Establishment of Private Wireless Network Using Open-source Software Magma

Soubhik Baral
Central Research Laboratory
Bharat Electronics Ltd.
Bangalore,India
soubhikbaral@bel.co.in

Chaitanya P. Umbare
Central Research Laboratory
Bharat Electronics Ltd.
Bangalore,India
umbarechaitanya@bel.co.in

Jeevitha L
Central Research Laboratory
Bharat Electronics Ltd.
Bangalore,India
jeevithal@bel.co.in

Nidhi Jain
Central Research Laboratory
Bharat Electronics Ltd.
Bangalore,India
nidhijain@bel.co.in

***Abstract*—In order to address the challenges of rural internet access, open source software Magma provides a flexible low-cost and scalable network solution. Magma ensures minimal development and deployment effort with access network agnostic. Evolved packet core is a vital component of a cellular network to provide any communication services or internet. This open source software Magma is a next-generation packet core that supports 4G LTE or 5G radios or any wireless network. This paper presents the establishment of private network on Citizens Broadband Radio Service band (CBRS: 3550Mhz to 3700Mhz) over 4G LTE network using Magma software deployed in KU551 kit. This private network deployment comprises Baicells Atom ID06G Customer Premise Equipment (CPE) for each client, Baicells Neutrino 430 eNB for 4G base station, i-7 processor based kit (KU551) for Magma Core Network (CN) and a server connected with KU551 for SIP communication.**

***Index Terms*—Private Network, Magma, CBRS, CPE**

I. Introduction

Establishment of Private Network in any organization enhances adaptability, security and effectiveness. With the establishment of Private Network, enterprises can have control and choice to make modifications on the network based on their requirements like reach of a network, quick network failure recoveries, maximum limit of a network and more [1].

Wi-Fi being the popular solutions for Private Network has some drawbacks. Wi-Fi doesn't uphold huge Internet of Things (IoT) administrations because of the restricted association per channel, Wi-Fi also has security concerns which is not favourable for any defence organizations [2]. Table I list the differences between Wi-Fi 6 and Private 5G. Wi-Fi also have restricted facilities when it comes to new technologies like self-driven car, smart cities etc. In contrast to that, Private 4G/5G networks can meet all such advance needs in recent times and also in near future [2].

With advancement of technologies in telecommunications, many companies need secure, reliable and fast private network which covers large areas and allows secure voice and data communications in the organization. Some enterprises also depends on Private Network environment for carry their experiment and research need. Hence, open-source platforms can fulfil such requirements [3].

TABLE I
Differences between Wi-Fi 6 and Private 5G

	Spectrum	Security	Reliability	Coverage
Wi-Fi 6	Low	Low	Low	Low
Private 5G	High	High	High	High

Private Networks can be established with the help of licensed mobile network operator but it is an expensive solution. Magma is an open-source software platform which enables network operators a flexible, open and extendable mobile core network. This paper presents the building of 4G enterprise grade private mobile network using unlicensed CBRS band. This Magma open source software is implemented on KU551 kit. We have also implemented Magma on SMARC Conga SA5 and I-Pi SMARC plus but due to poor performance we decided to use KU551 kit.This network setup comprises Baicells Atom ID06G CPE for client and Baicells Nuetrino 430 eNB for 4G LTE base station.Baicells Baicells Atom ID06G CPE , Baicells Nuetrino 430 eNB was used as it supports CBRS band which can be used to establish private network for our requirement.

After establishment of Private 4G LTE network, the following test-cases were also verified:

1) Attachment of Base station (eNodeB/gNodeB) to the Magma Core Network.
2) CPE's (2) attachment to Base Station and Magma Core Network (CN).
3) Uplink/Downlink throughput for TCP/UDP traffic.
4) Voice call between two CPE's over SIP

The paper contents are divided into 2.Literature Review 3.Methodology provides in-depth details on how Magma and Baicells Indoor eNodeB-pBS31010 is used for the set up private network 4.Test Results and finally we conclude with 5.Conclusion and Future work.

II. Literature Review

Like never before, Private Network is in huge demands with the advancement of AI technologies like robots ,self driving car,drones,sensors etc.Private Networks provides services to those devices that requires scalability, security, availability. Private Networks will assist with working on the worth of the venture by giving foundation that can keep on developing [2].

