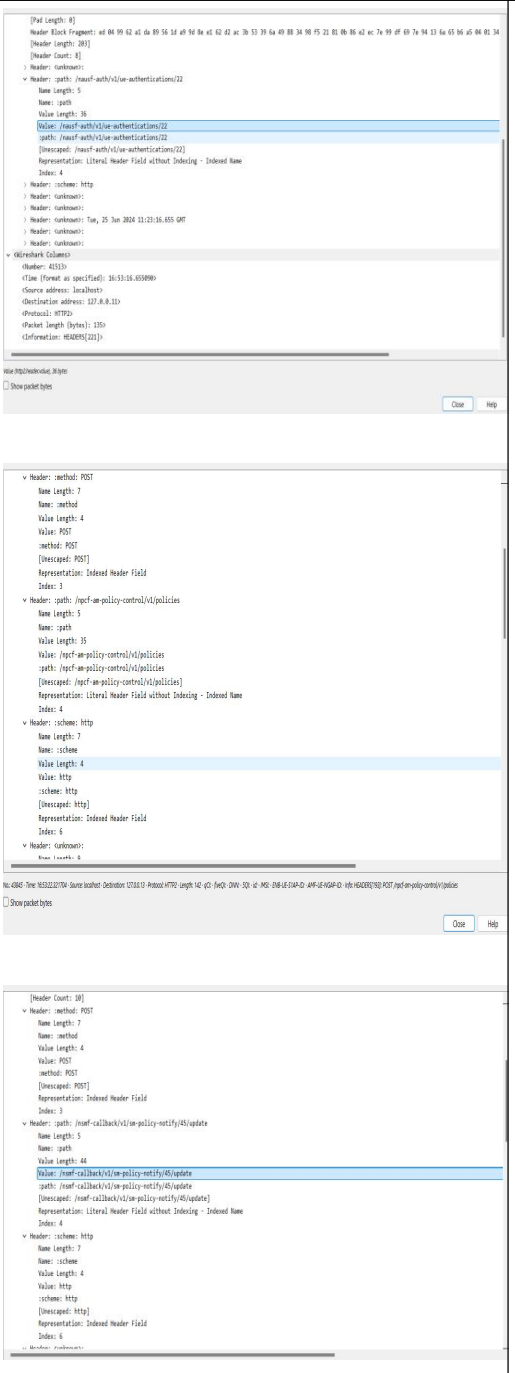
4.3.4 Network Segmentation/Slicing for Customer QoS for Data Connectivity

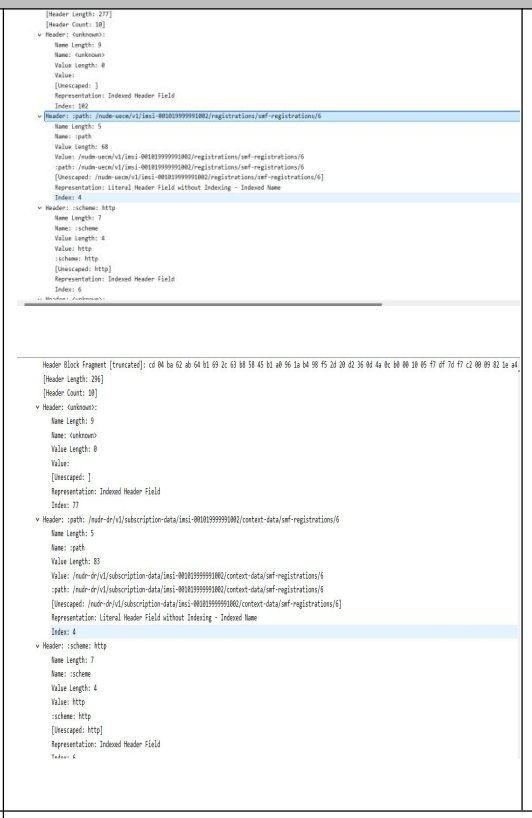
Test ID	**4.3.4 Network Segmentation/Slicing for Customer QoS for Data Connectivity**		
Requirement	Implement a modularized function design in the 5G network architecture, enabling flexible and efficient network slicing. This design should facilitate the independent and scalable deployment of network functions, enhancing adaptability to diverse service requirements and optimizing resource utilization within network slices.		
Test Objective	To check flexible and efficient network slicing		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. **Start Capturing Packets:** Initiate packet capturing to analyse network traffic.	**In packet Initial Context Setup Request:** • Identify the parameter id-Allowed NSSAI to find the s-NSSAI parameter. • Ensure sST: 01 and sd: 00 00 01 values are correctly configured based on the requested network slice configuration.	The steps outlined aim to validate the flexibility and efficiency of network slicing in the 5G architecture through detailed packet analysis. Specifically, by capturing and examining packets, we ensure correct configuration of slice-specific parameters like id-Allowed NSSAI, sST, and sd. This verification process is crucial for optimizing resource allocation within network slices, thereby enhancing overall network performance and adaptability to diverse service needs.
Overall Test Result	Pass: □	Fail: □	

4.3.6 VoNR

Test ID	**4.3.6 VoNR**		
Requirement	Make Voice Call between two mobile phones		
Test Objective	Using Native Dialer make Voice Calls		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ core-network status ims	IMS is listed with status Running UE Test 1. Insert Configured SIM in UE 2. Power ON UE 3. Check For Calling service on top right	
Overall Test Result	Pass: □	Fail: □	

4.3.7 Should support open AP-s - for example any O & M (OSS/BSS integration)

Test ID	**4.3.7 Should support open AP–s - for example any O&M (OSS/BSS integration)**		
Requirement	Open API Support		
Test Objective	Check From WireShark for various endpoints on services		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1) Start Wireshrak on PC 2) Run rpcapd Capture remote data from wireshark		

Test ID	4.3.7 Should support open AP–s - for example any O&M (OSS/BSS integration)		
			
Overall Test Result	Pass: □	Fail: □	

4.3.7 MEC platform integration

Test ID	4.3.7 MEC platform integration,		
Requirement	MEC platform integration		
Test Objective	Check for MEC service		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ core-network status mec	MEC Support Services are listed status Running For Detailed MEC UATs please refer to MEC UAT Document	
Overall Test Result	Pass: □	Fail: □	

4.3.10 uRLLC

Test ID	4.3.10 uRLLC		
Requirement	Support for uRLLC		
Test Objective	Check uRLLC Network Slice		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Open Coral5GS GUI. 2. Select the desired IMSI. 3. Enable different slices for the selected IMSI. 4. Verify	Check for configured slice id in wireshark.	
Overall Test Result	Pass: □	Fail: □	

4.3.11 mMTC

Test ID	**4.3.11 mMTC**		
Requirement	Support for mMTC		
Test Objective	Check mMTC Network Slice		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Open Coral5GS GUI. 2. Select the desired IMSI. 3. Enable different slices for the selected IMSI. 4. Verify	Check for configured slice id in wireshark	
Overall Test Result	Pass: □	Fail: □	

Section 4.4: 5G NR Radio

S.no	Description
4.4.1(a)	Functions for Radio Resource Management: Radio BearerControl, Radio Admission Control, Connection Mobility Control,Dynamic allocation of resources to UEs in both uplink and downlink (scheduling);
4.4.1(c)	Routing of User Plane data towards UPF(s);
4.4.1 (d)	Routing of Control Plane information towards AMF;
4.4.1(e)	Connection setup and release;
4.4.1 (f)	Scheduling and transmission of paging messages;
4.4.1 (g)	Scheduling and transmission of system broadcast information(originated from the AMF or OAM)
4.4.1(h)	Measurement and measurement reporting configuration for mobility and scheduling
4.4.1(i)	Transport level packet marking in the uplink
4.4.1(j)	Session Management
4.4.1(k)	Support of Network Slicing
4.4.1(l)	QoS Flow management and mapping to data radio bearers
4.4.1(n)	Distribution function for NAS messages
4.4.3(a)	The NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF
4.4.3(b)	The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RAN node and the UPF.
4.4.3(c)	NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF.
4.4.3(d)	Further details of NG-U compliance as per 3GPP standards
4.4.4(a)	NG-C provides the following functions
4.4.4(b)	NG interface management
4.4.4(c)	UE context management
4.4.4(e)	Transport of NAS messages
4.4.4(f)	Paging
4.4.4(g)	PDU Session Management
4.4.4(j)	Further details of NG-C compliance as per 3GPP standards
4.4.5(c)	Flow control.
4.4.7(a)	Protocol stack for the user plane, i.e. SDAP, PDCP, RLC andMAC sublayers (terminated in gNB on the network side) should perform the functions as per 3GPP Release 15.
4.4.7(b)	The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15
4.4.7(c)	PDCP, RLC and MAC sublayers (terminated in gNB on thenetwork side) should perform the functions listed in 3GPP Standards
4.4.7(d)	RRC (terminated in gNB on the network side) performs the functions listed in 3GPP Standards.
4.4.7(e)	NAS control protocol (terminated in AMF on the network side) performs the functions listed in 3GPP Standards.for instance:authentication, mobility management, security control

4.4.1(a) Funcition for Radio Resource Management :Radio Bearer Control, Radio Admission Control , Connectiln Mobility Control. Dynamic allocation of resources to UEs in voth uplink and Downlinj(Scheduling)

Test ID	**4.4.1.a Functions for Radio Resource Management: Radio Bearer Control, Radio Admission Control, Connection Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling);**				
Requirement					
Test Objective	To verify gNB supports Radio Resource Management functions: Radio Bearer Control, Radio Admission Control, Connection Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Establish a connection between the UE and gNB. Initiate video streaming to establish radio bearers. Modify QoS parameters for an existing bearer in Coral core and observe the changes. Release an existing radio bearer and verify its termination for Radio Bearer Control function. • Dynamic allocation of resource to UE in both uplink and downlink(scheduling) • Test 5G device from different location with respect to gNB to get variation in RSRP/RSRQ • Measure the throughput using speed test application	1.To verify End to End systems are configured & gNB is radiating. **<u>Testing methodology:</u>** 2.To verify successful bearer establishment, modification in RRC Connection Reconfiguration of Wireshark log . **Steps**: Filternr-rrc/ RRC Reconfiguration 1.Verify SRB0, SRB 1& SRB 2 in RRC Setup and RRC Reconfiguration Message 2.Verify the PDU session establishment procedure for DRB 1 and DRB 2 3.Check the RRC Reconfiguration message in PCAP 7 show the mapping between QFI and DRB Identifier indicates Radio bearer control 4.Intiate flight mode on to initiate PDU session release followed by RRC Connection release.			

	• Check the PCAP logs of gNB for resource allocation	**Result:** SRB0, SRB1, SRB2, DRB1 bearer formed rrcSetup i)Item 2: id-SRBID ProtocolIE-Field id: id-SRBID (64) criticality: reject (0) value SRBID: 0 radioBearerConfig srb-ToAddModList: 1 item Item 0 SRB-ToAddMod srb-Identity: 1 iii)srb-ToAddModList { { srb-Identity 2, iv) drb-ToAddModList cnAssociation sdap-Config : pdu-Session 1, sdap-HeaderDL present, sdap-HeaderUL present, defaultDRB FALSE, mappedQoS-FlowsToAdd 1 drb-Identity 1, **Result:** Verify RRC Radio Beraers			
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)	Verified that gNB supports Radio Resource Management functions: Radio Bearer Control, Radio Admission Control, Connection Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(c) Routing of User Plane Data towards UPF(s);

Test ID	**4.4.1.c Routing of User Plane data towards UPF(s);**				
Requirement	Verify Routing of User Plane data towards UPF(s);				
Test Objective	To verify that gNB supports Routing of User Plane data towards UPF(s)		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Register UE with gNodeB start the data transfer (Ping to 8.8.8.8) in UL and Verify GTP-U information from gNodeB PCAP log • Verify the PDU session Resource setup Request for Tunnel ID. • Verify the packet list to check the data being transferred using the Tunnel ID	**Testing methodology:** 1. UE received data and verified via iperf application in UE. To verify the GTP/UDP packets in gNB via Pcap logs **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] PW: Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark > File > open pcap log > Apply UDP/GTP filters. **Result:** Tunnel establishment via PDU session resource PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 23 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value	Ok Ok		Check the Tunnel ID in PDUSession Resource setup and GTP-U Packets and ensure they are same

		RAN-UE-NGAP-ID: 23 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 1 pDUSessionNAS-PDU: 7e02a59878f3137e00680100552e0109c2110009010006313101 01ff010603f42403f4242905010a2d000522040103060979000601204101010 97b001a8080210a0200000a8106c0a80f0a000d04c0a80f0a001002057825090869 6e7465726e65741201 Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0xa59878f3 Sequence number: 19 Encrypted data s-NSSAI sST: 01 sD: 030609 pDUSessionResourceSetupRequestTransfer: 0000040082000a0c3b9aca00303b9aca00008b000a01f0c0a80f0a0000d2d70086000100008800070001000 0091c00 PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate ProtocolIE-Field id: id-PDUSessionAggregateMaximumBitRate (130) criticality: reject (0)			

		value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1000000000bits/s pDUSessionAggregateMaximumBitRateUL: 1000000000bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80f0a [bit length 32, 1100 0000 1010 1000 0000 1111 0000 1010 decimal value 3232239370] **TransportLayerAddress (IPv4): 192.168.15.10** **gTP-TEID: 0000d2d7**			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports Routing of User Plane data towards UPF(s)				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(d) Routing of Control Plane information towards AMF;

Test ID	**4.4.1(d) Routing of Control Plane information towards AMF;**				
Requirement	Verify Routing of Control Plane information towards AMF;				
Test Objective	To verify that gNB supports Routing of Control Plane information towards AMF.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Configure AMF IP, N2 interface & ports in gNB & register UE with gNB. • Verify using gNodeB PCAP logs for NGAP SETUP Request and Response	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify that NGAP protocol message exchanges in Pcap log between gNB & AMF for UE PDU session, **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] PW: root Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark > File > open pcap log > Apply NGAP filters **Result**: NGAP messages shall updated successfully between gNB & AMF **NGSetupRequest** protocolIEs: 3 items Item 0: id-GlobalRANNodeID ProtocolIE-Field id: id-GlobalRANNodeID (27) criticality: reject (0) value GlobalRANNodeID: globalGNB-ID (0)			Verified that gNB supports Routing of Control Plane information towards AMF via pcap log.

Test ID	**4.4.1(d) Routing of Control Plane information towards AMF;**				
		globalGNB-ID pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) gNB-ID: gNB-ID (0) gNB-ID: 0000000f [bit length 32, 0000 0000 0000 0000 0000 0000 0000 1111 decimal value 15] Item 1: id-SupportedTAList NG Application Protocol **(NGSetupResponse)** NGAP-PDU: successfulOutcome (1) successfulOutcome			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports Routing of Control Plane information towards AMF via pcap log.				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(e) Connection setup and release;

Test ID	**4.4.1(e) Connection setup and release;**				
Requirement	Verify Connection setup and release;				
Test Objective	To verify that gNB supports Connection setup and release		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Run the gNodeB Connect the UE Call and Video streaming should happen Put UE in Airplane mode .This will disconnects the Ue from gNodeB Remove from airplane mode Verify UE context release command & UE context release complete	1.**Testing methodology:** **UEContextReleaseCommand** protocolIEs: 2 items Item 0: id-UE-NGAP-IDs ProtocolIE-Field id: id-UE-NGAP-IDs (114) criticality: reject (0) value UE-NGAP-IDs: uE-NGAP-ID-pair (0) uE-NGAP-ID-pair aMF-UE-NGAP-ID: 6 rAN-UE-NGAP-ID: NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-UEContextRelease (41) criticality: reject (0) value **UEContextReleaseComplete** protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: ignore (1) value AMF-UE-NGAP-ID: 6 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: ignore (1) value RAN-UE-NGAP-ID: 6	Ok Ok Ok		Verified that gNB supports Connection setup and release via QXDM UE log.
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments					

Test ID	**4.4.1(e) Connection setup and release;**
(If Any)	Verified that gNB supports Connection setup and release.
Name & Signature	**NAME OF VERIFIER**

4.4.1(f) Scheduling and transmission of paging messages;

Test ID	**4.4.1(f) Scheduling and transmission of paging messages;**				
Requirement	Verify Scheduling and transmission of paging messages;				
Test Objective	To verify that gNB supports Scheduling and transmission of paging messages		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Register UE to gNobdeB and collect wireshark log and check for paging message	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** **Paging** protocolIEs: 2 items Item 0: id-UEPagingIdentity ProtocolIE-Field id: id-UEPagingIdentity (115) criticality: ignore (1) value UEPagingIdentity: fiveG-S-TMSI (0) fiveG-S-TMSI aMFSetID: 0040 [bit length 10, 6 LSB pad bits, 0000 0000 01.. .... decimal value 1] aMFPointer: 00 [bit length 6, 2 LSB pad bits, 0000 00.. decimal value 0] fiveG-TMSI: 3221227364 (0xc0000764) Item 1: id-TAIListForPaging ProtocolIE-Field id: id-TAIListForPaging (103) criticality: ignore (1) value TAIListForPaging: 1 item Item 0 TAIListForPagingItem tAI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) tAC: 1 (0x000001)	Ok Ok		Verified that gNB supports Scheduling and transmission of paging messages
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments	Verified that gNB supports Scheduling and transmission of paging messages				

Test ID	**4.4.1(f) Scheduling and transmission of paging messages;**
(If Any)	
Name & Signature	**NAME OF VERIFIER**

4.4.1(g) Scheduling and transmission of system broadcast information (originated from the AMF or OAM);

Test ID	**4.4.1(g) Scheduling and transmission of system broadcast information (originated from the AMF or OAM)**				
Requirement	Verify Scheduling and transmission of system broadcast information (originated from the AMF or OAM)				
Test Objective	Verify that gNB supports Scheduling and transmission of system broadcast information		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Turn on Gnb and Register 5G UE Check gnodeB PCAP logs (apply nr-rrc) for MIB and SIB message	1.To verify End to End systems are configured & gNB is radiating. **<u>Testing methodology:</u>** .To verify all the SIB configurations through wireshark log **System Information Block Type 1** SystemInformationBlockType1 Message, Msg Length = 129 SIB Mask in SI = 0x02 Interpreted PDU: value BCCH-DL-SCH-Message ::= { message c1 : systemInformationBlockType1 : { cellSelectionInfo { q-RxLevMin -60, q-RxLevMinSUL -50, q-QualMin -30 }, cellAccessRelatedInfo { plmn-IdentityList { { plmn-IdentityList {	Ok Ok Ok		Verified that gNB supports Scheduling and transmission of system broadcast information

		{
		mcc
		{
		0,
		0,
		1
		},
		mnc
		{
		0,
		1
		}
		}
		},
		trackingAreaCode
		'00000000 00000000
		00000001'B,
		cellIdentity '00000000
		00000000 00000000
		00001111 0001'B,
		cellReservedForOperato
		rUse notReserved
		}
		}
		},
		si-SchedulingInfo
		{
		schedulingInfoList
		{
		{
		si-BroadcastStatus
		broadcasting,
		si-Periodicity rf128,
		sib-MappingInfo
		{
		{
		type sibType2,
		valueTag 0,
		areaScope true
		}
		}
		},
		{
		si-BroadcastStatus
		broadcasting,
		si-Periodicity rf512,
		sib-MappingInfo
		{
		{
		type sibType4,
		valueTag 0,			

		areaScope true
		},
		{
		type sibType5,
		valueTag 0,
		areaScope true
		}
		}
		}
		},			

Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports Scheduling and transmission of system broadcast information (originated from the AMF or OAM).				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(h) Measurment and measurement reporting configuration for mobility and scheduling;

Test ID	**4.4.1(h) Measurement and measurement reporting configuration for mobility and scheduling**				
Requirement	Verify Measurement and measurement reporting configuration formobility and scheduling				
Test Objective	To verify Measurement and measurement reporting configuration for mobility and scheduling		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Apply the filter in Wireshark nr-rrc (NR Radio Resource control) protocol . • Check for RRC reconfiguration for gnb configuring for measurement and measurement report from the UE	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 1 MeasConfig reportConfigToRemoveList: 1 item Item 0: ReportConfigId: 1 reportConfigToAddModList: 1 item Item 0: ReportConfigToAddMod reportConfigId: 2 reportConfig: reportConfigNR (0) reportConfigNR reportType: eventTriggered (1) eventTriggered eventId: eventA3 (2) eventA3 a3-Offset: rsrp (0) rsrp: 1.0dB (2) .... ..0. reportOnLeave: False hysteresis: 0.5dB (1) timeToTrigger: ms1024 (12) 0... .... useAllowedCellList: False rsType: ssb (0) reportInterval: ms640 (3) reportAmount: r1 (0) reportQuantityCell .1.. .... rsrp: True ..0. .... rsrq: False	OK OK OK		Verified Measurement and measurement reporting configuration for mobility and scheduling

Test ID	**4.4.1(h) Measurement and measurement reporting configuration for mobility and scheduling**				
		...0 .... sinr: False maxReportCells: 1 ....0 includeBeamMeasurements: False reportAddNeighMeas: setup (0).			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified Measurement and measurement reporting configuration for mobility and scheduling				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(i) Transport level packet marking in the uplink

Test ID	4.4.1(i) Transport level packet marking in the uplink				
Requirement	Verify Transport level packet marking in the uplink				
Test Objective	To verify that gNB supports Transport level packet marking in the uplink		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and connected with Sngrep IMS node& attach UE. • In wireshark capture apply filters ngap || gtp , • Verify TEID match in the PDUsessionsetuipRequest ad GTP packets	1.To verify End to End systems are configured & gNB is radiating. **<u>Testing methodology:</u>** **PDUSessionResourceSetupRequest** protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 23 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 23 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 1 pDUSessionNAS-PDU: 7e02a59878f3137e00680100552e0109c211000901000631310101ff0106	Ok Ok Ok Ok		Verified that gNB supports Transport level packet marking in the uplink.

		03f42403f4242905010a 2d000522040103060979 000601204101010 97b00 1a8080210a0200000a81 06c0a80f0a000d04c0a8 0f0a0010020578250908 696e7465726e65741201 Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0xa59878f3 Sequence number: 19 Encrypted data s-NSSAI sST: 01 sD: 030609 UPTransportLayerInfor mation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80f0a [bit length 32, 1100 0000 1010 1000 0000 1111 0000 1010 decimal value 3232239370] TransportLayerAddress (IPv4): 192.168.15.10 **gTP-TEID**: **0x00009f71**. Internet Protocol Version 4, Src: 192.168.15.15, Dst: 192.168.15.10 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-			

		ECT) 0000 00.. = **Differentiated Services Codepoint:** Default (0) .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) **GPRS Tunneling Protocol** Flags: 0x34 001. .... = Version: GTP release 99 version (1) ...1 .... = Protocol type: GTP (1) .... 0... = Reserved: 0 .... .1.. = Is Next Extension Header present?: Yes .... ..0. = Is Sequence Number present?: No ....0 = Is N-PDU number present?: No Message Type: T-PDU (0xff) Length: 72 **TEID: 0x00009f71**			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports Transport level packet marking in the uplink.				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(j) Session Management;

Test ID	**4.4.1(j) Session Management**				
Requirement	Verify Session Management				
Test Objective	To verify that gNB supports Session Management		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Register the UE with NGC. • In wireshark log filter out for NGAP message • Verify PDUsession setup request and PDU session response message alternatively ,check for PDU session Establishment Request and PDU session Establishment Accept message in wireshark log	1.To verify End to End systems are configured & gNB is radiating. Testing methodology: From gNodeB PCAP logs: Verify PDU session setup request and PDU session response message PDUSessionResourceSetupRequest protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 23 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 23 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 2 pDUSessionNAS-PDU: 7e02766ff46a147e0068010059 2e020ac211000901000631310	Ok Ok Ok		Verified that gNB supports Session Management

Test ID	**4.4.1(j) Session Management**				
		101ff0106010f0a0105fa59322 905010a2e0005220401030609 790006012041010105 7b00218 080210a0200000a8106c0a80f0 a000d04c0a80f0a000c04c0a80 f0a0010020578250403696d73 1202 Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0x766ff46a Sequence number: 20 Encrypted data s-NSSAI sST: 01 sD: 030609 NG Application Protocol (PDUSessionResourceSetupResponse) NGAP-PDU: successfulOutcome (1) successfulOutcome			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports Session Management				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(k) Support of Network Slicing;

Test ID	**4.4.1(k) Support of Network Slicing**				
Requirement	Verify Support of Network Slicing				
Test Objective	To verify that gNB supports Network Slicing		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Configure Network slicing parameters in gnb_config.xml of gNB. • Apply ngap filter in wireshark log and verify the network slice support in NGAP setup response • Alternatively check the 5G logs to check the network slice is correctly allocated	1.To verify End to End systems are configured & gNB is radiating. **<u>Testing methodology:</u>** **NG Application Protocol** (NGSetupResponse) NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-NGSetup (21) criticality: reject (0) value NGSetupResponse sliceSupportList: 4 items Item 0: SliceSupportItem sNSSAI sST: 01 Item 1: SliceSupportItem s-NSSAI sST: 02 Item 2 : SliceSupportItem sNSSAI sST: 03 Item 3: SliceSupportItem sNSSAI sST: 01 sD: 030609			Verified configured Slice value in NG setup response & PDU session establishment accept Slice (NSSAI): SST: X, SD: XXX
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified configured Slice value in EMS Slice (NSSAI): SST: X, SD: XXX				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(l) QoS flow management and mapping to data radio bearers;

Test ID	**4.4.1(l) QoS Flow management and mapping to data radio bearers**				
Requirement	Verify QoS Flow management and mapping to data radio bearers				
Test Objective	Verified that gNB supports QoS Flow management and mapping to data radio bearers		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • In the Wireshark log check the following: • Apply ngap filter and check PDUsessionResourceSetuprequest • Apply the filter for nr-rrc message and check for RRC reconfiguration during Registration Accept • In the RRC Reconfiguration message check the QFI/5QI That was created during PDUsessionResourceSetuprequest is correctly assigned a Data Radio Bearer.	**PDU Session Resource setup Request** for Radio bearer control.gnb/core network assign QFI:1 for internet default bearer with QFI value of 9 (**PDUSessionResourceSetup)** NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 2 Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0x766ff46a Sequence number: 20	Ok Ok		Verified that gNB supports QoS Flow management and mapping to data radio bearers.

Test ID	4.4.1(l) QoS Flow management and mapping to data radio bearers				
		Encrypted data s-NSSAI sST: 01 sD: 030609 value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 3850000bits/s pDUSessionAggregateMaximumBitRateUL: 1530000bits/s QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem qosFlowIdentifier: 1 qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) nonDynamic5Q **fiveQI: 9**			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports QoS Flow management and mapping to data radio bearers.				
Name & Signature	**NAME OF VERIFIER**				

4.4.1(n) Distribution function for NAS message ;

Test ID	**4.4.1(n) Distribution function for NAS messages**				
Requirement	Verify Distribution function for NAS messages				
Test Objective	To verify that gNB support Distribution function for NAS messages		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• gNodeB and AMF are powerd on and operational • UE Registered and within coverage of the gnodeB • intiate the NAS message from the UE(e.g .,Registartion Request) by powering on UE with right configuration to register with 5G network • gnodeB receive the NAS message • gNodeB forward the NAS message to the appropriate AMF • AMF process the Received NAS message • AMF send a response NAS message back to the gNodeB	In wireshark filter ngap and then check Intial Ue message Registration Request Downlink NAS Transport Uplink NAS transport Authentication Request Authentication Response Registration Accept	Ok		Verified that gNB supports Distribution function for NAS
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports Distribution function for NAS.				
Name & Signature	**NAME OF VERIFIER**				

4.4.3(a) Distribution function for NAS message ;

Test ID	**4.4.3(a) The NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF**				
Requirement	Verify The NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.				
Test Objective	To verify that NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Run iperf –c 10.45.0.23 –u –i1 –b100M –t 60 from NGC (client) for DL.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.UE received DL data and verified via iperf application in UE. To verify GTP/UDP packets is exchanged between gNB & UPF via Pcap logs by the existence of NG-U interface. **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply UDP/GTP filters. **Result:** UE shall successfully receive the DL data.	Ok Ok		Verified that NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.				
Name & Signature	**NAME OF VERIFIER**				

4.4.3(b) The transport network layer is built on IP Transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RANnode and the UPF ;

Test ID	**4.4.3(b) The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RAN node and the UPF.**				
Requirement	Verify Distribution function for NAS messages				
Test Objective	To verify that gNB support Distribution function for NAS messages		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• gNodeB and AMF are powerd on and operational • UE Registered and within coverage of the gnodeB • intiate the NAS message from the UE(e.g .,Registartion Request) by powering on UE with right configuration to register with 5G network • gnodeB receive the NAS message • gNodeB forward the NAS message to the appropriate AMF • AMF process the Received NAS message • AMF send a response NAS message back to the gNodeB	In wireshark filter ngap and then check Intial Ue message Registration Request Downlink NAS Transport Uplink NAS transport Authentication Request Authentication Response Registration Accept	Ok		Verified that gNB supports Distribution function for NAS
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports Distribution function for NAS.				
Name & Signature	**NAME OF VERIFIER**				

4.4.3(c) NG-U Provide non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF ;

Test ID	**4.4.3(c):NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF.**				
Requirement	Verify NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF				
Test Objective	Verified that NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• To verify End to End systems are configured & gNB is radiating and attach UE with gNB. • To use iperf tool to verify the DL/UL packets transaction between UE and 5G NGC. **Downlink Test:** **On the UE side:** Open the iperf application in UE, Run iperf –s –u –i1 **On the NGC side:** Open the terminal in NGC, Run iperf –c [Ue IP] –u –i1 –b200M –t 60 **Uplink Test:** **On the UE side:** Open the iperf application in UE, Run iperf –c [Ue IP] –u –i1 –b200M –t 60 **On the NGC side:** Open the terminal in NGC, Run iperf –s –u –i1 • Configure Measurement events & report configurations in gnb_config.xml of gNB and perform S1 HO by moving away the UE from Source gNB to Target gNB.	1.End to End systems to be configured with valid network parameters and the gNB is brought up. **<u>Testing methodology:</u>** 2.To verify that user-plane traffic on the NG-U interface is encapsulated with GTP-U headers & the traffic conforms to the 3GPP standard for GTP-U encapsulation in pcap log. **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply UDP/GTP filters **Result:** NG-U traffic shall be successful 3. To verify that NGAP HO is successful in pcap log & packets are routed properly from Source gNB to Target gNB using NG-U, **Steps:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply NGAP filter **Result**: NGAP HO handover shall be	Ok OK		Verified that gNB supports NG-U compliance as per 3GPP standards

Test ID	**4.4.3(c):NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF.**				
		successful.	Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports NG-U compliance as per 3GPP standards.				
Name & Signature	**NAME OF VERIFIER**				

4.4.3(d) Futher details of NG-U compliances as per 3GPP standards ;

Test ID	**4.4.3(d): Further details of NG-U compliance as per 3GPP standards**				
Requirement	Verify Further details of NG-U compliance as per 3GPP standards				
Test Objective	To verify that gNB supports NG-U compliance as per 3GPP standards		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• To verify End to End systems are configured & gNB is radiating and attach UE with gNB. • To use iperf tool to verify the DL/UL packets transaction between UE and 5G NGC. **Downlink Test:** **On the UE side:** Open the iperf application in UE, Run iperf –s –u –i1 **On the NGC side:** Open the terminal in NGC, Run iperf –c [Ue IP] –u –i1 –b200M –t 60 **Uplink Test:** **On the UE side:** Open the iperf application in UE, Run iperf –c [Ue IP] –u –i1 –b200M –t 60 **On the NGC side:** Open the terminal in NGC, Run iperf –s –u –i1 • Configure Measurement events & report configurations in gnb_config.xml of gNB and perform S1 HO by moving away the UE from Source gNB to Target gNB.	1.End to End systems to be configured with valid network parameters and the gNB is brought up. **<u>Testing methodology:</u>** 2.To verify that user-plane traffic on the NG-U interface is encapsulated with GTP-U headers & the traffic conforms to the 3GPP standard for GTP-U encapsulation in pcap log. **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply UDP/GTP filters **Result:** NG-U traffic shall be successful 3. To verify that NGAP HO is successful in pcap log & packets are routed properly from Source gNB to Target gNB using NG-U, **Steps:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply NGAP filter	Ok OK		Verified that gNB supports NG-U compliance as per 3GPP standards

Test ID	**4.4.3(d): Further details of NG-U compliance as per 3GPP standards**				
		Result: NGAP HO handover shall be successful.	Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RAN node and the UPF.				
Name & Signature	**NAME OF VERIFIER**				

4.4.4(a) NG-C provides the following funcition

Test ID	**4.4.4 (a) NG-C provides the following functions**				
Requirement	Verify NG-C provides the following functions				
Test Objective	To verify that gNB supports NG-C functions		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Initiate a UE registration with gNB & deregister the UE from the gNB.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify that NG interface management, UE context management, Transport of NAS messages, PDU Session establishment in Wireshark log. **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply NGAP/NAS filter **Result:** The UE shall be send successful pdu session establishment accept message.	Ok Ok		Verified that gNB supports NG interface management, UE context management, Transport of NAS messages, PDU Session establishment.
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)	Verified that gNB supports NG interface management, UE context management, Transport of NAS messages, PDU Session establishment.				
Name & Signature	**NAME OF VERIFIER**				

4.4.4(b) NG interface management

Test ID	**4.4.4.b NG interface management**				
Requirement	Verify NG interface management				
Test Objective	To verify that gNB supports NG interface management		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Initiate UE registration with gNB. • Configure Measurement events & report configurations in gnb_config.xml of • To use iperf tool to verify the latency between UE and 5G NGC. **Downlink Test:** **On the UE side:** Open the iperf application in UE, Run iperf –s –u –i1 **On the NGC side:** Open the terminal in NGC, Run iperf –c [Ue IP] –u –i1 –b200M –t 60	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify that NG-C interface handles UE registration, authentication and NAS signalling in Wireshark log. **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply NGAP/NAS filter **Result:** UE shall successfully registered the with the NGC To verify that NG-U interface handles data transaction successfully between UE and NGC. **Steps:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply UDP filter **Result:** Successful data transmission between UE	Ok Ok Ok		Verified that gNB supports NG interface management

		and NGC through NG-U interface.	Ok		
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports NG interface management.				
Name & Signature	**NAME OF VERIFIER**				

4.4.4(c) UE context management

Test ID	4.4.4 (c) UE context management			
Requirement	Verify UE context management			
Test Objective	To verify that gNB supports UE context management		Result	Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up and attach UE with gNB. • Initiate UE registration with gNB. • Configure Measurement events & report configurations in gnb_config.xml of gNB.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify that UE registration procedure is successful through UE context creation between gNB & AMF log. Steps: Filter→NR5G→NAS→Registration accept **Result:** UE shall be successfully register with gNB 3.To verify that UE context is transferred to target gNB & handover is successful in Wireshark log. **Steps:** To Login gNB via mobaxtrem, Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark app in laptop. Open Wireshark → File → open pcap log → Apply NGAP/NAS filter **Result**: Handover shall be successful between the gNBs	Ok Ok Ok	
Overall Test Result	Pass: □	Fail: □		

4.4.4(e) Transport of NAS message

Test ID	4.4.4 (e)Transport of NAS messages				
Requirement	Verify Transport of NAS messages.				
Test Objective	To verify that gNB supports Transport of NAS messages		Result		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Register the UE with NGC from flight mode.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify that NAS transport messages between UE&AMF via gNB. To verify it via Wireshark log. **Result:** UE shall be successfully update the NAS message's between UE and AMF	Ok Ok		Verified that gNB supports Transport of NAS messages
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports Transport of NAS messages.				
Name & Signature	**NAME OF VERIFIER**				

4.4.4(f) Paging

Test ID	**4.4.4 (f) Paging.**				
Requirement	Paging;				
Test Objective	To verify Paging		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Register the UE with NGC from flight mode. • Keep the UE is in idle state & initiate MT call to the UE.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** 2.To verify that UE registration procedure is successful through UE context creation between gNB & AMF **Result:** 1.To verify the paging message initiated from NGC to gNB to UE are successful in Wireshark log . **Steps:** Open mobaxtrem in laptop, Type, root@ [gNB IP] Run, tcpdump -i [Ethernet/optical interface of gNB] -w filename. pcap **Validation:** Open Wireshark → File → open pcap log → Apply NGAP **Result**: Paging shall be successful between UE & gNB	OK OK OK		Verified Paging.
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified the paging message.				
Name & Signature	**NAME OF VERIFIER**				

4.4.4(g) PDU Session management

Test ID	**4.4.4 (g) PDU Session Management**				
Requirement	Verify PDU Session Management.				
Test Objective	To verify that gNB supports PDU Session Management		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up &. • Register the UE with NGC and Sngrep IMS node. • Perform VoNR call from UE. • Deregister the UE from the NGC.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** To verify that PDU session in RRC connection Reconfiguration in PDU session establishment request/accept in pcap log. To verify that PDU session modification command/complete in The UE shall successfully update the pdu session modification message in Wireshark log. The UE shall successfully update the pdu session release request/command message wireshark log	Ok Ok Ok Ok		Verified that gNB supports PDU Session Management functions
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports PDU Session Management functions				
Name & Signature	**NAME OF VERIFIER**				

4.4.4(j) Further details of NG-C compliance as per 3GPP standards

Test ID	**4.4.4.j)Further details of NG-C compliance as per 3GPP standards**				
Requirement	Verify Further details of NG-C compliance as per3GPP standards.				
Test Objective	To verify that gNB supports NG-C compliance as per 3GPP standards.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Initiate UE registration with gNB.	1.To verify End to End systems are configured & gNB is radiating. **Testing methodology:** To verify that NG-C interface handles UE registration, authentication and NAS signalling in wireshark log.	Ok Ok Ok		Verified that gNB supports NG-C compliance as per3GPP standards
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RAN node and the UPF.				
Name & Signature	**NAME OF VERIFIER**				

4.4.5(c) Flow control.

Test ID	**4.4.5.c Flow control.**				
Requirement	Verify Flow control.				
Test Objective	To verify flow control		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	• End to End systems to be configured with valid network parameters and the gNB is brought up. • Attach UE with valid SIM to NGC for Authentication and security control functions.	1.To verify End to End systems are configured & gNB is radiating. 2.To verify authentication request & authentication response message exchanges between UE & AMF in Pcap log. Steps: Open Wireshark > File > open pcap log > Apply nas-5gs filter to verify max no. of PDU session Result: UE shall successfully registered with the NGC after the authentication request and response. 3.To verify security mode command & security mode complete message exchanges between UE & AMF in Pcap log. Steps: Open Wireshark > File > open pcap log > Apply nas-5gs filter to verify max no. of PDU session Result: UE shall successfully registered with the NGC after the security mode complete	OK OK		Verified the flow control
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)	Verified the flow control				
Name & Signature	**NAME OF VERIFIER**				

4.4.7(a) Protocol stack for the user plane, i.e. SDAP, PDCP, RLC andMAC sublayers (terminated in gNB on the network side) should perform the functions as per 3GPP Release 15.

Test ID	**4.4.7.a Protocol stack for the user plane, i.e. SDAP, PDCP, RLC andMAC sublayers (terminated in gNB on the network side) should perform the functions as per 3GPP Release 15.**				
Requirement	Verify Protocol stack for the user plane, i.e. SDAP, PDCP, RLC and MAC sublayers (terminated in gNB on the network side) should perform the functions as per 3GPP Release 15.				
Test Objective	All 5G Radio protocol should be supported while establishing a connection and data transfer		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	

	• End to End systems to be configured with valid network parameters and the gNB is brought up with coral core.
	• power on the 5G UE and ensure that it successfully registers with 5G gNodeB/core.
	• Apply the filter for nr-rrc in the pCAP log and check the RRC Reconfiguration message the reconfigures SDAP, PDCP,RLC and MAC sublayer
		Wireshark log:
		
		rrcReconfiguration :
		{
		rrc-TransactionIdentifier 1,
		criticalExtensions rrcReconfiguration :
		{
		radioBearerConfig
		{
		srb-ToAddModList
		{
		{ srb-Identity 2, pdcp-Config
		{ t-Reordering ms40
		}
		}
		},
		drb-ToAddModList
		{
		{
		cnAssociation **sdap-Config :**
		
		{ pdu-Session 1, sdap-HeaderDL present,
		sdap-HeaderUL present,
		defaultDRB FALSE,
		mappedQoS-FlowsToAdd
		
		{ 1
		} },
			OK
			
			OK
			
			OK
					Verified Protocol stack for the user plane, i.e. SDAP, PDCP, RLC and MAC sublayers should perform the functions as per 3GPP Release 15.

		drb-Identity 1, **pdcp-Config** { drb { discardTime r infinity, pdcp-SN-SizeUL len18bits, pdcp-SN-SizeDL len18bits, headerCompression notUsed : NULL, statusReportRequired true }, t-Reordering ms240, cipheringDisabled true logicalChannelIdentity 2, servedRadioBearer srb- Identity : 2, **rlc-Config am** : { ul-AM- RLC { sn- FieldLength size12, t-PollRetransmit ms45, pollPDU p4, pollByte infinity, maxRetxThreshold t8 }, dl-AM-RLC { sn- FieldLength size12, t-Reassembly ms40, t-StatusProhibit ms80 } }, **mac-** **LogicalChannelConfig** { ul- SpecificParameters { priority 1, prioritisedBitRate infinity, bucketSizeDuration ms150, logicalChannelGroup 0, schedulingRequestID 0, logicalChannelSR-Mask FALSE, logicalChannelSR- DelayTimerApplied FALSE }	OK OK		

		} }, { logicalChannelIdentity 4, servedRadioBearer drb-Identity : 1, rlc-Config am : { ul-AM-RLC { sn-FieldLength size18, t-PollRetransmit ms80, pollPDU p64, pollByte kB100, maxRetxThreshold t8 }, dl-AM-RLC { sn-FieldLength size18, t-Reassembly ms80, t-StatusProhibit ms10 } } **mac-LogicalChannelConfig** { ul-SpecificParameters { priority 4, prioritisedBitRate infinity, bucketSizeDuration ms150, logicalChannelGroup 2, schedulingRequestID 0, logicalChannelSR-Mask FALSE, logicalChannelSR-DelayTimerApplied FALSE } } } }, **mac-CellGroupConfig** { drx-Config setup : { drx-onDurationTimer			

		milliSeconds : ms10, drx-InactivityTimer ms40, drx-HARQ-RTT-TimerDL 56, drx-HARQ-RTT-TimerUL 56, drx-RetransmissionTimerDL sl16, drx-RetransmissionTimerUL sl16, drx-LongCycleStartOffset ms160 : 26, drx-SlotOffset 1 }, skipUplinkTxDynamic FALSE, }			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified Protocol stack for the user plane, i.e. SDAP, PDCP, RLC and MAC sublayers (terminated in gNB on the network side) should perform the functions as per 3GPP Release 15.				
Name & Signature	**NAME OF VERIFIER**				

4.4.7(b) The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15

Test ID	**4.4.7.b The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15**				
Requirement	Verify The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15				
Test Objective	To Verify The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	As updated in 4.47.a				
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)	Verified The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15				
Name & Signature	**NAME OF VERIFIER**				

4.4.7(c) PDCP, RLC and MAC sublayers (terminated in gNB on thenetwork side) should perform the functions listed in 3GPP Standards

<table>
<tr><td>Test ID</td><td colspan="4">4.4.7.c PDCP, RLC and MAC sublayers (terminated in gNB on thenetwork side) should perform the functions listed in 3GPP Standards</td></tr>
<tr><td>Requirement</td><td colspan="4">Verify PDCP, RLC and MAC sublayers (terminated in gNB on thenetwork side) should perform the functions listed in 3GPP Standards</td></tr>
<tr><td>Test Objective</td><td colspan="2">To Verify PDCP, RLC and MAC sublayers functionality</td><td colspan="2">Result</td><td rowspan="2">Remarks</td></tr>
<tr><td rowspan="2">Test Description</td><td>Set Steps</td><td>Acceptance Criteria</td><td>OK</td><td>NOK</td></tr>
<tr><td>As updated in 4.47.a</td><td></td><td>Ok</td><td></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass: □</td><td colspan="3">Fail: □</td></tr>
<tr><td>Remarks / Comments (If Any)</td><td colspan="4">Verified PDCP, RLC and MAC sublayers (terminated in gNB on the network side) should perform the functions listed in 3GPP Standards</td></tr>
<tr><td rowspan="2">Name & Signature</td><td colspan="4">NAME OF VERIFIER</td></tr>
<tr><td colspan="4"></td></tr>
</table>

4.4.7(d) RRC (terminated in gNB on the network side) performs the functions listed in 3GPP Standards.

Test ID	**4.4.7.d RRC (terminated in gNB on the network side) performs the functions listed in 3GPP Standards.**				
Requirement	Verify RRC Performs the functions listed in 3GPP standards.				
Test Objective	To verify the RRC performs the functions		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Apply the filter nr-rrc in the wireshark log and review the contents of RRC Setup and RRC Reconfiguration for establishing RRC connection and data radio bearer.	NR Radio Resource Control (RRC) protocol DL-CCCH-Message message: c1 (0) c1: rrcSetup (1) rrcSetup rrc-TransactionIdentifier: 0 criticalExtensions: rrcSetup (0) rrcSetup radioBearerConfig srb-ToAddModList: 1 item Item 0 SRB-ToAddMod srb-Identity: 1 pdcp-Config t-Reordering: ms40 (10) masterCellGroup […]: 5c00b001100aec841061e a007c0184a83cd20106b0 c96606540247fffffffffe6 000022b0dc31080009c45 b4810000c820000c0214c a01ac04380c800266aa2b 28f8002081840a1838812 2858c1a3879022489942a 58b983268d9c3a78fd3a1 448d2254c9d40a2900440 050 CellGroupConfig cellGroupId: 0 rlc-BearerToAddModList: 1 item Item 0 RLC-BearerConfig logicalChannelIdentity: 1	OK		

		servedRadioBearer: srb-Identity (0) srb-Identity: 1 **RRC Reconfiguration :** : id-DRBs-Setup-List ProtocolIE-Field id: id-DRBs-Setup-List (27) criticality: ignore (1) value DRBs-Setup-List: 1 item Item 0: id-DRBs-Setup-Item ProtocolIE-SingleContainer id: id-DRBs-Setup-Item (26) criticality: ignore (1) value DRBs-Setup-Item dRBID: 1 dLUPTNLInformation-ToBeSetup-List: 1 item Item 0 DLUPTNLInformation-ToBeSetup-Item dLUPTNLInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: 00000000 [bit length 32, 0000 0000 0000 0000 0000 0000 0000 0000 decimal value 0] IPv4 transportLayerAddress: 0.0.0.0 **gTP-TEID: 00000000**			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified RRC functionalities.				
Name & Signature	**NAME OF VERIFIER**				

4.4.7(e) NAS control protocol (terminated in AMF on the network side) performs the functions listed in 3GPP Standards.for instance:authentication, mobility management, security control

Test ID	**4.4.7.e NAS control protocol (terminated in AMF on the network side) performs the functions listed in 3GPP Standards.for instance:authentication, mobility management, security control**				
Requirement					
Test Objective	To verify that gNB supports NAS protocol functions authentication, mobility management, security control		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Run the tcpdump command to collect PCAP sudo tcpdump -i any -w filename.pcap RUN the setup with default config 1. gNB and AMF are powered on and operational. 2. UE is registered and attached to the gNB. Once setup Up then connect the UE. Observe the Nas Control protocol messages which do functions like Registration, authentication,mobility management, security control.	1.In wireshark capture apply filters ‘’nas-5gs NR RRC/NAS-5GS/NAS-ULRRCMessageTransfer, RRC Setup Complete, Registration request, Registration request. NGAP/NAS-DownlinkNASTransport, Identity request NR RRC/NAS-5GS ULRRCMessageTransfer, UL Information Transfer, Identity response. NGAP/NAS-SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request. NGAP/NAS-UplinkNASTransport, Authentication response. NGAP/NAS-DownlinkNASTransport, Security mode command. NR RRC/NAS-5GS/NAS-ULRRCMessageTransfe			Verified that gNB supports NAS protocol functions authentication, mobility management, security control

		r, UL Information Transfer, Security mode complete, Registration request. NGAP/NAS-InitialContextSetupRequest,Registration accept NR RRC/NAS-5GS DLRRCMessageTransfer, DL Information Transfer, Registration accept NGAP/NAS-UplinkNASTransport,Registration complet			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)	Verified that gNB supports NAS protocol functions authentication, mobility management, security control				
Name & Signature	**NAME OF VERIFIER**				

Section 4.5 Multi-access Edge Computing framework

S.no	Description
4.5	Check Virtualisation Support
4.5	Verify KVM Installation
4.5	Verify Dockers Installation
4.5	Check Mec Nodes
4.5	Check Mec Cloud status
4.5	Check Mec Edge Status
4.5	Access the Mec Application
4.5	Check Resource allocation
4.5	Validate Network Configuration
4.5	Validate Storage
4.5	Deploy & Validate

4.5 Check Virtualisation Support

Test ID	**4.5.1 Check Virtualisation Support**		
Requirement	The MEC host shall support virtualization technology to run MEC applications on virtual machines		
Test Objective	Ensure the CPU supports virtualization		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	Run command
	$ mec status cpu-support
		command returns a value greater than 0, e.g., 4
		`root@cloudcore:~# mec status cpu-support`
		`Fetching CPU support information...`
		`Architecture: x86_64`
		`CPU op-mode(s): 32-bit, 64-bit`
		`Byte Order: Little Endian`
		`Address sizes: 40 bits physical, 48 bits virtual`
		`CPU(s): 2`	

Overall Test Result	Pass: □	Fail: □	

4.5 Verify KVM Installation

Test ID	**4.5.1 Verify KVM Installation**		
Requirement	The MEC host shall have KVM installed to provide the virtualization infrastructure for running MEC applications.		
Test Objective	Ensure KVM is installed and running		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	Run command
	$ mec status kvm
		Following is displayed on screen
		kvm support version : 1.01, status enabled and running
		`● libvirtd.service - Virtualization daemon`
		`Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; preset: enabled`
		`Active: active (running) since Fri 2024-07-26 09:55:47 UTC; 1min 52s ago`
		`TriggeredBy: ● libvirtd-admin.socket`
		`● libvirtd-ro.socket`
		`● libvirtd.socket`
		`Docs: man:libvirtd(8)`
		`https://libvirt.org`
		`Main PID: 592 (libvirtd)`	

Overall Test Result	Pass: □	Fail: □	

4.5 Verify Dockers Installation

Test ID	**4.5.1 Verify Dockers Installation**	
Requirement	The MEC host shall have Dockers installed to run containerized MEC applications.	
Test Objective	Ensure Dockers is installed and running for container virtualization.	**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**

	Run command
	$ mec status docker
		Following is displayed on screen
		docker status enabled and running
		`root@cloudcore:~# mec status docker`
		`Checking Docker status...`
		`● docker.service - Docker Application Container Engine`
		`Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)`
		`Active: active (running) since Tue 2024-07-23 09:54:06 IST; 3 days ago`
		`Docs: https://docs.docker.com`
		`Main PID: 612 (dockerd)`

Overall Test Result	Pass: □	Fail: □

4.5 Check Mec Nodes

Test ID	**4.5 Check Mec Nodes**	
Requirement	The MEC system shall use Kubernetes to orchestrate MEC applications.	
Test Objective	Ensure edge nodes are registered.	**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**

	Run command
	$ mec status nodes
		nodes are listed with status Ready
		Along with additional information
		• NAME
		• STATUS
		• ROLES
		• AGE
		• VERSION
		`NAME STATUS ROLES AGE VERSION`
		`cloudcore Ready control-plane 42h v1.28.12`
		`coraloptiplex790 Ready agent,edge 26h v1.28.6-kubeedge-v1.17.0`
		`coraloptiplex7901 Ready agent,edge 24h v1.28.6-kubeedge-v1.17.0`
		`edgecore Ready agent,edge 41h v1.28.6-kubeedge-v1.17.0`

Overall Test Result	Pass: □	Fail: □

4.5 Check Mec Cloud status

Test ID	**4.5 Check Mec Cloud status**		
Requirement	The MEC management system shall include for managing edge nodes.		
Test Objective	Ensure Management System is running.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	Run command
	$ mec status central-core
	$mec status cloud-core
		central-core is listed with status Running
		`root@cloudcore:~# mec status cloud-core`
		`NAME NAME READY STATUS RESTARTS AGE`
		`task-cloudcore-69d64c8b78-dkkcz 1/1 Running 0 43h`	

Overall Test Result	Pass: □	Fail: □	

4.5.5 Deploy Sample Mec Application

<table>
<tr><td>Test ID</td><td colspan="3">4.5.5 Deploy Sample Mec Application</td></tr>
<tr><td>Requirement</td><td colspan="3">The MEC host shall run MEC applications on the virtualization infrastructure</td></tr>
<tr><td>Test Objective</td><td colspan="2">Verify that the MEC host can run containerized applications.</td><td rowspan="2">Remarks</td></tr>
<tr><td rowspan="2">Test Description</td><td>Set Steps</td><td>Acceptance Criteria</td></tr>
<tr><td>Run command
$ mec deploy application.yaml

$ mec status app mec-application</td><td>mec-application is listed with status Running

and other information:
• ip address
• age</td><td>
<pre>
apiVersion: apps/v1
kind: Deployment
metadata:
  name: myapp-vr-app-deployment
  labels:
    app: myapp
spec:
  replicas: 1
  selector:
    matchLabels:
      app: myapp
  template:
    metadata:
      labels:
        app: myapp
    spec:
      hostNetwork: true
      nodeSelector:
        role: cloudcore
      containers:
      - name: myapp-vr-app-deployment
        image: localhost:5000/myapp-vr-apache:v1
        imagePullPolicy: IfNotPresent
        command: ["/bin/sh", "-c"]
        args:
          - apachectl -D FOREGROUND;
        ports:
        - containerPort: 80
</pre>
</td></tr>
<tr><td>Overall Test Result</td><td>Pass: □</td><td colspan="2">Fail: □</td></tr>
</table>

4.5 Check Mec Edge Status

<table>
<tr><td>Test ID</td><td colspan="3">4.5 Check Mec Edge Status</td></tr>
<tr><td>Requirement</td><td colspan="3">The MEC host shall include MEC Edge Core for managing applications and devices at the edge.</td></tr>
<tr><td>Test Objective</td><td colspan="2">Ensure edge controller is running on the edge node.</td><td rowspan="2">Remarks</td></tr>
<tr><td rowspan="2">Test Description</td><td>Set Steps</td><td>Acceptance Criteria</td></tr>
<tr><td>Run command
$ mec status edge-core</td><td><pre>root@edgecore:~# mec status edge-core
Active: active (running) since Fri 2024-07-26</pre>
edge-core is listed with status Running</td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass: □</td><td colspan="2">Fail: □</td></tr>
</table>

4.5 Access the Mec Application

Test ID	**4.5.1 Access the Mec Application**		
Requirement	MEC applications shall be accessible over the network		
Test Objective	Ensure connectivity to the deployed MEC application.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ curl http://192.168.1.10:80	<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="logo.png"/><meta name="viewport" content="width=device width,initial-scale=1"/><meta name="theme color" content="#000000"/><meta name="description" content="Web site created using create-react-app"/><link rel="apple touch-icon" href="logo.png"/><link rel="manifest" href="/manifest.json"/><title>Coral VR Player</title><script defer="defer" src="/static/js/main.4352be0e.js"></script><link href="/static/css/main.57964f65.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript> </body></html>	
Overall Test Result	Pass: □	Fail: □	

4.5 Check Resource allocation

Test ID	**4.5.1 Check Resource allocation**		
Requirement	The MEC host shall provide compute, storage, and network resources for running MEC applications		
Test Objective	Verify that the MEC host provides necessary compute, storage, and network resources		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	$ mec status resources	Sufficient resources are allocated and available and following information is displayed: • cpu • load-average • memory-installed • memory-used • storage root@cloudcore:~# mec status resources top - 16:19:05 up 3 days, 6:27, 2 users, load average: 0.00, 0.00, 0.00 %Cpu(s): 2.9 us, 2.9 sy, 0.0 ni, 94.1 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st MiB Mem : 3946.9 total, 3149.3 free, 218.4 used, 579.2 buff/cache MiB Swap: 0.0 total, 0.0 free, 0.0 used. 3439.9 avail Mem	
Overall Test Result	Pass: □	Fail: □	

4.5 Validate Network Configuration

Test ID	**4.5 Validate Network Configuration**		
Requirement	The MEC host shall have network interfaces correctly configured for MEC applications.		
Test Objective	Ensure network interfaces are correctly configured		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	$ mec status network	Network interfaces are configured correctly. 2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 52:54:00:11:98:8e brd ff:ff:ff:ff:ff:ff inet 192.168.20.100/24 brd 192.168.20.255 scope global enp1s0 valid_lft forever preferred_lft forever inet6 fe80::5054:ff:fe11:988e/64 scope link valid_lft forever preferred_lft forever 3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default link/ether 02:42:d3:e6:16:0a brd ff:ff:ff:ff:ff:ff inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0 valid_lft forever preferred_lft forever inet6 fe80::42:d3ff:fee6:160a/64 scope link valid_lft forever preferred_lft forever	
Overall Test Result	Pass: □	Fail: □	

4.5 Validate Storage

Test ID	4.5 Validate Storage		
Requirement	The MEC host shall provide persistent storage for MEC applications		
Test Objective	Ensure persistent storage volumes are available and correctly configured..		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	$ mec status persistent-storage	Persistent volumes and claims are correctly listed and bound. root@cloudcore:~# mec status persistent-storage NAME CAPACITY ACCESS MODES RECLAIM POLICY STATUS task-pv-volume 1Gi RWO Retain Availabl	
Overall Test Result	Pass: □	Fail: □	

4.5 Deploy & Validate

Test ID	4.5 Deploy & Validate		
Requirement	The MEC platform shall provide essential services like Radio Network Information and Traffic Management.		
Test Objective	Ensure MEC services like Radio Network Information Service and Traffic Management Service are deployed and functional..		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	$ mec deploy mec-services.yaml
	
	$ curl http://192.168.1.10/radio-network-info
		Service is deployed and accessible. Response in JSON output is displayed	

Overall Test Result	Pass: □	Fail: □	

Section 4.6 Support for Tracing & Testing

S.no	Description
4.6.3	Configure Trace Requirement for UE in subscription Data
4.6.4	AMF Propagates trace Requirements to Network Entities
4.6.4	AUSF has received Trace Requirement
4.6.7	SMF has received trace requirement
4.6.7	PCF has received trace requirements
4.6.7	UPF has received trace requirement
4.6.7	Disable Trace
4.6.7	Review trace events

4.6.3 Configure Trace Requirement for UE in subscription Data

Test ID	**4.6.3 Configure Trace Requirement for UE in subscription Data**		
Requirement	Trace Requirements about a UE be configured in subscription data of the UE and delivered by the UDM.		
Test Objective	Ensure that Trace Requirements are correctly configured in the subscription data of a UE		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	Run command
	$ core-network trace start supi 123456789012345
		Trace Requirements are correctly configured and retrievable from the UDM.
		<pre>{
		"ueId": "123456789012345",
		"traceRequirements": {
		"traceReference": "TRACE123",
		"traceCollectionEntity": "10.0.0.1"
		}
		}</pre>	

Overall Test Result	Pass: □	Fail: □	

4.6.4 AMF Propagates trace Requirements to Network Entities

Test ID	**4.6.4 AMF Propagates trace Requirements to Network Entities**		
Requirement	The AMF shall enable Trace Requirements about a UE.		
Test Objective	Ensure that the AMF correctly applies Trace Requirements.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	Run command
	$ core-network trace status amf TRACE123
		AMF applies Trace Requirements to the relevant network entities without including SUPI or PEI information.
		<pre>{
		"traceReference": "TRACE123",
		"traceCollectionEntity": "10.0.0.1"
		}</pre>	

Overall Test Result	Pass: □	Fail: □	

4.6.4 AUSF has received Trace Requirement

Test ID	**4.6.4 AUSF has received Trace Requirement**		
Requirement	The AUSF applies Trace Requirements about a UE received from the UDM		
Test Objective	Ensure that the AUSF correctly applies Trace Requirements.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ core-network trace status ausf TRACE123	AUSF applies Trace Requirements to the relevant network entities without including SUPI or PEI information. 	
Overall Test Result	Pass: □	Fail: □	

4.6.7 SMF has received trace requirement

Test ID	**4.6.7 SMF has received trace requirement**		
Requirement	The SMF applies Trace Requirements about a UE received from the UDM		
Test Objective	Ensure that the SMF correctly applies Trace Requirements.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ core-network trace status smf TRACE123	SMF applies Trace Requirements to the relevant network entities without including SUPI or PEI information 	
Overall Test Result	Pass: □	Fail: □	

4.6.7 PCF has received trace requirements

Test ID	**4.6.7 PCF has received trace requirements**		
Requirement	The PCF applies Trace Requirements about a UE received from the UDM		
Test Objective	Ensure that the PCF correctly applies Trace Requirements.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ core-network trace status pcf TRACE123	PCF applies Trace Requirements to the relevant network entities without including SUPI or PEI information. 	
Overall Test Result	Pass: □	Fail: □	

4.6.7 UPF has received trace requirement

Test ID	**4.6.7 UPF has received trace requirement**		
Requirement	The UPF applies Trace Requirements about a UE received from the UDM		
Test Objective	Ensure that the SMF correctly applies Trace Requirements.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ core-network trace status upf TRACE123	UPF applies Trace Requirements to the relevant network entities without including SUPI or PEI information 	
Overall Test Result	Pass: □	Fail: □	

4.6.7 Disable Trace

Test ID	**4.6.7 Disable Trace**		
Requirement	Trace Requirements about a UE can be deactivated		
Test Objective	Ensure that trace deactivation for a UE is correctly handled		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run command $ core-network trace disable TRACE123	UPF applies Trace Requirements to the relevant network entities without including SUPI or PEI information `{ "traceReference": "TRACE123", "traceCollectionEntity": "10.0.0.1" }`	
Overall Test Result	Pass: □	Fail: □	

4.6.7 Review trace events

Test ID	**4.6.7 Review trace events**		
Requirement	The MEC system shall use Kubernetes to orchestrate MEC applications		
Test Objective	Ensure edge nodes are registered.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	Run command
	
	$ core-network trace list TRACE123
		[
		{
		"ngapMessage": {
		"procedureCode": "initialContextSetup",
		"ueNgapId": "1001",
		"amfNgapId": "2001",
		"traceActivation": {
		"traceReference": "TRACE123",
		"traceCollectionEntity": "10.0.0.1"
		},
		"eventEpoch": 1627382914
		}
		},
		{
		"ngapMessage": {
		"procedureCode": "handoverRequest",
		"ueNgapId": "1001",
		"sourceAmfNgapId": "2001",
		"targetAmfNgapId": "2002",
		"traceActivation": {
		"traceReference": "TRACE123",
		"traceCollectionEntity": "10.0.0.1"
		},
		"eventEpoch": 1627383014
		}
		},
		{
		"ngapMessage": {
		"procedureCode": "pathSwitchRequest",
		"ueNgapId": "1001",
		"sourceAmfNgapId": "2001",
		"traceActivation": {
		"traceReference": "TRACE123",
		"traceCollectionEntity": "10.0.0.1"
		},
		"eventEpoch": 1627383114
		}
		},
		{
		"ngapMessage": {
		"procedureCode": "ueContextModification",	

Test ID	**4.6.7 Review trace events**		

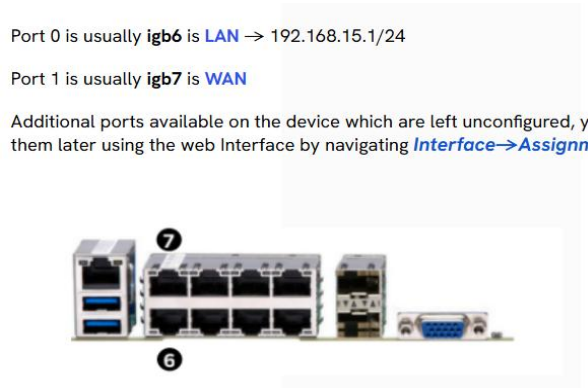
		"ueNgapId": "1001",
		"amfNgapId": "2001",
		"traceActivation": {
		"traceReference": "TRACE123",
		"traceCollectionEntity": "10.0.0.1"
		},
		"eventEpoch": 1627383214
		}
		},
		{
		"ngapMessage": {
		"procedureCode": "initialUEMessage",
		"ueNgapId": "1001",
		"amfNgapId": "2001",
		"traceActivation": {
		"traceReference": "TRACE123",
		"traceCollectionEntity": "10.0.0.1"
		},
		"eventEpoch": 1627383314
		}
		}
		]	

Overall Test Result	Pass: □	Fail: □	

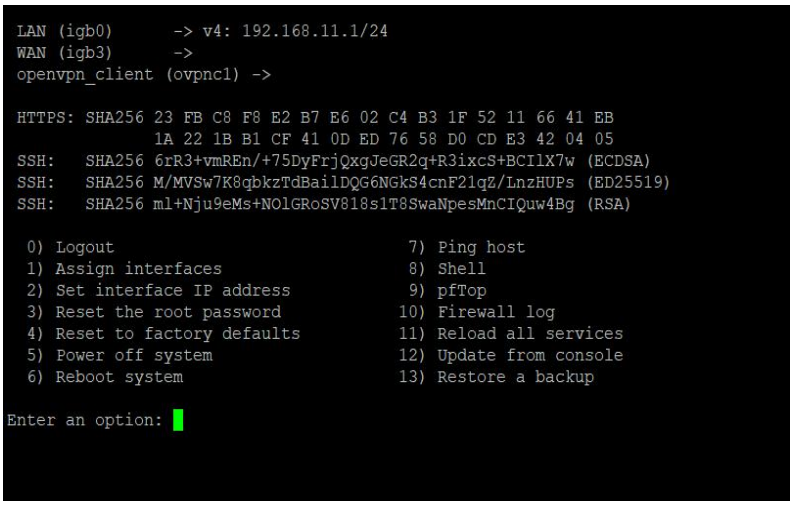
Section 4.8 Firewall with Router / SD-WAN Functional / Technical Specification

S.no	Description
	Basic Hardware Setup
	Accessing Web GUI / Management Console
4.8.1.1	Gigabit Base-T (Cu) = 6 ports or higher(as required) | 1 Gs Fiber (SFP) = 4 ports
4.8.1.2	WAN Interfaces
4.8.1.3	Management Port
4.8.2	Firewall Features
4.8.3	Baseline Throughput Performance
4.8.3.1	Firewall throughput of 1 Gbps
4.8.3.2	Threat Protection – 500 Mbps
	Application Specific Throughput (optional)
4.8.4	Prerequisite for Web Filtering
4.8.4.1	Control access to websites and website categories(e.g. business, news, sports, social media)
4.8.4.2	Integrate into Active Directory, applying policies to specific users or user groups
4.8.4.3	Enforce Safe Search
4.8.4.4	Block or control access to Cloud services.
4.8.4.5	Detailed web access reports (by user, group, website)
4.8.4.6	Full SSL Inspection support
4.8.4.7	Transparent solution (or explicit proxy support)
4.8.5	Preventing Intrusion Attempts
	DDoS Attack Protection
4.8.5.1	Detect and block network borne attacks
4.8.5.2	Protect mail, web and remote-access servers fromattacks (IIS, Exchange, Citrix)
4.8.5.3	Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat)
4.8.5.4	Common web platform protection (e.g. .NET, PHP,WordPress, CRM)
4.8.5.5	Customizable rule-set and signatures
4.8.6.1	SSL and IPSec VPN support
4.8.6.2	Web-Portal and full VPN client application
4.8.6.3	Site-to-Site IPSec VPN (with Dynamic Routing)
4.8.6.4	Optional: RADIUS/Active-Directory integration
4.8.6.5	Optional: Granular network access policies
4.8.6.6	Two-Factor authentication support (e.g. Secure Token)
4.8.6.7	High performance VPN concentrator Solution
4.8.7.1	Control and monitor cloud application usage (e.g.Dropbox, Box, Google Apps)
4.8.7.2	Full network visibility of HTTP and HTTPS traffic
4.8.7.3	Control access to specific applications (e.g. WebGames, Video Streaming)
4.8.7.4	Block access to malicious content or websites
4.8.7.5	Detailed reporting and network visibility
4.8.8.1	Dynamic routing (OSPF/BGP/RIP)
4.8.8.2	Optional: Granular network access policies
4.8.8.3	802.1Q VLAN and Layer2 switching support
4.8.8.4	Rich traffic/shaping QOS support
4.8.8.5	Dynamic routing over VPN (e.g. OSPF)

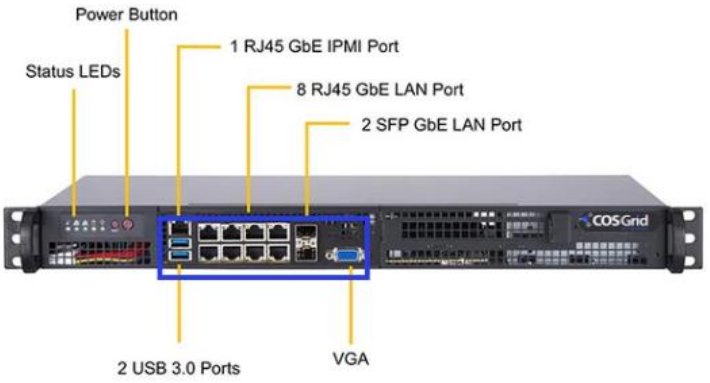
Basic Hardware Setup

Test ID	**Basic Hardware Setup**		
Requirement	Check the Basic Hardware setup		
Test Objective	To verify the Hardware setup support		**Remarks**
Test Description	**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 	
Overall Test Result	Pass: □	Fail: □	

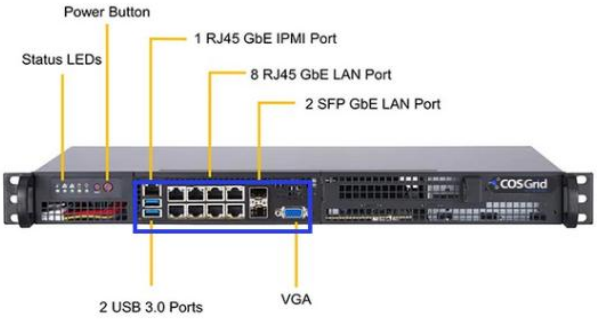
Accessing Web GUI / Management Console

Test ID	**Accessing Web GUI / Management Console**		
Requirement	Check accessing web GUI / management console.		
Test Objective	To verify web GUI/management console support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	After following the steps mentioned in 2.1.2. Access the Web GUI in your browser at **192.168.15.1.** 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. Login to the GUI / Console with credentials provided by the provider.	It should take you to the COSGrid Next Gen Firewall Web Interface. And the Login option should be displayed. In the console, you should be able to access the firewall. And prompts for login should be displayed. You should be able to access the functionality of firewall   	
Overall Test Result	Pass: □	Fail: □	

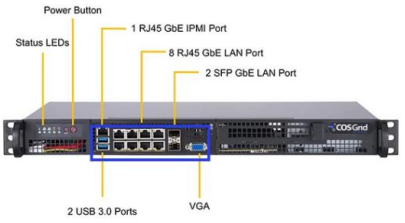
4.8.1.1 Gigabit Base-T (Cu) = 6 ports or higher(as required) | 1 Gs Fiber (SFP) = 4 ports

Test ID	**4.8.1.1 Gigabit Base-T (Cu) = 6 ports or higher(as required) | 1 Gs Fiber (SFP) = 4 ports**		
Requirement	Check the Hardware configurations - Network Interface port		
Test Objective	To verify the Hardware support compliance		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Networking Interface Check the hardware appliance port LAN Interface	1 Gigabit Base-T (Cu) = 6 ports or higher(as required) 1 Gs Fiber (SFP) = 4 ports 	
Overall Test Result	Pass: □	Fail: □	

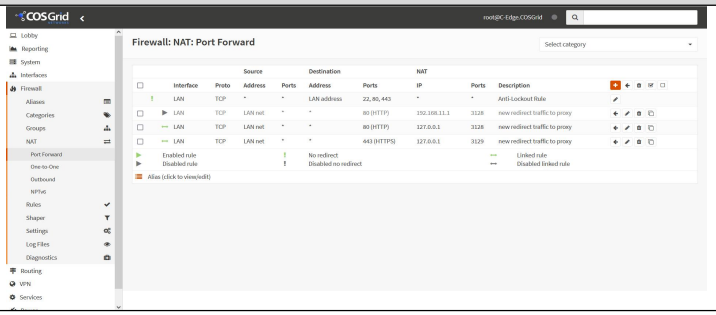
4.8.1.2 WAN Interfaces

Test ID	**4.8.1.2 WAN Interfaces**		
Requirement	Check the Hardware configurations - Interface port		
Test Objective	To verify the Hardware support compliance		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	WAN interface	2 x 1G Gigabit Ethernet SFP+ ports 	
Overall Test Result	Pass: □	Fail: □	

4.8.1.3 Management Port

Test ID	**4.8.1.3 Management Port**		
Requirement	Check the Hardware configurations - Interface port		
Test Objective	To verify the Hardware support compliance		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check above the USB ports	10/100 Mbps RJ 45 Management port 	
Overall Test Result	Pass: □	Fail: □	

4.8.2 Firewall Features

Test ID	**4.8.2 Firewall Features**		
Requirement	Check the Firewall Features		
Test Objective	To verify the Firewall features		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In the Nav bar of side menu select **Firewall, under it firewall features available**		
Overall Test Result	Pass: □	Fail: □	

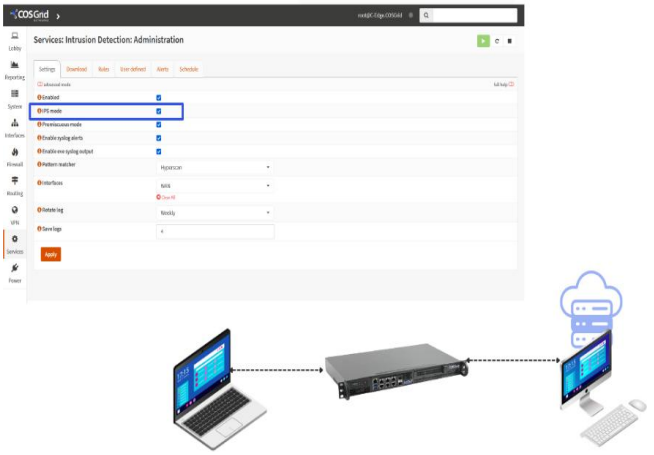
4.8.3 Performance Requirement

Test ID	**Baseline Throughput Performance**		
Requirement	Firewall baseline Throughput performance		
Test Objective	Verify that the COSGrid Firewall can sustain the desired network throughput without significant performance degradation or affecting user experience.		**Remarks**
Test Description	**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.	
Overall Test Result	Pass: □	Fail: □	

4.8.3.1 Firewall throughput of 1 Gbps

Test ID	4.8.3.1 Firewall throughput of 1 Gbps		
Requirement	Throughput performance		
Test Objective	Verify that the COSGrid Firewall can sustain the desired network throughput without significant performance degradation or affecting user experience.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Activate the COSGrid Firewall with relevant security policies configured. Repeat the throughput measurements using the same benchmarking tools and methodology as in Case 1 (iPerf3 or SpeedTest). Compare the obtained throughput values with the baseline measurements.	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). Throughput degradation should not impact user experience in terms of application responsiveness, file transfers, or overall network performance. Firewall Throughput - 1Gbps 	
Overall Test Result	Pass: □	Fail: □	

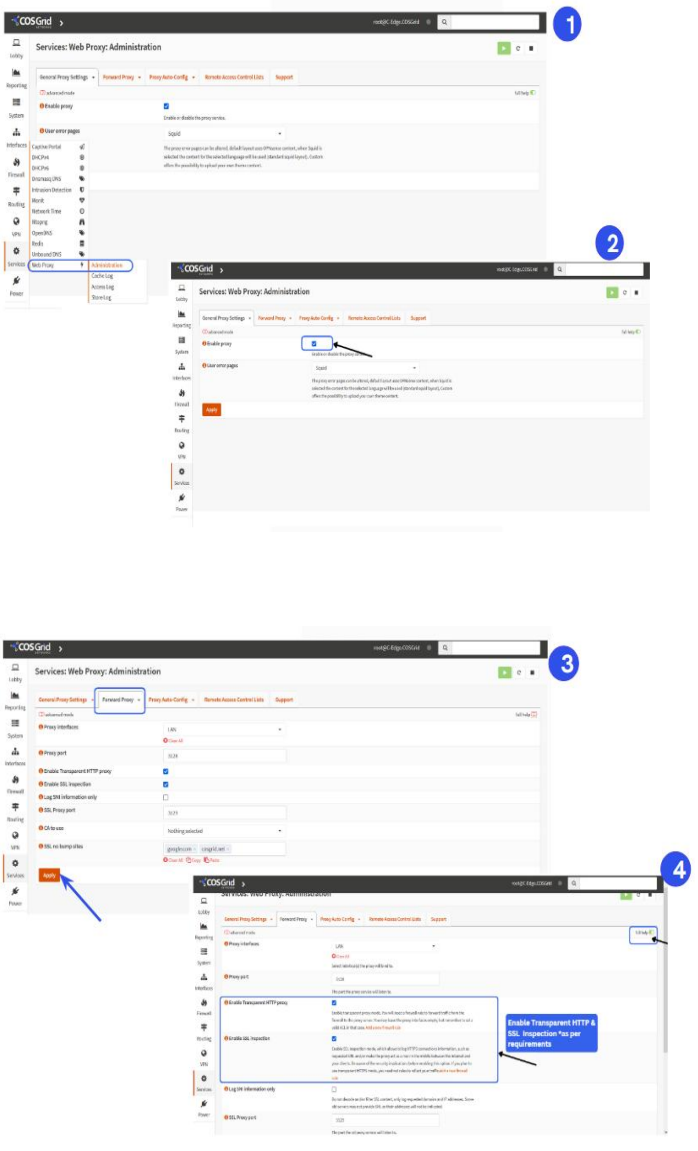
4.8.3.2 Threat Protection – 500 Mbps

Test ID	**4.8.3.2 Threat Protection – 500 Mbps**		
Requirement	Threat Protection Throughput		
Test Objective	Verify that the COSGrid Firewall can sustain the desired network throughput without significant performance degradation or affecting user experience.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Navigate ***Services > Intrusion Detection > Administration*** Enable the IPS mode	Threat Protection - 500 Mbps 	
Overall Test Result	Pass: □	Fail: □	

Application Specific Throughput (optional)

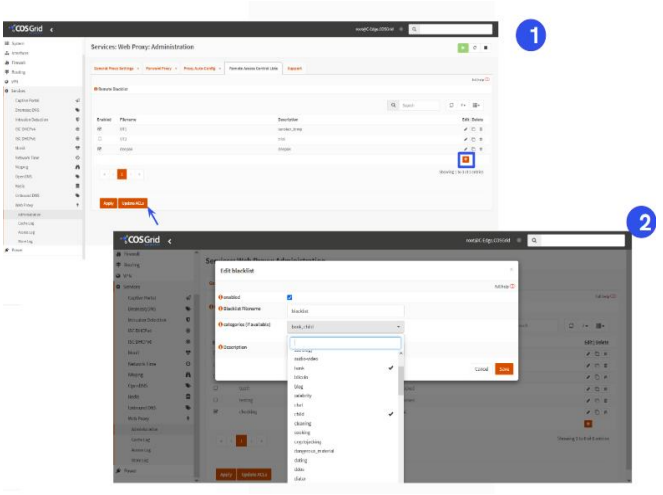
Test ID	**Application Specific Throughput (optional)**		
Requirement	Application Specific Throughput performance		
Test Objective	Verify that the COSGrid Firewall can sustain the desired network throughput without significant performance degradation or affecting user experience.		**Remarks**
Test Description	**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.	
Overall Test Result	Pass: □	Fail: □	

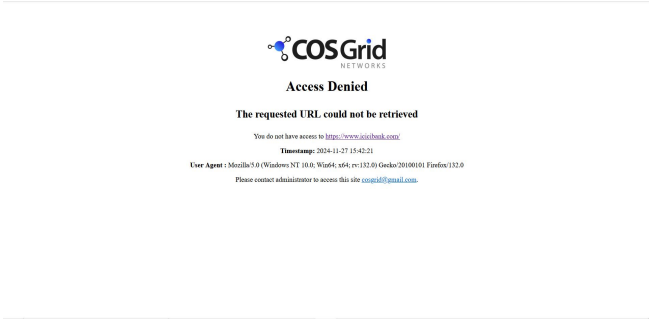
4.8.4 Web Filtering

Test ID	**4.8.4 Prerequisite for Web Filtering**	
Requirement	Web Filtering enablement	
Test Objective	Prerequisite for Web filtering	**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to ***Services > Web Proxy > Administration > General Proxy Settings .*** Configure proxy by checked the Enable Proxy Check in Box Then Click the Tab ***Forward Proxy .*** Toggle the Full help button on the top right where you can enable Transparent HTTP proxy or SSL inspection or both 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	Web Filtering enablement 

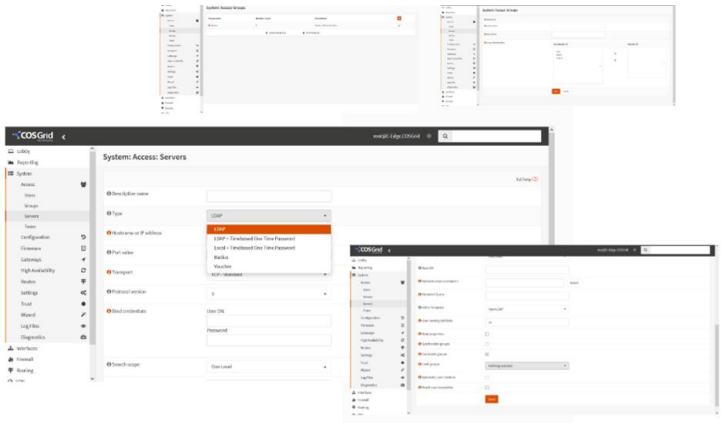
Test ID	**4.8.4 Prerequisite for Web Filtering**		
	Forward window pops up where you can - Add firewall rule for Transparent Proxy, - Add firewall rule for SSL inspection to redirect network Traffic And Scroll down click **Save** button		
Overall Test Result	Pass: □	Fail: □	

4.8.4.1 Control access to websites and website categories(e.g. business, news, sports, social media)

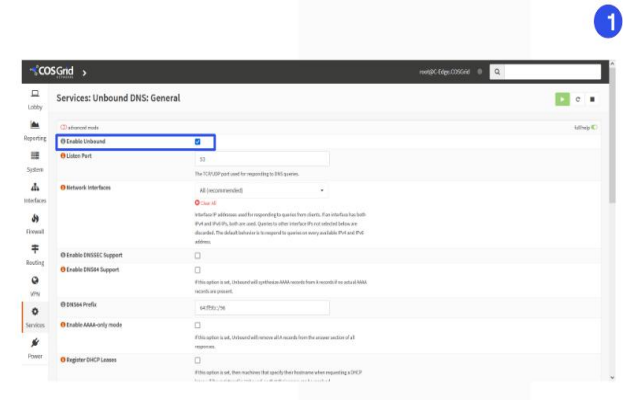
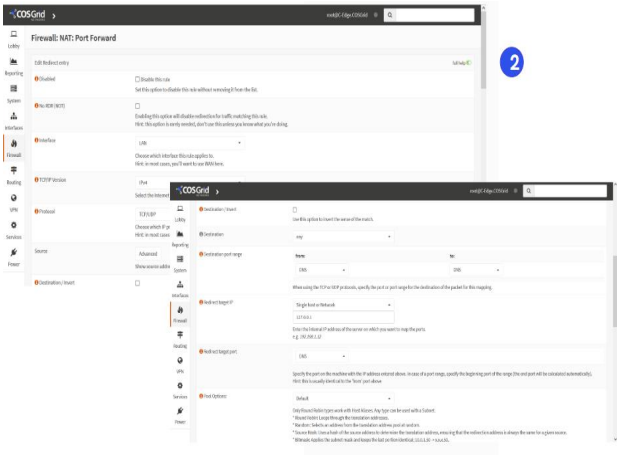
Test ID	**4.8.4.1 Control access to websites and website categories(e.g. business, news, sports, social media)**		
Requirement	Firewall logs contain accurate records of blocked and allowed web tr		
Test Objective	Validate that the firewall logs contain accurate records of blocked and allowed web traffic.		**Remarks**
Test Description	**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***. Figure:3	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.* Websites in blocked categories should be inaccessible.	
	Attempt to access websites belonging to the blocked categories. (say facebook.com)	Websites not in blocked categories should be accessible.	
	Attempt to access websites that do not belong to the blocked categories.	Firewall logs should accurately reflect blocked and allowed traffic based on categories.	
	Go to ***Services > Web Proxy > Access Log.***Check the firewall logs for accurate logging of		

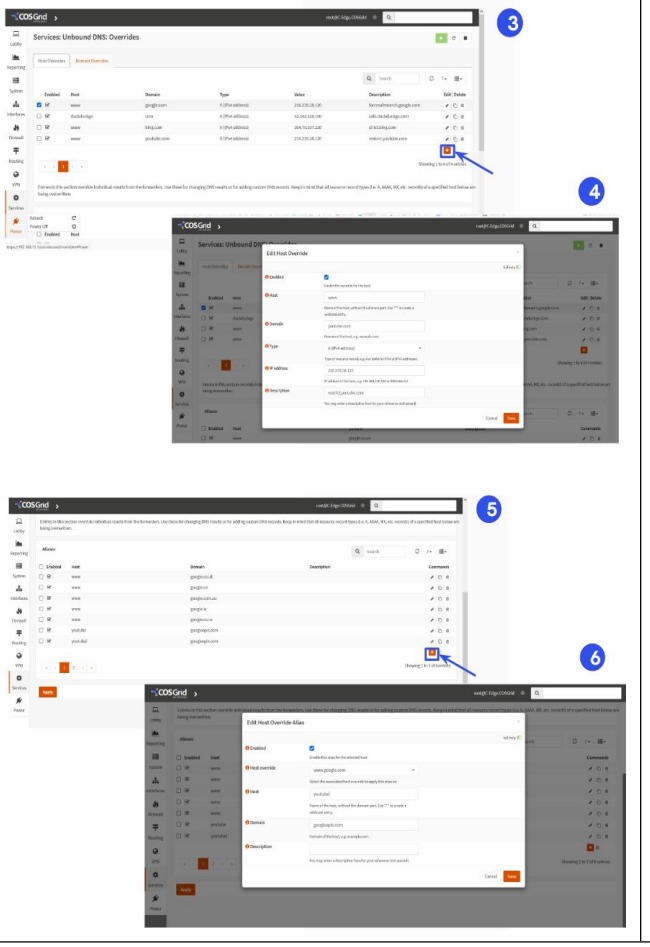
Test ID	**4.8.4.1 Control access to websites and website categories(e.g. business, news, sports, social media)**		
	blocked and allowed traffic.		
Overall Test Result	Pass: □	Fail: □	

4.8.4.2 Integrate into Active Directory, applying policies to specific users or user groups

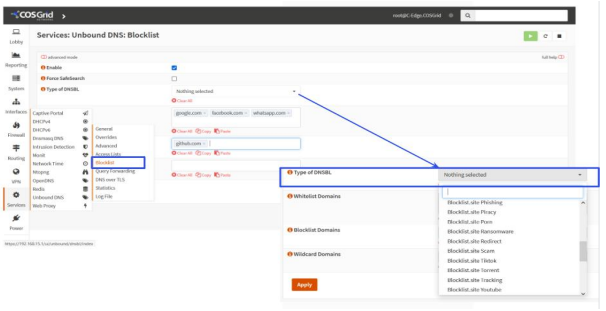
Test ID	**4.8.4.2 Integrate into Active Directory, applying policies to specific users or user groups**		
Requirement	Integrate into Active Directory, applying policies to specific users or user groups.		
Test Objective	Verify that the COSGrid Firewall effectively integrates into AD		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Navigate ***System > Users*** & ***System > Groups*** to create a user and groups Go to ***System > Access Server >*** In The Type dropdown field you can Select LDAP which is AD (Active Directory) Scroll down & check the specific groups	**Integration into Active Directory, applying policies to specific users or user groups.** 	
Overall Test Result	Pass: □	Fail: □	

4.8.4.3 Enforce Safe Search

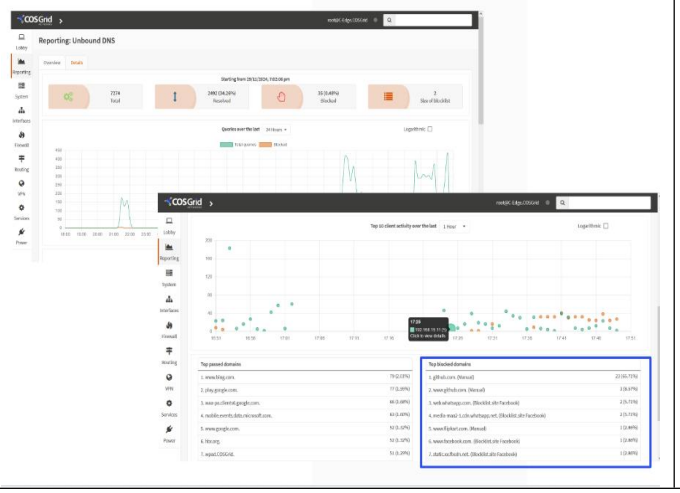
Test ID	**4.8.4.3 Enforce Safe Search**		
Requirement	Safesearch is enforced		
Test Objective	Verify that the COSGrid Firewall effectively enforce Safe search		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > Unbound DNS > General*** and make sure the "*Enable Unbound*" box is checked. Go to ***Firewall > NAT > Port forward*** and click on add to create a new rule. Apply the following settings: Interface = LAN Protocol = TCP/UDP Destination = any Destination port range / from = DNS Destination port range / to = DNS Redirect target IP = Single host or network = 127.0.0.1 Redirect target port = DNS Description = DNS redirection 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	Safe search is enforced   	

Test ID	**4.8.4.3 Enforce Safe Search**		
	IP = 216.239.38.120 Description = forcesafesearch.google.com 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		
Overall Test Result	Pass: □	Fail: □	

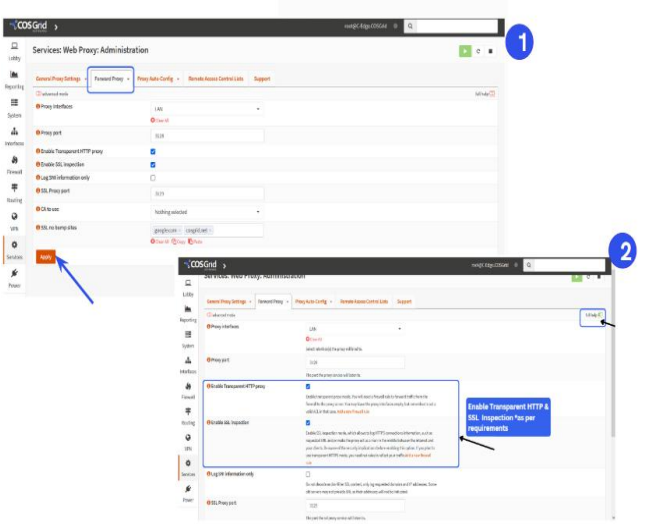
4.8.4.4 Block or control access to Cloud services.

