ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"VIRTUALIZACIÓN DE UNA CENTRAL 4G CON SOFTWARE DE CÓDIGO ABIERTO EN EL LABORATORIO DE COMUNICACIONES DE LA FIE"

Trabajo de Integración Curricular

Tipo: Propuesta Tecnológica

Presentado para optar el grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR

HENRY EZEQUIEL YUGSIN SANCHEZ

Riobamba – Ecuador

2022

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

"VIRTUALIZACIÓN DE UNA CENTRAL 4G CON SOFTWARE DE CÓDIGO ABIERTO EN EL LABORATORIO DE COMUNICACIONES DE LA FIE"

Trabajo de Integración Curricular

Tipo: Propuesta Tecnológica

Presentado para optar el grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: HENRY EZEQUIEL YUGSIN SANCHEZ

DIRECTOR: Ing. DIEGO FERNANDO VELOZ CHERREZ.

Riobamba – Ecuador

2022

Yo, Henry Ezequiel Yugsin Sanchez, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 4 de mayo del 2022

Henry Ezequiel Yugsin Sanchez

1850022409

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

El Tribunal del Trabajo de Titulación certifica que: el Trabajo de Titulación: Tipo Propuesta Tecnológica **"VIRTUALIZACION DE UNA CENTRAL 4G CON SOFTWARE DE CODIGO ABIERTO EN EL LABORATORIO DE COMUNICACIONES DE LA FIE",** realizado por el señor **HENRY EZEQUIEL YUGSIN SANCHEZ**, ha sido minuciosamente revisado por los Miembros del Tribunal del trabajo de titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Dr. Jorge Vinicio Tuapanta Dacto. **PRESIDENTE DEL TRIBUNAL**		2022-05-04
Ing. Diego Fernando Veloz Cherrez. **DIRECTOR DEL TRABAJO DE TITULACIÓN**		2022-05-04
Ing. Jefferson Ribadeneira Ramirez. **MIEMBRO DEL TRIBUNAL**		2022-05-04

DEDICATORIA

Este trabajo de Titulación, así como todos mis logros profesionales y personales van dedicados a mi familia que son los que siempre me han brindado su apoyo incondicional. A mis padres German y Martha los cuales son el pilar fundamental en mi vida y que son los que me han enseñado que con trabajo y dedicación se pueden alcanzar los sueños además me han inculcado valores para formarme como una persona educada y honrada. A mis hermanos Jonathan, David y Jordan los cuales son mi inspiración para seguir cumpliendo mis metas y quiero decirles que siempre les apoyare para que ustedes también puedan alcanzar sus objetivos profesionales y personales.

Henry Ezequiel Yugsin Sanchez

AGRADECIMIENTO

Primero quiero agradecer a Dios quien es el que me da salud y vida para poder cumplir mis metas. De igual manera agradecer a mi querida Escuela Superior Politécnica de Chimborazo la cual me ha dado la oportunidad de formarme como profesional y así contribuir al desarrollo de mi querido país Ecuador. A mi facultad FIE y todo el personal que la conforma. A todos los profesores que han compartido su conocimiento conmigo para que así yo pueda alcanzar mi meta.