Additionally, in this present reality where information breaks are quite common, high-innovation modern organizations require the utilization of their own modified security strategies and privately put away information, which may not be upheld by a portion of the customary public cell organizations. Because of these deficiencies, private organizations, which are likewise named non-public organizations in the third Generation Partnership Project (3GPP) [4], have drawn in huge interest.

Magma open-source platform has evolved as a community, and with major collaborations it provides its community to build advance networks [5] which supports Wi-Fi,LTE,5G communications. It can deftly uphold a radio access network with negligible turn of events and arrangement exertion, and incorporates three significant parts:Access Gateway,Orchestrator,Federation Gateway.

III. Methodology

With the increase of business requirement of private 4G/5G network, Magma the open-source Mobile core solutions provides cost-effective, reliable, scalable and feasible solutions for operators providing network accessibility in remote areas. Fig 1. depicts the high level Magma architecture which is 3GPP generation and access network agnostic. The key components of Magma architecture are Access Gateway (AGW), Orchestrator (ORC8r) and Federation Gateway (FEG). A typical Magma network will have many AGW for scaling with radio network. In Magma, the Access Gateway provides the network services and policy enforcement. The AGW is light weight software that provides EPC (Evolved packet core) functionalities and it contains MME (Mobility Management Entity), S-GW (Serving Gateway), P-GW (Packet Data Network Gateway) as some of the components. The major functionalities of AGW is subscriber registration, authorization, subscribers mutual authentication, IP address allocation to subscriber, subscriber deregistration, upgrading current serving MME id of the subscriber to HSS, pull the subscriber data from HSS, tracking of inactive subscribers etc. The orchestrator plays vital role in setting up a network and it allows configuring and monitoring the entire network and gateways centrally. The Network Management System (NMS) of Orchestrator is based on REST API that allows configuring AGW such as adding subscriber and policies to the network and displays the current status of network. Orchestrator is built with micro services frame work and it can be deployed in public or private cloud. The micro services of orchestrator are nghttpx, obsidian, certifier, bootstrapper, config, streamer, metricsd and datastore. The Federation Gateway is an optional component which acts

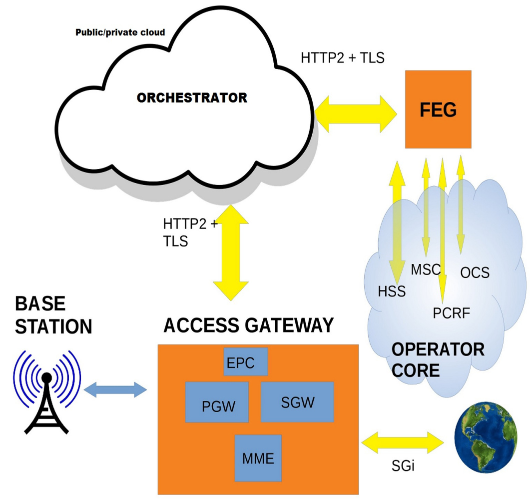


Fig. 1. Magma Architecture

as a proxy between Magma AGW and operator's network and facilitates major functions such as policy enforcement, data plans, authentication and charging to stay uniform between an existing MNO networks. This federation gateway expands the Magma with operator's network. Without federating onto and existing mobile core Magma can operate in stand-alone mode. This paper presents a 4G LTE private network without Federation gateway. The Fig 2. depicts the overall workflow of our 4G LTE private establishment. The main components in this setup are Magma, Baicells Indoor CPE and Baicells Indoor eNodeB. Magma was deployed on i-7 processor based kit (KU551) which Provides important framework like MME, HSS, SGW, PGW for providing data and voice LTE services. The Baicells Indoor eNodeB base station connects devices like mobile phones/ CPEs to core network using CBRS radio frequency is configured. Magma uses eth1 as the default S1 interface. Hence to connect our eNodeB to the Magma gateway eth1 interface was used. Magma's enodebd service can also be used for automatic eNodeB connection but here we have configured manually. After successful attachment of eNodeB and Magma EPC, Magma will be running a DHCP server to assign an IP address to the connected eNodeB, which gets IP 192.168.60.245 from the Magma core network. The assigned IP address to the eNodeB can be verified using the dnsd service. To check for successful attachment of eNodeB and core network s1 traffic was validated. Now CPE's can be attached to the network once when eNodeB starts transmitting. CPE's attachment can be success- ful once AGW accepts the authentication based on configuration of IMSI, APN and other network configuration. For CPE's attachment, network configuration such as APN, subscriber needed to be configured under Magma's APN. Once the Magma's AGW picks the APN configuration CPE1 and CPE2 are connected to the Network. Both the CPEs were allocated IPs, under APN by the Magma Access Gateway, the IP range can be set in the NMS. The