Test ID	**4.8.4.4 Block or control access to Cloud services.**		
Requirement	Block or control access to Cloud services..		
Test Objective	Verify that the COSGrid Firewall effectively Block or control access to Cloud services		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Navigate ***Services > Unbound DNS > Blocklist*** Select Type of DNSBL / Cloud Services to block from the Dropdown	Block or control access to Cloud services 	
Overall Test Result	Pass: □	Fail: □	

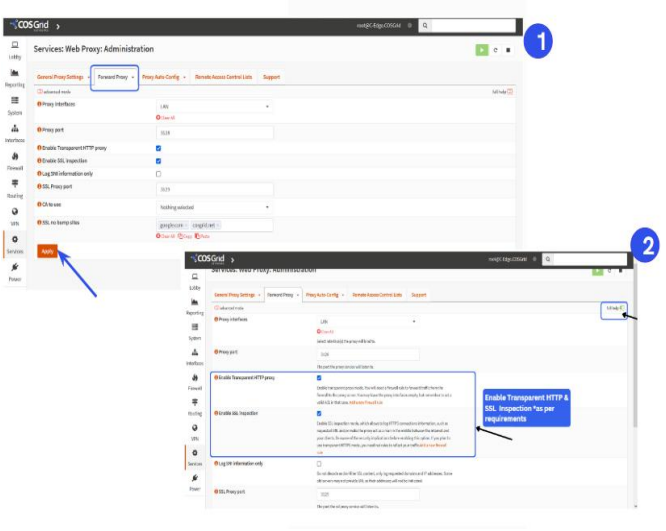
4.8.4.5 Detailed web access reports (by user, group, website)

Test ID	**4.8.4.5 Detailed web access reports (by user, group, website)**	
Requirement	Detailed web access reports (by user, group, website)	
Test Objective	Verify that the COSGrid Firewall effectively reports detailed web access reports (by user, group, website)	**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**
	Navigate ***Reporting > Unbound DNS*** Scroll Down to see the detailed Web access reports	Detailed web access reports (by user, group, website) 
Overall Test Result	Pass: □	Fail: □

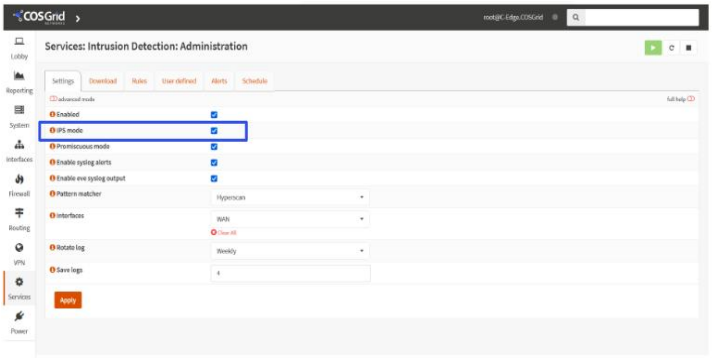
4.8.4.6 Full SSL Inspection support

Test ID	**4.8.4.6 Full SSL Inspection support**		
Requirement	Full SSL Inspection support		
Test Objective	Verify that the COSGrid Firewall effectively have Full SSL Inspection support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > Web Proxy > Administration > Forward Proxy .*** Toggle the Full help button on the top right where you can enable Transparent HTTP proxy or SSL inspection or both	Full SSL Inspection support 	
Overall Test Result	Pass: □	Fail: □	

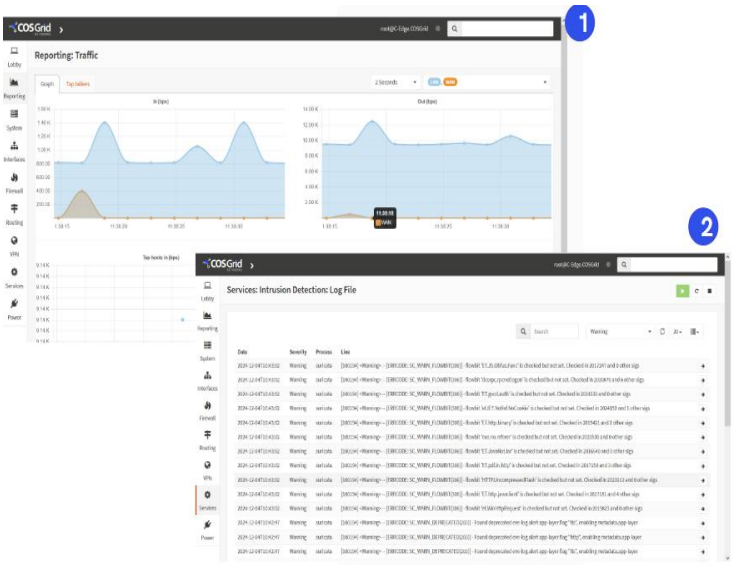
4.8.4.7 Transparent solution (or explicit proxy support)

Test ID	**4.8.4.7 Transparent solution (or explicit proxy support)**		
Requirement	Transparent solution (or explicit proxy support)		
Test Objective	Verify that the COSGrid Firewall effectively enables Transparent solution (or explicit proxy support)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > Web Proxy > Administration > Forward Proxy .*** Toggle the Full help button on the top right where you can enable Transparent HTTP proxy or SSL inspection or both	Transparent solution (or explicit proxy support) 	
Overall Test Result	Pass: □	Fail: □	

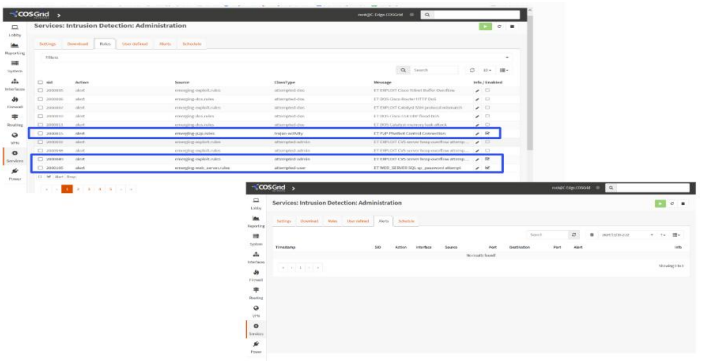
4.8.5 Optional: Intrusion Prevention System

Test ID	4.8.5 Preventing Intrusion Attempts		
Requirement	IPS Performance Compliance		
Test Objective	Validate that it prevents intrusion attempts and malicious traffic		**Remarks**
Test Description	**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. Use tools like Nmap, Nessus, and Metasploit. ***Go to Services > Intrusion Detection > Log File***. Monitor the firewall's response and logging. As mentioned in **set step 2**.	The firewall should detect and block **intrusion attempts**. It should generate alerts or notifications for security events. Logs should provide detailed information about the intrusion attempts and actions taken by the firewall. 	
Overall Test Result	Pass: □	Fail: □	

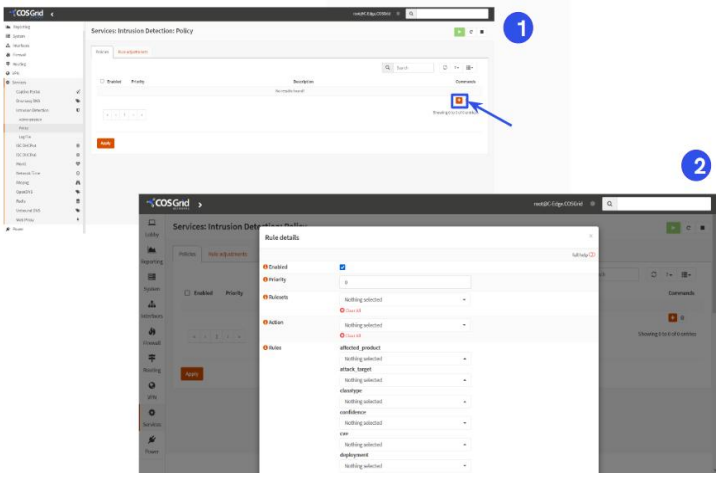
DDoS Attack Protection

Test ID	**DDoS Attack Protection**		
Requirement	DDoS attack Protection enablement		
Test Objective	Verify the effectiveness in detecting and mitigating DDoS attacks		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Generate a high volume of traffic (e.g., **UDP, ICMP, SYN** floods) to simulate a volumetric attack. Go to ***Reporting > Traffic.*** Monitor firewall's response, including traffic analysis, rate limiting, and traffic shaping. Figure:5 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. Figure:7	Detects and blocks network borne attacks. Discussed in the third step There should be **high traffic flow** in the graphs. There should be **alert logs in the file** that should contain the information about the specific protocol.  	
Overall Test Result	Pass: □	Fail: □	

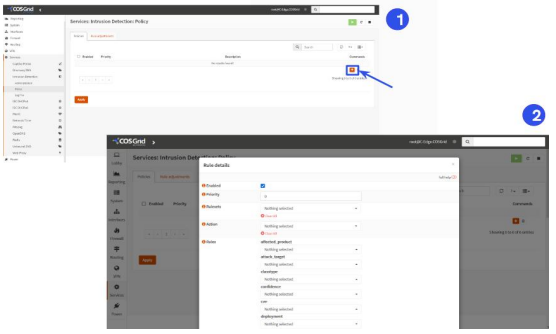
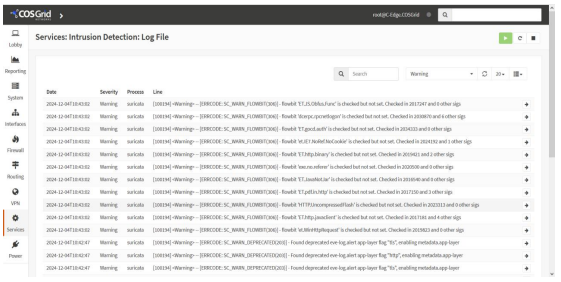
4.8.5.1 Detect and block network borne attacks

Test ID	**4.8.5.1 Detect and block network borne attacks**		
Requirement	Detect and block network borne attacks		
Test Objective	Ensure the firewall's ability to Detect and block network borne attacks		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	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.	Detect and block network borne attacks 	
Overall Test Result	Pass: □	Fail: □	

4.8.5.2 Protect mail, web and remote-access servers fromattacks (IIS, Exchange, Citrix)

Test ID	4.8.5.2 Protect mail, web and remote-access servers fromattacks (IIS, Exchange, Citrix)		
Requirement	Application Level attack protection support		
Test Objective	Ensure the firewall's ability to control and restrict access to specific applications		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > Intrusion Detection > Policy.*** Create application control policies to allow, deny, or restrict specific applications or categories. Go to ***Services > Intrusion Detection > Log File.*** Verify that the firewall enforces policies accurately and blocks unauthorized applications.	Protect mail, web and remote-access servers from attacks (IIS, Exchange, Citrix) The logs should indicate the attack and the response action. 	
Overall Test Result	Pass: □	Fail: □	

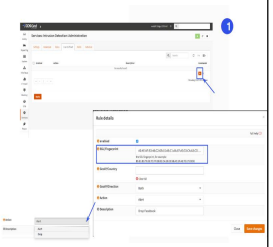
4.8.5.3 Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat)

Test ID	**4.8.5.3 Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat)**		
Requirement	Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat)		
Test Objective	Ensure the firewall's ability to Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > Intrusion Detection > Policy.*** Create application control policies to allow, deny, or restrict specific applications or categories Test application access under different policy configurations. Go to ***Services > Intrusion Detection > Log File.*** Verify that the firewall enforces policies accurately and blocks unauthorized applications.	Protect staff and internal systems from application level attacks (e.g. Office, Adobe Acrobat). The logs should indicate the attack and the response action.   	
Overall Test Result	Pass: □	Fail: □	

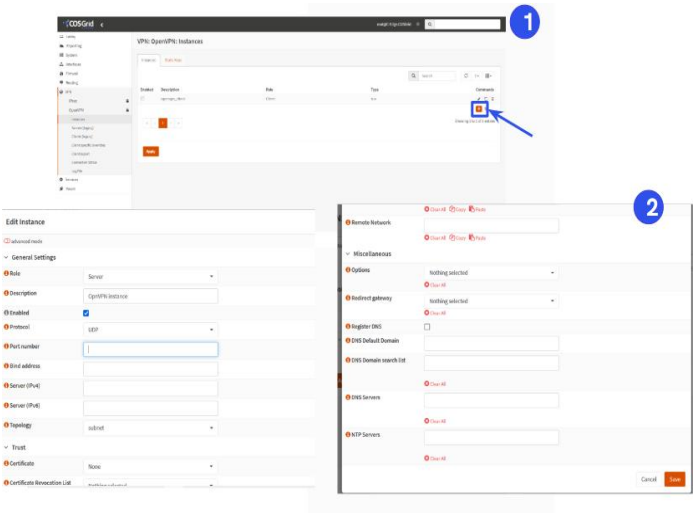
4.8.5.4 Common web platform protection (e.g. .NET, PHP,WordPress, CRM)

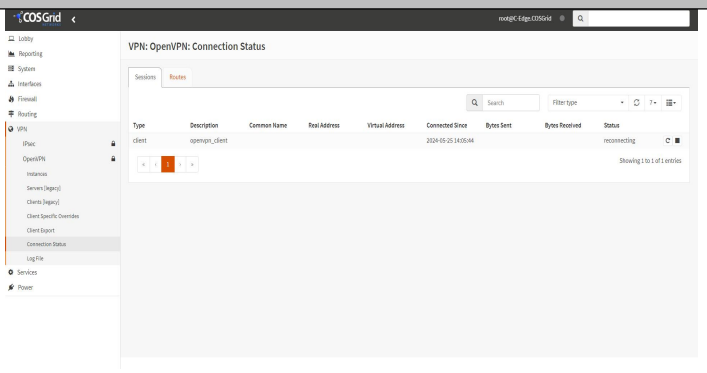
Test ID	**4.8.5.4 Common web platform protection (e.g. .NET, PHP,WordPress, CRM)**		
Requirement	Common web platform protection (e.g. .NET, PHP,WordPress, CRM)		
Test Objective	Ensure the firewall's ability to Common web platform protection (e.g. .NET, PHP,WordPress, CRM)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
		Common web platform protection (e.g. .NET, PHP,WordPress, CRM)	
Overall Test Result	Pass: □	Fail: □	

4.8.5.5 Customizable rule-set and signatures

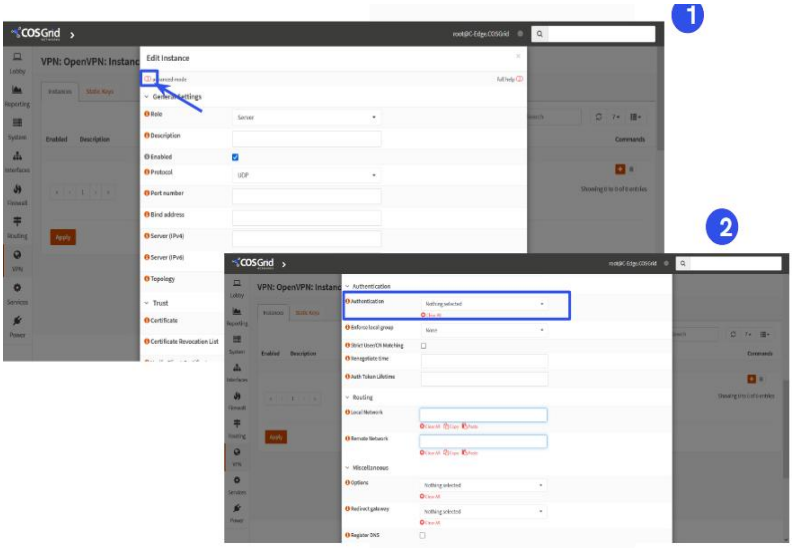
Test ID	**4.8.5.5 Customizable rule-set and signatures**		
Requirement	Customizable rule-set and signatures		
Test Objective	Ensure the firewall's ability toCustomizable rule-set and signatures		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Navigate ***Services > Intrusion Detection > Administration > Settings*** and Enable IPS Mode Click on the User Defined Tab andclick 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 : 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	Customizable rule-set and signatures 	
Overall Test Result	Pass: □	Fail: □	

4.8.6.1 SSL and IPSec VPN support

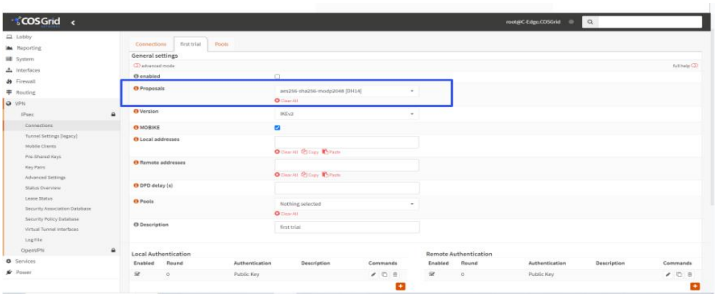
Test ID	**4.8.6.1 SSL and IPSec VPN support**		
Requirement	OpenVPN - SSL VPN		
Test Objective	Verify the seamless integration of OpenVPN		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Access the COSGrid Firewall's configuration interface.	User-friendly options for enabling and configuring all three features.	
	Go to ***VPN > OpenVPN.*** Verify the presence of options to enable and configure OpenVPN and authentication services.	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.	
	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. 	

Test ID	**4.8.6.1 SSL and IPSec VPN support**		
			
Overall Test Result	Pass: □	Fail: □	

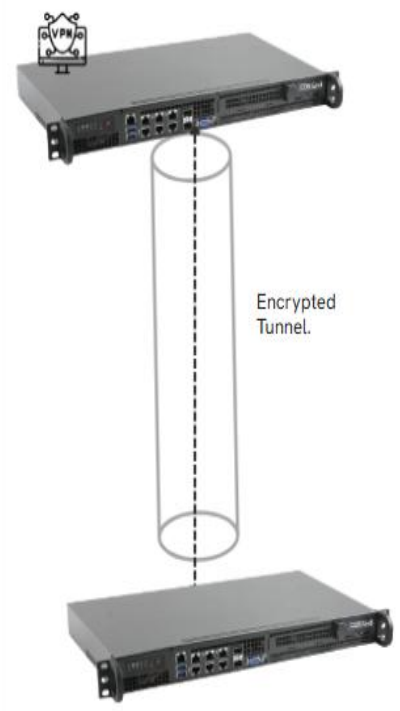
4.8.6.2 Web-Portal and full VPN client application

Test ID	**4.8.6.2 Web-Portal and full VPN client application**		
Requirement	VPN traffic Encryption and access OpenVPN - Web Portal		
Test Objective	To check the VPN performance and configurations		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***VPN > OpenVPN > Instances >*** **(Go to one instance)** **Auth** Dropdown (Advanced Mode) Establish VPN connections using your desired encryption algorithms and initiate data transfer.	All VPN traffic encrypted with robust algorithms should be present in the options. The connection between two devices should only be established if they share the same encryption techniques. 	
Overall Test Result	Pass: □	Fail: □	

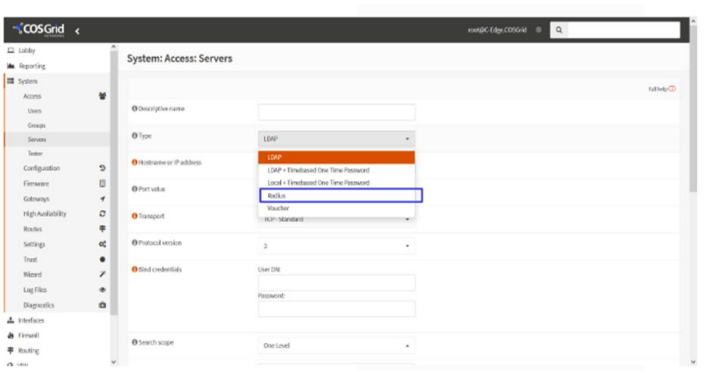
4.8.6.2 Web-Portal and full VPN client application

Test ID	**4.8.6.2 Web-Portal and full VPN client application**		
Requirement	VPN traffic Encryption and access IPsec		
Test Objective	To check the VPN performance and configurations		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***VPN > IPsec > Connections>*** (Go to one connection) ***> Proposals.*** Establish VPN connections using specific proposals and initiate data transfer.	All VPN proposals should be listed down. The connection between two devices should only be established if they share the same encryption techniques. 	
Overall Test Result	Pass: □	Fail: □	

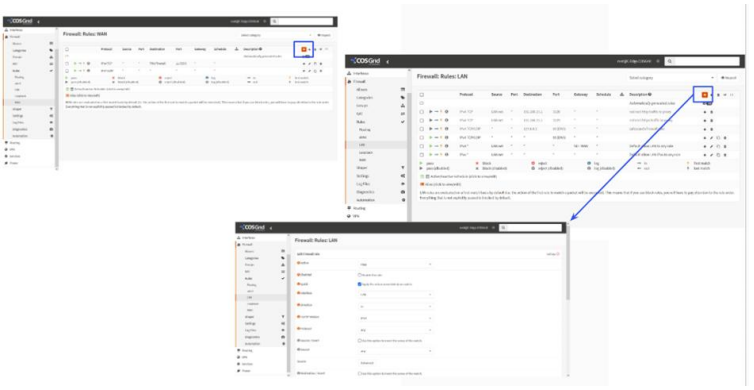
4.8.6.3 Site-to-Site IPSec VPN (with Dynamic Routing)

Test ID	**4.8.6.3 Site-to-Site IPSec VPN (with Dynamic Routing)**		
Requirement	Site-to-Site IPSec VPN (with Dynamic Routing)		
Test Objective	Assess the Site-to-Site IPSec VPN (with Dynamic Routing)		**Remarks**
Test Description	**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 	
Overall Test Result	Pass: □	Fail: □	

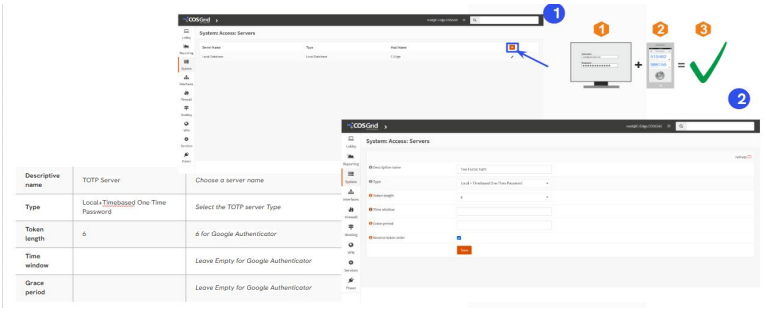
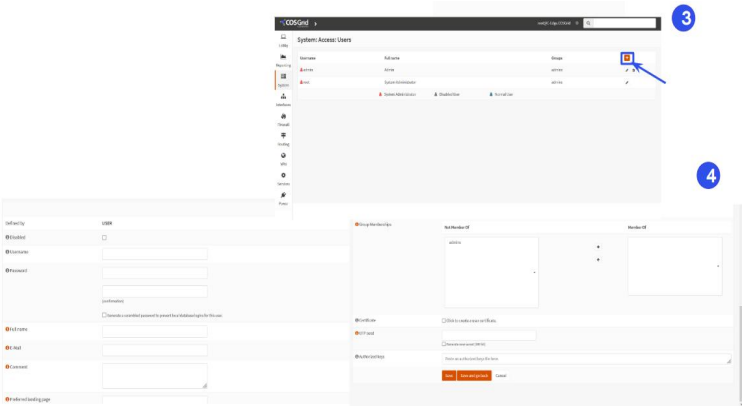
4.8.6.4 Optional: RADIUS/Active-Directory integration

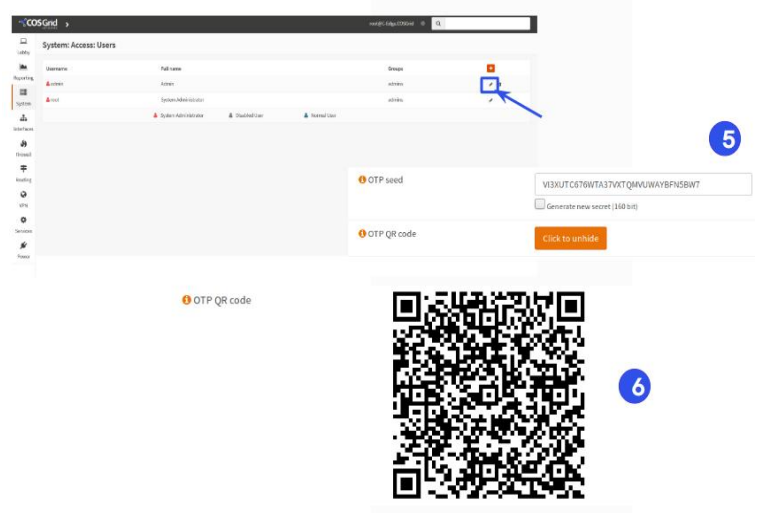
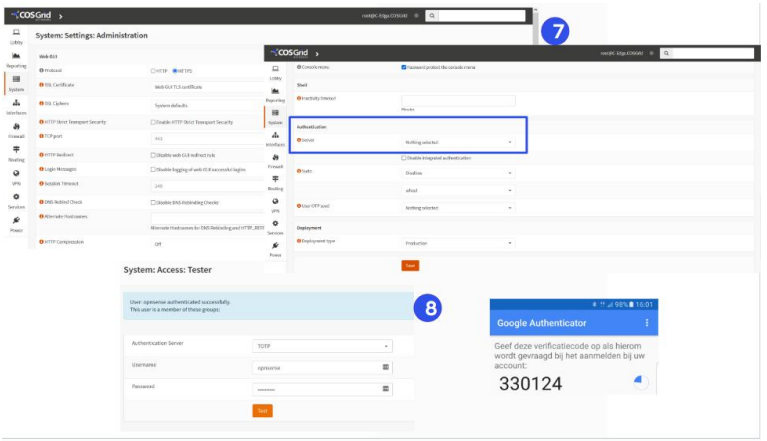
Test ID	**4.8.6.4 Optional: RADIUS/Active-Directory integration**		
Requirement	RADIUS/Active-Directory integration		
Test Objective	RADIUS/Active-Directory integration with Firewall		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***System > Access > Server >*** In The Type dropdown field you can Select LDAP which is AD (Active Directory)or RADIUS	Optional: RADIUS/Active-Directory integration 	
Overall Test Result	Pass: □	Fail: □	

4.8.6.5 Optional: Granular network access policies

Test ID	**4.8.6.5 Optional: Granular network access policies**		
Requirement	Granular network access policies		
Test Objective	Granular network access policies in Firewall		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Navigate ***Firewall > Rules > WAN*** ***Firewall > Rules > LAN*** In the WAN and LAN policy you can add the rule which allows the users for fine grained granular access	Optional: Granular network access policies 	
Overall Test Result	Pass: □	Fail: □	

4.8.6.6 Two-Factor authentication support (e.g. Secure Token)

Test ID	**4.8.6.6 Two-Factor authentication support (e.g. Secure Token)**		
Requirement	Two factor authentication Support		
Test Objective	Assess the user's 2FA		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Navigate ***System*** ‣ ***Access*** ‣ ***Servers*** and press **Add server** in the top right corner. 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**. To activate your new OTP seed on the Google Authenticator, Navigate ***System*** ‣ ***Access*** ‣ ***Servers*** and press	Two-Factor authentication support (e.g. Secure Token)  	

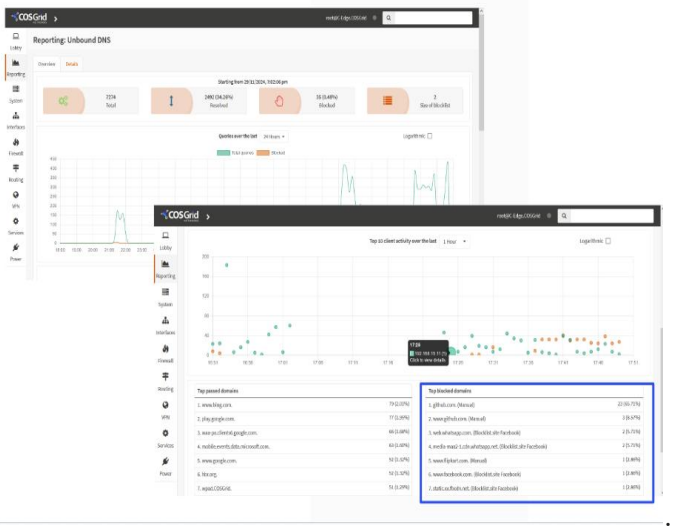
Test ID	4.8.6.6 Two-Factor authentication support (e.g. Secure Token)		
	Add server. Later,Navigate **System > Access > Add users** Then enable Generate New secret Checkbox , You will get a OTP QR Code or reopen the created user you just created by clicking on the pencil icon. Navigate ***System ▸ Settings ▸ 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***	 	

Test ID	**4.8.6.6 Two-Factor authentication support (e.g. Secure Token)**		
	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**.		
Overall Test Result	Pass: □	Fail: □	

4.8.6.7 High performance VPN concentrator Solution

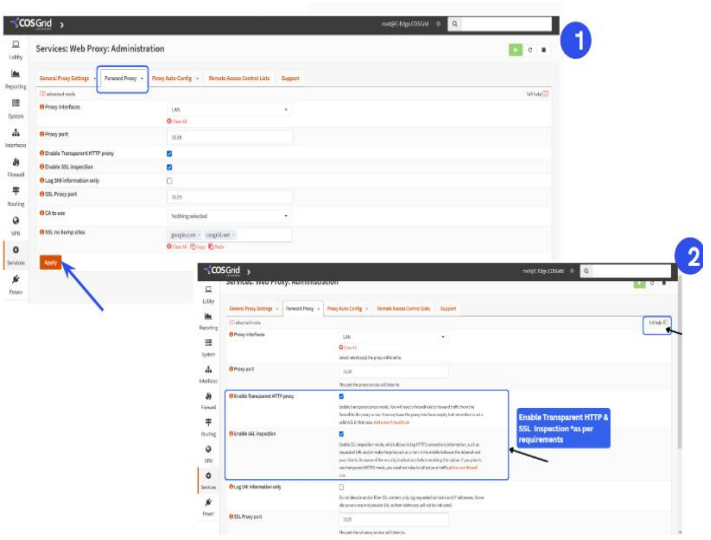
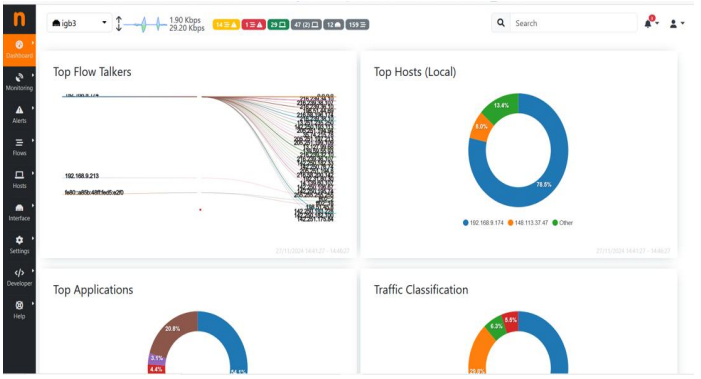
Test ID	**4.8.6.7 High performance VPN concentrator Solution**		
Requirement	Acceptable Latency and Enhanced User Experience		
Test Objective	Assess the user experience across different authentication methods		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Measure throughput and **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 	
Overall Test Result	Pass: □	Fail: □	

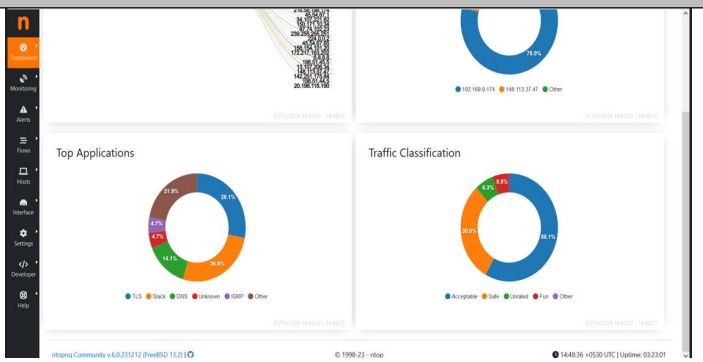
4.8.7.1 Control and monitor cloud application usage (e.g.Dropbox, Box, Google Apps)

Test ID	**4.8.7.1 Control and monitor cloud application usage (e.g.Dropbox, Box, Google Apps)**		
Requirement	Control and monitor cloud application usage (e.g.Dropbox, Box, Google Apps)		
Test Objective	Validate that the firewall Control and monitor cloud application usage (e.g.Dropbox, Box, Google Apps)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > Web Proxy > Administration > Remote Access Control Lists.*** Configure filtering rules to block specific *categories of Applications (e.g., google, dropbox). Do not forget to press the ***Update ACLs button***. Attempt to access applications belonging to the blocked categories. Attempt to access Application that do not belong to the blocked categories. Go to ***Services > Web Proxy > Access Log.***Check the firewall logs for accurate logging of blocked and allowed traffic. **Reporting > unbound**	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*. Applications in blocked categories should be inaccessible. Applications not in blocked categories should be accessible. Firewall logs should accurately reflect blocked and allowed traffic based on categories 	

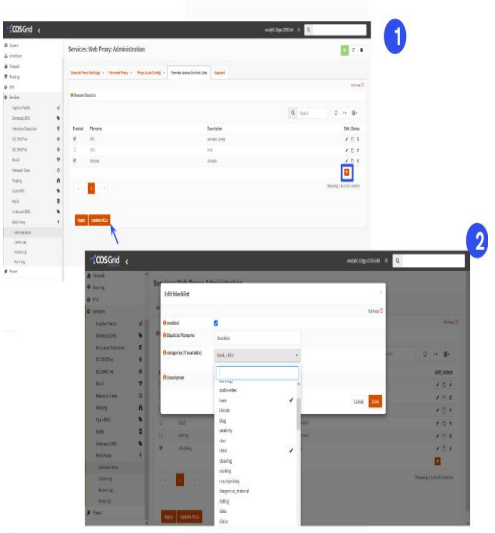
Test ID	4.8.7.1 Control and monitor cloud application usage (e.g.Dropbox, Box, Google Apps)		
	DNS		
Overall Test Result	Pass: □	Fail: □	

4.8.7.2 Full network visibility of HTTP and HTTPS traffic

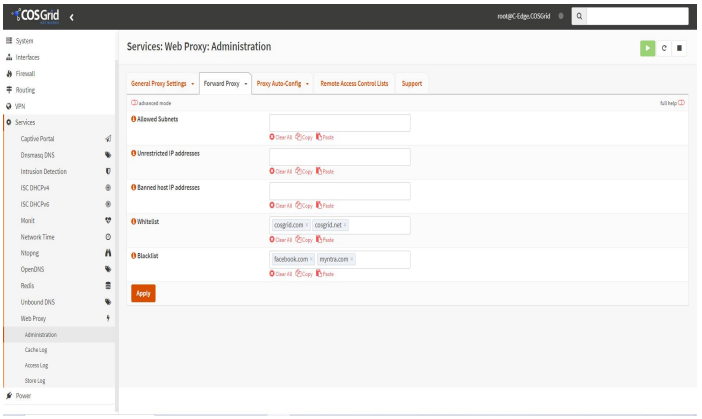
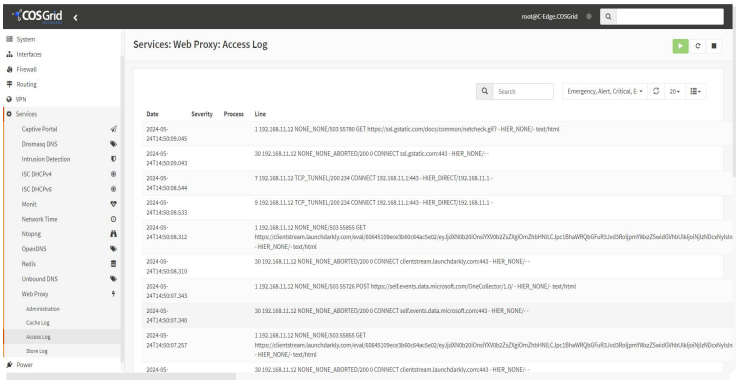
Test ID	**4.8.7.2 Full network visibility of HTTP and HTTPS traffic**		
Requirement	Full Network Visibility of HTTP & HTTPS traffic		
Test Objective	Full Network Visibility of HTTP & HTTPS traffic of Firewall		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > Web Proxy > Administration > Forward Proxy .*** Toggle the Full help button on the top right where you can enable Transparent HTTP proxy Visit your Firewall IP : 3000 (port) in the browser for visibility	Full Network Visibility of HTTP & HTTPS traffic  	

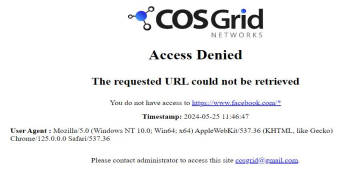
Test ID	**4.8.7.2 Full network visibility of HTTP and HTTPS traffic**		
			
Overall Test Result	Pass: □	Fail: □	

4.8.7.3 Control access to specific applications (e.g. WebGames, Video Streaming)

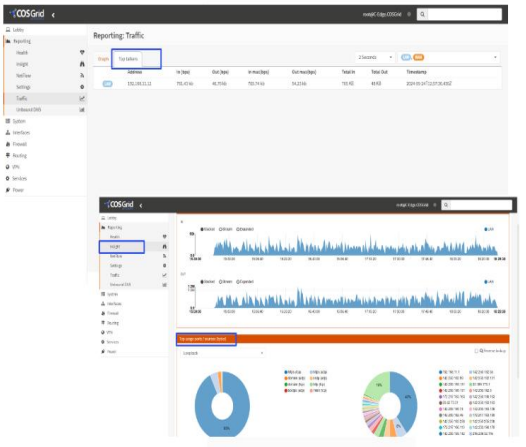
Test ID	**4.8.7.3 Control access to specific applications (e.g. WebGames, Video Streaming)**		
Requirement	Ensure that allowed websites are accessible without restrictions.		
Test Objective	To verify that allowed websites are accessible		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > Web Proxy > Administration > Remote Access Control Lists.*** Configure filtering rules to block specific *categories of Applications (e.g., webgames). Do not forget to press the ***Update ACLs button*** Attempt to access an application in your browser that is not restricted by the filtering rules. Verify that the website loads and functions as expected. Go to ***Services > Web Proxy > Access Log.*** Check the firewall logs to ensure that the website access is not logged as blocked.	The Application should be accessible without any restrictions. The Application should be rendered properly. The firewall logs should not show any blocked entries for allowed websites 	
Overall Test Result	Pass: □	Fail: □	

4.8.7.4 Block access to malicious content or websites

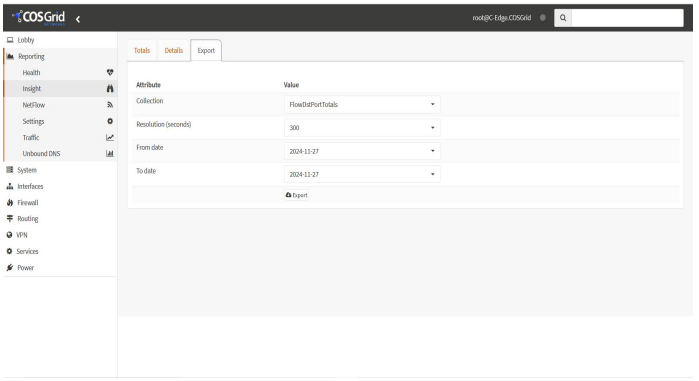
Test ID	**4.8.7.4 Block access to malicious content or websites**		
Requirement	Blocks access to websites and effective control		
Test Objective	Verify that the COSGrid Firewall effectively blocks access to websites based on configured filtering rules.		**Remarks**
Test Description	**Set Steps**	**Acceptance 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. Check for a clear and informative message indicating that the website is blocked. Go to ***Services > Web Proxy > Access Log.*** Inspect the firewall logs to confirm that the website access attempt was logged as	The website should be inaccessible. A clear blocking message should be displayed. The firewall logs should accurately reflect the blocked access attempt.   	

Test ID	**4.8.7.4 Block access to malicious content or websites**		
	blocked.		
Overall Test Result	Pass: □	Fail: □	

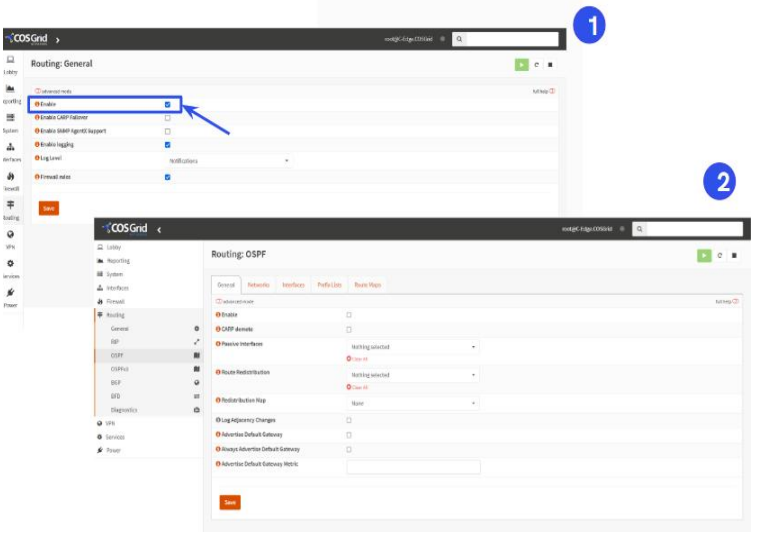
4.8.7.5 Detailed reporting and network visibility

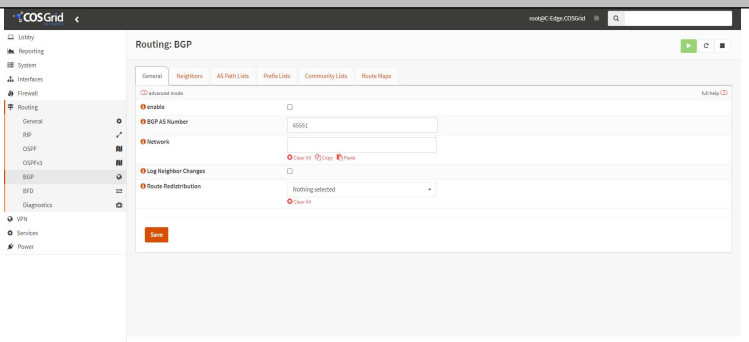
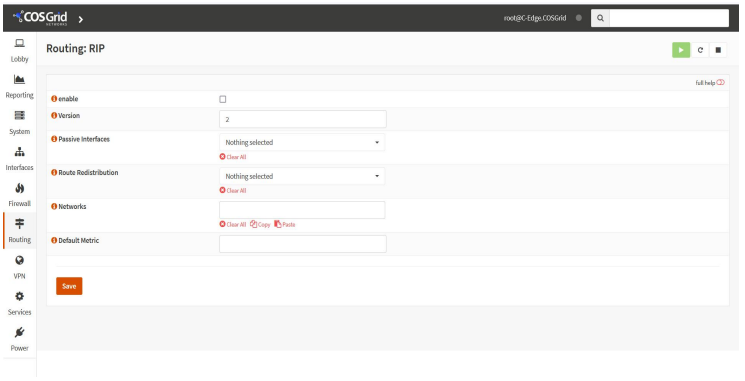
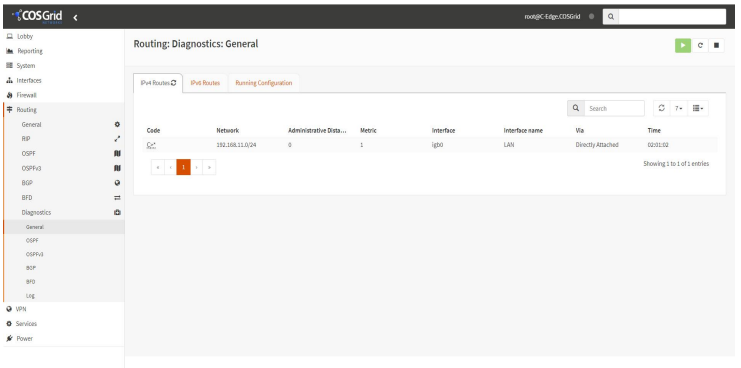
Test ID	**4.8.7.5 Detailed reporting and network visibility**		
Requirement	Verify the monitor and management compliance		
Test Objective	To check the Network Visibility support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Reporting > Traffic > Top Talkers.*** Generate various types of network traffic Go to ***Reporting > Insight***.Utilize visual tools to observe traffic flows, including ● Source and destination devices ● Application types ● Traffic volumes ● Bandwidth utilization Go to ***Reporting > Insight > Details***. Filter and drill down into specific traffic patterns for detailed analysis.	Detailed Network Visibility Full network visibility of different interface traffic Clear and informative visual representations of network traffic flows. Should be able to use **filters** and see **detailed** traffic information. 	
Overall Test Result	Pass: □	Fail: □	

4.8.7.5 Detailed reporting and network visibility

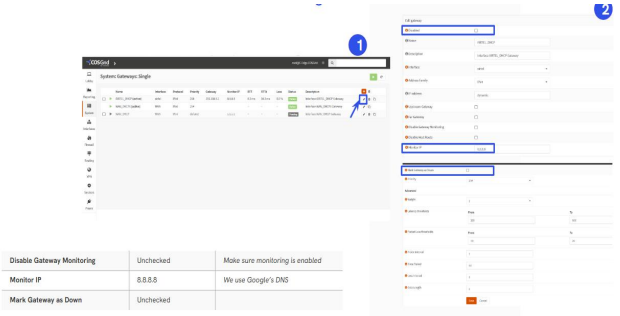
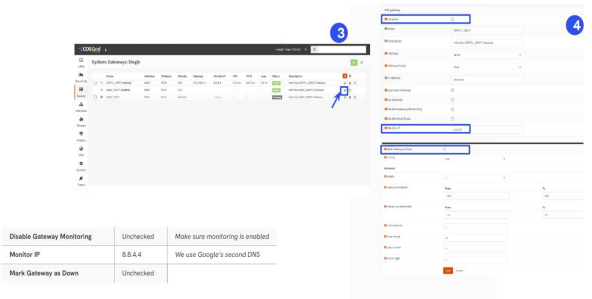
Test ID	**4.8.7.5 Detailed reporting and network visibility**		
Requirement	Ensure the accessibility and customization of reports to meet user needs		
Test Objective	Verify the accuracy, completeness, clarity, and usefulness of reports generated by the COSGrid Firewall		**Remarks**
Test Description	**Set 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. 	
Overall Test Result	Pass: □	Fail: □	

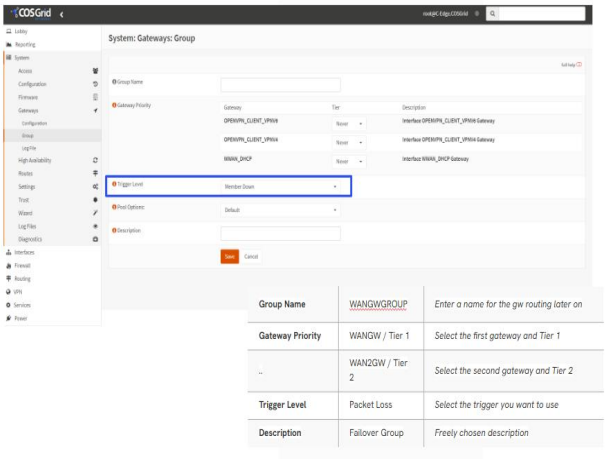
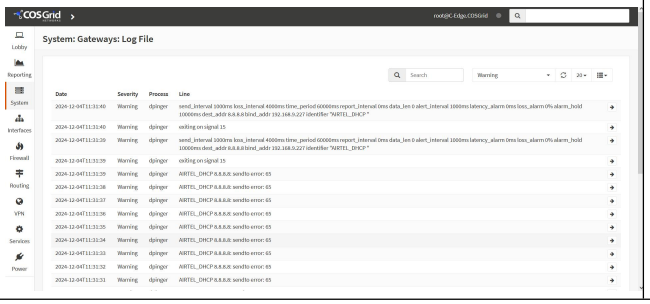
4.8.8.1 Dynamic routing (OSPF/BGP/RIP)

Test ID	**4.8.8.1 Dynamic routing (OSPF/BGP/RIP)**		
Requirement	Ensure the Network features enhance network performance, manage traffic efficiently, and prioritize critical applications.		
Test Objective	Verify the correct configuration and functionality of routing		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	To enable Routing Go to ***Routing > General.*** Then, Go to ***Routing > OSPF or BGP or RIP*** Configure a dynamic routing protocol (e.g., OSPF, BGP, RIP) Test neighbor establishment, route exchange, and route convergence. Simulate network changes and observe dynamic route updates. Go to ***Routing > Diagnostics > General***.	Should be able to configure routing with different functionalities like **CARP and AS Number.** Check the running configuration (**mentioned in Set step 3**) You should be able to see the routing configuration and which configuration in running (**Running Configuration** tab) 	

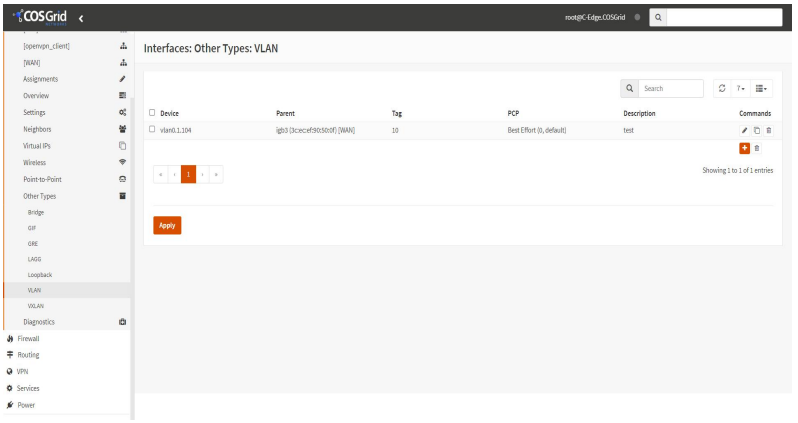
Test ID	4.8.8.1 Dynamic routing (OSPF/BGP/RIP)	
		  
Overall Test Result	Pass: □	Fail: □

4.8.8.2 Load-Balancing and ECMP

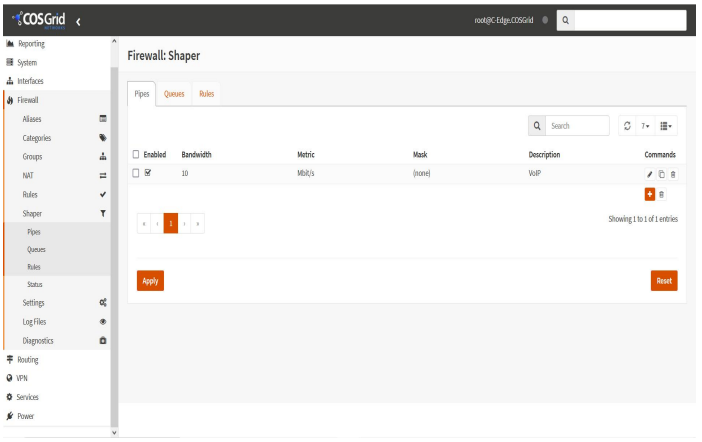
Test ID	4.8.8.2 Optional: Granular network access policies		
Requirement	Verify the network load balancing		
Test Objective	Verify the correct configuration and functionality of load balancing		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***System ‣ Gateways ‣ Configuration*** and click on the pencil symbol to edit the first & second gateway. Now make sure the following is configured Go to ***Systems > Gateways > Group.*** Configure load balancing for multiple servers or services. To setup load balancing follow the same configuration procedure as for Failover, choose same **Tier** for both Gateways This will change the behavior from failover to equal balancing between the two gateways. Go to **System ‣ Settings ‣ General** and make sure	It should show **"online"** in the general table. It should **show equal distribution.**   	

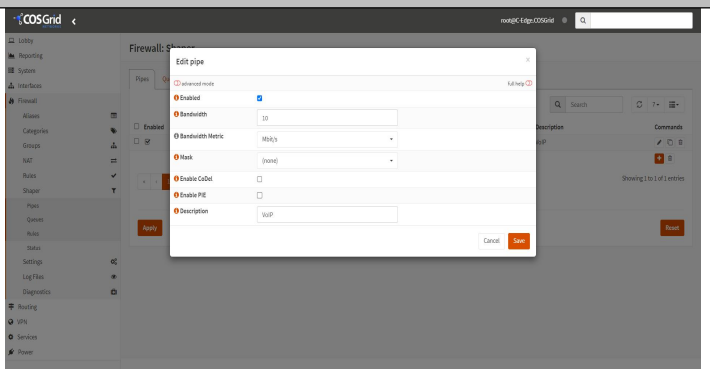
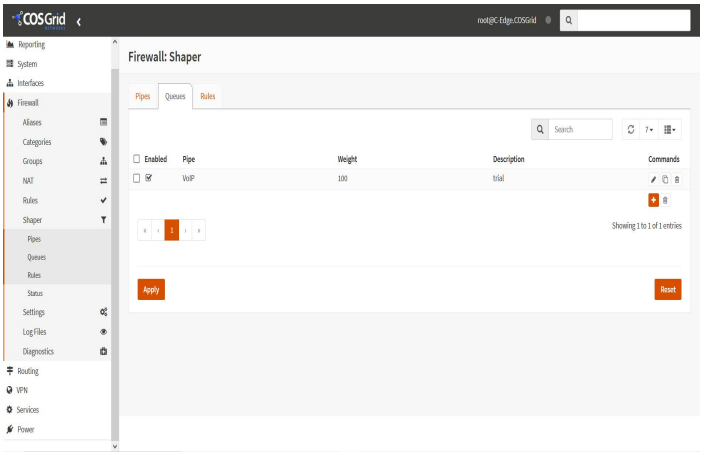
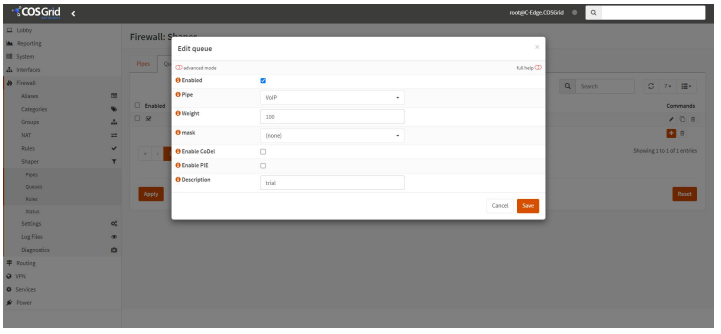
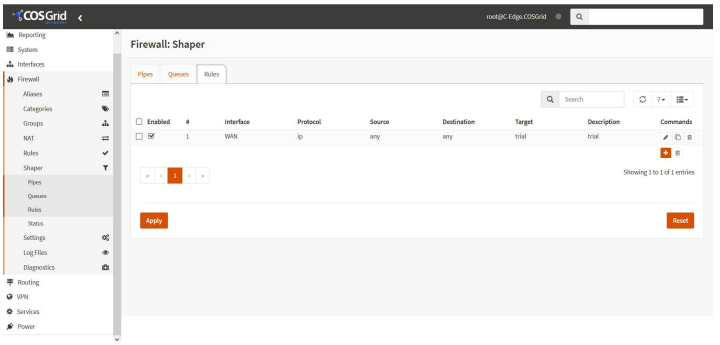
Test ID	**4.8.8.2 Optional: Granular network access policies**	
	each gateway has its own DNS setup: like this: DNS servers 8.8.8.8 WANGW 8.8.4.4 WAN2GW Go to ***Systems > Gateways > Log File.*** Verify equitable distribution of traffic across servers.	 
Overall Test Result	Pass: □	Fail: □

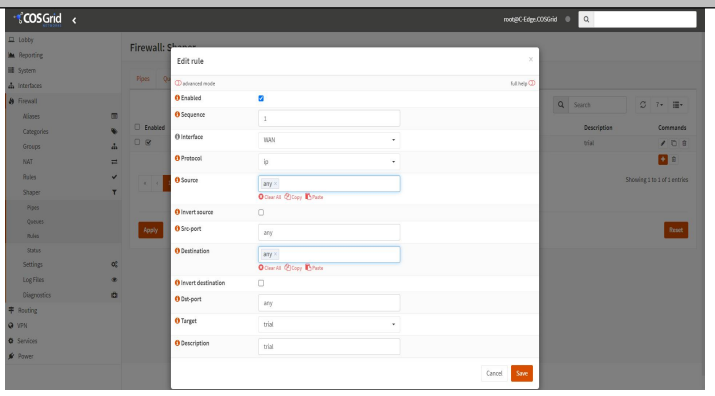
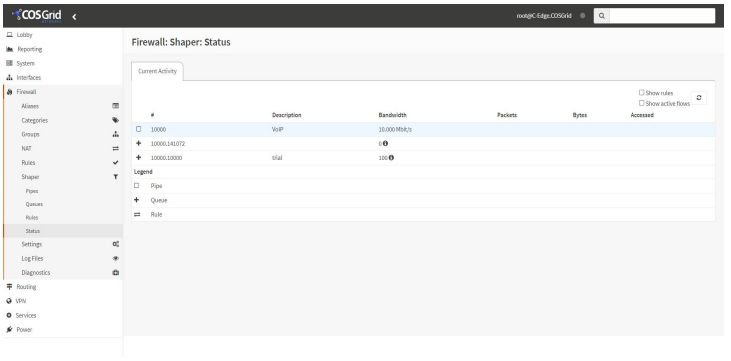
4.8.8.3 802.1Q VLAN and Layer2 switching support

Test ID	**4.8.8.3 802.1Q VLAN and Layer2 switching support**		
Requirement	Verify the VLAN and Switching compliances		
Test Objective	To check the VLAN and Switching support		**Remarks**
Test Description	**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 	
Overall Test Result	Pass: □	Fail: □	

4.8.8.4 Rich traffic/shaping QOS support

Test ID	**4.8.8.4 Rich traffic/shaping QOS support**		
Requirement	Verify the QoS and Network Traffic		
Test Objective	To check the Network Traffic		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Firewall > Shaper > Pipes.*** Define a Pipe with your desired **Bandwidth and its metric**. Go to ***Firewall > Shaper > Queue.*** Define a Queue that **refers to your pipe**. Go to ***Firewall > Shaper > Rule.*** Define a Rule with **interface, source and ports**. Go to ***Firewall > Shaper > Status.*** Check the status.	You should be able to see the status of Pipe (**mentioned in Set Step 4**) Should be able to see the queue and its referred pipe in status. Should be able to see the status when the **show rules option is checked**. Should be able to check activity of **Pipes, Queues, Rules and their Packet Flow**. 	

Test ID	4.8.8.4 Rich traffic/shaping QOS support		
			
			
			
			

Test ID	**4.8.8.4 Rich traffic/shaping QOS support**		
		 	
Overall Test Result	Pass: □	Fail: □	

4.8.8.5 Dynamic routing over VPN (e.g. OSPF)

Test ID	**4.8.8.5 Dynamic routing over VPN (e.g. OSPF)**		
Requirement	Dynamic routing over VPN (e.g. OSPF)		
Test Objective	Assess the Dynamic routing over VPN (e.g. OSPF)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Configure the VPN -OpenVPN/ 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	
Overall Test Result	Pass: □	Fail: □	

Section 4.9 Server 1 with 5G Core, IMS and NMS software

S.no	Description
4.9.1	Processor
4.9.2	Memory
4.9.3	Storage
4.9.4	Operating System And Virtualization Software
4.9.5	Network Interface
4.9.6	PCIe Slots
4.9.7.1	Support out of band upgrades, Agentless out-of-band management, integrateddiagnostics and Power monitoring, Virtual Media, HTML5 remote control.
4.9.7.2	The server should support industry standard management protocols i.e. IPMI, Red Fish API etc.
4.9.7.3	One 1-Gbps RJ-45 management port
4.9.7.4	Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc.
4.9.7.5	Auto generated technical support logs and forwarding to technical support for faster resolution.
4.9.7.6	Automated hardware configuration and Operating System deployment to multiple servers
4.9.7.7	The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues
4.9.7.8	The proposed management solution should analyze current configurations & identify potential issues due to driver & firmware incompatibility
4.9.7.9	The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status
4.9.7.10	The server should support multiple management interfaces including web user interface and command line interface.
4.9.8.1	The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 104-2 validated) or equivalent.
4.9.8.2	Server management system should provide anticounterfeit
4.9.8.3	The server should provide hardware policy based security, Detection of anyConfiguration drifts
4.9.8.4	The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letterhead)
4.9.8.5	The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent

4.9.1 Processor

Test ID	**4.9.1 Processor**		
Requirement	3th Generation Intel® Xeon Gold 2.1 GHz or equivalent 24 Core (minimum). Each servers with minimum 1 Processors and 2 Socket or higher as required.		
Test Objective	Verify the Processors in server1		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	by Google chrome Ip address:192.168.15.50:10000 User Name:support Password:(Support@817&&) Go to>System Information>Processor information	Intel(R) Xeon(R) Gold 5317 CPU @ 3.00GHz, 48 cores	

Test ID	4.9.1 Processor		
Overall Test Result	Pass: □	Fail: □	

4.9.2 Memory

Test ID	4.9.2 Memory		
Requirement	To verify server memory DDR4 or above 64 GB scalable upto 256 GB or above		
Test Objective	To Verify Server Memory		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	by Google chrome Ip address:192.168.15.50:10000 User Name:support Password:(Support@817&&) Go to>System Information>Processor information	server memory DDR4 or above 64 GB	
Overall Test Result	Pass: □	Fail: □	

4.9.3 Storage

Test ID	4.9.3 Storage		
Requirement	To verify server storage SAS SSD Storage = 1TB		
Test Objective	To Verify Server Storage		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	by Google chrome Ip address:192.168.15.50:10000 User Name:support Password:(Support@817&&)	storage SAS SSD Storage = 1TB	

Test ID	**4.9.3 Storage**		
	Go to>System Information>Processor information		
Overall Test Result	Pass: □	Fail: □	

4.9.4 Operating System And Virtualization Software

Test ID	**4.9.4 Operating System And Virtualization Software**		
Requirement	To verify Operating System And Virtualization Software		
Test Objective	Verify OS and VS		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Login serverby Ip address:192.168.60.50 User Name:root Password:(in server IDreck password at service tag)	Go to search bar and search **virtual machine** **Open virtual machine and see the different virtual machine**	**OS Linux machines also have virtualization enabled.**

Test ID	4.9.4 Operating System And Virtualization Software		
	Open virtual consol Host machine screen is come and login through these credential **User: support** **Pass: Support@817&&**		
Overall Test Result	Pass: □	Fail: □	

4.9.5 Network Interface

Test ID	4.9.5 Network Interface		
Requirement	To verify Dual port 1G SFP+ card, 4 x 1G BaseT		
Test Objective	Verify Physically Network Interface		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify physical network interfaces.	Dual port 10G SFP+ card, 4 x 1G BaseT	
Overall Test Result	Pass: □	Fail: □	

4.9.6 PCIe Slots

Test ID	4.9.6 PCIe Slots		
Requirement	To verify PCIe Slots		
Test Objective	To verify PCIe Slots		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Kindly check Physically Network Interface	Minimum 4 x PCIe 16x 4.0 slots for I/O Connectivity or higher as required.	
Overall Test Result	Pass: □	Fail: □	

4.9.7.1Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.

Test ID	**4.9.7.1 Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.**				
Requirement	Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.				
Test Objective	Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to idrac → Maintenance→ system update	To be shown in Idrac			
	Go To idrac setting→ services →Automated System Recovery Agent	To be shown in Idrac			
	Go to configuration → Power management	To be shown in Idrac			
	Go to configuration→ virtual media	To be shown in Idrac			
	Go to maintenance→ trouble shooting .	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.7.2 The server should support industry standard management protocols i.e. IPMI, Red Fish API etc

Test ID	**4.9.7.2 The server should support industry standard management protocols i.e. IPMI, Red Fish API etc**				
Requirement	The server should support industry standard management protocols i.e. IPMI, Red Fish API etc				
Test Objective	The server should support industry standard management protocols i.e. IPMI, Red Fish API etc		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to Idrac setting → services→ redfish .	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.7.3 One 1-Gbps RJ-45 management port

Test ID	**4.9.7.3 One 1-Gbps RJ-45 management port**				
Requirement	One 1-Gbps RJ-45 management port				
Test Objective	One 1-Gbps RJ-45 management port		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Iderc port	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.7.4 One 1-Gbps RJ-45 management port Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc

<table>
<tr><td>Test ID</td><td colspan="4">4.9.7.4 Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc</td></tr>
<tr><td>Requirement</td><td colspan="4">Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc</td></tr>
<tr><td>Test Objective</td><td colspan="2">Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc</td><td colspan="2">Result</td><td rowspan="2">Remarks</td></tr>
<tr><td rowspan="2">Test Description</td><td>Set Steps</td><td>Acceptance Criteria</td><td>OK</td><td>NOK</td></tr>
<tr><td>Go to dashboard</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass: □</td><td colspan="4">Fail: □</td></tr>
<tr><td>Remarks / Comments (If Any)</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Name & Signature</td><td colspan="4">NAME OF VERIFIER</td></tr>
<tr><td colspan="4"></td></tr>
</table>

4.9.7.5 Auto generated technical support logs and forwarding to technical support for faster resolution.

Test ID	**4.9.7.5 Auto generated technical support logs and forwarding to technical support for faster resolution.**				
Requirement	Auto generated technical support logs and forwarding to technical support for faster resolution.				
Test Objective	Auto generated technical support logs and forwarding to technical support for faster resolution.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to Maintenance	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.7.6 Automated hardware configuration and Operating System deployment to multiple servers

Test ID	**4.9.7.6 Automated hardware configuration and Operating System deployment to multiple servers**				
Requirement	Automated hardware configuration and Operating System deployment to multiple servers				
Test Objective	Automated hardware configuration and Operating System deployment to multiple servers		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Explain				
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.7.7 The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues

Test ID	**4.7.7 (g) The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues**				
Requirement	The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues				
Test Objective	The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to configuration→ system security	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.7.8 The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility

Test ID	**4.9.7.8 The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility**				
Requirement	The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility				
Test Objective	The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to dash board → system overview	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.7.9 The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status

Test ID	**4.9.7.9 The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status**				
Requirement	The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status				
Test Objective	The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Debian 10 not supported & its provide alerts				
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.7.10 The server should support multiple management interfaces including web user interface and command line interface.

Test ID	**4.9.7.10 The server should support multiple management interfaces including web user interface and command line interface.**				
Requirement	The server should support multiple management interfaces including web user interface and command line interface.				
Test Objective	The server should support multiple management interfaces including web user interface and command line interface.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Idrac & ssh iderc-ip	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.8.1 The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 104-2 validated) or equivalent.

Test ID	**4.9.8.1 The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 104-2 validated) or equivalent.**				
Requirement	The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 1 0 4 -2 validated) o r equivalent.				
Test Objective	The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 1 0 4 -2 validated) o r equivalent.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Explain				
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.8.2 Se rver management system should provide anti counter feit

Test ID	**4.7.8 (b) Server management system should provide anti counter feit**				
Requirement	Server management system should provide anti counter feit				
Test Objective	Server management system should provide anti counter feit		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.8.3 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.

Test ID	**4.7.8 (c) The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.**				
Requirement	The server should provide hardware policy based security, Detection of any Configuration drifts				
Test Objective	The server should provide hardware policy based security, Detection of any Configuration drifts		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.8.4 The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head)

Test ID	**4.7.8 (d) The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head)**				
Requirement	The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head)				
Test Objective	The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head)		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.9.8.5 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.

<table>
<tr><td>Test ID</td><td colspan="4">4.9.8.5 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.</td></tr>
<tr><td>Requirement</td><td colspan="4">The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.</td></tr>
<tr><td>Test Objective</td><td colspan="2">The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.</td><td colspan="2">Result</td><td rowspan="2">Remarks</td></tr>
<tr><td rowspan="2">Test Description</td><td>Set Steps</td><td>Acceptance Criteria</td><td>OK</td><td>NOK</td></tr>
<tr><td>Open this thing on Google</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass: □</td><td colspan="3">Fail: □</td></tr>
<tr><td>Remarks / Comments (If Any)</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Name & Signature</td><td colspan="4">NAME OF VERIFIER</td></tr>
<tr><td colspan="4"></td></tr>
</table>

Section 4.10 Server 2 with 5G MEC Platform and Application Server

S.no	Description
4.10.1	Processor
4.10.2	Memory
4.10.3	Storage
4.10.4	Operating System And Virtualization Software
4.10.5	Network Interface
4.10.6	PCIe Slots
4.10.8.1	Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.
4.10.8.2	The server should support industry standard management protocols i.e. IPMI, Red Fish API etc.
4.10.8.3	One 1-Gbps RJ-45 management port
4.10.8.4	Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc.
4.10.8.5	Auto generated technical support logs and forwarding to technical support for faster resolution.
4.10.8.6	Automated hardware configuration and Operating System deployment to multiple servers
4.10.8.7	The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues
4.10.8.8	The proposed management solution should analyze current configurations & identify potential issues due to driver & firmware incompatibility
4.10.8.9	The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status
4.10.8.10	The server should support multiple management interfaces including web user interface and command line interface.
4.10.9.1	The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 104-2 validated) or equivalent.
4.10.9.2	Server management system should provide anticounterfeit
4.10.9.3	The server should provide hardware policy based security, Detection of anyConfiguration drifts
4.10.9.4	The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letterhead)
4.10.9.5	The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent

4.10.1 Processor

Test ID	4.10.1 Processor		
Requirement	To verify server 2 Processor		
Test Objective	Processor detail		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	by Google chrome Ip address:192.168.15.51:10000 User Name:support Password:(Support@817&&) Go to>System Information>Processors	Intel(R) Xeon(R) Gold 5317 CPU @ 3.00GHz, 48 cores	
Overall Test Result	Pass: □	Fail: □	

4.10.2 Memory

Test ID	4.10.2 Memory		
Requirement	Verify Server Memory DDR5-4800 or higher, 128 GB scalable upto 512 GB		
Test Objective	To Verify Server Memory		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	by Google chrome Ip address:192.168.15.51:10000 User Name:support Password:(Support@817&&) Go to>System Information>Processor information	DDR5-4800 or higher, 128 GB scalable upto 512 GB	
Overall Test Result	Pass: □	Fail: □	

4.10.3 Storage

Test ID	**4.10.3 Storage**		
Requirement	Verify Server Storage SAS SSD Storage = 4TB Usable expandable to 8 TB or above		
Test Objective	To Verify Server Storage		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	by Google chrome Ip address:192.168.15.51:10000 User Name:support Password:(Support@817&&) Go to>System Information>Processor information	SAS SSD Storage = 6TB Usable expandable to 8 TB or above	
Overall Test Result	Pass: □	Fail: □	

4.10.4 Operating System And Virtualization Software

Test ID	**4.10.4** Operating System And Virtualization Software		
Requirement	To verify Operating System And Virtualization Software		
Test Objective	Verify OS and VS		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Login serverby Ip address:192.168.60.51 User Name:root Password:(in server IDreck password at service tag) **Open virtual consol** Host machine screen is come and login through these credential **User: support** **Pass: Support@817&&**	Go to search bar and search **virtual machine** **Open virtual machine and see the different virtual machine**	**OS Linux machines also have virtualization enabled.**
Overall Test Result	Pass: □	Fail: □	

4.10.5 Network Interface

Test ID	**4.10.5 Network Interface**		
Requirement	To verify Dual port 1G SFP+ card, 4 x 1G BaseT		
Test Objective	Verify Physically Network Interface		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Kindly check Physically Network Interface.	Dual port 10G SFP+ card, 4 x 1G BaseT	
Overall Test Result	Pass: □	Fail: □	

4.10.6 PCIe Slots

Test ID	**4.10.6 PCIe Slots**		
Requirement	To verify PCIe Slots		
Test Objective	To verify PCIe Slots		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Kindly check Physically Network Interface	Minimum 4 x PCIe 16x 4.0 slots for I/O Connectivity or higher as required	
Overall Test Result	Pass: □	Fail: □	

4.10.8.1Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.

Test ID	**4.10.8.1 Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.**				
Requirement	Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.				
Test Objective	Support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring, Virtual Media, HTML5 remote control.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to idrac → Maintenance→ system update Go To idrac setting→ services →Automated System Recovery Agent Go to configuration → Power management Go to configuration→ virtual media Go to maintenance→ trouble shooting .	To be shown in Idrac To be shown in Idrac To be shown in Idrac To be shown in Idrac To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.8.2 The server should support industry standard management protocols i.e. IPMI, Red Fish API etc

Test ID	**4.10.8.2 The server should support industry standard management protocols i.e. IPMI, Red Fish API etc**				
Requirement	The server should support industry standard management protocols i.e. IPMI, Red Fish API etc				
Test Objective	The server should support industry standard management protocols i.e. IPMI, Red Fish API etc		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to Idrac setting → services→ redfish .	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.8.3 One 1-Gbps RJ-45 management port

Test ID	**4.10.8.3 One 1-Gbps RJ-45 management port**				
Requirement	One 1-Gbps RJ-45 management port				
Test Objective	One 1-Gbps RJ-45 management port		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Iderc port	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.8.4 One 1-Gbps RJ-45 management port Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc

<table>
<tr><td>Test ID</td><td colspan="4">4.10.8.4 Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc</td></tr>
<tr><td>Requirement</td><td colspan="4">Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc</td></tr>
<tr><td>Test Objective</td><td colspan="2">Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP etc</td><td colspan="2">Result</td><td rowspan="2">Remarks</td></tr>
<tr><td rowspan="2">Test Description</td><td>Set Steps</td><td>Acceptance Criteria</td><td>OK</td><td>NOK</td></tr>
<tr><td>Go to dashboard</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass: □</td><td colspan="4">Fail: □</td></tr>
<tr><td>Remarks / Comments (If Any)</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Name & Signature</td><td colspan="4">NAME OF VERIFIER</td></tr>
<tr><td colspan="4"></td></tr>
</table>

4.10.8.5 Auto generated technical support logs and forwarding to technical support for faster resolution.

Test ID	**4.10.8.5 Auto generated technical support logs and forwarding to technical support for faster resolution.**				
Requirement	Auto generated technical support logs and forwarding to technical support for faster resolution.				
Test Objective	Auto generated technical support logs and forwarding to technical support for faster resolution.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to Maintenance	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.8.6 Automated hardware configuration and Operating System deployment to multiple servers

<table>
<tr><td>Test ID</td><td colspan="4">4.10.8.6 Automated hardware configuration and Operating System deployment to multiple servers</td></tr>
<tr><td>Requirement</td><td colspan="4">Automated hardware configuration and Operating System deployment to multiple servers</td></tr>
<tr><td>Test Objective</td><td colspan="2">Automated hardware configuration and Operating System deployment to multiple servers</td><td colspan="2">Result</td><td rowspan="2">Remarks</td></tr>
<tr><td rowspan="2">Test Description</td><td>Set Steps</td><td>Acceptance Criteria</td><td>OK</td><td>NOK</td></tr>
<tr><td>Explain</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass: □</td><td colspan="4">Fail: □</td></tr>
<tr><td>Remarks / Comments (If Any)</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Name & Signature</td><td colspan="4">NAME OF VERIFIER</td></tr>
<tr><td colspan="4"></td></tr>
</table>

4.10.8.7 The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues

<table>
<tr><td>Test ID</td><td colspan="4">4.10.8.7 The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues</td></tr>
<tr><td>Requirement</td><td colspan="4">The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues</td></tr>
<tr><td>Test Objective</td><td colspan="2">The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues</td><td colspan="2">Result</td><td rowspan="2">Remarks</td></tr>
<tr><td rowspan="2">Test Description</td><td>Set Steps</td><td>Acceptance Criteria</td><td>OK</td><td>NOK</td></tr>
<tr><td>Go to configuration→ system security</td><td>To be shown in Idrac</td><td></td><td></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass: □</td><td colspan="3">Fail: □</td></tr>
<tr><td>Remarks / Comments (If Any)</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Name & Signature</td><td colspan="4">NAME OF VERIFIER</td></tr>
<tr><td colspan="4"></td></tr>
</table>

4.10.8.8 The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility

Test ID	**4.10.8.8 The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility**				
Requirement	The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility				
Test Objective	The proposed management solution should analyse current configurations & identify potential issues due to driver & firmware incompatibility		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Go to dash board → system overview	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.8.9 The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status

Test ID	**4.10.8.9 The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status**				
Requirement	The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status				
Test Objective	The management system should report validation based on compatibility of server model, processor, firmware, adapters, operating system and drivers & share compliance status		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Debian 10 not supported & its provide alerts				
Overall Test Result	Pass: ☐	Fail: ☐			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.8.10 The server should support multiple management interfaces including web user interface and command line interface.

Test ID	**4.10.8.10 The server should support multiple management interfaces including web user interface and command line interface.**				
Requirement	The server should support multiple management interfaces including web user interface and command line interface.				
Test Objective	The server should support multiple management interfaces including web user interface and command line interface.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Idrac & ssh iderc-ip	To be shown in Idrac			
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.9.1 The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 104-2 validated) or equivalent.

Test ID	**4.10.9.1 The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 104-2 validated) or equivalent.**				
Requirement	The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 1 0 4 -2 validated) o r equivalent.				
Test Objective	The server should provide cryptographic firmware updates, (Every SW upgrade will be FIPS 1 0 4 -2 validated) o r equivalent.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Explain				
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.9.2 Server management system should provide anti counter feit

Test ID	**4.10.9.2 Server management system should provide anti counter feit**				
Requirement	Server management system should provide anti counter feit				
Test Objective	Server management system should provide anti counter feit		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.9.3 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.

Test ID	**4.10.9.3 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.**				
Requirement	The server should provide hardware policy based security, Detection of any Configuration drifts				
Test Objective	The server should provide hardware policy based security, Detection of any Configuration drifts		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.9.4 The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head)

Test ID	**4.10.9.4 The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head)**				
Requirement	The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head)				
Test Objective	The proposed server OEM should certify malicious code free design (undertaking to be submitted on OEM letter head)		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

4.10.9.5 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.

Test ID	**4.10.9.5 The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.**				
Requirement	The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.				
Test Objective	The server should provide Hardware root of trust for Secure Boot Image Failsafe as per NIST SP800-147(B) or equivalent.		**Result**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	**OK**	**NOK**	
	Open this thing on Google				
Overall Test Result	Pass: □	Fail: □			
Remarks / Comments (If Any)					
Name & Signature	**NAME OF VERIFIER**				

Section 4.11 5G rewriteable SIM (programmable)

Test ID	**4.11**		
Requirement			
Test Objective			**Remarks**
Test	**Set Steps**	**Acceptance Criteria**	

Test ID	**4.11**		
Description			
Overall Test Result	Pass: □	Fail: □	

Section 4.12 5G Evaluation Board

S.no	Description
4.12.a	RG520F 5G Module
4.12.b	4 Cellular Modem-RF
4.12.c	Performance Enhancement Technologi
4.12. d	Physical and Wi-Fi Interface Modules.
4.12.e	UART, SPI, I2C and GPIO Interface
4.12 f	Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications
4.12.g	SD Card Connector

4.12.h	PCIe to USB Connector
4.12.i	Dual (U)SIM card supported
4.12.j	1 digital audio codec board interface
4.12.k	Debug URAT
4.12.l	USB Type C Interface
4.12.m	LEDs indication
4.12.n	Power key, Reset key, USB Boot, Power Switch
4.12.o	12 Antenna Interfaces
4.12.p	Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors
4.12.q	AT command (external MCU integration) and SDK support (within the module)
4.12.r	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech
4.12.a	Quectel RG520F 5G Module
4.12.b	Cellular Modem-RF
4.12.c	Performance Enhancement Technologies
4.12.d	Physical and Wi-Fi Interface Modules
4.12.e	UART, SPI, I2C and GPIO Interface
4.12.f	Sensor interfaces for medical devices, smart-home appliances and smart-city applications
4.12.g	SD Card Connector
4.12.h	PCI to USB Connector
4.12.i	Dual (U)SIM card supported
4.12.j	1 digital audio codec board interface
4.12.k	COM1 and COM2. Also support Main URAT, Debug URAT
4.12.l	USB Type C
4.12.m	LEDs indication
4.12.n	Power key, Reset key, USB Boot, Power Switch
4.12.o	12 Antenna Interface
4.12.p	Minimum Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors
4.12.q	AT command (external MCU integration) and SDK support (within the module)
4.12.r	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc.

4.12.a RG520F 5G Module

Test ID	**4.12.a RG520F 5G Module**		
Requirement	RG520F Modem		
Test Objective	To verify RG520F Modem		Remarks
Test	Set Steps	Acceptance Criteria	

Description	RG520F Modem 1. Open the up plate and heat sink of5G Evb . 2. The modem is connect with 5G Evolution board.		
Overall Test Result	Pass: □	Fail: □	

4.12.b Cellular Modem-RF

Test ID	**4.12.b Cellular Modem-RF**		
Requirement	Cellular Modem-RF RG520F		
Test Objective	To verify 100 MHz carrier aggregation (DL) andabove, 100/200 MHz bandwidth		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Cellular Modem-RFRG520F		**1. Carrier aggregation and bandwidt h verified from data sheet**
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.c Performance Enhancement Technologies

Test ID	**4.12.c Performance Enhancement Technologies**		
Requirement	RG520F Modem		
Test Objective	To verify 100 MHz envelope tracking	**Remarks**	

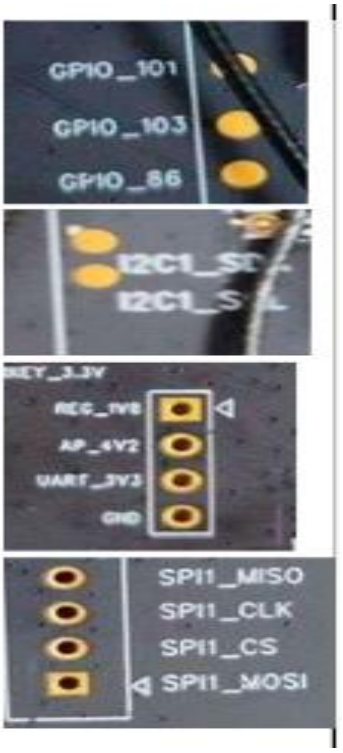
Test Description	**Set Steps** • RG520F Modem	**Acceptance Criteria** 	**1 can be check by modem's datasheet.**
Overall Test Result	Pass: ☐	Fail: ☐	

4.12. d Physical and Wi-Fi Interface Modules.

Test ID	**4.12. d Physical and Wi-Fi Interface Modules.**		
Requirement	FC60E Module		
Test Objective	To verify Physical and Wi-Fi Interface Modules.		**Remarks**
Test Description	**Set Steps** FC60E Module 1 Open the 5G Evb up plate of box 2 the Wi-Fi Interface Module is connected on the Evb.	**Acceptance Criteria**  	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.e UART, SPI, I2C and GPIO Interface

Test ID	**4.12.e UART, SPI, I2C and GPIO Interface**	
Requirement	UART , SPI, I2C and GPIO Interface	
Test Objective	To verify UART , SPI, I2C and GPIO interface	**Remarks**

Test Description	**Set Steps**	**Acceptance Criteria**	
	• GPIO • I2C • SPI • UART		1 Open the 5G Evb up plateof box. 2 all the interfaces are left side of the board.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12 f Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications

Test ID	**4.12. f Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications**

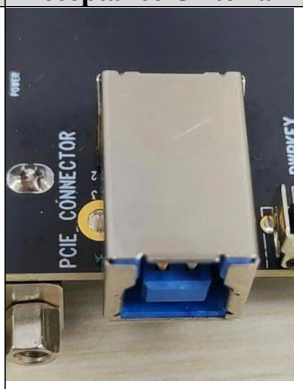
Requirement	Sensor Interfaces		
Test Objective	Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Sensors interfaces can be performed by 5G or Wi-Fi interfaces.	1 the sensor can connect withthe Wi-Fi or Cellular of Evb and it can monitor & manage with help of 5G Evb	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.g SD Card Connector

Test ID	**4.12.g SD Card Connector**		
Requirement	SD Card Connector		
Test Objective	To verify SD Card Connector		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. SD Card		1. The SD card can see on the right side of 5G Evb.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.h PCIe to USB Connector

Test ID	**4.12.h PCIe to USB Connector**	
Requirement	PCI to USB Connector	
Test	To verify PCI to USB Connector	

Objective			
Test Description	**Set Steps**	**Acceptance Criteria**	**Remarks**
	• PCIe to USB connector		1 The PCIE to USB connector is shown on front side of 5G Evb.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.i Dual (U)SIM card supported

Test ID	**4.12.i Dual (U)SIM card supported**		
Requirement	Dual (U)SIM card		
Test Objective	To Verify Dual (U)SIM card supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• USIM card 1 & • USIM card 2	 	1 the sim card slot are left side 2 chech the sim status using standard AT command tester Application on “sim status”.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12j Digital audio codec board interface

Test ID	**4.12.j 1 digital audio codec board interface**	
Requirement	1 digital audio codec board interface	
Test Objective	To Verify 1 digital audio codec board interface	**Remarks**

Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Digital audio codec board		Open the top plate of 5G Evb and see left side of board**.**
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.k Debug URAT

Test ID	**4.12.k Debug URAT**	
Requirement	Debug URAT	
Test	To verify Debug URAT	

Objective			Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	
	• UART & • Debug UART	 	Both debug port shown in front side of 5G Evb.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.l USB Type C Interface

Test ID	**4.12.l USB Type C Interface**		
Requirement	USB Type C Interface		
Test Objective	To Verify USB Type C Interface		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• USB Type C interface		1. The USB type c interface is shown right side of 5G Evb 2. Connect the type c Data cable to use the 5GEvb with your PC.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.m LEDs indication

Test ID	**4.12.m LEDs indication**
Requirement	LEDs lights

Test Objective	To Verify LEDs indication		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• LEDs lights		1. LEDs are top on the board 2 open Top plate of 5G Evb box the LEDs are below theWi-Fi card. 3 when board is power up the power LED (Red light) on. And other LEDs are on when the corresponding work do.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.n Power key, Reset key, USB Boot, Power Switch

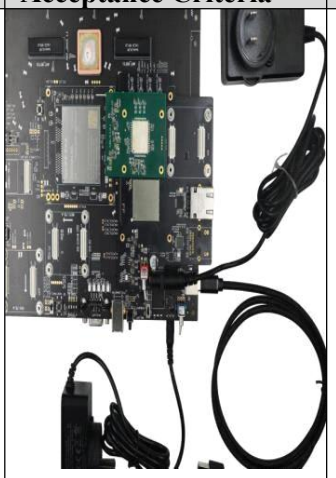
Test ID	**4.12.n Power key, Reset key, USB Boot, Power Switch**		
Requirement	Power key, Reset key, USB Boot, Power Switch		
Test Objective	To Verify Power key, Reset key, USB Boot, Power Switch		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• Power Key • Reset key • USB boot • Power switch		1. All the keys are top on theboard to see open the Top plate of 5G Evb. 2. The functionality will check according the us of the keys.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.o 12 Antenna Interfaces

Test ID	**4.12.o 12 Antenna Interfaces**

Requirement	12 Antenna (8 cellular, 2 Wi-Fi & 2GPS)		
Test Objective	To verify 12 Antenna Interfaces		**Remarks**
Test Description	• ANT0, ANT1 700 MHz–6 GHz ANT2–ANT7 1.7 GHz–6 GHz		1 Open the top plate of 5G Evb and antenna are mounted on board at three side. 2 The frequency is written on antenna
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.p Cables Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi,Ethernet, Audio, PCI TO USB, Power Adaptors

Test ID	**4.12.p Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors**		
Requirement	Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors		
Test Objective	To verify these cables		**Remarks**
Test Description	**Set Steps** 1. Cables 2. Antenna 3. Power adaptors 4. Wi-Fi Ethernet 5. PCI TO USB 6. Audio earphone	**Acceptance Criteria** 	1. the cable are provided with 5g Evb a . Power adapter b. Audio earphone c. PCI to USB cable d. Type C data cable e. UAR T debugging cable f. Antenna and wifi mounted on board.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.q AT command (external MCU integration) and SDK support (within the module

Test ID	**4.12.q AT command (external MCU integration) and SDK support (within the module)**		
Requirement	At command (external MCU integration) and SDK support (within the module)		
Test Objective	At command (external MCU integration) and SDK support (within the module)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Supported by both the module	1. Power up the 5G Evb and connect your pc with Evb using typeC data cable 2. Using a mcu with specific code you can check the manufacturer details at end of mcu.	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech

Test ID	**4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech**		
Requirement	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech		
Test Objective	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
		• You can configure a mcu for smart city or medical devices • You can monitor or manage it by using 5G Evb	1. You can check as per devices
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.a Quectel RG520F 5G Module

Test ID	4.12.a Quectel RG520F 5G Module		
Requirement	RG520F module		
Test Objective	Verify the RG520F 5G module		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• Connect the module to Coral Anubhav Board • Bands tested and result measures	OUTPUT WITH COMMAND ATI Quectel RG520F-EB Revision:RG520FEBDER03A01M4G_OCPU_BETA_20240307A OK ATI Quectel RG520F-EB Revision: RG520FEBDER03A01M4G_OCPU_BETA_20240307A OK • Power up the board and connect with pc using type c cable • Use any standard at command tester for see details of modem using (ATI) command	Power up the board and connect with pc using type c cable . Use any standard at command testerfor see details ofmodem using (ATI) command
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.b Cellular Modem-RF

Test ID	4.12.b Cellular Modem-RF		
Requirement	Verify the RG520F module		
Test Objective	To check the RG520F Module uplink and Downlink in sub 6GHz band		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• Sub 6 GHz band n78 is for bandwidth • Uplink and downlink can be verified by latch process.	• To check the uplink and downlink you can connect the hotspot of the 5G Evb and check the speed using standard network speed site	
Overall Test Result	Pass: ☐	Fail: ☐	

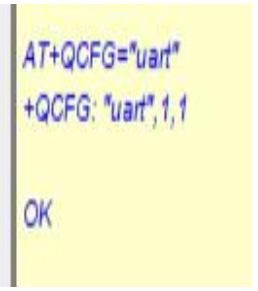
4.12.c Performance Enhancement Technologies

Test ID	4.12.c Performance Enhancement Technologies		
Requirement	Performance Enhancement Technologies		
Test Objective	To verify Performance Enhancement Technologies		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• MIMO(using multiple antenna at the receiver side)	  1.There are multiple antennas of same frequency range are available on board for perform MIMO application 2. To manage MIMO in 5G EVB use following command: - AT+ QNWCFG="dis_4 mimo enable - AT+QNWCFG= "nr5g_4mimo_enable	there are multiple antennas of same frequency range are available on boardfor perform MIMO 
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.d Physical and Wi-Fi Interface Modules

Test ID	4.12.d Physical and Wi-Fi Interface Modules		
Requirement	Quectel FC60E		
Test Objective	Verify Physical and Wi-Fi Interface Modules		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect modem to the system 2. Test data transmission through physical interface 3. Received data correctly on the other hand.	1. Insert the sim and power up the board. 2. Search the Wi-Fi from your PC to connect with ssid of 5G Evb.	Evb wifi is connected with PC
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.e UART, SPI, I2C and GPIO Interface

Test ID	4.12.e UART, SPI, I2C and GPIO Interface		
Requirement	Coral Anubhav board		
Test Objective	To verify UART, SPI, I2C and GPIO		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Baud rate 115200 is used and transmit and receive large amount of data 2. Configure CPOL and CPHA settings, communicate with SPI device 3. Set 2 master on the bus & perform read write operation 4. Configured 1 GPIO as input & 1 GPIO as output results verified at ground	 1. Power up the board and connect with your pc using type c data cable. 2. Check the interfaces by below AT commands AT+QCFG="uart" b other interfaces check if you connect to the board.	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.f Sensor interfaces for medical devices, smart-home appliances and smart-city applications

Test ID	**4.12.f Sensor interfaces for medical devices, smart-home appliances and smart-city applications**		
Requirement	Sensor interfaces for medical devices, smart-home appliances and smart-city applications		
Test Objective	To check sensor interfaces for different-2 application		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connected coral gyan sensor to coral Anubhav & measure soil moisture 2. Collect the data and verified	1. Power up the board 2. Connect coral gyan with hotspot of 5G Evb. 3. You can send the data to your desired API or application using 5G Evb network.	
Overall Test Result	Pass: ☐	Fail: ☐	

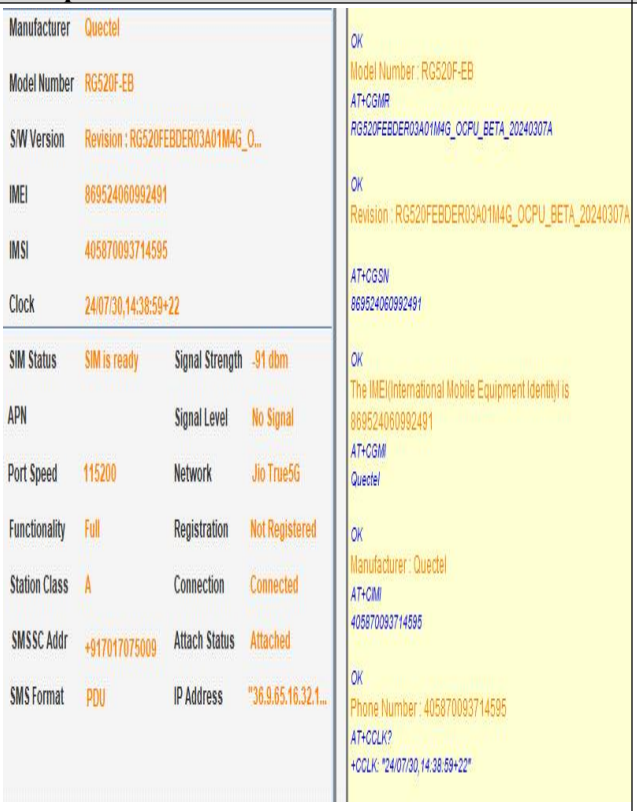
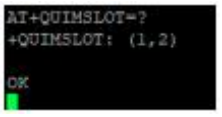
4.12.g SD Card Connector

Test ID	**4.12.g SD Card Connector**		
Requirement	SD card		
Test Objective	To check SD card		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1 Micro SD card support, it can be verified on hardware level	1 Take the access of board using ADB and run"df-h" to see the storage details of board and SD card.	The SD card slot ,right side of 5G Evb.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.h PCI to USB Connector

Test ID	**4.12.h PCI to USB Connector**		
Requirement	PCI to USB Connector		
Test Objective	To verify PCI to USB Connector		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1 Connect the cable to Coral Anubhav 5G board 2. And, it can be verified on hardware level	1. Connect the PCI to USB connector for use of user requirement at PCIE connector. 2. Now user can take the log.	The SD card slot ,right side of 5G Evb.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.i Dual (U)SIM card supported

Test ID	4.12.i Dual (U)SIM card supported		
Requirement	SIM Card Supported		
Test Objective	SIM Card Supported		Remarks
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Insert the sim in port 1 or 2 2. Micro Sim card supported it can be verified on hardware	  1. "AT+QUIMSLOT?" - Query the(U) SIM slot currently used. 2. AT+QUIMSLOT=<slot>.Switch to (U)SIM slot use 2 or 1.	1. Power up the board and connect the type c data cable between your pc and EV board. 2. Use the AT command tester to see the details of sim
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.j 1 digital audio codec board interface

Test ID	**4.12.j 1 digital audio codec board interface**		
Requirement	Codec board		
Test Objective	To check digital audio codec board interface		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Power up the codec board 2. Initialize code using initialization sequence 3. Status of register to confirm successful initialization	 1.Insert the sim and power up the board . 2 Using AT command tester call to a number like this "ATD1234567890;"	Now you can talk above number by using Audio earphone.
Overall Test Result	Pass: ☐	Fail: ☐	

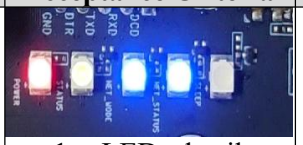
4.12.k COM1 and COM2. Also support Main URAT, Debug URAT

Test ID	**4.12.k COM1 and COM2. Also support Main URAT, Debug URAT**		
Requirement	COM1 and COM2 interfaces		
Test Objective	To check the COM1 and COM2 interfaces		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• Boot up the system • COM1 & COM2 should be detected and listed in the system	1. Power up the board and connect the type c data cable between your pc and EV board. 2. Connect the cable and use the command or logcat to take the log of the 5G Evb.	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.l USB Type C

Test ID	**4.12.l USB Type C**		
Requirement	USB type C cable		
Test Objective	To check USB type C cable		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	• Connect USB type C to Coral Anubhav board • This USB interface is used for AT command communication , data transmission and firmware upgrade.	1. Cable is provided with 5G evb. 2. Power up the board and connect the type c data cable between your pc and EV board. 3. Use the AT command tester to see the details of modem.	
Overall Test Result	Pass: ☐		

4.12.m LEDs indication

Test ID	**4.12.m LEDs indication**		
Requirement	Verify the LEDs indication		
Test Objective	To check the LEDs indication		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Switch on board 2. For all the operation LEDs are blinking	 1. LEDs details a) red led for power up indication b) Green for debug mode c) blue light for registration status d) 2nd blue led show connectivity e.) Last LED light is for sleep mode	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.n Power key, Reset key, USB Boot, Power Switch

Test ID	4.12.n Power key, Reset key, USB Boot, Power Switch		
Requirement	Verify the Power key, Reset key, USB Boot, Power Switch		
Test Objective	To Check Power key, Reset key, USB Boot, Power Switch		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1 Power key, Reset key, USB Boot, Power Switch it can be verified on hardware level 2 After the connection	1. All functionality check by user at hardware level.	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.o 12 Antenna Interface

Test ID	4.12.o 12 Antenna Interface		
Requirement	Supports Sub-6G bands: FR-1, N78		
Test Objective	Supports Sub-6G bands: FR-1, N78		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1 Connect all antenna to the 5G and Wi-Fi module 2 Power on the system 3 Check at result at the other used end like SNR and BER	1. All supported band of antenna for Sub 6GHz are available on board.	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.p Minimum Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors

Test ID	4.12.p **Minimum Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors**		
Requirement	Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors		
Test Objective	Minimum Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1 All cables are connected and verified at hardware level.	All cables are connected and verified at hardware level for different use according to use or requirement.	
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.q AT command (external MCU integration) and SDK support (within the module)

Test ID	**4.12.q AT command (external MCU integration) and SDK support (within the module)**		
Requirement	AT command (external MCU integration) and SDK support (within the module)		
Test Objective	AT command (external MCU integration) and SDK support (within the module)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
		1.By use of MCU use all the supported AT command 2 User want to write a code in mcu for sending AT command and receive the response at default baud rate (115200) at mcu serial monitor.	1.By use of MCU use all the supported AT command 2 User want to write a code in mcu for sending AT command and receive the response at default baud rate (115200) at mcu serial monitor.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc.