Henry Ezequiel Yugsin Sanchez

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ECUACIONES

ÍNDICE DE ANEXOS

ÍNDICE DE ABREVIATURAS

2G	Segunda Generación
3G	Tercera Generación
3GPP	Proyecto de asociación de tercera generación
4G	Cuarta Generación
5G	Quinta Generación
AN	Red de acceso
AuC	Centro de autenticación
AAA	Autenticación, autorización y contabilización
ARQ	Solicitud de repetición automática
BNG	Pasarelas de red de banda ancha
CN	Core Network
CS	Conmutación de circuitos
dB	Decibelios
DHCP	Protocolo de configuración dinámica de host
eNB	Nodo B evolucionado
E-UTRAN	Red de acceso radio para LTE
EPC	Núcleo de paquete envuelto
ePDG	Puerta de enlace de paquetes de datos envuelta
EPS	Sistema de paquetes envuelto
ESM	Gestión de sesiones EPS
GHz	Giga Hertz
GSM	Sistema global para las comunicaciones móviles
GPRS	Paquete general de Radio servicio
GERAN	Red de acceso por radio GSM EDGE
GPRS	Servicio global de radio por paquetes
GRE	Encapsulación de enrutamiento genérico
GTP	Protocolo de túnel de GPRS
HSPA	Acceso a paquetes de alta velocidad
HSS	Servidor de abonado doméstico
HA	Agente de casa
HLR	Registro de ubicación de casa
IP	Protocolo de Internet
IMS	Subsistema Multimedia IP
IETF	Grupo de Trabajo de Ingeniería de Internet

IPsec	Seguridad del protocolo de Internet
LTE	Evolución a largo plazo
MANO	Administración y Orquestación
Mbps	Mega bits por segundo
ME	Equipo Móvil
MME	Entidad de gestión de movilidad
MIMO	Múltiple entrada Múltiple salida
MAC	Control de acceso al medio
NAS	Estrato sin acceso
NFV	Virtualización de funciones de red
NFVI	Infraestructura NFV
OFDMA	Acceso múltiple por división de frecuencias ortogonales
OCS	Sistema de carga online
OFCS	Sistema de carga offline
PS	Conmutación de paquetes
P-GW	Pasarela de red de paquetes de datos
PCRF	Servidor de funciones de políticas y reglas de cobro
PDCP	Protocolo de convergencia de paquetes de datos
QoS	Calidad de servicio
RB	Portadoras de radio
RRC	Control de recursos de radio
RLC	Control de radioenlace
RNL	Capa de red de radio
SIM	Modulo de identidad del subscriptor
SIP	Protocolo inicial de sesión
SAE	Evolución de la arquitectura del sistema
S-GW	Puerta de enlace de servicio
SCTP	Protocolo de transmisión de control de flujo
SDR	Radio definido por software
TNL	Capa de red de transporte
TCP	Protocolo de Control de Transmisión
TEID	Identificador de punto final de túnel
UMTS	Sistema Universal de Telecomunicaciones Móviles
UICC	Tarjeta de circuito integrada universal
UE	Equipo de Usuario
USIM	SIM Universal
UTRAN	Red de acceso de radio terrestre UMTS

UDP	Protocolo de datagrama de usuario
USRP	Periférico de radio de software universal
VNF	Funciones de red virtualizadas
WiFi	Fidelidad inalámbrica
WCDMA	Acceso múltiple por división de código de banda ancha
WiMAX	Interoperabilidad mundial para acceso por microondas
WLAN	Red de área local inalámbrica

RESUMEN

El presente trabajo de titulación tuvo como objetivo virtualizar una central 4G con software de código abierto en el laboratorio de comunicaciones de la FIE. Mediante una revisión bibliográfica se procedió a realizar el estudio del arte de la tecnología de redes móviles 4G, en este estudio se obtuvo información acerca de la estructura y funcionamiento de las redes móviles 4G basados en los Releases de 3GPP. De igual manera se investigo acerca de la técnica de virtualización de funciones de red con la ayuda de diferentes softwares de código abierto, en dicha investigación se escogió al software OpenAirInterface OAI para la realización de este proyecto. Para la virtualización de la central 4G se planteó dos escenarios, el primer escenario consistió en un entorno totalmente virtual, en el cual las entidades conocidas como EPC, eNB y UE fueron virtualizados con la ayuda del software OAI. Para el segundo escenario se utilizó un equipo SDR específicamente la USRPB210, la misma que cumplió con las funciones radio de E-UTRAN de la red 4G. Para la validación de estos dos escenarios se realizaron diferentes pruebas, para el primero se realizaron pruebas de conectividad por parte del UE hacia la propia red 4G y hacia redes externas. Mientras que para la validación del segundo escenario se utilizó el analizador de espectro E8600B para medir los diferentes parámetros del enlace de bajada de E-UTRAN. Los resultados obtenidos fueron exitosos ya que para el primer escenario se tuvo conectividad del UE con redes internas y externas, mientras que para el segundo escenario los parámetros de potencia, ancho de banda y transmisión de datos de control fueron encontrados en los valores admisibles. Se concluye que las redes 4G siguen sufriendo diferentes mejoramientos y se recomienda investigar información sobre la estructura de redes 4G en fuentes confiables.