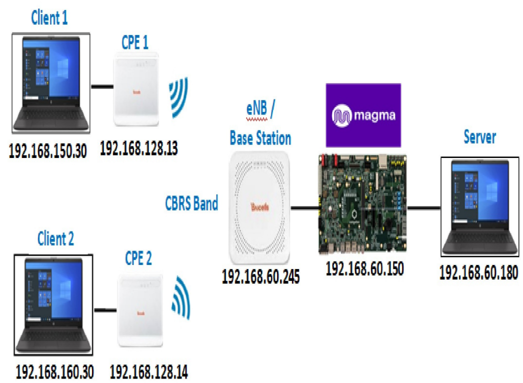


Fig. 2. 4G LTE private network setup

server in the network is used to check the uplink and downlink traffic of client1 and client2 which are connected to the CPE1 and CPE2 respectively. Server is also used as a SIP proxy for making voice calls between client1 and client2.

The Network Management System (NMS) of the Magma orchestrator is used for the core network functionality and GUI provided by Baicell's for CPE is used for its configuration.

Overall software/hardware platforms used for End to End private 4G/5G Test Bed setup:

1) Magma Core Network (CN)
2) Baicells Indoor eNodeB
3) Baicells Indoor CPE
4) Client 1 for CPE1
5) Client 2 for CPE2
6) Server

A.*Magma Deployment*

The aim of Magma was to provide mobile core solutions that are cost-effective, reliable, scalable and accessibility in remote areas. Magma followed the basic principle of SDN that is separa- tion of control plane from date plane, Access Gateway stores the run-time states at the edges, whereas Orchestrator stores the configuration states which allow UE's like mobile phones to connect to the network. The EPC functionalities are configured in Magma's Access Gateway (AGW) which relays the run-time functionality to the Orchestrator. Magma Access Gateway (AGW) is deployed on Ubuntu 20.04 and also can be deployed using Vagrant and VirtualBox [9].For the deployment of AGW, hardware configuration required are shown in TABLE II. Vagrant is an open-source software product for building and maintaining portable virtual software development environments. We have deployed AGW using Vagrant and VirtualBox on i-7 processor based kit (KU551). Following every step for deployment of Access Gateway using Vagrant and VirtualBox in Ubuntu 18.04 as per reference [9] we have installed our Magma Mobile core.

TABLE II
HARDWARE CONFIGURATION FOR DEPLOYMENT OF ACCESS GATEWAY

FACET	VALUES
Magma Tag	v1.6
OS	Ubuntu 18.04
vCPU	4
RAM	(16 GB)
Memory	(90 GB)

TABLE III
AGW AND OCHESTRATOR IP'S FOR TEST BED SETUP

FACET	VALUES
Magma Tag	v1.6
AGW IP	192.168.60.150
AGW OS	Ubuntu 18.04
Controller IP	192.168.60.248
Bootstrapper IP	192.168.60.248
Fluentd IP	192.168.60.247

The Orchestrator functionality can be implemented in private or a public cloud. Here we have deployed Orchestrator using Docker and have registered it in Docker hub account using scripts provided in Magma repository.

By accepting the self-assigned certificate provided by the Magma [10] we used NMS for controlling and Management of the Network. NMS was used to configure our gateways and related eNodeBs. After proper deployment of AGW and Orchestrator, using the NMS, configuration was made for AGW connection. TABLE III shows the characteristics for Orchestrator and AGW.

B.*Baicells Indoor eNodeB*

The Baicells Neutrino430 is a high level two-transporter indoor eNodeB (eNB) consistent with 3GPP LTE TDD innovation. Baicells Indoor eNodeB works on Carrier Aggregation (CA) mode or Dual Carrier (DC)/split mode. It supports HaloB operating mode which is e necessary to core network functions of the eNB. Fig. 3 depicts the basic eNodeB settings that are configured for our network.Fig. 3 shows the Basic configuration information of eNB.