Test ID	**4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc.**		
Requirement	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc.		
Test Objective	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect application Microcontroller Unit (MCU) development boards & these are integral to developing and prototyping various IoT (Internet of Things) applications, including smart homes, smart cities, medical devices, and agritech.	1.Using the network of 5G Evb . 2. User can monitor and manage the data of MCUs. 3. For the example user can use coral gyan with 5G Evb. 4.MCU with Linux OS we can integrate easily. Using minicom applications,users can use any suppored command for their use.	1.Using the network of 5G Evb . 2. User can monitor and manage the data of MCUs. 3. For the example user can use coral gyan with 5G Evb.
Overall Test Result	Pass: ☐	Fail: ☐	

4.12.q AT command (external MCU integration) and SDK support (within the module)

Test ID	**4.12.q AT command (external MCU integration) and SDK support (within the module)**		
Requirement	AT command (external MCU integration) and SDK support (within the module)		
Test Objective	AT command (external MCU integration) and SDK support (within the module)		**Remarks**
Test Description	Set Steps	Acceptance Criteria	
	1. Supported by both the module		
Overall Test Result	Pass: □	Fail: □	

4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech

Test ID	**4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech**		
Requirement	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech		
Test Objective	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
Overall Test Result	Pass: □	Fail: □	

4.12.a Quectel RG520F 5G Module

Test ID	4.2.a Quectel RG520F 5G Module		
Requirement	RG520F modem		
Test Objective	Verify the RG520F 5G module		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect the module to Coral Anubhav Board 2. Bands testedand result measures		
Overall Test Result	Pass: □	Fail: □	

4.12.b Cellular Modem-RF

Test ID	4.2.b Cellular Modem-RF		
Requirement	Verify the RG520F module		
Test Objective	To check the RG520F module uplink and downlink insub-6 GHz band and bandwidth		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Sub 6 GHz bandn78 is for bandwidth 2. Uplink and downlink can be verified by latchprocess.		
Overall Test Result	Pass: □	Fail: □	

4.12.c Performance Enhancement Technologies

Test ID	4.2.c Performance Enhancement Technologies		
Requirement	Performance Enhancement Technologies		
Test Objective	To verify Performance Enhancement Technologies		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. MIMO(using multiple antenna at the receiver side)		
Overall Test Result	Pass: □	Fail: □	

4.2.d Physical and Wi-Fi Interface Modules

Test ID	4.2.d Physical and Wi-Fi Interface Modules		
Requirement	Quectel FC60E		
Test Objective	Verify Physical and Wi-Fi Interface Modules		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect modemto the system 2. Test data transmission through physicalinterface 3. Received data correctly on theother hand		
Overall Test Result	Pass: □	Fail: □	

4.12.e UART, SPI, I2C and GPIO Interface

Test ID	4.2.e UART, SPI, I2C and GPIO Interface		
Requirement	Coral Anubhav board		
Test Objective	To verify UART, SPI, I2C and GPIO		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Baud rate 115200 isused and transmit and receive large amount of data 2. Configure CPOLand CPHA settings , communicate withSPI device 3. Set 2 master on the bus & perform readwrite operation 4. Configured 1 GPIOas input & 1 GPIO as output results verified at ground	.	
Overall Test Result	Pass: □	Fail: □	

4.12.f Sensor interfaces for medical devices, smart-home appliances and smart-city application

Test ID	**4.12.f Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications**		
Requirement	Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications		
Test Objective	To check sensor interfaces for different-2 application		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connected coral gyan sensor to coral Anubhav & measure soilmoisture 2. Collect the data and verified		
Overall Test Result	Pass: □	Fail: □	

4.12.g SD Card Connector

Test ID	**4.12.g SD Card Connector**		
Requirement	SD card		
Test Objective	To check SD card		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Micro SD card support, it can be verified on hardware level		
Overall Test Result	Pass: □	Fail: □	

4.12.h PCI to USB Connector

Test ID	**4.12.h PCI to USB Connector**		
Requirement	PCI to USB Connector		
Test Objective	To verify PCI to USB Connector		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect the cable to Coral Anubhav 5G board 2. And, it can be verified on hardware level		
Overall Test Result	Pass: □	Fail: □	

4.12.i Dual (U)SIM card supported

Test ID	4.12.i Dual (U)SIM card supported		
Requirement	SIM Card Supported		
Test Objective	SIM Card Supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Insert the simin port 1 or 2 2. Nano Sim card supported itcan be verified on hardware	Able to access the internet	
Overall Test Result	Pass: □	Fail: □	

4.12.j 1 digital audio codec board interface

Test ID	4.2.j 1 digital audio codec board interface		
Requirement	Codec board		
Test Objective	To check digital audio codec board interface		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Power up thecodec board 2. Initialize codeusing initialization sequence 3. Status of register to confirm successful initialization		
Overall Test Result	Pass: □	Fail: □	

4.12.k COM1 and COM2. Also support Main URAT, Debug URAT

Test ID	4.12.k COM1 and COM2. Also support Main URAT, Debug URAT		
Requirement	COM1 and COM2 interfaces		
Test Objective	To check the COM1 and COM2 interfaces		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Boot up thesystem 2. COM1 & COM2 should be detected andlisted in the system		
Overall Test Result	Pass: □	Fail: □	

4.2.l USB Type C

Test ID	4.2.l USB Type C		
Requirement	USB type C cable		
Test Objective	To check USB type C cable		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect USB type C to Coral Anubhav board 2. This USB interface is used for AT command communication , data transmission and firmware upgrade.		
Overall Test Result	Pass: □		

4.12.m LEDs indication

Test ID	4.12.m LEDs indication		
Requirement	Verify the LEDs indication		
Test Objective	To check the LEDs indication		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Switch onboard 2. For all the operation LEDs are blinking		
Overall Test Result	Pass: □	Fail: □	

4.12.n Power key, Reset key, USB Boot, Power Switch

Test ID	4.2.n Power key, Reset key, USB Boot, Power Switch		
Requirement	Verify the Power key, Reset key, USB Boot, Power Switch		
Test Objective	To Check Power key, Reset key, USB Boot, PowerSwitch		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Power key, Reset key, USBBoot, Power Switch it can be verified on hardware level 2. After the connection		
Overall Test Result	Pass: □	Fail: □	

4.12.o Antenna Interface

Test ID	**4.2.o 12 Antenna Interface**		
Requirement	Supports Sub-6G bands: FR-1, N78		
Test Objective	Supports Sub-6G bands: FR-1, N78		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect all antenna to the5G and Wi-Fimodule 2. Power on thesystem 3. Check at result at the other used end like SNR and BER		
Overall Test Result	Pass: □	Fail: □	

4.2.p Minimum Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors

Test ID	4.2.p **Minimum Cables, Antenna, Audio earphone, USB Driver, Requiredmodules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors**		
Requirement	Cables, Antenna, Audio earphone, USB Driver, Requiredmodules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors		
Test Objective	Minimum Cables, Antenna, Audio earphone, USB Driver, Requiredmodules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. All cables are connected and verified at hardware level.		
Overall Test Result	Pass: □	Fail: □	

4.2.q AT command (external MCU integration) and SDK support (within the module)

Test ID	**4.2.q AT command (external MCU integration) and SDK support (within the module)**		
Requirement	AT command (external MCU integration) and SDK support (within themodule)		
Test Objective	AT command (external MCU integration) and SDK support (within the module)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
Overall Test Result	Pass: □	Fail: □	

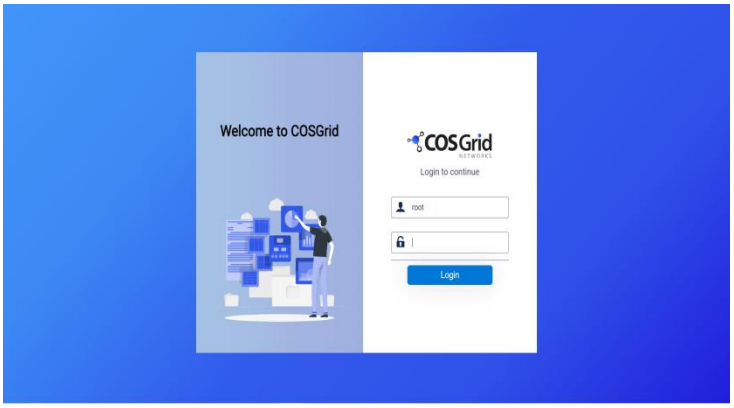
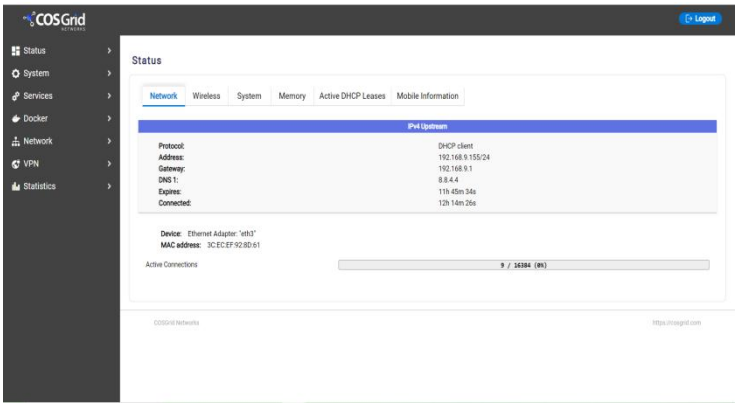
4.2.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc

Test ID	**4.2.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc.**		
Requirement	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc.		
Test Objective	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech etc.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect application Microcontroller Unit (MCU) development boards & these are integral to developing and prototyping various IoT (Internet of Things) applications, including smart homes, smart cities, medical devices, and agritech.		
Overall Test Result	Pass: □	Fail: □	

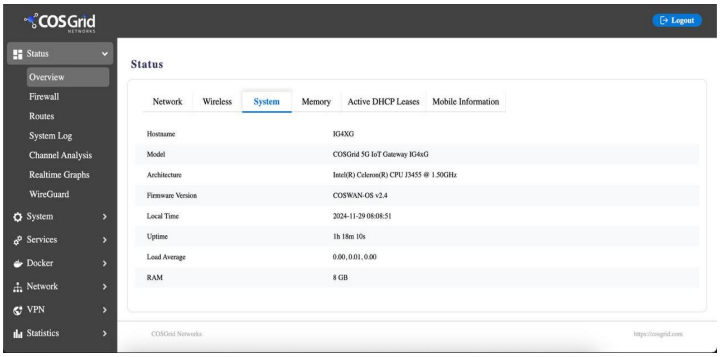
Section 4.13 IOT Gateway

S.no	Description
	Basic Hardware Setup
4.13.1.1	CPU : Qualcomm or equivalent, Dual core or Higher
4.13.1.2	RAM -256 Mb
4.13.1.3	Module: 5G Sub-6Ghz SA 1/2 Gbps DL (4x4 MIMO) or higher , 900/600 Mbps UL (2x2)
4.13.1.4	Status: Signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP Bytes sent/received, connected band, IMSI, ICCID
4.13.1.5	SMS/ Call Status
4.13.1.6	Supports sending and reading Unstructured Supplementary Service Data messages
4.3.1.7	APN
4.13.1.8	Possibility to use different PDNs for multiple network access and services
4.13.2.1	Supports 802.11b/g/n/ac
4.13.2.2	WiFi Security : WPA X /WEP/ TKIP variants as per the latest version
4.13.2.3	Support minimum 30 simultaneous WiFi User connections
4.13.2.4	Optional: Support LoRa, Sigfox any of the LPWAN
4.13.3.1	Supports all required Network Protocols
4.13.3.2	Supports Static and dynamic routing
4.13.3.3	Supports static and dynamic IP allocation
4.13.4.1	Multiple clients and a server can run simultaneously
4.13.4.2	WireGuard VPN client and server support
4.13.4.3	Port and tag-based VLAN separation
4.13.4.4	Supports up to 5 x VPn IPsec tunnels with differentAES/DES encryption
4.13.5.1	Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI; NAT; NAT-T
4.13.5.2	DDOS prevention (port scan prevention)
4.13.5.4	Blacklist for blocking out unwanted websites, Whitelistfor specifying allowed sites only
4.13.6.1	Status, configuration, FW update, CLI, troubleshoot,event log, system log.
4.13.6.2	Allows monitoring of: Device data, Mobile data,Network info, Availability
4.13.6.3	Allows monitoring of: Device Model, Revision and Serial Number, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP
4.13.6.4	Allows monitoring of: WAN Type, WAN IP, Mobile Operator Name, Mobile Signal Strength, Mobile Network Type
4.13.6.5	Firmware update from server, automatic notification
4.13.6.6	Management API over HTTP/HTTPS
4.13.7.1	Supports 1 or more SIMs
4.13.7.2	Supports Location Tracking
4.13.7.3	Supports USB
4.13.7.4	Supports Digital I/O Support
4.13.7.5	Supports minimum 4 nos 10/100/1000 Ethernet ports
4.13.7.6	Supports 1G WAN port.
4.13.7.7	Supports status LED
4.13.7.8	Supports PoE and DC power socket.

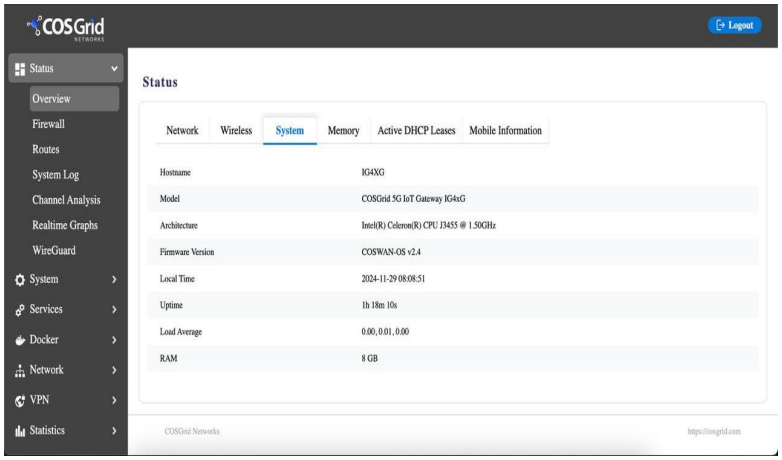
Basic Hardware Setup

Test ID	**Basic Hardware Setup**		
Requirement	Check the Hardware setup		
Test Objective	To check connectivity of hardwares.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Turn on the device after plugging in the power. Connect the ethernet cable to the LAN port and your laptop. Then you can go to the **IP Address provided by the provider** in your browser. Enter the credential provided by the provider.	The LED in the device should blink. The login window to access COSGrid IoT Gateway should be visible. You should be able to login and see the functionalities. Figure:2   	
Overall Test Result	Pass: □	Fail: □	

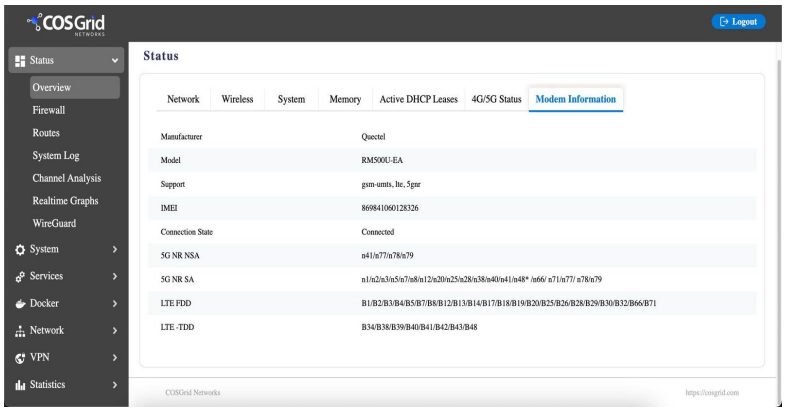
4.13.1.1 CPU : Qualcomm or equivalent, Dual core or Higher

Test ID	4.13.1.1 CPU : Qualcomm or equivalent, Dual core or Higher		
Requirement	Check the Hardware configurations		
Test Objective	To check the hardware compliances & Support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In GUI, ***Status > Overview > Systems***	CPU : Qualcomm or equivalent, Dual core or Higher 	
Overall Test Result	Pass: □	Fail: □	

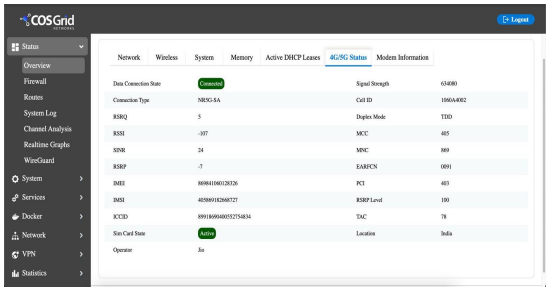
4.13.1.2 RAM -256 Mb

Test ID	4.13.1.2 RAM -256 Mb		
Requirement	Check the Hardware configurations		
Test Objective	To check the hardware compliances & Support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In GUI, ***Status > Overview > Systems***	RAM: 256 MB 	
Overall Test Result	Pass: □	Fail: □	

4.13.1.3 Module: 5G Sub-6Ghz SA 1/2 Gbps DL (4x4 MIMO) or higher , 900/600 Mbps UL (2x2)

Test ID	**4.13.1.3 Module: 5G Sub-6Ghz SA 1/2 Gbps DL (4x4 MIMO) or higher , 900/600 Mbps UL (2x2)**		
Requirement	Check the module configurations		
Test Objective	To check the module status		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In GUI, ***Status > Overview > Modem Information***	Support 5G andshows module name and model 	
Overall Test Result	Pass: □	Fail: □	

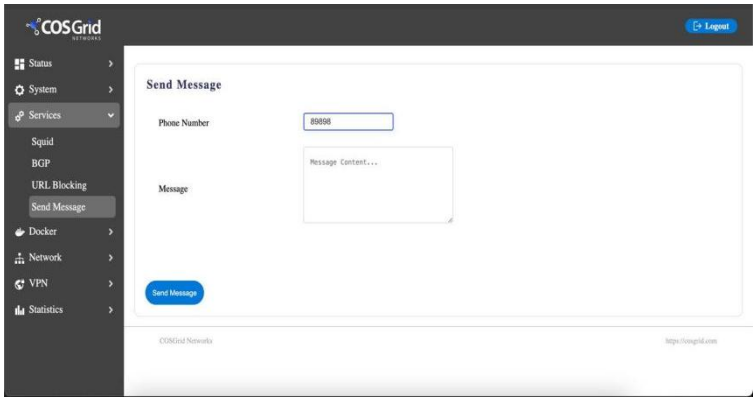
4.13.1.4 Status: Signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP Bytes sent/received, connected band, IMSI, ICCID

Test ID	**4.13.1.4 Status: Signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP Bytes sent/received, connected band, IMSI, ICCID**		
Requirement	Check the Status of Signal Strength		
Test Objective	To check the signal strength status		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In GUI, ***Status > Overview > 4G/5G status***	Shows the RSSI and other required Signal Status 	
Overall Test Result	Pass: □	Fail: □	

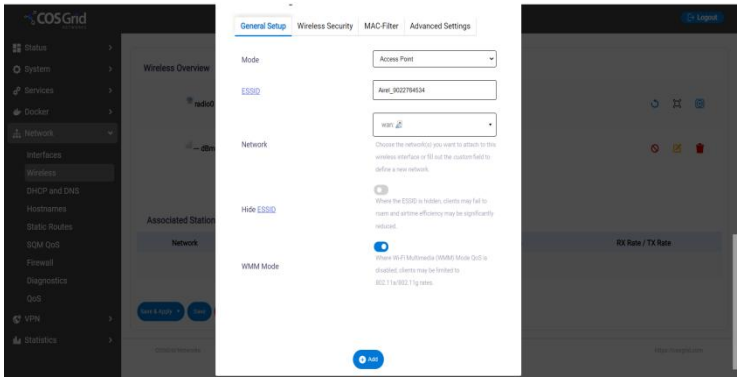
4.13.1.5 SMS/ Call Status

Test ID	**4.13.1.5 SMS/ Call Status**		
Requirement	Check the Status of SMS/ CALL		
Test Objective	To check the SMS/Call status		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In GUI, ***Status > Overview >SMS status (Currently its is in roadmap)****	Shows the SMS status	
Overall Test Result	Pass: □	Fail: □	

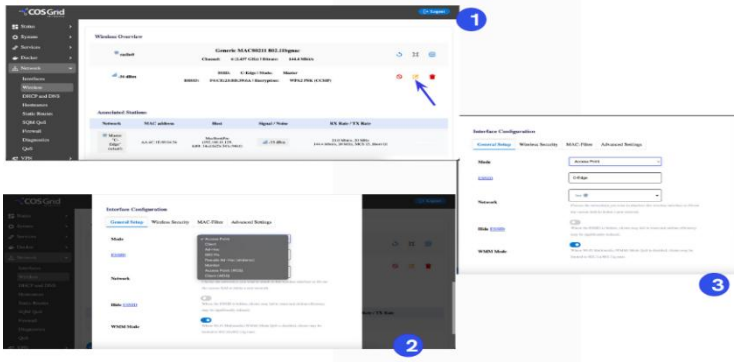
4.3.1.6 Supports sending and reading Unstructured Supplementary Service Data messages

Test ID	**4.13.1.6 Supports sending and reading Unstructured Supplementary Service Data messages**		
Requirement	Check the Status of SMS/ CALL		
Test Objective	To check the SMS/Call status		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In GUI, ***Status > Overview >SMS status (Currently its is in roadmap)****	Shows the SMS status 	
Overall Test Result	Pass: □	Fail: □	

4.3.1.7 APN

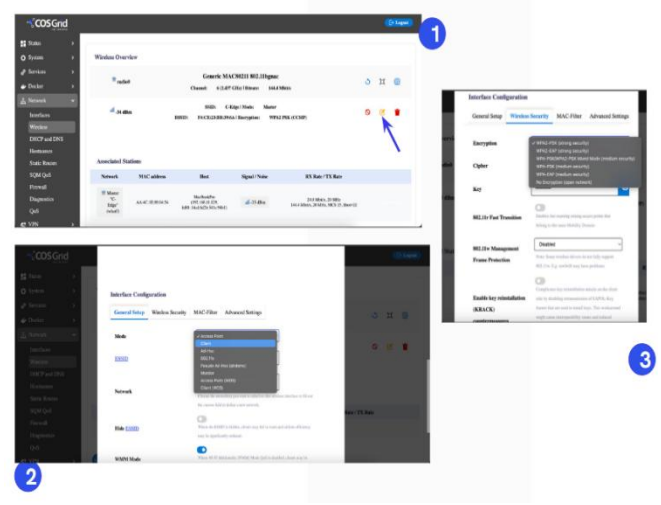
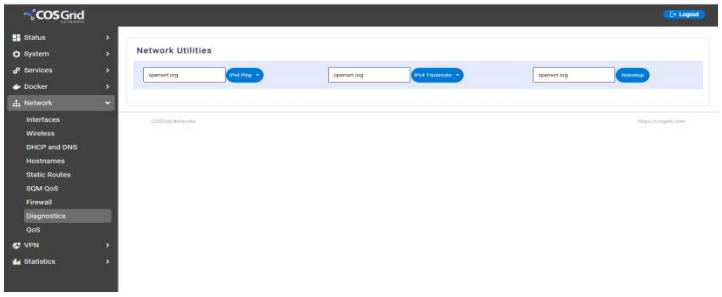
Test ID	**4.3.1.7 APN**		
Requirement	Verify that APN support		
Test Objective	To check the Wifi Access points and its security compliance		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In Side Bar ***Network > Wireless.*** ***Select Access Point Mode.*** Confirm the settings for **SSID, security protocols (WPA2, WPA3).** 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.	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. Support minimum 30 simultaneous WiFi users connections. The network should work seamlessly on every device. 	
Overall Test Result	Pass: □	Fail: □	

4.13.1.8 Possibility to use different PDNs for multiple network access and services

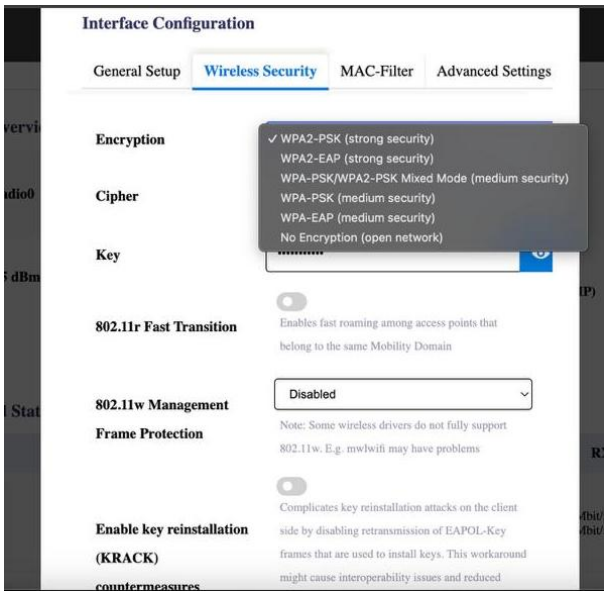
Test ID	4.13.1.8 Possibility to use different PDNs for multiple network access and services		
Requirement	Verify that PDN		
Test Objective	To check the possibility to use different PDN		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In Side Bar ***Network > Wireless.*** ***Select 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. 	
Overall Test Result	Pass: □	Fail: □	

4.13.2.1 Supports 802.11b/g/n/ac

Test ID	4.13.2.1 Supports 802.11b/g/n/ac		
Requirement	Verify that the WiFi Client is configured correctly		
Test Objective	To check the Wifi Client and its security compliance		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In Side Bar ***Network > Wireless.*** ***Select Client 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. You should be able to ping any running website.	

Test ID	**4.13.2.1 Supports 802.11b/g/n/ac**		
	Check the Internet Connection. **You can do a ping test**. Go to ***Network > Diagnostics.***	 	
Overall Test Result	Pass: □	Fail: □	

4.13.2.2 WiFi Security : WPA X /WEP/ TKIP variants as per the latest version

Test ID	**4.13.2.2 WiFi Security : WPA X /WEP/ TKIP variants as per the latest version**		
Requirement	Verify that the WiFi Client is configured correctly		
Test Objective	To check the Wifi and its security compliance		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In Side Bar ***Network > Wireless.*** ***Select Client /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. 	
Overall Test Result	Pass: □	Fail: □	

4.13.2.3 Support minimum 30 simultaneous WiFi User connections

Test ID	**4.13.2.3 Support minimum 30 simultaneous WiFi User connections**		
Requirement	Verify the WiFi User connections		
Test Objective	To check Wifi User connections minimum 30		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	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.	
Overall Test Result	Pass: □	Fail: □	

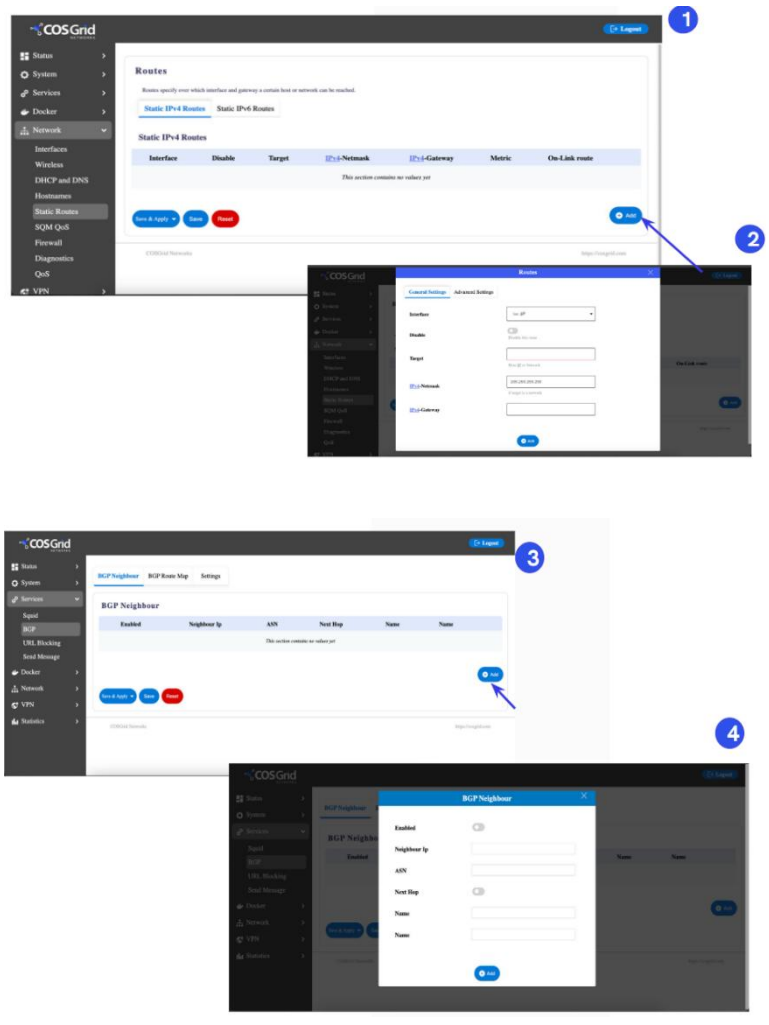
4.13.2.4 Optional: Support LoRa, Sigfox any of the LPWAN

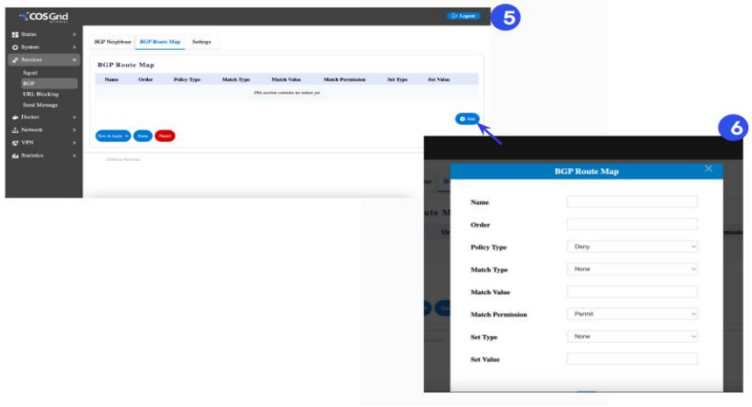
Test ID	**4.13.2.4 Optional: Support LoRa, Sigfox any of the LPWAN**		
Requirement	Verify the Optional Supports		
Test Objective	To check LoRa/ any LPWAN support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Ensure that LoRa, SigfoX or LPWAN connected to the hardware WAN ports/ USB ports Test the compatibility of various devices /sensors (laptops, smartphones, IoT devices) with the Access Point. (*Currently in roadmap)	Optional: Support LoRa, Sigfox any of the LPWAN	
Overall Test Result	Pass: □	Fail: □	

4.13.3.1 Supports all required Network Protocols

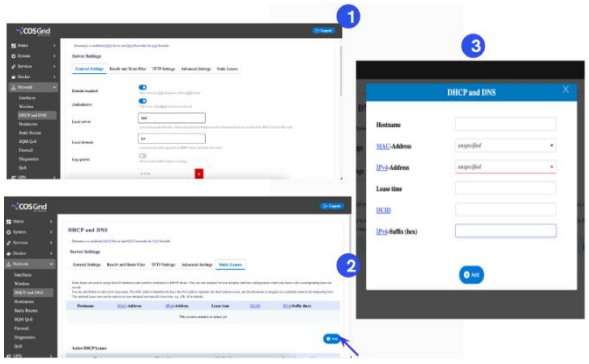
Test ID	**4.13.3.1 Supports all required Network Protocols**		
Requirement	Verify the iot gateway Supports all required Network protocols		
Test Objective	Verify that the COSGrid IoT gateway allows for the configuration of DHCP and DNS server settings.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Network > DHCP and DNS.*** Test the ability to define DHCP and DNS parameters.	The configuration should work for all the devices connected.	
	Go to ***Network > DHCP and DNS. Under the Static Leases Tab,*** Verify leases creation.	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.	
Overall Test Result	Pass: □	Fail: □	

4.13.3.2 Supports Static and dynamic routing

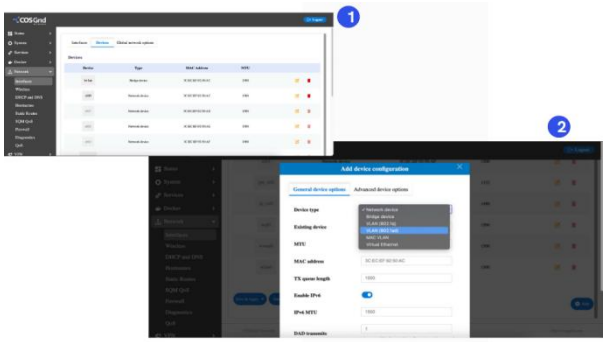
Test ID	4.13.3.2 Supports Static and dynamic routing		
Requirement	Verify that the COSGrid IoT gateway can dynamically adapt to changes in the network topology.		
Test Objective	Verify that the COSGrid IoT gateway allows for the configuration of static routing settings.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Network > Static Routes.*** Test the implementation of static routing. Configure a Route by adding your desired Target and Gateway. Go to ***Network > BGP > Neighbor*** Test the implementation of Dynamic Routing Go to ***Network > BGP > BGP Route Map*** Test the implementation of Dynamic Routing	Options to add **Target, Netmask** etc. should be there. Should be able to see the route configuration in the table. **Note** : *Route will work or not will depend on your configuration.* Options to add **Neighbor, ASN** etc. should be there. 	

Test ID	4.13.3.2 Supports Static and dynamic routing		
			
Overall Test Result	Pass: □	Fail: □	

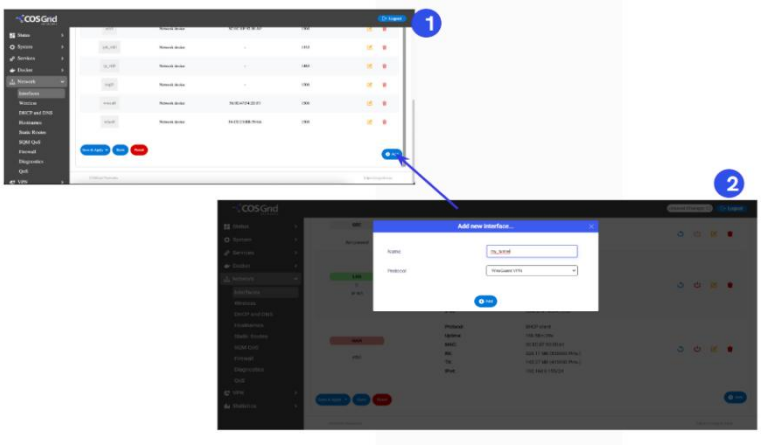
4.13.3.3 Supports static and dynamic IP allocation

Test ID	4.13.3.3Supports static and dynamic IP allocation		
Requirement	Verify that DHCP and DNS server configurations can be applied successfully.		
Test Objective	Verify that the COSGrid IoT gateway allows for the configuration of DHCP and DNS server settings.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Network > DHCP and DNS.*** Test the ability to define DHCP and DNS parameters. Go to ***Network > DHCP and DNS. Under the Static Leases Tab,*** Verify leases creation. ***Under the Static Leases Tab.*** Verify that devices successfully renew their IP addresses as leases expire.	The configuration should work for all the devices connected. A lease should be assigned to every device that is connected. After the mentioned Lease time the device lease should be renewed. 	
Overall Test Result	Pass: □	Fail: □	

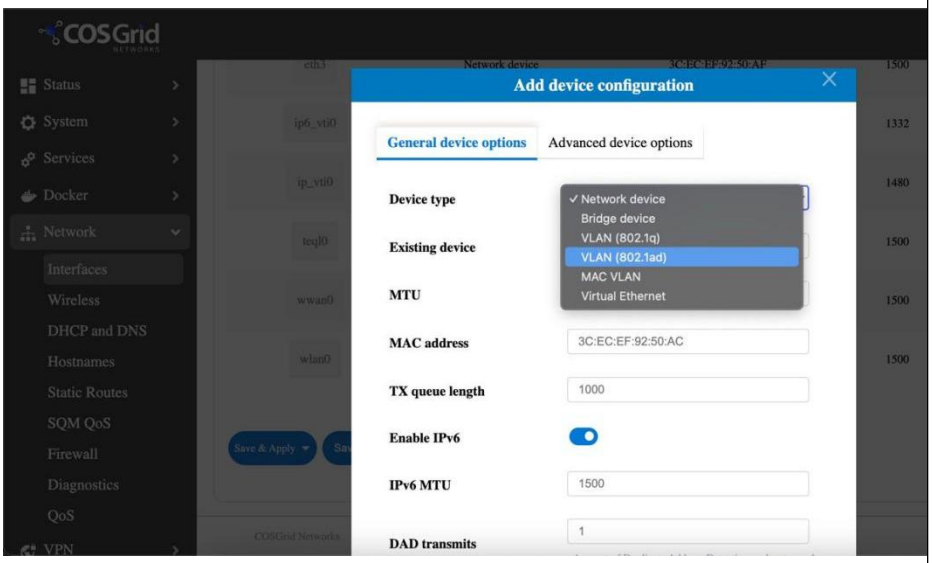
4.13.4.1 Multiple clients and a server can run simultaneously

Test ID	**4.13.4.1 Multiple clients and a server can run simultaneously**	
Requirement	Verify that the COSGrid IoT gateway allows for the configuration of VLAN settings.	
Test Objective	Test the ability to define and modify VLANs.	**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**
	Go to ***Network > Interface, Under Devices tab.*** Test the capability to configure a VLAN by choosing the **device type as VLAN**. .	You should be able to add VLAN using some base (parent) device. 
Overall Test Result	Pass: □	Fail: □

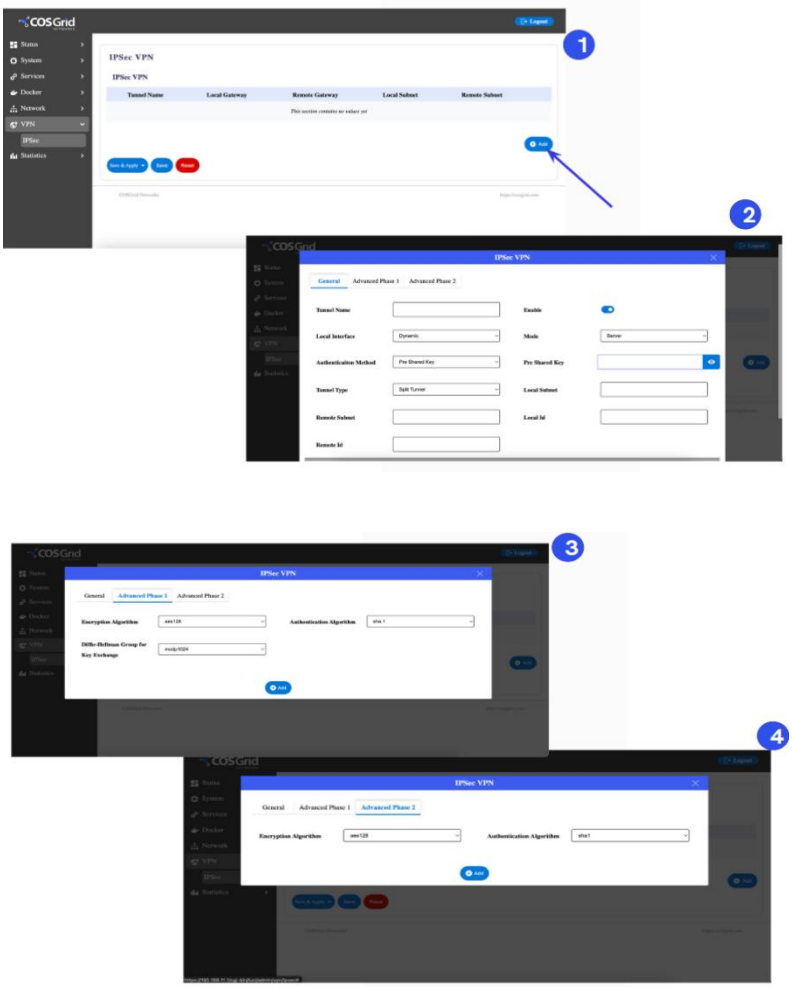
4.13.4.2 WireGuard VPN client and server support

Test ID	**4.13.4.2 WireGuard VPN client and server support**		
Requirement	Verify that the COSGrid IoT gateway allows for the configuration of WireGuard VPN settings.		
Test Objective	Test the ability to define and modify WireGuard configurations.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Network > Interfaces, add an interface with protocol as WireGuard,*** Test the ability to establish WireGuard VPN tunnels. .	The configuration should be listed down in the interfaces table. 	
Overall Test Result	Pass: □	Fail: □	

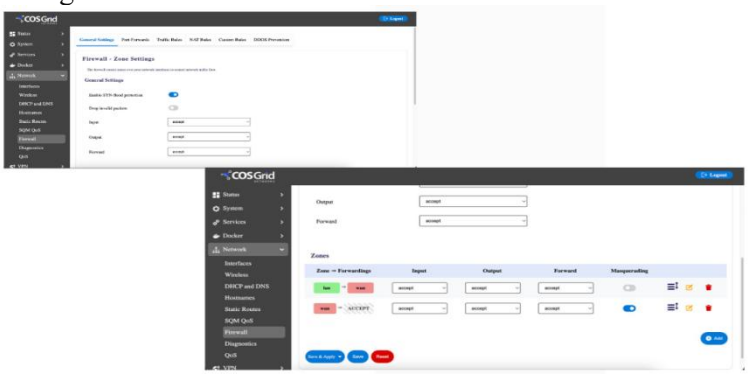
4.13.4.3 Port and tag-based VLAN separation

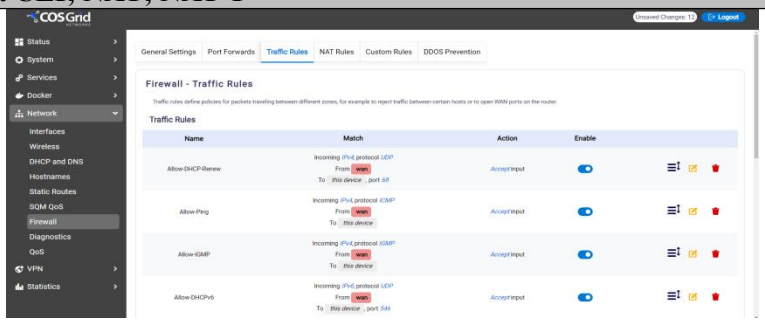
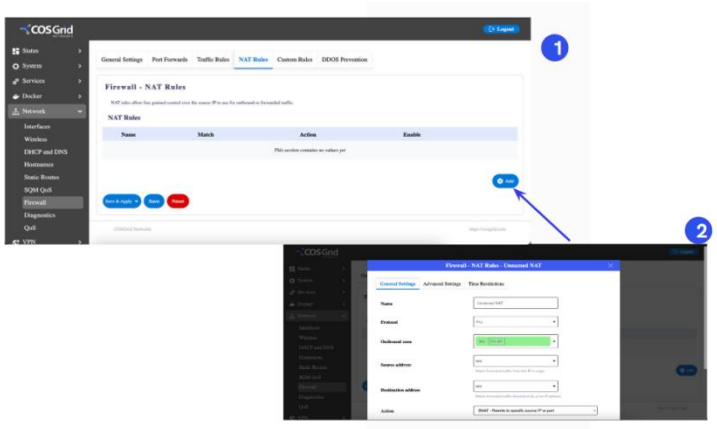
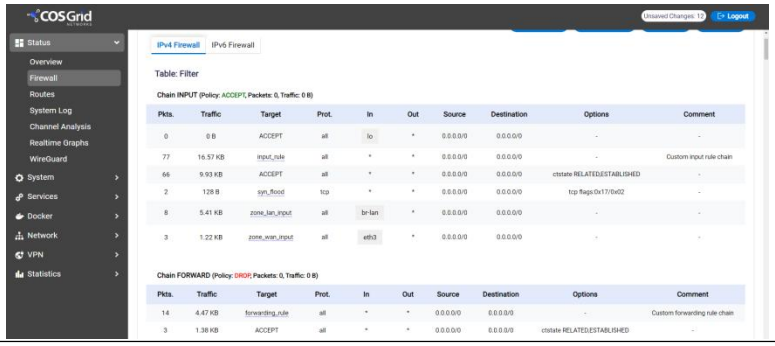
Test ID	**4.13.4.3 Port and tag-based VLAN separation**		
Requirement	Verify that the COSGrid IoT gateway allows for the configuration of VLAN settings.		
Test Objective	Test the ability to define and modify VLANs.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Network > Interface, Under Devices tab.*** Test the capability to configure a VLAN by choosing the **device type as VLAN**. .	You should be able to add VLAN using some base (parent) device. 	
Overall Test Result	Pass: □	Fail: □	

4.13.4.4 Supports up to 5 x VPn IPsec tunnels with differentAES/DES encryption

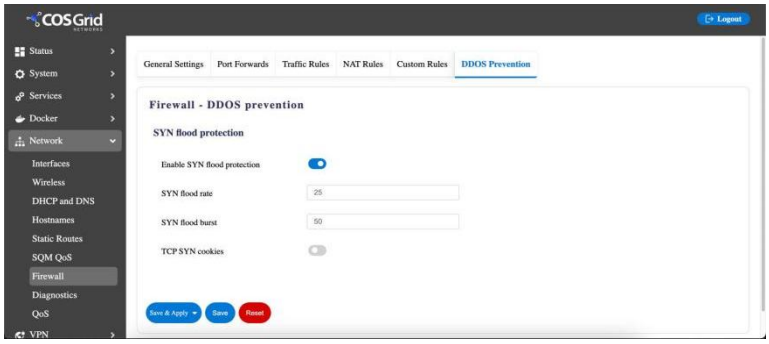
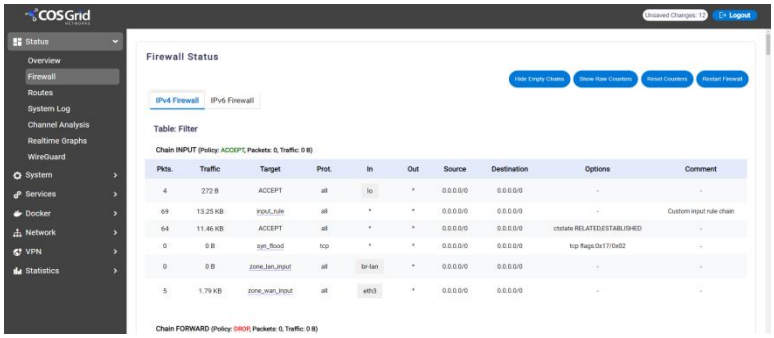
Test ID	**4.13.4.4 Supports up to 5 x VPn IPsec tunnels with differentAES/DES encryption**		
Requirement	Verify that the COSGrid IoT gateway allows for the configuration of IPsec settings..		
Test Objective	Test the ability to define and modify IPsec policies and configurations.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***VPN > IPsec.*** Test the ability to establish IPsec tunnels between the COSGrid IoT gateway and remote devices or networks. Go to ***VPN > IPsec.*** Try to add a tunnel with customized encryption algorithms under ***Advanced Phase 1/2 tab***.	Supports up to 5 x VPn IPsec tunnels with different AES/DES encryption 	
Overall Test Result	Pass: □	Fail: □	

4.13.5.1 Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI; NAT; NAT-T

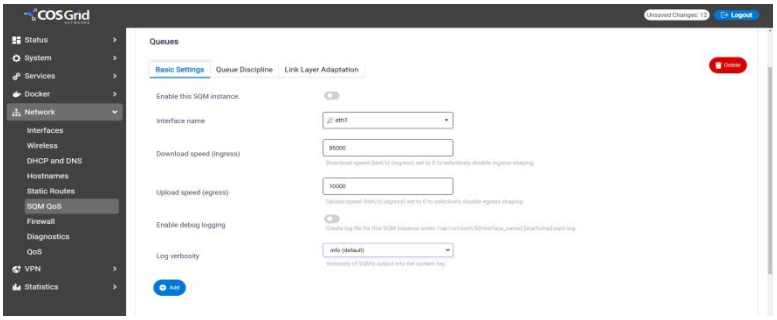
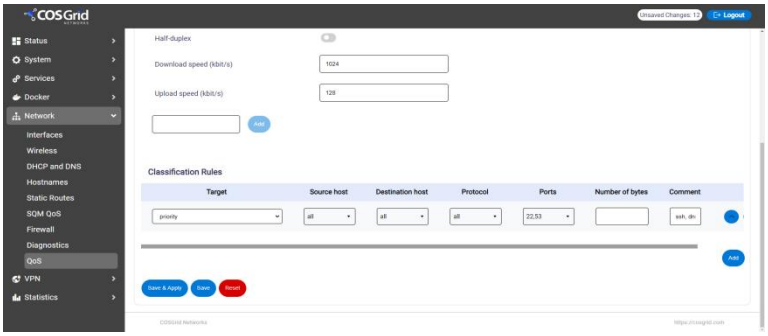
Test ID	**4.13.5.1 Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI; NAT; NAT-T**		
Requirement	Verify that the COSGrid IoT gateway allows for the configuration of firewall settings.		
Test Objective	Test the ability to define and modify firewall rules.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Network > Firewall.*** Test the ability of the firewall to filter incoming and outgoing traffic **based on zone**. Go to ***Network > Firewall, Under Traffic Rules tab.*** You should be able to add a traffic rule based on **source address and destination address**. Go to ***Network > Firewall, Under NAT Rules tab.*** You should be able to add a NAT rule based on **protocol, source address and**	After saving a zone configuration, it should be shown in the table. Now the rule should be displayed in the table also. For working you can follow Set Step 4. Now the rule should be displayed in the table also. For working you can follow Set Step 4. Here you should be able to see firewall logs of above configurations. 	

Test ID	**4.13.5.1 Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI; NAT; NAT-T**
	destination address. Go to ***Status > Firewall.*** Verify the configuration.	  
Overall Test Result	Pass: □	Fail: □

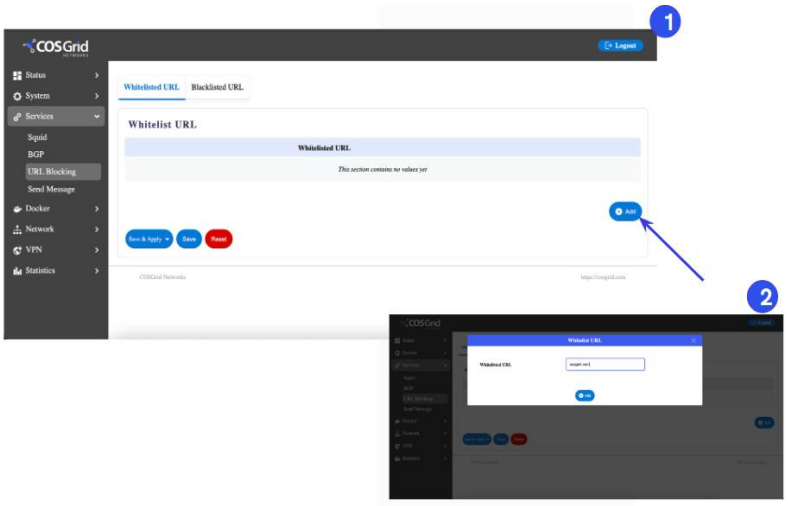
4.13.5.2 DDOS prevention (port scan prevention

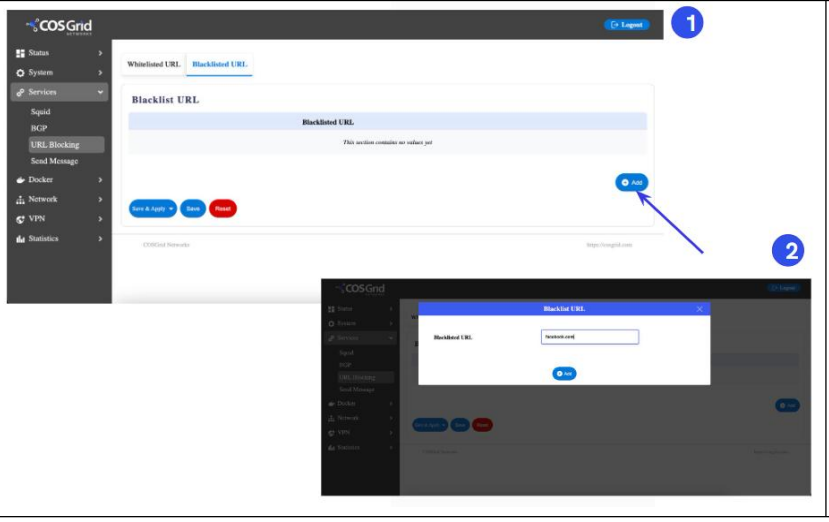
Test ID	**4.13.5.2 DDOS prevention (port scan prevention)**		
Requirement	Verify that the COSGrid IoT gateway allows for the configuration of DDoS protection settings.		
Test Objective	Test the ability to define and modify DDoS protection policies.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Network > Firewall. Under the DDOS Prevention tab,*** Test the DDoS protection feature's ability to monitor incoming traffic for anomalies. Figure:21 Go to ***Status > Firewall*** Verify that abnormal traffic patterns are detected.	DDoS prevention (port scan prevention) You should be able to see logs related to DDoS attacks.   	
Overall Test Result	Pass: □	Fail: □	

4.13.5.3 Sets up custom data limits for SIM card

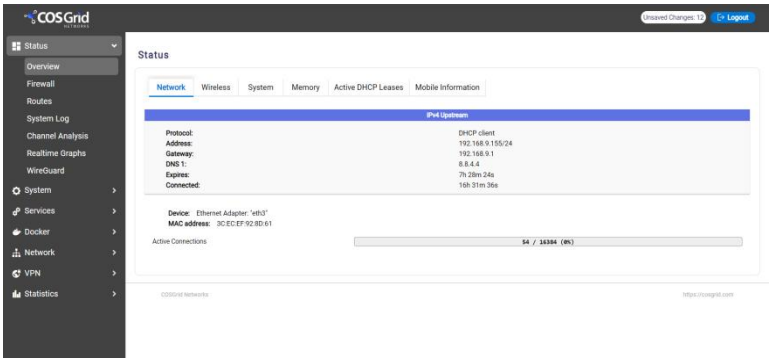
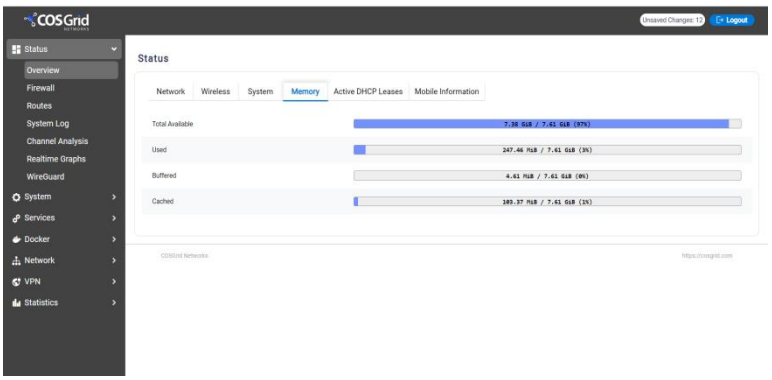
Test ID	**4.13.5.3 Sets up custom data limits for SIM card**		
Requirement	Verify that SQM QoS configurations can be applied successfully.		
Test Objective	Verify that the COSGrid IoT gateway allows for the configuration of SQM QoS settings.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Network > SQM QoS.*** Test the ability to define and modify Queues. Go to ***Network > QoS.*** Test the ability to define and modify QoS policies. Test the allocation of bandwidth to different classes of traffic	Options of Download and Upload Speed should be mentioned. After refreshing the bandwidth configuration should be shown. You should be able to add a rule.   	
Overall Test Result	Pass: □	Fail: □	

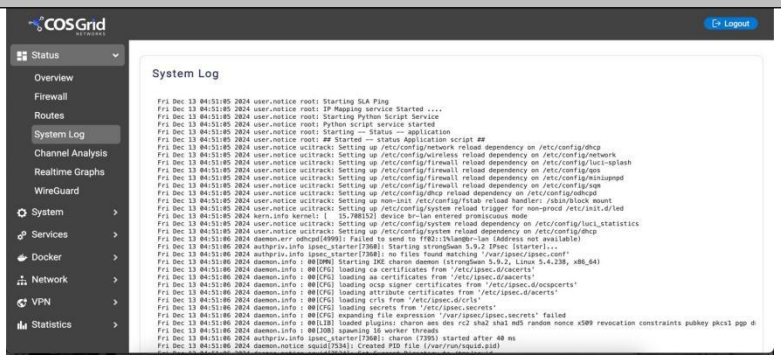
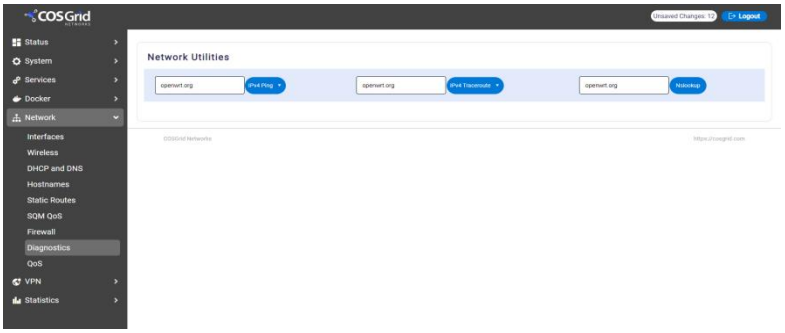
4.13.5.4 Blacklist for blocking out unwanted websites, Whitelistfor specifying allowed sites only

Test ID	**4.13.5,4 Blacklist for blocking out unwanted websites, Whitelistfor specifying allowed sites only**		
Requirement	Verify that the COSGrid IoT gateway allows for the configuration of web filtering settings.		
Test Objective	Test the ability to define and modify web filtering policies.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Services > URL Blocking. Under the Whitelist Url tab,*** Test the ability to configure whitelist websites. Go to ***Services > URL Blocking. Under the Blacklist Url tab,*** Test the ability to configure blacklist websites.	Options to add a whitelist should be there. Blacklist for specifying blocked sites only 	

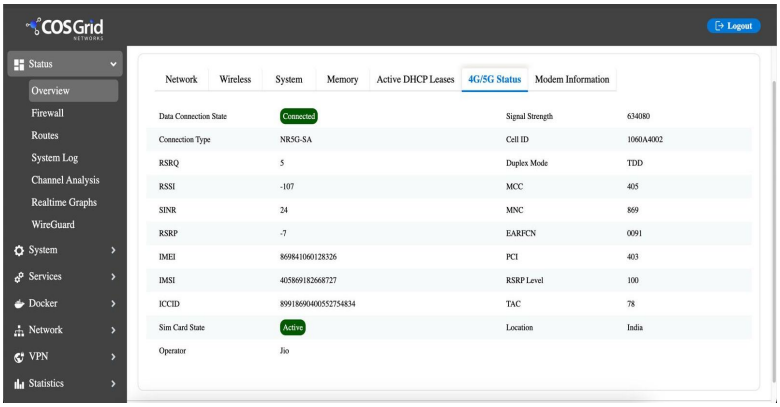
Test ID	**4.13.5,4 Blacklist for blocking out unwanted websites, Whitelistfor specifying allowed sites only**	
		
Overall Test Result	Pass: □	Fail: □

4.13.6.1 Status, configuration, FW update, CLI, troubleshoot,event log, system log.

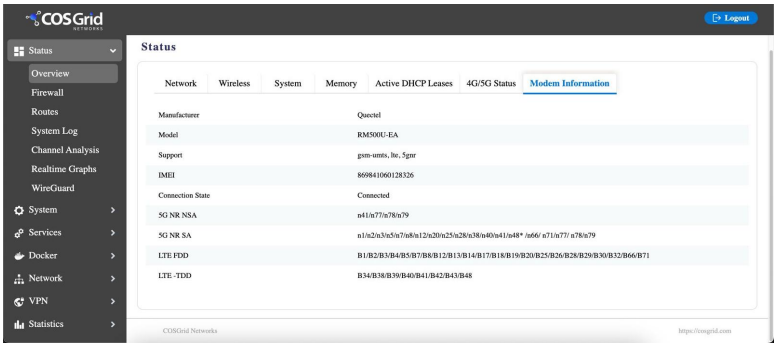
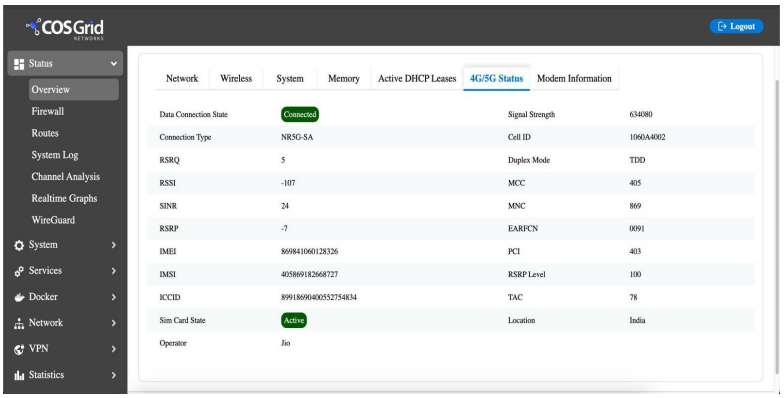
Test ID	**4.13.6.1 Status, configuration, FW update, CLI, troubleshoot,event log, system log.**		
Requirement	Verify that the COSGrid IoT gateway provides a comprehensive status overview of the system.		
Test Objective	Test the visibility of critical system parameters such as CPU usage, memory utilization, and storage capacity.		**Remarks**
Test Description	**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. Go to ***Status > Overview. Under the Memory,*** Verify the memory status. Go to ***Network > Diagnostics*** Test tools such as ping, traceroute. **Status > System Logs**	Status should contain proper parameters to define it. Visibility of critical system parameters such as CPU usage, memory utilization, and storage capacity. Ensure they provide meaningful result System log shown in   	

Test ID	4.13.6.1 Status, configuration, FW update, CLI, troubleshoot,event log, system log.	
		 
Overall Test Result	Pass: □	Fail: □

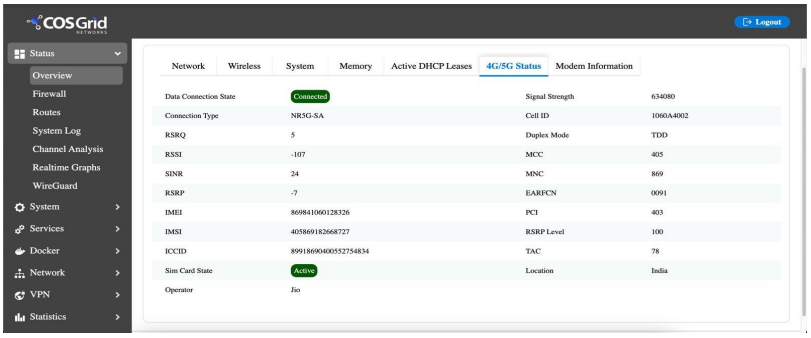
4.13.6.2 Allows monitoring of: Device data, Mobile data,Network info, Availability

Test ID	**4.13.6.2 Allows monitoring of: Device data, Mobile data,Network info, Availability**		
Requirement	Verify that the COSGrid IoT gateway allows for accurate monitoring of device information.		
Test Objective	Test the real-time representation of device model, revision, and serial number.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Status > Overview > 4G/5G status*** Verify the capability of the IoT gateway to monitor Mobile Cell ID.	Allows monitoring of: Device data, Mobile data,Network info, Availability 	
Overall Test Result	Pass: □	Fail: □	

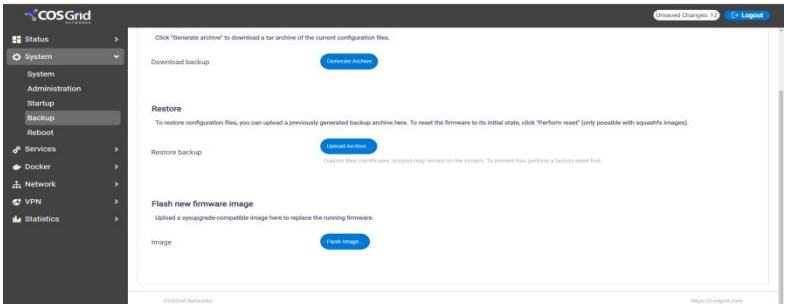
4.13.6.3 Allows monitoring of: Device Model, Revision and Serial Number, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP

Test ID	**4.13.6.3 Allows monitoring of: Device Model, Revision and Serial Number, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP**		
Requirement	Verify that the COSGrid IoT gateway allows for accurate monitoring of device information.		
Test Objective	Test the real-time representation of device model, revision, and serial number.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Status > Overview. Under the Modem Information, & Status > Overview > 4G/5G status***	Allows monitoring of: Device Model, Revision and Serial Number, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP  	
Overall Test Result	Pass: □	Fail: □	

4.13.6.4 Allows monitoring of: WAN Type, WAN IP, Mobile Operator Name, Mobile Signal Strength, Mobile Network Type

Test ID	**4.13.6.4 Allows monitoring of: WAN Type, WAN IP, Mobile Operator Name, Mobile Signal Strength, Mobile Network Type**		
Requirement	Verify that the COSGrid IoT gateway allows for accurate monitoring of device information.		
Test Objective	Test the real-time representation WAN type and operator name		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Go to ***Status > Overview > 4G/5G status***		
Overall Test Result	Pass: □	Fail: □	

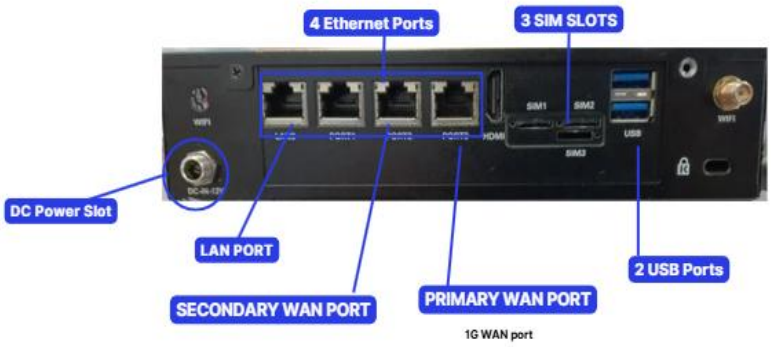
4.13.6.5 Firmware update from server, automatic notification

Test ID	**4.13.6.5 Firmware update from server, automatic notification**		
Requirement	Verify that the COSGrid IoT gateway can receive firmware image.		
Test Objective	Test the initiation of firmware image from the server.		**Remarks**
Test Description	**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** 	
Overall Test Result	Pass: □	Fail: □	

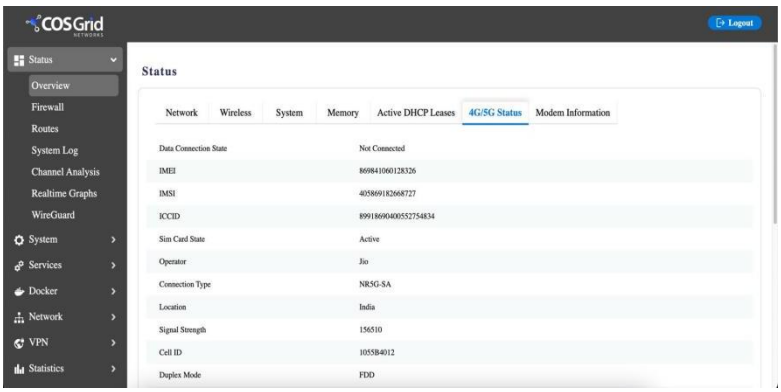
4.13.6.6 Management API over HTTP/HTTPS

Test ID	**4.13.6.6 Management API over HTTP/HTTPS**		
Requirement	Verify that the COSGrid IoT Gateway provides the expected channel to manage it remotely.		
Test Objective	Test the availability and correctness of endpoint URLs.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	You can manage the IoT Gateway device remotely. It uses JSON-RPC. & command prompt/Terminal Type the 1st Command along with device username & password given in the Terminal & get the token Copy the token and paste in the second Command	Tools to handle the device should be available   	
Overall Test Result	Pass: □	Fail: □	

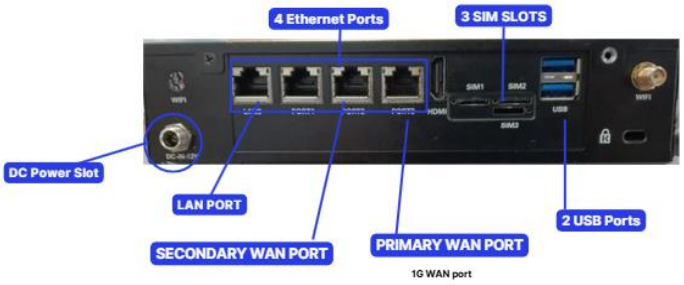
4.13.7.1 Supports 1 or more SIMs

Test ID	4.13.7.1 Supports 1 or more SIMs		
Requirement	Check the Hardware configurations		
Test Objective	To verify SIM Support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check the Hardware Back panel	Supports 1 or more SIMs 	
Overall Test Result	Pass: □	Fail: □	

4.13.7.2 Supports Location Tracking

Test ID	4.13.7.2 Supports Location Tracking		
Requirement	Check the location tracking		
Test Objective	To verify location is shown correct		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In GUI ***Status > Overview > 4G/5G Status***	Supports location Tracking 	
Overall Test Result	Pass: □	Fail: □	

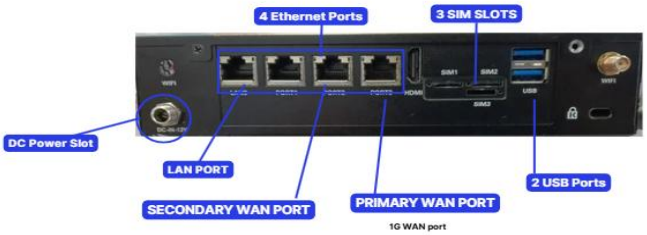
4.13.7.3 Supports USB

Test ID	**4.13.7.3 Supports USB**		
Requirement	Check the hardware ports		
Test Objective	To verify USB port is there and supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check the Hardware back panel	Supports USB 	
Overall Test Result	Pass: □	Fail: □	

4.13.7.4 Supports Digital I/O Support

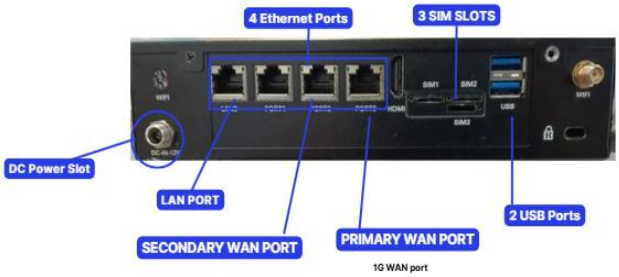
Test ID	4.13.7.4 Supports Digital I/O Support		
Requirement	Check the Hardware configurations Supports minimum 4 nos 10/100/1000 Ethernet ports		
Test Objective	To check Digital Input / Output Support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify digital input/output Support via external USB cable as shown	Supports digital input/output  	
Overall Test Result	Pass: □	Fail: □	

4.13.7.5 Supports minimum 4 nos 10/100/1000 Ethernet ports

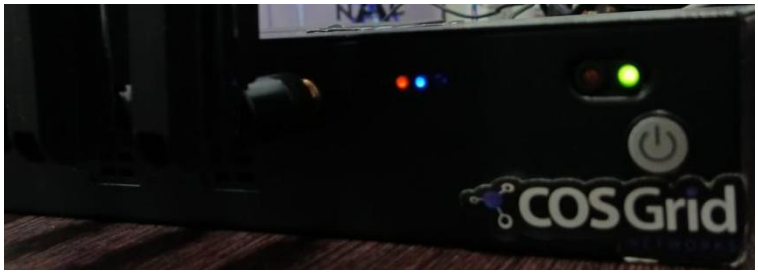
Test ID	4.13.7.5 Supports minimum 4 nos 10/100/1000 Ethernet ports		
Requirement	Check the hardware ports		
Test Objective	To verify required Ethernet is there and supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check the Hardware back panel	Supports minimum 4 nos 10/100/1000 Ethernet Ports 	
Overall Test Result	Pass: □	Fail: □	



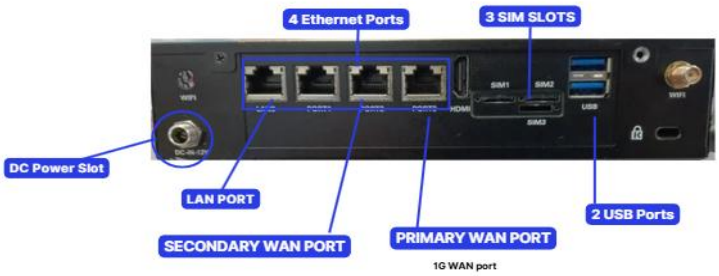
4.13.7.6 Supports 1G WAN port.

Test ID	4.13.7.6 Supports 1G WAN port.		
Requirement	Check the hardware ports		
Test Objective	To verify 1G WAN port is there and supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check the Hardware back panel	Supports 1G WAN port. 	
Overall Test Result	Pass: □	Fail: □	

4.13.7.7 Supports status LED

Test ID	4.13.7.7 Supports status LED		
Requirement	Check the Status LED		
Test Objective	To verify Status LED blinking		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check the Hardware Front panel (Check Datasheet for Status LED description)	LED is blinking 	
Overall Test Result	Pass: □	Fail: □	

4.13.7.8 Supports PoE and DC power socket.

Test ID	**4.13.7.8 Supports PoE and DC power socket.**		
Requirement	Check the hardware ports		
Test Objective	To verify poE and DC power socket is there and supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check the Hardware back panel	Supports PoE and DC power socket. 	
Overall Test Result	Pass: □	Fail: □	

Section 4.14 5G Mini Drones

S.no	Description
4.14.1.1,4.14.1.13(a) (m)	5G enabled and controlled drone 5G Modem (n78 band)
4.14.1.2 4.14.1.3 4.14.1.15	TSupports 5G nano SIM Connectivity Options: Cellular (5G) and Wi-Fi for ubiquitous and long-range connectivity Wi-Fi (2.4/5 GHz)
4.14.1.4	Qualcomm or equivalent onboard processing engine for AI/ML analytics Should support MEC applications
4.14.1.5	Autonomy: Visual Inertial Odometry (VIO), path planning, PX4, GPS-denied navigation, BVLOS, follow me.
4.14.1.6	360 obstacle avoidance: Depth estimation, obstacle detection, map60ping and VOA
4.14.1.7	Payload Capacity – 500g/1 Kg or above
4.14.1.8	GPS or NAVIC enabled
4.14.1.9	Geo Fencing
4.14.1.10 4.14.1.11	Tracking sensor Image Sensor

4.14.1.1,4.14.1.13(a) 5G enabled and controlled drone (m) 5G Modem (n78 band)

Test ID	**4.14.1.1,4.14.1.13(a) 5G enabled and controlled drone (m) 5G Modem (n78 band)**		
Requirement	To Check Drone is integrated into the System and supports 5G Modem (n78 band)		
Test Objective	To Check Drone is integrated into the System and supports 5G Modem (n78 band)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Verify the 5G network is on N78 band only. Step-2: Insert the 5G SIM into the drone and Power ON the drone by inserting the battery. Step-3: The drone will automatically send the UE attach message to the 5G network. After successful attach and IP assignment, the drone can be connected via the GCS. Step-3: Open the GCS - ***'iDronam Enterprise'.*** Connect to the drone. Step-4: Check if all the drone data are coming - ○ 3D Map data. ○ Video data. ○ Drone Telemetry data	All the drone data - 1. 3D Map Data. 2. Video data. 3. Drone Telemetry data. should be available on the GCS - 'iDronam Enterprise' via 5G.	It is verifiedDrone is integrated and supporting Band 78
Overall Test Result	Pass: □	Fail: □	

4.14.1.2 TSupports 5G nano SIM

4.14.1.3 Connectivity Options: Cellular (5G) and Wi-Fi for ubiquitous and long-range connectivity

4.14.1.15 Wi-Fi (2.4/5 GHz)

Test ID	**4.14.1.2 TSupports 5G nano SIM** **4.14.1.3 Connectivity Options: Cellular (5G) and Wi-Fi for ubiquitous and long-range connectivity** **4.14.1.15 Wi-Fi (2.4/5 GHz)**		
Requirement	Verify Drone supported Nano Sim and (2.4/5 GHz)		
Test Objective	To verify support of 5G Nano Sim and 5G enabled and controlled and Wi-Fi for ubiquitous and long-range connectivity		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Take a 5G Nano SIM and Insert into the drone SIM card slot. Step-2: Connect the GCS to the 5G network. Step-3: Connect the GCS to the drone. Step-4: Check for the drone connection and information being displayed on the GCS screen. WI fI Step-1: Turn ON the Drone and wait for the drone to initialize Step-1: Open GCS. Step-2: Connect the GCS WiFi to Drone's WiFi. Step-3: Open iDronam and connect to the drone.	Verify in below packet in wireshark Successful insertion of 5G Nano SIM in SIM Slot of 5G Communication Module of Drone. Successful connection and display of drone data on the screen. GCS and drone must be on the same wifi network and the drone should successfully connect to the drone over WiFi.	Successful insertion of 5G Nano SIM in SIM Slot of 5G and Wi Fi supported
Overall Test Result	Pass: □	Fail: □	

4.14.1.4 Qualcomm or equivalent onboard processing engine for AI/ML analytics Should support MEC applications

Test ID	**4.14.1.4 Qualcomm or equivalent onboard processing engine for AI/ML analytics Should support MEC applications**		
Requirement	Onboard processing engine for AI/ML analytics and MEC application support.		
Test Objective	To Check drone capabilities for AI/ML and MEC.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Connect to the web page is hosted inside the drone. Open the webpage by going to the drone's IP - 10.42.0.1:5000 using a browser. Step-2: The page will open and the user can upload an image to the drone. Step-3: After processing, the drone will return the results of object detection in image and JSON formats. These can be downloaded for further use. Should support MEC applications The drone is ME UE which is offloading the drone video stream. Step-1: Connect the MEC Server to the drone. Step-2: An MEC application will be running on the MEC server which will receive the incoming video stream. Step-3: After processing the output can be viewed on the web page hosted in MEC.	The webpage should successfully be opened. Using this drone's AI/ML capabilities can be seen. The webpage should successfully be opened. Using this drone's AI/ML capabilities can be seen.	
Overall Test Result	Pass: □	Fail: □	

4.14.1.5 Autonomy: Visual Inertial Odometry (VIO), path planning, PX4, GPS-denied navigation, BVLOS, follow me

Test ID	**4.14.1.5 Autonomy: Visual Inertial Odometry (VIO), path planning, PX4, GPS-denied navigation, BVLOS, follow me.**		
Requirement	Verify To Check Drone Autonomy		
Test Objective	To Check Drone Autonomy		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Connect the drone to MAVLink Packet Decoder (e.g, Mission Planner) Step-2: Start Capturing the MAVLink Data Stream.v Step-3: Check for the data being published by drone. Step-4: Look for the "VISION_POSITION_ ESTIMATE" , "LOCAL_POSITION_ NED" , "OBSTACLE_DISTAN CE" data packets for Visual inertial Odometry	"VISION_POSITION_ESTI MA TE", "LOCAL_POSITION_NED" , "OBSTACLE_DISTANCE" msg should be present.	
Overall Test Result	Pass: □	Fail: □	

4.14.1.6 360 obstacle avoidance: Depth estimation, obstacle detection, map60ping and VOA

Test ID	**4.14.1.6 360 obstacle avoidance: Depth estimation, obstacle detection, map60ping and VOA**		
Requirement	360 obstacle avoidance, Depth estimation, obstacle detection, mapping and VOA		
Test Objective	To Verify Drone Obstacle Avoidance and Mapping		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1:Connect the drone to a MAVLink Decoder(Mission Planner) and look for “OBSTACLE_DISTANCE”, and “RANGEFINDER” messages for obstacle and depth estimation respectively. Mapping and VOA Step-1: Place the drone on the floor, connect the ‘iDronam Enterprise’ Software to the drone and subscribe to“/map” for 3d map and Dynamic Obstacle plotter.	360 obstacle avoidance, Depth Estimation and obstacle detection: Before arming the drone a test object can be placed within a distance of ~20cm at 45-degree intervals covering 360 degrees around the drone. The drone will detect it and give a pre-arm warning giving the details of the angle and distance of the object Take off the drone to 1-1.2 m altitude. The mapping algorithm will map the surroundings of the drone as it takes off. A test object can be brought close to the drone from the front face and the drone will back off once a threshold of 1.5m is crossed by the object. “OBSTACLE_DISTANCE”, “RANGEFINDER” messages should be defined and changed as youincrease drone height and environment change. The map should be visible on the GCS.	1.5m is crossed by the object. “OBSTACLE_DISTANCE”, “RANGEFINDER” messages ged as you increase drone height and environment change. The map should be visible on the GCS.
Overall Test Result	Pass: □	Fail: □	

4.14.1.7 Payload Capacity – 500g/1 Kg or above

Test ID	4.14.1.7 Payload Capacity – 500g/1 Kg or above		
Requirement	To Check Payload Capacity		
Test Objective	To Check Payload Capacity		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Take the drone outdoors. Step-2: Attach the 500gm Payload and Turn on the Drone Step-3: Wait for the drone to initialize. Step-4: Takeoff the Drone.(Read Proper Manual Before Flying) Step-5: Land the Drone	Drone Takes off up to a height of 1.2m and hovers in its place for a duration of 1 min.	
Overall Test Result	Pass: □	Fail: □	

4.14.1.8 GPS or NAVIC enabled

Test ID	4.14.1.8 GPS or NAVIC enabled		
Requirement	To Check GPS		
Test Objective	To verify GNSS Capabilities		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Connect the drone to GCS and read the sensor status for GPS/Navic at Serial4/UART8. Drone should be placed in an outdoor environment under clear skies and location should not be near buildings of height greater than 20m. Step-2: Turn on the drone and connect to GCS	The drone should have a GPS lock which will be indicated in GCS. An accuracy of 3m is expected. It should return “3D FIX” AND “3D DGPS” or relevant status depending upon the GPS Locking	
Overall Test Result	Pass: □	Fail: □	

4.14.1.9 Geo Fencing

Test ID	**4.14.1.9 Geo Fencing**		
Requirement	To Check Geo Fencing		
Test Objective	To Check Geo Fencing		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: Turn ON the Drone. Step-2: Connect the drone to GCS and in the plan section create a fence	After Uploading the Fence. Click on the Read Fence Button to read to fence Drone stored.	
Overall Test Result	Pass: □	Fail: □	

4.14.1.10 Tracking sensor

4.14.1.11 Image Sensor

Test ID	**4.14.1.10 Tracking sensor** **4.14.1.11 Image Sensor**		
Requirement	To Check Sensors		
Test Objective	To Check Tracking sensor and Image Sensor		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Step-1: The drone should be placed in an outdoor environment where GPS Signals are uninterrupted. Step-2: Once 3D Fix has come the GPS will have a good lock of Drone Position. Step-3: The Drone can be tracked. Image sensor: Step-1: Turn ON the drone. Step-2: Connect the drone to the iDronam software.	After GPS Fix, the drone is successfully tracked via the GCS. The Live Stream of the drone camera will be displayed in iDronam.	
Overall Test Result	Pass: □	Fail: □	

Section 4.15 XR (AR/VR) Device

S.no	Description
4.15.1.1	XR(AR/VR) Device Specifications
4.15.2.1	Bluetooth
4.15.2.2	Wi-fi
4.15.2.4	3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass)
4.15.3.1	Display:24°field-of-view, 24-bitcolor LCD ,outdoor visible ,HD resolution
4.15.3.2	Microphone
4.15.3.3	Speaker
4.15.1.1	XR(AR/VR) Device Specifications
4.15.2.1	Bluetooth
4.15.2.2	Wi-fi

4.15.1.1 XR(AR/VR) Device Specifications

Test ID	4.15.1.1 XR(AR/VR) Device Specifications		
Requirement	Chipset:2.0 GHz 8-core Qualcomm		
Test Objective	Chipset:2.0 GHz 8-core Qualcomm		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify From the AjnaXR Data sheet Qualcomm XR2+ Gen 1 CPU Octa-core Kryo 585		
Overall Test Result	Pass: □	Fail: □	

4.15.1.2 XR(AR/VR) Device Specifications

Test ID	4.15.1.2 XR(AR/VR) Device Specifications		
Requirement	Memory: 64 GB Internal storage/4GB RAM/Micro SD slot		
Test Objective	Memory: 64 GB Internal storage/4GB RAM/Micro SD slot		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	Storage: 128GB RAM: 8GB	
Overall Test Result	Pass: □	Fail: □	

4.15.1.3 XR(AR/VR) Device Specifications

Test ID	4.15.1.3 XR(AR/VR) Device Specifications		
Requirement	Port: USB Type C and Audio		
Test Objective	Port: USB Type C and Audio		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Visual inspection. USB Type C port can be located.		
Overall Test Result	Pass: □	Fail: □	

4.15.2.1 Bluetooth

Test ID	4.15.2.1 Bluetooth		
Requirement	Bluetooth 5.0 Should be supported		
Test Objective	Bluetooth 5.0 Should be supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	Bluetooth 5	
Overall Test Result	Pass: □	Fail: □	

4.15.2.2 Wi-fi

Test ID	4.15.2.2 Wi-fi		
Requirement	802.11a/b/g/n/ac- 2.4GHz and 5GHz		
Test Objective	Wifi Range-~ 25meter		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet and also connect to companion device to stream the video	From data sheet device supports Wi-Fi 6 which supports both 2.4 and 5 GHz : Wi-Fi 6	
Overall Test Result	Pass: □	Fail: □	

4.15.2.4 3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass)

Test ID	4.15.2.4 3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass)		
Requirement	3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass)		
Test Objective	Wifi Range-~ 25meter		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify visually		
Overall Test Result	Pass: □	Fail: □	

4.15.3.1 Display:24°field-of-view, 24-bitcolor LCD ,outdoor visible ,HD resolution

Test ID	**4.15.3.1 Display:24°field-of-view, 24-bitcolor LCD ,outdoor visible ,HD resolution**		
Requirement	Display:24°field-of-view, 24-bitcolor LCD ,outdoor visible ,HD resolution		
Test Objective	Display:24°field-of-view, 24-bitcolor LCD ,outdoor visible ,HD resolution		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from data sheet	Resolution: 3200*1600 Refresh Rate: 90Hz Fov: 95°~105° PPI: 1058	
Overall Test Result	Pass: □	Fail: □	

4.15.3.2 Microphone

Test ID	**4.15.3.2 Microphone**		
Requirement	Microphone		
Test Objective	Microphone		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Visual inspection		
Overall Test Result	Pass: □	Fail: □	

4.15.3.3 Speaker

Test ID	**4.15.3.3 Speaker**		
Requirement	Speaker: Internal 94 dBA loudspeaker		
Test Objective	Speaker: Internal 94 dBA loudspeaker		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Visual inspection		
Overall Test Result	Pass: □	Fail: □	

Section 4.16 5G Indoor CPE

S.no	Description
4.16.1 4.16.1.1 4.16.1.2	Processor - Qualcomm or equivalent CPU Clock Speed 1.0GHz or higher CPU Cores Dual-core Cortex-A53 Arm or equivalent
4.16.1 4.16.1.1 4.16.1.2	Processor - Qualcomm or equivalent CPU Clock Speed 1.0GHz or higher CPU Cores Dual-core Cortex-A53 Arm or equivalent
4.16.3.1	3GPP Release
4.16.3.1	3GPP Release
4.16.3.2	Sub-6 Band n78:TDD
4.16.3.3	5G Modem
4.16.3.4	Bandwidth Support
4.16.3.5	MIMO
4.16.3.6	Download speed
4.16.5.1	Wireless
4.16.5.2	Dynamic Frequency Selection
4.16.5.3	Standards: IEEE802.11a/b/g/n/acwave2
4.16.5.4:	Wireless MIMO Support
4.16.5.5:	Wireless PHY rate
4.16.5.6:	IPv4/IPv6 support
4.16.6.a:	Wireless Antenna
4.16.6.b:	Transmit power
4.16.6.c:	Receiver Sensitivity
4.16.6.d:	RF Management
4.16.6.e:	RF Control Plane
4.16.7.c	Security: All version and latest WPA Support
4.16.7 e	Security: IPSec,PPTP,IP-Filtering
4.16.7g	MAC address authentication
4.16.8 a	Interface
4.16.8 b	SIM Slot
4.16.8 c	POE
4.16.9.1	Management
4.16.9.3	IEEE 802.11e Standard
4.16.9.4	Intelligent RF Control Plane for self-healing and Self-Optimization

4.16.1 Processor - Qualcomm or equivalent

4.16.1.1 CPU Clock Speed 1.0GHz or higher

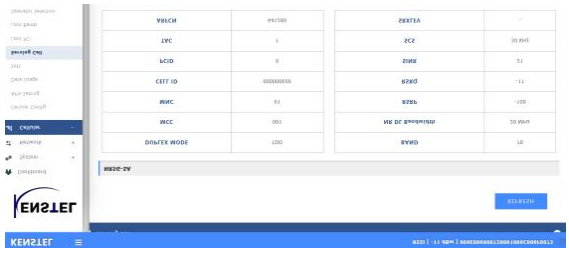
4.16.1.2 CPU Cores Dual-core Cortex-A53 Arm or equivalent

Test ID	**4.16.1 Processor - Qualcomm or equivalent** **4.16.1.1 CPU Clock Speed 1.0GHz or higher** **4.16.1.2 CPU Cores Dual-core Cortex-A53 Arm or equivalent**		
Requirement	To verify Processor, Clock speed and ARM Core		
Test Objective	To verify Processor, Clock speed and ARM Core		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify the from the data sheet for KCP- 5G-510I Indoor 5G CPE.	From the data sheet Qualcomm® 1Ghz MHz Dual Core CPU | ARM Cortex A53	
Overall Test Result	Pass: □	Fail: □	

4.16.2 Memory: 512 MB RAM or higher

Test ID	**4.16.2 Memory: 512 MB RAM or higher**		
Requirement	To verify Memory: 512 **MB RAM** or higher		
Test Objective	Verify RAM Space		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify the from the data sheet for KCP- 5G-510I Indoor 5G CPE	From the data sheet: Memory 512MB RAM | 256MB NAND FLASH	Verify that RAM detail having 512 MB
Overall Test Result	Pass: □	Fail: □	