Palabras clave: <REDES MÓVILES 4G>, <EQUIPO SDR>, <SOFTWARE DE CÓDIGO ABIERTO>, <VIRTUALIZACIÓN DE FUNCIONES DE RED>**,** <FUNCIONES RADIO DE E-UTRAN>**.**

SUMMARY

The objective of this degree work was to virtualize a 4G central with open source software in the FIE´s communications laboratory. Through a literature review, we proceeded to study the art of 4G mobile network technology, in this study information was obtained about the structure and operation of 4G mobile networks based on 3GPP Releases. In the same way, the network functions virtualization technique was investigated with the help of different open source software, In this research, the Open Air Interface OAI software was chosen to carry out this project. in which the entities known as EPC, eNB and UE were virtualized with the help of OAI software. For the second scenario, an SDR equipment was used, specifically the USRPB210, the same one that fulfilled the radio functions of E-UTRAN of the 4G network. For the validation of these two scenarios, different tests were carried out. For the first one, connectivity tests were carried out by the UE towards the 4G network itself and towards external networks. While for the validation of the second scenario, the E8600B spectrum analyzer is used to measure the different parameters of the E-UTRAN downlink. The results obtained were successful since for the first scenario there was connectivity of the UE with internal and external networks, while for the second scenario the parameters of power, bandwidth and transmission of control data were found in the admissible values. It is concluded that 4G networks continue to undergo different improvements and it is recommended to investigate information on the structure of 4G networks in reliable sources.

Keywords: <VIRTUALIZATION>, <4G MOBILE NETWORKS>, <SDR EQUIPMENT>, <OPEN SOURCE SOFTWARE>, <VIRTUALIZATION OF NETWORK FUNCTIONS>, <E-UTRAN RADIO FUNCTIONS>, <OPENAIRINTERFACE>, <3GPP RELEASES>.

Firmado electrónicamente por:
WILSON GONZALO
ROJAS YUMISACA

MSc. Wilson G. Rojas

NOMBRE Y FIRMA PROFESOR

C.I 0602361842

INTRODUCCIÓN

En la actualidad las redes de comunicaciones móviles desempeñan un rol fundamental ya que la comunicación es una necesidad inherente del ser humano y está sujeta a un constante proceso de evolución. La aparición de los sistemas de telecomunicaciones desarrollados especialmente a partir del siglo XX y su generalización durante dicho periodo ha traído consigo una verdadera revolución en las sociedades modernas (Markus, 1988).

Según un reciente informe sobre movilidad presentado por Ericsson las redes de comunicaciones móviles experimentan un crecimiento constante con alrededor de 8000 millones de subscriptores en la actualidad y una proyección de 9000 millones para el 2025. De igual manera se espera que 2800 millones utilicen tecnología 5G, pero la tecnología que liderara las comunicaciones móviles por algunos años más seguirá siendo 4G. Es por ello que respaldar el enorme y rápido crecimiento de la cantidad de datos transmitidos y la conectividad supone un problema para las redes 4G LTE actuales (Ericsson, 2020).