After connection of AGW with the Orchestrator, we provisioned our eNodeB in NMS. We have manually configured eNodeB by enabling the"eNodeB managed externally" option under RAN settings. To add subscribers to the network, we initially provisioned an Access Point Network. APN can be easily added using the "ADD APN" functionality under APN configuration in NMS. After adding APN any number of UEs/CPEs can be attached to the network. Here we have added two CPEs for testing our network.

C.*Baicells Indoor CPE*

Customer Premise(s) Equipment, which points to any connected equipment that is basically used for accessing web or getting the services from the service providers whether connected directly to the network or indirectly connected to the network. Baicells CPE provides wireless access and routing functionalities to bring data and voice services to end-users. It transform high speed Long-Term Evolution (LTE) Time

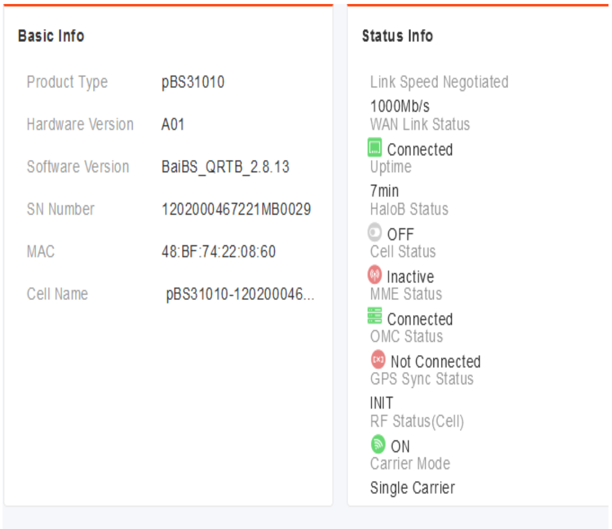


Fig. 3. enodeB Settings

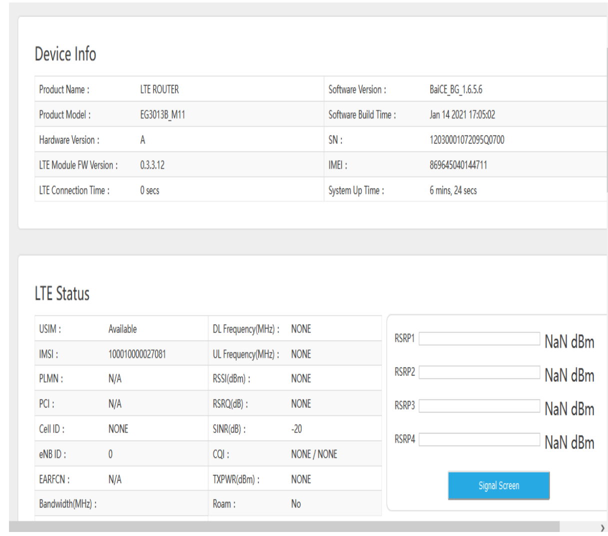


Fig. 4. CPE's GUI based device information

Division Duplexing (TDD) signals over CBRS band on the local area network (LAN).

After adding the APN as mentioned in the previous section, CPEs needed to be attached to the network.CPE can be configured either by Baicells Indoor CPE's GUI locally or remote web management of Magma core network. Fig 4 shows the GUI-based management portal that is used for our network configuration.

After the configuration of CPEs, AGW picks the APN for CPE1 and CPE, and are connected to the network. Once after the successful attachment of the CPE to the network both the CPEs were assigned IPs, under APN configuration provided by the Magma. In this established 4G LTE private network over CBRS band, SIP voice call communication is tested between client1 and client2 with SIP proxy server.