4.16.3.1 3GPP Release

Test ID	**4.16.3.1 3GPP Release**		
Requirement	3GPP Release 15 or above support		
Test Objective	3GPP Release 15 or above support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify if the CPE registers successfully to 5G SA network. Registering to 5G SA indicates support for Rel 15		
Overall Test Result	Pass: □	Fail: □	

4.16.3.2 Sub-6 Band n78:TDD

Test ID	**4.16.3.2 Sub-6 Band n78:TDD**		
Requirement	Sub-6 Band n78:TDD to be supported		
Test Objective	Sub-6 Band n78:TDD to be supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify if the CPE registers successfully to 5G SA network in band n78. Check the band registered in Kenstel Web GUI as shown.		
Overall Test Result	Pass: □	Fail: □	

4.16.3.3 5G Modem

Test ID	**4.16.3.3 5G Modem**		
Requirement	5G Modem: Snapdragon SDX62/65 or Equivalent		
Test Objective	N78 Band to be supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	TECHNICAL SPECIFICATION Processor Qualcomm® 1Ghz MHz Dual-Core CPU | ARM Cortex A53 **Snapdragon X62 modem** Memory 512MB RAM | 256MB NAND FLASH	
Overall Test Result	Pass: □	Fail: □	

4.16.3.4 Bandwidth Support

Test ID	**4.16.3.4 Bandwidth Support**		
Requirement	Bandwidth support: 20/40/60/80/100 MHz		
Test Objective	Bandwidth support: 20/40/60/80/100 MHz		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	From the data sheet **5G** ❖ 5G Technology: 5G NR FDD, 5G NR TDD, SA, NSA[19] ❖ 5G Spectrum: mmWave, sub-6 GHz, 5G/4G spectrum sharing ❖ 5G Modes: FDD, TDD, SA NSA ❖ 5G mmWave : 800 MHz bandwidth, 8 carriers, 2x2 MIMO ❖ 5G sub-6 GHz : 200 MHz bandwidth, 4x4 MIMO ❖ 5G Peak Download Speed: 7500 Mbit/s ❖ 5G Peak Upload Speed: 3000 Mbit/s ❖ 5G RF: 100 MHz envelope tracking, Adaptive antenna tuning ❖ Performance Enhancement Technologies: Qualcomm 5G PowerSave, Qualcomm Signal Boost, Qualcomm Smart Transmit technology, Qualcomm RF Gaming Mode Boost, Qualcomm Wideband Envelope Tracking	
Overall Test Result	Pass: □	Fail: □	

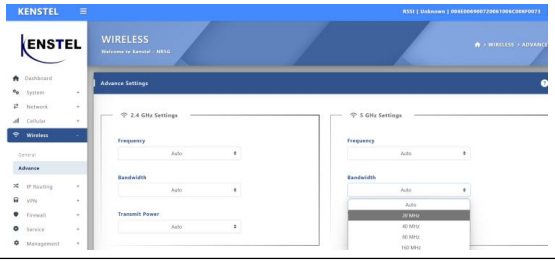
4.16.3.5 MIMO

Test ID	**4.16.3.5 MIMO**		
Requirement	MIMO 4x4 or higher		
Test Objective	MIMO 4x4 or higher		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	From the data sheet: **Kenstel KCP-5G-510I** is a two-radio, 4x4 MIMO 802.11ax 5G CPE. Designed for general purpose, next-generation deployments in harsh outdoor locations and industrial I conditions, the KCP-5G-510I offers performance, enterprise-grade security, and intuitive management. The KCP-5G-510I delivers a maximum 5.4 Gbps aggregate frame rate with concurrent 2.4 GHz and 5 GHz radios. KCP-5G-510I delivers the high throughput, reliability, and flexibility required by the most demanding business applications like voice and high-definition streaming video, even in the harshest outdoor environments	
Overall Test Result	Pass: □	Fail: □	

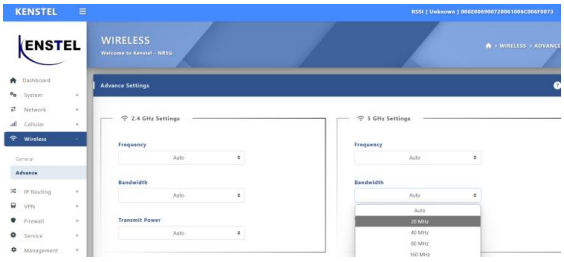
4.16.3.6 Download speed

Test ID	**4.16.3.6 Download speed**		
Requirement	Download speed : Up to 1000 mbps		
Test Objective	Download speed : Up to 1000 mbps		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	From the data sheet: ❖ 5G Peak Download Speed: 7500 Mbit/s ❖ 5G Peak Upload Speed: 3000 Mbit/s	
Overall Test Result	Pass: □	Fail: □	

4.16.5.1 Wireless

Test ID	**4.16.5.1 Wireless**		
Requirement	AP Type: Indoor, dual radio, 2.4,5-GHz		
Test Objective	AP Type: Indoor, dual radio, 2.4,5-GHz		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Goto Wireless- >Advanced General on the Kenstel Web GUI		
Overall Test Result	Pass: □	Fail: □	

4.16.5.2 Dynamic Frequency Selection

Test ID	**4.16.5.2 Dynamic Frequency Selection**		
Requirement	Dynamic Frequency Selection		
Test Objective	Dynamic Frequency Selection GHz		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet or Web GUI Goto Wireless- >Advanced General on the Kenstel Web GUI	2.4 GHz or 5GHz can be supported. 	
Overall Test Result	Pass: □	Fail: □	

4.16.5.3 Standards: IEEE802.11a/b/g/n/acwave2

Test ID	**4.16.5.3 Standards: IEEE802.11a/b/g/n/acwave2**		
Requirement	Standards: IEEE802.11a/b/g/n/acwave2		
Test Objective	Standards: IEEE802.11a/b/g/n/acwave2		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	From the data sheet ❖ IEEE 802.11a/b/g/n/ac/ax compliant ❖ 2.4GHz and 5GHz concurrent radios	
Overall Test Result	Pass: □	Fail: □	

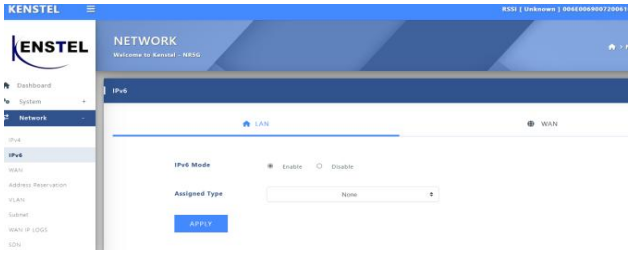
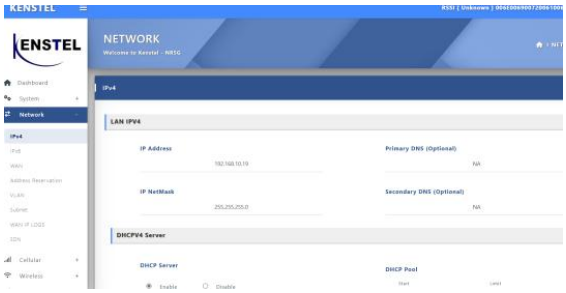
4.16.5.4: Wireless MIMO Support

Test ID	**4.16.5.4: Wireless MIMO Support**		
Requirement	2x2 MU-MIMO with 2 spatial streams		
Test Objective	2x2 MU-MIMO with 2 spatial streams		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	From the data sheet **Supported Radio Technologies** 802.11b: Direct-Sequence Spread Spectrum (DSSS) 802.11a/g/n/ac/ax: Orthogonal Frequency-Division Multiplexing (OFDM) 802.11n/ac/ax: 4x4 MIMO with 4 Streams	
Overall Test Result	Pass: □	Fail: □	

4.16.5.5: Wireless PHY rate

Test ID	**4.16.5.5: Wireless PHY rate**		
Requirement	PHY Rate: 500 Mbps (2.4GHz) 2048 Mbps(5 GHz)		
Test Objective	PHY Rate: 500 Mbps (2.4GHz) 2048 Mbps(5 GHz)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	From the data sheet WiFi ❖ 802.11b/g/n/ac/ax. 2.4GHz Wi-Fi2x2 MIMO up to 600Mbps,5GHzWi-Fi 4x4MIMO up to 4.8Gbps.	
Overall Test Result	Pass: □	Fail: □	

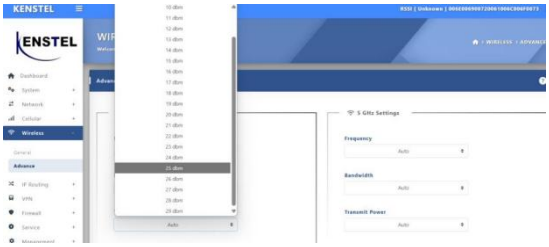
4.16.5.6: IPv4/IPv6 support

Test ID	4.16.5.6: IPv4/IPv6 support		
Requirement	IPv4 and IPv6 dual stack support		
Test Objective	IPv4 and IPv6 dual stack support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In Web GUI for CPE, Under Network, Check for IPv4 and IPv6 support	 	
Overall Test Result	Pass: □	Fail: □	

4.16.6.a: Wireless Antenna

Test ID	4.16.6.a: Wireless Antenna		
Requirement	Integrated Omni directional Antenna		
Test Objective	Integrated Omni directional Antenna		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check from the data sheet for Antenna details	From the data sheet Antenna WLAN :Four (4) Internal 3/5 dBi Dual-Concurrent Omni-Directional Antenna| N-Type WWAN: Four (4) Internal 5dBi dBi Wide BAnd Omni-Directional Antenna WWAN MMWAVE: QTM527 with 64 dual polarization antenna elements capable of transmitting power of more than 40dBm (Power Class 1)	
Overall Test Result	Pass: □	Fail: □	

4.16.6.b: Transmit power

Test ID	4.16.6.b: Transmit power		
Requirement	TransmitPower: 25dBm on 2.4GHz; 25dBm on 5GHz		
Test Objective	Integrated Omni directional Antenna		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Check from the data sheet for Antenna details And also from Web GUI: Wireless> Advanced	Transmit Power 2.4 GHz: 26 dBm | 5 GHz: 26 dBm From Web GUI:  	
Overall Test Result	Pass: □	Fail: □	

4.16.6.c: Receiver Sensitivity

Test ID	4.16.6.c: Receiver Sensitivity		
Requirement	Supports-95dBm or better Receiver Sensitivity		
Test Objective	Supports-95dBm or better Receiver Sensitivity		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
Overall Test Result	Pass: □	Fail: □	

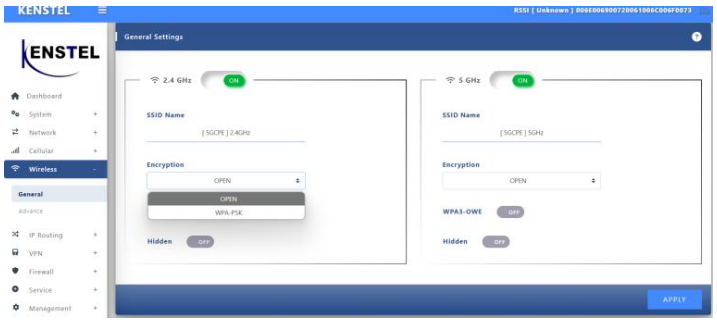
4.16.6.d: RF Management

Test ID	**4.16.6.d: RF Management**		
Requirement	Supports RF Management		
Test Objective	Supports RF Management		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data shee	❖ 5G RF: 100 MHz envelope tracking, Adaptive antenna tuning ❖ Performance Enhancement Technologies: Qualcomm 5G PowerSave, Qualcomm Signal Boost, Qualcomm Smart Transmit technology, Qualcomm RF Gaming Mode Boost, Qualcomm Wideband Envelope Tracking	
Overall Test Result	Pass: □	Fail: □	

4.16.6.e: RF Control Plane

Test ID	**4.16.6.e: RF Control Plane**		
Requirement	Intelligent RF control plane for self-healing and self-optimization		
Test Objective	Intelligent RF control plane for self-healing and self-optimization		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	❖ 5G RF: 100 MHz envelope tracking, Adaptive antenna tuning ❖ Performance Enhancement Technologies: Qualcomm 5G PowerSave, Qualcomm Signal Boost, Qualcomm Smart Transmit technology, Qualcomm RF Gaming Mode Boost, Qualcomm Wideband Envelope Tracking	
Overall Test Result	Pass: □	Fail: □	

4.16.7.c Security: All version and latest WPA Support

Test ID	4.16.7.c Security: All version and latest WPA Support		
Requirement	All version and latest WPA Support		
Test Objective	All version and latest WPA Support		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from Kenstel Web GUI : Wireless > General Settings	Support for WPA-PSK Encryption algorithm can be verified 	
Overall Test Result	Pass: □	Fail: □	

4.16.7 e Security: IPSec,PPTP,IP-Filtering

Test ID	4.16.7 e Security: IPSec,PPTP,IP-Filtering		
Requirement	IPSecurity (IPSec),PPTP, IP-Filtering		
Test Objective	IPSecurity (IPSec),PPTP, IP-Filtering		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	❖ VPN client service (L2TP, PPTP)	
Overall Test Result	Pass: □	Fail: □	

4.16.7g MAC address authentication

Test ID	4.16.7g MAC address authentication		
Requirement	MAC address authentication		
Test Objective	MAC address authentication		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet. Also in Web GUI: Firewall >Anti ARP Spoofing, there is an option to bind MAC address which helps in MAC address collision	**Wireless Security** WPA2 AES-PSK/WPA2 Enterprise Hide SSID in Beacons MAC Address Filtering, Up to 32 MACs per SSID Wireless STA (Client) Connected List Https SSH Client Isolation	
Overall Test Result	Pass: □	Fail: □	

4.16.8 a Interface

Test ID	4.16.8 a Interface		
Requirement	2x1000 Base-T Ethernet		
Test Objective	2x1000 Base-T Ethernet		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	**Physical Interface** 1x 10/100/1000/2500 BASE-T, RJ-45 Ethernet Port 1x 10/100/1000 BASE-T, RJ-45 Ethernet Port	
Overall Test Result	Pass: □	Fail: □	

4.16.8 b SIM Slot

Test ID	4.16.8 b SIM Slot		
Requirement	1X SIM card slot (Nano-SIM)		
Test Objective	1X SIM card slot (Nano-SIM)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	physical verification		
Overall Test Result	Pass: □	Fail: □	

4.16.8 c POE

Test ID	4.16.8 c POE		
Requirement	Power on Ethernet or DC Power		
Test Objective	Power on Ethernet or DC Power		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	From the data sheet, Physical verification or Web GUI	Power Source Power-over-Ethernet: 802.3af/at or Proprietary 48V |IEEE 802.11e Compliant Source| Active Ethernet (PoE)	
Overall Test Result	Pass: □	Fail: □	

4.16.9.1 Management

Test ID	4.16.9.1 Management		
Requirement	Management: Standalone (via GUI) or through on premise based solution or cloud-based		
Test Objective	Management: Standalone (via GUI) or through on premise based solution or cloud-based		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	The management wepage is accessible via the gateway ip of the CPE either via the ethernet or wifi connectivity		
Overall Test Result	Pass: □	Fail: □	

4.16.9.3 IEEE 802.11e Standard

Test ID	4.16.9.3 IEEE 802.11e Standard		
Requirement	Compliant with IEEE 802.11e Standard		
Test Objective	Compliant with IEEE 802.11e Standard		Remarks
Test Description	Set Steps	Acceptance Criteria	
	Verify from the data sheet	QoS (Quality of Service) Compliant with IEEE 802.11e Standard | WMM	
Overall Test Result	Pass: □	Fail: □	

4.16.9.4 Intelligent RF Control Plane for self-healing and Self-Optimization

Test ID	**4.16.9.4 Intelligent RF Control Plane for self-healing and Self-Optimization**		
Requirement	Intelligent RF Control Plane for self-healing and Self-Optimization		
Test Objective	Intelligent RF Control Plane for self-healing and Self-Optimization		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Verify from the data sheet	❖ Self-configuring, Self-healing mesh	
Overall Test Result	Pass: □	Fail: □	

Section 4.17 5G Camera

S.no	Description
4.17.1	Advanced AI/ML video analytics
4.17.2	Supports Sub-6G bands: FR-1, N78
4.17.3	SIM Card Supported
4.17.4	Interfaces 10/100/1000 Ethernet port. Audio Port Alarm Port
4.17.5 (a)	5M / 8M effective resolution
4.17.5 (b)	Wide Dynamic Range (WDR)=120dB
4.17.5 (c)	IR distance
4.17.5 (d)	Memory: Micro SD & SDXC slot up to 256GB
4.17.6 (a)	Lens: Motorized, vary focal (2.7mm-13.5mm).
4.17.6 (b)	Field of View (FOV): Horizontal – 98 Deg wide. Vertical – 50 Deg wide.
4.17.6 (c)	Focus and IRIS Control: Auto
4.17.7 (a)	Video Compression: H.265 / H.264 / MJPEG or equivalent
4.17.8	Power: PoE (802.3at)
4.17.1	Advanced AI/ML video analytics
4.17.2	Supports Sub-6G bands: FR-1, N78
4.17.3	SIM Card Supported
4.17.4	Interfaces 10/100/1000 Ethernet port. Audio Port Alarm Port
4.17.5 (a)	5M / 8M effective resolution
4.17.8	Power: PoE (802.3at)

4.17.1 Advanced AI/ML video analytics

Test ID	**4.17.1 Advanced AI/ML video analytics**		
Requirement	On edge video analytics		
Test Objective	To check edge AI (Face recognition)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Open camera on web. IP:192.168.128.10 Username:admin Password:admin1234 2. Add face in database. 3. Then ask added person to came in front of camera		Verified Face recognition by white list and Black list People
Overall Test Result	Pass: □	Fail: □	

4.17.2 Supports Sub-6G bands: FR-1, N78

Test ID	**4.17.2 Supports Sub-6G bands: FR-1, N78**		
Requirement	Supports Sub-6G bands: FR-1, N78		
Test Objective	Supports Sub-6G bands: FR-1, N78		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Camera support N78 band, it can be verified by latching camera over N78 band frequency	verify by login also by https://192.168.128.1	
Overall Test Result	Pass: □	Fail: □	

4.17.3 SIM Card Supported

Test ID	**4.17.3 SIM Card Supported**		
Requirement	SIM card supported		
Test Objective	SIM card Supported		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	. Nano Sim card supported it can be verified on hardware.		
Overall Test Result	Pass: □	Fail: □	

4.17.4 Interfaces

10/100/1000 Ethernet port.

Audio Port

Alarm Port

Test ID	**4.17.4 Interfaces** **10/100/1000 Ethernet port.** **Audio Port** **Alarm Port**		
Requirement	Interface 10/100/1000 Ethernet port.Audio Port Alarm Port		
Test Objective	Interface 10/100/1000 Ethernet port.Audio Port Alarm Port		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	All these options can be verified on hardware.		
Overall Test Result	Pass: □	Fail: □	

4.17.5 (a) 5M / 8M effective resolution

Test ID	**4.17.5 (a) 5M / 8M effective resolution**		
Requirement	5M / 8M effective resolution		
Test Objective	5M / 8M effective resolution		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Image sensor is5MP, it can be verified by opening cameraon web also canbe verified by checking RTSP stream properties in VLC player.	Login gui 192.168.128.10 and go to Encode setting: select **5M / 8M effective resolution**	
Overall Test Result	Pass: □	Fail: □	

4.17.5 (b) Wide Dynamic Range (WDR)=120dB

Test ID	**4.17.5 (b) Wide Dynamic Range (WDR)=120dB**		
Requirement	Wide Dynamic Range (WDR)=120dB		
Test Objective	Wide Dynamic Range (WDR)=120dB		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Supported, it can be verifiedon ground.	Verify by light off near camera and Outside on and check feed in MEC	
Overall Test Result	Pass: □	Fail: □	

4.17.5 (c) IR distance

Test ID	**4.17.5 (c) IR distance**		
Requirement	IR distance		
Test Objective	IR distance		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Supported = 30meter, it can beverified on ground.	**Verify by image taken from far end**	
Overall Test Result	Pass: □	Fail: □	

4.17.5 (d) Memory: Micro SD & SDXC slot up to 256GB

Test ID	**4.17.5 (d) Memory: Micro SD & SDXC slot up to 256GB**		
Requirement	Memory: Micro SD & SDXC slot up to 256GB		
Test Objective	Memory: Micro SD & SDXC slot up to 256GB		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Micro SD card support, it Canbe verified on hardware.	Insert Micro SD Card in slot in and verify by login 192.168.128.10 memory space in camera	
Overall Test Result	Pass: □	Fail: □	

4.17.6 (a) Lens: Motorized, vary focal (2.7mm-13.5mm).

Test ID	**4.17.6 (a) Lens: Motorized, vary focal (2.7mm-13.5mm).**		
Requirement	Lens: Motorized, vary focal (2.7mm-13.5mm)		
Test Objective	Lens: Motorized, vary focal (2.7mm-13.5mm)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Yes, it can be tested on ground.	It can be focus in focus out as per desire focal length by GOI login 192.168.128.10	
Overall Test Result	Pass: □	Fail: □	

4.17.6 (b)Field of View (FOV):

Horizontal – 98 Deg wide.

Vertical – 50 Deg wide.

Test ID	**4.17.6 (b)Field of View (FOV): Horizontal – 98 Deg wide. Vertical – 50 Deg wide.**		
Requirement	Field of View (FOV) : Horizontal – 98 Deg wide. Vertical – 50 Deg wide.		
Test Objective	Field of View (FOV) : Horizontal –98 Degwide. Vertical – 50 Deg wide.		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Complied, it canbe tested on ground	It can be verify by put Image sensors size and lens details on any FOV calculation plateform. And as per data sheet.	
Overall Test Result	Pass: □	Fail: □	

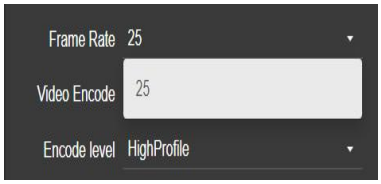
4.17.6 (c) Focus and IRIS Control: Auto

Test ID	**4.17.6 (c) Focus and IRIS Control: Auto**		
Requirement	Focus and IRIS Control: Auto		
Test Objective	Focus and IRIS Control: Auto		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Complied, it can be tested on ground.	As per data sheet	
Overall Test Result	Pass: □	Fail: □	

4.17.7 (a) Video Compression: H.265 / H.264 / MJPEG or equivalent

Test ID	**4.17.7 (a) Video Compression: H.265 / H.264 / MJPEG or equivalent**		
Requirement	Video Compression: H.265 / H.264 / MJPEG or equivalent		
Test Objective	Video Compression: H.265 / H.264 / MJPEG orequivalent		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	H.264/265 Supported, it can be verified bro camera webinterface		
Overall Test Result	Pass: □	Fail: □	

4.17.7 (a) Frame Rate = 1 -30/60

Test ID	**4.17.7 (a) Frame Rate = 1 -30/60**		
Requirement	Frame Rate = 1 -30/60		
Test Objective	Frame Rate = 1 -30/60		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1.25/30 Supported, it can be verified bro camera webinterface.		
Overall Test Result	Pass: □	Fail: □	

4.17.8 Power: PoE (802.3at)

Test ID	**4.17.8 Power: PoE (802.3at)**		
Requirement	Power: PoE (802.3at)		
Test Objective	Power: PoE (802.3at)		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Supported, it can be tested byusing PoE switch.	**Verify Physically**	
Overall Test Result	Pass: □	Fail: □	

5G LAB

User Acceptance Test

Document history

Version	Date	Author	Change Sections	Change Description / reference

Contents

1	**Introduction**	**4**
1.1	**Purpose and Scope**	**4**
1.2	**Terms and Abbreviations**	**4**

1 Introduction

This UAT document serves the purpose of ensuring that the software/hardware meets the business requirements and is ready for deployment by validating its functionality in a real-world environment. It allows end-users to test the software/hardware to ensure it meets their needs and operates as expected, helping to identify and fix any issues before the final release. UAT is crucial for quality assurance and customer satisfaction, as it ensures that the software/hardware is user-friendly, reliable, and meets all specified criteria.

1.1 Purpose and Scope

This document is referred to as a UAT document which will be used for acceptance testing and confirmation of the 5G Lab up and running. The purpose of this document is to validate systems, and networks for users. UAT ensures that the system can handle real-world tasks and perform to development specifications. Users are allowed to interact with the system before its official release to see if any features were overlooked or if any bugs exist. This document is meant for stakeholders, customers, institutes, testers.

1.2 Terms and Abbreviations

The following table contains terms and abbreviations used in this project either directly explained or translated accordingly:

Term / abbreviation	Explanation

Section 4.1: - Physical Material Verification

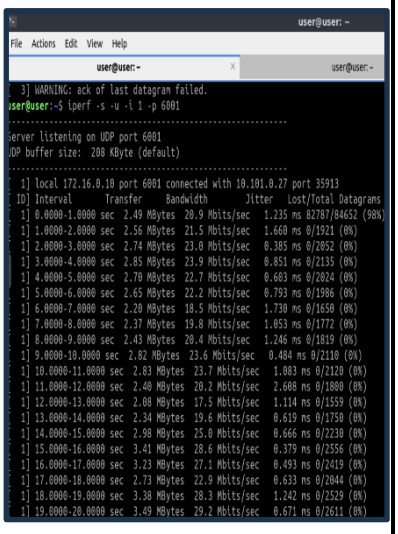
Equipment/Device Checklist/Spec verification				
SN	**Equipment/Devices**	**Qty**	**Make/Model**	**Sr No**
1	**5G Core**	**1**		
2	**5G Radio**	**1**		
3	**IMS solution**	**1**		
4	**MEC & Application server**	**1**		
5	**NMS (with Dashboard)**	**1**		
6	**Router with Firewall**	**1**		
7	**5G SIMs(4 Digit phy no+IMSI)**	**50**		
8	**5G Evaluation Board / Hardware and Software Development Kit.**	**1**		
9	**IoT Gateway**	**1**		
10	**IoT sensors with analytic software (Loaded in Application server)**	**4**		
10.1	**Temperature &; Humidity sensor**	**1**		
10.2	**Light sensor**	**1**		
10.3	**Soil sensor (NPK)**	**1**		
10.4	**Water (TDS/chlorine) sensor**	**1**		
11	**5G Mini Drone**	**1**		
12	**5G XR(AR/VR/MR)**	**1**		
13	**5G Indoor CPE**	**1**		
14	**5G Camera with AI enabled Video Analytic (Face/Object/Motion detection, people counting etc.)**	**1**		
15	**5G Handsets(IMEI No)**	**2**		
16	**Adjustable Tripod Pole (3m)**	**1**		
17	**24 U Rack**	**1**		
18	**UPS 5KVA (1hr backup)**	**1**		
19	**32 inch FHD Display + VGA cable**	**1**		
20	**L2 Managed Switch (24 port)**	**1**		
21	**Testing & Tracing Tools(Version)**	**1**		

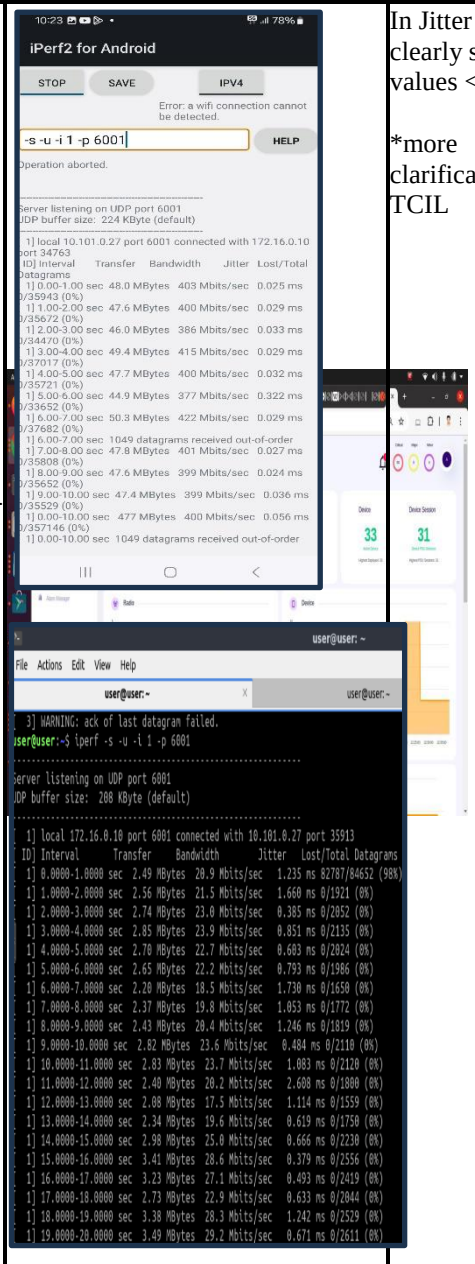
Section 4.2:- 5G Network specs (Core+RAN)

Test ID	**4.2 (i) Radio Configuration**		
Requirement	**Radio Configuration should be as RFP submitted**		
Test Objective	**To Check Radio Configuration for Disintegrated RAN.**		**Remarks**
ption	**Set Steps**	**Acceptance Criteria**	
	Physical verification of CU,DU and RU. **Login CU/DU(172.16.0.4)with following :** **ssh candor@172.16.0.4** **Password-wisig321** **To go to root login :** **sudo su** **cd /home/candor/SMO/gNB_O1_hdl/O-RAN/Slot0/l2l3/gNB_CU/cfg** **ls** **vi TR196_gNodeB_CU_Data_Model.xml** **cd /home/candor/SMO/gNB_O1_hdl/O-RAN/Slot0/l2l3/gNB_DU/cfg** **ls**	**Radio is configured disintegrated with RU, DU & CU** **User will be Logged in to home location of CU/DU I.e candor@candor:** **TR196_gNodeB_CU_Data_Model.xml** **TR196_gNodeB_DU_Data_Model.xml** **<!-- F1AP IP address -->**	**This is a CU config file.** **This is the DU config file.**
		<IPInterfaceIPAddre	

	vi TR196_gNodeB_DU_Data_Model.xml **Search F1AP** **RU Login from DU** **ssh root@192.168.4.50** **Password :vvdn**	**ss>172.16.1.4</IPInterfaceIPAddress>** **root@vvdn_lpru:~$**	**F1ap is a protocol between CU and DU.** **IP addresses between CU and DU can be located under F1AP protocol.** **FH Split B/W DU and RU (High Phy at DU Side and Low Phy at RU side)**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (ii) 3GPP Release**		
Requirement	**Rel 15 Compliant & upgradable to Rel 16 (by Sep 2024)**		
Test Objective	**To check 5G Lab setup follow Rel 15 and above releases.**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.2 (iii) Data Rate (DL+UL)		
Requirement	>= 200Mbps		
Test Objective	To check End User experience for 5G services.		Remarks
Test Description	Set Steps	AcceptanceCriteria	
	For DL throughput checking: 1. Running iperf server inside the mobile app (iperf2 for android) **Command:** -s -u -i 1 -p 6001 **2. Login to the iperf vm of Core server to pump DL traffic at rate of 400mbps to UE** **Command:** iperf -c 10.101.0.x -l1400 -i 1 -p 6001 -b 400m -t 999999 -u **For UL throughput checking:** 1. Running the iperf server inside the iperf vm of Core server **Command:** iperf -s -u -i 1 -p 6001 2. From the mobile app pumping the UL traffic to the iperf vm of Core Server (iperf2 for android) at rate of 20mbps **Command:** iperf -c 172.16.0.10 -l1400 -i 1 -p 6001 -b 20m -t 999999 -u	 	
Overall Test Result	**Pass:** □	**Fail:** □	

Test ID	4.2 (iv) Latency		
Requirement	<=15ms Upgrade to Rel 16 should meet the latency as per the 3GPP standards		
Test Objective			Remarks
Test Description	Set Steps	Acceptance Criteria	
	For DL latency checking: 2. Running iperf server inside the mobile app (iperf2 for android) **Command:** -s -u -i 1 -p 6001 **2. Login to the iperf vm of Core server to pump DL traffic at rate of 400mbps to UE** **Command:** iperf -c 10.101.0.x -l1400 -i 1 -p 6001 -b 400m -t 999999 -u **For UL latency checking:** 3. Running the iperf server inside the iperf vm of Core server **Command:** iperf -s -u -i 1 -p 6001 4. From the mobile app pumping the UL traffic to the iperf vm of Core Server (iperf2 for android) at rate of 20mbps **Command:** iperf -c 172.16.0.10 -l1400 -i 1 -p 6001 -b 20m -t 999999 -u		In Jitter part clearly shows values <=15ms *more clarification from TCIL
Overall Test Result	**Pass:** □	**Fail:** □	

Test ID	4.2 (v) Max No. of active devices (That network can connect)

Requirement	**30 (min)**		
Test Objective	**To verify at least 30 devices should be connected at same time.**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Open UE simulator in edge cloud by following: **NMS->Edgecloud->5G Core server->Niralsimulator->** **VMdetails->open Qterminal** **Register UE Simulator by below commands:** **./start_gnb.sh-->(Terminal1)** **sudo ./build/nr-ue -c config/niralos-ue.yaml -n 30 -------- >(Terminal2)** **Password:Niral@12345**	**Devices connected more than 30 minimum shown in PDU Session**	**It is verified that 33 devices connected in Radio Networks**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (vi) Radio Power**		
Requirement	**Upto 100mW**		
Test Objective	**To verify output power**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	After login RU, check all channels radiating power. **Login to RU console and run below command to getRU power per port:** **tail -f /media/sd-mmcblk0p4/TransceiverStatistics.txt**	**Transmitter Statistics** ************************ **PA Output Power : 19.29 dBm** **Antenna Output Power : 16.29 dBm**	**Out power should be 20 dbm(100mw)**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.2 (vii) Duplexing Mode		
Requirement	TDD		
Test Objective	Need to check system compatibility in TDD mode		Remarks
Test Description	Set Steps	Acceptance Criteria	
	Login RU from CU/DU FH Interface(ens2f3) ssh root@192.168.4.50 Password:vvdn Check the RU Configuration File. sysrepocfg --edit=cat -d running	root@vvdn_lpru:~$ Verify following under Tx and Rx array carriers <absolute-frequency-center>643452</absolute-frequency-center> <center-of-channel-bandwidth>3651780000</center-of-channel-bandwidth>	In TDD ,the same frequency is Configured for Both Uplink and Downlink Path . The Same can be observe in UE/Mobile
Overall Test Result	Pass: □	Fail: □	

Test ID	4.2 (viii) Channel Bandwidth		
Requirement	20MHz, 40MHz, 60MHz, 80MHz, 100MHz		
Test Objective	To verify different bandwidth supported by radio units.		Remarks
Test Description	Set Steps	Acceptance Criteria	
	Login to RU and check Band & BW supported byRatio Unit. tail -f /media/sd-mmcblk0p4/TransceiverStatistics.txt	CHANNEL NO : 1,2,3,4 ---------- Band : N78 [3.6Ghz - 3.8Ghz] BandWidth 100 MHz Tx frequency : 3651780000 Hz	Bandwidth showing 100Mhz Verified in MobTracing Tool (G-nettracker)

	Verify Bandwidth in attached 5G devices.	**Rx frequency : 3651780000 Hz**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (ix) Band support**		
Requirement	**n78 (Must be Tunable to center frequency with desired channel bandwidth-100MHz in the whole n78 band i.e 3300MHz to 3800MHz)**		
Test Objective	**To verify that device is supporting n78 band with desired channel bandwidth**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	Login to RU and check Band & BW supported byRatio Unit. **tail -f /media/sd-mmcblk0p4/TransceiverStatistics.txt** **Verify center frequency inattached 5G devices.**	**CHANNEL NO : 1,2,3,4** **----------** **Band : N78 [3.6Ghz - 3.8Ghz]** **BandWidth 100 MHz** **Tx frequency : 3651780000 Hz** **Rx frequency : 3651780000 Hz**	**Radio Supportedn78** **Verify in Mob Tracing Tool (G-nettracker)**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (x) MIMO Configuration**		
Requirement	**2T2R (min)**		
Test Objecti ve	**To verify MIMO supported by 5G Lab Setup**		**Remarks**
Test Descripti	**Set Steps**	**Acceptance Criteria**	

on	**Login to RU and open configuration file to check Layer configure and verify with radio counters using below command.** **Configuration at RU Side** **cat /etc/configs/iot_config.xml** **cd /etc/scripts** **ls** **Run the script:** **./stat_ru.sh**	**<prach_layer0_PCID >4</prach_layer0_PC ID>** **<prach_layer1_PCID >5</prach_layer1_PC ID>** **<prach_layer2_PCID >6</prach_layer2_PC ID>** **<prach_layer3_PCID >7</prach_layer3_PC ID>** **<pxsch_layer0_PCID >0</pxsch_layer0_PC ID>** **<pxsch_layer1_PCID >1</pxsch_layer1_PC ID>** **<pxsch_layer2_PCID >2</pxsch_layer2_PC ID>** **<pxsch_layer3_PCID >3</pxsch_layer3_PC ID>** **stat_ru.sh** **----------** **eCPRI Framer U/L COUNTERS** **----------** **U/L U-PLANE** **------ AT LAYER 0 : 27456** **------ AT LAYER 1 : 27520** **------ AT LAYER 2 : 27568** **------ AT LAYER 3 : 27648** **U/L U-PLANE PRACH** **------ AT LAYER 0 : 5196** **------ AT LAYER 1 : 5208** **------ AT LAYER 2 : 5220** **------ AT LAYER 3 : 5226**	**Configuration atRU Side** **Output Packets at RU Side.**

		------ Total No. of UL Pkts o/p are : 132667	
Overall Test Result	**Pass: □**	**Fail: □**	

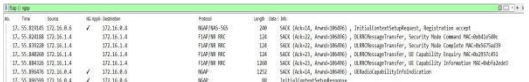
Test ID	**4.2 (xi) Synchronization**		
Requirement	**IEEE 1588**		
Test Objective			**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Physical verification of sync by LED at RU . **By Command** **tail -f /var/log/synctimingptp2.log |grep sync**	**Sync LED Should be Green .** **[2024-07-02_11:23:56.041418] LOOPCONTROL(101): error 2 ns, e_variation 2 ns, slope 49.926, s_variation 0, delay 313, synchronized**	**Synchronization B/W RU and DUWill be shown as synchronized**
Overall Test Result	**Pass: □**	**Fail: □**	

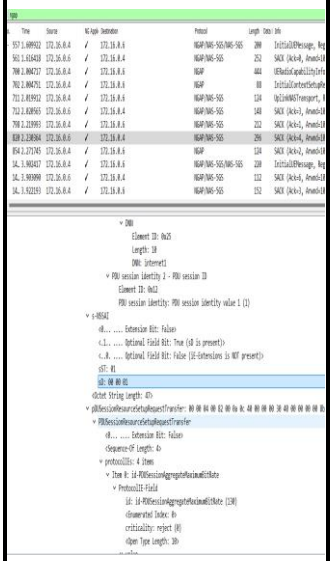
Test ID	**4.2 (xii) Antenna**		
Requirement	**External or Internal**		
Test Objective	**To verify antenna type used**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	Physical Test of radio unit connected with external or internal antenna.	**Internal antenna attached to Radio Unit**	**Internal antenna inbuilt inside themechanical.**
Overall Test Result	**Pass: □**	**Fail: □**	

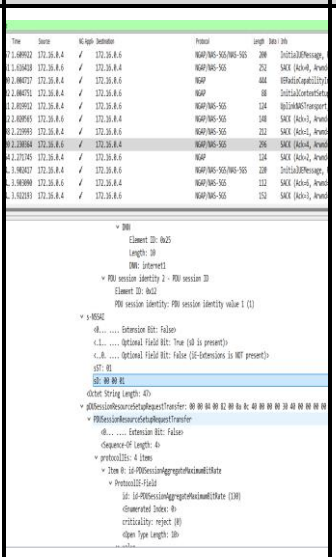
Test ID	**4.2 (xiii) Mechanical/Environmental**		
Requirement	**IP54/QM333 wherever applicable. (Environmental Testing). Temperature andHumidity as per the Indian Geographical conditions**		
Test Objecti ve			**Remarks**
Test Descripti on	**Set Steps**	**Acceptance Criteria**	
	Operating Temperature: -40 to 55C **IP 65** **root@vvdn_lpru:** **tail -f /media/sd-mmcblk0p4/temp_log.txt**	**Required Factory Test report attached** **Temperature Sensor 0 : 52** **Temperature Sensor 1 : 45** **Temperature Sensor 2 : 52** **Temperature Sensor 3 : 49** **Temperature Sensor 4 : 52** **Temperature Sensor 5 : 0** **Temperature Sensor 6 : 0** **Temperature Sensor 7 : 0**	**5,7 and 8 are reserved for future**
Overall Test Result	**Pass: □**	**Fail: □**	

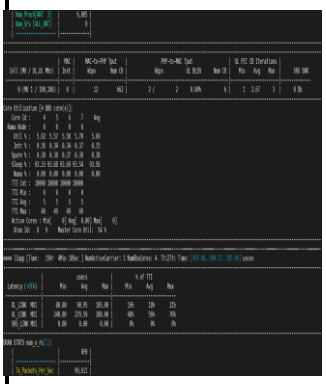
Test ID	**4.2 (xv) Network Slicing**
Requirement	**Support for slicing, Pre-configured 3 different slices (min). Support for configuring slices by Institutions.**



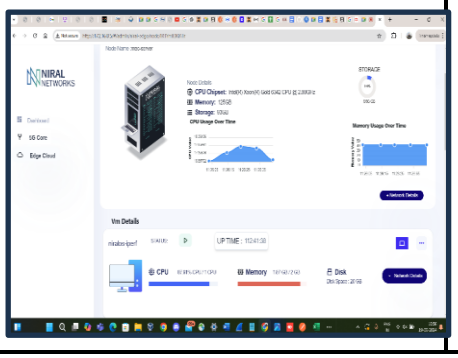
Test Objective			Remarks
Test Description	Set Steps	Acceptance Criteria	
	3 Different Slices configured at RAN and Core end **Slice 1:** **sst: 1 sd: 010203,** **dnn: internet** **Take tcp dump pcap in CU/DU By below command:** **tcpdump -i any -w test.pcap** **Slice 2:** **sst: 1 sd: 000001** **dnn: internet1** **Take tcp dump pcap in CU/DU By below command:** **tcpdump -i any -w test1.pcap** **slice 3: sst: 1 sd: 000002 dnn: internet2** **Take tcp dump pcap in CU/DU By below command:** **tcpdump -i any -w test.pcap** **All 3 Mobiles set APN as internet, internet1 and internet2.**		**In pcap file,opn PDUSessionResourceSetupRequest and check the SD and DNN.** **In pcap file, open PDUSessionResourceSetupRequest message and check the SD and DNN.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.2 (xvi) 5G Use case scenarios

Requirement	**eMBB (R15), URLLC(R16), MMTC (R16)**		
Test Objective	**Test to verify SST -1(eMBB)**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Register mob to 5G NWS **Start capture pcap for observe Embb by following command:** **tcpdump -i any -w test.pcap** **Open with wireshark tool and verify**		**In pcap file,opn PDUSessionResourceSetupRequest and verify sst -1** **sst-2 ,sst-3pending.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (xvii) Uptime**		
Requirement	**99%**		
Test Objective	**Test setup working status with stability**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Login CU/DU **ssh candor@172.16.0.4** **Username :candor** **Password:wisig321** **run command** **cd /home/candor/SMO/gNB_O1_hdl/O-RAN/Slot0/runBharatRan/logs** **In this path run below command:**	**l1app [Time: 15Hr 5Min 40Sec]** 	**Check in log running time**

	tail -f l1_output.txt		
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (xviii) MEC**		
Requirement	**Should support integration with edge compute and cloud platforms.**		
Test Objective			**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Login into NMS Dashboard (172.16.0.5) **User name:admin** **Password :admin@1234** **Go to Edge cloud ->mec-server->details-> create vm**		
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (xix) VoNR**		
Requirement	**Should support VoNR**		
Test Objective	**Verify Voice and Video call over N/W**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	In the roadmap		**Verify Voice andVideo call by VoIP**

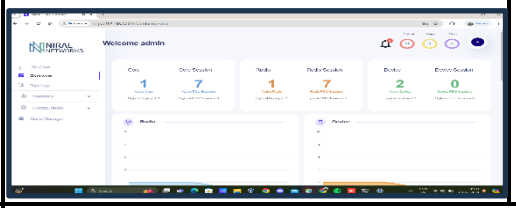
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (xx) APIs**		
Requirement	**Should support APIs – for example any NMS, MEC platform integration, OT/IT integrations.**		
TestObjective	**APIs should be supported in NMS, MEC platformand OT/IT integrations.**		**Remarks**
T	**Set Steps**	**Acceptance Criteria**	

estDescription	**1. Connect any laptop or Desktop Device to theRouter to Attain IP in Range of**
	172.16.0.X/24 Subnet
	2. Open Postman on theconnected Laptop or Desktop
	Niral Networks SDN Controller (NMS API)
	Login:
	Method:
	POST http://IP-ADDRESS:8082/token
	JSON Body:
	{
	"username":"admin",
	"password":"admin@1234"
	}
	
	5G Core Overview:
	Method: GET
	http://172.16.0.5:8082/5gcoredata/overview/range=hour
	Paste the token in the authorization tab inside
		{
		"accessToken": "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImV4cCI6MTcyNjIzMDA5NywiaWF0IjoxNzI2MjI5ODU3fQ.LcOFVve4-yhezaZLvL4VgqmiXRwKNRy9K68jNbg2WWz-dr8hiu0_CaypTui6ImZCT8xrl9aS_zDkSw52K08d6w",
		"refreshToken": "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImV4cCI6MTcyNjI1NjE1NCwiaWF0IjoxNzI2MjI5ODU3fQ.T52fqZx1v8EjDUgorXCyut-CkXvpkQtW2IWIzq99pUafusPMV84OBvBRKspU4msn9UH-t8HMQuwEshDKPr_pPg"
		}
		
		{
		"liveDataModel": {
		"controllerClientId": "ncc-f80JxSJCGBckvLDAwmXflj",
		"activeAmfSession": "0",
		"totalAmfSession": "9",
		"activeamf": "1",
		"totalamf": "1",
		"activeUe": "1",
		"totalUe": "3",
		"activeUeSession": "0",
		"totalUeSession": "0",
		"activeGnb": "1",
		"totalGnb": "1",
		"activeGnbSession": "0",
		"totalGnbSession": "0",
		"siteId": "5G-Lab",
		"tenentId": "TCIL",
		"nfType": "amf",
		"nfName": "niralos-amf-1"
		}
		}
			Is supporting APIs – for example any NMS, MEC platform integration, OT/IT integrations.

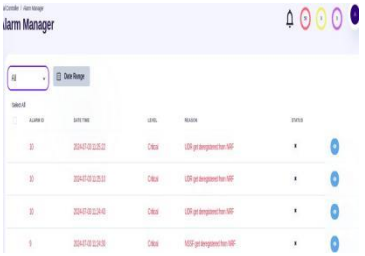
	token portion and then click send		

Overall Test Result	**Pass: □**	**Fail: □**	

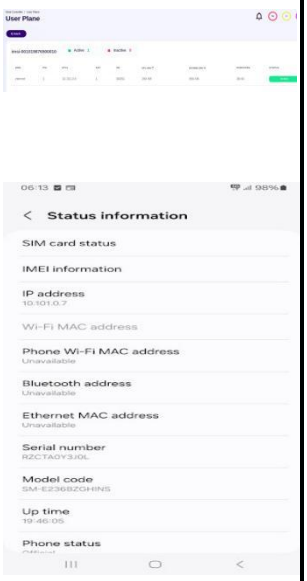
Test ID	4.2 (xxi) NMS with dashboards		
Requirement	Integrated with Core / Radio / other IT devices.		
Test Objective	Verify Core integrated with NMS		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1.Login to 172.16.0.5 2. click on the NiralOS 5G Core icon		
Overall Test Result	Pass: □	Fail: □	

Test ID	4.2 (xxii) Security		
Requirement	Features to ensure system security (security features for Core, RAN and devices, solution for internal and external attack vectors, proactive security monitoring, reporting and alarms, are the security alerts stored including supporting data & logs)Security considerations in deployment of solution – both interface and application level to be considered		
Test Objective	Verify system security		Remarks
Test Description	Set Steps	Acceptance Criteria	

	In postman hit the below url
	
	Method: GET
	
	http://172.16.0.5:8082/edge/node/get_internal_data
		{
		"error": "Full authentication is required to access this resource"
		}
			Session expired, no access to system. Need new Token to accessthe particular system for

			Security.
	For Alarm Monitoring:Login to NMS (172.16.0.5) Click on 5G Core->Alarm Manager		**Particular Alarms showing in NMS Dashboard.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2 (xxiii) 5G Devices**		
Requirement	**All 5G devices to support private PLMN IDs**		
Test Objective			**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Register Device in 5G Networks , check PLMN ID in G-Net Tracker. **cd /home/candor/SMO/gNB_O1_hdl/O-RAN/Slot0/l2l3/gNB_CU/cfg** **ls** **vi TR196_gNodeB_CU_Data_Model.xml** **search PlmnID**	**MCC:001 MNC:01** **TR196_gNodeB_CU_Data_Model.xml** **<PLMNID>00101</PLMNID>**	**Verify PLMN IDin G-Net Tracker android application.** **This is Cu configfile.** **Verify PLMN IDin CU file.**
Overall Test Result	**Pass: □**	**Fail: □**	
Test ID	**4.2 (xxiv) IP communication**		

Requirement	**IPV4 and IPV6 should be supported**		
Test Objecti ve	**To Verify IPV4 Rel15**		**Remarks**
Test Descripti on	**Set Steps**	**Acceptance Criteria**	
	Login to NMS (172.16.0.5) **Dashboard->5G core->Statistics-> Devices->Userplane** **Then click on the imsi values inside UE Information part**		**IPV4 showing inNMS and can beverified in UE.** **IPV4 format showing in particular tab.**
Overall Test Result	**Pass: □**	**Fail: □**	

Section 4.3:- Functional Specifications: 5G SA Core Networks

4.3.2 The 5G System architecture consists of the following network functions (NF).

Test ID	**4.3.2 (a) Authentication Server Function (AUSF)**		
Requirement	**AUSF**		
Test Objective	**To verify authentication server function registration inNRF.**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. AUSF registration with NRF **1.1 AUSF request to NRF:** **HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/d5c3908c-718c-41ef-944a-**	Value: AUSF user-agent: AUSF	AUSF registered with NRF

a17d68dae56e Header: user-agent: AUSF	Value: NRF
Header: 3gpp-sbi-discovery-target-nf-type: NRF	
1.2 NRF response to AUSF: **HEADERS[33]: 201 Created** Header: :status: 201 Created	Value: 201 :status: 201
Json Body: **DATA[33], JSON (application/json) Object** Member: nfInstanceId Member: nfType	Member: nfType [Path with value: /nfType:AUSF] [Member with value: nfType:AUSF] String value: AUSF Key: nfType [Path: /nfType] **Member: nfStatus** **[Path with value: /nfStatus:REGISTERED]** **[Member with value: nfStatus:REGISTERED]** **String value: REGISTERED** **Key: nfStatus** **[Path: /nfStatus]**
Member: nfStatus	
Member: heartBeatTimer Member: nfProfileChangesInd	**Value: nausf-auth**
2. Service provide by AUSF **url : /nausf-auth/v1/ue-authentications** **SBI Interface Refrence Point - N12(Between**	Member: supiOrSuci [Path with value: /supiOrSuci:suci-0-001-01-0-0-0-9876500015] [Member with value: supiOrSuci:suci-0-001-01-0-0-0-9876500015]

	AUSF and AMF) Header: 3gpp-sbi-discovery-service-names: nausf-auth Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: AUSF **Json body: DATA[3], JSON (application/json) Object** Member: supiOrSuci Member: servingNetworkName	Member: servingNetworkName [Path with value: /servingNetworkName:5G:mnc001.mcc001.3gppnetwork.org] [Member with value: servingNetworkName:5G:mnc001.mcc001.3gppnetwork.org]
	SBI Interface Refrence APIs – **API - /nudm-ueau/v1/security-information/generate-auth-data(Between AUSF and UDM)** Method – POST Interface Refrence Point – N13 **Header: 3gpp-sbi-discovery-service-names: nudm-ueau** **Header: user-agent: AUSF** **Header: 3gpp-sbi-discovery-target-nf-type: UDM**	Value: nudm-ueau Value: AUSF user-agent: AUSF Value: UDM

Response from UDM to AUSF	
HEADERS[13]: 200 OK	Value: 200 :status: 200
Header: :status: 200 OK	
DATA[13], JSON (application/json)	String value: 5G_AKA Key: authType
Object	
Member: authType	Member: rand [Path with value: /authenticationVector/rand:16e64004e2c156c1b28fc647f6b88729] [Member with value: rand:16e64004e2c156c1b28fc647f6b88729]
Member: authenticationVector	Member: autn [Path with value: /authenticationVector/autn:27c315cb79a0800038168b97dc39fc70] [Member with value: autn:27c315cb79a0800038168b97dc39fc70] Member: kausf [Path with value: /authenticationVector/kausf:6de380fa118331e5c0415dedce0daa9f68df449b0c6246c91e6bfaaeb22005c8] [Member with value: kausf:6de380fa118331e5c0415dedce0daa9f68df449b0c6246c91e6bfaaeb22005c8] Member: supi [Path with value: /supi:imsi-001019876500015] [Member with value: supi:imsi-001019876500015]
	Value: 201 :status: 201
Member: supi	
Response from AUSF to AMF	
HEADERS[3]: 201 Created	
Header: :status: 201 Created	
DATA[23], JSON (application/3gpphal+json)	
Object	
Member: authType	**Member: authType** **[Path with value: /authType:5G_AKA]**

	Member: 5gAuthData Member: _links	**[Member with value: authType:5G_AKA]** **Member: rand** **[Path with value: /5gAuthData/rand:16e64004e2c156c1b28fc647f6b88729]** **[Member with value: rand:16e64004e2c156c1b28fc647f6b88729]** **Member: autn** **[Path with value: /5gAuthData/autn:27c315cb79a0800038168b97dc39fc70]** **[Member with value: autn:27c315cb79a0800038168b97dc39fc70]**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.3.2 (b) Access and Mobility Management Function (AMF)**		
Requirement	**AMF**		
Test Objective	**Verify Access and Mobility Management Function.**		
	Set Steps	**Acceptance Criteria**	

	AMF registration with NRF: **1.1 AMF request to NRF** **HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/d5810b90-718c-41ef-b1f1-7d1be304863e** Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: NRF **1.2 NRF response to AMF** **HEADERS[19]: 201 Created** Header: :status: 201 Created **Json body:** **DATA[305], JSON (application/json-patch+json)** Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd	**Value: 201** **:status: 201** Member: nfType [Path with value: /nfType:AMF] [Member with value: nfType:AMF] **Member: nfStatus** **[Path with value: /nfStatus:REGISTERED]** **[Member with value: nfStatus:REGISTERED]**	AMF registered with NRF
2.1	**Verification of Communication service API:** - **UE Registration Registration request** **from UE to AMF on N1** **Interface:** **InitialUEMessage,** **Registration request,** **Registration request** **[RRCEstablishmentCause=mo-Signalling]** protocolIEs: 5 items Item 0: id-RAN-UE-	RAN-UE-NGAP-ID: 3 userLocationInformationNR nR-CGI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001)	

NGAP-ID	Mobile Network Code (MNC): Unknown (01)
Item 1: id-NAS-PDU	0000 0000 0000 0000 0000 0000 1101 0000 0101 .... = nRCellIdentity: 0x000000d05
Item 2: id-UserLocationInformation	tAI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) tAC: 12594 (0x003132)
	AMF-UE-NGAP-ID: 4 RAN-UE-NGAP-ID: 3
Item 3: id-RRCEstablishmentCause	s-NSSAI sST: 01 sD: 010203
Item 4: id-UEContextRequest	
Registration accept from AMF to UE **InitialContextSetupRequest, Registration accept**	SecurityKey: a4b983b20924ca89327f0d1760cb7cb0ef86b98c05cd2193d9dcdda745ba4d42 [bit length 256] .... .001 = 5GS registration result: 3GPP access (1)
protocolIEs: 8 items Item 0: id-AMF-UE-NGAP-ID	
Item 1: id-RAN-UE-NGAP-ID	
Item 2: id-GUAMI	AMF-UE-NGAP-ID: 4
Item 3: id-AllowedNSSAI	RAN-UE-NGAP-ID: 3 Message type: Registration complete (0x43)
Item 4: id-UESecurityCapabilities	tAC: 12594 (0x003132)
Item 5: id-SecurityKey	

	Item 6: id-MaskedIMEISV	
	Item 7: id-NAS-PDU	**Value: nausf-auth**
	Registration complete from UE to AMF	
	UplinkNASTransport, Registration complete protocolIEs: 4 items	
	Item 0: id-AMF-UE-NGAP-ID	Member: supiOrSuci [Path with value: /supiOrSuci:suci-0-001-01-0-0-0-9876500015] [Member with value: supiOrSuci:suci-0-001-01-0-0-0-9876500015]
	Item 1: id-RAN-UE-NGAP-ID	Member: servingNetworkName [Path with value: /servingNetworkName:5G:mnc001.mcc001.3gppnetwork.org] [Member with value: servingNetworkName:5G:mnc001.mcc001.3gppnetwork.org]
	Item 2: id-NAS-PDU	
	Item 3: id-UserLocationInformation	
	Service between AMF to AUSF	**Member: authType** **[Path with value: /authType:5G_AKA]** **[Member with value: authType:5G_AKA]**
	url : POST /nausf-auth/v1/ue-authentications	**Member: rand** **[Path with value: /5gAuthData/rand:16e64004e2c156c1b28fc647f6b88729]** **[Member with value: rand:16e64004e2c156c1b28fc647f6b88729]**
	SBI Interface Refrence Point - N12(Between AUSF and AMF) Header: 3gpp-sbi-discovery-service-names: nausf-auth Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: AUSF	**Member: autn** **[Path with value: /5gAuthData/autn:27c315cb79a0800038168b97dc39fc70]** **[Member with value: autn:27c315cb79a0800038168b97dc39fc70]**
	Response from AUSF to AMF **Json body:** **DATA[3], JSON (application/json)** **Object** Member: supiOrSuci	
	Member: servingNetworkName	**Value: 201** **:status: 201**
		Object

	DATA[23], JSON (application/3gpphal+json) Object Member: authType Member: 5gAuthData	**Value: nsmf-pdusession** **Value: AMF** **Value: SMF**	
3.	Member: _links **From AMF to Radio InitialContextSetupRequest, Registration accept** **From Radio to AMF InitialContextSetupResponse** **From Radio to AMF UEContextReleaseRequest [Cause: RadioNetwork=failure-in-radio-interface-procedure]** **From AMF to Radio UEContextReleaseCommand [Cause: RadioNetwork=failure-in-radio-interface-procedure]**		

	From Radio to AMF **UEContextReleaseCompl** **ete**	
	Interface between AMF to SMF on N11 **PDU session control message** **Request from AMF to SMF POST /nsmf-pdusession/v1/sm-contexts** Header: 3gpp-sbi-discovery-service-names: nsmf-pdusession Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: SMF **Response from SMF to AMF HEADERS[111]: 201 Created** **DATA[111], JSON (application/json)** **Stream: DATA, Stream ID: 111, Length 3** **JavaScript Object Notation: application/json**	Member: supi [Path with value: /request/supi:imsi-001019876500015] [Member with value: supi:imsi-001019876500015] Member: accessType [Path with value: /request/accessType:3GPP_ACCESS] [Member with value: accessType:3GPP_ACCESS] Member: uplink [Path with value: /request/ueAmbr/uplink:1048576 Kbps] [Member with value: uplink:1048576 Kbps] Member: downlink [Path with value: /request/ueAmbr/downlink:1048576 Kbps] [Member with value: downlink:1048576 Kbps] String value: 1048576 Kbps
	Interface : **SBI interface reference point N15:** **Between PCF and AMF** **Communication service API: Access Management policies request during Registration request and accept event:** **HEADERS[127]: POST /npcf-am-policy-control/v1/policies** Header: user-agent: AMF	**Value: 201** **:status:201** Member: mcc [Path with value: /guami/plmnId/mcc:001] [Member with value: mcc:001] Member: mnc [Path with value: /guami/plmnId/mnc:01] [Member with value: mnc:01] String value: 01 Key: mnc [Path: /guami/plmnId/mnc] Member: amfId [Path with value: /guami/amfId:020040] [Member with value: amfId:020040

Header: 3gpp-sbi-discovery-target-nf-type: PCF
Header: 3gpp-sbi-target-apiroot: http://172.18.0.7:7777
Header: 3gpp-sbi-max-rsp-time: 10000
Header: 3gpp-sbi-discovery-service-names: npcf-am-policy-control
DATA[127], JSON (application/json)

JavaScript Object Notation: application/json
Object
Member: request
Object
Member: notificationUri
Member: supi

Member: accessType

allowedSnssais
Member: ueAmbr
Object
Member: uplink

Member: downlink

SBI interface reference point N8: Between AMF and UDM: Service:nudm-uecm

AMF to UDM:
Stream: HEADERS, Stream ID: 57, Length 91, PUT /nudm-uecm/v1/imsi-001019876500006/registrations/amf-3gpp-access

	Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: UDM **UDM responses to AMF: Stream: HEADERS, Stream ID: 57, Length 74, 201 Created** **JSON body** Member: mcc Member: mnc Member: amfId		
Overall Test Result	**Pass:** □	**Fail:** □	

Test ID	4.2 (c) Data Network (DN), e.g. operator services, Internet access or 3rd party services		
Requirement	**Data Network(DN)**		
Test Objective	**Verify the Data Network -Internet access by 3rd party service.**		
	Set Steps	**Acceptance Criteria**	
	Ping request from UE to DN: **Echo (ping) request id=0x002a, seq=2/512, ttl=64 (reply in 11)** GPRS Tunneling Protocol TEID: 0x00002f82 (12162) Internet Protocol Version 4, Src: 10.101.0.x (10.101.0.x), Dst: dns.google (8.8.8.8) Source Address: 10.101.0.x (10.101.0.x) Destination Address: dns.google (8.8.8.8) [Stream index: 0] **Ping reply from DN to UE:** **Echo (ping) reply id=0x002a, seq=2/512, ttl=55 (request in 6)** GPRS Tunneling Protocol Flags: 0x34 Message Type: T-PDU (0xff) Length: 92 TEID: 0x00000001 (1) Source Address: dns.google (8.8.8.8) Destination Address: 10.101.0.x (10.101.0.x) [Stream index: 0]	TEID: 0x00002f82 (12162) Source Address: 10.101.0.x Destination Address: dns.google (8.8.8.8) TEID: 0x00000001 (1) Source Address: dns.google (8.8.8.8) Destination Address: 10.101.0.x (101.202.0.2)	**Successfully able to ping internet**
Overall Test Result	**Pass:** □	**Fail:** □	

Test ID	4.3.2 (e)Network Repository Function (NRF)		
Requirement	NRF		
Test Objective	Verify NRF (Network Repository Function)		
	Set Steps	Acceptance Criteria	
	Interface: **SBI** **NF discovery service triggering by SMF for UDM to NRF:** **HEADERS[471]: GET /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=SMF&service-names=nudm-sdm&target-nf-type=UDM** Header: :path: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=SMF&service-names=nudm-sdm&target-nf-type=UDM Header: :authority: niralos-nrf-1:7777 **Response from NRF** **HEADERS[471]: 200 OK** **Json body:** **DATA[471], JSON (application/json)** Object Member: validityPeriod Member: nfInstances Array Object Member:	**Value: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=SMF&service-names=nudm-sdm&target-nf-type=UDM** **Value: niralos-nrf-1:7777** **Value: 200 ok** **:status: 200 ok** **String value: UDM**	**SMF asks the UDM IP to NRF**

	nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: ipv4Addresses Member: nfServiceList	**String vaue: REGISTER** **String value: 172.18.0.5** **Member: serviceName** **[Path with value: /nfInstances/[]/nfServiceList/d5e40b00-718c-41ef-afbc-19030dd1418a/serviceName:nudm-sdm]** **[Member with value: serviceName:nudm-sdm]**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.3.2 (f)Network Slice Selection Function (NSSF)**		
Requirement	**NSSF**		
Test Objective	**Verify the NSSF (Network Slice Selection Function)**		
	Set Steps	**Acceptance Criteria**	

1. **NSSF to NRF register:**

URL: /nnrf-nfm/v1/nf-instances/d6d50d34-718c-41ef-ba2b-77faccd0271f

Header: user-agent: NSSF

Header: 3gpp-sbi-discovery-target-nf-type: NRF

Member: nfServiceList

[Path with value: /nfServiceList/d6d554d8-718c-41ef-ba2b-77faccd0271f/serviceName:nnssf-nsselection]
[Member with value: serviceName:nnssf-nsselection]

Response from NRF to NSSF

HEADERS[61]: 201 Created

Value: 201
:status: 201

Json body:

DATA[61], JSON (application/json)

Object

Member: nfInstanceId

Member: nfType

Member: nfType
[Path with value: /nfType:NSSF]
[Member with value: nfType:NSSF]
String value: NSSF
Key: nfType
[Path: /nfType]

Member: nfStatus

Member: nfStatus
[Path with value: /nfStatus:REGISTERED]
[Member with value: nfStatus:REGISTERED]
String value: REGISTERED
Key: nfStatus
[Path: /nfStatus]

Member: heartBeatTimer

Member: nfProfileChangesInd

Overall Test Result	**Pass: □**		

Test ID	4.3.2 (g)Policy Control Function (PCF)			control/v1/policies Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: PCF Header: 3gpp-sbi-target-apiroot: http://172.18.0.7:7777 Header: 3gpp-sbi-max-rsp-time: 10000 Header: 3gpp-sbi-discovery-service-names: npcf-am-policy-control
Requirement	PCF			
Test Objective	PCF (Policy Control Function)			
	Set Steps	Acceptance Criteria		
	PCF registration with NRF: PCF To NRF: **/nnrf-nfm/v1/nf-instances/e7c0552c-712d-41ef-900a-cfc4690b64be** Header: user-agent: PCF Header: 3gpp-sbi-discovery-target-nf-type: NRF Header: accept: **Response:** **From NRF To PCF** **HEADERS[1]: 201 Created** **DATA[1], JSON (application/json)** Object Member: nfInstanceId Member: nfType Member: nfStatus Member:heartBeatTimer Member: nfProfileChangesInd **Interface :** **SBI interface reference point N15** **Between PCF and AMF** **Communication service API:** **HEADERS[127]: POST /npcf-am-policy-**	**value: 201 :status:201** Member: nfType [Path with value: /nfType:PCF] [Member with value: nfType:PCF] String value: PCF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]		**PCF success fully registe redwith NRF** **DATA[127], JSON (application/json)** JavaScript Object Notation: application/json Object Member: request Object Member: notificationUri Member: supi Member: accessType allowedSnssais Member: ueAmbr Object Member: uplink Member: downlink

	Between PCF and SMF on interface N7 to show session related parameter 5QI value: **HEADERS[55]: POST /npcf-smpolicycontrol/v1/sm-policies** Header: 3gpp-sbi-discovery-service-names: npcf-smpolicycontrol Header: user-agent: SMF Header: 3gpp-sbi-discovery-target-nf-type: PCF Response **Json body: DATA[55], JSON (application/json)** Object Member: sessRules Member: 5qi Member: suppFeat	**Number value: 9** **Key: 5qi** Member: uplink [Path with value: /sessRules/1/authSessAmbr/uplink:1048576 Kbps] [Member with value: uplink:1048576 Kbps] Member: downlink [Path with value: /sessRules/1/authSessAmbr/downlink:1048576 Kbps] [Member with value: downlink:1048576 Kbps] Supported Features: 4000000 ...0 = TSC: False ..0. = ResShare: False .0.. = 3GPP-PS-Data-Off: False 0... = ADC: False ...0 = UMC: False ..0. = NetLoc: False .0.. = RAN-NAS-Cause: False 0... = ProvAFsignalFlow: False ...0 = PCSCF-Restoration-Enhancement: False ..0. = PRA: False .0.. = RuleVersioning: False 0... = SponsoredConnectivity: False ...0 = RAN-Support-Info: False ..0. = PolicyUpdateWhenUESuspends: False .0.. = AccessTypeCondition: False 0... = MultiIpv6AddrPrefix: False ...0 = SessionRuleErrorHandling: False ..0. = AF_Charging_Identifier: False .0.. = ATSSS: False 0... = PendingTransaction: False		**Communication between PCF and UDR on N36 interface to get access management parameters** Request from PCF to UDR GET /nudr-dr/v1/policy-data/ues/imsi-001019876500015/am-data Header: 3gpp-sbi-discovery-service-names: nudr-dr Header: user-agent: PCF Header: 3gpp-sbi-discovery-target-nf-type: UDR Response from UDR to PCF HEADERS[77]: 200 OK		...0 = UP ..0. = Ma .0.. = W 0... = Qo ...0 = Au ..0. = En .1.. = DN 0... = PD Value:201 :status:201 **Member:** **[Path w** **010203/sns** **[Membe** **Member:** **[Path w** **010203/sns** **[Membe** **Membe** **[Path w** **010203/sm** **[Membe**

	Member: smPolicySnssaiData		**Test ID**	**4.3.2 (h)Session Management Func**		
			Requirement	**SMF**		
			Test Objective	**Verify the SMF (Session Manageme**		
				Set Steps		
Overall Test Result	**Pass: □**	**Fail: □**				

	SMF registration with NRF: **SMF To NRF:** **HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/d5dda71a-718c-41ef-b9a9-5b526d41caa7** Header: 3gpp-sbi-discovery-target-nf-type: NRF Header: user-agent: SMF		**SMF successfully Registered with NRF**
	Response from NRF to SMF **HEADERS[41]: 201 Created** **Json body:** **HEADERS[1]: 201 Created** Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd **Service provide by SMF to PCF over N7 interface** **HEADERS[55]: POST /npcf-smpolicycontrol/v1/sm-policies** Header: 3gpp-sbi-discovery-service-names: npcf-smpolicycontrol Header: user-agent: SMF Header: 3gpp-sbi-discovery-target-nf-type: PCF Response **Json body:** **DATA[55], JSON (application/json)** Object Member: sessRules Member: 5qi	Member: nfType [Path with value: /nfType:SMF] [Member with value: nfType:SMF] String value: SMF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	

	Member: suppFeat **Interface between AMF to SMF on N11** **Request from AMF to SMF** **For Session context after PDU Session Request Message** **POST /nsmf-pdusession/v1/sm-contexts** Header: 3gpp-sbi-discovery-service-names: nsmf-pdusession Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: SMF **Response from SMF to AMF** /namf-comm/v1/ue-contexts/imsi-001019876500006/n1-n2-messages DATA[1], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequestTransfer Non-Access-Stratum 5GS (NAS)PDU **Session establishment request from SMF to UPF on N4 inteface** **PFCP Session Establishment Request** Packet Forwarding Control Protocol PDN Type : IPv4 User ID : APN/DNN : internet **Response From UPF to SMF on N4 interface** **PFCP Session Establishment Response** Node ID : IPv4 address: 172.18.0.9 Cause : Request accepted(success)	**Number value: 9** **Key: 5qi** ..00 0001 = Qos flow identifier: 1 Session-AMBR for downlink: 1 Gbps (1) Session-AMBR for uplink: 1 Gbps (1) PDU address information: 10.101.0.2 (10.101.0.2) DNN: internet Member: pduSessionType [Path with value: /pduSessionType:IPV4] [Member with value: pduSessionType:IPV4] IMSI: 001019876500006 Member: dnn [Path with value: /dnn:internet] [Member with value: dnn:internet]	

		IPv4: upf (172.18.0.9) Cause: Request accepted(success) (1) TEID: 0x000720e6	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.3.2 (i) Unified Data Management (UDM)**		
Requirement	**UDM**		
Test Objective	**Verify the UDM (Unified Data Management Function)**		**Reamark**
	Set Steps	**Acceptance Criteria**	

	UDM: **1.UDM registration with NRF:** **1.1UDM To NRF:** **URL: /nnrf-nfm/v1/nf-instances/d5e3d77a-718c-41ef-afbc-19030dd1418a** Header: user-agent: UDM Header: 3gpp-sbi-discovery-target-nf-type: NRF **1.2 Response from NRF to UDM** **Stream: HEADERS, Stream ID: 1, Length 116, 201 Created** **JSON body:** **JavaScript Object Notation: application/json** Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd **2.Service provided by UDM:** **2.1.SBI interface reference point N13: Between AUSF and UDM for authentication related parameters before Authentication request message** **Service : nudm-ueau** **AUSF TO UDM:** **Stream: HEADERS, Stream ID: 23, Length 74, POST /nudm-ueau/v1/imsi-001019876500006/auth-events** Header: user-agent: AUSF Header: 3gpp-sbi-discovery-target-nf-type: UDM **UDM RESPONSES TO AUSF:** **Stream: HEADERS, Stream ID: 25, Length 62, 201 Created** **JSON body:** Object Member: nfInstanceId Member: success	**value: 201** **:status: 201** Member: nfType [Path with value: /nfType:UDM] [Member with value: nfType:UDM] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] **Value: 201** **:status:201** Member: success [Path with value: /success:true] [Member with value: success:true] Member: authType [Path with value: /authType:5G_AKA] [Member with value: authType:5G_AKA]	UDM succesfuully registered with NRF

	Member: timeStamp Member: authType Member: servingNetworkName **2.2.SBI interface reference point N8: Between AMF and UDM for access related parameters after security mode complete** **Service:nudm-uecm** **AMF to UDM:** **Stream: HEADERS, Stream ID: 57, Length 91, PUT /nudm-uecm/v1/imsi-001019876500006/registrations/amf-3gpp-access** Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: UDM **UDM responses to AMF:** **Stream: HEADERS, Stream ID: 57, Length 74, 201 Created** **JSON body** Member: mcc Member: mnc Member: amfId **2.2.SBI interface reference point N10: Between SMF and UDM for session related parameters** **Service: nudm-sdm** **SMF to UDM:** **GET /nudm-sdm/v2/imsi-001019876500006/sm-data** Header: user-agent: SMF Header: 3gpp-sbi-discovery-target-nf-type: UDM Header: 3gpp-sbi-discovery-service-names: nudm-sdm	**Value: 201** **:status:201** Member: mcc [Path with value: /guami/plmnId/mcc:001] [Member with value: mcc:001] Member: mnc [Path with value: /guami/plmnId/mnc:01] [Member with value: mnc:01] String value: 01 Key: mnc [Path: /guami/plmnId/mnc] Member: amfId [Path with value: /guami/amfId:020040] [Member with value: amfId:020040] Member: singleNssai Object Member: sst [Path with value: /[]/singleNssai/sst:1] [Member with value: sst:1] Number value: 1 Key: sst [Path: /[]/singleNssai/sst] Member: sd	

	UDM response to SMF: Stream: HEADERS, Stream ID: 53, Length 77, 200 OK **JSON BODY:** JavaScript Object Notation: application/json Array Object Member: singleNssai	[Path with value: /[]/singleNssai/sd:010203] [Member with value: sd:010203] [Member with value: 5qi:9]	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.3.2 (j) Unified Data Repository (UDR)**		
Requirement	**UDR**		
Test Objective	**Verify the UDR (Unified Data Repository).**		**Remark**
	Set Steps	**Acceptance Criteria**	
	UDR: **1.UDR registration with NRF:** **1.1 UDR To NRF:** **Stream: HEADERS, Stream ID: 1, Length 254, PUT /nnrf-nfm/v1/nf-instances/d6059392-718c-41ef-ada8-b5bbefd3b673** Header: user-agent: UDR Header: 3gpp-sbi-discovery-target-nf-type: NRF **1.2 Response from NRF to UDR**		**UDR successfully registered With NRF**

Stream: HEADERS, Stream ID: 1, Length 117, 201 Created	
	value:201 :status:201
JSON body: **JavaScript Object Notation: application/json**	
Object	
Member: nfInstanceId	
Member: nfType	
	Member: nfType [Path with value: /nfType:UDR] [Member with value: nfType:UDR]
Member: nfStatus	
	Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]
Member: heartBeatTimer	
Member: nfProfileChangesInd	
2.Service provided by UDR:	
2.1.SBI interface reference point N35:	
Between UDM and UDR for subscription related parameters	
Stream: HEADERS, Stream ID: 31, Length 105, GET /nudr-dr/v1/subscription-data/imsi-001019876500006/authentication-data/authentication-subscription	
Header: user-agent: UDM	
Header: 3gpp-sbi-discovery-target-nf-type: UDR	
UDR responses to UDM:	
HEADERS[35]: 200 OK	
	value:201 :status:201
JSON BODY: **JavaScript Object Notation: application/json**	
Object	
Member: authenticationMethod	
	Member: authenticationMethod [Path with value: /authenticationMethod:5G_AKA] [Member with value: authenticationMethod:5G_AKA]
Member: encPermanentKey	Member: encPermanentKey [Path with value: /encPermanentKey:18528600000000000000000000000000

	Member: sequenceNumber Member: encOpcKey	0] [Member with value: encPermanentKey:18528600000000000000000000000000] Member: sequenceNumber Object Member: sqn [Path with value: /sequenceNumber/sqn:00000000d721] [Member with value: sqn:00000000d721] Member: encOpcKey [Path with value: /encOpcKey:bf6e133cd11b662a2ae639219409b7ea] [Member with value: encOpcKey:bf6e133cd11b662a2ae639219409b7ea]	
Overall Test Result	**Pass:** □	**Fail:** □	

Test ID	**4..3.2 (k) User Plane Function (UPF)**		
Requirement	**UPF**		
Test Objective	**Verify UPF (User Plane Function)**		**Remark**
	Set Steps	**Acceptance Criteria**	
	Registration with SMF: **Request from SMF side** **PFCP Association Setup Request over N4 interface** Packet Forwarding Control Protocol Message Type: PFCP Association Setup Request (5) Node ID : IPv4 address: 172.18.0.3 **Response from UPF side** **PFCP Association Setup Response over N4** Packet Forwarding Control Protocol	IPv4: smf (172.18.0.3)	**UPF successfully registered with SMF**

	Message Type: PFCP Association Setup Response (6) Node ID : IPv4 address: 172.18.0.9 Cause : Request accepted(success)	IPv4: upf (172.18.0.9) accepted(success) (1)
	Service API: **Session Connection** **From SMF side to UPF** **PFCP Session Establishment Request on N4** Packet Forwarding Control Protocol Message Type: PFCP Session Establishment Request (50) PDN Type : IPv4 User ID : APN/DNN : internet	.. .001 = PDN Type: IPv4 (1) IMSI: 001019876500006 APN/DNN: internet
	Response from UPF **PFCP Session Establishment Response on N4** Packet Forwarding Control Protocol Message Type: PFCP Session Establishment Response (51) Node ID : IPv4 address: 172.18.0.9 Cause : Request accepted(success) F-SEID : SEID: 0x0000000000003016, IPv4 172.18.0.9	Request accepted(success) (1) SEID: 0x0000000000003016
	From SMF to UPF over N4 interface **PFCP Session Modification Request** Message Type: PFCP Session Modification Request (52) SEID: 0x0000000000003016	
	PFCP Session Modification Response from UPF to SMF over N4 interface Message Type: PFCP Session Modification Response (53) Cause : Request accepted(success)	Cause: Request accepted(success) (1)
	PING service: **UL packet from UE to DN** Echo (ping) request id=0x002a, seq=3/768, ttl=64 (reply in 17) GPRS Tunneling Protocol	

	Extension header (PDU Session container) Internet Protocol Version 4, Src: 101.202.0.2 (101.202.0.2), Dst: 8.8.8.8 (8.8.8.8) Internet Control Message Protocol **DL packet from DN to UE** Echo (ping) reply id=0x002a, seq=7/1792, ttl=55 (request in 36) GPRS Tunneling Protocol Extension header (PDU Session container) Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 101.202.0.2 (101.202.0.2) Internet Control Message Protocol	TEID: 0x00002f82 (12162) QoS Flow Identifier (QFI): 1 TEID: 0x00000001 (1) QoS Flow Identifier (QFI): 1	
Overall Test Result	**Pass:** □	**Fail:** □	

Requirement	**4.4.1. A Functions for Radio Resource Management: Radio Bearer Control, Radio Admission Control, Connection Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling);**		
Test Objective	**Radio Bearer Control, Radio Admission Control,**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Run the tcpdump command to collect PCAP **sudo tcpdump -i any -w filename.pcap** **Check Following Me** **RRC setup request:**	**protocolIEs: 5 items** **Item 0: id-gNB-DU-UE-F1AP-ID** **ProtocolIE-Field** **id: id-gNB-DU-UE-F1AP-ID (41)** **criticality: reject (0)** **Item 1: id-NRCGI** **Item 2: id-C-RNTI** **ProtocolIE-Field** **id: id-C-RNTI (95)** **criticality: reject (0)** **value** **C-RNTI: 20000** **Item 3: id-RRCContainer** **id: id-RRCContainer** **criticality: reject (0)** **ue-Identity: randomValue (1)** **randomValue: xxx (40 Bit)** **establishmentCause: mo-Signalling (3)** **Item 4: id-DUtoCURRCContainer** **Value** **CellGroupConfig** **rlc-BearerToAddModList: 1 item** **mac-CellGroupConfig** **physicalCellGroupConfig** **spCellConfig**	

	RRC Setup

		[Configuration: SRB-1 (direction=Uplink, plane=Signalling)] **NR Radio Resource Control (RRC) protocol** **5G-TMSI: 3221227417 (0xc0000799)** **5GS tracking area identity - Last visited registered TAI** **Element ID: 0x52** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **TAC: 12594** **S-NSSAI 1** **Length: 4** **Slice/service type (SST): eMBB (1)** **Slice differentiator (SD): 66051**	
Overall Test Result	**Pass: □**		

Test ID	4.4.1 a) Dynamic allocation of resources to UEs in both uplink and downlink (scheduling);		
Requirement	Dynamic allocation of resources to UEs in both uplink and downlink (scheduling);		
Test Objective	This test case evaluates the impact of LA on the DL and UL throughput,measuring the throughput achieved under different channel scenarios.		
	Set Steps	Acceptance Criteria	
	1. Connect any commercial UE andensure you get 5G . 2. Once UE is camped, you can goto any browser of your choice e.g. chrome or firefox and type the following URL, www.fast.com. It will start a speed test. 3. While in the middleof the speed test you stop the gNB by terminating PHY, this can be done by giving command stopphy. This will generate afile named PhyStats-c0_wls.txt .	<DlLaInfoParmas> <!-- LA feature enabled or disabled Range : 0:Diabled, 1:Enabled, default : 1 --> <DlLaEnabled>1</DlLaEnabled> <!-- LA feature Mode	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.4.1 (b) Header compression, encryption and integrity protection of data		
Requirement	Ciphering and Integrity Protection		
Test Objective	Verify that the gNB applies security for data protection.		Remarks
	Set Steps	Acceptance Criteria	
	Ciphering And Integrity: **RRC Registration request** **UE Capability Information**	**Item : id-RRCContainer** **[UE Security** (ciphering=NEA0 (NULL), integrity=NIA1 (SNOW3G))] [Ciphering Algorithm: NEA0 (NULL) (0)] [Integrity Algorithm: NIA1 (SNOW3G) (1)] **UE security capability** Element ID: 0x2e Length: 2 1... .... = 5G-EA0: Supported .1.. .... = 128-5G-EA1: Supported ..1. .... = 128-5G-EA2: Supported ...1 .... = 128-5G-EA3: Supported .1.. .... = 128-5G-IA1: Supported ..1. .... = 128-5G-IA2: Supported ...1 .... = 128-5G-IA3: Supported **pdcp-Parameters** **supportedROHC-Profiles** **.... ..0. profile0x0000:** False ....0 profile0x0001: False 0... .... profile0x0002: False	GNB is Supported, if we want verify need a UE logs.	

		.0.. .... profile0x0003: False ..0. .... profile0x0004: False ...0 .... profile0x0006: False .... 0... profile0x0101: False .... .0.. profile0x0102: False .... ..0. profile0x0103: False ....0 profile0x0104: False maxNumberROHC-ContextSessions: cs24 (5) shortSN: supported (0)		
		decompressed messages at UE.		
Overall Test Result	**Pass:** □	**Fail:** □		

Test ID	4..4.1 (c) Routing of User Plane data towards UPF(s)		
Requirement	Routing of User Plane data towards UPF(s)		
Test Objecti ve	Verify that the gNB routes user plane data correctly towards theUPF(s)		Remarks
Test Descripti	Set Steps	Acceptance Criteria	

on	**Verifying data routing from gNB to UPF** **Filter** **NGAP & GTP** **(PDU sessionestablishment acceptt)** **GPRS Tunneling Protocol**	NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceSetupListSUReq PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-**PDUSessionAggregateMaximumBitRate** **Item 1: id-UL-NGU-UP-TNLInformation** **UPTransportLayerInformation: gTPTunnel (0)** **gTPTunnel** **transportLayerAddress: ac100007 XXXX** **TransportLayerAddress (IPv4): 172.16.0.7** **gTP-TEID: 000993d2** Item 2: id-PDUSessionType Item 3: id-QosFlowSetupRequestList Item 3: id-UEAggregateMaximumBitRate	**Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.7** **Tunnel created successfully for user plane data towards UPF** **UL-NGU-UP-TNLInformation For Routing of gnb to UPF** **gTP-TEID: 000993d2**

Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4..4.1 (d) Routing of Control Plane information towards AMF;**		
Requirement	**Routing of Control Plane information towards AMF**		
Test Objective	**Verify that the gNB routes control plane informationcorrectly towards the AMF.**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	Filter NGAP in a PCAP **Registration Reqest** **Gnb to AMF**	**protocolIEs: 4 items** **Item 0: id-GlobalRANNodeID** **Item 1: id-RANNodeName** **Item 2: id-SupportedTAList** **value** **SupportedTAList: 1 item** **Item 0** **SupportedTAItem** **tAC: 12594 (0x003132)** **broadcastPLMNList: 1 item** **Item 0** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **tAISliceSupportList: 3 items** **Item 0** **SliceSupportItem** **s-NSSAI** **sST: 01** **sD: 010203**	**Verify** **· gNB successfully routes the control plane signaling message to the AMF.** **· AMF successfully processes the received control plane message & response .**

	NGSetupResponse	**Item 3: id-DefaultPagingDRX** **Item 0: id-AMFName** **ProtocolIE-Field** **id: id-AMFName (1)** **criticality: reject (0)** **value** **AMFName: XYZ-amf0** **Item 1: id-ServedGUAMIList** **Item 2: id-RelativeAMFCapacity** **Item 3: id-PLMNSupportList**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4..4.1 (e) Connection setup and release		
Requirement	Connection setup and release		
Test Objective	Verify that the gNB correctly sets up and releasesconnections with the UE		Remarks
Test Description	Set Steps	Acceptance Criteria	
	Filter NGAP in PCAP (UEContextReleaseRequest)	protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceListCxtRelReq Item 3: id-Cause id: id-Cause (15) criticality: ignore (1) value Cause: radioNetwork (0) radioNetwork: user-inactivity(20)	
	UEContextReleaseCommand	protocolIEs: 2 items Item 0: id-UE-NGAP-IDs Item 1: id-Cause value Cause: radioNetwork (0) radioNetwork: user-inactivity(20)	Release verify by user-inactivity(20)
	UEContextReleaseComplete	protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-PDUSessionResourceListCxtRelCpl PDUSessionResourceListCxtRelCpl: 1 item Item 0 PDUSessionResourceItemCxtRelCpl pDUSessionID: 1	
Overall Test Result	Pass: □	Fail: □	

Test ID	4..4.1 (f) Scheduling and transmission of paging messages;		
Requirement	To Verify the message of paging messages		
Test Objective	verify paging message		Remarks
Test Description	Set Steps	Acceptance Criteria	
	Filter NGAP in PCAP Paging	protocolIEs: 2 items Item 0: id-UEPagingIdentity ProtocolIE-Field id: id-UEPagingIdentity (115) criticality: ignore (1) value UEPagingIdentity: fiveG-S-TMSI (0) fiveG-S-TMSI aMFSetID: 10 Bit() aMFPointer: 6 bit length Item 1: id-TAIListForPaging ProtocolIE-Field id: id-TAIListForPaging (103) criticality: ignore (1) value TAIListForPaging: 1 item Item 0 TAIListForPagingItem tAI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) tAC: 12594	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.4.1 (g)Scheduling and transmission of system broadcast information		
Requirement	To Verify the message of paging messages		
Test Objective	Verify MIB & SIB		Remarks
Test Description	Set Steps	Acceptance Criteria	
	Filter F1ap in Pcap (F1SetupRequest) MIB

Test ID	4.4.4.1 i)Transport level packet marking in the uplink		
Requirement	Transport level Packet marking		
Test Objective	To Verify Transport level packet marking in the uplink		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1.In wireshark capture apply filters 'f1ap || ngap ||gtp'. -NGAP/NAS-5GS PDUSessionResourceSetup Request, DL NAS transport, PDU session establishment accept UE>>>>>UPF	-id-UL-NGU-UP-TNLInformation (139) -UPTransportLayerInformation: gTPTunnel (0) -TransportLayerAddress (IPv4): 172.16.0.7 -gTP-TEID: 00 06 97 a8	Verify the ul gtp Traffic flow in The pcap. Whether it going in the Mentioned Address & teid for a Particular PDU session It is verified the tunnel id, In gtp packets verify: -Version: GTP release 99 version (1) -Message Type: T-PDU (0xff) -TEID: 0x000697a8 (432040)

Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4..4.1 (j) Session Management**		
Requirement	**Session Management**		
Test Objective	**Verify that the gNB can manage sessions correctly.**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	F1AP/NGAP andthen check the PDU session Message in PCAP **PDUSessionResourceSetupRequest,** **DL NAS transport, PDU sessionestablishment accept**	**protocolIEs: 4 items** **Item 0: id-AMF-UE-NGAP-ID** **Item 1: id-RAN-UE-NGAP-ID** **Item 2: id-PDUSessionResourceSetupListSUReq** **· PDU addressinformation: 10.101.0.82** **S-NSSAI** **Slice/service type(SST): eMBB (1)** **Session-AMBR foruplink: 1 Gbps** **(1)gTP-TEID: 00 06** **3f b4** **5QI: 9** **PDU session identity2 - PDU session ID** **Item 2:** **id-PDUSessionType** **Item 3:** **id-UEAggregateMaximumBitRate**	**Verified in wireshark log that PDU session establishment is done.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4..4.1 (k) Support of Network Slicing		
Requirement	Support of Network Slicing		
Test objective	Verify that the gNB supports and manages network slicing correctly.		Remarks
Test Description	Set Steps	Acceptance Criteria	
	In Wireshark filter f1ap & ngap and then check InitialContextSetupRequest, Service accept	protocolIEs: 11 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-UEAggregateMaximumBitRate Item 3: id-GUAMI Item 4: id-PDUSessionResourceSetupListCxtReq Item 5: id-AllowedNSSAI id: id-AllowedNSSAI (0) criticality: reject (0) value AllowedNSSAI: 1 item Item 0 AllowedNSSAI-Item s-NSSAI sST: 01 sD: 010203 Item 6: id-UESecurityCapabilities Item 7: id-SecurityKey Item 8: id-UERadioCapability Item 9: id-MaskedIMEISV Item 10: id-NAS-PDU	Verified in wireshark log N-SSAI Is Allowed
Overall Test Result	Pass: □	Fail: □	

Test ID	4..4.1 (m) Support of UEs in RRC_INACTIVE state		
Requirement	Support of UEs in RRC_INACTIVE state		
Test Objective	This test case verifies the gNB's ability to correctly manage the transition of a User Equipment (UE) to the RRC Inactive state,		Remarks
	Set Steps	Acceptance Criteria	

OverallTest Result	**Pa**

Test ID	4..4.1 (n) Distribution function for NAS messages		
Requirement	Distribution function for NAS messages		
Test Objective	Verify that the gNB correctly distributes NAS messages to theappropriate network entities.		Remarks
	Set Steps	Acceptance Criteria	
	In Wireshark filter f1ap& ngap and then check NAS Message	NGSetupRequest, NGSetupResponse, DownlinkNASTransport, Identity request UplinkNASTransport, Identity response Authentication request, Authentication Parameter RAND - 5G authentication challenge RAND value: fb c6 3b cc 18 52 92 d5 5f 14 53 76 27 18 6e ff AUTN value: d6 d6 8d 29 10 5b 80 00 14 2a ab d1 a2 d6 97 15 Authentication response Message type: Authentication response (0x57) RES: 4e 47 8a a2 85 78 f7 00 0a 25 5c 62 dc 65 a4 41 Registration accept Item 7: id-NAS-PDU Message type: Registration accept (0x42) TAC: 12594 uplinkNASTransport, Registration complete NAS-PDU Message type: Registration complete PDU session establishment request PDU session type: IPv4 Request type: Initial request PDUSessionResourceSetupRequest, PDU session establishment accept PDU address information: 10.101.0.2 S-NSSAI QoS flow description 1 - 5QI 5QI: 9 DNN: internet PDU session identity: PDU session identity value 1 (1) PDUSessionResourceSetupRequestTransfer gTP-TEID: 00 06 3f b4 PDUSessionType: ipv4 (0) qosFlowIdentifier: 1 PDUSessionResourceSetupResponse	· UE successfully forwards the NAS message via gNB to the correct AMF.