Actualmente existen diversos proyectos de investigación los cuales desarrollan maneras de hacer frente a la explotación de trafico mediante LTE y su futura migración hacia la nueva red 5G. Es de allí donde nace el concepto de virtualización de funciones de red y su aplicabilidad en redes de comunicaciones móviles. Es por ello que en este trabajo de titulación se virtualiza una central 4G con la ayuda de software de código abierto en el laboratorio de comunicaciones de la FIE para así poder analizar el funcionamiento de toda esta tecnología y los beneficios que podría dar al mundo de las comunicaciones móviles en especial para 4G. Para la realización de este proyecto, la central 4G se basa en los parámetros y características técnicas especificadas por 3GPP al igual que las demás entidades comprendidas dentro de la red LTE denominadas eNB y UE.

La finalidad de este trabajo es demostrar que se puede virtualizar una central 4G y aprovechar todas sus funcionalidades para realizar análisis y pruebas de laboratorio acerca del rendimiento de la misma y de todas sus entidades adjuntas como el eNB y el UE.

ANTECEDENTES

El concepto de redes de comunicaciones móviles nace a inicios de 1981 cuando Ericsson lanza el sistema NMT450, el mismo que trabaja a una frecuencia de 450 MHz y usaba como método de transmisión canales analógicos, este sistema móvil fue conocido mundialmente como primera generación (1G). En 1990 nacen nuevos sistemas como GSM y D-AMPS que trabajan en canales digitales a frecuencias de 900 y 1800 MHz además utilizan técnicas de acceso al medio como TDMA y CDMA, el sistema es conocido mundialmente como segunda generación (2G). Luego se incorpora el sistema UMTS conocido como la tercera generación (3G), trabajando en frecuencias de 2600 MHz además se aumenta la seguridad de transmisión y nace 3GPP, organización dedicada a estandarizar los sistemas móviles a nivel mundial. A comienzos de 2007 surge la cuarta generación (4G) sus principales características son las grandes velocidades que se planea conseguir (Teóricamente a 100 Mbps de bajada). Dentro de estas tecnologías se considera Wii Max y LTE/advanced. Por ultimo nace la quinta generación (5G) con capacidades mucho mayores a las de su antecesor. La Release 15 del 3GPP, finalizada en 2018, desarrolla la tecnología conocida como New Radio (NR) para la 5G, y ha sido adoptada en el marco de la hoja de ruta IMT-2020 de la UIT como el estándar para la nueva generación de redes móviles. Dichas especificaciones contemplan dos posibles arquitecturas para las redes 5G. NSA (Non-Stand-Alone) y SA (Stand-Alone). Ambas suponen el despliegue de una red de acceso radio (RAN) con estaciones base gNB (gNodeB) basadas en NR, pero NSA sigue dependiendo de del núcleo de red, denominado (Evolved Packet Core), y las estaciones base eNB (eNodeB) de LTE (Moya, 2013). Uno de los avances más significativos en el 5G se encuentra en la arquitectura de red, ya que implementan nuevas técnicas de NFV y SDN, las cuales realizan una tarea importante a la hora del despliegue de 5G.

Se considera que NFV comienza a tomar forma en 2012, cuando un grupo de operadores de telecomunicaciones publican un libro en blanco describiendo la versión original de este concepto y los principios en torno a los cuales deben desarrollarse. El llamamiento a otros actores del sector que se realiza al final del documento condujo a la creación de un grupo de especificaciones de la industria sobre la virtualización de funciones de red (ISG NFV) bajo el paraguas del ETSI (European Telecommunications Standards Institute) (Jaeger, 2015).

En febrero de 2018 nace O-RAN (Open-Ran) cuyo enfoque principal está en la arquitectura de red, la virtualización, la interoperabilidad y la accesibilidad a las redes móviles 5G y 4G. Esta iniciativa fue fundada por diferentes operadores móviles a nivel mundial y además diferentes universidades e institutos del mundo realizan diferentes investigaciones e implementaciones para validar su funcionamiento.