D.*Client 1 and Client 2*

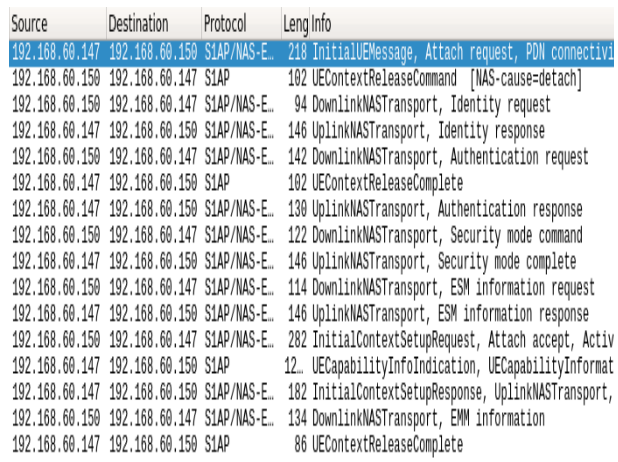
Client1 is connected to CPE 1 and client2 is connected to CPE 2 over LAN. To establish voice communication VOIP clients are installed on client1 and client2. User ID for client1 and client2 was set as 9001 and 9002 respectively. Clients are also used to access the GUI of CPEs for the configurations of network. Some examples of VOIP Clients are Blink Call, Ekiga, Jitsi etc.

E.*Server*

Server was installed behind the magma for the checking of Uplink and Downlink traffic to and from the Server. Here we have verified both TCP and UDP traffic flow. For VOIP communication we have set your own VoIP server. Asterisk server was installed as a VOIP server.To make communication with our VOIP clients we have registered 2 users 9001 and 9002 under SIP.conf file in Asterisk.

IV. Test Results

In this section we come up with the results for the test-case mentioned above:



Source	Destination	Protocol	Leng	Info
192.168.60.147	192.168.60.150	S1AP/NAS-E…	218	InitialUEMessage, Attach request, PDN connectivi
192.168.60.150	192.168.60.147	S1AP	102	UEContextReleaseCommand [NAS-cause=detach]
192.168.60.150	192.168.60.147	S1AP/NAS-E…	94	DownlinkNASTransport, Identity request
192.168.60.147	192.168.60.150	S1AP/NAS-E…	146	UplinkNASTransport, Identity response
192.168.60.150	192.168.60.147	S1AP/NAS-E…	142	DownlinkNASTransport, Authentication request
192.168.60.147	192.168.60.150	S1AP	102	UEContextReleaseComplete
192.168.60.147	192.168.60.150	S1AP/NAS-E…	130	UplinkNASTransport, Authentication response
192.168.60.150	192.168.60.147	S1AP/NAS-E…	122	DownlinkNASTransport, Security mode command
192.168.60.147	192.168.60.150	S1AP/NAS-E…	146	UplinkNASTransport, Security mode complete
192.168.60.150	192.168.60.147	S1AP/NAS-E…	114	DownlinkNASTransport, ESM information request
192.168.60.147	192.168.60.150	S1AP/NAS-E…	146	UplinkNASTransport, ESM information response
192.168.60.150	192.168.60.147	S1AP/NAS-E…	282	InitialContextSetupRequest, Attach accept, Activ
192.168.60.147	192.168.60.150	S1AP	12…	UECapabilityInfoIndication, UECapabilityInformat
192.168.60.147	192.168.60.150	S1AP/NAS-E…	182	InitialContextSetupResponse, UplinkNASTransport,
192.168.60.150	192.168.60.147	S1AP/NAS-E…	134	DownlinkNASTransport, EMM information
192.168.60.147	192.168.60.150	S1AP	86	UEContextReleaseComplete

Fig. 5. CPE attached to Base Station and Core Network

1) *Attachment of Base station (Baicells Neutrino 430 eNodeB) to the Magma Core Network*: Fig 6. shows S1SetupRequest and S1SetupResponse which validates the attachment of base station with eNodeB. Fig 7. shows that over GUI of eNB that MME is connected to the Base Station which also validates the Attachment of Base Station to the Magma Core Network.
2) *Attachment of CPE (Baicells Atom ID06G)* Fig 5. shows that requested CPE attachment was successfully granted by eNB and Core Network (CN).
3) Verified Uplink and Downlink throughput for TCP/UDP traffic and also voice call between the CPEs using SIP proxy

V. Conclusions and Future Work

This Paper presented the private network establishment based on 4G LTE over CBRS band, the network setup comprises Baicells indoor eNodeB Base station, Baicells indoor