		PDUSessionResourceSetupResponseTransfer **TransportLayerAddress (IPv4): 172.16.0.4** **gTP-TEID: 01 00 0f ff**	

Overall Test Result	**Pass: □**	**Fail: □**

Test ID	4..4.1 (l) QoS Flow management and mapping to data radio bearers	
Requirement	QoS Flow management and mapping to data radio bearers	
Test Objective	Verify that the gNB manages QoS flows and maps them correctly to data radio bearers.	Remarks

	Set Steps	Acceptance Criteria	
	In Wireshark filter f1ap &ngap and then check UEContextSetupRequest	protocolIEs: 9 items Item 0: id-gNB-CU-UE-F1AP-ID Item 1: id-gNB-DU-UE-F1AP-ID Item 2: id-SpCell-ID Item 3: id-ServCellIndex Item 4: id-CUtoDURRCInformation Item 5: id-SRBs-ToBeSetup-List dRB-QoS qoS-Characteristics: non-Dynamic-5QI (0) non-Dynamic-5QI fiveQI: 9 nGRANallocationRetentionPriority priorityLevel: highest (1) pre-emptionCapability: shall-not-trigger-pre-emption (0) pre-emptionVulnerability: not-pre-emptable (0) Item 6: id-DRBs-ToBeSetup-List Item 7: id-RRCContainer Item 8: id-GNB-DU-UE-AMBR-UL	QoS Flow management and mapping to data radio bearers is Successful.

Overall Test Result	Pass: □	Fail: □	

4.4.2 NG User Plane:-

Test ID	4.4.3 (a) The NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.		
Requirement	Verify how NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.		
Test Objective	To Verify how NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.		Remarks
	Set Steps	Acceptance Criteria	

	1. In wireshark capture apply filters 'gtp'. **Protocol type: GTP** **PDU Type: DL PDU SESSION INFORMATION (0)** **PDU Type: UL PDU SESSION INFORMATION (1)**	**Source Address: 172.16.0.4** **Destination Address: 172.16.1.4** **Message Type: T-PDU** **Message Type: T-PDU (0xff)** **Length: 1247** **TEID: 0x01001000 (16781312)** **QoS Flow Identifier (QFI): 1** **QoS Flow Identifier (QFI): 1**	**All the user data between RAN & UPF** **flow through GTP packets with extension header - PDU Session container.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.4.3 (b)The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RAN node and the UPF.**	
Requirement	**Verify how The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RAN node and the UPF**	
	To verify the The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP	**Remarks**

Test Description	**Set Steps**	**Acceptance Criteria**	
	In wiresharkcapture apply filters 'gtp'. **observe the gtppackets stack structure**	**ipv4** **Src: 172.16.0.7, Dst: 172.16.0.4** **-User Datagram Protocol,** **Src Port: 2152,** **Dst Port: 2152** **- GPRS Tunneling Protocol.**	**In gtp packets we can observe The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP.**
Overall Test Result	**Pass: □**	**Fail: □**	

TestID	**4.4.3 (c):NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF.**		
Requ irement	**Verify how NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF.**		
Test Objective	**Verify the non-guaranteed delivery of User plane PDU.**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	apply filters ‘f1ap || ngap||gtp’. **DL NAS transport, PDU session establishment accept**	**protocolIEs: 4 items** **Item 0: id-AMF-UE-NGAP-ID** **Item 1: id-RAN-UE-NGAP-ID** **Item 2: id-PDUSessionResourceSetupListSUReq** **QoS flow description 1 - 5QI** **..00 0001 = Qos flow identifier: 1** **001. .... = Operation code: Create new** **QoS flow description (1)** **.1.. .... = E bit: 1** **..00 0001 = Number of parameters:1** **Parameter 1** **Parameter identifier: 5QI (1)** **Length: 1** **5QI: 9** **Item3:UEAggregateMaximumBitRate** **UEAggregateMaximumBitRate** **uEAggregateMaximumBitRateDL: 1073741824bits/s** **uEAggregateMaxim umBitRateUL: 1073741824bits/s**	**The 5QI:9Is mappedto QFI:1. which is non-guaranteed 5QI.All the GTP NG-U traffic packets will transfer through QFI 1.**

Overall Test Result	**Pass: □**	**Fail: □**

Test ID	**4.4.3 (d):NG-U compliance as per 3GPP standards**		
Requirement	**Verify the NG-U compliance as per 3GPP standards**		
Test Objective	**To Verify NG-U compliance as per 3GPP standards**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	1.In wireshark capture apply filters 'gtp'.	**Protocol type: GTP** **Message Type: T-PDU (0xff)** **Next extension header type: PDU Session container (0x85)** **PDU Type: DL PDU SESSION INFORMATION (0)** **QoS Flow Identifier (QFI): 1** **PDU Type: UL PDU SESSION INFORMATION (1)** **QoS Flow Identifier (QFI): 1**	**All the user data between RAN & UPF flow through gtp packets with extension header - PDU Session container.**
Overall Test Result	**Pass: □**	**Fail: □**	

4.4.3 NG Control Plane:-

Test ID	**4..4.4 (a) NG-C provides the following functions:** **(b) NG interface management**		
Requirement	**NG interface management**		
Test Objective	**Verify that the gNB manages the NG interface correctly.**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	In Wireshark filter ngap and then check **NGSetupRequest** **NGSetupResponse**	**NGSetupRequest** **protocolIEs: 4 items** **Item 0: id:** **id-GlobalRANNodeID (27)** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **Item 1: id-RANNodeName** **Item 2: id-SupportedTAList** **SupportedTAList: 1 item** **Item 0** **SupportedTAItem** **tAC: 12594 (0x003132)** **broadcastPLMNList: 1 item** **Item 0** **BroadcastPLMNItem** **pLMNIdentity: 00f110** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **tAISliceSupportList: 3 items** **Item 0** **SliceSupportItem** **s-NSSAI** **SST: 01** **sD:010203** **Item 1** **SliceSupportItem** **s-NSSAI** **sST: 01** **sD: 010203** **Item 3: id-DefaultPagingDRX**	**Verify NG interface connection between gNB and AMF**

	NGSetupResponse	**NGSetupResponse** **protocolIEs: 4 items** **Item 0: id-AMFName** **AMFName: xxxxx-amf0** **Item 1: id-ServedGUAMIList** **Item 1: id-ServedGUAMIList** **ProtocolIE-Field** **id: id-ServedGUAMIList (96)** **criticality: reject (0)** **value** **ServedGUAMIList: 1 item** **Item 0** **ServedGUAMIItem** **gUAMI** **pLMNIdentity:** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **aMFRegionID: 02 [bit length 8]** **aMFSetID: 0040 [bit length 10]** **aMFPointer: 00 [bit length 6]** **Item 2: id-RelativeAMFCapacity** **Item 3: id-PLMNSupportList** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **SliceSupportItem**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4..4.4 (c) UE context management**		
Requirement	**UE context management**		
Test Objective	**Verify that the gNB correctly manages the UE context throughout its lifecycle.**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	In Wireshark filter F1AP and then check UE context management the PCAP **UEContextSetupRequest**	**protocolIEs: 8 items** **Item 0: id-gNB-CU-UE-F1AP-ID** **Item 1: id-gNB-DU-UE-F1AP-ID** **Item 2: id-SpCell-ID** **NRCGI** **pLMN-Identity: 00f110** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **nRCellIdentity: 000000d050 [bit length 36]** **Item 3:idServCellInde** **Item 4: id-CUtoDURRCInformation** **UE-CapabilityRAT-ContainerList: 1 item** **UE-NR-Capability** **pdcp-Parameters** **rlc-Parameters** **mac-Parameters** **phy-Parameters** **phy-ParametersFR1** **rf-Parameters** **nonCriticalExtension** **Item 5: id-SRBs-ToBeSetup-List** **SRBs-ToBeSetup-Item** **sRBID: 2** **Item 6: id-DRBs-ToBeSetup-List** **DRBs-ToBeSetup-Item** **dRBID: 5** **dRB-QoS** **qoS-Characteristics: non-Dynamic-5QI (0)** **fiveQI: 9** **Item 7: id-GNB-DU-UE-AMBR-UL** **Item 7: id-GNB-DU-UE-AMBR-UL** **value** **BitRate: 1073741824**	**Verify** **UE context is created and stored correctly during the attach procedure.** **Successfully created SRB & DRB, Tunnel.**
	UEContextSetupResponse	**protocolIEs: 4 items** **Item 0: id-gNB-CU-UE-F1AP-ID** **Item 1: id-gNB-DU-UE-F1AP-ID** **Item 2: id-DUtoCURRCInformation** **cellGroupConfig** **rlc-BearerToAddModList: 2 items** **RLC-BearerConfig**	.

	.	**servedRadioBearer: srb-Identity (0)** **rlc-Config: am (0)** **mac-LogicalChannelConfig** **spCellConfig** **spCellConfigDedicated** **initialDownlinkBWP** **uplinkConfig** **pdsch-ServingCellConfig: setup (1)** **Item 3: id-DRBs-Setup-List** **DRBs-Setup-List: 1 item** **value** **DRBs-Setup-Item** **dRBID: 5** **dLUPTNLInformation: gTPTunnel (0)** **gTPTunnel** **transportLayerAddress: ac100104 IPv4** **transportLayerAddress: 172.16.1.4 gTP-TEID: 01001000**	

Overall Test Result	**Pass: □**	**Fail: □**

Test ID	**4..4.4 (e) Transport of NAS messages**		
Requirement	**Transport of NAS messages;**		
Test Objective	**Verify that the gNB correctly transports NAS messages between the UE and the core network.**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	filter f1ap & ngapand then check **InitialUEMessage**	**protocolIEs: 5 items** **Item 0: id-RAN-UE-NGAP-ID** **Item 1: id-NAS-PDU** **value** **NAS-PDU:** **Non-Access-Stratum 5GS (NAS)PDU** **010 = Type of identity: 5G-GUTI (2)** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **AMF Region ID: 2** **= AMF Set ID: 1** **= AMF Pointer: 0** **5G-TMSI: 3221227417 (0xc0000799)** **UE security capability** **5G-EA0: Supported** **128-5G-EA1: Supported** **128-5G-EA2: Supported** **128-5G-EA3: Supported** **128-5G-IA1: Supported** **128-5G-IA2: Supported** **128-5G-IA3: Supported** **NAS message container** **Element ID: 0x71** **Length: 48** **Encrypted data** **Item 2: id-UserLocationInformation** **tAI** **pLMNIdentity: 00f110** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **tAC: 12594 (0x003132)** **Item 3: id-RRCEstablishmentCause** **RRCEstablishmentCause: mo-Signalling (3)** **Item 4: id-UEContextRequest** **value** **UEContextRequest: requested (0)**	**Verify** **gNB successfully receives and forwards the NAS message from the UE to the AMF.**
	InitialContextSetupResponse	**protocolIEs: 2 items** **Item 0: id-AMF-UE-NGAP-ID** **ProtocolIE-Field** **id: id-AMF-UE-NGAP-ID (10)** **criticality: ignore (1)** **value** **AMF-UE-NGAP-ID: 17** **Item 1: id-RAN-UE-NGAP-ID**	

		ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: ignore (1) value AMF-UE-NGAP-ID: 17	
	DownlinkNASTransport		
		protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-NAS-PDU NAS-PDU: Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) Spare Half Octet: 0 Security header type: Integrity protected and ciphered (2) Message authentication code: 0x4565d4b1 Sequence number: 27 Encrypted data	
	UplinkNASTransport		
		protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-NAS-PDU NAS-PDU: Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0x65aefa6b Sequence number: 37 Encrypted data Item 3: id-UserLocationInformation Item 3: id-UserLocationInformation ProtocolIE-Field id: id-UserLocationInformation (121) criticality: ignore (1) value UserLocationInformation: userLocationInformationNR (1) userLocationInformationNR nR-CGI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) nRCellIdentity: 0x000000d05	

		tAI **pLMNIdentity: 00f110** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC): Unknown (01)** **tAC: 12594 (0x003132)**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4..4.4 (g) PDU Session Management;**

Requirement	**PDU Session Management;**		
Test Objective	**Verify that the gNB correctly manages PDU sessions.**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	In Wireshark filter F1AP/NGAP and thencheck the PDU sessionMessage in PCAP **PDU session establishment request**		**Verify gNB successfully establishes the session with correct QoS parameters.**
		protocolIEs: 4 items **Item 0: id-AMF-UE-NGAP-ID** **Item 1: id-RAN-UE-NGAP-ID** **Item 2: id-PDUSessionResourceSetupListSUReq** **PDU session type: IPv4** **Request type: Initial request** **PDUSessionResourceSetupRequest,** **PDU session establishment accept** **PDU address information: 10.101.0.2** **S-NSSAI** **QoS flow description 1 - 5QI** **5QI: 9** **DNN: internet** **PDU session identity: PDU session identity value 1 (1)** **PDUSessionResourceSetupRequestTransfer** **gTP-TEID: 00 06 3f b4** **PDUSessionType: ipv4 (0)** **qosFlowIdentifier: 1** **PDUSessionResourceSetupResponse** **PDUSessionResourceSetupResponseTransfer** **TransportLayerAddress (IPv4): 172.16.0.4** **gTP-TEID: 01 00 0f ff** **Item 3: id-UEAggregateMaximumBitRate**	
PDUSessionResourceSetupResponse			
		protocolIEs: 3 items **Item 0: id-AMF-UE-NGAP-ID** **Item 1: id-RAN-UE-NGAP-ID** **Item 2: id-PDUSessionResourceSetupListSURes** **value** **PDUSessionResourceSetupListSURes: 1 item** **Item 0** **PDUSessionResourceSetupItemSURes** **pDUSessionID: 1** **pDUSessionResourceSetupResponseTransfer: 0003e0ac10000401000fff0001** **PDUSessionResourceSetupResponseTransfer**	

Overall Test Result	**Pass: □**	**Fail: □**

Test ID	**4.4.4.j)NG-C compliance as per 3GPP standards**		
Requirement	**Verify the NG-C compliance as per 3GPP.**		
Test Objective	**To Verify the NG-C compliance and to validate Ngap messages as per 3gpp standards.**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	1.In wireshark captureapply filters ‘ ngap’. **Observe the following NGAP messages & respective IE’s:**	**NGSetupRequest** **NGSetupResponse** **UplinkNASTransport** **DownlinkNASTransport** **InitialUEMessage** **UERadioCapabilityInfolndication** **InitialContextSetupRequest** **InitialContextSetupResponse** **PDUSessionResourceSetupRequest** **PDUSessionResourceSetupResponse** **UEContextReleaseCommand** **UEContextReleaseComplete**	**Observe all the mandatory message’s that are specified in 3gPP for UE attach & detach process and observe the following IE’s inside it.**

Overall Test Result	**Pass: □**	**Fail: □**

4.4.7 Radio Protocol Architecture:

Test ID	**4.4.7 (A) RLC procedures: Modes of Data transmission**		
Requirement	**Modes of Data transmission**		
Test Objective	**Verify that gNB supports RLC data transmission modes AM and UM (for DRBs)**		**Remarks**
	Set Steps	**Acceptance Criteria**	

	1. In wireshark capture applyfilters 'f1ap || ngap'. **RRC Reconfiguration**	**protocolIEs: 4 items** **Item 0: id-gNB-CU-UE-F1AP-ID** **Item 1: id-gNB-DU-UE-F1AP-ID** **Item 2: id-SRBID** **Item 3: id-RRCContainer** **sdap-Config** **pdu-Session: 1** **sdap-HeaderDL: absent (1)** **sdap-HeaderUL: present (0)** **.... 1... defaultDRB: True** **mappedQoS-FlowsToAdd: 1 item** **Item 0** **QFI: 1** **pdcp-Config** **drb** **discardTimer: infinity (15)** **pdcp-SN-SizeUL: len18bits (1)** **pdcp-SN-SizeDL: len18bits (1)** **headerCompression: notUsed (0)** **notUsed: NULL** **t-Reordering: ms220 (20)** **cipheringDisabled: true (0)** **rlc-Config: am (0)** **am** **ul-AM-RLC** **sn-FieldLength: size12 (0)** **t-PollRetransmit: ms300 (50)** **pollPDU: p4 (0)** **pollByte: kB10 (4)** **maxRetxThreshold: t32 (7)** **dl-AM-RLC** **sn-FieldLength: size12 (0)** **t-Reassembly: ms5 (1)** **t-StatusProhibit: ms0 (0)** **mac-LogicalChannelConfig**	**1.To verify the SDAP ,PDCP RLC & MAC Layer Parameter Verified.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.4.7 (B &C &D) The Protocol Stack for the control plane Should Perfom the function as detailed in 3GPP Release 15		
Require ment	Control Plane message Verification		
Test Obje ctive	Verify that gNB RLC supports		Remarks
	Set Steps	AcceptanceCriteria	
	RRC Setup Request	protocolIEs: 5 items Item 0: id-gNB-DU-UE-F1AP-ID Item 1: id-NRCGI Item 2: id-C-RNTI Item 2: id-C-RNTI ProtocolIE-Field id: id-C-RNTI (95) criticality: reject (0) value C-RNTI: 20000 Item 3: id-RRCContainer Item 4: id-DUtoCURRCContainer	Control Plane stack verified
	RRC Setup	DLRRCMessageTransfer protocolIEs: 4 items Item 0: id-gNB-CU-UE-F1AP-ID Item 1: id-gNB-DU-UE-F1AP-ID Item 2: id-SRBID Item 3: id-RRCContainer	
	RRC Setup Complete	protocolIEs: 4 items Item 0: id-gNB-CU-UE-F1AP-ID Item 1: id-gNB-DU-UE-F1AP-ID Item 2: id-SRBID Item 3: id-RRCContainer	
	Registration request	InitialUEMessage protocolIEs: 5 items Item 0: id-RAN-UE-NGAP-ID Item 1: id-NAS-PDU	

		Item 2: id-UserLocationInformation **Item 3: id-RRCEstablishmentCause** **Item 4: id-UEContextRequest**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.4.7 (e)NAS control protocol (terminated in AMF on the network side) performs the functions listed in 3GPP Standards.for instance: authentication, mobility management, security control.**		
Requirement	**NAS control protocol**		
Test Objective	**To verify NAS control protocol functions:authentication, mobility management, security control.**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	.In wireshark capture applyfilters ‘’nas-5gs||NGAP||F1AP **Security Mode Command**	**protocolIEs: 4 items** **Item 0: id-gNB-CU-UE-F1AP-ID** **Item 1: id-gNB-DU-UE-F1AP-ID** **Item 2: id-SRBID** **Item 2: id-SRBID** **ProtocolIE-Field** **id: id-SRBID (64)** **criticality: reject (0)** **value** **SRBID: 1** **Item 3: id-RRCContainer** **value** **RRCContainer: 0000220808b56dcd87** **PDCP-NR (SN=0)** **[Configuration: SRB-1 (direction=Downlink, length: 12]** **[MAC-I Present: True]** **[UE Security (ciphering=NEA0 (NULL), integrity=NIA1 (SNOW3G))]** **[Ciphering Algorithm: NEA0 (NULL) (0)]** **[Integrity Algorithm: NIA1 (SNOW3G) (1)]** **securityModeCommand** **rrc-TransactionIdentifier: 1** **criticalExtensions: securityModeCommand (0)** **securityModeCommand** **securityConfigSMC** **securityAlgorithmConfig** **cipheringAlgorithm: nea0 (0)** **integrityProtAlgorithm: nia1 (1)**	

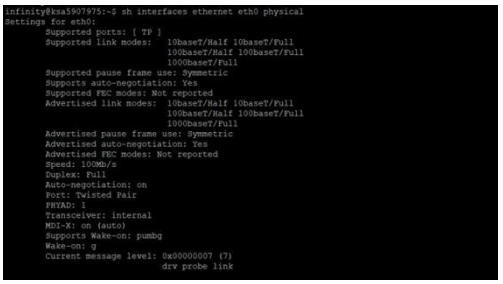
	Security Mode Complete	protocolIEs: 4 items Item 0: id-gNB-CU-UE-F1AP-ID Item 1: id-gNB-DU-UE-F1AP-ID Item 2: id-SRBID ProtocolIE-Field id: id-SRBID (64) criticality: reject (0) value SRBID: 1 Item 3: id-RRCContainer value RRCContainer: 00012a009ccbede4 PDCP-NR (SN=1) [Configuration: SRB-1 (direction=Uplink, plane=Signalling)] [Direction: Uplink (0)] [Plane: length: 12] [MAC-I Present: True] [UE Security (ciphering=NEA0 (NULL), integrity=NIA1 (SNOW3G))] [Ciphering Algorithm: NEA0 (NULL) (0)] [Integrity Algorithm: NIA1 (SNOW3G) (1)] 0000 .... = Reserved: 0 .... 0000 0000 0001 = Seq Num: 1 NR Radio Resource Control (RRC) protocol securityModeComplete (5) securityModeComplete rrc-TransactionIdentifier: 1 criticalExtensions: securityModeComplete (0) securityModeComplete ULRRCMessageTransfer protocolIEs: 4 items Item 0: id-gNB-CU-UE-F1AP-ID Item 1: id-gNB-DU-UE-F1AP-ID Item 2: id-SRBID Item 3: id-RRCContainer	

Overall Test Result	**Pass: □**	**Fail: □**

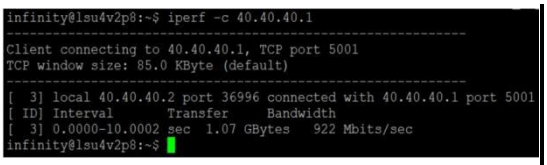
4.8 Firewall with Router / SD-WAN Functional / Technical Specification

4.8.1 Network Interfaces

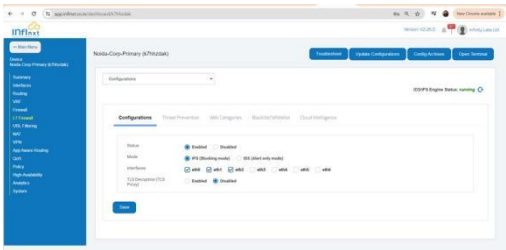
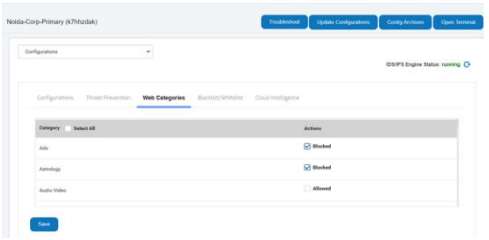
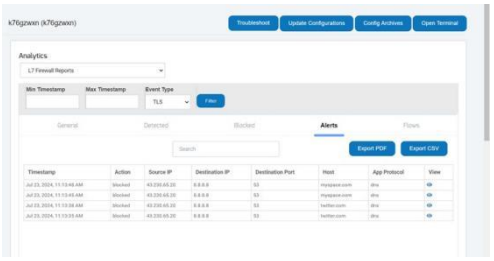
4.8 Firewall with Router

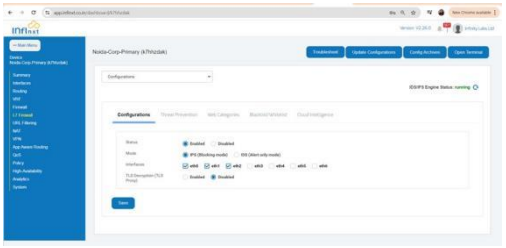
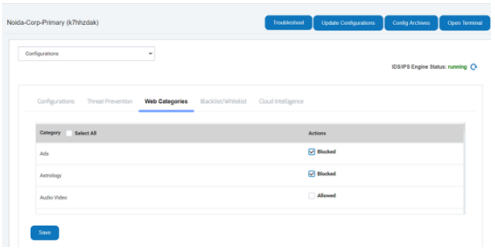
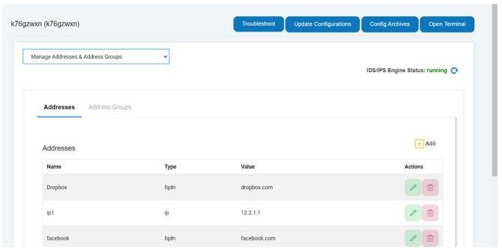
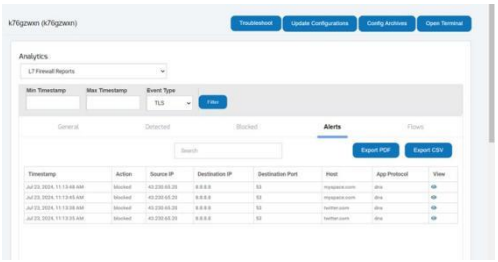
Test ID	4.8.1 Networking Interfaces		
Requirement	Verify 1. Gigabit Base-T (Cu) = 6 ports or higher(as required)and 1 Gs Fiber (SFP) = 4 ports b) WAN Interface 2 x 10 Gigabit Ethernet SFP+ ports c)Management Port 10/100 Mbps RJ 45 Management port		
Test Objective	Test SFP and Ethernet port		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. It can be verified by Physically . Or Run command in Firewall terminal *show interface ethernet <interface> physical* *show interface ethernet <interface> transceiver*	Verify Physically or By Command:  	It can be verified by Physically .
Overall Test Result	Pass: □	Fail: □	

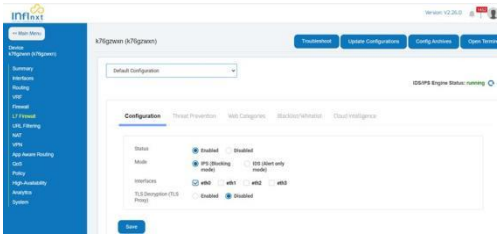
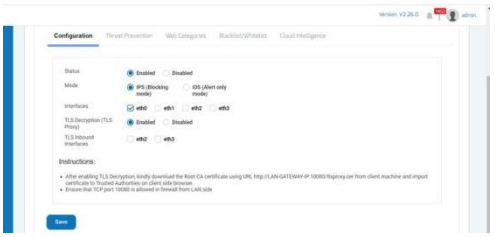
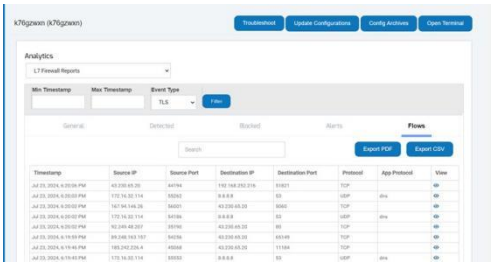
Test ID	4.8.3 Performance requirements		
Requirement	Verify 1 a). Firewall throughput of 1 Gbps b) Threat Protection – 500 Mbps		
Test Objective	Verify Firewall throughput and Threat Protection		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. 1. Connect the SD-WAN devices	Verify Throughput	It can be verified

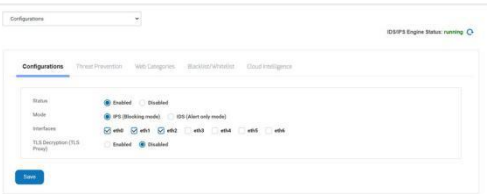
	2. Configure the firewall rules and policies for SD-WAN device. **3. Measure the firewall throughput via iperf tool.** **Threat Protection** **1. Enable and configure the Threat Prevention feature on the SD-** **WAN device.** **2. Verify the signatures and configure the policy** **3. Measure and record the device#39;s performance metrics, including throughput, latency, and CPU utilization.** **4.Verify the test results to identify the SD-WAN device#39;s threat prevention capabilities.**		**1 Gbps**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.8.4 Web Filtering**
Require ment	**Verify 1 a). Control access to websites and website categories (e.g. business, news, sports, social media)b). Integrate into Active Directory, applying policies to specific users or user groups.**

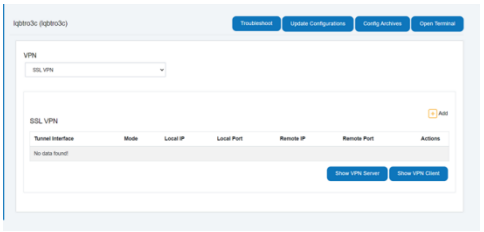
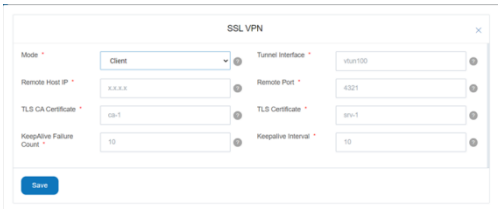
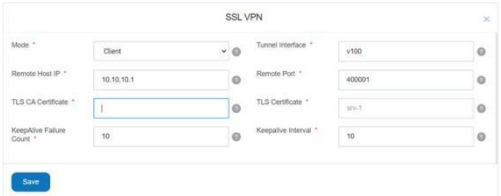
Test Objective	**Verify access controlling**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Configure the SD-WAN device to recognize and categorize websites based on predefined categories (e.g., business, news, sports, social media). **2. Create policy rules specifying which categories are permitted to access.** **3. Test accessing websites from client devices to ensure policies are correctly enforced.** **4.Monitor the performance of the SD-WAN device during testing.**	**Enable the IDS/IPS Mode**  **Select the categories to block**  **Generate the traffic and verify result** 	**Allowed websites and web categories should be accessible.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.8.4 Web Filtering		
Requirement	Verify 1 d). Block or control access to Cloud services.		
Test Objective	Verify Block or control access to Cloud services.		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Login to the controller via UI. 2. Navigate to the L7 firewall tab and then click on web categories. 3. Select the categories user wants to block. 4. Block File Hosting web category or specific site by FQDN/domain name. 5. To block specific websites user needs to configure manage address and address groups.	Enable the IDS/IPS mode  Select the category to block  Configure the address  Verify the logs 	Blocked web categories should not be accessible
Overall Test Result	Pass: □	Fail: □	

Test ID	4.8.4 Web Filtering		
Requirement	Verify 1 e). Detailed web access reports (by user, group, website) f)Full SSL Inspection support		
Test Objective	Verify Detailed web access reports (by user, group, website)		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Login to the controller via UI. 2. Navigate to the L7 firewall tab. 3. Enable the IDSmode with TLS proxy. 4. Generate the traffic and verify the logs. 5. To verify the logs, navigate to the Analytics 6. Select the L7 firewall reports. 7. Verify that L7 reports shows TLS decrypted interface name for SSL decrypted traffic.	Enable the IDS/IPS  Enable the TLS proxy  Verify logs 	Web access reports should be available.
Overall Test Result	Pass: □	Fail: □	

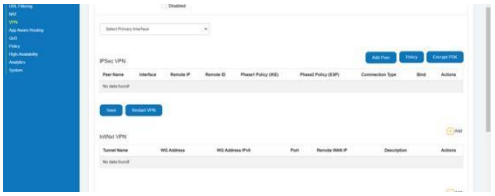
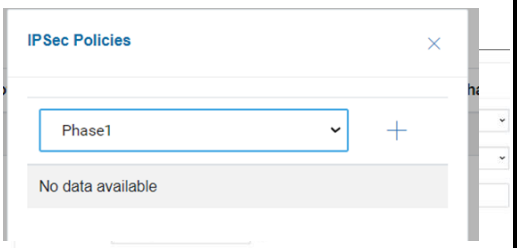
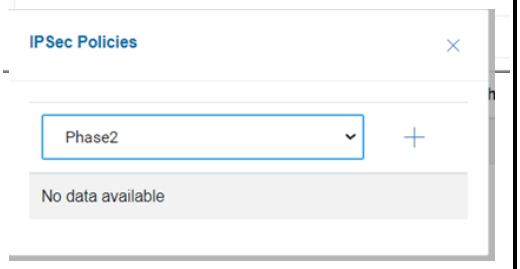
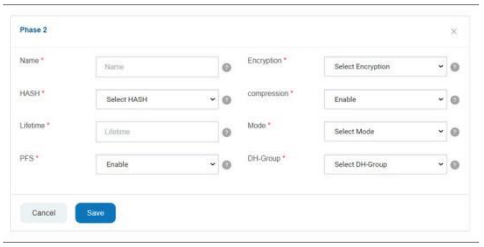
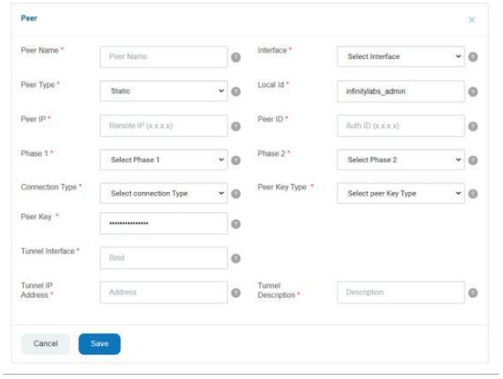
Test ID	4.8.4 Web Filtering		
Requirement	Verify 1 e). Transparent solution (or explicit proxy support)		
Test Objective	Verify Transparent solution (or explicit proxy support)		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Login to thedevice. 2. Configure the necessary firewall policies. 3. Internet should be accessible, when the firewall policies run.	Enable IDS/IPS  Verify Internet works $ ping 101.0.0.1 PING 101.0.0.1 (101.0.0.1) 56(84) bytes of data. 64 bytes from 101.0.0.1: icmp_seq=1 ttl=64 time=0.999 ms 64 bytes from 101.0.0.1: icmp_seq=2 ttl=64 time=0.877 ms 64 bytes from 101.0.0.1: icmp_seq=3 ttl=64 time=0.739 ms 64 bytes from 101.0.0.1: icmp_seq=4 ttl=64 time=1.06 ms --- 101.0.0.1 ping statistics --- 4 packets transmitted, 4 received, 0% packet loss, time 3050ms rtt min/avg/max/mdev = 0.739/0.917/1.055/0.121 ms	Verify that the internet works.
Overall Test Result	Pass: □	Fail: □	

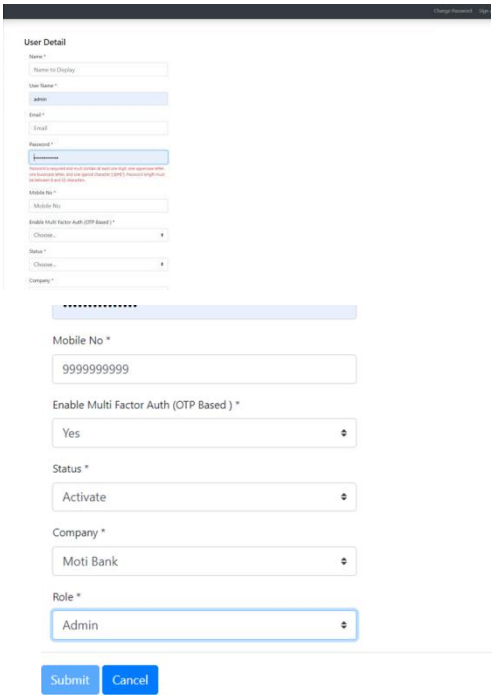
Test ID	4.8.6 Secure Remote Access	
Requirement	Verify 1 a). SSL and IPSec VPN support	
Test Objective	Verify SSL and IPSec VPN support	Remarks

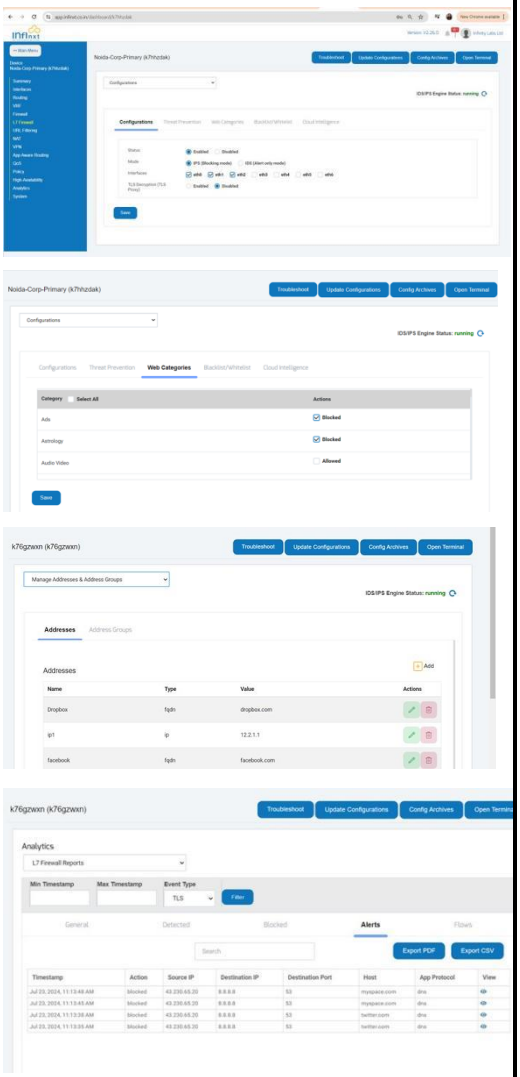
Test Description	Set Steps	Acceptance Criteria	
	1. Log in to the management interface of SD-WAN device (web UI). **2. Navigate to the VPN tab and select SSL VPN.** **3. Configure the policies for the server and the client** **4. Generate SSL certificates for VPN authentication and encryption.** **5. Verify that users can securely access internal resources through the SSL VPN tunnel.** **6.Select the InfiNxt VPN to create the tunnel between the devices.** **7. Configure all the parameters (tunnel name, IP address, etc.)** **8. Verify that the server and the client devices are reachable to each other.**	**Navigate to VPN page and select SSL VPN**   **Conf SSL**  	**SSL and IPSEC VPN must support.**
Overall Test Result	**Pass: □**	**Fail: □**	

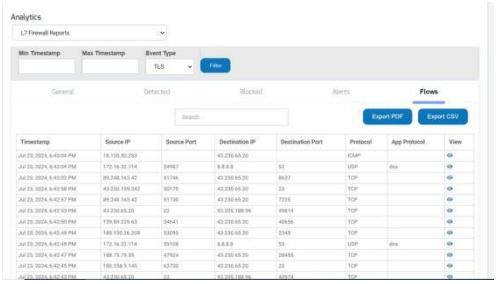
Test ID	4.8.6 Secure Remote Access		
Requirement	Verify 1 b). Web-Portal and full VPN client application		
Test Objective	Verify Web-Portal and full VPN client application		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Login to the controller as web-portal VPN client application exists for RA-VPN. Also, VPN client available with INFIVPN mobile app.	Check Web portal is working fine	It is controlled by web -portat
Overall Test Result	Pass: □	Fail: □	

Test ID	4.8.6 Secure Remote Access		
Requirement	Verify 1 c). Site-to-Site IPSec VPN (with Dynamic Routing)		
Test Objective	Verify Site-to-Site IPSec VPN (with Dynamic Routing)		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1.Connect the SDWAN devices.	Check Web portal is working fine	Site-to-site IPSEC VPN must support.

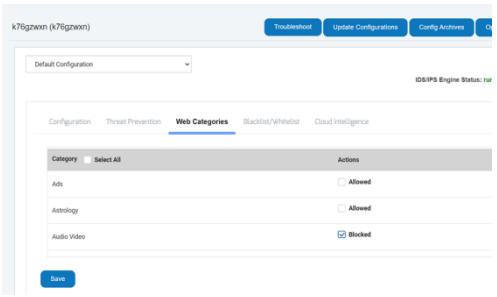
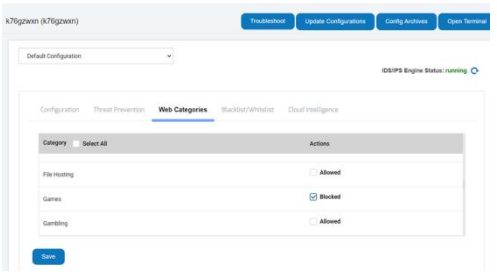
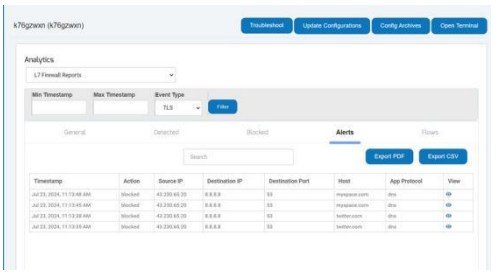
	2.Navigate to the VPN tab to configure the IPSEC VPN. **3. Configure the Phase 1 and Phase 2 parameters including encryption algorithms, authentication methods (like pre-shared keys or certificates), and DH group settings.** **4. Add the peer configuration for the devices.** **5. Verify that both devices have matching IPSec configurations to establish a secure tunnel.** **6.Configure the dynamic routing (OSPF/BGP) on the sdwan devices and verify the neighborship between the devices.** **7.Ping or trace route from devices in each subnet to devices in the opposite subnet.**	**Conf policies for phase-1 and phase-2**     
Overall Test Result	**Pass: □**	**Fail: □**

Test ID	4.8.6 Secure Remote Access		
Requirement	Verify 1 f). Two-Factor authentication support (e.g. Secure Token)		
Test Objective	Verify Two-Factor authentication support (e.g. Secure Token)n		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1.Create a user on the admin portal. 2. Fill all the required details 3. Enable the multi-factor auth. 4.Re-login to the controller and fill the one-time password (OTP). 5. User should be able to login via OTP. OTP based two factor authentication supported for controller login.		SDWAN should supports Two-factor authentication.
Overall Test Result	Pass: □	Fail: □	

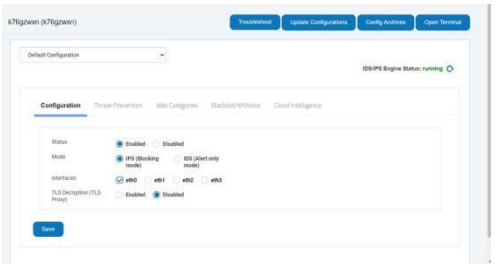
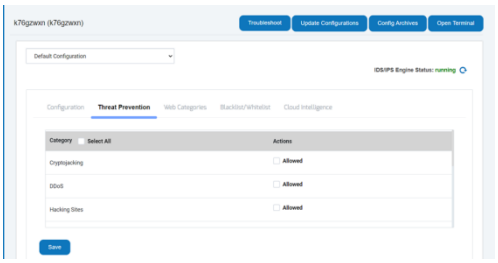
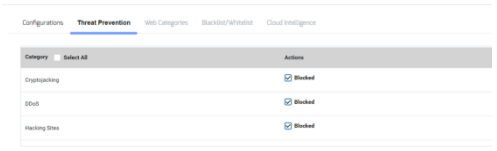
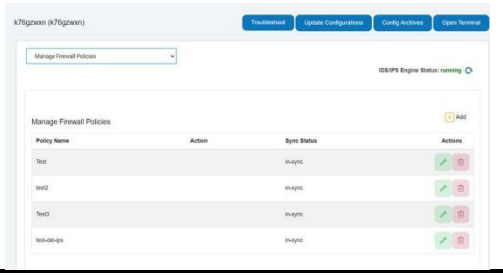
Test ID	4.8.7 Application Control		
Requirement	Verify 1 a). Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps)		
Test Objective	Verify Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps)		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Login to the controller via UI. 2. Navigate to the L7firewall tab and thenclick on web categories. 3. Select the categories user wantsto block. 4. Block File Hosting web category or specific site by FQDN/domain name. 5. To block specific websites user needs to configure manageaddress and addressgroups.		Verify Control and monitor cloudapplication usage
Overall Test Result	Pass: □	Fail: □	

Test ID	4.8.7 Application Control		
Requirement	Verify b). Full network visibility of HTTP and HTTPS traffic		
Test Objective	VerifyFull network visibility of HTTP and HTTPS traffic		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Access the Analytics tab and select L7 firewall tab. 2. Verify the logs from the log table. 3. Verify that inspected HTTP and HTTPs traffic is shown in Flow logs report. 4. User can filter the logs for specific date and time.		Verify Control and monitor cloud application usage
Overall Test Result	Pass: □	Fail: □	

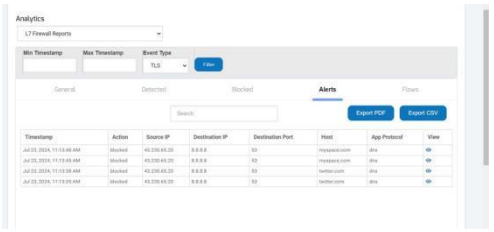
Test ID	4.8.7 Application Control		
Requirement	Verify c). Control access to specific applications (e.g. Web Games, Video Streaming)		
Test Objective	Control access to specific applications (e.g. Web Games, Video Streaming)		Remarks
Test Description	Set Steps	Acceptance Criteria	

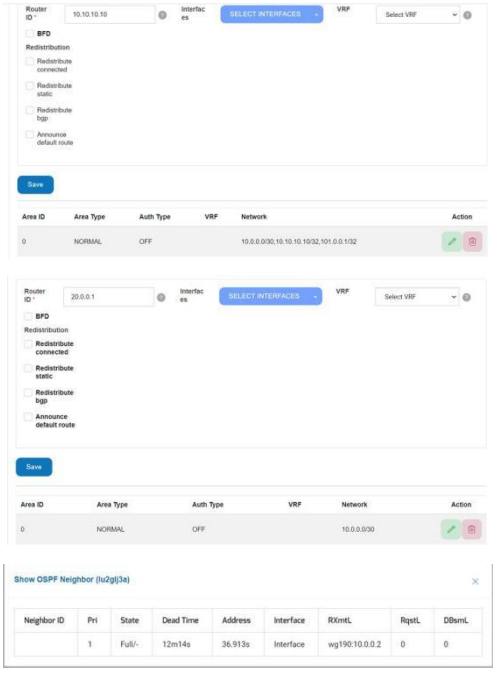
	1. Navigate to the L7 firewall tab. **2. Enable the IDS/IPS mode and click on the web category.** **3. Block the games and audio-video category to block games and video streaming.** **4. Verify ea.com and Netflix/YouTube is blocked.** **5. Verify the logs under L7 reports tab.**	  	**User should be able to control access to specific applications.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.8.7 Application Control**		
Requirement	**Verify d). Block access to malicious content or websites**		
Test Objective	**Verify Block access to malicious content or websites**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Navigate to the L7 firewall tab		**Malicious content should be blocked.**

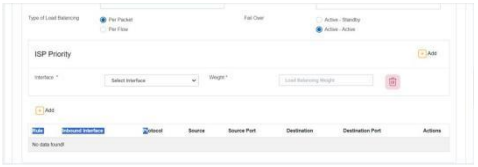
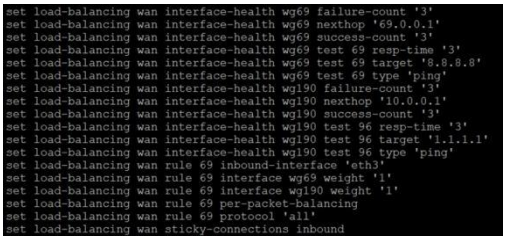
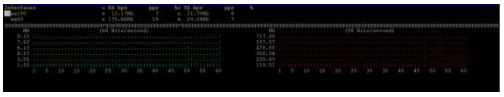
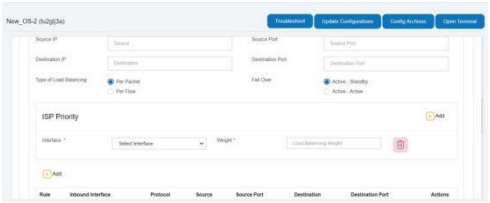
	2. Enable the IDS/IPS mode and click on the threat prevention tab. **3. Select the websitesand block threat prevention categories.** **4. define rules and policies to inspect traffic at the network.** **5.Generate the trafficand verify them.**	   
Overall Test Result	**Pass: □**	**Fail: □**

Test ID	**4.8.7 Application Control**		
Requirement	**Verify e). Detailed reporting and network visibility**		
Test Objective	**VerifyDetailed reporting and network visibility**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	1. Login to the controller via UI. **2. Verify the logs under the L7 firewall tab.**		**Verify Control and monitor cloud application usage**
Overall Test Result	**Pass: □**	**Fail: □**	

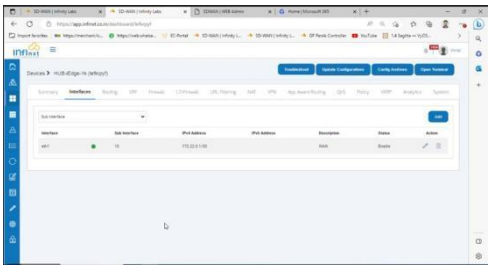
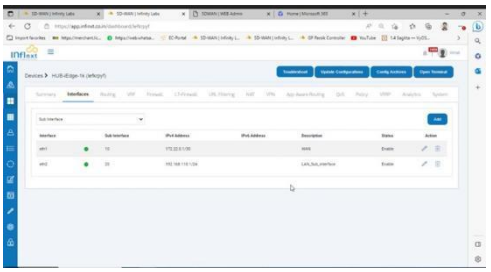
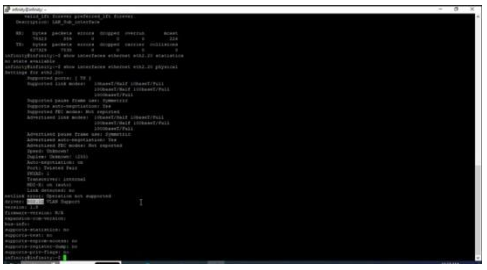
Test ID	**4.8.8 Intelligent Networking**		
Requirement	**Verify a). Dynamic routing (OSPF/BGP/RIP)**		
Test Objective	**VerifyDynamic routing (OSPF/BGP/RIP)**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect a CPE **2. Create an overlay service from one device to another device.** **3. Configure dynamic protocol OSPF on overlay with LAN.** **4. Verify neighborship is established and both the devices are reachable to each other.**		**OSPF routing should support.**

		$ ping 101.0.0.1 PING 101.0.0.1 (101.0.0.1) 56(84) bytes of data. 64 bytes from 101.0.0.1: icmp_seq=1 ttl=64 time=0.999 ms 64 bytes from 101.0.0.1: icmp_seq=2 ttl=64 time=0.877 ms 64 bytes from 101.0.0.1: icmp_seq=3 ttl=64 time=0.739 ms 64 bytes from 101.0.0.1: icmp_seq=4 ttl=64 time=1.06 ms --- 101.0.0.1 ping statistics --- 4 packets transmitted, 4 received, 0% packet loss, time 3050ms rtt min/avg/max/mdev = 0.739/0.917/1.055/0.121 ms	
Overall Test Result	**Pass: □**	**Fail: □**	

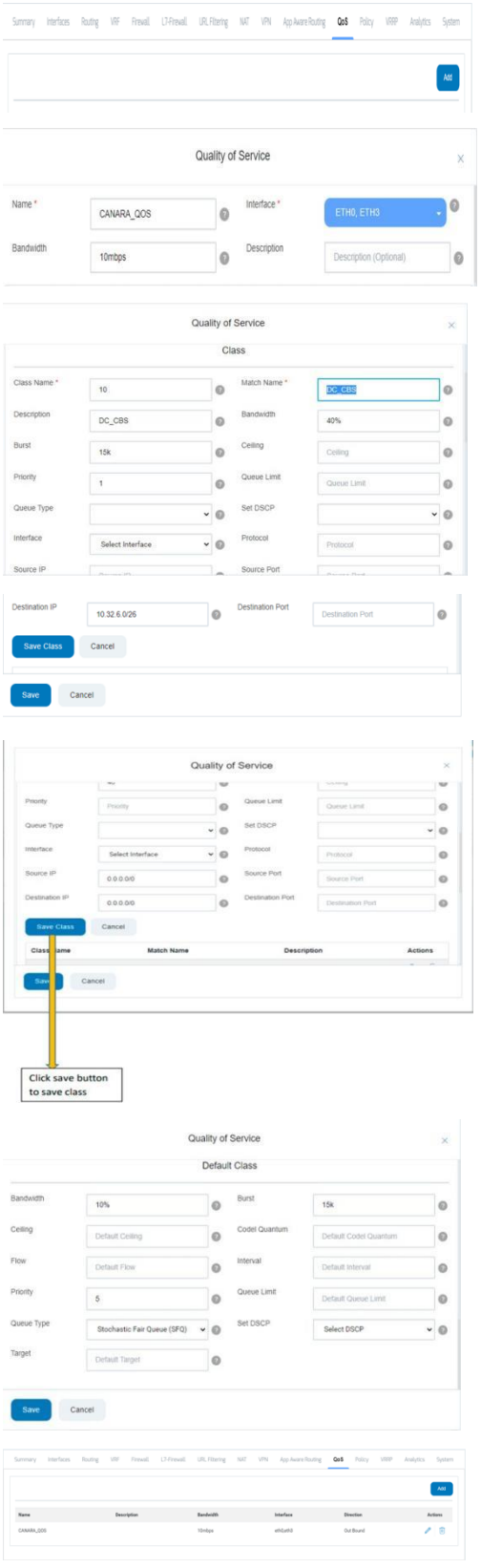
Test ID	**4.8.8 Intelligent Networking**		
Requirement	**b). Load-Balancing and ECMP**		
Test Objective	**VerifyLoad-Balancing and ECMP**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect a CPE with dual uplinks in Active/Active mode. **2. Configure ECMPmode to enable load balancing across multiple links.** **3. Send multiple traffic flows between devices and verify flows are load balanced across multiple uplinks.**	  set load-balancing wan interface-health wg69 failure-count '3' set load-balancing wan interface-health wg69 nexthop '69.0.0.1' set load-balancing wan interface-health wg69 success-count '3' set load-balancing wan interface-health wg69 test 69 resp-time '3' set load-balancing wan interface-health wg69 test 69 target '8.8.8.8' set load-balancing wan interface-health wg69 test 69 type 'ping' set load-balancing wan interface-health wg190 failure-count '3' set load-balancing wan interface-health wg190 nexthop '10.0.0.1' set load-balancing wan interface-health wg190 success-count '3' set load-balancing wan interface-health wg190 test 96 resp-time '3' set load-balancing wan interface-health wg190 test 96 target '1.1.1.1' set load-balancing wan interface-health wg190 test 96 type 'ping' set load-balancing wan rule 69 inbound-interface 'eth3' set load-balancing wan rule 69 interface wg69 weight '1' set load-balancing wan rule 69 interface wg190 weight '1' set load-balancing wan rule 69 per-packet-balancing set load-balancing wan rule 69 protocol 'all' set load-balancing wan sticky-connections inbound   	**Multiple flows should be load balanced across multiple uplinks.**

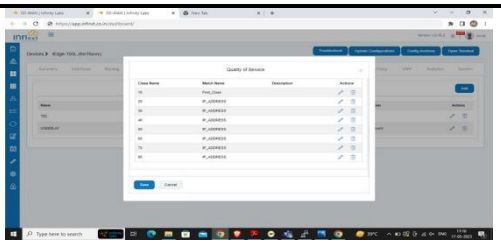
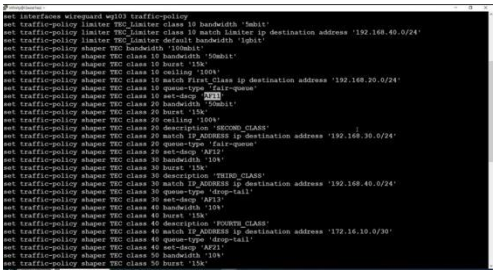
		set load-balancing wan interface-health wg69 failure-count '3' set load-balancing wan interface-health wg69 nexthop '69.0.0.1' set load-balancing wan interface-health wg69 success-count '3' set load-balancing wan interface-health wg69 test 69 resp-time '3' set load-balancing wan interface-health wg69 test 69 target '8.8.8.8' set load-balancing wan interface-health wg69 test 69 type 'ping' set load-balancing wan interface-health wg190 failure-count '3' set load-balancing wan interface-health wg190 nexthop '10.0.0.1' set load-balancing wan interface-health wg190 success-count '3' set load-balancing wan interface-health wg190 test 96 resp-time '3' set load-balancing wan interface-health wg190 test 96 target '1.1.1.1' set load-balancing wan interface-health wg190 test 96 type 'ping' set load-balancing wan rule 69 failover set load-balancing wan rule 69 inbound-interface 'eth3' set load-balancing wan rule 69 interface wg69 weight '5' set load-balancing wan rule 69 interface wg190 weight '3' set load-balancing wan rule 69 protocol 'all' set load-balancing wan sticky-connections inbound infinity@lu2glj3a:~$ Tracing route to google.com [142.250.77.238] over a maximum of 30 hops: 1 <1 ms <1 ms <1 ms 110.0.0.1 2 1 ms 1 ms 1 ms 69.0.0.1 3 1 ms 1 ms 1 ms 192.168.252.254 4 5 ms 5 ms 6 ms 180.151.91.153 5 * * * Request timed out. 6 3 ms 5 ms 13 ms 203.122.50.25 7 9 ms 9 ms 6 ms 72.14.194.202 8 4 ms 5 ms 3 ms 142.251.77.187 ^C **Verify trace route** Tracing route to google.com [142.250.77.238] over a maximum of 30 hops: 1 <1 ms <1 ms <1 ms 110.0.0.1 2 * * 1 ms 10.0.0.1 3 7 ms 2 ms 1 ms 192.168.252.254 4 2 ms 2 ms 2 ms 180.151.91.153 5 * * * Request timed out. 6 3 ms 3 ms 4 ms 203.122.50.25 7 7 ms 6 ms 9 ms 72.14.194.202 ^C C:\Users\infinity>tracert -d -w 1 google.com Tracing route to google.com [142.250.77.238] over a maximum of 30 hops: 1 <1 ms <1 ms <1 ms 110.0.0.1 2 4 ms 1 ms <1 ms 69.0.0.1 3 1 ms 1 ms 1 ms 192.168.252.254 4 8 ms 3 ms 2 ms 180.151.91.153 5 * * * Request timed out. 6 4 ms 3 ms 11 ms 203.122.50.25 7 5 ms 4 ms 4 ms 72.14.194.202 8 14 ms 11 ms 4 ms 142.251.77.187 9 4 ms 4 ms 5 ms 142.251.54.75 10 4 ms 4 ms 5 ms 142.250.77.238 Trace complete.	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.8.8 Intelligent Networking**	
Requirement	**Verify c). 802.1Q VLAN and Layer2 switching support**	
Test Objective	**Verify 802.1Q VLAN and Layer2 switching support**	**Remarks**

Test Description	Set Steps	Acceptance Criteria	
	1. Configure SDWAN CPE WAN port and LAN port with 802.1Q encapsulation from policy management engine. 2. Verify point to point IPs are reachable on LAN port as well as on WAN port with correct 802.1Q VLAN.	   	Point to point IP on LAN and WAN interface should be reachable using correct 802.1Q VLAN.
Overall Test Result	Pass: □	Fail: □	

Test ID	4.8.8 Intelligent Networking	
Requirement	Verify d). Rich traffic/shaping QOS support	
Test Objective	VerifyRich traffic/shaping QOS support	Remarks

Test Description	Set Steps	Acceptance Criteria	
	1. Connect a device and create an overlay service. **2. Configure a QoS policy to mark the traffic flow on overlay service to selective Forwarding class based on DSCP value or 5 tuples.** **3. Map each traffic type with the Forwarding classes.** **4. Configure the queues and respective rates.** **5. Map the forwarding classes to the queues.** **6. Apply QoS configuration on LAN and WAN egress port.**		**Traffic flows should be policed / filtered on ingress and egress ports.**

		 	
Overall Test Result	**Pass: □**	**Fail: □**	

4.9 Server 1 with 5G Core, IMS and NMS software

Test ID	4.9.1 Processor		
Requirement	To verify server 1 Processor		
Test Objective	Processor detail		Remark
	Set Steps	Acceptance Criteria	
	Login server by ILO port. by Google chrome Ip address:172.16.0.12 User Name:Administrator Password:(Mentioned in server) Go to>System Information>Processors	Processor 2.4 GHz or equivalent 24 Core (minimum).	
Overall Test Result	Pass: □	Fail: □	

Test ID	Test ID	4.9.2 Memory		
Requirement	Requirement	To verify server memory DDR4 or above 64 GB scalable upto 256 GB or above		
Test Objective	Test Objective	Verify Memory		Remark
		Set Steps	Acceptance Criteria	
		Login server by ILO port. by Google chrome Ip address:172.16.0.12 User Name:Administrator Password:(Mentioned in server) Go to>System Information>Memory	server memory DDR4 or above 64 GB	

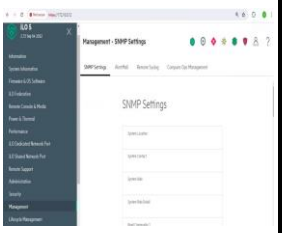
Overall Test Result	**Overall Test Result**	**Pass: □**	**Fail: □**

Test ID	**Test ID**	**4.9.3 Storage**		
Requirement	**Requirement**	**To verify server storage SAS SSD Storage = 1TB**		
Test Objective	**Test Objective**	**Verify storage**		**Remark**
		Set Steps	**Acceptance Criteria**	
		Login server by ILO port. **by Google chrome** **Ip address:172.16.0.12** **User Name:Administrator** **Password:(Mentioned in server)** **Go to>System Information>Storage**	**storage SAS SSD Storage = 1TB**	
Overall Test Result	**Overall Test Result**	**Pass: □**	**Fail: □**	

Test ID	Test ID	4.9.4 Operating System And Virtualization Software		
Requirement	Requirement	To verify Operating System And Virtualization Software		
Test Objective	Test Objective	Verify OS and VS		Remark
		Set Steps	Acceptance Criteria	
		Login serverby Ip address:172.16.0.2 User Name:root Password:(#Niral@7896#) uname -a lscpu |grep Virtualization	Linux pve 5.15.102-1-pve #1 SMP PVE 5.15.102-1 (2023-03-14T13:48Z) x86_64 GNU/Linux root@pve:~# root@pve:~# lscpu |grep Virtualization Virtualization: VT-x root@pve:~#	OS Linux machines also have virtualization enabled.
Overall Test Result	Overall Test Result	Pass: □	Fail: □	

Test ID	Test ID	4.9.5 Network Interface		
Requirement	Requirement	To verify Dual port 1G SFP+ card, 4 x 1G BaseT		
Test Objective	Test Objective	Verify Physically Network Interface		Remark
		Set Steps	Acceptance Criteria	
		Kindly check Physically Network Interface	Dual port 10G SFP+ card, 4 x 1G BaseT	
Overall Test Result	Overall Test Result	Pass: □	Fail: □	

Test ID	Test ID	4.9.6 PCIe Slots		
Requirement	Requirement	To verify PCIe Slots		
Test Objective	Test Objective	To verify PCIe Slots		Remark
		Set Steps	Acceptance Criteria	
		Kindly check Physically Network Interface	Minimum 4 x PCIe 16x 4.0 slots for I/O Connectivity or higher as required.	
Overall Test Result	Overall Test Result	Pass: □	Fail: □	

Test ID	Test ID	4.9.7 Management 4.9.8 Security		
Requirement	Requirement	To verify Management /Security		
Test Objective	Test Objective	To verify Management /Security		Remark
		Set Steps	Acceptance Criteria	
		Login server by ILO port. by Google chrome Ip address:172.16.0.12 User Name:Administrator Password:(Mentioned in server) Go to>Management>Security	Kindly check Management and Security 	
Overall Test Result	Overall Test Result	Pass: □	Fail: □	

4.10 Server 2 with 5G MEC Platform and Application Server

Test ID	4.10.1 Processor		
Requirement	To verify server 1 Processor		
Test Objective	Processor detail		Remark
	Set Steps	Acceptance Criteria	

	Login server by ILO port. by Google chrome Ip address:172.16.0.13 User Name:Administrator Password:(Mentioned in server) Go to>System Information>Processors	Processor 2.4 GHz or equivalent 24 Core (minimum).	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.10.2 Memory		
Requirement	To verify server memory DDR4 or above 64 GB scalable upto 256 GB or above		
Test Objective	Verify Memory		Remark
	Set Steps	Acceptance Criteria	
	Login server by ILO port. by Google chrome Ip address:172.16.0.13 User Name:Administrator Password:(Mentioned in server)	DDR4 or higher, 128 GB scalable upto 512 GB	
	Go to>System Information>Memory		
Overall Test Result	Pass: □	Fail: □	

Test ID	4.10.3 Storage		
Requirement	To verify server storage SAS SSD Storage = 1TB		
Test Objective	Verify storage		Remark
	Set Steps	Acceptance Criteria	

	Login server by ILO port. **by Google chrome** **Ip address:172.16.0.12** **User Name:Administrator** **Password:(Mentioned in server)** **Go to>System Information>Storage**	**storage SAS SSD Storage = 4TB** **HDD 4TB**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.10.4 Operating System And Virtualization Software**		
Requirement	**To verify Operating System And Virtualization Software**		
Test Objective	**Verify OS and VS**		**Remark**
	Set Steps	**Acceptance Criteria**	
	Login serverby Ip address:172.16.0.3 **User Name:root** **Password:(#Niral@7896#)** **uname -a** **lscpu |grep Virtualization**	**Linux pve 5.15.102-1-pve #1 SMP PVE 5.15.102-1 (2023-03-14T13:48Z) x86_64 GNU/Linux** **root@pve:~#** **root@pve:~# lscpu |grep Virtualization** **Virtualization: VT-x** **root@pve:~#**	**OS Linux machines also have virtualization enabled.**
Overall Test Result	**Pass: □**	**Fail: □**	

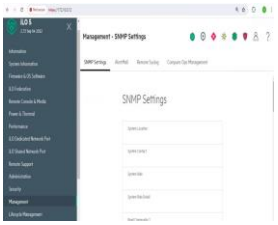
Test ID	**4.10.5 Network Interface**

Requirement	**To verify Dual port 1G SFP+ card, 4 x 1G BaseT**		
Test Objective	**Verify Physically Network Interface**		**Remark**
	Set Steps	**Acceptance Criteria**	

	Kindly check Physically Network Interface	**Dual port 10G SFP+ card, 4 x 1G BaseT**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**Test ID**	**4.10.6 PCIe Slots**		
Requirement	**Requirement**	**To verify PCIe Slots**		
Test Objective	**Test Objective**	**To verify PCIe Slots**		**Remark**
		Set Steps	**Acceptance Criteria**	
		Kindly check Physically Network Interface	**Minimum 4 x PCIe 16x 4.0 slots for I/O Connectivity or higher as required.**	
Overall Test Result	**Overall Test Result**	**Pass: □**	**Fail: □**	

Test ID	**Test ID**	**4.10.7 Management** **4.10.8 Security**	
Requirement	**Requirement**	**To verify Management /Security**	
Test Objective	**Test Objective**	**To verify Management /Security**	**Remark**

		Set Steps	**Acceptance Criteria**	
		Login server by ILO port. **by Google chrome** **Ip address:172.16.0.13** **User Name:Administrator** **Password:(Mentioned in server)** **Go to>Management>Security**	**Kindly check Management and Security** 	
Overall Test Result	**Overall Test Result**	**Pass: □**	**Fail: □**	

4.12 Evaluation Board

Test ID	**4.12.a RG520F 5G Module**		
Requirement	**RG520F Modem**		
Test Objective	**To verify RG520F Modem**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	RG520F Modem **1. Open the up plate and heat sink of5G Evb .** **2 The modem is connect with 5G Evolution board.**		
Overall Test Result	**Pass: □**	**Fail: □**	

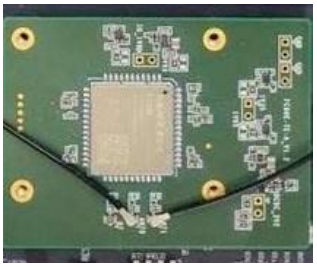
Test ID	**4.12.b Cellular Modem-RF**
Requirement	**Cellular Modem-RF RG520F**

Test Objective	To verify 100 MHz carrier aggregation (DL) andabove, 100/200 MHz bandwidth	Remarks

Test Description	Set Steps	Acceptance Criteria	
	1. Cellular Modem-RF RG520F		1. Carrier aggregation and bandwidth verified from data sheet
Overall Test Result	Pass: □	Fail: □	

Test ID	4.12.c Performance Enhancement Technologies		
Requirement	RG520F Modem		
Test Objective	To verify 100 MHz envelope tracking		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. RG520F Modem		1 can be check by modem's datasheet.
Overall Test Result	Pass: □	Fail: □	

Test ID	4.12. d Physical and Wi-Fi Interface Modules.
Requirement	FC60E Module

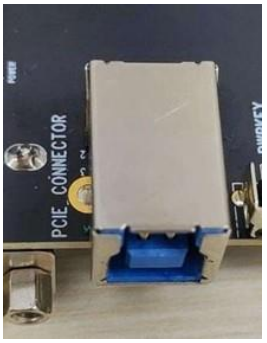
Test Objective	**To verify Physical and Wi-Fi Interface Modules.**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	FC60E Module **1 Open the 5G Evb up plate of box.** **2 the Wi-Fi Interface Module is connected on the Evb.**	 	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.12.e UART, SPI, I2C and GPIO Interface**		
Requirement	**UART , SPI, I2C and GPIO Interface**		
Test Objective	**To verify UART , SPI, I2C and GPIO interface**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

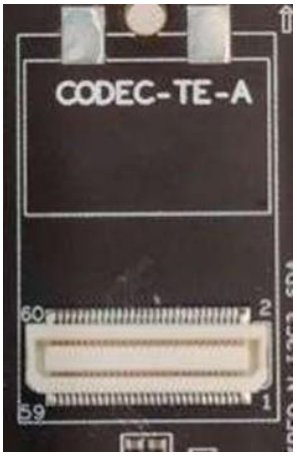
	1. GPIO 2. I2C 3. SPI 4. UART	   	1 Open the 5G Evb up plateof box . 2 all the interfaces are left side of the board.
Over all Test Result	Pass: □	Fail: □	

Test ID	4.12.f Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications		
Requirement	Sensor Interfaces		
Test Objective	Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Sensors interfaces can be performed by 5G or Wi-Fi interfaces.	1 the sensor can connect withthe Wi-Fi or Cellular of Evb and it can monitor & manage with help of 5G Evb.	
Over all Test Result	Pass: □	Fail: □	

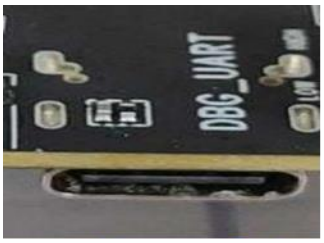
Test ID	4.1.g SD Card Connector		
Requirement	SD Card Connector		
Test Objective	To verify SD Card Connector		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. SD Card		1 the SD card can see on the right side of 5G Evb.
Overall Test Result	Pass: □	Fail: □	

Test ID	4.1.h PCIe to USB Connector		
Requirement	PCI to USB Connector		
Test Objective	To verify PCI to USB Connector		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. PCIe to USB connector		1 The PCIE to USB connector Is shown on front side of 5G Evb.
Overall Test Result	Pass: □	Fail: □	

Test ID	4.1.i Dual (U)SIM card supported		
Requirement	Dual (U)SIM card		
Test Objectiv e	To Verify Dual (U)SIM card supported		Remarks
Test Descriptio n	Set Steps	Acceptance Criteria	
	1. USIM card 1 & 2. USIM card 2	 	1 the sim card slot are left side 2 chech the sim status using standard AT command tester Application on “sim status”.
Overall Test Result	Pass: □	Fail: □	

Test ID	4.1.j 1 digital audio codec board interface		
Requirement	1 digital audio codec board interface		
Test Objectiv e	To Verify 1 digital audio codec board interface		Remarks
Test Descriptio n	Set Steps	Acceptance Criteria	
	1. Digital audio codec board		1 open the top plate of 5G Evb and see left side of board.

Overall Test Result	**Pass: □**	**Fail: □**

Test ID	**4.1.k Debug URAT**		
Requirement	**Debug URAT**		
Test Objective	**To verify Debug URAT**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. UART & **2. Debug UART**	 	**1. Both debug port shown in front side of 5G Evb**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.1.l USB Type C Interface**		
Requirement	**USB Type C Interface**		
Test Objective	**To Verify USB Type C Interface**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	1. USB Type C interface	 **1-The USB type c interfac e is shownright side of 5G Evb** **2.Connect the type c Data cable touse the 5G Evb with your PC.**	
Over all Test Resul t	**Pass: □**	**Fail: □**	

Test ID	**4.1.m LEDs indication**		
Requireme nt	**LEDs lights**		
Test Objec tiv e	**To Verify LEDs indication**		**Remarks**
Test Descrip tio n	**Set Steps**	**Acceptance Criteria**	
	1. LEDs lights		**1 LEDs are top on the board** **2 open Top plate of 5G Evb box the LEDs are below the Wi-Fi card .** **3 when board is power up the power LED(Red light) on. And other LEDs are on when the corresponding work do.**

Overall Test Result	**Pass: □**	**Fail: □**

Test ID	**4.1.n Power key, Reset key, USB Boot, Power Switch**		
Requirement	**Power key, Reset key, USB Boot, Power Switch**		
Test Objective	**To Verify Power key, Reset key, USB Boot, PowerSwitch**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Power Key **2. Reset key** **3. USB boot** **4. Power switch**	   	**1 All the keys are top on the board to see open the Top plate of 5G Evb.** **2 the**

			functionality will check according the use of the keys.
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.1.o 12 Antenna Interfaces**		
Requirement	**12 Antenna (8 cellular, 2 Wi-Fi & 2GPS)**		
Test Objective	**To verify 12 Antenna Interfaces**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. ANT0, ANT1 700 MHz–6 GHz **2. ANT2–ANT 7 1.7 GHz–6 GHz**		**1. open the top plate of 5G Evb and antenna are mounted on board at three side.** **2. The frequency is written on antenna**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.1.p Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi,Ethernet, Audio, PCI TO USB, Power Adaptors**

Requirement	**Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi- Fi,Ethernet, Audio, PCI TO USB, Power Adaptors**		
Test Objective	**To verify these cables**		
Test Description	**Set Steps**	**Acceptance Criteria**	**Remarks**
	1. Cables **2. Antenna** **3. Power adaptors** **4. Wi-Fi Ethernet** **5. PCI TO USB** **6. Audio earphone**		**1. the cable are provided with 5g Evb** **a) Power adapter** **b) Audio earphone** **c) PCI to USB cable** **d) Type** **C data cable** **e) UAR T debugging cable** **f) Antenna and wifi mounted on board.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.1.q AT command (external MCU integration) and SDK support (within the module)**		
Requirement	**AT command (external MCU integration) and SDK support (within the module)**		
Test Objective	**AT command (external MCU integration) and SDK support (within the module)**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	1. Supported by both the module	1. Power up the 5G Evband connect your pc with Evb using typeC data cable 2. Using a mcu with specific code youcan check the manufact urer details at end of mcu.	
Overall Test Result	**Pass: □**	**Fail: □**	

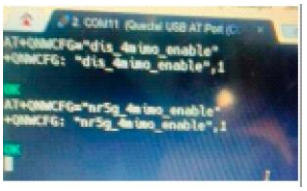
Test ID	**4.1.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech**		
Requirement	**Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech**		
Test Objective	**Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agritech**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
		You can configure a mcu for smart city or medical devices . You can monitor or manage it by using 5G Evb.	**1. You can check as per devices.**
Overall Test Result	**Pass: □**	**Fail: □**	

Functional Verification

Test ID	4.2.a Quectel RG520F 5G Module		
Requirement	RG520F module		
Test Objective	Verify the RG520F 5G module		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Connect the module to CoralAnubhav Board 2. Bands testedand result measures	OUTPUT WITH COMMAND ATI Quectel RG520F-E B Revision: RG520FEBDER03A01M4G_OCPU_BETA_20240307A OK ATI Quectel RG520F-EB Revision: RG520FEBDER03A01M4G_OCPU_BETA_20240307A OK **Power up the board and connect with pc using type c cable .** Use any standard at command tester for see details of modem using (ATI) command.	1. Power up the board and connect with pc using type c cable . 2. Use any standard at command testerfor see details ofmodem using (ATI) command .
Overall Test Result	Pass: □	Fail: □	

Test ID	4.2.b Cellular Modem-RF		
Requirement	Verify the RG520F module		
Test Objective	To check the RG520F Module uplink and Downlink in sub6GHz band		
Test Descript	Set Steps	Acceptance Criteria	Remarks

ion	**1. Sub 6 GHz bandn78 is for bandwidth** **2. Uplink and downlink can be verified by latchprocess.**	To check the uplink and downlink you can connect the hotspot of the 5G Evb and check the speed using standard network speed site .	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2.c Performance Enhancement Technologies**		
Requirement	**Performance Enhancement Technologies**		
Test Objective	**To verify Performance Enhancement Technologies**		**Remar ks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. MIMO(using multiple antenna at the receiver side)	 1.There are multiple antennas of same frequency range are available on board for perform MIMO application 2. To manage MIMO in 5G EVB use following command: - AT+ QNWCFG="dis_4 mimo enable - AT+QNWCFG= "nr5g_4mimo_enable	**1 there are multiple antennas of same frequency range are available on boardfor perform MIMO** **application** 
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.2.d Physical and Wi-Fi Interface Modules

Requirement	**Quectel FC60E**		
Test Objective	**Verify Physical and Wi-Fi Interface Modules**		**Remarks**
Test Descriptio n	**Set Steps**	**Acceptance Criteria**	
	1. Connect modemto the system 2. Test data transmission through physicalinterface 3. Received data correctly on theother hand	**1 insert the sim and power up the board . 2 search the Wi- Fi from your PC to connect with ssid of 5G Evb.**	**Evb wifi is connected with PC**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2.e UART, SPI, I2C and GPIO Interface**		
Requirement	**Coral Anubhav board**		
Test Objective	**To verify UART, SPI, I2C and GPIO**		**Remarks**
Test Descriptio n	**Set Steps**	**Acceptance Criteria**	
	1. Baud rate 115200 isused and transmit and receive large amount of data 2. Configure CPOL and CPHA settings , communicate withSPI device 3. Set 2 master on thebus & perform readwrite operation 4. Configured 1 GPIOas input & 1 GPIO as output results verified at ground	AT+QCFG="uart" +QCFG: "uart",1,1 OK **1 power up the board and connect with your pc usingtype c data cable. 2 Check the interfaces bybelow AT commands a. AT+QCFG="uart" b other interfaces check if you connect to the board.**	
Overall Test Result	**Pass: □**	**Fail: □**	

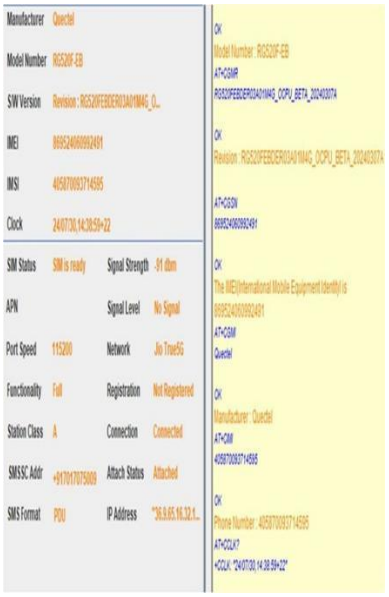
Test ID	4.2.f Sensor interfaces for medical devices, smart-home appliances and smart-city applications		
Requirement	Sensor interfaces for medical devices, smart-home appliances and smart-cityapplications		
Test Objective	To check sensor interfaces for different-2application		Remarks
Test Descriptio n	Set Steps	AcceptanceCriteria	
	1. Connected coral gyan sensor to coral Anubhav & measure soilmoisture 2. Collect the data and verified	1 power up the board 2 connectcoral gyan with hotspot of 5G Evb. 3 you can send the data to your desired API or application using5G Evb network.	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.2.g SD Card Connector		
Requireme nt	SD card		
Test Objective	To check SD card		Remarks
Test Descript ion	Set Steps	Acceptance Criteria	
	1. Micro SD card support, it can be verified on hardware level	. Take the access of board using ADB and run"df-h" to see the storage details of board and SD card.	1 The SD card slot ,right side of 5G Evb.
Overall Test Result	Pass: □	Fail: □	

Test ID	4.2.h PCI to USB Connector

Requireme nt	**PCI to USB Connector**		
Test Objective	**To verify PCI to USB Connector**		**Remarks**
Test Descript ion	**Set Steps**	**Acceptance Criteria**	
	1. Connect the cable to Coral Anubhav 5G board 2. And, it can be verified on hardware level	**1 connect the PCI to USBconnector for use of user requirement at PCIE connector. 2 - now user can take the log .**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2.i Dual (U)SIM card supported**		
Requirement	**SIM Card Supported**		
Test Objective	**SIM Card Supported**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	1. Insert the simin port 1 or 2 **2. Micro** **Sim card supported itcan be verified on hardware**	 1-"AT+QUIMSLOT?" - Query the(U) SIM slot currently used. 2-AT+QUIMSLOT=<slot>.Switch to (U)SIM slot use 2 or 1.	**1 power up the board and connect the type c data cable between your pc andEV board.** **2 use the AT command tester to see the details ofsim like sim no.**
Over all Test Resul t	**Pass: □**	**Fail: □**	

Test ID	**4.2.j 1 digital audio codec board interface**		
Requirement	**Codec board**		
Test Objective	**To check digital audio codec board interface**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	

	1. Power up thecodec board 2. Initialize codeusing initialization sequence 3. Status of register to confirm successful initialization	 insert the sim and power up the board . using AT command tester call to a number like this “ATD1234567890;”	Now you can talk above number by using Audio earphone.
Overall Test Result	Pass: □	Fail: □	

Test ID	4.2.k COM1 and COM2. Also support Main URAT, Debug URAT		
Requirement	COM1 and COM2 interfaces		
Test Objective	To check the COM1 and COM2 interfaces		Remarks
Test Descriptio n	Set Steps	AcceptanceCriteria	
	1. Boot up thesystem 2. COM1 & COM2 should be detected andlisted in the system	3. power up the board and connect the type c data cablebetween your pc and EV board. 4. connect the cable and usethe command or logcat to take the log of the 5G Evb	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.2.l USB Type C		
Requirement	USB type C cable		
Test Objective	To check USB type C cable		Remarks
	Set Steps	Acceptance Criteria	

Test Description	**1. Connect USB type C to Coral Anubhav board** **2. This USB interface is used for AT command communication , data transmission and firmware upgrade.**	**1 cable is provided with5G evb.** **2 power up the board and connect the type c data cable between yourpc and EV board.** **3use the AT command tester to see the details of modem.**	**4**
Overall Test Result	**Pass: □**		

Test ID	**4.2.m LEDs indication**		
Requirement	**Verify the LEDs indication**		
Test Objective	**To check the LEDs indication**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Switch onboard **2. For all theoperation LEDs are blinking**	 . LEDs details a) red led for power up indication b) yellow for debug mode c) blue light for registration status d) 2nd blue led show connectivity e.) Last LED light is for sleep mode	**1 LEDs details** **a) red led for powerup indication** **b) yellow for debugmode** **c) blue light for registration status** **d) 2nd blue led show connectivity**
Overall Test	**Pass: □**	**Fail: □**	

Test ID	**4.2.n Power key, Reset key, USB Boot, Power Switch**

Requirement	**Verify the Power key, Reset key, USB Boot, Power Switch**		
Test Objective	**To Check Power key, Reset key, USB Boot, PowerSwitch**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Power key, Reset key, USB Boot, Power Switchit can be verified on hardware level **2. After the connection**	**1 all functionality check byuser at hardware level .**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2.o 12 Antenna Interface**		
Requirement	**Supports Sub-6G bands:** **FR-1, N78**		
Test Objective	**Supports Sub-6G bands:** **FR-1, N78**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect all antenna to the5G and Wi-Fimodule **2. Power on thesystem** **3. Check at result at the other usedend like SNR and BER**	**1 all supported band of antenna for Sub 6GHz are available on board.**	

Overall Test Result	**Pass: □**	**Fail: □**

Test ID	**4.2.p Minimum Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors**		
Requirement	**Cables, Antenna, Audio earphone, USB Driver, Requiredmodules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors**		
Test Objective	**Minimum Cables, Antenna, Audio earphone, USB Driver, Requiredmodules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. All cables are connected and verified at hardware level.	**All cables are connected and verified at hardware level fordifferent use according to useor requirement.**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2.q AT command (external MCU integration) and SDK support (within the module)**		
Requirement	**AT command (external MCU integration) and SDK support (within themodule)**		
Test Objective	**AT command (external MCU integration) and SDK support(within themodule)**		**Remarks**
Test Description	**Set Steps**	**AcceptanceCriteria**	

		1.By use of MCU use all the supported AT command 2 User want to write a code in mcu for sending AT command and receive the response at default baud rate(115200) at mcu serial monitor.	**1 by use of MCU use all the supported AT command** **2 user want to write a code in mcu for sending AT command and receive the response at default** **baud rate(115200) at mcu serialmonitor.**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.2.r Application MCU Development Board for Applications like Smart Home,** **Smart City, Medical Devices, Agritech etc.**		
Requirement	**Application MCU Development Board for Applications like Smart Home, Smart** **City, Medical Devices, Agritech etc.**		
Test Objective	**Application MCU Development Board for Applications like Smart Home, Smart City,Medical Devices, Agritech etc.**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Connect application Microcontroller Unit (MCU) development boards & these are integral to developing and prototyping various IoT (Internet of Things) applications, including smart homes, smart cities, medical devices, and agritech.	.Using the network of 5G Evb . 2. User can monitor and manage the data of MCUs. 3. For the example user can use coral gyan with 5G Evb. 4.MCU with Linux OS we can integrate easily. Using minicom applications,users can use any suppored command for their use.	**1 using the network of 5G Evb .** **2 user can monitor and managethe data of MCUs.** **3 for the example user can useclral gyan with 5G Evb.**
Overall Test Result	**Pass: □**	**Fail: □**	

4.13 IOT Gateway

Test ID	4.13.a) CPU : Qualcomm or equivalent, Dual core or Higher b)RAM: 256 MB c)Status: Signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP Bytes sent/received, connected band, IMSI, ICCID. 4.13.7 a,b,c,d,e,f,g,h)All can be verified Physically		
Test Objective	Check RAM ,Processor and RF Parameters in IoT Gateway.		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. SSH into the router via Router IP address. 2. Use command 'cat /proc/cpuinfo' RAM Use command 'free -m'. Check in GUI by login 192.168.1.1 in RF part		
Overall Test Result	Pass: □	Fail: □	

4.14	5G Mini Drones

Test ID	4.14 (a) 5G enabled and controlled drone (m) 5G Modem (n78 band)		
Requirement	To Check Drone is integrated into the System and supports 5G Modem (n78 band)		
Test Objective	To Check Drone is integrated into the System and supports 5G Modem (n78 band)		Remark
	Set Steps	Acceptance Criteria	
	Step-1: Verify the 5G network is on N78 band only. Step-2: Insert the 5G SIM into the drone and Power ON the drone by inserting the battery. Step-3: The drone will automatically send the UE-attach message to the 5G network. After successful attach and IP assignment, the drone can be connected via the GCS. Step-3: Open the GCS - 'iDronam Enterprise'. Connect to the drone. Step-4: Check if all the drone data are coming - ○ 3D Map data. ○ Video data. ○ Drone Telemetry	All the drone data - 1. 3D Map Data. 2. Video data. 3. Drone Telemetry data. should be available on the GCS - 'iDronam Enterprise' via 5G.	It is verifiedDrone is integrated and supporting Band 78

	data.		
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.14 (b) TSupports 5G nano SIM (c) Connectivity Options: Cellular (5G) and Wi-Fi for ubiquitous and long-range connectivity (o) Wi-Fi (2.4/5 GHz)**		
Requirement	**Verify Drone supported Nano Sim and (2.4/5 GHz)**		
Test Objective	**To verify support of 5G Nano Sim and 5G enabled and controlled and Wi-Fi for ubiquitous and long-range connectivity**		**Remark**
	Set Steps	**Acceptance Criteria**	
	Step-1 : Take a 5G Nano SIM and Insert into the drone SIM card slot. Step-2: Connect the GCS to the 5G network. Step-3: Connect the GCS to the drone. Step-4: Check for the drone connection and information being displayed on the GCS screen. WI fI Step-1: Turn ON the Drone and wait for the drone to	**Verify in below packet in wireshark Successful insertion of 5G Nano SIM in SIM Slot of 5G Communication Module of Drone. Successful connection and display of drone data on the screen. GCS and drone must be on the same wifi network and the drone should successfully**	**Successful insertion of 5G Nano SIM in SIM Slot of 5G and Wi Fi supported**

	initialize. **Step-1: Open GCS.** **Step-2: Connect the GCS WiFi to** **Drone's WiFi.** **Step-3: Open iDronam and connect** **to the drone.**	**connect to the drone over** **WiFi.**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.4 (d) Qualcomm or equivalent onboard processing engine for AI/ML analytics Should support MEC applications		
Requirement	Onboard processing engine for AI/ML analytics and MEC application support.		
Test Objective	To Check drone capabilities for AI/ML and MEC.		Remarks
Test Description	Set Steps	Acceptance Criteria	
	Step-1: Connect to the drone. A web page is hosted inside the drone. Open the webpage by going to the drone's IP - 10.42.0.1:5000 using a browser. Step-2: The page will open and the user can upload an image to the drone. Step-3: After processing, the drone will return the results of object detection in image and JSON formats. These can be downloaded for further use. Should support MEC applications The drone is ME UE which	The webpage should successfully be opened. Using this drone's AI/ML capabilities can be seen.	

	is **offloading the drone video** **stream.** **Step-1: Connect the MEC Server** **to the drone.** **Step-2: An MEC application will** **be running on the MEC server** **which will receive the incoming** **video stream.** **Step-3: After processing the** **output can be viewed on the web** **page hosted in MEC.**	**The webpage should successfully be opened. Using this drone's AI/ML capabilities can be seen.**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.14 (e) Autonomy: Visual Inertial Odometry (VIO), path planning, PX4, GPS-denied navigation, BVLOS, follow me.		
Requirement	Verify To Check Drone Autonomy		
Test Objective	To Check Drone Autonomy		Remark
IMPORTANT: PX4 uses MAVLink Protocol for Drone Communication	Set Steps	Acceptance Criteria	
	Step-1: Connect the drone to MAVLink Packet Decoder (e.g, Mission Planner) Step-2: Start Capturing the MAVLink Data Stream. Step-3: Check for the data being published by drone. Step-4: Look for the "VISION_POSITION_ESTIMATE", "LOCAL_POSITION_NED", "OBSTACLE_DISTANCE" data packets for Visual inertial Odometry	"VISION_POSITION_ESTIMATE", "LOCAL_POSITION_NED", "OBSTACLE_DISTANCE" msg should be present.	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.14 (f) 360 obstacle avoidance: Depth estimation, obstacle detection, map60ping and VOA		
Requirement	360 obstacle avoidance, Depth estimation, obstacle detection, mapping and VOA (Clause 4.14 (f))		
Test Objective	To Verify Drone Obstacle Avoidance and Mapping		Remark
	Set Steps	Acceptance Criteria	
	Step-1:Connect the drone to a MAVLink Decoder(Mission Planner) and look for "OBSTACLE_DISTANCE", and "RANGEFINDER" messages for obstacle and depth estimation respectively. Mapping and VOA Step-1: Place the drone on the floor, connect the 'iDronam Enterprise' Software to the drone and subscribe to "/map" for 3d map and Dynamic Obstacle plotter.	360 obstacle avoidance, Depth Estimation and obstacle detection: Before arming the drone a test object can be placed within a distance of ~20cm at 45-degree intervals covering 360 degrees around the drone. The drone will detect it and give a pre-arm warning giving the details of the angle and distance of the object. Take off the drone to 1-1.2 m altitude. The mapping algorithm will map the surroundings of the drone as it takes off. A test object can be brought close to the drone from the front face and the drone will back off once a threshold of 1.5m is crossed by the object. "OBSTACLE_DISTANCE", "RANGEFINDER" messages should be defined and changed as you	1.5m is crossed by the object. "OBSTACLE_DISTANCE", "RANGEFINDER" messages ged as you increase drone height and environment change. The map should be visible on the GCS.

		increase drone height and environment **change.** **The map should be visible on the** **GCS.**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.14 (g) Payload Capacity – 500g/1 Kg or above**		
Requirement	**To Check Payload Capacity**		
Test Objective	**To Check Payload Capacity**		**Remark**
	Set Steps	**Acceptance Criteria**	
	Step-1: Take the drone outdoors. **Step-2: Attach the 500gm Payload and Turn on the Drone** **Step-3: Wait for the drone to initialize.** **Step-4: Takeoff the Drone.(Read Proper Manual Before Flying)** **Step-5: Land the Drone**	**Drone Takes off up to a height of 1.2m and hovers in its place for a duration of 1 min.**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.14 (h) GPS or NAVIC enabled		
Requirement	To Check GPS		
Test Objective	To verify GNSS Capabilities		Remark
	Set Steps	Acceptance Criteria	
	Step-1: Connect the drone to GCS and read the sensor status for GPS/Navic at Serial4/UART8. Drone should be placed in an outdoor environment under clear skies and location should not be near buildings of height greater than 20m. Step-2: Turn on the drone and connect to GCS.	The drone should have a GPS lock which will be indicated in GCS. An accuracy of 3m is expected. It should return “3D FIX” AND “3D DGPS” or relevant status depending upon the GPS Locking.	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.14 (i) Geo Fencing

Requirement	**To Check Geo Fencing**		
Test Objective	**To Check Geo Fencing**		**Remark**
	Set Steps	**Acceptance Criteria**	
	Step-1: Turn ON the Drone. **Step-2: Connect the drone to GCS and in the plan section create a fence.** .	**After Uploading the Fence. Click on the Read Fence Button to read to fence Drone stored.**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.14 (k) Tracking sensor** **(l) Image Sensor**		
Requirement	**To Check Sensors**		
Test Objective	**To Check Tracking sensor and Image Sensor**		**Remark**
n	**Set Steps**	**Acceptance Criteria**	
	Step-1: The drone should be placed in an outdoor environment where GPS Signals are uninterrupted. **Step-2: Once 3D Fix has come the GPS will have a good lock of Drone Position.** **Step-3: The Drone can be tracked.** **Image sensor:** **Step-1: Turn ON the drone.** **Step-2: Connect the drone to the iDronam software.**	**After GPS Fix, the drone is successfully tracked via the GCS.** **The Live Stream of the drone camera will be displayed in iDronam.**	

Overall Test Result	**Pass: □**	**Fail: □**	

4.15 XR (AR/VR) Device

Test ID	**4.15.1 AR/VR Device** **(a) Chipset : 2.0 GHz 8-core Qualcomm** **(b)Memory : 64GB internal storage / 4GB RAM** (d) USB type C and Audio		
Requirement	**To verify Chipset**		
Test Objective	**To verify Processor and Clock speed and memory**		**Remark**
	Set Steps	**Acceptance Criteria**	
	Verify Chipset and Memory of AR/VR Device C-Type USB port and Audio verify Physicaly	**As per data sheet of Meta Quest 2 below are Chipset and Memory details** ***CPU: Snapdragon XR2, octa-core,*** ***128 GB storage and 6GB RAM*** ***C-type USB port present and also able to listen***	**Verify that mentioned Processor having details** **Integrated surround sound Integrated microphone 3.5 mm jack plug**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.15.2Processor – Qualcomm or equivalent** **(a) Bluetooth 5.0** **(b) 802.11 a/b/g/n/ac - 2.4 GHz and 5GHz**	
Requirement	**To verify Bluetooth and Wifi**	
Test Objective	**To verify Bluetooth and wifi port**	**Remark**

	Set Steps	Acceptance Criteria	
	1-Firstly go to Bluetooth option and check properties. 2-Go to seting in wifi And check specs	**Device support Bluetooth 5.0 and both wifi 2.4 and 4 ghz**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.15.2 Processor – Qualcomm or equivalent** **(d)3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass)** **(e)NavIC or GPS location support**		
Requirement	**To verify 3IMUs and GPS**		
Test Objective	**To verify 3 NavIC or GPS location support**		**Remark**
	Set Steps	**Acceptance Criteria**	
	1-Go to map and set location for tracking	**It support 3 IMUs Gyroscope Accelerometer Magnetometer And support GPS location**	**Verify that mentioned details**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.15.3 Input/Output** **(a)Display: 24° field-of-view, 24-bit color LCD, outdoor visible, HD resolution** **(b)Microphone** **(c) Speaker : Internal 94 dBA loudspeaker**		
Requirement	**To verify 3IMUs and GPS**		
Test Objective	**To verify 3 NavIC or GPS location support**		**Remark**
	Set Steps	**Acceptance Criteria**	
	To verify speaker and Microphone insert headphone and say anything by clicking mic also play songs to listen	**As per data specs mentioned** **Display: Single Fast switch LCD** **Resolution: 3664 x 1920 pixels (1832 x 1920 pixels per eye)** **Refresh rate: 60, 72, 90 Hz** **Integrated surround sound** **Integrated microphone 3.5 mm jack plug**	**Verify that mentioned details**
Overall Test Result	**Pass: □**	**Fail: □**	

4.16 5G Indoor CPE

Test ID	**4.16.1 Processor – Qualcomm or equivalent** **(d) CPU Clock Speed 1.0GHz or higher** **(e) CPU Cores Dual-core Cortex-A53 Arm or equivalent**

Requirement	**To verify Processor**		
Test Objective	**To verify Processor and Clock speed**		**Remark**
	Set Steps	**Acceptance Criteria**	
	.Login CPE **Ip:192.168.1.1** **User Name:admin** **Password:Vvdn@123** **Go to system Logs and verify CPU Details**	**verify in log cpu details** **CPU: ARMv7 Processor [51af8014] revision 4 (ARMv7)**	**Verify that mentioned Processor having details** **ARM ARMv7 Processor rev 4 (v7l) 4 Core 1200 MHz**
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.16.2 Memory : 512 MB RAM or higher**		
Requirement	**To verify Memory : 512 MB RAM or higher**		
Test Objective	**Verify RAM Space**		**Remark**
	Set Steps	**Acceptance Criteria**	

	.Login CPE Ip:192.168.1.1 User Name:admin Password:Vvdn@123 Go to system Logs and verify Memory Details	verify in log Memory details memory: 40000000 536870912 b(avl 447709184) items 4 active_cores 1	Verify that RAM detail having 512 MB
Overall Test Result	Pass: □	Fail: □	

Test ID	4.16.3 5G		
Requirement	(a) 5G Sub 6 Band: n78 TDD (b) 5G Modem : Snapdragon X62/X65 or equivalent (c) Bandwidth Support : 100 MHz (d) MIMO : 4 x 4 or higher 4.16.6 (d)Supports RF management (ei)intelligent RF control plane for self-healing and self-optimization 4.16.4 GPS Supported.		
Test Objective	Verify Band supported,Modem,BW and MIMO		Remark
	Set Steps	Acceptance Criteria	
	.Login CPE Ip:192.168.1.1 User Name:admin Password:Vvdn@123 Go to Cellular Info	verify in log Memory details We user.notice Cellular: [NR5G-SA] MCC: 001, MNC: 01, TAC: 12594, CID: 3333, PCID: 11, BAND: 78, BW: 100, ARFCN: 640704, RSRP: -69, RSRQ: -11, SINR: 25 PTP clock support registered 	Verify that supported Band n78 TDD BW 100 MHz,MIMO and RF control

		2023/08/09 20:10:17 We kern.err kernel: [4.754919] ipq5018-pinctrl 1000000.pinctrl: invalid function qspi2 in map table 2023/08/09 20:10:17 We kern.err kernel: [4.747281] ipq5018-pinctrl 1000000.pinctrl: invalid function qspi1 in map table 2023/08/09 20:10:17 We kern.err kernel: [4.746987] ipq5018-pinctrl 1000000.pinctrl: invalid function qspi0 in map table	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.16.5 Wireless**		
Requirement	**4.16.5 (a) AP type: Indoor, dual radio, 2.4, 5-GHz** **(c) Standards: IEEE 802.11 a/b/g/n/ac wave 2** **(f) IPv4 and IPv6 dual stack support** **4.16.7 © All version and Latest WPA support.**		
Test Objective	**Verify RAM Space**		**Remark**
	Set Steps	**Acceptance Criteria**	
	.Login CPE **Ip:192.168.1.1** **User Name:admin** **Password:Vvdn@123** **Go to system Logs and verify .**	**2023/08/09 18:04:45 We user.debug : [IPQCM: ipqcm_enable_bh_v4:1987] dsi_start_data_callv4 success rval 0** **2023/08/09 18:04:45 We daemon.info hostapd: ath1: STA 82:0b:46:49:cf:ea WPA: sending 3/4 msg of 4-Way Handshake** **2023/08/09 18:04:45 We daemon.info hostapd: ath1: STA 82:0b:46:49:cf:ea WPA: sending 1/4 msg of 4-Way Handshake** **2023/08/09 18:04:45 We daemon.info hostapd: ath1: STA 82:0b:46:49:cf:ea WPA: received EAPOL-Key frame (4/4 Pairwise)** **2023/08/09 18:04:45 We daemon.info hostapd: ath1: STA 82:0b:46:49:cf:ea WPA: received EAPOL-Key frame (2/4 Pairwise)**	**Verify that RAM detail having 512 MB**

		2023/08/09 18:04:45 We daemon.info hostapd: ath1: STA 82:0b:46:49:cf:ea WPA: pairwise key handshake completed (RSN) **2023/08/09 18:04:45 We daemon.info hostapd: ath1: STA 82:0b:46:49:cf:ea RADIUS: starting accounting session C36AA50CF8ABA514** **2023/08/09 18:04:45 We daemon.info hostapd: ath1: STA 82:0b:46:49:cf:ea IEEE 802.11: associated (aid 2)**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.16.8 Interface**		
Requirement	**To verify Physically**		
Test Objective	**(a) 2 X 1000 Base-T Ethernet** **(b) 1 X SIM card slot (Nano-SIM)** **(c) Power-over-Ethernet or DC Power**		**Remark**
	Set Steps	**Acceptance Criteria**	
	.Kindly Verify Physically as per Test	**2 X 1000 Base-T Ethernet** **(d) 1 X SIM card slot (Nano-SIM)** **(e) DC Power with adapter**	
Overall Test Result	**Pass: □**	**Fail: □**	

4.16 5G Camera

Test ID	4.17.1 Advanced AI/ML video analytics		
Requirement	On edge video analytics		
Test Objective	To check edge AI (Face recognition)		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Open camera on web. IP:192.168.128.10 Username:admin Password:admin1234 2. Add face in database. 3. Then ask added person to came in front of camera		Verified Face recognition by white list and Black list People.
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.2 Supports Sub-6G bands: FR-1, N78		
Requirement	Supports Sub-6G bands: FR-1, N78		
Test Objective	Supports Sub-6G bands: FR-1, N78		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Camera support N78 band, it can be verified by latching camera over N78 band frequency.	verify by login also by https://192.168.128.1	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.3 SIM Card Supported

Requirement	**SIM Card Supported**		
Test Objective	**SIM Card Supported**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Nano Sim card supported it can be verified on hardware.		
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.17.4 Interface 10/100/1000 Ethernet port. Audio Port Alarm Port**		
Requirement	**Interface 10/100/1000 Ethernet port. Audio Port Alarm Port**		
Test Objective	**Interface 10/100/1000 Ethernet port. Audio Port Alarm Port**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. All these options can be verified on hardware.		
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.17.5 5M / 8M effective resolution**
Requirement	**5M / 8M effective resolution**

Test Objective	**5M / 8M effective resolution**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Image sensor is 5MP, it can be verified by opening camera on web also can be verified by checking RTSP stream properties in VLC player.	Login goi 192.168.128.10 and goto Encode setting: select **5M / 8M effective resolution**	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	**4.17.5 bWide Dynamic Range (WDR)=120dB**		
Requirement	**Wide Dynamic Range (WDR)=120dB**		
Test Objective	**Wide Dynamic Range (WDR)=120dB**		**Remarks**
Test Description	**Set Steps**	**Acceptance Criteria**	
	1. Supported, it can be verified on ground.	Verify by light off near camera and Outside on and check feed in MEC	
Overall Test Result	**Pass: □**	**Fail: □**	

Test ID	4.17.5c IR distance		
Requirement	IR distance		
Test Objective	IR distance		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. supported = 30 meter, it can be verified on ground.	Verify by image taken from far end	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.5 d Memory: Micro SD & SDXC slot up to 256GB		
Requirement	Memory: Micro SD & SDXC slot up to 256GB		
Test Objective	Memory: Micro SD & SDXC slot up to 256GB		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Micro SD card support, it can be verified on hardware.	Insert Micro SD Card in slot in and verify by login 192.168.128.10 memory space in camera.	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.6 Lens: Motorized, vary focal (2.7mm-13.5mm)		
Requirement	Lens: Motorized, varifocal (2.7mm-13.5mm)		
Test Objective	Lens: Motorized, varifocal (2.7mm-13.5mm)		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Yes, it can be tested on ground.	It can be focus in focus out as per desire focal length by GOI login 192.168.128.10	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.6 Field of View (FOV) : Horizontal – 98 Deg wide. Vertical – 50 Deg wide.		
Requirement	Field of View (FOV) : Horizontal – 98 Deg wide. Vertical – 50 Deg wide.		
Test Objective	Field of View (FOV) : Horizontal – 98 Deg wide. Vertical – 50 Deg wide.		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Compiled, it can be tested on ground.	It can be verify by put Image sensors size and lense details on any FOV calculation plateform. And as per data sheet.	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.6 c Focus and IRIS Control: Auto		
Requirement	Focus and IRIS Control: Auto		
Test Objective	Focus and IRIS Control: Auto		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Complied, it can be tested on ground.	As per data sheet	
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.7 Video Compression: H.265 / H.264 / MJPEG or equivalent		
Requirement	Video Compression: H.265 / H.264 / MJPEG or equivalent		
Test Objective	Video Compression: H.265 / H.264 / MJPEG or equivalent		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. H.264/265 Supported, it can be verified bro camera web interface.		
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.7 Frame Rate = 1 -30/60		
Requirement	Frame Rate = 1 -30/60		
Test Objective	Frame Rate = 1 -30/60		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. 25/30 Supported, it can be verified bro camera web interface.		
Overall Test Result	Pass: □	Fail: □	

Test ID	4.17.8 Power: PoE (802.3at)		
Requirement	Power: PoE (802.3at)		
Test Objective	Power: PoE (802.3at)		Remarks
Test Description	Set Steps	Acceptance Criteria	
	1. Supported, it can be tested by using PoE switch.	Verify Physically	
Overall Test Result	Pass: □	Fail: □	

5G LAB

User Acceptance Test

Signaltron Confidential. Do not copy

Internal Document history

Version	Date	Author	Changed Sections	Change Description/Reference
1.0	6 Sep 2024	Signaltron	Initial Version	
1.2	9th Oct 2024	Signaltron	Incorporated changes based on received Vol 1 & 2 documents	
1.3	10th Oct 2024	Signaltron	Incorporated the initial review comments based on the conference call with TCIL team.	
1.4	18th Oct 2024	Signaltron	Updated the Acceptance criteria of several test cases with UE or gNB PCAP log snippet	
1.5	19th Oct 2024	Signaltron	Updated Drone related Test cases	
1.7	3rd Nov 2024	Signaltron	Updated the document based on the review comments provided during Pre-UAT workshop	
1.8	7th Nov 2024	Signaltron	Updated 5G CPE, Firewall, 5G Camera, XR(AR/VR) Sections	

Signaltron Confidential. Do not copy

Copyrights by Signaltron Systems Pvt Ltd. All rights reserved worldwide.

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

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

Signaltron Confidential. Do not copy

1. Introduction

This UAT document serves the purpose of ensuring that the software/hardware meets the business requirements and is ready for deployment by validating its functionality in a real-world environment. It allows end-users to test the software/hardware to ensure it meets their needs and operates as expected, helping to identify and fix any issues before the final release. UAT is crucial for quality assurance and customer satisfaction, as it ensures that the software/hardware is user-friendly, reliable, and meets all specified criteria.

2. Purpose and Scope

This document is referred to as a UAT document which will be used for acceptance testing and confirmation of the 5G Lab up and running. The purpose of this document is to validate systems, and networks for users. UAT ensures that the system can handle real-world tasks and perform to development specifications. Users are allowed to interact with the system before its official release to see if any features were overlooked or if any bugs exist. This document is meant for stakeholders, customers, institutes, testers.

Signaltron Confidential. Do not copy

3. Terms and Abbreviations

The following table contains terms and abbreviations used in this document either directly explained or translated accordingly:

Term / abbreviation	Explanation
API	Application Programming Interface
AR	Augmented Reality
CPE	Customer Premises Equipment
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of things
MR	Mixed Reality
NMS	Network Management Subsystem
RAN	Radio Access Network
SIM	Subscriber Identity Module
VR	Virtual Reality
UAT	User Acceptance Test

Signaltron Confidential. Do not copy

4.1 Section: - Physical Material Verification

Equipment/Device Check List/Spec verification				
SN	**Equipment/Devices**	**Qty**	**Make/Model**	**Sr No**
1	5G Core	1	Niral Networks	
2	5G Radio	1	Signaltron	
3	IMS solution	1	Niral Networks	
4	MEC &Application server	1	Niral Networks	
5	NMS (with Dashboard)	1	Niral Networks	
6	Router with Firewall	1	COSGrid	
7	5G SIMs (4 Digit Phy No. + IMSI)	50	Signaltron	
8	5G Evaluation Board / Hardware and Software Development Kit.	1	Signaltron	
9	IoT Gateway	1	COSGrid	
10	IoT sensors with analytic software (Loaded in Application server)	4	COTS	
10.1	Temperature &; Humidity sensor	1	COTS	
10.2	Light sensor	1	COTS	
10.3	Soil sensor (NPK)	1	COTS	
10.4	Water (TDS/chlorine) sensor	1	COTS	
11	5G Mini Drone	1	Signaltron	
12	5G XR(AR/VR/MR)	1	Ajna	
13	5G Indoor CPE	1	Kenstel	
14	5G Camera with AI enabled Video Analytic (Face/Object/Motion detection, people counting etc.)	1	Sparsh	
15	5G Handsets (IMEI No)	2	Samsung	
16	Adjustable Tripod Pole (3m)	1	COTS	
17	24 U Rack	1	Signaltron	
18	UPS 5KVA (1hr backup)	1	MicroTek	
19	32-inch FHD Display + VGA cable	1	Samsung	
20	L2 Managed Switch (24 port)	1	Nivetti	
21	Testing & Tracing Tools (Version)	1	Signaltron	

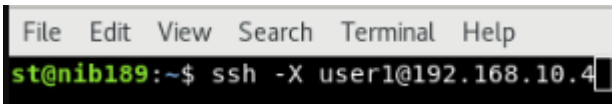
Signaltron Confidential. Do not copy

Network Nodes and IP Address:

Network Node Name	IPv4 Address
gNB	192.168.10.4
AMF	192.168.10.6
UPF	192.168.10.7
NiralOS SDN dashboard	192.168.88.13
T1 Server (Core)	192.168.10.2
T2 Server (MEC)	192.168.10.3
Controller (in T1)	192.168.10.5
MEC VM IP	192.168.10.12

Login into gNB:

Command : ssh -X user1@192.168.10.4
Passwd : user1

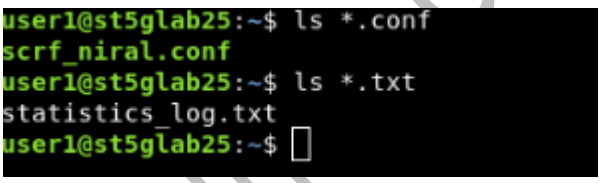


Major files available:

1) Scripts to start and stop gNB



2) Configuration file to configure various parameters of gNB like Bandwidth, Central frequency etc – scrf_niral.conf and log file that captures parameters like Radio power, temperature – statistics_log.txt.



Signaltron Confidential. Do not copy

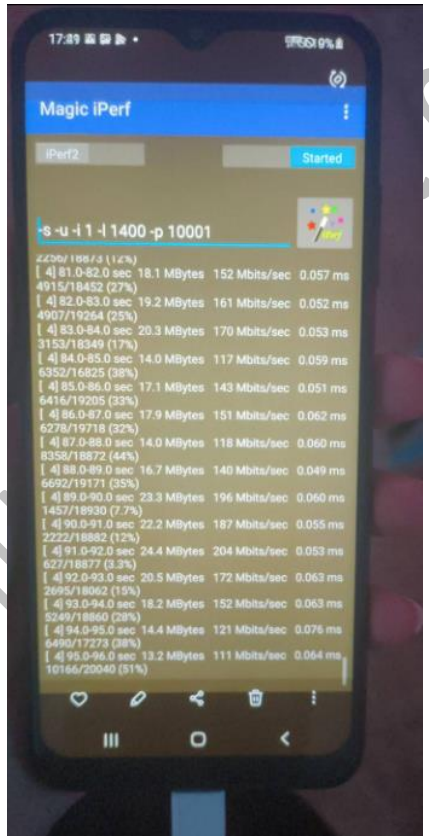
4.2 Section: - 5G Network Specs (Core+RAN)

Test ID	4.2(i). Radio Configuration		
Requirement	Radio Configuration should be as RFP submitted.		
Test Objective	To check Radio Configuration for Integrated RAN		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	• gNodeB can be accessed using CLI (command line Interface). To access through CLI, follow the below steps. • Login: user1 Password: user1. Open terminal.	Signaltron gNodeB is an integrated RAN. There is only one application that needs to be started. Inside /home/user1, there will be 2 scripts- start_gnb.sh and stop_gnb.sh To start and stop the gNodeB.	
Test Result	Pass ☐	Fail ☐	

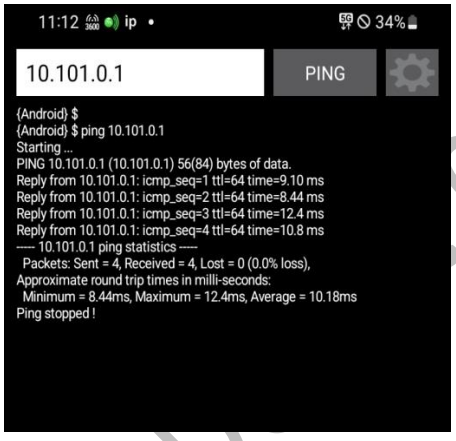
Signaltron Confidential. Do not copy

Test ID	4.2(ii) 3GPP Spec		
Requirement	Rel. 15 compliant & upgradable to Rel. 16 (by Sep 2024)		
Test Objective	To check 5G Lab setup follows Rel. 15 and is upgradable to Rel. 16		
Description	Test Steps	Acceptance Criteria	Remarks
	One of the features of Rel. 15 is standalone 5G. The setup we are providing runs 5G in SA mode itself. Hence, we can say the system is Rel. 15 compliant. Release 16 features in the roadmap		
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(iii) Data Rate (DL+UL)		
Requirement	>= 200 Mbps		
Test Objective	To check 5G performance at end user.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Install *iperf for Android* in Mobile from Google Play Store. iPerf is already installed on Core Server. To run iPerf on core, login to core first DL – • Login to RAN and pump traffic to UE for DL throughput – *iperf -u -c <server-ip-addr> -b 250M -t 100000 -i 1 -p 10001 -l 1400* • Open iperf in UE and listen for the above pumped data – *iperf -s -u -i 1 -l 1400 -p 10001* UL – • Login to RAN and listen to data from UE for UL throughput – *iperf -s -u -i 1 -l 1400 -p 10001* • Open iperf2 in UE and pump data – *iperf -u -c <server-ip-addr> -b 250M -t 100000 -i 1 -p 10001 -l 1400.* • Alternatively, perform speed test using speedtest.com to check the downlink and uplink data rate.	Through iPerf required TP should be pushed and checked  	
Test Result	Pass ☐	Fail ☐	

Signaltron confidential copy

Test ID	4.2(iv) Latency		
Requirement	<= 15ms. Upgrade to Rel. 16 should meet the latency as per 3GPP standards.		
Test Objective			
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	• Ping Core from UE and run it for some time (15 secs). • Stop the ping and check average RTT.	This number should be <= 15 ms. 	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(v) Max no. of active devices (That network can connect)		
Requirement	30 (minimum)		
Test Objective	To verify that at least 30 devices should be connected at the same time.		
Description	Test Steps	Acceptance Criteria	Remarks
	• Power on 30 5G UEs and let them register to the network.	30 UEs registered with 5G network. The same can be shown on NMS.	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(vi) Radio Power		
Requirement	Upto 100 mW per port		
Test Objective	To verify output power is within limits		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Connect each antenna port to signal analyzer (VSA) in operating condition and check the power reported by it. In the absence of VSA , log file print needs to be shown. Please check the logs at /home/user1/statistics_log.txt	Should be less than or equal to 100 mW.	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(vii) Duplexing Mode		
Requirement	TDD		
Test Objective	Need to check system compatibility in TDD mode.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Check the configuration file scrf_niral.conf for the frequency configured in downlink and uplink. In TDD , both uplink and downlink frequency should be same. Check UE registration with provided n78 gNodeB. N78 band specific for TDD. Check the UE logs or using NetMonster Application installed on the UE to check the band, Centre frequency on which UE is camped.	**In scrf_niral.conf file:** following confirm TDD duplexing: **absoluteFrequencySSB = 641280;** **dl_frequencyBand = 78;** **ul_frequencyBand = 78;** **From the UE logs:** check the Duplex mode as highlighted below *** Mode Report Message type: NR 5G ML1 DL Dedicated Config Device: EQ1 CurrentRAT: Nr Cell Group Add Mod Log Mask : 1 Per CC Cfg Cell Info Band : n78 Phy Cell ID : 0 SSB Sub Carrier Spacing : 30 kHz DL Cell Frequency : 641280 Duplex Mode : **TDD**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(viii) Channel Bandwidth		
Requirement	20 MHz, 40 MHz, 50 MHz, 80 MHz and 100 MHz		
Test Objective	To verify different bandwidths supported.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	In **scrf_niral.conf** file search for **'dl_carrierBandwidth = 273; #51; #106;'** and set the value appropriately. For eg: 51 for 20 MHz, 273 for 100 MHz. The value of these signifies the following – 13750 – 20 Mhz; 51 max. RBs 28875 – 40 Mhz; 106 max. RBs 36300 – 50 Mhz; 133 max. RBs 16499 – 80 Mhz; 217 max. RBs 1099 – 100 Mhz; 273 max. RBs The same can be observed in UE log.	**From UE Logs:** *** Layer 3 Message type: SIB1 (BCCH-DL-SCH) Device: EQ1 MessageDirection: DL MessageProtocol: NR-RRC MessageChannel: BCCH-SCH Channel CurrentRAT: Nr servingCellConfigCommon **carrierBandwidth : 51** initialDownlinkBWP genericParameters locationAndBandwidth : **13750** subcarrierSpacing : kHz30	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(ix) Band Support		
Requirement	n78 (Must be Tunable to center frequency with desired channel bandwidth-100MHz in the whole n78 band i.e 3300MHz to 3800MHz).		
Test Objective	To verify that device supports n78 band.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	In configuration file(scrf_niral.conf), search for *'dl_frequencyBand'* and *'ul_frequencyBand'*. *To set the centre frequency, set the appropriate value for absoluteFrequencySSB in the scrf_niral.conf file.* *After UE attaches to 5G network check the SIB1 message from the UE log or Check the camped frequency in Netmonster application.*	**From Configuration file we can see below**: **dl_frequencyBand = 78;** **ul_frequencyBand = 78;** **absoluteFrequencySSB = 641280;** **UE Log** *** Mode Report Message type: NR 5G ML1 DL Dedicated Config Device: EQ1 CurrentRAT: Nr Cell Group Add Mod Log Mask : 1 Per CC Cfg Cell Info **Band : n78**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(x) MIMO Configuration		
Requirement	2T2R (min)		
Test Objective	To verify MIMO is supported by the setup.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Check RRC Reconfiguration message in PCAP log to check MIMO Layers configured by the gNB (Apply filter for nr-rrc in wireshark). Check the UE logs as well to confirm 2x2 MIMO being configured.	From RRC Reconfiguration message from gNB **PCAP log**: pdsch-ServingCellConfig: setup (1) setup **maxMIMO-Layers: 2** **UE log:** *** Mode Report Message type: NR 5G MAC PDSCH Status Device: EQ1 CurrentRAT: Nr **Num Rx : 2x2 MIMO**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(xi) Synchronization		
Requirement	IEEE 1588 Precision Time protocol		
Test Objective			
Description	Test Steps	Acceptance Criteria	Remarks
	IEEE 1588 PTP Server is running in gNB and synchronization is with core network. The same can be seen in gNB PCAP logs	**From gNB PCAP logs:** Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface any, id 0 Linux cooked capture v1 Internet Protocol Version 4, Src: 192.168.10.7, Dst: 224.0.1.129 User Datagram Protocol, Src Port: 319, Dst Port: 319 **Precision Time Protocol (IEEE1588)** 0000 .... = majorSdoId: Unknown (0x0) .... 0000 = messageType: Sync Message (0x0) 0000 .... = minorVersionPTP: 0 .... 0010 = versionPTP: 2 messageLength: 44 domainNumber: 0 minorSdoId: 0 flags: 0x0200 **correctionField: 0.000000 nanoseconds** messageTypeSpecific: 0 **ClockIdentity: 0x0242c0fffea80a07** SourcePortID: 1 sequenceId: 16 controlField: Sync Message (0) logMessagePeriod: 0 (1.000000 s) originTimestamp (seconds): 0 originTimestamp (nanoseconds): 0 [This is a Sync to Follow Up in Frame: 2] [Community ID: 1:7j1jCCJSKEdT7mFEVcvyrkKQs58=]	
Test Result	Pass ☐	Fail ☐	

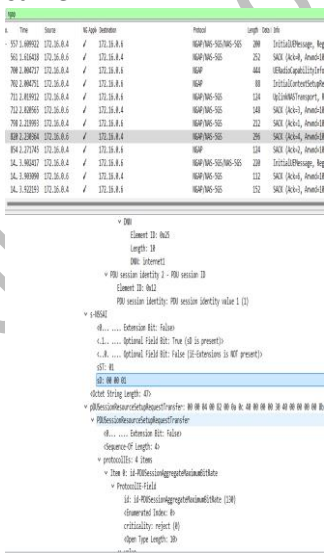
Signaltron Confidential Do not copy

Test ID	4.2(xii) Antenna		
Requirement	External or Internal		
Test Objective	To verify antenna type used.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	External antenna is used and can be verified physically.	Physical Verification	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(xiii)Mechanical/Environmental		
Requirement	IP54/QM333 wherever applicable. Environment testing. Temperature and Humidity as per the Indian Geographical conditions.		
Test Objective			
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Product is designed to be dust resistant. Product to be tested under various operating temperature, humidity and environment. Verify from gNB Statistics log at Please check the logs at /home/user1/statistics_log.txt	Physical Verification and ensure gNB operates without any fault by checking the 5G devices connected. Verify from the gNB statistics log.	
Test Result	Pass ☐	Fail ☐	

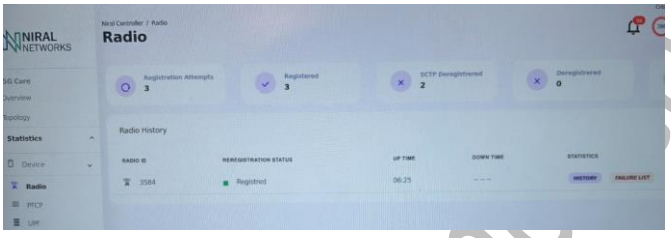
Signaltron Confidential. Do not copy

Test ID	4.2(xv) Network Slicing		
Requirement	Support for slicing. Preconfigured 3 different slices (min). Support for configuring slices by Institutions.		
Test Objective			
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	3 Different Slices configured at RAN andCore end **Slice 1:** **sst: 1 sd: 010203,dnn:** **internet** **Take tcp dump pcap inCU/DU By below command:** **tcpdump -i any -w test.pcap** **Slice 2:** **sst: 1 sd: 000001dnn:** **internet1** **Take tcp dump pcap inCU/DU By below command:** **tcpdump -i any -wtest1.pcap** **Slice 3:** **sst: 1 sd: 000002dnn: internet2** **Take tcp dump pcap inCU/DU By below command:** **tcpdump -i any -w test.pcap** **All 3 Mobiles set APN asinternet, internet1 and internet2.** **Apply the filter "ngap" in wireshark log. Check the NGSetupResponse and check the sliceSupportedList**	As per the test case. **From the UE logs:** we can verify the network slices configured. Need to check PDU Session Establishment Accept message for the same.  **PCAP log:** NG Application Protocol (NGSetupResponse) NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-NGSetup (21) criticality: reject (0) value NGSetupResponse **sliceSupportList: 1 item** **Item 0** **SliceSupportItem** **s-NSSAI** **sST: 01** **sD: 000007**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential not copy

Test ID	4.2(xvi) 5G Use case scenarios		
Requirement	eMBB(R15), URLLC(R16), MMTC(R16)		
Test Objective	Test to verify SST -1(eMBB)		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Power on 5G UEs and let it Register with 5G Network provided. Filter for NGAP messages in Wireshark log. Verify in PDUSessionSetupRequest for SST. Alternatively, Cross check the UE log for SST in PDU Session Establishment Accept message. URLLC and MMTC - Roadmap	**From gNB PCAP log:** NG Application Protocol (PDUSessionResourceSetupRequest) NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest s-NSSAI **sST: 01** **sD: 000007** **From UE log:** *** Layer 3 Message type: PDU Session Establishment Accept S-NSSAI **Slice/service type (SST) : (1) eMBB - Slice suitable for the handling of 5G enhanced Mobile Broadband** **Slice differentiator (SD) : 7 (000007 hex)**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(xvii) Uptime		
Requirement	99% availability		
Test Objective	To check stability of the system		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Keep the setup up for overnight (12Hr) Login into NMS (Refer to NiralOS_UserGuideVer1.0, Section 6.1). Run uptime and show the screen shot.	Check that setup is not down for more than 1% of the time. It can be verified from Niral NMS screen shown as below:  .	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(xviii) MEC		
Requirement	Should support integration with edge compute and cloud platforms.		
Test Objective			
Description	Test Steps	Acceptance Criteria	Remarks
	Login into NMS Dashboard(172.16.0.5) User name:admin Password :admin@1234 Go to Edge cloud ->Mec server->details- > create vm		It supports integration with edge compute Cloud platformwill be in Phase2
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(xix) VoNR		
Requirement	Should support VoNR		
Test Objective	Verify Voice and Video call over N/W		
Description	Test Steps	Acceptance Criteria	Remarks
	In the roadmap	Roadmap	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

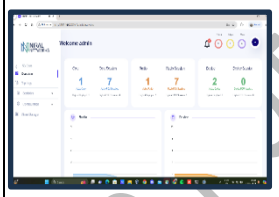
<table>
<tr><td>Test ID</td><td colspan="3">4.2(xx) APIs</td></tr>
<tr><td>Requirement</td><td colspan="3">Should Support APIs- for example any NMS, MEC Platform integration, OT/IT integrations</td></tr>
<tr><td>Test Objective</td><td colspan="3">APIs should be supported in NMS, MEC platform and OT/IT integrations.</td></tr>
<tr><td rowspan="2">Description</td><td>Test Steps</td><td>Acceptance Criteria</td><td>Remarks</td></tr>
<tr><td>1. Connect any laptop or Desktop Device to theRouter to Attain IP in Range of
172.16.0.X/24 Subnet
2. Open Postman on theconnected Laptop or Desktop
Niral Networks SDN Controller (NMS API)
Login:
Method:
POST http://IP-ADDRESS:8082/token
JSON Body:
{
"username":"admin",
"password":"admin@1234"
}

5G Core Overview:

Method: GET
http://172.16.0.5:8082/5gcoredata/overview/range=hour

Paste the token in the authorization tab inside token portion and then click send</td><td>{
"accessToken": "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImV4cCI6MTcyNjIzMDA5NywiaWF0IjoxNzI2MjI5ODU3fQ.LcOFVve4-yhezaZLvL4VgqmiXRwKNRy9K68jNbg2WWz-dr8hiu0_CaypTui6ImZCT8xrl9aS_zDkSw52K08d6w",
"refreshToken": "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImV4cCI6MTcyNjI1NjE1NCwiaWF0IjoxNzI2MjI5ODU3fQ.T52fqZx1v8EjDUgorXCyut-CkXvpkQtW2IWIzq99pUafusPMV84OBvBRKspU4msn9UH-t8HMQuwEshDKPr_pPg"
}
{
"liveDataModel": {
"controllerClientId": "ncc-f80JxSJCGBckvLDAwmXflj",
"activeAmfSession": "0",
"totalAmfSession": "9",
"activeamf": "1",
"totalamf": "1",
"activeUe": "1",
"totalUe": "3",
"activeUeSession": "0",
"totalUeSession": "0",
"activeGnb": "1",
"totalGnb": "1",
"activeGnbSession": "0",
"totalGnbSession": "0",
"siteId": "5G-Lab",
"tenentId": "TCIL",
"nfType": "amf",
"nfName": "niralos-amf-1"
}
}</td><td>Is supportingAPIs – for example any NMS, MEC platform integration, OT/IT integrations.</td></tr>
<tr><td>Test Result</td><td>Pass ☐</td><td>Fail ☐</td><td></td></tr>
</table>

Signaltron Confidential Do not copy

Test ID	4.2(xxi) NMS with dashboards		
Requirement	Integrated with Core / Radio / other IT devices.		
Test Objective	Verify Core integrated with NMS		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	I.Login to 172.16.0.5 2. click on the NiralOS 5G Core icon	Check that all devices status is visible on NMS 	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.2(xxii)Security		
Requirement	Features to ensure system security (security features for Core, RAN and devices, solution for internal and external attack vectors, proactive security monitoring, reporting and alarms, are the security alerts stored including supporting data & logs). Security considerations in deployment of solution – both interface and application level to be considered.		
Test Objective	Verify system security		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**

	In postman following commands to access system
	Get http://172.16.0.5:8082/edge/node/get_internal_data
	
	For Alarm Monitoring: Login NMS Goto 5G Core->Alarm Manager
		{
		"error": "Full authentication is required to access this resource"
		}
			Session expired,no access to system. Need new Token to access the particular system for Security.

Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

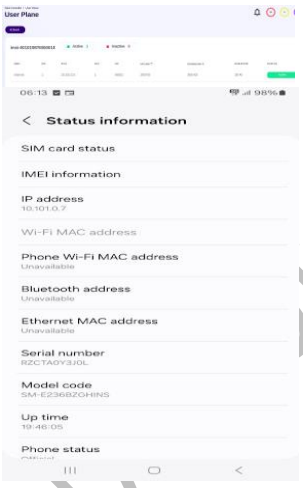
Test ID	4.2(xxiii) 5G Devices		
Requirement	All 5G devices to support private PLMN IDs.		
Test Objective	Verify system security		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**

	Configure the Private PLMN ID for the Core Network using the configuration file Scrf_niral.conf
	
	Insert the SIM card with Private PLMN ID into 5G devices and power on.
	Show the PLMN ID in the PCAP log for SIB1, RRC Setup complete, Registration Accept or show it Netmonster tool application on the smartphone
		In scrf_niral.conf:
		below indicates the configured PLMN ID:
		gNBs =
		(
		{
		////////// Identification parameters:
		gNB_ID = 0xe00;
		gNB_name = "gNB-ST";
		
		// Tracking area code, 0x0000 and 0xfffe are reserved values
		tracking_area_code = 1;
		plmn_list = ({
		mcc = 001;
		mnc = 01;
		
		In the UE log:
		we can check the PLMN ID configured by checking SIB1 content
		
		Ensure the 5G devices are able to register with Private PLMN IDs.
		
		*** Layer 3 Message type: SIB1 (BCCH-DL-SCH)
		Device: EQ1
		MessageDirection: DL
		MessageProtocol: NR-RRC
		MessageChannel: BCCH-SCH
		Channel
		Physical Cell ID : 0
		Frequency : 641280
		SFN : 3226206212
		cellSelectionInfo
		Q-RxLevMin : -65
		cellAccessRelatedInfo
		plmn-IdentityInfoList
		PLMN-IdentityInfoList :
		[0] :
		plmn-IdentityList :
		[0] :
		MCC : 001
		MNC : 01	

Signaltron Confidential. Do not copy

Test Result	Pass ☐	Fail ☐

Signaltron Confidential. Do not copy

Test ID	4.2(xxiv) IP Communication		
Requirement	IPv4 and IPv6 should be supported		
Test Objective	To verify IPv4 Rel 15		
Description	Test Steps	Acceptance Criteria	Remarks
	Login to NMS (172.16.0.5) Dashboard->5G core->Statistics->Devices->Userplane Then click on the imsi values inside UE Information part		IPV4 showing in NMS and can be verified in UE. IPV4 format showing in particular tab.
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

4.3 Section:- Functional Specifications: 5G SA Core Networks

Test ID	4.3 (i)		
Requirement			
Test Objective			Remarks
Test Description	Test Steps	Acceptance Criteria	
Overall Test Result	Pass: □	Fail: □	

Signaltron Confidential. Do not copy

4.3.2 The 5G System architecture consists of the following network functions (NF).

Test ID	4.3.2 (a) Authentication Server Function (AUSF)		
Requirement	AUSF		
Test Objective	To verify authentication server function registration in NRF.		
Test Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	1. AUSF registration with NRF 1.1 AUSF request to NRF: HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/d5c3908c-718c-41ef-944a-a17d68dae56e Header: user-agent: AUSF Header: 3gpp-sbi-discovery-target-nf-type: NRF 1.2 NRF response to AUSF: HEADERS[33]: 201 Created Header: :status: 201 Created Json Body: DATA[33], JSON (application/json) Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd 2. Service provide by AUSF url : /nausf-auth/v1/ue-authentications SBI Interface Refrence Point - N12(Between AUSF and AMF)	Value: AUSF user-agent: AUSF Value: NRF Value: 201 :status: 201 Member: nfType [Path with value: /nfType:AUSF] [Member with value: nfType:AUSF]	AUSF registered with NRF

Signaltron Confidential. Do not co

	Header: 3gpp-sbi-discovery-service-names: nausf-auth Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: AUSF Json body: DATA[3], JSON (application/json) Object Member: supiOrSuci Member: servingNetworkName SBI Interface Refrence APIs – API - /nudm-ueau/v1/security-information/generate-auth-data(Between AUSF and UDM) Method – POST Interface Refrence Point – N13 Header: 3gpp-sbi-discovery-service-names: nudm-ueau Header: user-agent: AUSF Header: 3gpp-sbi-discovery-target-nf-type: UDM Response from UDM to AUSF HEADERS[13]: 200 OK Header: :status: 200 OK DATA[13], JSON (application/json) Object Member: authType Member: authenticationVector Member: supi Response from AUSF to AMF HEADERS[3]: 201 Created Header: :status: 201 Created DATA[23], JSON (application/3gpphal+json) Object Member: authType Member: 5gAuthData	String value: AUSF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus] Value: nausf-auth Member: supiOrSuci [Path with value: /supiOrSuci:suci-0-001-01-0-0-0-9876500015] [Member with value: supiOrSuci:suci-0-001-01-0-0-0-9876500015] Member: servingNetworkName [Path with value: /servingNetworkName:5G:mnc001.mcc001.3gppnetwork.org] [Member with value: servingNetworkName:5G:mnc001.mcc001.3gppnetwork.org] Value: nudm-ueau	

Signaltron Confidential. Do not copy

	Member: _links	Value: AUSF user-agent: AUSF Value: UDM Value: 200 :status: 200 String value: 5G_AKA Key: authType Member: rand [Path with value: /authenticationVector/rand:16e64004e2c156c1b28fc647f6b88729] [Member with value: rand:16e64004e2c156c1b28fc647f6b88729] Member: autn [Path with value: /authenticationVector/autn:27c315cb79a0800038168b97dc39fc70] [Member with value: autn:27c315cb79a0800038168b97dc39fc70] Member: kausf [Path with value: /authenticationVector/kausf:6de380fa118331e5c0415dedce0daa9f68df449b0c6246c91e6bfaaeb22005c8] [Member with value: kausf:6de380fa118331e5c0415dedce0daa9f68df449b0c6246c91e6bfaaeb22005c8] Member: supi [Path with value: /supi:imsi-001019876500015] [Member with value: supi:imsi-001019876500015] Value: 201 :status: 201 Member: authType [Path with value: /authType:5G_AKA] [Member with value: authType:5G_AKA] Member: rand [Path with value: /5gAuthData/rand:16e64004e2c156c1b28fc647f6b88729] [Member with value: rand:16e64004e2c156c1b28fc647f6b88729]	

Signaltron Confidential. Do not copy

		Member: autn [Path with value: /5gAuthData/autn:27c315cb79a0800038168b97dc39fc70] [Member with value: autn:27c315cb79a0800038168b97dc39fc70]	
Overall Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.3.2 (b) Access and Mobility Management Function (AMF)		
Requirement	AMF		
Test Objective	Verify Access and Mobility Management Function.		Remarks
	Test Steps	Acceptance Criteria	
	AMF registration with NRF: 1.1 AMF request to NRF HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/d5810b90-718c-41ef-b1f1-7d1be304863e Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: NRF 1.2 NRF response to AMF HEADERS[19]: 201 Created Header: :status: 201 Created Json body: DATA[305], JSON (application/json-patch+json) Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd Verification of Communication service API: - UE Registration Registration request from UE	Value: 201 :status: 201 Member: nfType [Path with value: /nfType:AMF] [Member with value: nfType:AMF] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] RAN-UE-NGAP-ID: 3 userLocationInformationNR nR-CGI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) 0000 0000 0000 0000 0000 0000 1101 0000 0101 .... = nRCellIdentity: 0x000000d05 tAI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001)	AMF Registered with NRF Successfully

Signaltron Confidential. Do not copy

	to AMF on N1 Interface: InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] protocolIEs: 5 items Item 0: id-RAN-UE-NGAP-ID Item 1: id-NAS-PDU Item 2: id-UserLocationInformation Item 3: id-RRCEstablishmentCause Item 4: id-UEContextRequest Registration accept from AMF to UE InitialContextSetupRequest, Registration accept protocolIEs: 8 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-GUAMI Item 3: id-AllowedNSSAI Item 4: id-UESecurityCapabilities Item 5: id-SecurityKey Item 6: id-MaskedIMEISV Item 7: id-NAS-PDU Registration complete from UE to AMF UplinkNASTransport, Registration complete	Mobile Network Code (MNC): Unknown (01) tAC: 12594 (0x003132) AMF-UE-NGAP-ID: 4 RAN-UE-NGAP-ID: 3 s-NSSAI sST: 01 sD: 010203 SecurityKey: a4b983b20924ca89327f0d1760cb7cb0ef86b98c05cd2193d9dcdda745ba4d42 [bit length 256] .... .001 = 5GS registration result: 3GPP access (1) AMF-UE-NGAP-ID: 4 RAN-UE-NGAP-ID: 3 Message type: Registration complete (0x43) tAC: 12594 (0x003132) Value: nausf-auth Member: supiOrSuci [Path with value: /supiOrSuci:suci-0-001-01-0-0-0-9876500015] [Member with

Signaltron Confidential. Do not copy

	protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID Item 1: id-RAN-UE-NGAP-ID Item 2: id-NAS-PDU Item 3: id- UserLocationInformation Service between AMF to AUSF url : POST /nausf-auth/v1/ue-authentications SBI Interface Refrence Point - N12(Between AUSF and AMF) Header: 3gpp-sbi-discovery-service-names: nausf-auth Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: AUSF Response from AUSF to AMF Json body: DATA[3], JSON (application/json) Object Member: supiOrSuci Member: servingNetworkName DATA[23], JSON (application/3gpphal+json) Object Member: authType Member: 5gAuthData Member: _links From AMF to Radio InitialContextSetupRequest, Registration accept From Radio to AMF InitialContextSetupResponse From Radio to AMF UEContextReleaseRequest [Cause: RadioNetwork=failure-in-radio-interface-procedure]	value: supiOrSuci:suci-0-001-01-0-0-0-9876500015] Member: servingNetworkNam e [Path with value: /servingNetworkNam e:5G:mnc001.mcc00 1.3gppnetwork.org] [Member with value: servingNetworkNam e:5G:mnc001.mcc00 1.3gppnetwork.org] Member: authType [Path with value: /authType:5G_AKA] [Member with value: authType:5G_AKA] Member: rand [Path with value: /5gAuthData/rand:16e64004e2c156c1b28fc647f6b88729] [Member with value: rand:16e64004e2c156c1b28fc647f6b88729] Member: autn [Path with value: /5gAuthData/autn:27c315cb79a0800038168b97dc39fc70] [Member with value:

Signaltron Confidential. Do not copy

	From AMF to Radio UEContextReleaseCommand [Cause: RadioNetwork=failure- in-radio-interface-procedure] From Radio to AMF UEContextReleaseComplete Interface between AMF to SMF on N11 PDU session control message Request from AMF to SMF POST /nsmf-pdusession/v1/sm-contexts Header: 3gpp-sbi-discovery-service-names: nsmf-pdusession Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: SMF Response from SMF to AMF HEADERS[111]: 201 Created DATA[111], JSON (application/json) Stream: DATA, Stream ID: 111, Length 3 JavaScript Object Notation: application/json Interface : SBI interface reference point N15: Between PCF and AMF Communication service API: Access Management policies request during Registration request and accept event: HEADERS[127]: POST /npcf-am-policy-control/v1/policies Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: PCF Header: 3gpp-sbi-target-apiroot:	autn:27c315cb79a080003816 8b97dc39fc70 Value: 201 :status: 201 Object Value: nsmf-pdusession Value: AMF Value: SMF Member: supi [Path with value: /request/supi:imsi-001019876500015] [Member with value: supi:imsi-001019876500015] Member: accessType [Path with value: /request/accessType:3GPP_ACCESS] [Member with value: accessType:3GPP_ACCESS] Member: uplink [Path with value: /request/ueAmbr/uplink:1048576 Kbps] [Member with value: uplink:1048576 Kbps] Member: downlink [Path with value: /request/ueAmbr/downlink:1048576 Kbps] [Member with value: downlink:1048576 Kbps] String value: 1048576 Kbps Value: 201 :status:201 Member: mcc [Path with value: /guami/plmnId/mcc:001] [Member with value: mcc:001] Member: mnc [Path with value:

Signaltron Confidential: Do not copy

	http://172.18.0.7:7777 Header: 3gpp-sbi-max-rsp-time: 10000 Header: 3gpp-sbi-discovery-service-names: npcf-am-policy-control DATA[127], JSON (application/json) JavaScript Object Notation: application/json Object Member: request Object Member: notificationUri Member: supi Member: accessType allowedSnssais Member: ueAmbr Object Member: uplink Member: downlink SBI interface reference point N8: Between AMF and UDM: Service:nudm-uecm AMF to UDM: Stream: HEADERS, Stream ID: 57, Length 91, PUT /nudm-uecm/v1/imsi-001019876500006/registrations/amf-3gpp-access Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: UDM UDM responses to AMF: Stream: HEADERS, Stream ID: 57, Length 74, 201 Created JSON body Member: mcc Member: mnc Member: amfId	/guami/plmnId/mnc:01] [Member with value: mnc:01] String value: 01 Key: mnc [Path: /guami/plmnId/mnc] Member: amfId [Path with value: /guami/amfId:020040] [Member with value: amfId:020040	
Overall Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.3.2 (c) Data Network (DN), e.g. operator services, Internet access or 3rd party services		
Requirement	Data Network (DN)		
Test Objective	Verify the Data Network -Internet access by 3rd party service.		Remarks
	Test Steps	Acceptance Criteria	
	Ping request from UE to DN(www.google.com). Check the PCAP logs with udp filter.	Echo (ping) request id=0x002a, seq=2/512, ttl=64 (reply in 11) GPRS Tunneling Protocol Flags: 0x34 Message Type: T-PDU (0xff) Length: 92 TEID: 0x00002f82 (12162) Next extension header type: PDU Session container (0x85) Extension header (PDU Session container) Internet Protocol Version 4, Src: 101.202.0.2 (101.202.0.2), Dst: dns.google (8.8.8.8) 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 84 Identification: 0x662f (26159) 010. .... = Flags: 0x2, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: ICMP (1) Header Checksum: 0x5e9e [validation disabled] [Header checksum status: Unverified] Source Address: 101.202.0.2 (101.202.0.2) Destination Address: dns.google (8.8.8.8) [Stream index: 0] Ping reply from DN to UE: Echo (ping) reply id=0x002a, seq=2/512, ttl=55 (request in 6) GPRS Tunneling Protocol	

Signaltron Confidential. Do not co

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

Signaltron Confidential. Do not copy

Test ID	4.3.2 (e)Network Repository Function (NRF)		
Requirement	NRF		
Test Objective	Verify NRF (Network Repository Function)		Remarks
	Test Steps	Acceptance Criteria	

Signaltron Confidential. Do not co

	Interface: SBI NF discovery service triggering by SMF for UDM to NRF: HEADERS[471]: GET /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=SMF&service-names=nudm-sdm&target-nf-type=UDM Header: :path: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=SMF&service-names=nudm-sdm&target-nf-type=UDM Header: :authority: niralos-nrf-1:7777 Response from NRF HEADERS[471]: 200 OK Json body: DATA[471], JSON (application/json) Object Member: validityPeriod Member: nfInstances Array Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: ipv4Addresses Member: nfServiceList	Value: /nnrf-disc/v1/nf-instances?requester-features=20&requester-nf-type=SMF&service-names=nudm-sdm&target-nf-type=UDM Value: niralos-nrf-1:7777 Value: 200 ok :status: 200 ok String value: UDM String vaue: REGISTER String value: 172.18.0.5 Member: serviceName [Path with value: /nfInstances/[]/nfServiceList/d5e40b00-718c-41ef-afbc-19030dd1418a/serviceName:nudm-sdm] [Member with value: serviceName:nudm-sdm]	SMF asks the UDM IP to NRF
Overall Test Result	**Pass: □**	**Fail: □**	

Signaltron Confidential. Do not copy

Test ID	4.3.2 (f)Network Slice Selection Function (NSSF)		
Requirement	NSSF		
Test Objective	Verify the NSSF (Network Slice Selection Function)		Remarks
	Test Steps	Acceptance Criteria	
Test Description	1. NSSF to NRF register: URL: /nnrf-nfm/v1/nf-instances/d6d50d34-718c-41ef-ba2b-77faccd0271f Header: user-agent: NSSF Header: 3gpp-sbi-discovery-target-nf-type: NRF Member: nfServiceList Response from NRF to NSSF HEADERS[61]: 201 Created Json body: DATA[61], JSON (application/json) Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd	**[Path with value: /nfServiceList/d6d554d8-718c-41ef-ba2b-77faccd0271f/serviceName:nnssf-nsselection]** **[Member with value: serviceName:nnssf-nsselection]** **Value: 201** **:status: 201** Member: nfType [Path with value: /nfType:NSSF] [Member with value: nfType:NSSF] String value: NSSF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	NSSF should be registered with NRF successfully.
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.3.2 (g)Policy Control Function (PCF)		
Requirement	PCF		
Test Objective	PCF (Policy Control Function)		Remarks
	Test Steps	Acceptance Criteria	

Signaltron Confidential. Do not

	PCF registration with NRF: PCF To NRF: **/nnrf-nfm/v1/nf-instances/e7c0552c-712d-41ef-900a-cfc4690b64be** Header: user-agent: PCF Header: 3gpp-sbi-discovery-target-nf-type: NRF Header: accept: application/json,application/problem+json Header: 3gpp-sbi-sender-timestamp: Thu, 12 Sep 2024 17:39:04.742 GMT Header: 3gpp-sbi-max-rsp-time: 10000 Header: 3gpp-sbi-discovery-service-names: nnrf-nfm Header: content-length: 1645 **Response:** **From NRF To PCF** **HEADERS[1]: 201 Created** **DATA[1], JSON (application/json)** Object Member: nfInstanceId Member: nfType Member: nfStatus Member:heartBeatTimer Member: nfProfileChangesInd **Interface :** **SBI interface reference point N15:** **Between PCF and AMF** **Communication service API:** **HEADERS[127]: POST /npcf-am-**	**value: 201** **:status:201** Member: nfType [Path with value: /nfType:PCF] [Member with value: nfType:PCF] String value: PCF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus] Member: supi [Path with value: /request/supi:imsi-001019876500015] [Member with value: supi:imsi-001019876500015] String value: imsi-001019876500015 Key: supi [Path: /request/supi] Member: accessType [Path with value: /request/accessType:3GPP_ACCESS] [Member with value: accessType:3GPP_ACCESS] String value: 3GPP_ACCESS Key: accessType [Path: /request/accessType] Member: uplink [Path with value: /request/ueAmbr/uplink:1048576 Kbps] [Member with value: uplink:1048576 Kbps] String value: 1048576 Kbps Key: uplink [Path: /request/ueAmbr/uplink] Member: downlink [Path with value:	**PCF successfully registered with NRF** **Note:All control plane Network function register with NRF with same message**

Signaltron Confidential. Do not copy

	policy-control/v1/policies Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: PCF Header: 3gpp-sbi-target-apiroot: http://172.18.0.7:7777 Header: 3gpp-sbi-max-rsp-time: 10000 Header: 3gpp-sbi-discovery-service-names: npcf-am-policy-control **DATA[127], JSON (application/json)** JavaScript Object Notation: application/json Object Member: request Object Member: notificationUri Member: supi Member: accessType allowedSnssais Member: ueAmbr Object Member: uplink Member: downlink	/request/ueAmbr/downlink:1048576 Kbps] [Member with value: downlink:1048576 Kbps] String value: 1048576 Kbps Key: downlink [Path: /request/ueAmbr/downlink] **Number value: 9** **Key: 5qi** Member: uplink [Path with value: /sessRules/1/authSessAmbr/uplink:1048576 Kbps] [Member with value: uplink:1048576 Kbps] Member: downlink [Path with value: /sessRules/1/authSessAmbr/downlink:1048576 Kbps] [Member with value: downlink:1048576 Kbps] Supported Features: 4000000 ...0 = TSC: False ..0. = ResShare: False .0.. = 3GPP-PS-Data-Off: False 0... = ADC: False ...0 = UMC: False ..0. = NetLoc: False .0.. = RAN-NAS-Cause: False	

Signaltron Confidential. Do not copy

	Between PCF and SMF on interface N7 to show session related parameter 5QI value: **HEADERS[55]: POST /npcf-smpolicycontrol/v1/sm-policies** Header: 3gpp-sbi-discovery-service-names: npcf-smpolicycontrol Header: user-agent: SMF Header: 3gpp-sbi-discovery-target-nf-type: PCF Response **Json body:** **DATA[55], JSON (application/json)** Object Member: sessRules Member: 5qi Member: suppFeat **Communication between PCF and UDR on N36 interface to get access management parameters** Request from PCF to UDR GET /nudr-dr/v1/policy-data/ues/imsi-001019876500015/am-data Header: 3gpp-sbi-discovery-service-names: nudr-dr Header: user-agent: PCF Header: 3gpp-sbi-discovery-target-nf-type: UDR Response from UDR to PCF HEADERS[77]: 200 OK	0... = ProvAFsignalFlow: False ...0 = PCSCF-Restoration-Enhancement: False ..0. = PRA: False .0.. = RuleVersioning: False 0... = SponsoredConnectivity: False ...0 = RAN-Support-Info: False ..0. = PolicyUpdateWhenUESuspends: False .0.. = AccessTypeCondition: False 0... = MultiIpv6AddrPrefix: False ...0 = SessionRuleErrorHandling: False ..0. = AF_Charging_Identifier: False .0.. = ATSSS: False 0... = PendingTransaction: False ...0 = URLLC: False ..0. = MacAddressRange: False .0.. = WWC: False 0... = QosMonitoring: False ...0 = AuthorizationWithRequiredQoS: False ..0. = EnhancedBackgroundDataTransfer: False .1.. = DN-Authorization: True 0... = PDUSessionRelCause: False Value:201 :status:201 **Member: sst** **[Path with value: /smPolicySnssaiData/1-010203/snssai/sst:1]** **[Member with value: sst:1]** **Member: sd** **[Path with value: /smPolicySnssaiData/1-010203/snssai/sd:010203]** **[Member with value: sd:010203]** **Member: dnn** **[Path with value: /smPolicySnssaiData/1-**	

Signaltron Confidential. Do not copy

	Member: smPolicySnssaiData	**010203/smPolicyDnnData/internet/dnn:internet]** **[Member with value: dnn:internet]**	
Overall Test Result	**Pass: □**	**Fail: □**	

Signaltron Confidential. Do not copy

Test ID	4.3.2 (h)Session Management Function (SMF)		
Requirement	SMF		
Test Objective	Verify the SMF (Session Management Function)		Remark
	Test Steps	Acceptance Criteria	

Signaltron Confidential. Do not cop

	SMF registration with NRF: SMF To NRF: HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/d5dda71a-718c-41ef-b9a9-5b526d41caa7 Header: 3gpp-sbi-discovery-target-nf-type: NRF Header: user-agent: SMF Response from NRF to SMF HEADERS[41]: 201 Created Json body: HEADERS[1]: 201 Created Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd Service provide by SMF to PCF over N7 interface HEADERS[55]: POST /npcf-smpolicycontrol/v1/sm-policies Header: 3gpp-sbi-discovery-service-names: npcf-smpolicycontrol Header: user-agent: SMF Header: 3gpp-sbi-discovery-target-nf-type: PCF	Member: nfType [Path with value: /nfType:SMF] [Member with value: nfType:SMF] String value: SMF Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus] Number value: 9 Key: 5qi ..00 0001 = Qos flow identifier: 1 Session-AMBR for downlink: 1 Gbps (1) Session-AMBR for uplink: 1 Gbps (1) PDU address information: 10.101.0.2 (10.101.0.2) DNN: internet Member: pduSessionType [Path with value: /pduSessionType:IPV4] [Member with value: pduSessionType:IPV4] String value: IPV4 Key: pduSessionType [Path: /pduSessionType] Member: dnn [Path with value: /dnn:internet] [Member with value: dnn:internet] String value: internet Key: dnn [Path: /dnn] IPv4: upf (172.18.0.9) Cause: Request accepted(success)	**SMF Registered with NRF Successfully**

Signaltron Confidential. Do not copy

	Response Json body: DATA[55], JSON (application/json) Object Member: sessRules Member: 5qi Member: suppFeat Interface between AMF to SMF on N11 Request from AMF to SMF For Session context after PDU Session Request Message POST /nsmf-pdusession/v1/sm-contexts Header: 3gpp-sbi-discovery-service-names: nsmf-pdusession Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: SMF Response from SMF to AMF /namf-comm/v1/ue-contexts/imsi-001019876500006/n1-n2-messages DATA[1], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequestTransfer Non-Access-Stratum 5GS (NAS)PDU Session establishment request from SMF to UPF on N4 inteface PFCP Session Establishment Request Packet Forwarding Control Protocol PDN Type : IPv4 User ID :	(1) TEID: 0x000720e6	

Signaltron Confidential. Do not copy

	APN/DNN : internet Response From UPF to SMF on N4 interface PFCP Session Establishment Response Node ID : IPv4 address: 172.18.0.9 Cause : Request accepted(success)		
Overall Test Result	**Pass: □**	**Fail: □**	

Signaltron Confidential. Do not copy

Test ID	4.3.2 (i) Unified Data Management (UDM)		
Requirement	UDM		
Test Objective	Verify the UDM (Unified Data Management Function)		Remark
	Test Steps	Acceptance Criteria	

Signaltron Confidential. Do not cop

	UDM: **1.UDM registration with NRF:** **1.1UDM To NRF:** **URL: /nnrf-nfm/v1/nf-instances/d5e3d77a-718c-41ef-afbc-19030dd1418a** **UDM:** **1.UDM registration with NRF:** **1.1UDM To NRF:** **URL: /nnrf-nfm/v1/nf-instances/d5e3d77a-718c-41ef-afbc-19030dd1418a** Header: user-agent: UDM Header: 3gpp-sbi-discovery-target-nf-type: NRF **1.2 Response from NRF to UDM** **Stream: HEADERS, Stream ID: 1, Length 116, 201 Created** **JSON body:** **JavaScript Object Notation: application/json** Object Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd **2.Service provided by UDM:** **2.1.SBI interface reference point N13:** **Between AUSF and UDM for authentication related parameters before Authentication request message** **Service : nudm-ueau** **AUSF TO UDM:** **Stream: HEADERS, Stream ID: 23, Length 74, POST /nudm-ueau/v1/imsi-001019876500006/auth-events**	**value: 201** **:status: 201** Member: nfType [Path with value: /nfType:UDM] [Member with value: nfType:UDM] String value: UDM Key: nfType [Path: /nfType] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus] **Value: 201** **:status:201** Member: success [Path with value: /success:true] [Member with value: success:true] True value Key: success [Path: /success] Member: authType [Path with value: /authType:5G_AKA] [Member with value: authType:5G_AKA] String value: 5G_AKA Key: authType [Path: /authType] **Value: 201** **:status:201** Member: mcc [Path with value: /guami/plmnId/mcc:001] [Member with value: mcc:001] String value: 001 Key: mcc [Path: /guami/plmnId/mcc]	UDM registered with NRF succesfully

Signaltron Confidential. Do not copy

	Header: user-agent: AUSF Header: 3gpp-sbi-discovery-target-nf-type: UDM **UDM RESPONSES TO AUSF:** **Stream: HEADERS, Stream ID: 25, Length 62, 201 Created** **JSON body:** Object Member: nfInstanceId Member: success Member: timeStamp Member: authType Member: servingNetworkName **2.2.SBI interface reference point N8:** **Between AMF and UDM for access related parameters after security mode complete** **Service:nudm-uecm** **AMF to UDM:** **Stream: HEADERS, Stream ID: 57, Length 91, PUT /nudm-uecm/v1/imsi 001019876500006/registrations/amf-3gpp-access** Header: user-agent: AMF Header: 3gpp-sbi-discovery-target-nf-type: UDM **UDM responses to AMF:** **Stream: HEADERS, Stream ID: 57, Length 74, 201 Created** **JSON body** Member: mcc Member: mnc Member: amfId	Member: mnc [Path with value: /guami/plmnId/mnc:01] [Member with value: mnc:01] String value: 01 Key: mnc [Path: /guami/plmnId/mnc] Member: amfId [Path with value: /guami/amfId:020040] [Member with value: amfId:020040] String value: 020040 Key: amfId [Path: /guami/amfId] Member: singleNssai Object Member: sst [Path with value: /[]/singleNssai/sst:1] [Member with value: sst:1] Number value: 1 Key: sst [Path: /[]/singleNssai/sst] Member: sd [Path with value: /[]/singleNssai/sd:010203] [Member with value: sd:010203] [Member with value: 5qi:9]	

Signaltron Confidential. Do not copy

	2.2.SBI interface reference point N10: **Between SMF and UDM for session related parameters** **Service: nudm-sdm** **SMF to UDM:** **GET /nudm-sdm/v2/imsi-001019876500006/sm-data** Header: user-agent: SMF Header: 3gpp-sbi-discovery-target-nf-type: UDM Header: 3gpp-sbi-discovery-service-names: nudm-sdm **UDM response to SMF:** **Stream: HEADERS, Stream ID: 53, Length 77, 200 OK** **JSON BODY:** JavaScript Object Notation: application/json Array Object Member: singleNssai		
Overall Test Result	**Pass: □**	**Fail: □**	

Signaltron Confidential. Do not copy

Test ID	4.3.2 (j) Unified Data Repository (UDR)		
Requirement	UDR		
Test Objective	Verify the UDR (Unified Data Repository).		Remark
	Test Steps	**Acceptance Criteria**	
	UDR: **1.UDR registration with NRF:** **1.1 UDR To NRF:** **Stream: HEADERS, Stream ID: 1, Length 254, PUT /nnrf-nfm/v1/nf-instances/d6059392-718c-41ef-ada8-b5bbefd3b673** Header: user-agent: UDR Header: 3gpp-sbi-discovery-target-nf-type: NRF **1.2 Response from NRF to UDR** **Stream: HEADERS, Stream ID: 1, Length 117, 201 Created** **JSON body:** **JavaScript Object Notation: application/json** **Object** Member: nfInstanceId Member: nfType Member: nfStatus Member: heartBeatTimer Member: nfProfileChangesInd **2.Service provided by UDR:**	value:201 :status:201 Member: nfType [Path with value: /nfType:UDR] [Member with value: nfType:UDR] Member: nfStatus [Path with value: /nfStatus:REGISTERED] [Member with value: nfStatus:REGISTERED] String value: REGISTERED Key: nfStatus [Path: /nfStatus]	UDR registered with NRF successfully

Signaltron Confidential. Do not copy

	2.1.SBI interface reference point N35: **Between UDM and UDR for subscription related parameters** **Stream: HEADERS, Stream ID: 31, Length 105, GET /nudr-dr/v1/subscription-data/imsi-001019876500006/authentication-data/authentication-subscription** Header: user-agent: UDM Header: 3gpp-sbi-discovery-target-nf-type: UDR **UDR responses to UDM:** **HEADERS[35]: 200 OK** **JSON BODY:** **JavaScript Object Notation: application/json** Object Member: authenticationMethod Member: encPermanentKey Member: sequenceNumber Member: encOpcKey	value:201 :status:201 Member: authenticationMethod [Path with value: /authenticationMethod:5G_AKA] [Member with value: authenticationMethod:5G_AKA] Member: encPermanentKey [Path with value: /encPermanentKey:18528600000000000000000000000000] [Member with value: encPermanentKey:18528600000000000000000000000000] Member: sequenceNumber Object Member: sqn [Path with value: /sequenceNumber/sqn:00000000d721] [Member with value: sqn:00000000d721] Member: encOpcKey [Path with value: /encOpcKey:bf6e133cd11b662a2ae639219409b7ea] [Member with value: encOpcKey:bf6e133cd11b662a2ae639219409b7ea]	
Overall Test Result	**Pass: □**	**Fail: □**	

Signaltron Confidential: Do not copy

Test ID	4..3.2 (k) User Plane Function (UPF)		
Requirement	UPF		
Test Objective	Verify UPF (User Plane Function)		Remark
	Test Steps	Acceptance Criteria	

Signaltron Confidential. Do not copy

Description	**Registration with SMF:** **Request from SMF side** **PFCP Association Setup Request over N4 interface** Packet Forwarding Control Protocol Message Type: PFCP Association Setup Request (5) Node ID : IPv4 address: 172.18.0.3 **Response from UPF side** **PFCP Association Setup Response over N4** Packet Forwarding Control Protocol Message Type: PFCP Association Setup Response (6) Node ID : IPv4 address: 172.18.0.9 Cause : Request accepted(success) **Service API:** **Session Connection From SMF side to UPF** **PFCP Session Establishment Request on N4** Packet Forwarding Control Protocol Message Type: PFCP Session Establishment Request (50) PDN Type : IPv4 User ID : APN/DNN : internet **Response from UPF** **PFCP Session Establishment Response on N4** Packet Forwarding Control Protocol Message Type: PFCP Session Establishment Response (51) Node ID : IPv4 address: 172.18.0.9 Cause : Request accepted(success) F-SEID : SEID: 0x0000000000003016, IPv4 172.18.0.9	IPv4: smf (172.18.0.3) IPv4: upf (172.18.0.9) accepted(success) (1) .. .001 = PDN Type: IPv4 (1) IMSI: 001019876500006 APN/DNN: internet Request accepted(success) (1) SEID: 0x0000000000003016	**UPF successfully registered with SMF**

Signaltron Confidential. Do not copy

	From SMF to UPF over N4 interface **PFCP Session Modification Request** Message Type: PFCP Session Modification Request (52) SEID: 0x0000000000003016	Cause: Request
	PFCP Session Modification Response from UPF to SMF over N4 interface Message Type: PFCP Session Modification Response (53) Cause : Request accepted(success)	accepted(success) (1) TEID: 0x00002f82 (12162) QoS Flow Identifier (QFI): 1
	PING service: **UL packet from UE to DN** Echo (ping) request id=0x002a, seq=3/768, ttl=64 (reply in 17) GPRS Tunneling Protocol Extension header (PDU Session container) Internet Protocol Version 4, Src: 101.202.0.2 (101.202.0.2), Dst: 8.8.8.8 (8.8.8.8) Internet Control Message Protocol	
	DL packet from DN to UE Echo (ping) reply id=0x002a, seq=7/1792, ttl=55 (request in 36) GPRS Tunneling Protocol Extension header (PDU Session container) Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 101.202.0.2 (101.202.0.2) Internet Control Message Protocol	TEID: 0x00000001 (1) QoS Flow Identifier (QFI): 1

Signaltron Confidential. Do not copy

Overall Test Result	**Pass: □**	**Fail: □**

Signaltron Confidential. Do not copy

4.4 Section :- 5G NR Radio

1. gNodeB Functions

Test ID	4.4.1 Functions for Radio Resource Management		
Requirement	Functions for Radio Resource Management: Radio Bearer Control, Radio Admission Control, Connection Mobility Control		
Test Objective	Check RRC message in UL and DL.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Register UE with gNodeB Collect TEMS logs or gNodeB PCAP logs and verify 1) RRC setup procedure, 2) PDU session establishment procedure 3) Check the RRC reconfiguration in PCAP. Show the mapping between QFI and DRB Identifier Indicates Radio bearer control. 4) Initiate flight mode on to initiate PDU session release followed by RRC connection release.	**RRC Setup procedure for Radio Admission**: NR Radio Resource Control (RRC) protocol UL-CCCH-Message message: c1 (0) c1: rrcSetupRequest (0) rrcSetupRequest rrcSetupRequest ue-Identity: randomValue (1) randomValue: 022813c302 [bit length 39, 1 LSB pad bits, 0000 0010 0010 1000 0001 0011 1100 0011 0000 001. decimal value 4631159169] establishmentCause: mo-Signalling (3) NR Radio Resource Control (RRC) protocol DL-CCCH-Message message: c1 (0) c1: rrcSetup (1) rrcSetup rrc-TransactionIdentifier: 3 criticalExtensions: rrcSetup (0) rrcSetup radioBearerConfig srb-ToAddModList: 1 item Item 0 SRB-ToAddMod srb-Identity: 1 NR Radio Resource Control (RRC) protocol UL-DCCH-Message message: c1 (0) **c1: rrcSetupComplete (2)** rrcSetupComplete rrc-TransactionIdentifier: 3 criticalExtensions: rrcSetupComplete (0) rrcSetupComplete selectedPLMN-Identity: 1 registeredAMF amf-Identifier: 020040 [bit length 24, 0000 0010 0000 0000 0100 0000 decimal value 131136] guami-Type: native (0)	

Signaltron Confidential. Do not copy

		dedicatedNAS-Message: **PDU Session Resource Setup Request** for Radio bearer control. gNB/Core network assigns QFI:1 for Internet default bearer with 5QI value of 9. NG Application Protocol (**PDUSessionResourceSetupRequest**) NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest s-NSSAI sST: 01 sD: 000007 criticality: reject (0) value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1073741824bits/s pDUSessionAggregateMaximumBitRateUL: 1073741824bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a07 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0111 decimal value 3232238087] TransportLayerAddress (IPv4): 192.168.10.7 gTP-TEID: 000477bc QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem qosFlowIdentifier: 1 qosFlowLevelQosParameters	

Signaltron Confidential. Do not copy

		qosCharacteristics: nonDynamic5QI (0) nonDynamic5QI fiveQI: 9 allocationAndRetentionPriority priorityLevelARP: 1 pre-emptionCapability: shall-not-trigger-pre-emption (0) pre-emptionVulnerability: not-pre-emptable (0) In RRC Reconfiguration message, gNB assigns the Data Radio bearer ID of 1 for QFI1. NR Radio Resource Control (RRC) protocol DL-DCCH-Message message: c1 (0) **c1: rrcReconfiguration (0)** rrcReconfiguration rrc-TransactionIdentifier: 1 criticalExtensions: rrcReconfiguration (0) rrcReconfiguration radioBearerConfig srb-ToAddModList: 2 items Item 0 SRB-ToAddMod srb-Identity: 1 Item 1 SRB-ToAddMod srb-Identity: 2 drb-ToAddModList: 1 item Item 0 DRB-ToAddMod cnAssociation: sdap-Config (1) sdap-Config pdu-Session: 8 sdap-HeaderDL: absent (1) sdap-HeaderUL: absent (1) 1... .... defaultDRB: True mappedQoS-FlowsToAdd: 1 item Item 0 **QFI: 1** **drb-Identity: 1**	

Signaltron Confidential Do not copy

		PDU session release should be initiated when data is disabled or UE is detached followed by RRC connection release NG Application Protocol **(PDUSessionResourceReleaseCommand)** NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceRelease (28) criticality: reject (0) value PDUSessionResourceReleaseCommand protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 21 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 2: id-NAS-PDU ProtocolIE-Field id: id-NAS-PDU (38) criticality: ignore (1) value NAS-PDU: 7e02259f762e447e00680100052e0809d3241208 Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: **5G mobility management** messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0x259f762e Sequence number: 68 Encrypted data Item 3: id-PDUSessionResourceToReleaseListRelCmd ProtocolIE-Field id: id-PDUSessionResourceToReleaseListRelCmd (79) criticality: reject (0) value PDUSessionResourceToReleaseListRelCmd: 1 item Item 0	

Signaltron Confidential: Do not copy

		PDUSessionResourceToReleaseItemRelCmd pDUSessionID: 8 pDUSessionResourceReleaseCommandTransfer: 10 PDUSessionResourceReleaseCommandTransfer cause: nas (2) nas: normal-release (0) NG Application Protocol **(PDUSessionResourceReleaseResponse)** NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-PDUSessionResourceRelease (28) criticality: reject (0) value PDUSessionResourceReleaseResponse protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: ignore (1) value AMF-UE-NGAP-ID: 21 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: ignore (1) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceReleasedListRelRes ProtocolIE-Field id: id-PDUSessionResourceReleasedListRelRes (70) criticality: ignore (1) value PDUSessionResourceReleasedListRelRes: 1 item Item 0 PDUSessionResourceReleasedItemRelRes pDUSessionID: 8 pDUSessionResourceReleaseResponseTransfer: <MISSING> NG Application Protocol (**UEContextReleaseCommand**) NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-UEContextRelease (41) criticality: reject (0) value UEContextReleaseCommand	

Signaltron Confidential Do not copy

		protocolIEs: 2 items Item 0: id-UE-NGAP-IDs ProtocolIE-Field id: id-UE-NGAP-IDs (114) criticality: reject (0) value UE-NGAP-IDs: uE-NGAP-ID-pair (0) uE-NGAP-ID-pair aMF-UE-NGAP-ID: 21 rAN-UE-NGAP-ID: 0 Item 1: id-Cause ProtocolIE-Field id: id-Cause (15) criticality: ignore (1) value Cause: nas (2) nas: deregister (2) NG Application Protocol (**UEContextReleaseComplete**) NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-UEContextRelease (41) criticality: reject (0) value UEContextReleaseComplete protocolIEs: 2 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: ignore (1) value AMF-UE-NGAP-ID: 21 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: ignore (1) value RAN-UE-NGAP-ID: 0 NR Radio Resource Control (RRC) protocol DL-DCCH-Message message: c1 (0) c1: **rrcRelease (2)** rrcRelease rrc-TransactionIdentifier: 0 criticalExtensions: rrcRelease (0) rrcRelease	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential Do not copy

Test ID	4.4.1 a) Dynamic allocation of resources to UEs in both uplink and downlink (scheduling)		
Requirement	Dynamic allocation of resources to UE in both uplink and downlink(scheduling)		
Test Objective	This test case evaluates the impact of LA on the DL and UL throughput measuring the throughput achieved under different channel scenarios		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Test 5G devices from different locations with respect to gNB to get variation in RSRP /RSRQ Measure the throughput using speed test application Check the UE logs or PCAP logs of gNodeB for resource allocation For PUSCH allocation, DCI format 0_1 is used and the same can be found in UE log.	**UE log for downlink allocation:** *** Mode Report Message type: NR 5G MAC PDSCH Status Beam Change : 0 Signal Change : 0 DL Dynamic Cfg Change : 0 DL Config : 0 UL Config : 0 ML1 State Change : 0 Log Fields Change Bit Mask : 0x0000 Sub ID : 0 Num Records : 2 Records : [0] : Slot : 10 Numerology : 30 kHz Frame : 132 Num PDSCH Status : 1 PdschStatusInfo : [0] : Tech ID : 1 Opcode : 0 Conn ID : 0 SCell Id Raw : 0 SFN : 132 Slot : 10 Bandwidth : 3 Band Type : 0 VariantId : 0 Physical Cell ID : 0 EARFCN : 641280 TB Index : 0 TB Size : 84 SCS MU : 30 kHz Num RBs : 10 RV : 0 HARQ or MBSFN Area ID : 7 RNTI Type : 0 K1 or PMCH ID : 7 TCI : 0 Num Layers : 2 Iteration Index : 0 CRC Status : PASS New Tx Flag : 1 NDI : 1	

Signaltron Confidential. Do not copy

		Discard Mode : 0 Bypass Decode : 0 Bypass HARQ : 0 Num ReTx : 0 HD Onload Timeout : 0 HARQ Onload Timeout : 0 HD Offload Timeout : 0 HARQ Offload Timeout : 0 Did Recomb : 0 Is IOVec Valid : True Mod Type : QPSK High Clock Mode : 0 Num Rx : 4x4 MIMO Rx Antenna Mapping0 : 0 Rx Antenna Mapping1 : 0 Rx Antenna Mapping2 : 0 Rx Antenna Mapping3 : 0 [1] : Slot : 16 Numerology : 30 kHz Frame : 132 Num PDSCH Status : 1 PdschStatusInfo : [0] : Tech ID : 1 Opcode : 0 Conn ID : 0 SCell Id Raw : 0 SFN : 132 Slot : 16 Bandwidth : 3 Band Type : 0 VariantId : 0 Physical Cell ID : 0 EARFCN : 641280 TB Index : 0 TB Size : 42 SCS MU : 30 kHz **Num RBs : 5** RV : 0 HARQ or MBSFN Area ID : 9 RNTI Type : 0 K1 or PMCH ID : 2 TCI : 0 Num Layers : 2 Iteration Index : 0 CRC Status : PASS New Tx Flag : 1 NDI : 1 Discard Mode : 0 Bypass Decode : 0 Bypass HARQ : 0 Num ReTx : 0 HD Onload Timeout : 0 HARQ Onload Timeout : 0	

Signaltron Confidential: Do not copy

		HD Offload Timeout : 0 HARQ Offload Timeout : 0 Did Recomb : 0 Is IOVec Valid : True Mod Type : QPSK High Clock Mode : 0 Num Rx : 4x4 MIMO Rx Antenna Mapping0 : 0 Rx Antenna Mapping1 : 0 Rx Antenna Mapping2 : 0 Rx Antenna Mapping3 : 0 **For uplink scheduling, search for DCI format : Ul01 in the UE log** *** Mode Report Message type: NR 5G MAC DCI Info Device: EQ1 CurrentRAT: Nr Time : 15:22:19.073 Length : 68 Log Code (Hex) : 0xB885 HW Timestamp : (35538496.25 ms) 09:52:18.496 Version : 131077 (v2.5) MAC Version Minor : 5 Major : 2 Log Fields Change Sleep : 0 Beam Change : 0 Signal Change : 0 DL Dynamic Cfg Change : 0 DL Config : 0 UL Config : 0 ML1 State Change : 0 Log Fields Change BMask : 0x0000 Num Records : 1 Records : [0] : Slot : 5 Numerology : 30 kHz Frame : 65 Num DCI : 1 DCI Info : [0] : Carrier ID : 0 RNTI Type : C_RNTI **DCI Format : Ul01** Aggregation Level : Level2 Raw DCI Included : 1 Raw DCI Payload : [0] : 0 [1] : 134217728 [2] : 214508096	

Signaltron Confidential: Do not copy

		DCI Format : Ul01 Carrier ID : 0 NDI : 0 **MCS : 9** Freq Hopping Flag : 0 RV : 0 **HARQ ID : 9** PUSCH TPC : 0 UL SUL Ind : 0 Symbol Alloc Index : 2 BWP Ind : 0 PTRS DMRS Association : 0 Beta Offset Ind : 0 **RB Assignment : 204** UL SCH Ind : 1 DAI 1 : 0 DAI 2 : 0 SRS Resource Indication : 0 Precoding Layer Info : 63 Antenna Ports : 0 DMRS Seq Init Flag : 0 SRS Request : 0 CSI Request : 0 CBGTI : 0 RA Type : 1 Prune Reason MSB : NONE Pruned Mask : 0x00000000	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (b) Header compression, encryption and integrity protection of data		
Requirement	IP header compression, encryption and integrity protection of data;		
Test Objective	To verify Encryption and Integrity protection.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Register UE with gNodeB Check the content of RRC Reconfiguration message to verify gNB configuring ROHC, Ciphering and Integrity algorithms. Please note: ROHC will be enabled with VoNR support Show PCAP log	[Configuration frame: 126] **[Ciphering Algorithm: NEA0 (NULL) (0)]** **[Integrity Algorithm: NIA2 (AES) (2)]** NR Radio Resource Control (RRC) protocol DL-DCCH-Message message: c1 (0) c1: rrcReconfiguration (0) rrcReconfiguration rrc-TransactionIdentifier: 1 criticalExtensions: rrcReconfiguration (0) rrcReconfiguration radioBearerConfig QFI: 1 drb-Identity: 1 pdcp-Config drb discardTimer: infinity (15) pdcp-SN- SizeUL: len18bits (1) pdcp-SN- SizeDL: len18bits (1) **headerCompression: notUsed (0)**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (c)Routing of USER plane data towards UPF(s)		
Requirement	Routing of User Plane data towards UPF(s);		
Test Objective	Verify that the gNB routes user plane data correctly towards the UPF(s).		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Register UE with gNodeB Start the data transfer(ping to 8.8.8.8) in UL and verify GTP-U information from gNodeB PCAP logs Verify the PDU SessionResource Setup Request for tunnel ID. Verify the packet list to check the data being transferred using the Tunnel ID.	**Tunnel establishment via PDU Session Resource Setup Request:** NG Application Protocol (PDUSessionResourceSetupRequest) NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 6 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 10 pDUSessionNAS-PDU […]: Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0xd5d22915 Sequence number: 4 Encrypted data	Check Tunnel ID in PDUSessionResourceSetup and GTP-U packets and ensure they are same.