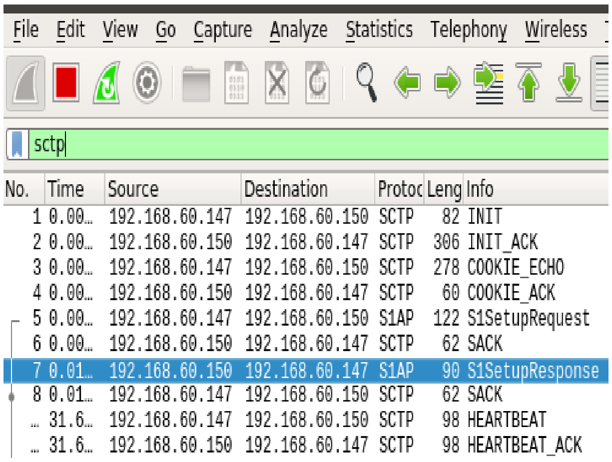


Fig. 6. Magma(CN) and Baicells Indoor enodeB attachment.

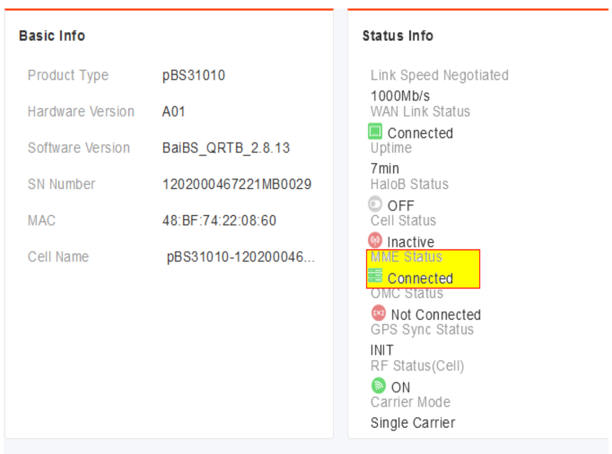


Fig. 7. Magma(CN) and Baicells Indoor enodeB attachment

CPEs for Client1 and Client2, KU551 kit for Magma deployment and server. This setup can be extended for the evaluation of 5G Standalone Mode (SA) using gNodeB. Further this work can be extended to integrate Federation Gateway (FEG) to scale up this private network with existing Mobile Network Operator(MNO). Here we have tested our network with one base station and 2 CPEs, which can be further scaled up to three base stations for wider range and multiple CPEs for checking the scalabilty of subscribers in the network.

VI. Acknowledgement

We thank our organization Central Research Lab of Bharat Electronics Ltd, Bangalore for providing support and required resources in order to carry out this work efficiently. Also, we would like to thank our colleagues for their insights on reviewing this work periodically and providing support during the development.

References

[1] R. Ferrus and O. Sallent, ”Extending the LTE/LTE-A business case: Mission- and business-critical mobile broadband communications”, IEEE Veh. Technol. Mag., vol. 9, no. 3, pp. 47-55, Sep. 2014.

[2] G. Brown, ”Private 5G mobile networks for industrial IoT” in, Qualcomm Inc, 2019.

[3] J. Liao and X. Ou, ”5G military application scenarios and private network architectures”, Proc. IEEE Int. Conf. Adv. Elect. Eng. Comput. Appl., pp. 726-732, 2020.

[4] ”Technical specification group services and system Aspects Study on management aspects of non-public networks (release 17)”, 3GPP, no. TR28.807, Oct. 2020.

[5] Navid Nikaein, Mahesh K. Marina, Saravana Manickam, Alex Dawson, Raymond Knopp and Christian Bonnet,”OpenAirInterface: A Flexible Platform for 5G Research”, ACM SIGCOMM Computer Communication ReviewVolume 44,October 2014.

[6] Navid Nikaein, Raymond Knopp, Florian Kaltenberger, Lionel Gauthier, Christian Bonnet, Dominique Nussbaum, Riadh Ghaddab“Demo: OpenAirInterface: an open LTE network in a PC” MobiCom ’14: Proceedings of the 20th annual international conference on Mobile computing and networking, September 2014.

[7] Ettus Research,The USRP Hardware Driver Repository, https://github.com/EttusResearch/uhd.

[8] Openairinterface 5G Wireless Implementation,

[9] Juan C. Caviedes V, https://github.com/caprivm/virtualization/wiki/AGW-Deployment-using-Vagrant.

[10] Magma.https://docs.magmacore.org/docs/basics/introduction.html.