Signaltron Confidential. Do not copy

		s-NSSAI sST: 01 sD: 000007 pDUSessionResourceSetupRequestTransfer: PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate ProtocolIE-Field id: id-PDUSessionAggregateMaximumBitRate (130) criticality: reject (0) value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1073741824bits/s pDUSessionAggregateMaximumBitRateUL: 1073741824bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) **gTP-TEID: 00044975** Item 2: id-PDUSessionType ProtocolIE-Field id: id-PDUSessionType (134) criticality: reject (0) value PDUSessionType: ipv4 (0) Item 3: id-QosFlowSetupRequestList ProtocolIE-Field id: id-QosFlowSetupRequestList (136) criticality: reject (0) value QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem	

Signaltron Confidential. Do not copy

		qosFlowIdentifier: 1 qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) nonDynamic5QI fiveQI: 9 **GPRS Tunneling Protocol** Flags: 0x34 001. .... = Version: GTP release 99 version (1) ...1 .... = Protocol type: GTP (1) .... 0... = Reserved: 0 .... .1.. = Is Next Extension Header present?: Yes .... ..0. = Is Sequence Number present?: No ....0 = Is N-PDU number present?: No Message Type: T-PDU (0xff) Length: 308 TEID: **0x00044975** (280949) Next extension header type: PDU Session container (0x85) Extension header (PDU Session container) Extension Header Length: 1 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 ....0 = Sequence Number Presence: Not Present 0... .... = N3/N9 Delay Ind: Not Present .0.. .... = New IE Flag: Not Present ..00 0001 = QoS Flow Identifier (QFI): 1 Next extension header type: No more extension headers (0x00) Internet Protocol Version 4, Src: 10.101.0.5, Dst: 8.8.8.8	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (d) Routing of Control plane information towards AMF		
Requirement	Routing of Control Plane information towards AMF;		
Test Objective	Verify that the gNB routes control plane information correctly towards the AMF.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Register UE with gNodeB Start the data transfer in UL and verify using gNodeB PCAP logs for NGAP SETUP Request and Response.	**NGAP SETUP REQUEST** Internet Protocol Version 4, Src: 192.168.10.85, Dst: 192.168.10.6 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 (1) Mobile Network Code (MNC): Unknown (01) **gNB-ID: gNB-ID (0)** **gNB-ID: 0000e000** **NGAP SETUP RESPONSE** Internet Protocol Version 4**, Src: 192.168.10.6, Dst: 192.168.10.85** NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-NGSetup (21) criticality: reject (0) value NGSetupResponse	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (e) Connection setup and release		
Requirement	Connection setup and release;		
Test Objective	Verify that the gNB correctly sets up and releases connections with the UE.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	• Run the gNodeB • Connect UE. • Call and video streaming should happen. • Put UE in airplane mode. This will disconnect the UE from gNodeB. • Remove from airplane mode. • UE context release command • UE context release complete • • gNB – put RRC connection release	**Connection release between Core and gNB for the UE.** NG Application Protocol (**UEContextReleaseComplete**) NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-UEContextRelease (41) criticality: reject (0) value UEContextReleaseComplete protocolIEs: 2 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) **criticality: ignore (1)** value AMF-UE-NGAP-ID: 21 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) **criticality: ignore (1)** value RAN-UE-NGAP-ID: 0 **RRC connection release between gNB and UE** NR Radio Resource Control (RRC) protocol DL-DCCH-Message message: c1 (0) **c1: rrcRelease (2)** rrcRelease rrc-TransactionIdentifier: 0 criticalExtensions: rrcRelease (0) rrcRelease	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (f) Scheduling and transmission of paging messages		
Requirement	Scheduling and transmission of paging messages;		
Test Objective	Verify paging message		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Register UE to gNodeB and collect UE logs and check for Paging messages	**From UE TEMS log:** ***** Layer 3 Message type: Paging (PCCH)** Device: EQ1 MessageDirection: DL MessageProtocol: NR-RRC MessageChannel: PCCH Channel CurrentRAT: Nr pagingRecordList PagingRecordList : [0] : ue-Identity PagingUE-Identity : ng-5G-S-TMSI ng-5G-S-TMSI AMF Set ID : 76 AMF Pointer : 18 5G-TMSI : 295907392 (11A33040 hex)	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential, Do not copy

Test ID	4.4.1 (g) Scheduling and transmission of broadcast information		
Requirement	Scheduling and transmission of system broadcast information (originated from the AMF or OAM);		
Test Objective	Verify MIB, SIB		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Turn on gNB and register 5G UE. Check UE or gNB PCAP logs(Apply filter nr-rrc) for MIB and SIB1 Messages	**From gNB PCAP log:** NR Radio Resource Control (RRC) protocol BCCH-BCH-Message **message: mib (0)** mib systemFrameNumber: 80 [bit length 6, 2 LSB pad bits, 1000 00.. decimal value 32] subCarrierSpacingCommon: scs30or120 (1) ssb-SubcarrierOffset: 0 dmrs-TypeA-Position: pos2 (0) pdcch-ConfigSIB1 controlResourceSetZero: 12 searchSpaceZero: 0 cellBarred: notBarred (1) intraFreqReselection: notAllowed (1) **From UE logs:** **SIB1:** ***** Layer 3 Message type: SIB1 (BCCH-DL-SCH)** Device: EQ1 MessageDirection: DL MessageProtocol: NR-RRC MessageChannel: BCCH-SCH Channel CurrentRAT: Nr RRC OTA Packet Header Version : 9 (v0.9) RRC Release Version : 15.9.0 RB ID : 0 Physical Cell ID : 0 Frequency : 641280 SFN : 30278148 PDU Number : NR5G_RRC_SIGMSGV9_BCCH_DL_SCH_Message SIB Mask In SI : 0x00000002 Msg Length : 129 Cell Info NR-ARFCN : 641280 PCI : 0	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (g) Measurement and Measurement reporting configuration for mobility and scheduling		
Requirement	gNB should configure measurement and UE should send measurement report		
Test Objective	gNB should configure measurement and UE should send measurement report		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Apply the filter in wiresharknr-rrc NRRadioResourceControl(RRC) protocol. Check for RRC reconfiguration message for gNB configuring for measurement and Measurement Report from the UE.	**From gNB PCAP log:** NR Radio Resource Control (RRC) protocol DL-DCCH-Message message: c1 (0) c1: **rrcReconfiguration (0)** rrcReconfiguration rrc-TransactionIdentifier: 2 criticalExtensions: rrcReconfiguration (0) rrcReconfiguration measConfig measObjectToAddModList: 1 item Item 0 MeasObjectToAddMod measObjectId: 1 measObject: measObjectNR (0) measObjectNR ssbFrequency: 641280 ssbSubcarrierSpacing: kHz30 (1) smtc1 periodicityAndOffset: sf20 (2) sf20: 2 duration: sf2 (1) referenceSignalConfig ssb-ConfigMobility .... ..1. deriveSSB-IndexFromCell: True absThreshSS-BlocksConsolidation thresholdRSRP: -121dBm <= SS-RSRP < -120dBm (36) nrofSS-BlocksToAverage: 8 quantityConfigIndex: 1 offsetMO freqBandIndicatorNR: 78 reportConfigToAddModList: 1 item Item 0 ReportConfigToAddMod reportConfigId: 1 reportConfig:	

Signaltron Confidential. Do not copy

		reportConfigNR (0) reportConfigNR reportType: periodical (0) periodical rsType: ssb (0) reportInterval: ms1024 (4) reportAmount: infinity (7) reportQuantityCell .1.. .... rsrp: True ..1. .... rsrq: True ...1 .... sinr: True maxReportCells: 4 reportQuantityRS-Indexes ....1 rsrp: True 1... .... rsrq: True .1.. .... sinr: True maxNrofRS- IndexesToReport: 4 ....1 includeBeamMeasurements: True 0... .... useAllowedCellList: False measIdToAddModList: 1 item Item 0 MeasIdToAddMod measId: 1 measObjectId: 1 reportConfigId: 1 quantityConfig quantityConfigNR-List: 1 item Item 0 QuantityConfigNR quantityConfigCell ssb-FilterConfig filterCoefficientRSRP: fc6 (6) csi-RS- FilterConfig filterCoefficientRSRP: fc6 (6) NR Radio Resource Control (RRC) protocol UL-DCCH-Message	

Signaltron Confidential. Do not copy

		message: c1 (0) c1: **measurementReport (0)** measurementReport criticalExtensions: measurementReport (0) measurementReport measResults measId: 1 measResultServingMOList: 1 item Item 0 MeasResultServMO servCellId: 0 measResultServingCell physCellId: 0 measResult cellResults **resultsSSB-Cell** **rsrp: -85dBm <= SS-RSRP < -84dBm (72)** **rsrq: 1.5dB <= SS-RSRQ < 2.0dB (90)** **sinr: 25.5dB <= SS-SINR < 26.0dB (98)** rsIndexResults resultsSSB-Indexes: 1 item Item 0 ResultsPerSSB-Index ssb-Index: 0 ssb-Results **rsrp: -85dBm <= SS-RSRP < -84dBm (72)** **rsrq: 1.5dB <= SS-RSRQ < 2.0dB (90)** **sinr: 25.5dB <= SS-SINR < 26.0dB (98)**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (i) Transport level Packet Marking		
Requirement	Transport level packet marking in the uplink;		
Test Objective	To Verify Transport level packet marking in the uplink.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Turn on gNB and register UE. • In wireshark capture apply filters ngap || gtp'. • Verify TEID match in the PDUSessionSetupRequest and GTP packets	**NGAP PDUSessionResourceSetupRequest:** NG Application Protocol (PDUSessionResourceSetupRequest) NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 6 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 10 pDUSessionNAS-PDU […]: s-NSSAI sST: 01 sD: 000007 pDUSessionResourceSetupRequestTransfer: PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate ProtocolIE-Field id: id-PDUSessionAggregateMaximumBitRate (130)	

Signaltron Confidential Do not copy

		criticality: reject (0) value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1073741824bits/s pDUSessionAggregateMaximumBitRateUL: 1073741824bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a07 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0111 decimal value 3232238087] TransportLayerAddress (IPv4): 192.168.10.7 **gTP-TEID: 00044975** Item 2: id-PDUSessionType ProtocolIE-Field id: id-PDUSessionType (134) criticality: reject (0) value PDUSessionType: ipv4 (0) Item 3: id-QosFlowSetupRequestList ProtocolIE-Field id: id-QosFlowSetupRequestList (136) criticality: reject (0) value QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem **qosFlowIdentifier: 1** qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0)	

Signaltron Confidential. Do not copy

		nonDynamic5QI **fiveQI: 9** allocationAndRetentionPriority priorityLevelARP: 1 pre-emptionCapability: shall-not-trigger-pre-emption (0) pre-emptionVulnerability: not-pre-emptable (0) Item 3: id-UEAggregateMaximumBitRate ProtocolIE-Field id: id-UEAggregateMaximumBitRate (110) criticality: ignore (1) value UEAggregateMaximumBitRate uEAggregateMaximumBitRateDL: 1073741824bits/s uEAggregateMaximumBitRateUL: 1073741824bits/s [Community ID: 1:t5py84GUCBEMkju42Qsqlv1OCAs=] **Data Packet** Source Address: 192.168.10.4 Destination Address: 192.168.10.7 [Stream index: 4] GPRS Tunneling Protocol Flags: 0x34 001. .... = Version: GTP release 99 version (1) ...1 .... = Protocol type: GTP (1) .... 0... = Reserved: 0 .... .1.. = Is Next Extension Header present?: Yes .... ..0. = Is Sequence Number present?: No ....0 = Is N-PDU number present?: No Message Type: T-PDU (0xff) Length: 1236 **TEID: 0x00044975 (280949)** Next extension header type: PDU Session container (0x85) Extension header (PDU Session container) Extension Header Length: 1 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 ....0 = Sequence Number Presence: Not Present 0... .... = N3/N9 Delay Ind: Not Present	

Signaltron Confidential. Do not copy

		.0.. .... = New IE Flag: Not Present ..**00 0001 = QoS Flow Identifier (QFI): 1** Next extension header type: No more extension headers (0x00) Internet Protocol Version 4, Src: 10.101.0.5, Dst: 8.8.8.8 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) **Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)** **0000 00.. = Differentiated Services Codepoint: Default (0)** .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 1228 Identification: 0xa05a (41050) 010. .... = Flags: 0x2, Don't fragment 0... .... = Reserved bit: Not set .1.. .... = Don't fragment: Set ..0. .... = More fragments: Not set ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: UDP (17) Header Checksum: 0x7b4d [validation disabled] [Header checksum status: Unverified] Source Address: 10.101.0.5 Destination Address: 8.8.8.8 [Stream index: 5] User Datagram Protocol, Src Port: 46059, Dst Port: 443 Source Port: 46059 Destination Port: 443 Length: 1208 Checksum: 0xdd7f [unverified] [Checksum Status: Unverified] [Stream index: 5] [Stream Packet Number: 1] [Timestamps] [Time since first frame: 0.000000000 seconds] [Time since previous frame: 0.000000000 seconds] UDP payload (1200 bytes) QUIC IETF QUIC Connection information [Connection Number: 0] [Packet Length: 312] 1... .... = Header Form: Long Header (1) .1.. .... = Fixed Bit: True ..00 .... = Packet Type: Initial (0) [.... 00.. = Reserved: 0] [.... ..00 = Packet Number Length: 1 bytes (0)] Version: 1 (0x00000001) Destination Connection ID Length: 16 Destination Connection ID: 50a8867574a376da2ca8e2beadb5c8fe Source Connection ID Length: 20 Source Connection ID: 8d70fdab4c7c1ddcaaee81a35d870c28eeb8a4eb	

Signaltron Confidential. Do not copy

Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (j) Session Management		
Requirement	Session Management;		
Test Objective	Verify that the gNB can manage sessions correctly.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Power on the UE and Register to 5G network. In wireshark log, filter out for NGAP messages. Verify PDUSessionSetupRequest and PDUSessionSetupResonse messages Alternatively, check for PDU Session Establishment Request and PDU Session Establishment Accept message in UE logs.	**From gNB PCAP logs:** verify for PDUSessionSetupRequest & PDUSessionSetupResponse messages NG Application Protocol **(PDUSessionResourceSetupRequest)** NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 10 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 2 pDUSessionNAS-PDU […]: Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... =	

Signaltron Confidential: Do not copy

		Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0x8bd1e774 Sequence number: 12 Encrypted data s-NSSAI sST: 01 sD: 000007 PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate ProtocolIE-Field id: id-PDUSessionAggregateMaximumBitRate (130) criticality: reject (0) value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1073741824bits/s pDUSessionAggregateMaximumBitRateUL: 1073741824bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a07 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0111 decimal value 3232238087] **TransportLayerAddress (IPv4): 192.168.10.7** **gTP-TEID: 0000e189** Item 2: id-	

Signaltron Confidential. Do not copy

		PDUSessionType ProtocolIE-Field id: id-PDUSessionType (134) criticality: reject (0) value PDUSessionType: ipv4 (0) Item 3: id-QosFlowSetupRequestList ProtocolIE-Field id: id-QosFlowSetupRequestList (136) criticality: reject (0) value QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem **qosFlowIdentifier: 1** qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) nonDynamic5QI **fiveQI: 9** allocationAndRetentionPriority priorityLevelARP: 1 pre-emptionCapability: shall-not-trigger-pre-emption (0) pre-emptionVulnerability: not-pre-emptable (0) Item 3: id-UEAggregateMaximumBitRate ProtocolIE-Field id: id-UEAggregateMaximumBitRate (110) criticality: ignore (1) value UEAggregateMaximumBitRate uEAggregateMaximumBitRateDL: 1073741824bits/s	

Signaltron Confidential. Do not copy

		uEAggregateMaximumBitRateUL: 1073741824bits/s **NG Application Protocol (PDUSessionResourceSetupResponse)** NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupResponse protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: ignore (1) value AMF-UE-NGAP-ID: 10 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: ignore (1) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSURes ProtocolIE-Field id: id-PDUSessionResourceSetupListSURes (75) criticality: ignore (1) value PDUSessionResourceSetupListSURes: 1 item Item 0 PDUSessionResourceSetupItemSURes pDUSessionID: 2 pDUSessionResourceSetupResponseTransfer: 0003e0c0a80a046d3788990001 PDUSessionResourceSetupResponseTransfer dLQosFlowPerTNLInformation uPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a04 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0100 decimal value 3232238084] **TransportLayerAddress (IPv4): 192.168.10.4** **gTP-TEID:**	

Signaltron Confidential: Do not copy

		6d378899 associatedQosFlowList: 1 item Item 0 AssociatedQosFlowItem qosFlowIdentifier: 1 **From UE logs:** following can be verified. ***** Layer 3 Message type: PDU Session Establishment Request** Device: EQ1 MessageDirection: UL MessageProtocol: 5GSM CurrentRAT: Nr Protocol Discriminator : 5GS session management messages PDU Session ID : 1 PTI : 2 Message Type : 193 Integrity Protection Maximum Data Rate Maximum data rate per UE for user-plane integrity protection for uplink : (0) 64 kbps Maximum data rate per UE for user-plane integrity protection for downlink : (0) 64 kbps PDU Session Type ***** Layer 3 Message type: PDU Session Establishment Accept** Device: EQ1 MessageDirection: DL MessageProtocol: 5GSM CurrentRAT: Nr Protocol Discriminator : 5GS session management messages PDU Session ID : 1 PTI : 2 Message Type : 194 Selected SSC mode Value : (1) SSC mode 1 Selected PDU session type Value : (1) IPv4 Session-AMBR Session-AMBR for downlink : 1 Gbps Session-AMBR for uplink : 1 Gbps **PDU Address** **Address : 10.101.0.3** S-NSSAI Slice/service type (SST) : (1) eMBB Slice differentiator (SD) : 7 (000007 hex)	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential, Do not copy

Test ID	4.4.1(k) Support of Network Slicing		
Requirement	Support of Network Slicing;		
Test Objective	Verify that the gNB supports and manages network slicing correctly.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Apply ngap filter in Wireshark log and verify the network slicing support in NGAP Setup Response. Alternatively Check the 5G UE logs to check the network slice is correctly allocated.	**From gNB PCAP log:** NG Application Protocol (NGSetupResponse) NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-NGSetup (21) criticality: reject (0) value NGSetupResponse **sliceSupportList: 1 item** **Item 0** **SliceSupportItem** **s-NSSAI** **sST: 01** **sD: 000007** **From UE log:** ***** Layer 3 Message type: PDU Session Establishment Accept** Device: EQ1 MessageDirection: DL MessageProtocol: 5GSM CurrentRAT: Nr Protocol Discriminator : 5GS session management messages PDU Session ID : 1 PTI : 2 Message Type : 194 Selected SSC mode Value : (1) SSC mode 1 Selected PDU session type Value : (1) IPv4 Session-AMBR Session-AMBR for downlink : 1 Gbps Session-AMBR for uplink : 1 Gbps PDU Address Address : 10.101.0.3 S-NSSAI **Slice/service type (SST) : (1) eMBB** **Slice differentiator (SD) : 7 (000007 hex)**	Slice information(SST,SD) allocated by AMF can be cross checked in UE log.
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (I) QoS flow management and mapping to data radio bearers		
Requirement	QoS Flow management and mapping to data radio bearers;		
Test Objective	Verify that the gNB manages QoS flows and maps them correctly to data radio bearers.		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Register UE to the gNodeB Start different type of traffic and capture wireshark. In the wireshark log, check for the following: 1) Apply ngap filter and check PDUSessionResourceSetupRequest 2) Apply the filter for nr-rrc message and check for RRC reconfiguration during Registration Accept. In the RRC Reconfiguration message check the QFI/5QI that was created during PDUSessionResourceSetupRequest is correctly assigned a Data Radio bearer.	PDU Session Resource Setup Request for Radio bearer control. gNB/Core network assigns QFI:1 for Internet default bearer with 5QI value of 9. NG Application Protocol **(PDUSessionResourceSetupRequest)** NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest s-NSSAI sST: 01 sD: 000007 criticality: reject (0) value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1073741824bits/s pDUSessionAggregateMaximumBitRateUL: 1073741824bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a07 [bit length 32, 1100 0000 1010 1000 0000	

Signaltron Confidential. Do not copy

		1010 0000 0111 decimal value 3232238087] TransportLayerAddress (IPv4): 192.168.10.7 gTP-TEID: 000477bc QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem **qosFlowIdentifier: 1** qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) nonDynamic5QI **fiveQI: 9** allocationAndRetentionPriority priorityLevelARP: 1 pre-emptionCapability: shall-not-trigger-pre-emption (0) pre-emptionVulnerability: not-pre-emptable (0) In RRC Reconfiguration message, gNB assigns the Data Radio bearer ID of 1 for QFI1. NR Radio Resource Control (RRC) protocol DL-DCCH-Message message: c1 (0) **c1: rrcReconfiguration (0)** rrcReconfiguration rrc-TransactionIdentifier: 1 criticalExtensions: rrcReconfiguration (0) rrcReconfiguration radioBearerConfig srb-ToAddModList: 2 items Item 0	

Signaltron Confidential. Do not copy

		SRB-ToAddMod srb-Identity: 1 Item 1 SRB-ToAddMod srb-Identity: 2 drb-ToAddModList: 1 item Item 0 DRB-ToAddMod cnAssociation: sdap-Config (1) sdap-Config pdu-Session: 8 sdap-HeaderDL: absent (1) sdap-HeaderUL: absent (1) 1... .... defaultDRB: True mappedQoS-FlowsToAdd: 1 item Item 0 **QFI: 1** **drb-Identity: 1**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential, Do not copy

Test ID	4.4.1 (m) Support of UEs in RRC_INACTIVE state		
Requirement	Support of UEs in RRC_INACTIVE state		
Test Objective	This test case verifies the gNB's ability to correctly manage the transition of UE to the RRC inactive state		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	In The roadmap	**In the roadmap**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.1 (n) Distribution function for NAS messages		
Requirement	Distribution function for NAS messages		
Test Objective	Verify that the gNB correctly distributes NAS messages to the appropriate network entities		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	1.gNB and AMF are powered on and operational. **2.UE is registered and within coverage of the gNB.** **3.initiate a NAS message from the UE (e.g., registration request) by powering on UE with right configuration to register with 5G Network.** **4.gNB receives the NAS message.** **5.gNB forwards the NAS message to the appropriate AMF.** **6.AMF processes the received NAS message.** **7.AMF sends a response NAS message back to the gNB.**	**In Wireshark filter ngap and then check** **InitialUEMessage, Registration request,** **DownlinkNASTransport** **UplinkNASTransport** **Authentication request** **Registration accept**	Verify 1)gNB successfully forwards the NAS message to the correct AMF. 2) AMF successfully processes the NAS message.
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

4.4.2 Network Interfaces:

4.4.3 NG User plane:

Test ID	4.4.3 (a) The NG user plane interface (NG-U) is defined between the NG-RAN node and the UPF.		
Requirement	Verify the interface between NG-RAN and UPF		
Test Objective	Verify N3 Interface		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Verify the data packets in wireshark log between NG-RAN and AMF and UPF Verify PDUSessionResourceSetup Request and PDU SessionResourceSetupResponse for GTP tunnel establishment	From gNB logs, verify for PDUSessionSetupRequest & PDUSessionSetupResponse messages NG Application Protocol **(PDUSessionResourceSetupRequest)** NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 10 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 2 pDUSessionNAS-PDU […]: Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended	GTP-U tunnel establishment can be verified.

Signaltron Confidential. Do not copy

		protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0x8bd1e774 Sequence number: 12 Encrypted data s-NSSAI sST: 01 sD: 000007 PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate ProtocolIE-Field id: id-PDUSessionAggregateMaximumBitRate (130) criticality: reject (0) value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1073741824bits/s pDUSessionAggregateMaximumBitRateUL: 1073741824bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a07 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0111 decimal value 3232238087] TransportLayerAddress (IPv4): 192.168.10.7	

Signaltron Confidential. Do not copy

		gTP-TEID: 0000e189 Item 2: id-PDUSessionType ProtocolIE-Field id: id-PDUSessionType (134) criticality: reject (0) value PDUSessionType: ipv4 (0) Item 3: id-QosFlowSetupRequestList ProtocolIE-Field id: id-QosFlowSetupRequestList (136) criticality: reject (0) value QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem qosFlowIdentifier: 1 qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) nonDynamic5QI fiveQI: 9 allocationAndRetentionPriority priorityLevelARP: 1 pre-emptionCapability: shall-not-trigger-pre-emption (0) pre-emptionVulnerability: not-pre-emptable (0) Item 3: id-UEAggregateMaximumBitRate ProtocolIE-Field id: id-UEAggregateMaximumBitRate (110) criticality: ignore (1) value UEAggregateMaximumBitRate	

Signaltron Confidential, Do not copy

uEAggregateMaximumBitRateDL: 1073741824bits/s

uEAggregateMaximumBitRateUL: 1073741824bits/s

NG Application Protocol (PDUSessionResourceSetupResponse)
NGAP-PDU: successfulOutcome (1)
successfulOutcome
procedureCode: id-PDUSessionResourceSetup (29)
criticality: reject (0)
value
PDUSessionResourceSetupResponse
protocolIEs: 3 items
Item 0: id-AMF-UE-NGAP-ID
ProtocolIE-Field
id: id-AMF-UE-NGAP-ID (10)
criticality: ignore (1)
value
AMF-UE-NGAP-ID: 10
Item 1: id-RAN-UE-NGAP-ID
ProtocolIE-Field
id: id-RAN-UE-NGAP-ID (85)
criticality: ignore (1)
value
RAN-UE-NGAP-ID: 0
Item 2: id-PDUSessionResourceSetupListSURes
ProtocolIE-Field
id: id-PDUSessionResourceSetupListSURes (75)
criticality: ignore (1)
value

PDUSessionResourceSetupListSURes: 1 item
Item 0

PDUSessionResourceSetupItemSURes
pDUSessionID: 2

pDUSessionResourceSetupResponseTransfer: 0003e0c0a80a046d3788990001

PDUSessionResourceSetupResponseTransfer

dLQosFlowPerTNLInformation

uPTransportLayerInformation: gTPTunnel (0)
gTPTunnel

transportLayerAddress: c0a80a04 [bit length 32,

Signaltron Confidential: Do not copy

		1100 0000 1010 1000 0000 1010 0000 0100 decimal value 3232238084] TransportLayerAddress (IPv4): 192.168.10.4 **gTP-TEID: 6d378899** associatedQosFlowList: 1 item Item 0 AssociatedQosFlowItem qosFlowIdentifier: 1	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	**4.4.3 (b) The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs between the NG-RAN node and the UPF.**		
Requirement	Verify the interface between NG-RAN and UPF		
Test Objective	Verify N3 Interface		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Verify the data packets in wireshark log between NG-RAN and AMF and UPF Verify PDUSessionResourceSetup Request and PDU SessionResourceSetupResponse for GTP tunnel establishment and verify packets in data path.	From gNB logs, verify for PDUSessionSetupRequest & PDUSessionSetupResponse messages NG Application Protocol **(PDUSessionResourceSetupRequest)** NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 10 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0 PDUSessionResourceSetupItemSUReq pDUSessionID: 2 pDUSessionNAS-PDU […]: Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0x8bd1e774 Sequence number:	Data packets are routed via the tunnel established by PDUSessionResourceSetupRequst and PDU SessionResourceSetupResponse

Signaltron Confidential. Do not copy

		12 Encrypted data s-NSSAI sST: 01 sD: 000007 PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate ProtocolIE-Field id: id-PDUSessionAggregateMaximumBitRate (130) criticality: reject (0) value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1073741824bits/s pDUSessionAggregateMaximumBitRateUL: 1073741824bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a07 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0111 decimal value 3232238087] **TransportLayerAddress (IPv4): 192.168.10.7** **gTP-TEID: 0000e189** Item 2: id-PDUSessionType ProtocolIE-Field id: id-PDUSessionType (134) criticality: reject (0) value PDUSessionType: ipv4 (0) Item 3: id-QosFlowSetupRequestList ProtocolIE-Field id: id-QosFlowSetupRequestList (136) criticality: reject (0)	

Signaltron Confidential: Do not copy

		value QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem qosFlowIdentifier: 1 qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) nonDynamic5QI fiveQI: 9 allocationAndRetentionPriority priorityLevelARP: 1 pre-emptionCapability: shall-not-trigger-pre-emption (0) pre-emptionVulnerability: not-pre-emptable (0) Item 3: id-UEAggregateMaximumBitRate ProtocolIE-Field id: id-UEAggregateMaximumBitRate (110) criticality: ignore (1) value UEAggregateMaximumBitRate uEAggregateMaximumBitRateDL: 1073741824bits/s uEAggregateMaximumBitRateUL: 1073741824bits/s **NG Application Protocol (PDUSessionResourceSetupResponse)** NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupResponse protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: ignore (1) value AMF-UE-NGAP-ID: 10 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: ignore (1) value	

Signaltron Confidential Do not copy

		RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSURes ProtocolIE-Field id: id-PDUSessionResourceSetupListSURes (75) criticality: ignore (1) value PDUSessionResourceSetupListSURes: 1 item Item 0 PDUSessionResourceSetupItemSURes pDUSessionID: 2 pDUSessionResourceSetupResponseTransfer: 0003e0c0a80a046d3788990001 PDUSessionResourceSetupResponseTransfer dLQosFlowPerTNLInformation uPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a04 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0100 decimal value 3232238084] **TransportLayerAddress (IPv4): 192.168.10.4** **gTP-TEID: 6d378899** associatedQosFlowList: 1 item Item 0 AssociatedQosFlowItem qosFlowIdentifier: 1 **Data Packet** Source Address: 192.168.10.4 Destination Address: 192.168.10.7 [Stream index: 4] **GPRS Tunneling Protocol** Flags: 0x34 001. .... = Version: GTP release 99 version (1) ...1 .... = Protocol type: GTP (1) .... 0... = Reserved: 0 .... .1.. = Is Next Extension Header present?: Yes .... ..0. = Is Sequence Number present?: No ....0 = Is N-PDU number present?: No Message Type: T-PDU (0xff) Length: 1236 **TEID: 0x00044975 (280949)** Next extension header type: PDU Session container (0x85) Extension header (PDU Session container) Extension Header Length: 1	

Signaltron Confidential Do not copy

		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 ....0 = Sequence Number Presence: Not Present 0... .... = N3/N9 Delay Ind: Not Present .0.. .... = New IE Flag: Not Present **..00 0001 = QoS Flow Identifier (QFI): 1** Next extension header type: No more extension headers (0x00) Internet Protocol Version 4, Src: 10.101.0.5, Dst: 8.8.8.8 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) **Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)** **0000 00.. = Differentiated Services Codepoint: Default (0)** .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 1228 Identification: 0xa05a (41050) 010. .... = Flags: 0x2, Don't fragment 0... .... = Reserved bit: Not set .1.. .... = Don't fragment: Set ..0. .... = More fragments: Not set ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: UDP (17) Header Checksum: 0x7b4d [validation disabled] [Header checksum status: Unverified] Source Address: 10.101.0.5 Destination Address: 8.8.8.8 [Stream index: 5] **User Datagram Protocol, Src Port: 46059, Dst Port: 443** Source Port: 46059 Destination Port: 443 Length: 1208 Checksum: 0xdd7f [unverified] [Checksum Status: Unverified] [Stream index: 5] [Stream Packet Number: 1] [Timestamps] [Time since first frame: 0.000000000 seconds] [Time since previous frame: 0.000000000 seconds] UDP payload (1200 bytes) QUIC IETF QUIC Connection information [Connection Number: 0] [Packet Length: 312] 1... .... = Header Form: Long Header (1) .1.. .... = Fixed Bit: True ..00 .... = Packet Type: Initial (0) [.... 00.. = Reserved: 0] [.... ..00 = Packet Number Length: 1 bytes (0)]	

Signaltron Confidential. Do not copy

		Version: 1 (0x00000001) Destination Connection ID Length: 16 Destination Connection ID: 50a8867574a376da2ca8e2beadb5c8fe Source Connection ID Length: 20 Source Connection ID: 8d70fdab4c7c1ddcaaee81a35d870c28eeb8a4eb	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.4.3 (c) NG-U provides non-guaranteed delivery of user plane PDUs between the NG-RAN node and the UPF.		
Requirement	Verify established PDU non-guaranteed		
Test Object iv e	Verify N3 Interlace		
	Test Steps	**Acceptance Criteria**	**Remark**
	Register UE to 5G and do a data session. In the wireshark log, filter out ngap and udp. Check for 5QI value. Value of 9 indicates non guaranteed bit rate. For GTP-U session, check the underlying protocol in the Wireshark packets. GTP-U packets over UDP indicates non-guaranteed delivery.	NG Application Protocol **(PDUSessionResourceSetupRequest)** NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupRequest protocolIEs: 4 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 10 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSUReq ProtocolIE-Field id: id-PDUSessionResourceSetupListSUReq (74) criticality: reject (0) value PDUSessionResourceSetupListSUReq: 1 item Item 0	It is verified N3 Interlace b/w RAN and UPF

Signaltron Confidential. Do not copy

		PDUSessionResourceSetupItemSUReq pDUSessionID: 2 pDUSessionNAS-PDU […]: Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0x8bd1e774 Sequence number: 12 Encrypted data s-NSSAI sST: 01 sD: 000007 PDUSessionResourceSetupRequestTransfer protocolIEs: 4 items Item 0: id-PDUSessionAggregateMaximumBitRate ProtocolIE-Field id: id-PDUSessionAggregateMaximumBitRate (130) criticality: reject (0) value PDUSessionAggregateMaximumBitRate pDUSessionAggregateMaximumBitRateDL: 1073741824bits/s pDUSessionAggregateMaximumBi	

Signaltron Confidential. Do not copy

		tRateUL: 1073741824bits/s Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a07 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0111 decimal value 3232238087] TransportLayerAddress (IPv4): 192.168.10.7 **gTP-TEID: 0000e189** Item 2: id-PDUSessionType ProtocolIE-Field id: id-PDUSessionType (134) criticality: reject (0) value PDUSessionType: ipv4 (0) Item 3: id-QosFlowSetupRequestList ProtocolIE-Field id: id-QosFlowSetupRequestList (136) criticality: reject (0) value QosFlowSetupRequestList: 1 item Item 0 QosFlowSetupRequestItem qosFlowIdentifier: 1	

Signaltron Confidential. Do not copy

		qosFlowLevelQosParameters qosCharacteristics: nonDynamic5QI (0) **nonDynamic5QI** **fiveQI: 9** allocationAndRetentionPriority priorityLevelARP: 1 pre-emptionCapability: shall-not-trigger-pre-emption (0) pre-emptionVulnerability: not-pre-emptable (0) Item 3: id-UEAggregateMaximumBitRate ProtocolIE-Field id: id-UEAggregateMaximumBitRate (110) criticality: ignore (1) value UEAggregateMaximumBitRate uEAggregateMaximumBitRateDL: 1073741824bits/s uEAggregateMaximumBitRateUL: 1073741824bits/s **NG Application Protocol (PDUSessionResourceSetupResponse)** NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value PDUSessionResourceSetupResponse protocolIEs: 3 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: ignore (1)	

Signaltron Confidential. Do not copy

		value AMF-UE-NGAP-ID: 10 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: ignore (1) value RAN-UE-NGAP-ID: 0 Item 2: id-PDUSessionResourceSetupListSURes ProtocolIE-Field id: id-PDUSessionResourceSetupListSURes (75) criticality: ignore (1) value PDUSessionResourceSetupListSURes: 1 item Item 0 PDUSessionResourceSetupItemSURes pDUSessionID: 2 pDUSessionResourceSetupResponseTransfer: 0003e0c0a80a046d3788990001 PDUSessionResourceSetupResponseTransfer dLQosFlowPerTNLInformation uPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a04 [bit length 32, 1100 0000 1010 1000 0000 1010 0000 0100 decimal value 3232238084] **TransportLayerAddress (IPv4): 192.168.10.4** **gTP-TEID: 6d378899** associatedQosFlowList: 1 item Item 0	

Signaltron Confidential. Do not copy

		AssociatedQosFlowItem qosFlowIdentifier: 1 **Data Packet** Source Address: 192.168.10.4 Destination Address: 192.168.10.7 [Stream index: 4] **GPRS Tunneling Protocol** Flags: 0x34 001. .... = Version: GTP release 99 version (1) ...1 .... = Protocol type: GTP (1) .... 0... = Reserved: 0 .... .1.. = Is Next Extension Header present?: Yes .... ..0. = Is Sequence Number present?: No ....0 = Is N-PDU number present?: No Message Type: T-PDU (0xff) Length: 1236 **TEID: 0x00044975 (280949)** Next extension header type: PDU Session container (0x85) Extension header (PDU Session container) Extension Header Length: 1 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 ....0 = Sequence Number Presence: Not Present 0... .... = N3/N9 Delay Ind: Not Present .0.. .... = New IE Flag: Not Present **..00 0001 = QoS Flow Identifier (QFI): 1** Next extension header type: No more extension headers (0x00) Internet Protocol Version 4, Src: 10.101.0.5, Dst: 8.8.8.8 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) **Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)** **0000 00.. = Differentiated Services Codepoint: Default (0)**	

Signaltron Confidential: Do not copy

		.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 1228 Identification: 0xa05a (41050) 010. .... = Flags: 0x2, Don't fragment 0... .... = Reserved bit: Not set .1.. .... = Don't fragment: Set ..0. .... = More fragments: Not set ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 64 **Protocol: UDP (17)** Header Checksum: 0x7b4d [validation disabled] [Header checksum status: Unverified] Source Address: 10.101.0.5 Destination Address: 8.8.8.8 [Stream index: 5] **User Datagram Protocol, Src Port: 46059, Dst Port: 443** Source Port: 46059 Destination Port: 443 Length: 1208 Checksum: 0xdd7f [unverified] [Checksum Status: Unverified] [Stream index: 5] [Stream Packet Number: 1] [Timestamps] [Time since first frame: 0.000000000 seconds] [Time since previous frame: 0.000000000 seconds] UDP payload (1200 bytes) QUIC IETF QUIC Connection information [Connection Number: 0] [Packet Length: 312] 1... .... = Header Form: Long Header (1) .1.. .... = Fixed Bit: True ..00 .... = Packet Type: Initial (0) [.... 00.. = Reserved: 0] [.... ..00 = Packet Number Length: 1 bytes (0)] Version: 1 (0x00000001) Destination Connection ID Length: 16 Destination Connection ID: 50a8867574a376da2ca8e2beadb5c8fe Source Connection ID Length: 20 Source Connection ID: 8d70fdab4c7c1ddcaaee81a35d870c28eeb8a4eb	

Signaltron Confidential. Do not copy

Overall Test Result	Pass:□	Fail:□

Signaltron Confidential. Do not copy

Test ID	4.4.3 (d):NG-U compliance as per 3GPP standards		
Requirement	Verify the NG-U compliance as per 3GPP standards		
Test Objective	To Verify NG-U compliance as per 3GPP standards		
	Test Steps	Acceptance Criteria	Remarks
	1. gNB and AMF are powered on and operational. 2. UE is registered and attached to the gNB. After UE is registered, run a data session on the UE	Internet Protocol Version 4, **Src: 192.168.10.85, Dst: 192.168.10.7** **GPRS Tunneling Protocol** Message Type: T-PDU (0xff) Extension header Extension Header Length: 1 PDU Session Container 0001 .... = PDU Type: UL PDU SESSION INFORMATION (1) .... 0000 = Spare: 0x0 00.. .... = Spare: 0x0 ..00 0001 = **QoS Flow Identifier (QFI): 1** Internet Protocol Version 4, Src: 192.168.10.7, Dst: 192.168.10.85 GPRS Tunneling Protocol Message Type: T-PDU (0xff) Extension Header Length: 1 PDU Session Container 0000 .... = PDU Type: DL PDU SESSION INFORMATION (0) .... 0000 = Spare: 0x0 0... .... = Paging Policy Presence (PPP): Not Present .0.. .... = Reflective QoS Indicator (RQI): Not Present **..00 0001 = QoS Flow Identifier (QFI): 1** Refer to **4.4.2 (a) for more details.**	All the user data between RAN & UPF flow through gtp packets with - PDU Session container.
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

4.4.4 NG Control Plane:-

Test ID	4..4.4 (a) NG-C provides the following functions: (b) NG interface management		
Require ment	NG interface management		
Test Objective	Verify that the gNB manages the NG interface correctly.		
Test Description	Test Steps	Acceptance Criteria	Remarks
	Routing of control plane data towards AMF. Filter out ngap messages. Check Wireshark logs to verify following messages NGSetupRequest and NGSetupResponse	**NGAP SETUP REQUEST** **Internet Protocol Version 4, Src: 192.168.10.85, Dst: 192.168.10.6** 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 (1) Mobile Network Code (MNC): Unknown (01) gNB-ID: gNB-ID (0) gNB-ID: 0000e000 **NGAP SETUP RESPONSE** **Internet Protocol Version 4, Src: 192.168.10.6, Dst: 192.168.10.85** NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-NGSetup (21) criticality: reject (0) value NGSetupResponse	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	4..4.4 (c) UE context management	
Requirement	UE context management	
Test Objective	Verify that the gNB correctly manages the UE context throughout its lifecycle.	

Test Steps	Acceptance Criteria	Remarks
Power on UE and attach to 5G Network. From gNB PCAP log, filter out ngap messages and verify the following: InitialContextSetupRequest and InitialContextSetupResponse	NG Application Protocol (**InitialContextSetupRequest**) NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-InitialContextSetup (14) criticality: reject (0) value InitialContextSetupRequest protocolIEs: 8 items Item 0: id-AMF-UE-NGAP-ID ProtocolIE-Field id: id-AMF-UE-NGAP-ID (10) criticality: reject (0) value AMF-UE-NGAP-ID: 21 Item 1: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 2: id-GUAMI ProtocolIE-Field id: id-GUAMI (28) criticality: reject (0) value **GUAMI** **pLMNIdentity: 00f110** **Mobile Country Code (MCC): Unknown (001)** **Mobile Network Code (MNC):**	

Signaltron Confidential. Do not copy

		Unknown (01) **aMFRegionID: 02 [bit length 8, 0000 0010 decimal value 2]** **aMFSetID: 0040 [bit length 10, 6 LSB pad bits, 0000 0000 01.. .... decimal value 1]** **aMFPointer: 00 [bit length 6, 2** LSB pad bits, 0000 00.. decimal value 0] Item 3: id-AllowedNSSAI ProtocolIE-Field id: id-AllowedNSSAI (0) criticality: reject (0) value AllowedNSSAI: 1 item Item 0 **AllowedNSSAI-Item** **s-NSSAI** **sST: 01** **sD: 000007** Item 4: id-UESecurityCapabilities ProtocolIE-Field id: id-UESecurityCapabilities (119) criticality: reject (0) value UESecurityCapabilities nRencryptionAlgorithms: e000 [bit length 16, 1110 0000 0000 0000 decimal value 57344] 1... .... = 128-NEA1: Supported .1.. .... = 128-NEA2: Supported ..1. .... = 128-NEA3: Supported ...0 0000 0000 0000 = Reserved: 0x0000 nRintegrityProtectionAlgorithms: e000 [bit length 16, 1110 0000 0000 0000 decimal value 57344] 1... .... = 128-NIA1: Supported .1.. .... = 128-NIA2:

Signaltron Confidential. Do not copy

		Supported ..1. .... = 128-NIA3: Supported ...0 0000 0000 0000 = Reserved: 0x0000 eUTRAencryptionAlgorithms: 0000 [bit length 16, 0000 0000 0000 0000 decimal value 0] 0... .... = 128-EEA1: Not supported .0.. .... = 128-EEA2: Not supported ..0. .... = 128-EEA3: Not supported ...0 0000 0000 0000 = Reserved: 0x0000 eUTRAintegrityProtectionAlgorithms: 0000 [bit length 16, 0000 0000 0000 0000 decimal value 0] 0... .... = 128-EIA1: Not supported .0.. .... = 128-EIA2: Not supported ..0. .... = 128-EIA3: Not supported .... ..0. .... = EIA7: Not supported ...0 00.0 0000 0000 = Reserved: 0x0000 Item 5: id-SecurityKey ProtocolIE-Field id: id-SecurityKey (94) criticality: reject (0) value SecurityKey: c9222ca62b037cdd48bac9660be48bb8664d7c98623181 49a51d69b5f5e99590 [bit length 256] Item 6: id-MaskedIMEISV ProtocolIE-Field id: id-MaskedIMEISV (34)

Signaltron Confidential. Do not copy

		criticality: ignore (1) value MaskedIMEISV: 3570038020ffff01 [bit length 64, 0011 0101 0111 0000 0000 0011 1000 0000 0010 0000 1111 1111 1111 1111 0000 0001 decimal value 3850581530246119169] Item 7: id-NAS-PDU ProtocolIE-Field id: id-NAS-PDU (38) criticality: ignore (1) value NAS-PDU: 7e02b22b168f417e0042010177000bf200f110020040c000256d54074000f1100000011505040100000721020100 5e01a9 Non-Access-Stratum 5GS (NAS)PDU Security protected NAS 5GS message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0010 = Security header type: Integrity protected and ciphered (2) Message authentication code: 0xb22b168f Sequence number: 65
Overall Test Result	Pass	Fail

Signaltron Confidential. Do not copy

Test ID	4..4.4 (c) UE Mobility Management	
Requirement	UE Mobility Management	
Test Objective	Check DL/UL NAS message transfer while UE registration	

	Test Steps	Acceptance Criteria	Remarks
	Power on UE and attach to 5G Network. From gNB PCAP log, filter out ngap messages and verify the following: InitialUEMessage	Payload protocol identifier: NGAP (60) Chunk padding: 00 NG Application Protocol **(InitialUEMessage)** NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-InitialUEMessage (15) criticality: ignore (1) value InitialUEMessage protocolIEs: 5 items Item 0: id-RAN-UE-NGAP-ID ProtocolIE-Field id: id-RAN-UE-NGAP-ID (85) criticality: reject (0) value RAN-UE-NGAP-ID: 0 Item 1: id-NAS-PDU ProtocolIE-Field id: id-NAS-PDU (38) criticality: reject (0) value NAS-PDU: Non-Access-Stratum 5GS (NAS)PDU 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)	

Signaltron Confidential. Do not copy

		Message authentication code: 0x674dfb55 Sequence number: 73 Plain NAS 5GS Message Extended protocol discriminator: 5G mobility management messages (126) 0000 .... = Spare Half Octet: 0 .... 0000 = Security header type: Plain NAS message, not security protected (0) Message type: Registration request (0x41) 5GS registration type .... 1... = Follow-On Request bit (FOR): Follow-on request pending .... .001 = 5GS registration type: initial registration (1) NAS key set identifier 0... .... = Type of security context flag (TSC): Native security context (for KSIAMF) .101 .... = NAS key set identifier: 5 5GS mobile identity Length: 11 1... .... = Spare: 1 .1.. .... = Spare: 1 ..1. .... = Spare: 1 ...1 .... = Spare: 1 .... 0... = Spare: 0 .... .010 = Type of identity: 5G-GUTI (2) Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) AMF Region ID: 2 0000 0000 01.. .... = AMF Set ID: 1 ..00 0000 = AMF Pointer: 0 5G-TMSI: 3221230491 (0xc000139b)

Signaltron Confidential. Do not copy

		UE security capability Element ID: 0x2e Length: 2 1... .... = 5G-EA0: Supported .1.. .... = 128-5G-EA1: Supported ..1. .... = 128-5G-EA2: Supported ...1 .... = 128-5G-EA3: Supported .... 0... = 5G-EA4: Not supported .... .0.. = 5G-EA5: Not supported .... ..0. = 5G-EA6: Not supported ....0 = 5G-EA7: Not supported 1... .... = 5G-IA0: Supported .1.. .... = 128-5G-IA1: Supported ..1. .... = 128-5G-IA2: Supported ...1 .... = 128-5G-IA3: Supported .... 0... = 5G-IA4: Not supported .... .0.. = 5G-IA5: Not supported .... ..0. = 5G-IA6: Not supported ....0 = 5G-IA7: Not supported NAS message container Element ID: 0x71 Length: 53 Encrypted data Item 2: id-UserLocationInformation ProtocolIE-Field id: id-UserLocationInformation (121)

Signaltron Confidential. Do not copy

		criticality: reject (0) value UserLocationInformation: userLocationInformationNR (1) userLocationInformationNR nR-CGI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) 0000 0000 0000 0000 1110 0000 0000 0000 0000 .... = nRCellIdentity: 0x0000e0000 tAI pLMNIdentity: 00f110 Mobile Country Code (MCC): Unknown (001) Mobile Network Code (MNC): Unknown (01) tAC: 1 (0x000001) Item 3: id-RRCEstablishmentCause ProtocolIE-Field id: id-RRCEstablishmentCause (90) criticality: ignore (1) value RRCEstablishmentCause: mo-Signalling (3) Item 4: id-UEContextRequest ProtocolIE-Field id: id-UEContextRequest (112) criticality: ignore (1) value UEContextRequest: requested (0)
Overall Test Result	Pass	Fail

Signaltron Confidential. Do not copy

Test ID	4..4.4 (e) Transport of NAS messages		
Requirement	Transport of NAS messages;		
Test Objective	Verify that the gNB correctly transports NAS messages between the UE and the core network.		
	Test Steps	Acceptance Criteria	Remarks
	• gNB and AMF are powered on and operational • Power on the UE and ensure it is registered • Filter out gNB PCAP packets with ngap filter and check for UplinkNASTransport and DownlinkNAS Transport messages	Internet Protocol Version 4, Src: 192.168.10.85, Dst: 192.168.10.6 NG Application Protocol NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-**UplinkNASTransport (46)** criticality: ignore (1) value: UplinkNASTransport Internet Protocol Version 4, Src: 192.168.10.6, Dst: 192.168.10.85 NG Application Protocol NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-DownlinkNASTransport (4) criticality: ignore (1) **value: DownlinkNASTransport** Refer to 4.4.4.(f) for more details.	gNB successfully receives and forwards the NAS message from the UE to the AMF.
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Requirement	4.4.4 (f)Paging		
Test Objective	Scheduling and transmission of paging messages;		
	Test Steps	Acceptance Criteria	Remarks
	Register UE to gNodeB and collect UE logs and check for Paging messages	**From UE Logs:** ***** Layer 3 Message type: Paging (PCCH)** Device: EQ1 MessageDirection: DL MessageProtocol: NR-RRC MessageChannel: PCCH Channel CurrentRAT: Nr pagingRecordList PagingRecordList : [0] : ue-Identity PagingUE-Identity : ng-5G-S-TMSI ng-5G-S-TMSI AMF Set ID : 76 AMF Pointer : 18 5G-TMSI : 295907392 (11A33040 hex)	gNB Pages the UE with its S-TMSI.
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Requirement	4.4.4 (g)PDU Session Management;	
Test Objective	Verify that the gNB correctly manages PDU sessions.	
	Test Steps	Acceptance Criteria	Remarks
	gNB and AMF are powered on and operational Power on the UE and ensure it is registered The UE is expected to automatically initiate PDU session establishment procedure. After its completion, initiate any data session	In Wireshark logs check for following messages PDUSessionResourceSetupRequest Internet Protocol Version 4, Src: 192.168.10.6, Dst: 192.168.10.85 NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-**PDUSessionResourceSetup** (29) criticality: reject (0) value PDUSessionResourceSetupRequest Item 1: id-UL-NGU-UP-TNLInformation ProtocolIE-Field id: id-UL-NGU-UP-TNLInformation (139) criticality: reject (0) value UPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a07 TransportLayerAddress (IPv4): 192.168.10.7 gTP-TEID: 00034594 PDUSessionResourceSetupResponse Internet Protocol Version 4, Src: 192.168.10.85, Dst: 192.168.10.6 NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-PDUSessionResourceSetup (29) criticality: reject (0) value **PDUSessionResourceSetupResponse** uPTransportLayerInformation: gTPTunnel (0) gTPTunnel transportLayerAddress: c0a80a55 TransportLayerAddress (IPv4): 192.168.10.85 gTP-TEID: 75bbc40b	gNB successfully receives and forwards the PDU message between the UE and the SMF.
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential: Do not copy

Test ID	4.4.4.(h) Configuration transfer		
Require ment	Verify Configuration transfer message		
Test Objective			
	Test Steps	Acceptance Criteria	Remarks

Signaltron Confidential. Do not copy

Test ID	4.4.4.(j) NG-C compliance as per 3GPP standards		
Requirement	Verify the NG-C compliance as per 3GPP.		
Test Objective	To Verify the NG-C compliance and to validate Ngap messages as per 3gpp standards.		
	Test Steps	Acceptance Criteria	Remarks
	• gNB and AMF are powered on and operational Power on the UE and ensure it is registered Verify following messages with wireshark logs by filtering out ngap logs.	Internet Protocol Version 4, Src: 192.168.10.85, Dst: 192.168.10.6 NG Application Protocol NGAP-PDU: initiatingMessage (0) initiatingMessage procedureCode: id-NGSetup (21) **Value NGSetupRequest** Internet Protocol Version 4, Src: 192.168.10.6, Dst: 192.168.10.85 NG Application Protocol NGAP-PDU: successfulOutcome (1) successfulOutcome procedureCode: id-NGSetup (21) **Value NGSetupResponse** Similarlly Following messages can be verified in wireshark **UplinkNASTransport** **DownlinkNASTransport** **InitialUEMessage** **UERadioCapabilityInfoIndication** **InitialContextSetupRequest** **InitialContextSetupResponse** **PDUSessionResourceSetupRequest** **PDUSessionResourceSetupResponse** **UEContextReleaseCommand** **UEContextReleaseComplete**	Observe all the mandatory message's that are specified in 3gPP for UE attach & detach process and observe the following IE's inside it
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

4.4.7 Radio Protocol Architecture:

Signaltron Confidential. Do not copy

Test ID	**4.4.7.a Protocol stack for the userplane,i.e. SDAP, PDCP, RLC and MAC sublayers (terminated in gNB on the networkside)should perform the functions as per 3GPP Release15.**	
Requirement	All 5G Radio protocols should be supported while establishing a connection and data transfer to/from UE	
Test Objective		
Test Description	Test Steps	Acceptance Criteria / Remarks
	Power the gNB and other systems. Power on the 5G UE and ensure that it succesfully registers with 5G gNB/Core Apply the filter for nr-rrc in the PCAP log and check the RRC Reconfiguration message that reconfigures SDAP, PDCP,RLC and MAC	NR Radio Resource Control (RRC) protocol DL-DCCH-Message message: c1 (0) c1: rrcReconfiguration (0) rrcReconfiguration rrc-TransactionIdentifier: 1 criticalExtensions: rrcReconfiguration (0) rrcReconfiguration radioBearerConfig srb-ToAddModList: 2 items Item 0 SRB-ToAddMod srb-Identity: 1 Item 1 SRB-ToAddMod srb-Identity: 2 drb-ToAddModList: 1 item Item 0 DRB-ToAddMod cnAssociation: sdap-Config (1) **sdap-Config** pdu-Session: 11 sdap-HeaderDL: absent (1) sdap-HeaderUL: absent (1) 1... .... defaultDRB: True mappedQoS-FlowsToAdd: 1 item Item 0 QFI: 1 drb-Identity: 1 **pdcp-Config** drb discardTimer: infinity (15) pdcp-SN-SizeUL: len18bits (1) pdcp-SN-SizeDL: len18bits (1) headerCompression: notUsed (0) notUsed: NULL t-Reordering: ms100 (14) CellGroupConfig cellGroupId: 0

Signaltron Confidential: Do not copy

rlc-
BearerToAddModList: 3 items
Item 0
RLC-BearerConfig

logicalChannelIdentity: 1

servedRadioBearer: srb-Identity (0)
srb-Identity: 1
rlc-Config: am (0)
am
ul-AM-RLC
sn-
FieldLength: size12 (0)
t-
PollRetransmit: ms45 (8)
pollPDU:
infinity (23)
pollByte:
infinity (43)

maxRetxThreshold: t8 (5)
dl-AM-RLC
sn-
FieldLength: size12 (0)
t-
Reassembly: ms35 (7)
t-
StatusProhibit: ms0 (0)
mac-
LogicalChannelConfig
ul-
SpecificParameters
priority: 1

prioritisedBitRate: infinity (15)

bucketSizeDuration: ms1000 (8)

logicalChannelGroup: 0

schedulingRequestID: 0
.... .0..
logicalChannelSR-Mask: False
.... ..0.
logicalChannelSR-DelayTimerApplied: False
Item 1
RLC-BearerConfig

logicalChannelIdentity: 2

servedRadioBearer: srb-Identity (0)
srb-Identity: 2
rlc-Config: am (0)
am
ul-AM-RLC
sn-
FieldLength: size12 (0)
t-
PollRetransmit: ms45 (8)
pollPDU:
infinity (23)
pollByte:

Signaltron Confidential. Do not copy

infinity (43)

maxRetxThreshold: t8 (5)

dl-AM-RLC

sn-

FieldLength: size12 (0)

t-

Reassembly: ms35 (7)

t-

StatusProhibit: ms0 (0)

mac-

LogicalChannelConfig

ul-

SpecificParameters

priority: 2

prioritisedBitRate: infinity (15)

bucketSizeDuration: ms5 (0)

logicalChannelGroup: 0

schedulingRequestID: 0

.... .0..

logicalChannelSR-Mask: False

.... ..0.

logicalChannelSR-DelayTimerApplied: False

Item 2

RLC-BearerConfig

logicalChannelIdentity: 4

servedRadioBearer: drb-Identity (1)

drb-Identity: 1

rlc-Config: am (0)

am

ul-AM-RLC

sn-

FieldLength: size18 (1)

t-

PollRetransmit: ms45 (8)

pollPDU:

p64 (4)

pollByte:

kB500 (13)

maxRetxThreshold: t32 (7)

dl-AM-RLC

sn-

FieldLength: size18 (1)

t-

Reassembly: ms15 (3)

t-

StatusProhibit: ms15 (3)

mac-

LogicalChannelConfig

ul-

SpecificParameters

priority: 13

prioritisedBitRate: kBps8 (1)

bucketSizeDuration: ms100 (4)

Signaltron Confidential. Do not copy

		logicalChannelGroup: 1 schedulingRequestID: 0 0... .... logicalChannelSR-Mask: False .0.. .... logicalChannelSR-DelayTimerApplied: False	

Signaltron Confidential. Do not copy

Test ID	4.4.7.(b) 3GPP Release 15 Support		
Requirement	The protocol stack for the control plane should perform the function as detailed in 3GPP Release 15		
Test Objective	The protocol stack for the control plane should perform the function as detailed in 3GPPRelease 15		
	Test Steps	Acceptance Criteria	Remarks
	As updated in 4.4.7.a		
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not co

<table>
<tr><td>Test ID</td><td colspan="3">4.4.7.(c)</td></tr>
<tr><td>Requirement</td><td colspan="3">PDCP,RLC and MAC sublayers(terminated in gNB on the network side should perform the functions listed in 3GPP Standards.</td></tr>
<tr><td>Test Objective</td><td colspan="3">All 5G Radio protocols should be supported while establishing a connection and data transfer to/from UE</td></tr>
<tr><td></td><td>Test Steps</td><td>Acceptance Criteria</td><td>Remarks</td></tr>
<tr><td></td><td>Same as 4.4.7(a)</td><td></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass:□</td><td colspan="2">Fail:□</td></tr>
</table>

Signaltron Confidential. Do not copy

Test ID	4.4.7 (C) RLC procedures: Modes of Data transmission		
Requirement	Modes of Data transmission		
Test Objective	Verify that gNB supports RLC data transmission modes AM and UM (for DRBs)		
	Test Steps	Acceptance Criteria	Remarks

Signaltron Confidential. Do not copy

Description	Power the gNB and other systems. Power on the 5G UE and ensure that it succesfully registers with 5G gNB/Core Check the Wireshark logs.	RLC-NR UEId=10 [UL] [AM] SRB:1 [DATA] (P) SN=29 [9-bytes.. [Context] **[Direction: Uplink (0)]** **[RLC Mode: Acknowledged Mode (4)]** [UEId: 10] [Bearer Type: SRB (4)] [Bearer Id: 1] [PDU Length: 11] [Sequence Number length: 12] AM Header (P) SN=29 1... .... = Data/Control: Data PDU .1.. .... = Polling Bit: Status report is requested ..01 .... = Segmentation Info: Data field contains the first segment of an RLC SDU (0x1) .... 0000 0001 1101 = Sequence Number: 29 AM Data: 001d3a0c3f017db81c Subheader: (Short BSR LCG ID=0 BS=0) 00.. .... = Reserved: 0x00 ..11 1101 = LCID: Short BSR (0x3d) 000. .... = LCG: 0 ...0 0000 = Buffer Size for LCG0: BS = 0 (0) Subheader: (PHR PH=57 PCMAX_f_c=50) 00.. .... = Reserved: 0x00 ..11 1001 = LCID: Single Entry PHR (0x39) 00.. .... = Reserved: 0x0 ..11 1001 = Power Headroom: 26 dB <= PH < 28 dB (57) 00.. .... = Reserved: 0x0 ..11 0010 = Pcmax,c,f: 20 dBm <= Pcmax,f,c < 21 dBm (50) Subheader: (Padding 13 bytes) 00.. .... = Reserved: 0x00 ..11 1111 = LCID: Padding (0x3f) Padding: f86549c34749203b6f4044dc62	1.
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential Do not copy

Test ID	4.4.7 (C) RLC procedures: Segmentation and Reassembly		
Requirement	Segmentation and Reassembly		
Test Objective	Verify that gNB RLC supports Segmentation & Reassembly of SDUs in modes AM and UM		
	Test Steps	Acceptance Criteria	Remarks

Signaltron Confidential. Do not cop

Description	Power the gNB and other systems. Power on the 5G UE and ensure that it succesfully registers with 5G gNB/Core Run Iperf Command In gNodeB: iperf –s –i 1 –p 10001 –l 1400 –B “gNodeB_IP” In UE: Iperf –c “gNodeB_IP” –u –i 1 –t 1000 –p 10001 –l 1400 –b 50M –B “UE_IP” Check Wireshark logs for Segmentation info	No. Time Source Destination Protocol Length Info 4597 52.563027422 10.101.0.5 10.101.0.1 RLC-NR 5572 UEId=1 [UL] [AM] DRB:1 [DATA] SN=92 SO=1190 ..209-bytes] || UEId=1 [UL] [AM] DRB:1 [DATA] SN=93 [1399-bytes] || UEId=1 [UL] [AM] DRB:1 [DATA] SN=94 [1399-bytes] || UEId=1 [UL] [AM] DRB:1 [DATA] SN=95 [1151-bytes] || UEId=1 [UL] [AM] DRB:1 [DATA] SN=96 [1311-bytes.. (Short BSR LCG ID=1 BS=30) (PHR PH=43 PCMAX_f_c=47 **MAC-NR UL-SCH (LCID:4 214 bytes) || (LCID:4 1402 bytes) || (LCID:4 1402 bytes) || (LCID:4 1154 bytes) || (LCID:4 1314 bytes)** (Short BSR LCG ID=1 BS=30) (PHR PH=43 PCMAX_f_c=47) [Context (RNTI=24677)] [Radio Type: TDD (2)] [Direction: Uplink (0)] [RNTI: 0x6065 (24677)] [RNTI Type: C-RNTI (3)] [UEId: 1] [System Frame Number: 351] [Slot: 18] [HarqId: 8] [PHR Type2 other cell PHR: False] Subheader: (LCID:4 214 bytes) RLC-NR UEId=1 [UL] [AM] DRB:1 [DATA] SN=92 SO=1190 ..209-bytes] [Context] [Direction: Uplink (0)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: DRB (5)] [Bearer Id: 1] [PDU Length: 214] [Sequence Number length: 18] AM Header SN=92 SO=1190 1... .... = Data/Control: Data PDU .0.. .... = Polling Bit: Status report not requested **..10 .... = Segmentation Info: Data field contains the last segment of an RLC SDU (0x2)** .... 00.. = Reserved: 0x00 .... ..00 0000 0000 0101 1100 = Sequence Number: 92 Segment Offset: 1190 AM Data: 31323334353637383930313233343536373839303132333 4â€¦ Subheader: (LCID:4 1402 bytes) RLC-NR UEId=1 [UL] [AM] DRB:1 [DATA] SN=93 [1399-bytes] [Context] [Direction: Uplink (0)] [RLC Mode: Acknowledged Mode (4)]	

Signaltron Confidential. Do not copy

		[UEId: 1] [Bearer Type: DRB (5)] [Bearer Id: 1] [PDU Length: 1402] [Sequence Number length: 18] AM Header SN=93 1... .... = Data/Control: Data PDU .0.. .... = Polling Bit: Status report not requested **..00 .... = Segmentation Info: Data field contains all bytes of an RLC SDU (0x0)** .... 00.. = Reserved: 0x00 .... ..00 0000 0000 0101 1101 = Sequence Number: 93 AM Data: 80005d45000574e452220440115a530a6500050a65000130â€¦ RLC-NR UEId=1 [UL] [AM] DRB:1 [DATA] SN=94 [1399-bytes] [Context] [Direction: Uplink (0)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: DRB (5)] [Bearer Id: 1] [PDU Length: 1402] [Sequence Number length: 18] AM Header SN=94 1... .... = Data/Control: Data PDU .0.. .... = Polling Bit: Status report not requested **..00 .... = Segmentation Info: Data field contains all bytes of an RLC SDU (0x0)** .... 00.. = Reserved: 0x00 .... ..00 0000 0000 0101 1110 = Sequence Number: 94 AM Data: 80005e45000574e45222b0401159a70a6500050a65000136â€¦ RLC-NR UEId=1 [UL] [AM] DRB:1 [DATA] SN=95 [1151-bytes] [Context] [Direction: Uplink (0)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: DRB (5)] [Bearer Id: 1] [PDU Length: 1154] [Sequence Number length: 18] AM Header SN=95 1... .... = Data/Control: Data PDU .0.. .... = Polling Bit: Status report not requested **..00 .... = Segmentation Info: Data field contains all bytes of an RLC SDU (0x0)** .... 00.. = Reserved: 0x00 .... ..00 0000 0000 0101 1111 = Sequence Number: 95 AM Data: 80005f4500047ce452035c401179f30a6500050a65	

Signaltron Confidential. Do not copy

		000132â€¦ RLC-NR UEId=1 [UL] [AM] DRB:1 [DATA] SN=96 [1311-bytes.. [Context] [Direction: Uplink (0)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: DRB (5)] [Bearer Id: 1] [PDU Length: 1314] [Sequence Number length: 18] AM Header SN=96 1... .... = Data/Control: Data PDU .0.. .... = Polling Bit: Status report not requested **..01 .... = Segmentation Info: Data field contains the first segment of an RLC SDU (0x1**) .... 00.. = Reserved: 0x00 .... ..00 0000 0000 0110 0000 = Sequence Number: 96 AM Data: 80006045000574e458200040115c510a6500050a65000183â€¦	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	4.4.7 (c) RLC procedures: ARQ Procedures		
Requirement	ARQ procedures		
Test Objective	Verify that gNB AM RLC supports ARQ procedures		
	Test Steps	Acceptance Criteria	Remarks

Signaltron Confidential. Do not c

	Power the gNB and other systems. Power on the 5G UE and ensure that it succesfully registers with 5G gNB/Core Run Iperf command In gNodeB: iperf –s –i 1 –p 10001 –l 1400 –B “gNodeB_IP” In UE: Iperf –c “gNodeB_IP” –u –i 1 –t 1000 –p 10001 –l 1400 –b 50M –B “UE_IP” Check Wireshark logs to verify for RLC NACK and retransmission	**gNB PCAP logs(Apply filter mac-nr and rlc-nr):** No. Time Source Destination Protocol Length Info 32824 86.141840716 127.0.0.1 127.0.0.1 RLC-NR 504 UEId=1 [DL] [AM] DRB:1 [DATA] SN=2512 SO=989 ..429-bytes.. RLC-NR UEId=1 [DL] [AM] DRB:1 [DATA] SN=2512 SO=989 ..429-bytes.. [Context] [Direction: Downlink (1)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: DRB (5)] [Bearer Id: 1] [PDU Length: 434] [Sequence Number length: 18] AM Header SN=2512 SO=989 1... .... = Data/Control: Data PDU .0.. .... = Polling Bit: Status report not requested ..11 .... = Segmentation Info: Data field contains neither the first nor last segment of an RLC SDU (0x3) .... 00.. = Reserved: 0x00 .... ..00 0000 1001 1101 0000 = Sequence Number: 2512 Segment Offset: 989 AM Data: 383930313233343536373839303132333435363738393031â€¦ **Received NACK for the above sent sequence number 2512** No. Time Source Destination Protocol Length Info 32891 86.163078076 127.0.0.1 127.0.0.1 RLC-NR 276 UEId=1 [UL] [AM] DRB:1 [CONTROL] **ACK_SN=2517 NACK_SN=2512** (SOstart=989 SOend=1417) (Short BSR LCG ID=0 BS=0) (PHR PH=56 PCMAX_f_c=50) (Padding 191 bytes) RLC-NR UEId=1 [UL] [AM] DRB:1 [CONTROL] ACK_SN=2517 **NACK_SN=2512** (SOstart=989 SOend=1417) [Context] [Direction: Uplink (0)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: DRB (5)] [Bearer Id: 1] [PDU Length: 10] [Sequence Number length: 18] AM Header ACK_SN=2517 (1 NACKs) 0... .... = Data/Control: Control PDU .000 .... = Control PDU Type: STATUS PDU (0x0) .... 0000 0010 0111 0101 01.. = ACK Sequence Number: 2517	

Signaltron Confidential. Do not copy

		.... ..1. = Extension bit 1: A set of NACK_SN, E1, E2 and E3 follows ....0 = Reserved: 0x00 0000 0010 0111 0100 00.. .... = NACK Sequence Number: 2512 [Expert Info (Warning/Sequence): Status PDU reports NACK (partial) on Uplink for UE 1] [Status PDU reports NACK (partial) on Uplink for UE 1] [Severity level: Warning] [Group: Sequence] ..0. .... = Extension bit 1: A set of NACK_SN, E1, E2 and E3 does not follow ...1 .... = Extension bit 2: A set of SOstart and SOend follows for this NACK_SN .... 0... = Extension bit 3: NACK range field does not follow for this NACK_SN .... .000 = Reserved: 0x00 SO start: 989 SO end: 1417 [Number of NACKs: 1] Retransmitting SN=2152 data again No. Time Source Destination Protocol Length Info 32892 86.163086237 127.0.0.1 **127.0.0.1 RLC-NR 504 UEId=1 [DL] [AM] DRB:1 [DATA] SN=2512 SO=989 ..429-bytes.** RLC-NR UEId=1 [DL] [AM] DRB:1 [DATA] SN=2512 SO=989 ..429-bytes.. [Context] [Direction: Downlink (1)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: DRB (5)] [Bearer Id: 1] [PDU Length: 434] [Sequence Number length: 18] AM Header SN=2512 SO=989 1... .... = Data/Control: Data PDU .0.. .... = Polling Bit: Status report not requested ..11 .... = Segmentation Info: Data field contains neither the first nor last segment of an RLC SDU (0x3) .... 00.. = Reserved: 0x00 .... ..00 0000 1001 1101 0000 = Sequence Number: 2512 Segment Offset: 989 AM Data: 383930313233343536373839303132333435363738393031â€¦	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential: Do not copy

Test ID	4.4.7(C)MAC HARQ Entity		
Requirement	MAC		
Test Objective	This test case verifies the functionality of MAC (Medium Access Control) HARQ (Hybrid Automatic Repeat Request) in the gNB		
	Test Steps	Acceptance Criteria	Remarks

Signaltron Confidential. Do not copy

	Power the gNB and other systems. Power on the 5G UE and ensure that it succesfully registers with 5G gNB/Core Run Iperf Command In gNodeB: iperf –s –i 1 –p 10001 –l 1400 –B "gNodeB_IP" In UE: Iperf –c "gNodeB_IP" –u –i 1 –t 1000 –p 10001 –l 1400 –b 50M –B "UE_IP" Check Wireshark logs	**gNB PCAP logs(Apply filter mac-nr):** No. Time Source Destination Protocol Length Info 164 40.403120134 127.0.0.1 127.0.0.1 RLC-NR 183 UEId=1 [UL] [AM] SRB:1 [DATA] (P) SN=0 SO=85 ..3-bytes] (Long BSR) (Padding 103 bytes) MAC-NR UL-SCH (LCID:1 7 bytes) (Long BSR) (Padding 103 bytes) [Context (RNTI=24677)] [Radio Type: TDD (2)] [Direction: Uplink (0)] [RNTI: 0x6065 (24677)] [RNTI Type: C-RNTI (3)] [UEId: 1] [System Frame Number: 159] [Slot: 18] [HarqId: 2] [PHR Type2 other cell PHR: False] No. Time Source Destination Protocol Length Info 166 40.403140201 127.0.0.1 127.0.0.1 MAC-NR 183 UL-SCH (Long BSR) (Padding 112 bytes) MAC-NR UL-SCH (Long BSR) (Padding 112 bytes) [Context (RNTI=24677)] [Radio Type: TDD (2)] [Direction: Uplink (0)] [RNTI: 0x6065 (24677)] [RNTI Type: C-RNTI (3)] [UEId: 1] [System Frame Number: 159] [Slot: 19] **[HarqId: 3]** [PHR Type2 other cell PHR: False]	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	**4.4.7 (c)MAC PDU (DL-SCH and UL-SCH except transparent MAC and Random Access Response)**		
Requirement	MAC		
Test Objective	MAC PDU (DL-SCH and UL-SCH except transparent MAC and Random Access Response)		
Test Description	Test Steps	Acceptance Criteria	Remarks
	Power the gNB and other systems. Power on the 5G UE and ensure that it succesfully registers with 5G gNB/Core Run Iperf Command In gNodeB: iperf –s –i 1 –p 10001 –l 1400 –B “gNodeB_IP” In UE: Iperf –c “gNodeB_IP” –u –i 1 –t 1000 –p 10001 –l 1400 –b 50M –B “UE_IP” Check Wireshark logs	**gNB PCAP logs(Apply filter mac-nr):** No. Time Source Destination Protocol Length Info 9525 62.822415611 127.0.0.1 127.0.0.1 MAC-NR **109** **DL-SCH** (TAG=0 TA=31) (Padding 39 bytes) MAC-NR DL-SCH (TAG=0 TA=31) (Padding 39 bytes) [Context (RNTI=24677)] [Radio Type: TDD (2)] [Direction: Downlink (1)] [RNTI: 0x6065 (24677)] [RNTI Type: C-RNTI (3)] [UEId: 1] [System Frame Number: 351] [Slot: 0] [HarqId: 10] Subheader: (TAG=0 TA=31) Subheader: (Padding 39 bytes) No. Time Source Destination Protocol Length Info 9524 62.822407753 127.0.0.1 127.0.0.1 MAC-NR 103 **UL-SCH** (Long BSR) (Padding 32 bytes) MAC-NR UL-SCH (Long BSR) (Padding 32 bytes) [Context (RNTI=24677)] [Radio Type: TDD (2)] [Direction: Uplink (0)] [RNTI: 0x6065 (24677)] [RNTI Type: C-RNTI (3)] [UEId: 1] [System Frame Number: 350] [Slot: 7] [HarqId: 5] [PHR Type2 other cell PHR: False] Subheader: (Long BSR) Subheader: (Padding 32 bytes)	

Signaltron Confidential. Do not copy

<table>
<tr><td>Test ID</td><td colspan="3">4.4.7. (C)MAC DRX (Discontinuous Reception) Configuration</td></tr>
<tr><td>Requirement</td><td colspan="3">MAC</td></tr>
<tr><td>Test Objective</td><td colspan="3">This test case verifies the configuration and functionality of MAC (Medium Access Control) DRX in the gNB</td></tr>
<tr><td></td><td>Test Steps</td><td>Acceptance Criteria</td><td>Remarks</td></tr>
<tr><td></td><td>In Roadmap</td><td></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass:□</td><td colspan="2">Fail:□</td></tr>
</table>

Signaltron Confidential. Do not copy

Test ID	4.4.7.(c) Buffer status MAC CEs		
Requirement	MAC		
Test Objective	To verify different BSR CEs are supported To verify Short BSR, Short truncated BSR, Long BSR, Long truncated BSR		
	Test Steps	Acceptance Criteria	Remarks
Description	Power the gNB and other systems. Power on the 5G UE and ensure that it succesfully registers with 5G gNB/Core Run Iperf Command In gNodeB: iperf –s –i 1 –p 10001 –l 1400 –B “gNodeB_IP” In UE: Iperf –c “gNodeB_IP” –u –i 1 –t 1000 –p 10001 –l 1400 –b 50M –B “UE_IP” Check Wireshark logs	**gNB PCAP logs(Apply filter mac-nr):** No. Time Source Destination Protocol Length Info 164 40.403120134 127.0.0.1 127.0.0.1 RLC-NR 183 UEId=1 [UL] [AM] SRB:1 [DATA] (P) SN=0 SO=85 ..3-bytes] **(Long BSR)** (Padding 103 bytes) RLC-NR UEId=1 [UL] [AM] SRB:1 [DATA] (P) SN=0 SO=85 ..3-bytes] [Context] [Direction: Uplink (0)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: SRB (4)] [Bearer Id: 1] [PDU Length: 7] [Sequence Number length: 12] AM Header (P) SN=0 SO=85 1... .... = Data/Control: Data PDU .1.. .... = Polling Bit: Status report is requested ..10 .... = Segmentation Info: Data field contains the last segment of an RLC SDU (0x2) .... 0000 0000 0000 = Sequence Number: 0 Segment Offset: 85 AM Data: 000000 Subheader: **(Long BSR)** No. Time Source Destination Protocol Length Info 190 40.452548997 127.0.0.1 127.0.0.1 PDCP-NR 276 UEId=1 [UL] [AM] SRB:1 [DATA] (P) SN=5 [20-bytes] (**Short BSR** LCG ID=0 BS=0) (Padding 182 bytes) RLC-NR UEId=1 [UL] [AM] SRB:1 [DATA] (P) SN=5 [20-bytes] [Context]	

Signaltron Confidential, Do not copy

		[Direction: Uplink (0)] [RLC Mode: Acknowledged Mode (4)] [UEId: 1] [Bearer Type: SRB (4)] [Bearer Id: 1] [PDU Length: 22] [Sequence Number length: 12] AM Header (P) SN=5 1... .... = Data/Control: Data PDU .1.. .... = Polling Bit: Status report is requested ..00 .... = Segmentation Info: Data field contains all bytes of an RLC SDU (0x0) .... 0000 0000 0101 = Sequence Number: 5 AM Data: 00050000000400de75aab0103ceb55405b73f56b PDCP-NR (SN=5) [Configuration: UEId= 1 SRB-1 (direction=Uplink, plane=Signalling)] [Direction: Uplink (0)] [Plane: Signalling (1)] [UE: 1] [Bearer type: DCCH (1)] [Bearer Id: 1] 0000 .... = Reserved: 0 .... 0000 0000 0101 = Seq Num: 5 [Sequence Analysis - OK] Previous frame for Bearer: 185 [OK: True] Signalling Data: 0000000400de75aab0103ceb5540 MAC: 0x5b73f56b Subheader: (**Short BSR** LCG ID=0 BS=0) Subheader: (Padding 182 bytes)	

Signaltron Confidential. Do not copy

Test ID	**4.4.7.(C) C-RNTIMAC CE**		
Requirement	MAC		
Test Objective	To verify C-RNTI MAC CE is supported		
	Test Steps	Acceptance Criteria	Remarks
	Power on multiple 5G UEs and let them register with 5G gNB/Core network successfully. Check Wireshark logs. Same can be seen in UE logs.	**gNB PCAP logs(Apply filter mac-nr):** No. Time Source Destination Protocol Length Info 191 40.452558426 127.0.0.1 127.0.0.1 RLC-NR 284 UEId=1 [DL] [AM] SRB:1 [CONTROL] ACK_SN=6 (Padding 210 bytes) MAC-NR DL-SCH (LCID:1 3 bytes) (Padding 210 bytes) [Context (RNTI=24677)] [Radio Type: TDD (2)] [Direction: Downlink (1)] **[RNTI: 0x6065 (24677)]** **[RNTI Type: C-RNTI (3)]** [UEId: 1] [System Frame Number: 165] [Slot: 4] [HarqId: 0]	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	**4.4.7.(C) Recommended bit rate MAC CE**		
Requirement	MAC		
Test Objective	To verify Recommended bit rate mac CE is supported		
	Test Steps	Acceptance Criteria	Remarks
	Power on multiple 5G UEs and let them register with 5G gNB/Core network successfully. "Recommended bit rate MAC-CE It will have 1. MAC header 2. LCID 3. Direction 4. Bitrate Reserve bit"	1. Open wireshark log or UE log 2. apply the filter: mac-nr && !icmp && mac-nr.ulsch.lcid = 0x35 It will have 1. MAC header (Without Length Field) 2. LCID (0x35) 3. Direction 4. Bitrate Reserve bit"	
Overall Test Result	Pass:	Fail	

Signaltron Confidential. Do not copy

Test ID	4.4.7.c Configured Grant Confirmation MAC CE		
Requirement	MAC		
Test Objective	To verify if mac support Configured Grant Confirmation MAC CE		
	Test Steps	Acceptance Criteria	Remarks
	Power on multiple 5G UEs and let them register with 5G gNB/Core network successfully. Initiate data session.	1. In wireshark capture General step for Verification 1. Open wireshark log or UE log 2. apply the filter: mac-nr && !icmp && mac-nr.ulsch.lcid == 0x37 It will have MAC header (Without Length Field and with LCID 0x37)	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	4.4.7(C) Single and Multiple Entry **PHR**		
Requirement	MAC		
Test Objective	To verify if mac support the following 1. Multiple Entry PHR (Four octet) 2. Multiple Entry PHR (One octet) 3. Single Entry **PHR**		
	Test Steps	Acceptance Criteria	Remarks

Signaltron Confidential. Do not copy

	1. Single Entry PHR it will have a. MAC header (Without length field) b. Reserve bit c. Power Headroom d. Reserve bit e. Pcmax,f,c 2. Multiple Entry PHR (One octet) a. MAC header (with 16 bit length field) b. Ci (0-7) c. Reserved bit d. V: Indicate if PH is based on real or reference transmission e. Power Headroom f. P: Indicate if power backoff is applied or not g.Pcmax,f,c 3. Multiple Entry PHR (Four octet) a. MAC header (with 16 bit length field) b. Ci (0-24) c. Reserved bit d. V: Indicate if PH is based on real or reference transmission e. Power Headroom f. P: Indicate if power backoff is applied or not g.Pcmax,f,c	1. In wireshark capture "General step for Verification 1. Open wireshark 2. apply the filter: mac-nr && !icmp &&(mac-nr.ulsch.lcid == 0x36 II mac-nr.ulsch.lcid == 0x38 II mac-nr.ulsch.lcid == 0x39) It will have 1. Single Entry PHR it will have a. MAC header (Without length field) b. Reserve bit c. Power Headroom d. Reserve bit e. Pcmax,f,c 2. Multiple Entry PHR (One octet) a. MAC header (with 16 bit length field) b. Ci (0-7) c. Reserved bit d. V: Indicate if PH is based on real or reference transmission e. Power Headroom f. P: Indicate if power backoff is applied or not g. Pcmax,f,c 3. Multiple Entry PHR (Four octet) a. MAC header (with 16 bit length field) b. Ci (0-24) c. Reserved bit d. V: Indicate if PH is based on real or reference transmission e. Power Headroom f. P: Indicate if power backoff is applied or not g. Pcmax,f,c" **Example of UE log as below:** **MCE Type : S-PHR** R : 0 R : 0 **Single PHR** PH : 62 R : 0 Pcmax fc : 51 R : 0	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	4.4.7 (d)		
Requirement	RRC (Terminated in gNB on the network side) performs the functions listed in 3GPP standards		
Test Objective	All 5G Radio protocols should be supported while establishing a connection and data transfer to/from UE.		
Test Description	Test Steps	Acceptance Criteria	Remarks
	Apply the filter nr-rrc in the wireshark log and review the contents of RRC Setup and RRC Reconfiguration for establishing RRC connection and data radio bearer..	NR Radio Resource Control (RRC) protocol DL-CCCH-Message message: c1 (0) **c1: rrcSetup (1)** rrcSetup rrc-TransactionIdentifier: 3 criticalExtensions: rrcSetup (0) rrcSetup radioBearerConfig srb-ToAddModList: 1 item Item 0 SRB-ToAddMod srb-Identity: 1 masterCellGroup [...]: CellGroupConfig cellGroupId: 0 rlc-BearerToAddModList: 1 item Item 0	

Signaltron Confidential. Do not copy

		RLC-BearerConfig logicalChannelIdentity: 1 servedRadioBearer: srb-Identity (0) srb-Identity: 1 rlc-Config: am (0) am ul-AM-RLC sn-FieldLength: size12 (0) t-PollRetransmit: ms45 (8) pollPDU: infinity (23) pollByte: infinity (43) maxRetxThreshold: t8 (5) dl-AM-RLC sn-FieldLength: size12 (0) t-Reassembly: ms35 (7) t-StatusProhibit: ms0 (0) mac-LogicalChannelConfig ul-SpecificParameters priority: 1 prioritisedBitRate: infinity (15)	

Signaltron Confidential. Do not copy

		bucketSizeDuration: ms1000 (8) logicalChannelGroup: 0 schedulingRequestID: 0 .... .0.. logicalChannelSR-Mask: False .... ..0. logicalChannelSR-DelayTimerApplied: False NR Radio Resource Control (RRC) protocol DL-DCCH-Message message: c1 (0) **c1: rrcReconfiguration (0)** rrcReconfiguration rrc-TransactionIdentifier: 1 criticalExtensions: rrcReconfiguration (0) rrcReconfiguration radioBearerConfig srb-ToAddModList: 2 items Item 0 SRB-ToAddMod srb-Identity: 1 Item 1 SRB-ToAddMod srb-Identity: 2 drb-ToAddModList: 1 item	

Signaltron Confidential. Do not copy

		Item 0 DRB-ToAddMod cnAssociation: sdap-Config (1) sdap-Config pdu-Session: 11 sdap-HeaderDL: absent (1) sdap-HeaderUL: absent (1) 1... .... defaultDRB: True mappedQoS-FlowsToAdd: 1 item Item 0 QFI: 1 drb-Identity: 1 pdcp-Config drb discardTimer: infinity (15) pdcp-SN-SizeUL: len18bits (1) pdcp-SN-SizeDL: len18bits (1) headerCompression: notUsed (0) notUsed: NULL t-Reordering: ms100 (14) CellGroupConfig	

Signaltron Confidential. Do not copy

		cellGroupId: 0 rlc-BearerToAddModList: 3 items Item 0 RLC-BearerConfig logicalChannelIdentity: 1 servedRadioBearer: srb-Identity (0) srb-Identity: 1 rlc-Config: am (0) am ul-AM-RLC sn-FieldLength: size12 (0) t-PollRetransmit: ms45 (8) pollPDU: infinity (23) pollByte: infinity (43) maxRetxThreshold: t8 (5) dl-AM-RLC sn-FieldLength: size12 (0) t-Reassembly: ms35 (7) t-StatusProhibit: ms0 (0) mac-LogicalChannelConfig	

Signaltron Confidential. Do not copy

		ul-SpecificParameters priority: 1 prioritisedBitRate: infinity (15) bucketSizeDuration: ms1000 (8) logicalChannelGroup: 0 schedulingRequestID: 0 .... .0.. logicalChannelSR-Mask: False .... ..0. logicalChannelSR-DelayTimerApplied: False Item 1 RLC-BearerConfig logicalChannelIdentity: 2 servedRadioBearer: srb-Identity (0) srb-Identity: 2 rlc-Config: am (0) am ul-AM-RLC sn-FieldLength: size12 (0) t-PollRetransmit: ms45 (8) pollPDU: infinity (23) pollByte: infinity (43)	

Signaltron Confidential. Do not copy

		maxRetxThreshold: t8 (5) dl-AM-RLC sn-FieldLength: size12 (0) t-Reassembly: ms35 (7) t-StatusProhibit: ms0 (0) mac-LogicalChannelConfig ul-SpecificParameters priority: 2 prioritisedBitRate: infinity (15) bucketSizeDuration: ms5 (0) logicalChannelGroup: 0 schedulingRequestID: 0 .... .0.. logicalChannelSR-Mask: False .... ..0. logicalChannelSR-DelayTimerApplied: False Item 2 RLC-BearerConfig logicalChannelIdentity: 4 servedRadioBearer: drb-Identity (1) drb-Identity: 1 rlc-Config: am (0)	

Signaltron Confidential, Do not copy

		am ul-AM-RLC sn-FieldLength: size18 (1) t-PollRetransmit: ms45 (8) pollPDU: p64 (4) pollByte: kB500 (13) maxRetxThreshold: t32 (7) dl-AM-RLC sn-FieldLength: size18 (1) t-Reassembly: ms15 (3) t-StatusProhibit: ms15 (3) mac-LogicalChannelConfig ul-SpecificParameters priority: 13 prioritisedBitRate: kBps8 (1) bucketSizeDuration: ms100 (4) logicalChannelGroup: 1 schedulingRequestID: 0 0... .... logicalChannelSR-Mask: False .0.. .... logicalChannelSR-DelayTimerApplied: False	

Signaltron Confidential. Do not copy

Overall Test Result	Pass:□	Fail:□

Signaltron Confidential. Do not copy

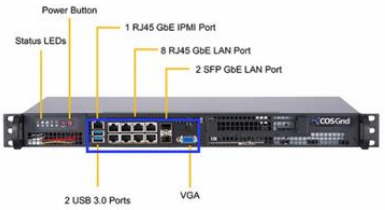
Test ID	4.4.7 (e)NAS control protocol (terminated in AMF on the network side) performs the functions listed in 3GPP Standards. For instance: authentication, mobility management, security control.		
Requirement	NAS control protocol		
Test Objective	To verify NAS control protocol functions: authentication, mobility management, security control.		
Test Description	Test Steps	Acceptance Criteria	Remarks
	Run the tcpdump command to collect PCAP sudo tcpdump -i any -w filename.pcap RUN the setup with default config 1. gNB and AMF are powered on and operational. 2. UE is registered and attached to the gNB. Once setup Up then connect the UE. Observe the Nas Control protocol messages which do functions like Registration, authentication, mobility management, security control.	1.In wireshark capture apply filters ''nas-5gs ". NR RRC/NAS-5GS/NAS-5Gs ULRRCMessageTransfer, RRC Setup Complete, Registration request, Registration request. NGAP/NAS-5GS DownlinkNASTransport, Identity request NR RRC/NAS-5GS ULRRCMessageTransfer, UL Information Transfer, Identity response. NGAP/NAS-5GS 152 SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request. NGAP/NAS-5GS 132 UplinkNASTransport, Authentication response. NGAP/NAS-5GS 116 DownlinkNASTransport, Security mode command. NR RRC/NAS-5GS/NAS-5GS ULRRCMessageTransfer, UL Information Transfer, Security mode complete, Registration request.	

Signaltron Confidential. D y

		NGAP/NAS-5GS InitialContextSetupRequest,Registration accept NR RRC/NAS-5GS DLRRCMessageTransfer, DL Information Transfer, Registration accept NGAP/NAS-5GS 124 UplinkNASTransport,Registration complete	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

4.8 Firewall with Router

Test ID	4.8.1.a Networking Interfaces		
Requirement	Verify 1. Gigabit Base-T(Cu)= 6 ports or higher(as required) and 1 Gs Fiber (SFP)= 4 ports		
Test Objective	Test SFP and Ethernet port		
Test Description	Test Steps	Acceptance criteria	Remarks
	it can be verified by Physically	 1 Gigabit Base-T (Cu) = 6 ports or higher(as required) 1 Gs Fiber (SFP) = 4 ports	It can be verified physically
Overall Test Result	Pass:	Fail:	

Test ID	4.8.1.b WAN interfaces		
Requirement	2x10 Gigabit Ethernet SFP+ Ports		
Test Objective	2x10 Gigabit Ethernet SFP+ Ports		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet	2. Hardware - Overview Networking Interfaces: 1 Gigabit Base-T (Cu) = 6 ports or higher (as required); 1 Gs Fiber (SFP) = 4 ports WAN Interface: 2 x 1G Gigabit Ethernet SFP+ ports. Management Port: 10/100 Mbps RJ 45 Management port	
Overall Test Result	Pass:	Fail:	

Test ID	4.8.1.c Management port		
Requirement	10/100 Mbps RJ45 Management port		
Test Objective	10/100 Mbps RJ45 Management port		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet	2. Hardware - Overview Networking Interfaces: 1 Gigabit Base-T (Cu) = 6 ports or higher (as required); 1 Gs Fiber (SFP) = 4 ports WAN Interface: 2 x 1G Gigabit Ethernet SFP+ ports. Management Port: 10/100 Mbps RJ 45 Management port	
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.2 Firewall Features		
Requirement	Firewall Features		
Test Objective	Firewall Features		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet	**2. Hardware - Overview** Networking Interfaces • 1 Gigabit Base-T (Cu) = 6 ports or higher (as required) • 1 Gs Fiber (SFP) = 4 ports WAN Interface • 2 x 1G Gigabit Ethernet SFP+ ports. Management Port • 10/100 Mbps RJ 45 Management port	
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.3 Performance Requirement		
Requirement	Verify 1 a). Firewall throughput of 1 Gbps b) Threat Protection - 500 Mbps		
Test Objective	Verify Firewall throughput and Threat Protection		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet or using iperf test	From the CosGrid data sheet: Performance ▪ Firewall throughput of 1 Gbps ▪ Threat Protection – 500 Mbps.	It can be verified 1 Gbps
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.4(a) Web Filtering		
Requirement	Verify: Control access to websites and website categories (e.g. business, news, sports, social media		
Test Objective	Verify access controlling		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet or Web GUI. For Web GUI, navigate to Services-> Web Proxy	From Cosgrid data sheet: Web Filtering ▪ Control access to websites and website categories (e.g. business, news, sports, social media) ▪ Integrate into Active Directory, applying policies to specific users or user groups. ▪ Block access to malicious content or websites ▪ Enforce Safe Search	Allowed websites and web categories should be accessible
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.4(b) Web Filtering		
Requirement	b). Integrate into Active Directory, applying policies to specific users or user groups.		
Test Objective	Verify access controlling		
Test Description	Test Steps	Acceptance criteria	Remarks
	Check from the data sheet	Web Filtering ▪ Control access to websites and website categories (e.g. business, news, sports, social media) ▪ Integrate into Active Directory, applying policies to specific users or user groups.	Allowed websites and web categories should be accessible
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.4.d Web Filtering		
Requirement	Verify c) Enforce Safe search d). Block or control access to Cloud services.		
Test Objective	Verify Block or control access to Cloud services.		
Test Description	Test Steps	Acceptance criteria	Remarks
	Check from the data sheet	Web Filtering ▪ Control access to websites and website categories (e.g. business, news, sports, social media) ▪ Integrate into Active Directory, applying policies to specific users or user groups. ▪ Block access to malicious content or websites ▪ Enforce Safe Search	Blocked web categories should not be accessible
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.4.Web Filtering		
Requirement	Verify e). Detailed web access reports (by user, group, website) f)Full SSL Inspection support		
Test Objective	Verify Detailed web access reports (by user, group, website)		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from data sheet of Cosgrid Firewall For Configuration, Navigate to Services-> Web Proxy -> Adminstration.	Application Control & Visiblity ▪ Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps) ▪ Full network visibility of HTTP and HTTPS traffic ▪ Control access to specific applications (e.g. Web Games, Video Streaming) ▪ Block or control access to Cloud services. ▪ Detailed web access reports (by user, group, website) ▪ Detailed reporting and network visibility	Web access reports should be accessible
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.4(iv) Web Filtering		
Requirement	Verify 1 e). Transparent solution (or explicit proxy support)		
Test Objective	Verify Transparent solution (or explicit proxy support)		
Test Description	Test Steps	Acceptance criteria	Remarks
	It can be configured via Web GUI. For Configuration, Navigate to Services-> Web Proxy -> Adminstration. The Adminstration Window opens and it has 5 tabs namely General Proxy settings, Forward Proxy, Proxy Auto configuration, Remote access control lists and support		
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.6.a Secure Remote Access		
Requirement	Verify 1 a). SSL and IPSec VPN support		
Test Objective	Verify SSL and IPSec VPN support		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from data sheet or Web GUI. From Web GUI: To configure IPSec VPN, select the VPN-> IPSec on the navigation bar. IPSec VPN configurations has Pre shared keys , key pairs , Lease status, Mobile clients ,connection status,logfiles etc.	Secure Remote Access ▪ SSL and IPSec VPN support ▪ Site-to-Site IPSec VPN (with Dynamic Routing) ▪ Two- Factor authentication support (e.g. Secure Token) ▪ High performance VPN concentrator solution	
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Not copy

Test ID	4.8.6.b Secure Remote Access		
Requirement	Verify 1 b). Web-Portal and full VPN client application		
Test Objective	Verify Web-Portal and full VPN client application		
Test Description	Test Steps	Acceptance criteria	Remarks
	Application and Web-Portal can be accessed over VPN by using the Open VPN Application. To configure OpenVPN, Select the VPN->OpenVPN on the navigator bar.		
Overall Test Result	Pass:	Fail:	

Test ID	4.8.6.c Secure Remote Access		
Requirement	Verify 1 c). Site-to-Site IPSec VPN (with Dynamic Routing)		
Test Objective	Verify Site-to-Site IPSec VPN (with Dynamic Routing)		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet.	Secure Remote Access ▪ SSL and IPSec VPN support ▪ Site-to-Site IPSec VPN (with Dynamic Routing) ▪ Two- Factor authentication support (e.g. Secure Token) ▪ High performance VPN concentrator solution	Site-to-site IPSEC VPN must support.
Overall Test Result	Pass:	Fail:	

Signaltron Confidential - Do not copy

Test ID	4.8.6.f Secure Remote Access		
Requirement	Verify f). Two-Factor authentication support (e.g. Secure Token)		
Test Objective	Verify Two-Factor authentication support (e.g. Secure Token)		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from data sheet	Secure Remote Access ▪ SSL and IPSec VPN support ▪ Site-to-Site IPSec VPN (with Dynamic Routing) ▪ Two- Factor authentication support (e.g. Secure Token) ▪ High performance VPN concentrator solution	SDWAN should supports Two-factor authentication.
Overall Test Result	Pass:	Fail:	

Test ID	4.8.7.a Application Control		
Requirement	Verify 1 a). Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps)		
Test Objective	Verify Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps)		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet	Application Control & Visiblity ▪ Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps) ▪ Full network visibility of HTTP and HTTPS traffic ▪ Control access to specific applications (e.g. Web Games, Video Streaming) ▪ Block or control access to Cloud services. ▪ Detailed web access reports (by user, group, website) ▪ Detailed reporting and network visibility	
Overall Test Result	Pass:	Fail:	

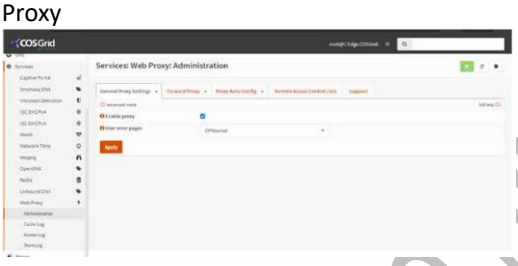
Signaltron Confidential. Not copy

Test ID	4.8.7.b Application Control		
Requirement	Verify b). Full network visibility of HTTP and HTTPS traffic		
Test Objective	Verify Full network visibility of HTTP and HTTPS traffic		
Test Description	Test Steps	Acceptance criteria	Remarks
	View the network traffic and its analytics through the firewall and can generate the analytical reports. To view the Network Visiblity of the firewall, access the web interface IP with Port 3000- 192.168.15.1:3000. The Network Analytics window of the Firewall opens. In the Dashboard section itself, you can view the overview of Network parameters like Top hosts, Applications, flow talkers, Traffic classifications etc. Alternatively, Verify from data sheet	Application Control & Visiblity ▪ Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps) ▪ Full network visibility of HTTP and HTTPS traffic ▪ Control access to specific applications (e.g. Web Games, Video Streaming) ▪ Block or control access to Cloud services. ▪ Detailed web access reports (by user, group, website) ▪ Detailed reporting and network visibility	
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.7.c Application Control		
Requirement	Verify c). Control access to specific applications (e.g. Web Games, Video Streaming)		
Test Objective	Control access to specific applications (e.g. Web Games, Video Streaming)		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet	Application Control & Visiblity ▪ Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps) ▪ Full network visibility of HTTP and HTTPS traffic ▪ Control access to specific applications (e.g. Web Games, Video Streaming) ▪ Block or control access to Cloud services. ▪ Detailed web access reports (by user, group, website) ▪ Detailed reporting and network visibility	User should be able to control access to specific applications.
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.7.d Application Control		
Requirement	Verify d). Block access to malicious content or websites		
Test Objective	Verify Block access to malicious content or websites		
Test Description	Test Steps	Acceptance criteria	Remarks
	Web Application or Verify from data sheet. 1. Enter the website to block by navigating services->webProxy. 2.From the devices connected, try accessing the web site. It should be blocked.	For Web Filtering, navigate to services->Web Proxy  Web Filtering ▪ Control access to websites and website categories (e.g. business, news, sports, social media) ▪ Integrate into Active Directory, applying policies to specific users or user groups. ▪ Block access to malicious content or websites ▪ Enforce Safe Search	
Overall Test Result	Pass:	Fail:	

Signaltron Confidential Do not copy

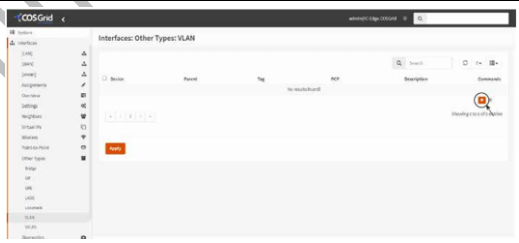
Test ID	4.8.7.e Application Control		
Requirement	Verify e). Detailed reporting and network visibility		
Test Objective	Verify Detailed reporting and network visibility		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from data sheet or Web GUI. 1.View the network traffic and its analytics through the firewall and can generate the analytical reports. 2.To view the Network Visibility of the firewall, access the web interface IP with Port 3000- 192.168.15.1:3000. The Network Analytics window of the Firewall opens. In the Dashboard section itself, you can view the overview of Network parameters like Top hosts, Applications, flow talkers, Traffic classifications etc..	Application Control & Visiblity ▪ Control and monitor cloud application usage (e.g. Dropbox, Box, Google Apps) ▪ Full network visibility of HTTP and HTTPS traffic ▪ Control access to specific applications (e.g. Web Games, Video Streaming) ▪ Block or control access to Cloud services. ▪ Detailed web access reports (by user, group, website) ▪ Detailed reporting and network visibility	
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

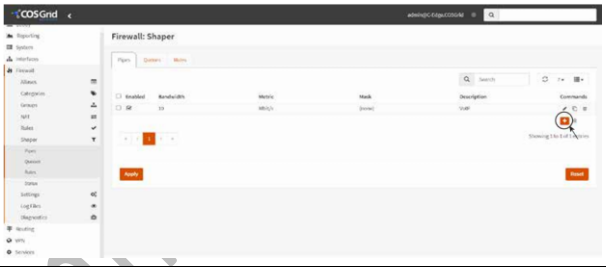
Test ID	4.8.8.a Intelligent Networking		
Requirement	Verify a). Dynamic routing (OSPF/BGP/RIP)		
Test Objective	Verify Dynamic routing (OSPF/BGP/RIP)		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the Data sheet or Web GUI. For Web GUI: Navigate the menu Routing->OSPF. The OSPF window appears and it contains 5 Tabs namely General, Networks Prefix lists and Route Maps	Intelligent Routing ▪ Dynamic routing (OSPF/BGP/RIP) ▪ Load-Balancing and ECMP ▪ 802.1Q VLAN and Layer2 switching support ▪ Rich traffic/shaping QOS support ▪ Dynamic routing over VPN (e.g. OSPF) groups	OSPF routing should support.
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Not copy

Test ID	4.8.8.b Intelligent Networking		
Requirement	Verify b). Load-Balancing and ECMP		
Test Objective	Verify Load-Balancing and ECMP		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from the data sheet	Intelligent Routing ▪ Dynamic routing (OSPF/BGP/RIP) ▪ Load-Balancing and ECMP ▪ 802.1Q VLAN and Layer2 switching support ▪ Rich traffic/shaping QOS support ▪ Dynamic routing over VPN (e.g. OSPF) groups	Multiple flows should be load balanced across multiple uplinks.
Overall Test Result	Pass:	Fail:	

Test ID	4.8.8.c Intelligent Networking		
Requirement	Verify c). 802.1Q VLAN and Layer2 switching support		
Test Objective	Verify 802.1Q VLAN and Layer2 switching support		
Test Description	Test Steps	Acceptance criteria	Remarks
	Verify from data sheet or Configure using Web GUI: VLANs, or Virtual LANs, allows for the partitioning of a solitary physical network into multiple virtual networks. This partitioning serves various objectives, with one of them being the facilitation of Quality of Service (QoS). Navigate to the menu Interfaces -> Other Types -> VLAN.	 Intelligent Routing ▪ Dynamic routing (OSPF/BGP/RIP) ▪ Load-Balancing and ECMP ▪ 802.1Q VLAN and Layer2 switching support ▪ Rich traffic/shaping QOS support ▪ Dynamic routing over VPN (e.g. OSPF) groups	Point to point IP on LAN and WAN interface should be reachable using correct 802.1Q VLAN.
Overall Test Result	Pass:	Fail:	

Signaltron Confidential. Do not copy

Test ID	4.8.8.d Intelligent Networking		
Requirement	Verify d). Rich traffic/shaping QOS support e) Dynamic routing over VPN (eg. OSPF) groups.		
Test Objective	Verify Rich traffic/shaping QOS support		
Test Description	Test Steps	Acceptance criteria	Remarks
	From data sheet or Web GUI: Pipe simulates a connection that possesses specific attributes such as bandwidth, propagation delay, queue size, and packet loss rate. As packets emerge from the classifier, they are queued in front of the pipe and subsequently transmitted through the pipe in accordance with its designated parameters. To Configure the pipe , select Firewall -> Shaper -> Pipes .	Intelligent Routing ▪ Dynamic routing (OSPF/BGP/RIP) ▪ Load-Balancing and ECMP ▪ 802.1Q VLAN and Layer2 switching support ▪ Rich traffic/shaping QOS support ▪ Dynamic routing over VPN (e.g. OSPF) groups 	Traffic flows should be policed/filtered on ingress and egress ports
Overall Test Result	Pass:	Fail:	

Signaltron Confidential do not copy

4.9 Section: - Server-1 with 5G Core, IMS and NMS software

Test ID	**4.9.1 Processors** **4th Generation Intel® Xeon Gold 2.4 GHz or equivalent 24 Core (minimum). Each servers with minimum 1 Processor and 2 Socket or higher as required.**		
Requirement	Servers 1 with minimum 1 Processors and 2 Socket or higher as required		
Test Objective	Verify the processors in server 1		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Login server by ILOport. by Google chrome Ip address:172.16.0.12 User Name:Administrator Password:(Mentionedin server) Go to>System Information>Processorrs	CPU configuration should be as per requirement. Processor 2.4 GHz or equivalent 24Core (minimum).	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.9.2 Memory		
Requirement	To verify memory DDR4 or above 64 GB scalable upto 256 GB or above		
Test Objective	Verify memory		
Description	Test Steps	Acceptance Criteria	Remarks
	Login server by ILOport. by Google chrome Ip address:172.16.0.12 User Name: Administrator Password:(Mentioned inserver) • Go to>System Information>Memory.	Total available memory should be greater than or equal to 64 GB.	
Test Result	Pass ☐	Fail ☐	

Test ID	4.9.3 Storage		
Requirement	To verify sencer storage SAS SSD Storage = 1 TB		
Test Objective	Verify storage		
	Test Steps	Acceptance Criteria	Remark
	Login sencer by ILO port. by Google chrome Ip address:172.16.0.12 User Name: Administrator Password:(Mentioned in sencer) Go to>System Information>Storage	storage SAS SSD Storage = 1 TB	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

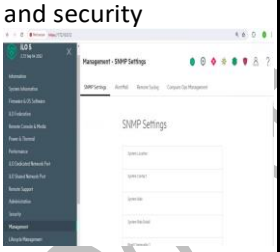
Test ID	4.9.4 Operating System And Virtualization Software		
Requirement	To verify Operating System And Virtualization Software		
Test Objective	Verify OS and VS		
	Test Steps	Acceptance Criteria	Remark
	Login serverby Ip address:172.16.0.2 User Name:root Password:(#Niral@7896#) uname-a lscpu lgrep Virtualization	Linux pve 5.15.102-1-pve #1 SMP PVE 5.15.102-1 (2023-03-14T13:48Z) x86 64 GNU/Linux root@pve:~# root@pve:~# lscpu lgrep Virtualization Virtualization: VT-x root@pve:~#	OS Linux machines also have virtualization enabled.
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.9.5 Network Interface		
Requirement	To verify Dual port lG SFP+ card, 4 x lG BaseT		
Test Objective	Verify Physically Network Interface		
	Test Steps	Acceptance Criteria	Remark
	Kindly check Physically Network Interface	Dual port lOG SFP+ card, 4 x 1G BaseT	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.9.6 PCie Slots		
Requirement	To verify PCie Slots		
Test Objective	To verify PCie Slots		
	Test Steps	Acceptance Criteria	Remark
	Kindly check Physically Network Interface	Minimum 4 x PCie 16x 4.0 slots for 1/0 Connectivity or higher as required.	
Overall Test Result	Pass:□	Fail: □	

Signaltron confidential. Do not copy

Test ID	4.9.7 Management 4.9.8 Security		
Requirement	To verify Management/Security		
Test Objective	To verify Management/Security		
	Test Steps	Acceptance Criteria	Remark
	Login server by ILOport. **by Google chrome** **Ip address:172.16.0.12 User** **Name:Administrator** **Password:(Mentioned inserver)** **Go to>Management>Security**	Check the Management and security 	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

4.10 Section: - Server-2 with 5G MEC Platform and Application Server

1 Processor

Test ID	4.10.1 MEC server processor configuration		
Requirement	3rd Generation Intel® Xeon Gold 2.4 GHz, 20 Core (mini). Each server with minimum 1 Processors and 2 Socket or higher as required.		
Test Objective	Verify Processor details		
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Login server by ILO port. **by Google chrome** **Ip address:172.16.0.13** **User Name: Administrator** **Password:(Mentioned in server)** **Go to>System Information>Processors**	**Processor 2.4 GHz or equivalent 24Core (minimum).**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

2 Memory

Test ID	4.10.2 MEC server memory configuration		
Requirement	DDR-3200 or above 64 GB scalable up to 128 GB		
Test Objective			
Description	**Test Steps**	**Acceptance Criteria**	**Remarks**
	Login server by ILO port. by Google chrome Ip address:172.16.0.13 User Name: Administrator Password:(Mentioned in server) **Go to>System Information>Memory**	**DDR4 or higher, 128 GB scalable upto 512GB**	
Test Result	Pass ☐	Fail ☐	

Signaltron Confidential. Do not copy

Test ID	4.10.3 Storage		
Requirement	To verify server storage SAS SSD Storage = 1TB		
Test Objective	Verify storage		
	Test Steps	Acceptance Criteria	Remark
	Login server by ILO port. by Google chrome Ip address:172.16.0.12 User Name: Administrator Password:(Mentioned in server) Go to>System Information>Storage	storage SAS SSD Storage= 4TB **HDD4TB**	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	4.10.5 Operating System And Virtualization Software		
Requirement	To verify Operating System And Virtualization Software		
Test Objective	Verify OS and VS		
	Test Steps	Acceptance Criteria	Remark
	Login serverby Ip address:172.16.0.3 User Name:root Password:(#Niral@7896#) uname-a lscpu lgrep Virtualization	Linux pve 5.15.102-1-pve #1 SMP PVE 5.15.102-1 (2023-03-14T13:48Z) x86 64 GNU/Linux root@pve:- # root@pve:-# lscpu lgrep Virtualization Virtualization: VT-x root@pve:-#	OS Linux machines also have virtualization enabled.
Overall Test Result	Pass:□	Fail:□	

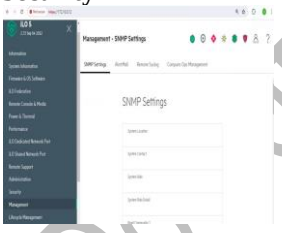
Signaltron Confidential. Do not copy

Test ID	4.10.6 Network Interlace		
Requirement	To verify Dual port lG SFP+ card, 4 x lG BaseT		
Test Objective	Verify Physically Network Interlace		
	Test Steps	Acceptance Criteria	Remarks
	Kindly check Physically Network Interlace	Dual port lOG SFP+ card, 4 x lG BaseT	
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	4.10.7 PCie Slots		
Requirement	To verify PCie Slots		
Test Objective	To verify PCie Slots		
	Test Steps	Acceptance Criteria	Remark
	Kindly check Physically Network Interface	Minimum 4 x PCie 16x 4.0 slots for 1/0 Connectivity or higher as required.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Do not copy

Test ID	**4.10.7 Management** **4.10.8 Security**		
Requirement	**To verify Management /Security**		
Test Objective	**To verify Management /Security**		
	Test Steps	Acceptance Criteria	Remark
	Login server by ILOport. **by Google chrome** **Ip address:172.16.0.13** **User Name:Administrator** **Password:(Mentioned in server)** **Go to>Management>Security**	**Kindly check Management and Security** 	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

4.11 5G Rewriteable SIM

Test ID	5G Rewriteable SIM		
Requirement	To verify the SIM can be programmed with required SUPI/IMSI		
Test Objective	To verify the SIM can be programmed with required SUPI/IMSI and Authentication key		
	Test Steps	Acceptance Criteria	Remark
	Re progamme the SIM card with SUPI/IMSI, Authentication key. White list the IMSI in the core network. Insert the SIM card into smartphone. Power on the smartphone and verify it attaches with 5G network	Verify if the smartphone attaches with 5G network and able to browse internet.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

4.12 5G Evaluation Board

Test ID	4.12 5G Evaluation board		
Requirement	To verify 5G Evaluation board successfully attaches to 5G Network		
Test Objective	To verify 5G Evaluation board successfully attaches to 5G Network		
	Test Steps	Acceptance Criteria	Remark
	Insert 5G SIM card into the Evaluation board Power on the evaluation board	Evaluation board should attach to 5G network. User connected with evaluation board should be able to browse internet.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

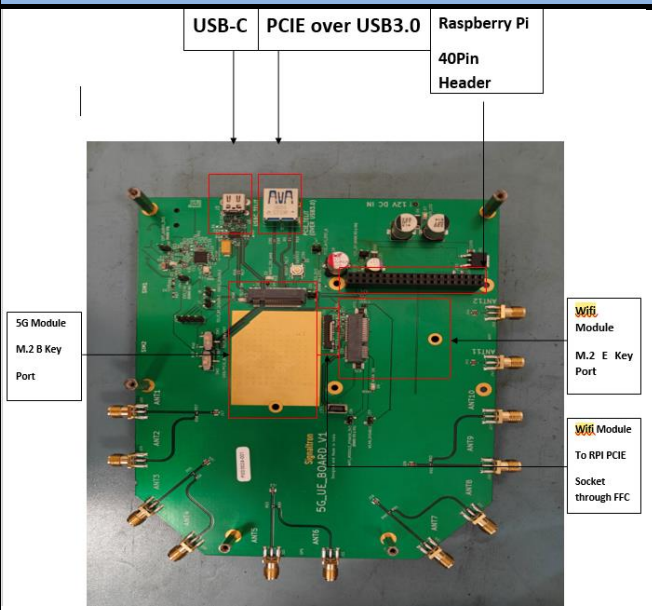
Test ID	4.12.a 5G Evaluation board specifications		
Requirement	5G Evaluation board to support 5G Qualcomm Snapdragon X62/65 or higher Modem-RF System supported		
Test Objective	5G Evaluation board to support 5G Qualcomm Snapdragon X62/65 or higher Modem- RF System supported		
	Test Steps	Acceptance Criteria	Remark
	1. Power up the board and connect with PC using Type C cable. 2. Use ATI AT command to get the 5G Evaluation model details 3. Cross check with Data sheet	ATI FN990A28 From the Product document for FN990A28 (TC_FN990Axx_Product_Brief.pdf) "FN990A28 data card is based on Qualcomm® Snapdragon™ X62 targeting mid-tier market needs"	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.12.b 5G Evaluation board specifications		
Requirement	Cellular Modem-RF Specs: 5x20 MHz carrier aggregation (DL) and above, 100/200 MHz bandwidth(Sub-6 GHz) Optional: 8 carriers(mmWave), 3x20 MHz carrier aggregation (UL), 800 MHz bandwidth(mmwave)		
Test Objective	Cellular Modem-RF Specs: 5x20 MHz carrier aggregation (DL) and above, 100/200 MHz bandwidth(Sub-6 GHz) Optional: 8 carriers(mmWave), 3x20 MHz carrier aggregation (UL), 800 MHz bandwidth(mmwave)		
	Test Steps	Acceptance Criteria	Remark
	1. Check with Data sheet TC_FN990Axx_Product_Brief.pdf for the supported CA and Bandwidth	From the Product document for FN990A28 (TC_FN990Axx_Product_Brief.pdf) For FR1 , following are supported: • 120 MHz, 2CC CA DL • 200 MHz, 3CC CA DL	
Overall Test Result	Pass:□	Fail: □	

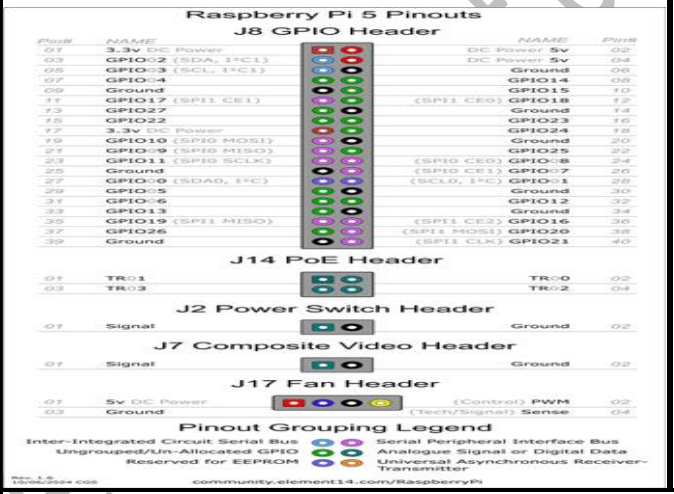
Test ID	4.12.c 5G Evaluation board specifications

Signaltron Confidential. Do not copy

Requirement	Performance Enhancement Technologies: 100 MHz envelope tracking, Adaptive Antenna tuning, Uplink Data compression(UDC),5G Envelope tracking		
Test Objective	Performance Enhancement Technologies: 100 MHz envelope tracking, Adaptive Antenna tuning, Uplink Data compression(UDC),5G Envelope tracking		
	Test Steps	Acceptance Criteria	Remark
	Check with Data sheet	From the qualcomm-snapdragon-x62-5g-modem-rf-system-product-brief.pdf: Qualcomm® Wideband Envelope Tracking (7th gen)	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.12.d Physical and Wi-Fi Interface Module		
Requirement	To verify Physical and Wi-Fi Interface Modules.		
Test Objective	To verify Physical and Wi-Fi Interface Modules.		
	Test Steps	Acceptance Criteria	Remark
	1. Connect 4G/5G Antenna to ANT1&9 2. Point Switch towards the marked pin for USB Boot 3. Turn the module on using the switch 4. Connect module to Raspberry pi via USBC-USBA Cable 5. Check FFC Cable for Raspberry Pi to Wifi Module 6. Connect micro HDMI to HDMI cable from raspberry pi to a monitor 7. Connect a mouse and keyboard to RPI 8. Connect DC Power Supply (12V-5A) 9. Connect earphones for sound 10. Check how to configure each of the peripherals in their respective sections shown in the diagram. This configuration ensures that 5G, wifi and audio systems are working.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

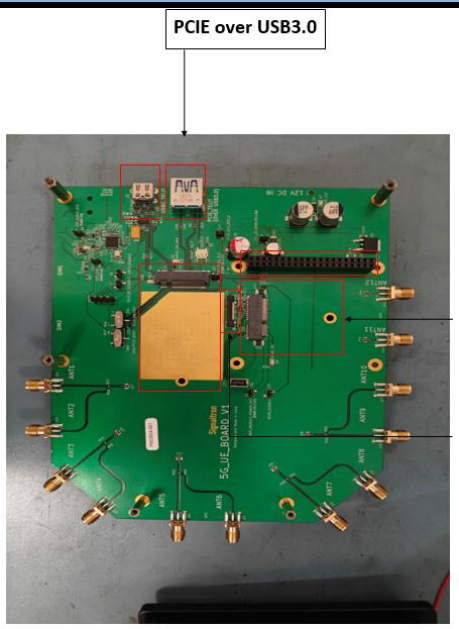
Test ID	4.12.e Peripheral Connectors		
Requirement	Peripheral connectors on the platform support UART,SPI,I2C and GPIO		
Test Objective	Peripheral connectors on the platform support UART,SPI,I2C and GPIO		
	Test Steps	Acceptance Criteria	Remark
	From the Raspberry Pi 5 Pinout data sheet, we can find the connectors for SPI,I2C and GPIO. For UART interface, Tera term utility can be used to configure the baud rate.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Copy

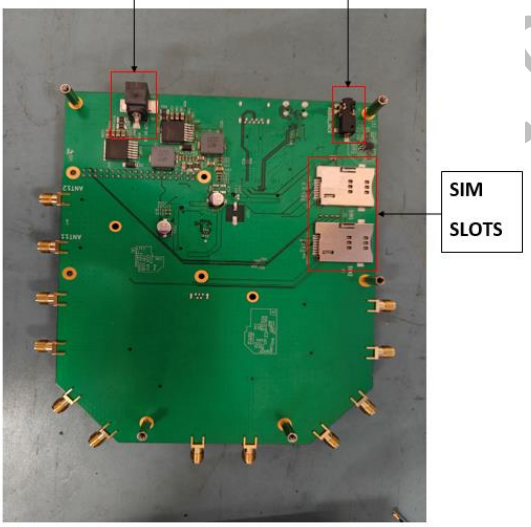
Test ID	4.12.f Sensor devices		
Requirement	Sensor interfaces for medical devices, smart-home appliances and Smart-city applications		
Test Objective	Sensor interfaces for medical devices, smart-home appliances and Smart-city applications		
	Test Steps	Acceptance Criteria	Remark
	Sensor devices can be connected to the Wi-Fi of Evaluation board	Sensor devices can be connected to the Wi-Fi of Evaluation board	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.12.g SD Card Connector		
Requirement	SD Card Connector		
Test Objective	To verify SD Card Connector		
	Test Steps	Acceptance Criteria	Remark
	To verify the SD card Physically		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential - Do not copy

Test ID	4.12.h PCI to USB Connector		
Requirement	PCI to USB Connector		
Test Objective	To verify PCI to USB Connector		
	Test Steps	Acceptance Criteria	Remark
	Verify it physically as shown.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential copy

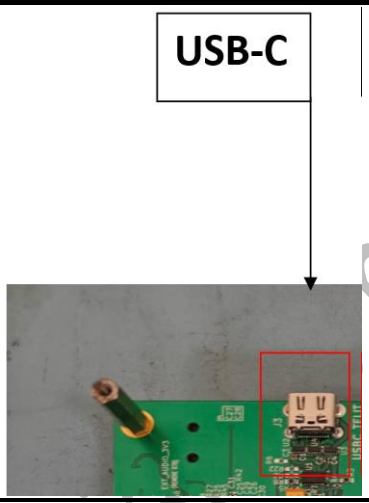
Test ID	4.12.i Dual (U) SIM card supported: 1.8v and 2.95 V		
Requirement	To verify the support for Dual SIM		
Test Objective	To verify the support for Dual SIM		
	Test Steps	Acceptance Criteria	Remark
	Verify it physically as shown.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Copy

Test ID	4.12.j 1 digital audio codec board interface		
Requirement	To verify the support for Audio codec		
Test Objective	To verify the support for Audio codec		
	Test Steps	Acceptance Criteria	Remark
	Options to verify: 1) Verify it physically as shown. 2) Insert Live Air SIM card and through ATD, make VoNR/VoLTE or Voice call and verify		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.12.k COM1 and COM2. Also support main UART and Debug UART		
Requirement	To verify COM1, COM2 ,main UART and Debug UART		
Test Objective	To verify COM1, COM2 ,main UART and Debug UART		
	Test Steps	Acceptance Criteria	Remark
	To verify Physically		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.12.l USB Type-C interface, USB 3.0 & USB 2.0 Supported		
Requirement			
Test Objective			
	Test Steps	Acceptance Criteria	Remark
	To verify Physically		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential - do not copy

Test ID	4.12.m LEDs Indication		
Requirement	To verify LEDs Indication		
Test Objective	To verify LEDs Indication		
	Test Steps	Acceptance Criteria	Remark
	To verify Physically		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.12.n Power Key,Reset Key,USB Boot, Power Switch etc.		
Requirement	To verify Power Key,Reset Key,USB Boot, Power Switch etc.		
Test Objective	To verify Power Key,Reset Key,USB Boot, Power Switch etc.		
	Test Steps	Acceptance Criteria	Remark
	To verify Physically		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.12.o 12 Antenna interfaces		
Requirement	To verify Evaluation board has 12 Antenna interfaces		
Test Objective	To verify Evaluation board has 12 Antenna interfaces		
	Test Steps	Acceptance Criteria	Remark
	To verify Physically	Antennas 11 & 12 are Wifi (2.4 GHz, 5GHz) Antennas 5 & 6 are for GNSS (GPS) Antennas 1,2,3,4,7,8,9 &10 are for 4G/5G.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.12.p Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors		
Requirement	To verify Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors		
Test Objective	To verify Cables, Antenna, Audio earphone, USB Driver, Required modules of Wi-Fi, Ethernet, Audio, PCI TO USB, Power Adaptors		
	Test Steps	Acceptance Criteria	Remark
	To verify Physically		
Overall Test Result	Pass:□	Fail: □	

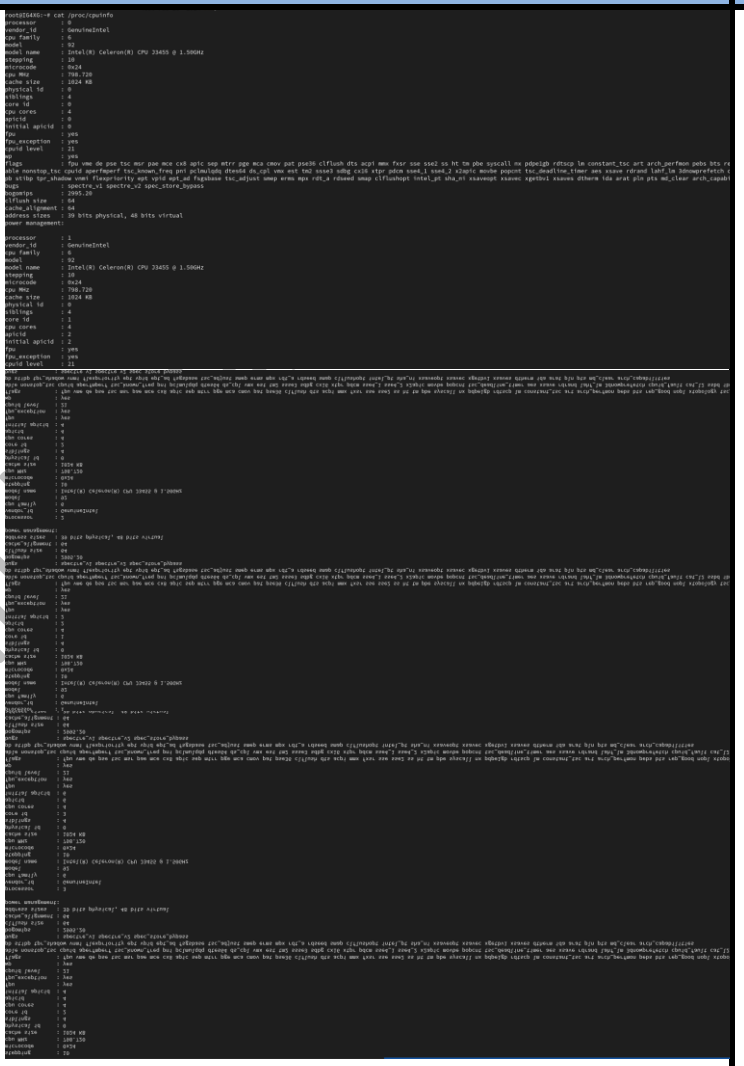
Test ID	4.12.q AT command (external MCU integration) and SDK support (within the module)		
Requirement	To verify AT command (external MCU integration) and SDK support (within the module)		
Test Objective	To verify AT command (external MCU integration) and SDK support (within the module)		
	Test Steps	Acceptance Criteria	Remark
	To send AT Commands to the Module, open terminal, there is a python file kept on the Desktop, type:- **sudo python3 AT_Commands.py**		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential: Do not copy

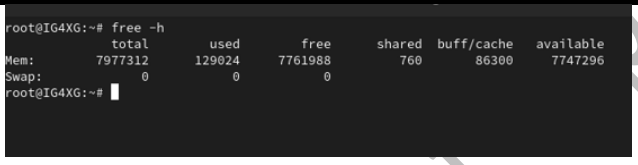
Test ID	4.12.r Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agri tech		
Requirement	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agri tech		
Test Objective	Application MCU Development Board for Applications like Smart Home, Smart City, Medical Devices, Agri tech		
	Test Steps	Acceptance Criteria	Remark
	1.MCU for smart city or medical devices can be configured 2. Monitor or manage it with 5G Evaluation board.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

4.13 IoT Gateway

Test ID	4.13.a IoT Gateway specifications		
Requirement	CPU: Qualcomm or equivalent, Dual core or Higher		
Test Objective	CPU: Qualcomm or equivalent, Dual core or Higher		
	Test Steps	Acceptance Criteria	Remark
	1. There are three ways to connect IoT Gateway to Laptop/PC. you could connect to iot gateway via lan cable, via wifi or via hdmi. 2. Login to IoT Gateway. 3. Access the IOT gateway either through web gui (entering 192.168.11.1 on firefox) or via ssh (ssh -x root@192.168.11.1). Password: ecsd-edge@3682 4. At the terminal execute the command cat /proc/cpuinfo	 IoT Gateway supports 3 processors/Cores as shown with screen shot above.	
Overall Test Result	Pass:□	Fail: □	

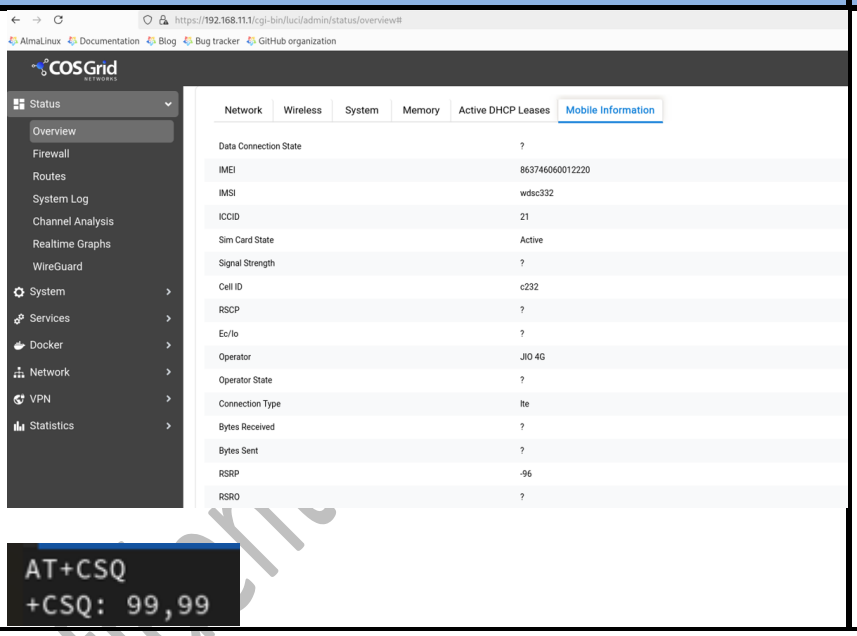
Signaltron Confidential

Test ID	4.13.b RAM		
Requirement	RAM: 256 MB		
Test Objective	RAM: 256 MB		
	Test Steps	Acceptance Criteria	Remark
	1. There are three ways to connect IoT Gateway to Laptop/PC. you could connect to iot gateway via lan cable, via wifi or via hdmi. 2. Login to IoT Gateway. 3. Access the IOT gateway either through web gui (entering 192.168.11.1 on firefox) or via ssh (ssh -x root@192.168.11.1). Password: ecsd-edge@3682 4. At the terminal execute the command cat free -h	 IoT Gateway supports more than 256 MB of RAM.	
Overall Test Result	Pass:□	Fail: □	

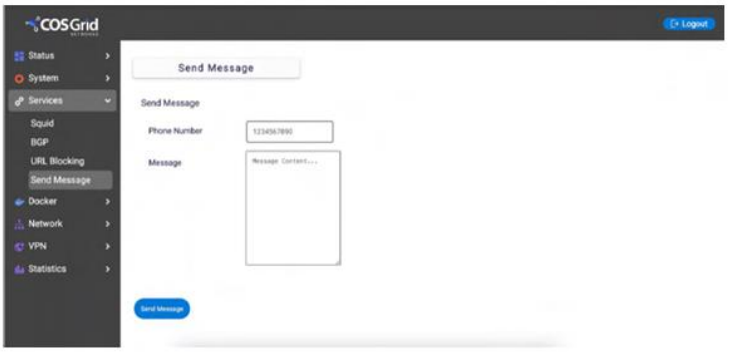
Signaltron Confidential. Do not copy

Test ID	4.13.c: Module :5GSub-6Ghz SA1 /2Gbps DL(4x4MIMO) or higher,900/600Mbps UL(2x2)		
Requirement	Module :5GSub-6Ghz SA1 /2Gbps DL(4x4MIMO) or higher,900/600Mbps UL(2x2)		
Test Objective	Module :5GSub-6Ghz SA1 /2Gbps DL(4x4MIMO) or higher,900/600Mbps UL(2x2)		
	Test Steps	Acceptance Criteria	Remark
	1. Verify from the data sheet	From the Quectel Quectel_RM500U-CN_5G_Specification_V1.0 data sheet: Data Rates (Max.)① 5G SA Sub-6 — 2 Gbps (DL)/ 1 Gbps (UL) Frequency Bands 5G: 5G NR — 3GPP Release 15 NSA/SA operation, Sub-6 GHz 5G NR NSA — n41/ 78/ 79 5G NR SA — n1/ 28/ 41/ 77/ 78/ 79 MIMO — DL 4 × 4 MIMO on n1/ 41/ 77/ 78/ 79	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

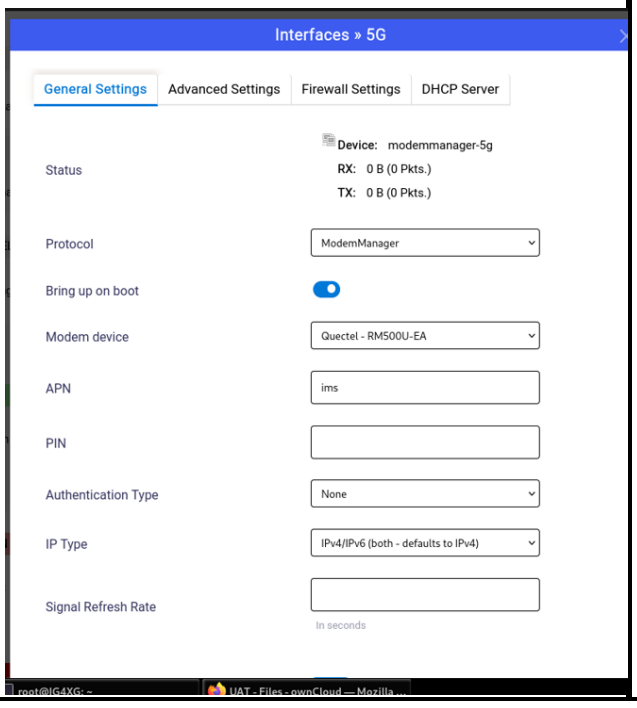
Test ID	4.13.d: Status: Signal strength (RSSI), SINR, RSRP, RSRQ,EC/IO,RSCP Bytes sent/received ,connected band ,IMSI,ICCID.		
Requirement	Status: Signal strength (RSSI), SINR, RSRP, RSRQ,EC/IO,RSCP Bytes sent/received ,connected band ,IMSI,ICCID.		
Test Objective	Status: Signal strength (RSSI),SINR,RSRP,RSRQ,EC/IO,RSCP Bytes sent/received ,connected band ,IMSI,ICCID.		
	Test Steps	Acceptance Criteria	Remark
	1. Verify from the Web GUI 2. Or verify from the AT Command.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential

Test ID	4.13.e: SMS		
Requirement	SMS/Call Status		
Test Objective	SMS/Call Status		
	Test Steps	Acceptance Criteria	Remark
	Insert a commercial SIM card into the device 1. Use AT Command "ATDnumber" to dial a call. 2. Use AT command AT+CMGS for sending SMS. Or In Web GUI Services -> Send message		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential

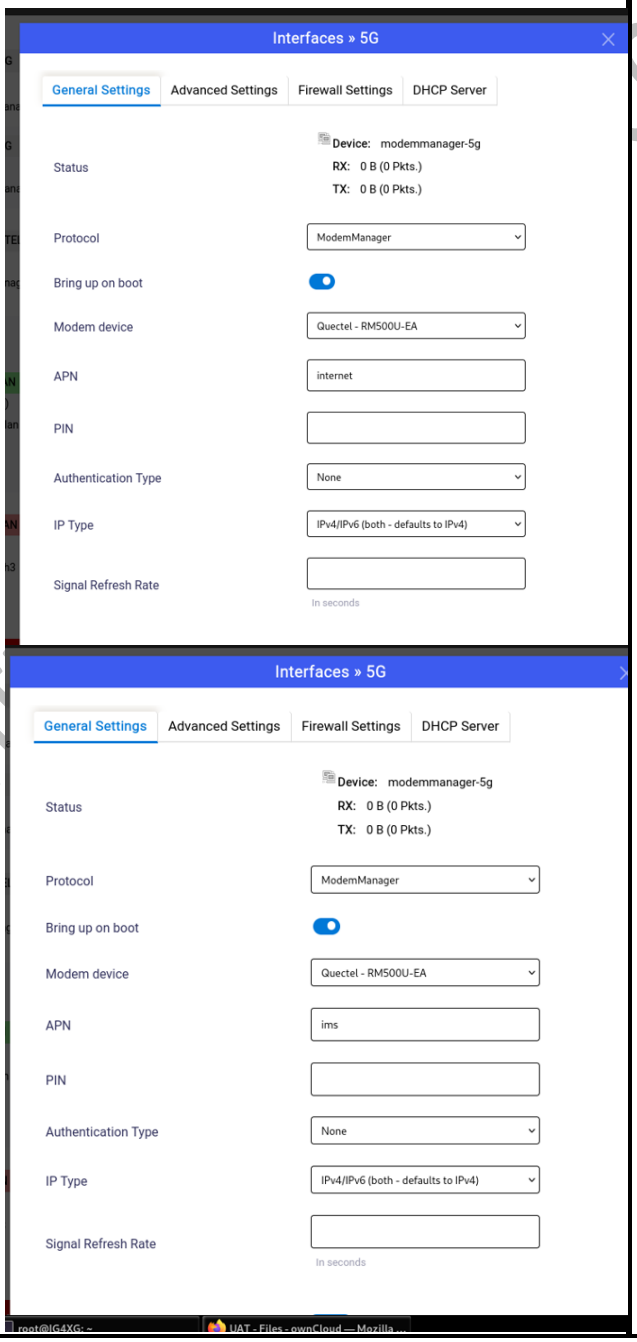
Test ID	4.13.f: USSD		
Requirement	Verify Supports sending and reading Unstructured Supplementary Service Data messages		
Test Objective	Verify Supports sending and reading Unstructured Supplementary Service Data messages		
	Test Steps	Acceptance Criteria	Remark
	1. Insert a commercial SIM card into the device 2. Use AT+CUSD to send USSD command (For eg: barring of incoming calls).		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.13.g: APN		
Requirement	To verify APN setting		
Test Objective	To verify APN setting		
	Test Steps	Acceptance Criteria	Remark
	1. Open the Web GUI 2. Under Network->Interfaces->5G->General Settings, select ModemManager under Protocol. 3. There is an option to edit the APN under this.		

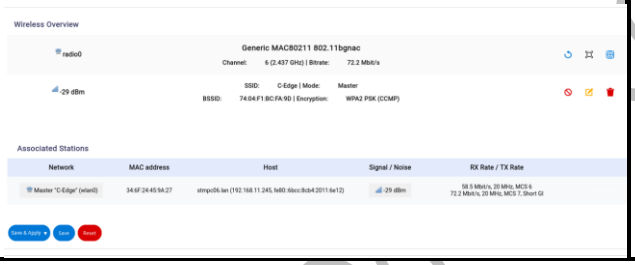
Signaltron Confidential. Do not copy

Overall Test Result	Pass:□	Fail: □

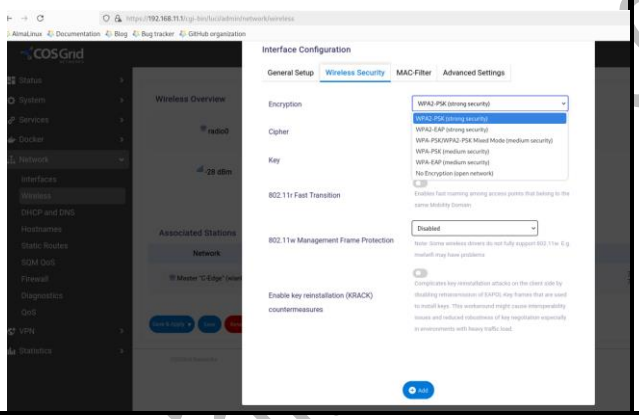
Signaltron Confidential. Do not copy

Test ID	4.13.h: PDNs		
Requirement	Possibility to use different PDNs for multiple network access and services		
Test Objective	Possibility to use different PDNs for multiple network access and services		
	Test Steps	Acceptance Criteria	Remark
	1. Open the Web GUI 2. Under Network->Interfaces->5G->General Settings, select ModemManager under Protocol. 3. There is an option to edit the APN under this. 4. Different/multiple APNs can be configured	 	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Copy

Test ID	4.13.2.a Access points		
Requirement	To verify Supports 802.11b/g/n/ac		
Test Objective	To verify Supports 802.11b/g/n/ac		
	Test Steps	Acceptance Criteria	Remark
	1. Open the Web GUI 2. Under Network->Interfaces->Wireless it can be seen support for 802.11b/g/n/ac		
Overall Test Result	Pass:□	Fail: □	

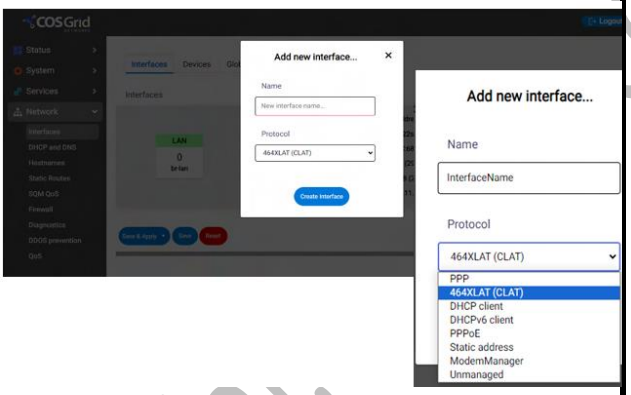
Signaltron Confidential. Do not copy

Test ID	4.13.2.b WiFi Security		
Requirement	WiFi Security: WPA X/WEP/TKIP variants as per the latest version.		
Test Objective	WiFi Security: WPA X/WEP/TKIP variants as per the latest version.		
	Test Steps	Acceptance Criteria	Remark
	1. Open the Web GUI 2. Under Network->Interfaces->Wireless->Interface configuration->Wireless Security Support for WPA Security can be seen.		
Overall Test Result	Pass:□	Fail: □	

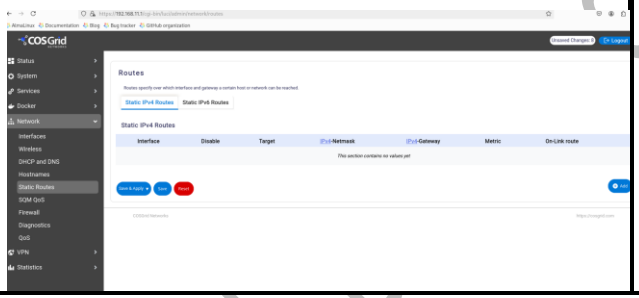
Signaltron Confidential Copy

Test ID	4.13.2.c WiFi – number of users		
Requirement	Support minimum 30 simultaneous Wifi users connection.		
Test Objective	Support minimum 30 simultaneous Wifi users connection.		
	Test Steps	Acceptance Criteria	Remark
	1. Verify in data sheet (Inter Or 2. Connect 30 Wifi Client	It is verified that 30 clients can be connected.	
Overall Test Result	Pass:□	Fail: □	

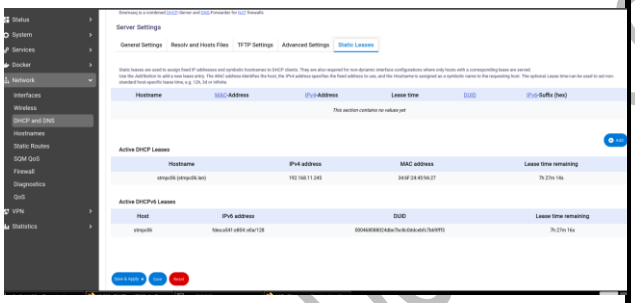
Signaltron Confidential. Do not copy

Test ID	4.13.3.a Network protocols		
Requirement	Support all required network protocols		
Test Objective	Support all required network protocols		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Network -> Interface 2) Select Add Button 3) It will give option where we can enter interface and protocol which is available in protocol drop down box.		
Overall Test Result	Pass:□	Fail: □	

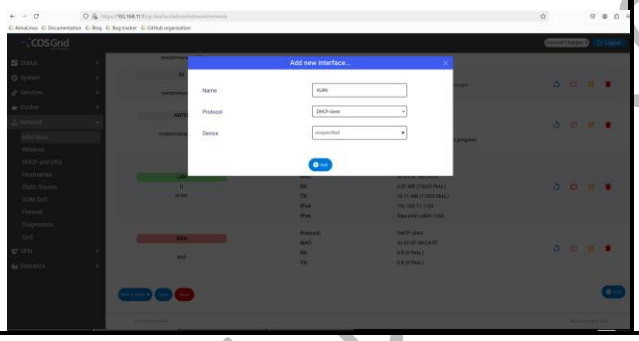
Signaltron Confidential. Copy

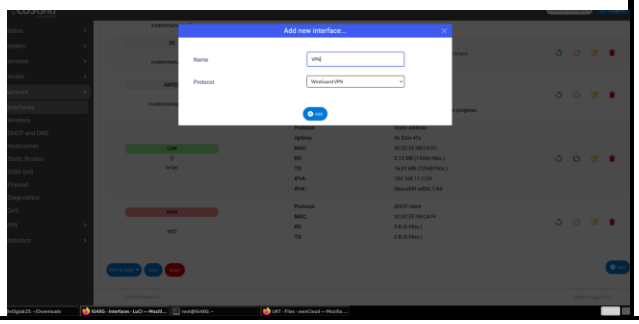
Test ID	4.13.3.b Routing		
Requirement	Support static and dynamic routing		
Test Objective	Support static and dynamic routing		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Network -> Static Routes 2) It gives option to add static IPv4 and IPv6 Routes		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.13.3.c IP allocation		
Requirement	Support static and dynamic IP allocation		
Test Objective	Support static and dynamic IP allocation		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Network -> DHCP and DNS 2) It gives option to assign Static IP address. By default, dynamic IP address allocation is done.		
Overall Test Result	Pass:□	Fail: □	

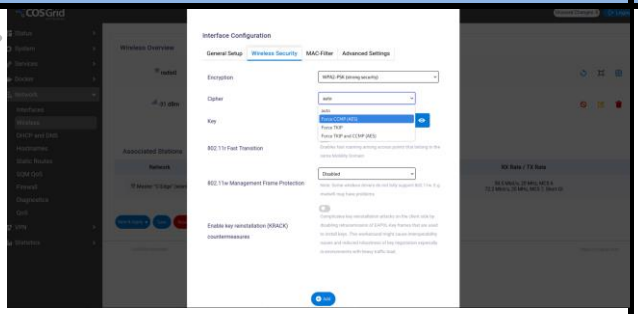
Signaltron Confidential. Do not copy

Test ID	4.13.4.a VLAN		
Requirement	Multiple clients and a server can run simultaneously		
Test Objective	Multiple clients and a server can run simultaneously		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Network -> Interfaces. 2) Add new Interface		
Overall Test Result	Pass:□	Fail: □	

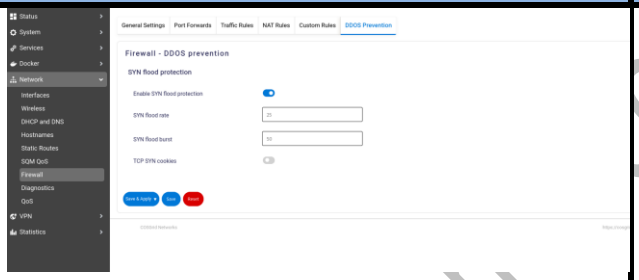
Test ID	4.13.4.b Wire Guard		
Requirement	Wire Guard VPN client and server support		
Test Objective	Wire Guard VPN client and server support		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Network -> Interfaces. 2) Add new Interface 3) In the protocol, select Wire Guard VPN Client		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

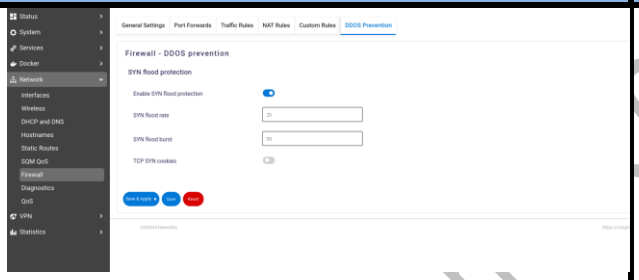
Test ID	4.13.4.c Port and Tag based VLAN Separation		
Requirement	Port and tag-based VLAN Separation		
Test Objective	Port and tag-based VLAN Separation		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Network -> Interfaces.		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.13.4.d		
Requirement	Supports up to 5x VPN IPsec tunnels with different AES/DES encryption methods.		
Test Objective	Supports up to 5x VPN IPsec tunnels with different AES/DES encryption methods.		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Wireless -> Interface configurations and 2) select AES Encryption algorithm from Cipher drop down.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential | Do not copy

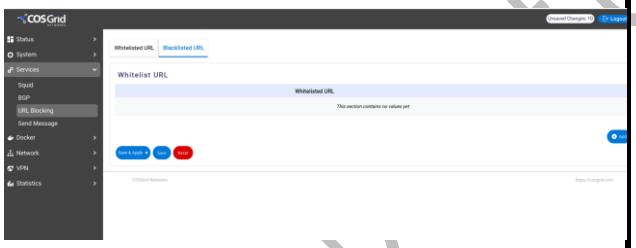
Test ID	4.13.5.a Security		
Requirement	Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI;NAT;NAT-T.		
Test Objective	Pre-configured firewall rules can be enabled via the WebUI, unlimited firewall configuration via CLI;NAT;NAT-T.		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Network -> Firewall in the Web UI 2) Verify the NAT rules can be configured. Or 3) From CLI: vi /etc/config/firewall	 	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Copy

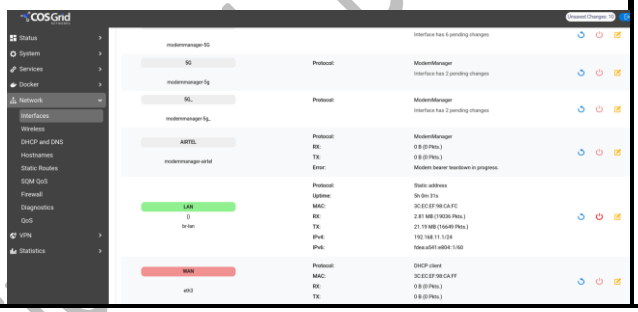
Test ID	4.13.5.b DDOS Prevention		
Requirement	DDOS Prevention (port scan prevention)		
Test Objective	DDOS Prevention (port scan prevention)		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Network -> Firewall in the Web UI 2) Verify DDOS Prevention feature along with various configuration		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.13.5.c Custom limit for SIM card		
Requirement	Sets up custom data limits for SIM card		
Test Objective	Sets up custom data limits for SIM card		
	Test Steps	Acceptance Criteria	Remark
	1)		
Overall Test Result	Pass:□	Fail: □	

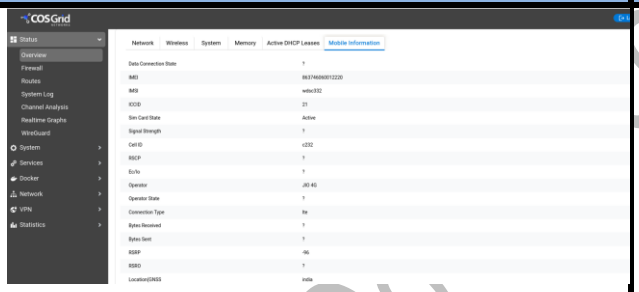
Signaltron Confidential. Do not copy

Test ID	4.13.5.d Black list for blocking out unwanted websites , White list for specifying allowed sites only		
Requirement	To verify Black list for blocking out unwanted websites , White list for specifying allowed sites only		
Test Objective	To verify Black list for blocking out unwanted websites , White list for specifying allowed sites only		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Services ->URL Blocking 2) Under whitelisted URL or Black listed URL, user can required websites.		
Overall Test Result	Pass:□	Fail: □	

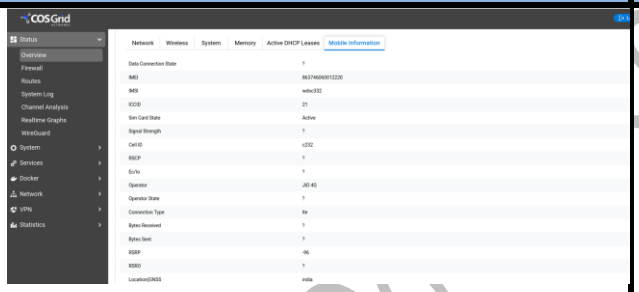
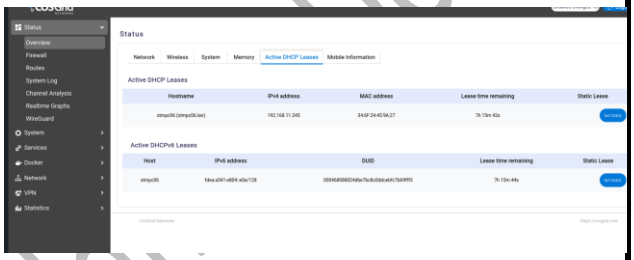
Signaltron Confidential

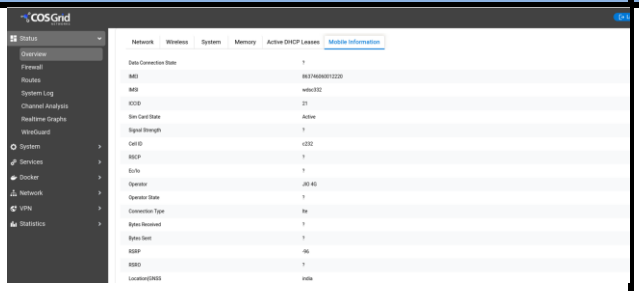
Test ID	4.13.6.a Management		
Requirement	To verify support for Status, Configuration, FW Update ,CLI, trouble shoot ,event log, system log		
Test Objective	To verify support for Status, Configuration, FW Update, CLI, trouble shoot, event log, system log		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Status->Logging 2) Open System logging which helps in troubleshooting. 3) Various other options like Channel analysis, Realtime analysis are provided for troubleshooting.	 	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Copy

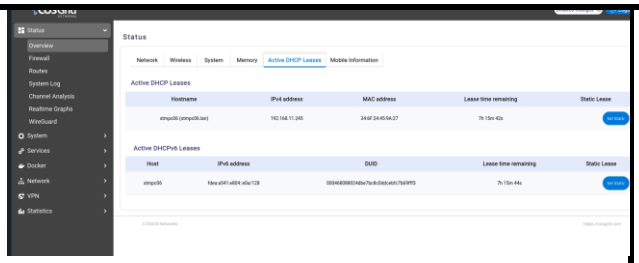
Test ID	4.13.6.b Management		
Requirement	Allows monitoring of: Device data, mobile data, Network info, availability		
Test Objective	Allows monitoring of: Device data, mobile data, Network info, availability		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Overview ->Mobile information 2) All the information are visible there		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do

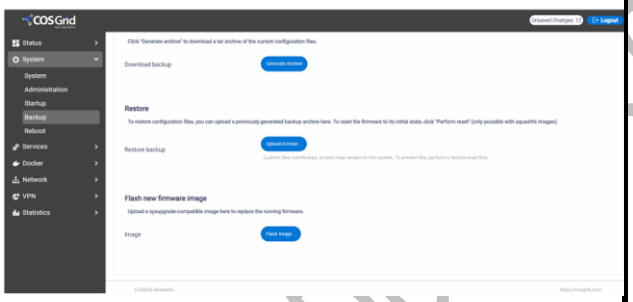
Test ID	4.13.6.c		
Requirement	Allows monitoring of: Device model, Revision and Serial number, Mobile Cell ID,ICCID, IMEI, Connection Type, Operator, Signal Strength, WAN Type and IP		
Test Objective	Allows monitoring of: Device data, mobile data, Network info, availability		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Overview ->Mobile information and Active DHCP Leases 2) All the information are visible there	 	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.13.6.d		
Requirement	Allows monitoring of: WAN Type and IP, Mobile operator Name, Mobile Signal strength, Mobile Network type		
Test Objective	Allows monitoring of: WAN Type and IP, Mobile operator Name, Mobile Signal strength, Mobile Network type		
	Test Steps	Acceptance Criteria	Remark
	1) Goto Overview ->Mobile information and Active DHCP Leases 2) All the information are visible there		

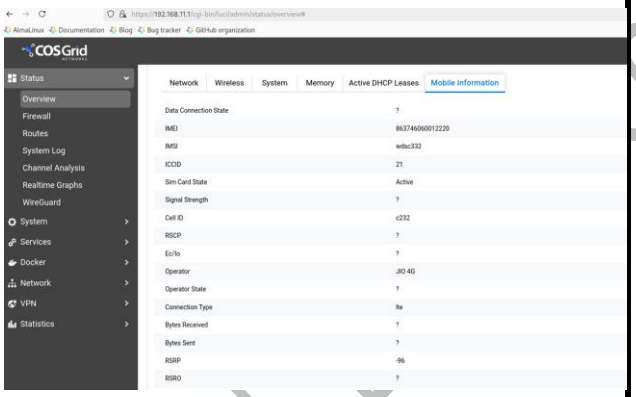
Signaltron Confidential Document Copy

			
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.13.6.e Firmware update from server ,automatic notification		
Requirement	Firmware update from server ,automatic notification		
Test Objective	Firmware update from server ,automatic notification		
	Test Steps	Acceptance Criteria	Remark
	1) Goto System ->Backup 2) Option exists for firmware update.		
Overall Test Result	Pass:□	Fail: □	

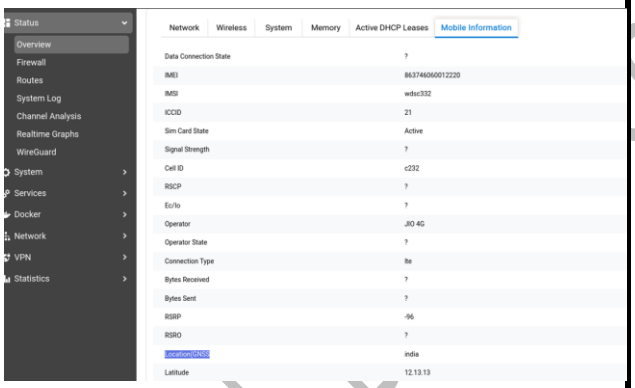
Signaltron Confidential. Do not Copy

Test ID	4.13.6.f Management API over HTTP/HTTPS		
Requirement	Management API over HTTP/HTTPS		
Test Objective	Management API over HTTP/HTTPS		
	Test Steps	Acceptance Criteria	Remark
	1) Management Web Page can be accessed via https://192.168.11.1		
Overall Test Result	Pass:□	Fail: □	

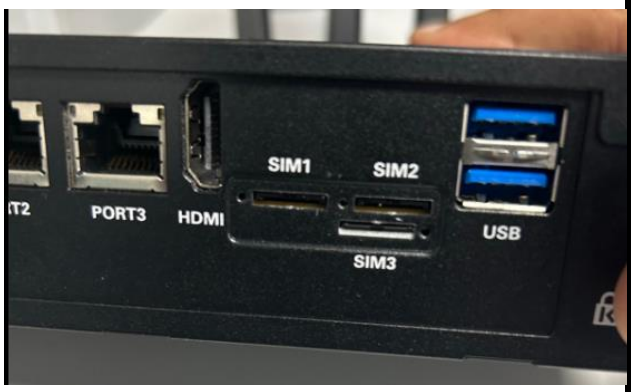
Signaltron Confidential. Do not copy

Test ID	4.13.7.a Supports 1 or more SIMs		
Requirement	Supports 1 or more SIMs		
Test Objective	Supports 1 or more SIMs		
	Test Steps	Acceptance Criteria	Remark
	Verify Physically		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Copy

Test ID	4.13.7.b Supports Location tracking		
Requirement	Supports Location tracking		
Test Objective	Supports Location tracking		
	Test Steps	Acceptance Criteria	Remark
	Verify from Web GUI Overview ->Mobile information ->GNSS		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.13.7.c USB		
Requirement	Supports USB		
Test Objective	Supports USB		
	Test Steps	Acceptance Criteria	Remark
	Verify physically		

Overall Test Result	Pass:□	Fail: □

Test ID	4.13.7.d Supports Digital input and output		
Requirement	Supports Digital input and output		
Test Objective	Supports Digital input and output		
	Test Steps	Acceptance Criteria	Remark
	Supports Digital input/output		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.13.7.e Supports minimum 4 nos 10/100/1000 Ethernet ports.		
Requirement	Supports minimum 4 nos 10/100/1000 Ethernet ports.		
Test Objective	Supports minimum 4 nos 10/100/1000 Ethernet ports.		
	Test Steps	Acceptance Criteria	Remark
	Verify Physically		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.13.7.f		
Requirement	Supports 1G WAN Support		
Test Objective	Supports 1G WAN Support		
	Test Steps	Acceptance Criteria	Remark
	Verify Physically		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.13.7.g

Signaltron Confidential. Do not copy

Requirement	Supports Status LED		
Test Objective	Supports Status LED		
	Test Steps	Acceptance Criteria	Remark
	Verify Physically		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.13.7.h		
Requirement	Supports PoE and DC power socket		
Test Objective	Supports PoE and DC power socket		
	Test Steps	Acceptance Criteria	Remark
	Verify Physically		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Do not copy

Signaltron Confidential. Do not copy

4.14 5G Mini Drone

Test ID	4.14 (a) 5G enabled and controlled drone (m) 5G Modem (n78 band)		
Requirement	To Check Drone is integrated into the System and supports 5G Modem (n78 band)		
Test Objective	To Check Drone is integrated into the System and supports 5G Modem (n78 band)		
	Test Steps	Acceptance Criteria	Remark
	Step-1: Verify the 5G network is on N78 band only. Step-2: Insert the 5G SIM into the drone and Power ON the drone by inserting the battery. Step-3: The drone will automatically send the Registration message to the 5G network. After successful attach and IP assignment, Open the application to check drone data.	All the drone data - 1. 3D Map Data. 2. Video data. 3. Drone Telemetry data should be available.	It is verified Drone is integrated and supporting Band 78
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.14 (b) Supports 5G nano SIM (c) Connectivity Options: Cellular (5G) and **Wi-Fi** for ubiquitous and long-range connectivity (o) **Wi-Fi** (2.4/5 **GHz)**		
Requirement	Verify Drone supported Nano Sim and (2.4/5 **GHz)**		
Test Objective	To verify support of 5G Nano Sim and 5G enabled and controlled and **Wi-Fi** for ubiquitous and long-range connectivity		
	Test Steps	Acceptance Criteria	Remark
	Step-1 : Take a 5G Nano SIM and Insert into the drone SIM card slot. Step-2: Check for the drone connection and information being displayed Wifl Step-1: Tum ON the Drone and wait for the drone to initialize. Step-1: Connect to drone WiFi. Step-2: Check drone data same as 5g.	**Check the below in UE logs** Successful insertion of 5G Nano SIM in SIM Slot of5G Communication Module of Drone. Successful connection and display of drone data on the screen. The display data will be same as 5g setup above.	Successful insertion of 5G Nano SIM in SIM Slot of5G and Wi Fi supported
Overall Test Result	Pass:□	Fail:□	

Signaltron Confidential. Do not copy

Test ID	4.14 (e) Autonomy: Visual Inertial Odometry (VIO), path planning, PX4, GPS-denied navigation, BVLOS, follow me.		
Requirement	Verify To Check Drone Autonomy		
Test Objective	To Check Drone Autonomy		Remark
Description	Test Steps	Acceptance Criteria	
	Step-1: Connect the drone. Step-2: Select Indoor mode with non gps setting. Step-3: Use Lidar, Vi feed and display data to control drone.	Check VIO status and display data. Using data the drone can be control without direct view. The Lidar and camera map shows drone surrounding.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not co

Test ID	4.14 (f) 360 obstacle avoidance Depth estimation, obstacle detection, mapping and VOA		
Requirement	360 obstacle avoidance, Depth estimation, obstacle detection, mapping and VOA (Clause 4.14 (f))		
Test Objective	To Verify Drone Obstacle Avoidance and Mapping		Remark
	Test Steps	Acceptance Criteria	
	Step-1: Place the drone on the floor. With enough open space. Step-2: Connect the drone. Step-3: The lidar map data is shown live to check for obstacles and terrain. Step-4: Fly drone when go signal is given in software.	360 obstacle avoidance, Depth Estimation and obstacle detection: Before arming the drone a test object can be placed within a distance of 1m around the drone for 360 deg check. The drone will detect it and give a warning on the map. Take off the drone to 1-1.2 m altitude after no object is around 2m. The mapping algorithm will show surroundings of the drone as it takes off. A test object can be brought close to the drone and it will back off once a threshold is crossed by the object. All sensor data is visible for flight and control.	
Overall Test Result	**Pass:**	Fail:	

Signaltron Confidential. Do not copy

Test ID	**4.14 (g) Payload Capacity - 500g/1 Kg or above**		
Requirement	To Check Payload Capacity		
Test Objective	To Check Payload Capacity		Remark
	Test Steps	Acceptance Criteria	
	Step-1: Take the drone outdoors. Step-2: Attach the 500gm Payload and Turn on the Drone Step-3: Wait for the drone to initialize. Step-4: Takeoff the Drone.(Read Proper Manual Before Flying) Step-5: Land the Drone	Drone Takes off up to a height of 1.2m and hovers in its place.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.14 (h) GPS or **NAVIC** enabled		
Requirement	To CheckGPS		
Test Objective	To verify GNSS Capabilities		Remark
	Test Steps	Acceptance Criteria	
	Step-1: Connect the drone. Step-2: Use software and manual to do flight planning. Save config. Step-3: Place drone outside far from trees and wire lines, read manual before flight. (wait for gps lock before start.) Step-4: Use on board start button to execute flight. Step-5: Once complete land drone.	The drone should have a GPS lock which will be indicated. Drone will fly with given GPS accuracy and execute the flight path.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.14 (h) Geo fencing		
Requirement	To Check Geo Fencing		
Test Objective	To Check Geo Fencing		Remark
	Test Steps	Acceptance Criteria	
	Step-1: Connect the drone. Step-2: Use software to fence area to avoid and save details. Step-3: Place drone outside far from trees and wire lines, read manual before flight. (wait for gps lock before start.) Step-4: Fly the drone and land drone.	The drone will avoid fenced gpd areas with in accuracy limits and will give warning.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.14 (k) Tracking sensor (I) Image Sensor		
Requirement	To Check Sensors		
Test Objective	To Check Tracking sensor and Image Sensor		Remark
	Test Steps	Acceptance Criteria	
	Step-1: The drone should be placed in an outdoor environment where GPS Signals are uninterrupted. Step-2: Fly using any of the chosen modes and check the lidar and camera data.	After GPS Fix, fly drone. The Live Stream of the drone camera will be displayed.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

4.15 XR(AR/VR)

Test ID	4.15.1.a XR(AR/VR) Device Specifications		
Requirement	Chipset:2.0 GHz 8-core Qualcomm		
Test Objective	Chipset:2.0 GHz 8-core Qualcomm		
	Test Steps	Acceptance Criteria	Remark
	Verify From the AjnaXR Data sheet Qualcomm XR2+ Gen 1 CPU Octa-core Kryo 585		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

<table>
<tr><td>Test ID</td><td colspan="3">4.15.1.b XR(AR/VR) Device Specifications</td></tr>
<tr><td>Requirement</td><td colspan="3">Memory: 64 GB Internal storage/4GB RAM/Micro SD slot</td></tr>
<tr><td>Test Objective</td><td colspan="3">Memory: 64 GB Internal storage/4GB RAM/Micro SD slot</td></tr>
<tr><td></td><td>Test Steps</td><td>Acceptance Criteria</td><td>Remark</td></tr>
<tr><td></td><td>Verify from the data sheet</td><td><table><tr><td>Storage</td><td>128GB</td></tr><tr><td>RAM</td><td>8GB</td></tr></table></td><td></td></tr>
<tr><td>Overall Test Result</td><td>Pass:□</td><td colspan="2">Fail: □</td></tr>
</table>

Signaltron Confidential. Do not copy

Test ID	4.15.1.d XR(AR/VR) Device Specifications		
Requirement	Port: USB Type C and Audio		
Test Objective	Port: USB Type C and Audio		
	Test Steps	Acceptance Criteria	Remark
	Visual inspection. USB Type C port can be located.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.15.2.a Bluetooth		
Requirement	Bluetooth 5.0 Should be supported		
Test Objective	Bluetooth 5.0 Should be supported		
	Test Steps	Acceptance Criteria	Remark
	Verify from the data sheet	Bluetooth 5	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.15.2.b Wi-fi		
Requirement	802.11a/b/g/n/ac- 2.4GHz and 5GHz		
Test Objective	Wifi Range-~25meters		
	Test Steps	Acceptance Criteria	Remark
	Verify from the data sheet and also connect to companion device to stream the video	From data sheet device supports Wi-Fi 6 which supports both 2.4 and 5 GHz : Wi-Fi 6	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Do not Copy

Test ID	4.15.2.d 3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass)		
Requirement	3 IMUs (including 3-axis accelerometers, gyroscopes, eCompass)		
Test Objective			
	Test Steps	Acceptance Criteria	Remark
	Verify visually		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.15.3.a Display:24°field-of-view, 24-bitcolor LCD ,outdoor visible ,HD resolution		
Requirement	Display:24°field-of-view, 24-bitcolor LCD ,outdoor visible ,HD resolution		
Test Objective			
	Test Steps	Acceptance Criteria	Remark
	Verify from data sheet	Resolution: 3200*1600 Refresh Rate: 90Hz Fov: 95°~105° PPI: 1058	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential - Do not copy

Test ID	4.15.3.b Microphone		
Requirement	Microphone		
Test Objective	Microphone		
	Test Steps	Acceptance Criteria	Remark
	Visual inspection		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

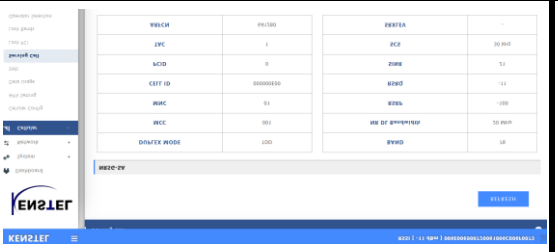
Test ID	4.15.3.c Speaker		
Requirement	Speaker: Internal 94 dBA loudspeaker		
Test Objective	Speaker: Internal 94 dBA loudspeaker		
	Test Steps	Acceptance Criteria	Remark
	Visual inspection		
Overall Test Result	Pass:□	Fail: □	

4.16 5G Indoor CPE

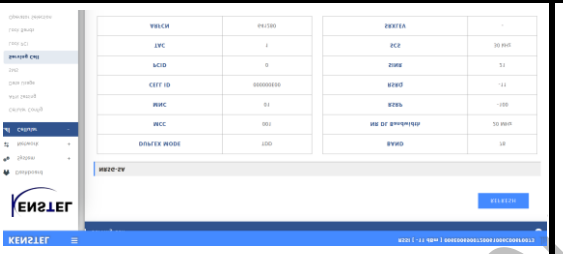
Test ID	4.16.1 Processor - Qualcomm or equivalent (a) CPU Clock Speed 1.0GHz or higher (b) CPU Cores Dual-core Cortex-A53 Arm or equivalent		
Requirement	To verify Processor, Clock speed and ARM Core		
Test Objective	To verify Processor, Clock speed and ARM Core		Remark
	Test Steps	Acceptance Criteria	
	Verify the from the data sheet for KCP-5G-510I Indoor 5G CPE.	From the data sheet Qualcomm® 1Ghz MHz Dual-Core CPU | ARM Cortex A53	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.16.2 Memory: 512 **MB RAM** or higher		
Requirement	To verify Memory: 512 **MB RAM** or higher		
Test Objective	Verify RAM Space		Remark
	Test Steps	Acceptance Criteria	
	Verify the from the data sheet for KCP-5G-510I Indoor 5G CPE.	From the data sheet: Memory 512MB RAM | 256MB NAND FLASH	Verify that RAM detail having 512 MB
Overall Test Result	Pass:□	Fail: □	

Test ID	4.16.3.a 3GPP Release		
Requirement	3GPP Release 15 or above support		
Test Objective	3GPP Release 15 or above support		Remark
	Test Steps	Acceptance Criteria	
	Verify if the CPE registers successfully to 5G SA network. Registering to 5G SA indicates support for Rel 15		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.16.3.b. Sub-6 Band n78:TDD		
Requirement	Sub-6 Band n78:TDD to be supported		
Test Objective	N78 Band to be supproted		Remark
	Test Steps	Acceptance Criteria	
	Verify if the CPE registers successfully to 5G SA network in band n78. Check the band registered in Kenstel Web GUI as shown.		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.16.3.c 5G Modem		
Requirement	5G Modem: Snapdragon SDX62/65 or Equivalent		
Test Objective	N78 Band to be supported		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet	TECHNICAL SPECIFICATION Processor Qualcomm® 1Ghz MHz Dual-Core CPU | ARM Cortex A53 **Snapdragon X62 modem** Memory 512MB RAM | 256MB NAND FLASH	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

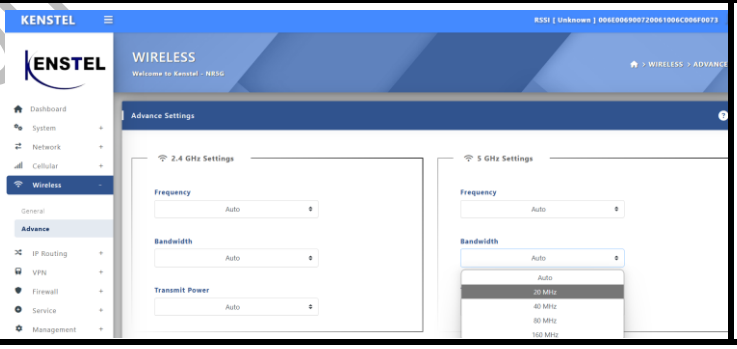
Test ID	4.16.3.d Bandwidth Support		
Requirement	Bandwidth support: 20/40/60/80/100 MHz		
Test Objective	Bandwidth support: 20/40/60/80/100 MHz		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet	From the data sheet: **5G** ❖ 5G Technology: 5G NR FDD, 5G NR TDD, SA, NSA[19] ❖ 5G Spectrum: mmWave, sub-6 GHz, 5G/4G spectrum sharing ❖ 5G Modes: FDD, TDD, SA NSA ❖ 5G mmWave : 800 MHz bandwidth, 8 carriers, 2x2 MIMO ❖ 5G sub-6 GHz : 200 MHz bandwidth, 4x4 MIMO ❖ 5G Peak Download Speed: 7500 Mbit/s ❖ 5G Peak Upload Speed: 3000 Mbit/s ❖ 5G RF: 100 MHz envelope tracking, Adaptive antenna tuning ❖ Performance Enhancement Technologies: Qualcomm 5G PowerSave, Qualcomm Signal Boost, Qualcomm Smart Transmit technology, Qualcomm RF Gaming Mode Boost, Qualcomm Wideband Envelope Tracking	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

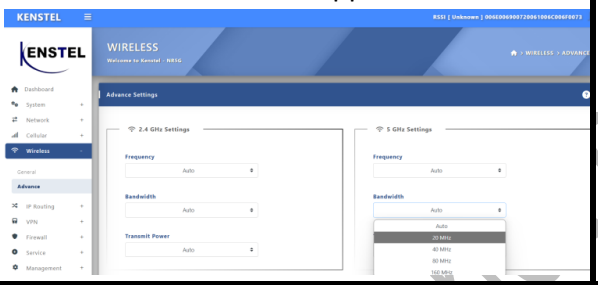
Test ID	4.16.3.e MIMO		
Requirement	MIMO 4x4 or higher		
Test Objective	MIMO 4x4 or higher		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet	From the data sheet: **Kenstel KCP-5G-510I** is a two-radio, 4x4 MIMO 802.11ax 5G CPE. Designed for general purpose, next-generation deployments in harsh outdoor locations and industrial I conditions, the KCP-5G-510I offers performance, enterprise-grade security, and intuitive management. The KCP-5G-510I delivers a maximum 5.4 Gbps aggregate frame rate with concurrent 2.4 GHz and 5 GHz radios. KCP-5G-510I delivers the high throughput, reliability, and flexibility required by the most demanding business applications like voice and high-definition streaming video, even in the harshest outdoor environments	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.16.3.e Download speed		
Requirement	Download speed : Up to 1000 mbps		
Test Objective	Download speed : Up to 1000 mbps		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet	From the data sheet: ❖ 5G Peak Download Speed: 7500 Mbit/s ❖ 5G Peak Upload Speed: 3000 Mbit/s	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.16.5.a Wireless		
Requirement	AP Type: Indoor, dual radio, 2.4,5-GHz		
Test Objective	AP Type: Indoor, dual radio, 2.4,5-GHz		Remark
	Test Steps	Acceptance Criteria	
	Goto Wireless->Advanced General on the Kenstel Web GUI		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.16.5.b Dynamic Frequency Selection		
Requirement	Dynamic Frequency Selection		
Test Objective	Dynamic Frequency Selection GHz		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet or Web GUI Goto Wireless->Advanced General on the Kenstel Web GUI	2.4 GHz or 5GHz can be supported. 	
Overall Test Result	Pass:□	Fail: □	

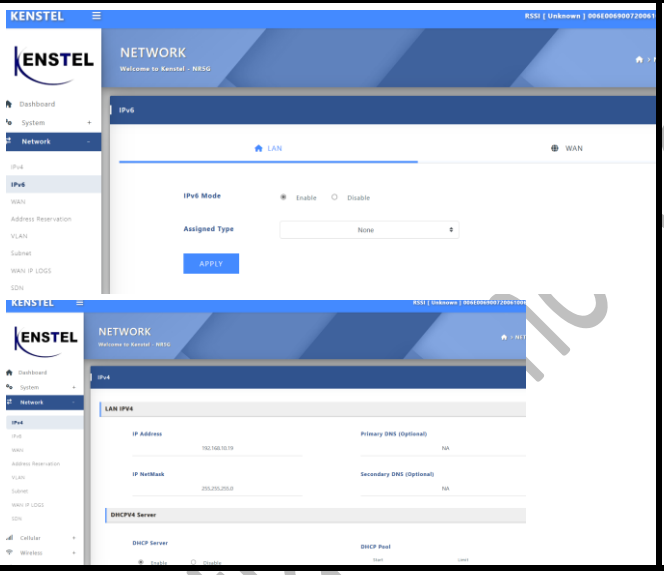
Test ID	4.16.5.c Standards: IEEE802.11a/b/g/n/acwave2		
Requirement	Standards: IEEE802.11a/b/g/n/acwave2		
Test Objective	Standards: IEEE802.11a/b/g/n/acwave2		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet	From the data sheet ❖ IEEE 802.11a/b/g/n/ac/ax compliant ❖ 2.4GHz and 5GHz concurrent radios	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.16.5.d: Wireless MIMO Support	
Requirement	2x2 MU-MIMO with 2 spatial streams	
Test Objective	2x2 MU-MIMO with 2 spatial streams	Remark
	Test Steps: Verify from the data sheet	Acceptance Criteria: From the data sheet **Supported Radio Technologies** 802.11b: Direct-Sequence Spread Spectrum (DSSS) 802.11a/g/n/ac/ax: Orthogonal Frequency-Division Multiplexing (OFDM) 802.11n/ac/ax: 4x4 MIMO with 4 Streams
Overall Test Result	Pass:□	Fail: □

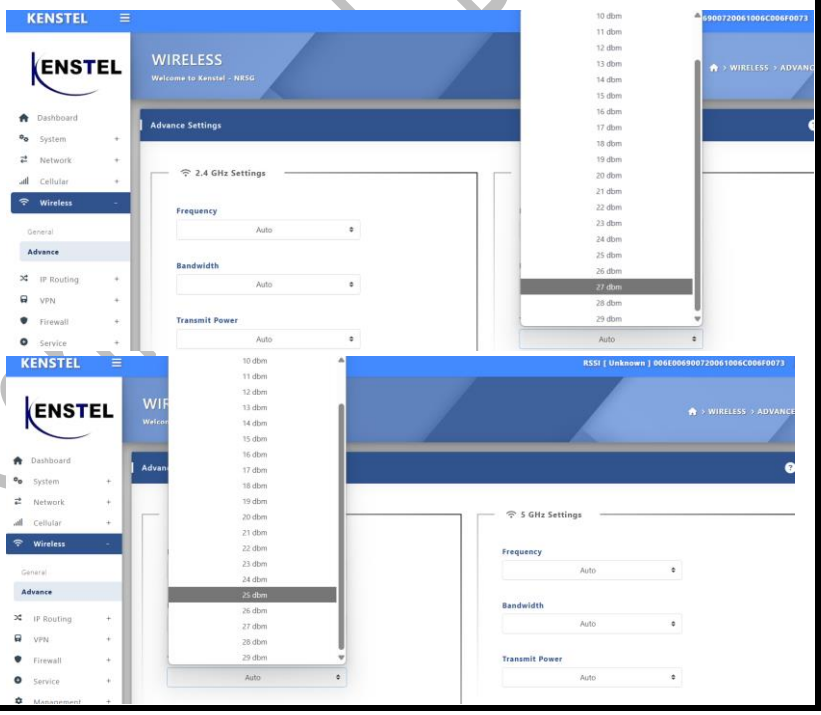
Test ID	4.16.5.e: Wireless PHY rate	
Requirement	PHY Rate: 500 Mbps (2.4GHz) 2048 Mbps(5 GHz)	
Test Objective	PHY Rate: 500 Mbps (2.4GHz) 2048 Mbps(5 GHz)	Remark
	Test Steps: Verify from the data sheet	Acceptance Criteria: From the data sheet **WiFi** ❖ 802.11b/g/n/ac/ax. 2.4GHz Wi-Fi2x2 MIMO up to 600Mbps,5GHzWi-Fi 4x4MIMO up to 4.8Gbps.
Overall Test Result	Pass: □	Fail: □

Signaltron Confidential | Do not copy

Test ID	4.16.5.f: IPv4/IPv6 support		
Requirement	IPv4 and IPv6 dual stack support		
Test Objective	IPv4 and IPv6 dual stack support		Remark
	Test Steps	Acceptance Criteria	
	In Web GUI for CPE, Under Network, Check for IPv4 and IPv6 support		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.16.6.a: Wireless Antenna		
Requirement	Integrated Omni directional Antenna		
Test Objective	Integrated Omni directional Antenna		Remark
	Test Steps	Acceptance Criteria	
	Check from the data sheet for Antenna details	Antenna WLAN :Four (4) Internal 3/5 dBi Dual-Concurrent Omni-Directional Antenna| N-Type WWAN: Four (4) Internal 5dBi dBi Wide BAnd Omni-Directional Antenna WWAN MMWAVE: QTM527 with 64 dual polarization antenna elements capable of transmitt power of more than 40dBm (Power Class 1)	
Overall Test Result	Pass: □	Fail: □	

Signaltron Confidential Copy

Test ID	4.16.6.a: Transmit power		
Requirement	TransmitPower: • 25dBm on 2.4GHz; • · 25dBm on 5GHz		
Test Objective	Integrated Omni directional Antenna		Remark
	Test Steps	Acceptance Criteria	
	Check from the data sheet for Antenna details And also from Web GUI: Wireless> Advanced	Transmit Power 2.4 GHz: 26 dBm | 5 GHz: 26 dBm From Web GUI: 	
Overall Test Result	Pass:□	Fail: □	

Signaltron (... Do not copy

Test ID	4.16.6.a: Receiver Sensitivity	
Requirement	Supports-95dBm or better Receiver Sensitivity	
Test Objective	Supports -95dBm or better Receiver Sensitivity	Remark
	Test Steps / Acceptance Criteria	
Overall Test Result	Pass:□	Fail: □

Test ID	4.16.6.a: RF Management	
Requirement	Supports RF Management	
Test Objective	Supports RF Management	Remark
	Test Steps	Acceptance Criteria
	Verify from the data sheet	❖ 5G RF: 100 MHz envelope tracking, Adaptive antenna tuning ❖ Performance Enhancement Technologies: Qualcomm 5G PowerSave, Qualcomm Signal Boost, Qualcomm Smart Transmit technology, Qualcomm RF Gaming Mode Boost, Qualcomm Wideband Envelope Tracking
Overall Test Result	Pass:□	Fail: □

Signaltron Confidential | Do not copy

Test ID	4.16.6.a: RF Control Plane		
Requirement	Intelligent RF control plane for self-healing and self-optimization		
Test Objective	Intelligent RF control plane for self-healing and self-optimization		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet	❖ 5G RF: 100 MHz envelope tracking, Adaptive antenna tuning ❖ Performance Enhancement Technologies: Qualcomm 5G PowerSave, Qualcomm Signal Boost, Qualcomm Smart Transmit technology, Qualcomm RF Gaming Mode Boost, Qualcomm Wideband Envelope Tracking	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.16.7.c Security: All version and latest WPA Support		
Requirement	All version and latest WPA Support		
Test Objective	All version and latest WPA Support		Remark
	Test Steps	Acceptance Criteria	
	Verify from Kenstel Web GUI : Wireless > General Settings	Support for WPA-PSK Encryption algorithm can be verified. 	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not

Test ID	4.16.7.c Security: IPSec,PPTP,IP-Filtering		
Requirement	IPSecurity (IPSec),PPTP, IP-Filtering		
Test Objective	IPSecurity (IPSec),PPTP, IP-Filtering		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet	❖ VPN client service (L2TP, PPTP)	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.16.7.g MAC address authentication		
Requirement	MAC address authentication		
Test Objective	MAC address authentication		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet. Also in Web GUI: Firewall >Anti ARP Spoofing, there is an option to bind MAC address which helps in MAC address collision	**Wireless Security** WPA2 AES-PSK/WPA2 Enterprise Hide SSID in Beacons MAC Address Filtering, Up to 32 MACs per SSID Wireless STA (Client) Connected List Https SSH Client Isolation	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.16.8.a Interface		
Requirement	2x1000 Base-T Ethernet		
Test Objective	2x1000 Base-T Ethernet		Remark
	Test Steps	Acceptance Criteria	
	Verify from data sheet	**Physical Interface** 1x 10/100/1000/2500 BASE-T, RJ-45 Ethernet Port 1x 10/100/1000 BASE-T, RJ-45 Ethernet Port	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.16.8.b SIM Slot		
Requirement	1X SIM card slot (Nano-SIM)		
Test Objective	1X SIM card slot (Nano-SIM)		Remark
	Test Steps	Acceptance Criteria	
	physical verification		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential, Do not Copy

Test ID	4.16.8.c POE	
Requirement	Power on Ethernet or DC Power	
Test Objective	Power on Ethernet or DC Power	Remark
	Test Steps	Acceptance Criteria
	From the data sheet, Physical verification or Web GUI	Power Source Power-over-Ethernet: 802.3af/at or Proprietary 48V |IEEE 802.11e Compliant Source| Active Ethernet (PoE)
Overall Test Result	Pass:□	Fail: □

Test ID	4.16.9 a Management	
Requirement	Management: Standalone (via GUI) or through on premise based solution or cloud-based	
Test Objective	Management: Standalone (via GUI) or through on premise based solution or cloud-based	Remark
	Test Steps	Acceptance Criteria
	The management wepage is accessible via the gateway ip of the CPE either via the ethernet or wifi connectivity	
Overall Test Result	Pass:□	Fail: □

Test ID	4.16.9 c IEEE 802.11e Standard	
Requirement	Compliant with IEEE 802.11e Standard	
Test Objective	Compliant with IEEE 802.11e Standard	

Signaltron Confidential. Do not copy

	Test Steps	Acceptance Criteria	Remark
	Verify from the data sheet	QoS (Quality of Service) Compliant with IEEE 802.11e Standard | WMM	
Overall Test Result	Pass:□	Fail: □	

Test ID	4.16.9 d Intelligent RF Control Plane for self-healing and Self-Optimization		
Requirement	Intelligent RF Control Plane for self-healing and Self-Optimization		
Test Objective	Intelligent RF Control Plane for self-healing and Self-Optimization		Remark
	Test Steps	Acceptance Criteria	
	Verify from the data sheet	❖ Self-configuring, Self-healing mesh	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential Do not copy

4.17 5G Camera

Test ID	4.17.1 Advanced AI/ML Video analytics	
Requirement	On edge video analytics	
Test Objective	To check edge AI	Remark
	Test Steps	Acceptance Criteria
	1. Open Camera on Web. 2. Add face in database 3. Then ask added person to come in front of camera 4. It should show the percentage of similarity	
Overall Test Result	Pass:□	Fail:□

Signaltron Confidential. Do not co

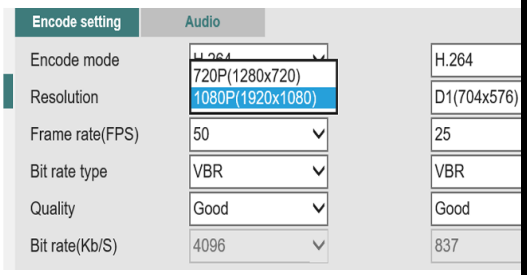
Test ID	4.17.2 5G enabled for private network		
Requirement	4.17.2 5G enabled for private network • Supports Sub-6 Bands • FR-1, n78		
Test Objective	4.17.2 5G enabled for private network • Supports Sub-6 Bands • FR-1, n78		Remark
	Test Steps	Acceptance Criteria	
	Camera support N78 band,it can be verified by attaching camera over N78 on the test network. Band frequency can also be viewed by Opening WEBUI and check the connected cell info.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not c

Test ID	4.17.3 SIM Card Supported: Nano SIM		
Requirement	4.17.3 SIM Card Supported: Nano SIM		
Test Objective			Remark
	Test Steps	Acceptance Criteria	
	Nano SIM card can be inserted and verified.		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not cop

Test ID	4.17.4 Interface	
Requirement	10/100/1000 Ethernet port. Audio Port Alarm Port	
Test Objective	10/100/1000 Ethernet port. Audio Port Alarm Port	Remark
	Test Steps	Acceptance Criteria
	To verify physically on the hardware	
Overall Test Result	Pass:□	Fail: □

Test ID	4.17.5.a Resolution	
Requirement	Sensor: 5M/8M effective resolution	
Test Objective	Sensor: 5M/8M effective resolution	Remark
	Test Steps	Acceptance Criteria
	The resolution can be updated using the Web GUI for Sparsh camera Config ->Encode setting	
Overall Test Result	Pass:□	Fail: □

Signaltron confidential. Do not copy

Test ID	4.17.5.b WDR		
Requirement	Wide Dynamic Range (WDR)=120dB to improve camera's image quality under high-contrast lighting conditions where both dimly and brightly lit areas are present in the field of view		
Test Objective	Wide Dynamic Range (WDR)=120dB to improve camera's image quality under high-contrast lighting conditions where both dimly and brightly lit areas are present in the field of view		Remark
	Test Steps	Acceptance Criteria	
	Supported and can be verified on ground	Image can be taken and verified	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not co

Test ID	4.17.5.c IR Distance supported		
Requirement	IR Distance supported = 30 meter		
Test Objective	IR Distance supported = 30 meter		Remark
	Test Steps	Acceptance Criteria	
	Supported and can be verified on ground	Image can be taken and verified	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.17.5.d Memory		
Requirement	Memory : Micro SD &SDXC slot upto 256GB		
Test Objective	Memory : Micro SD &SDXC slot upto 256GB		Remark
	Test Steps	Acceptance Criteria	
	Micro SD card support it and can be verified on hardware.	Verify Micro SD slot in the camera.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.17.6.a LENS		
Requirement	Lens: Motorized, vary focal (2.7mm-13.5mm)		
Test Objective	Lens: Motorized, vary focal (2.7mm-13.5mm)		Remark
	Test Steps	Acceptance Criteria	
	Supported and can be tested in ground		
Overall Test Result	Pass:□	Fail: □	

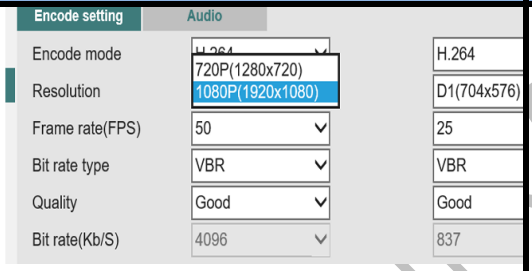
Signaltron Confidential. Do not copy

Test ID	4.17.6.b Field of View		
Requirement	Lens: Motorized, vary focal (2.7mm-13.5mm) Field of View(FOV): Horizontal–98 Deg wide. Vertical–50 Deg wide		
Test Objective	Lens: Motorized, vary focal (2.7mm-13.5mm) Field of View(FOV): Horizontal–98 Deg wide. Vertical–50 Deg wide		Remark
	Test Steps	Acceptance Criteria	
	Supported and can be tested in ground	It can be verifed by feeding Image sensors size and lense details on any FOV calculation platform. And as per data sheet.	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not

Test ID	4.17.6.c Focus and IRIS Control: Auto		
Requirement	Focus and IRIS Control: Auto		
Test Objective	Verify the IRIS Control features of the camera		Remark
	Test Steps	Acceptance Criteria	
	Supported and can be tested by varying the lighting conditions of the camera		
Overall Test Result	Pass:□	Fail: □	

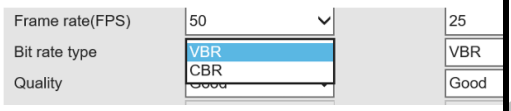
Signaltron Confidential. Do not copy

Test ID	4.17.7.a Video		
Requirement	Video Compression: H.265/H.264/MPJEG or equivalent		
Test Objective	Video Compression: H.265/H.264/MPJEG or equivalent		Remark
	Test Steps	Acceptance Criteria	
	Supported and can be verified from the camera		
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.17.7.a Video		
Requirement	High Speed live streaming capability		
Test Objective	Live Streaming of camera feed		Remark
	Test Steps	Acceptance Criteria	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy

Test ID	4.17.7.c Frame Rate		
Requirement	Frame Rate = 1 -30/60 fps		
Test Objective	Frame Rate = 1 -30/60 fps		Remark
	Test Steps	Acceptance Criteria	
	Supported ,it can be verified with web gui		
Overall Test Result	Pass:□	Fail: □	

Test ID	4.17.8 Power: PoE (802.3at)		
Requirement	Power: PoE (802.3at)		
Test Objective	Power: PoE (802.3at)		Remark
	Test Steps	Acceptance Criteria	
	Supported ,it can be verified using PoE Switch	Verify Physically	
Overall Test Result	Pass:□	Fail: □	

Signaltron Confidential. Do not copy