El instituto de investigación EURECOM en Francia desarrollo una plataforma de código abierto llamada OPEN AIR INTERFACE (OAI), la cual tiene como objetivo desarrollar herramientas para la implementación de una solución abierta para LTE y 5G. En la Universidad Politécnica de Valencia (UPV) en el año 2020 se han realizado diferentes proyectos de investigación y de implementación con la ayuda de software de código abierto como los descritos anteriormente. En 2020 en la Universidad de Cantabria de igual manera se ha realizado diversos estudios de simulación e implementación de redes 4G y 5G con ayuda de software libre y SDR.

A nivel nacional podemos encontrar diversas propuestas para la virtualización de redes de comunicaciones móviles. La Universidad Católica de Santiago de Guayaquil en un estudio describe como sería la virtualización de una red 4G para la convivencia con redes 5G. De igual manera la Escuela Politécnica Nacional ha realizado diversas investigaciones de la virtualización de redes móviles.

PLANTEAMIENTO DEL PROBLEMA

¿La virtualización de redes móviles permite una implementación más eficiente de infraestructura celular?

SISTEMATIZACIÓN DEL PROBLEMA

¿Existe bibliografía suficiente acerca de la virtualización de las redes móviles 4G en Ecuador y a nivel mundial?
¿Cuáles son los principios fundamentales del funcionamiento de redes móviles?
¿Cuáles son los principios fundamentales de la virtualización de redes móviles 4G?
¿Cuál es la metodología para virtualizar redes 4G?
¿Cuáles son las ventajas de la virtualización de una red 4G con Software de código abierto?

JUSTIFICACIÓN TEÓRICA

Debido a las crecientes demandas de trafico de las redes 4G y el futuro gran mercado que pretende abarcar las redes 5G hoy es más que necesario el interés hacia redes móviles totalmente interoperables. En ese sentido, el concepto de Virtualización de Redes Móviles surge como un intento de considerar el importante papel que desempeñan para la escalabilidad y la accesibilidad de aplicaciones actuales y futuras.
La Virtualización de Redes Móviles constituye una variable de vital importancia para que las redes futuras tengan éxito, ya que esto hará que se diversifique aún más sus aplicaciones como redes privadas, aplicaciones IoT seguras y potenciando la industria a niveles nunca antes visto todo esto con un costo menor. Esto aumenta aún más la necesidad de la investigación por encontrar una solución a todos estos problemas actuales y futuros.

JUSTIFICACIÓN APLICATIVA

Este trabajo se justifica porque la utilización de Software de código abierto facilita la virtualización de una central 4G para el despliegue de redes móviles, al mismo tiempo se busca la escalabilidad para demandas del tráfico de red. La utilización de Software de código abierto hace que la virtualización de una central 4G sea flexible ya que se puede modificar diferentes parámetros de la misma. Por ello, este estudio contribuirá con información relevante para el funcionamiento de una central 4G en entornos virtuales. Además, que será un antecedente para virtualizaciones de tecnologías móviles 4G en el laboratorio de comunicaciones de la FIE.

OBJETIVOS

OBJETIVO GENERAL

Virtualizar una central 4G con Software de código abierto en el Laboratorio de comunicaciones móviles de la FIE.

OBJETIVOS ESPECÍFICOS

Analizar el estado del arte de la tecnología de comunicaciones móviles 4G.

Investigar la virtualización de las redes móviles con la ayuda de diferentes herramientas de software de código abierto.

Virtualizar una central 4G usuario, eNodeB y core 4G mediante el uso de software de código abierto en el Laboratorio de Comunicaciones de la FIE.

Comprobar los resultados de conectividad de la central 4G y los usuarios mediante pruebas de ping en el entorno virtual.

CAPITULO I

En este capítulo se dará a conocer múltiples definiciones a tomar en cuenta para el desarrollo de este trabajo, como son los fundamentos de la cuarta generación de redes inalámbricas 4G, casos de uso, entidades que conforman la red 4G, funciones y características de cada entidad, interfaces de interconexión interna e externa, protocolos utilizados para la transferencia de los paquetes de datos, tipos de modulación, tipos de duplexación, fundamentos de virtualización de redes y definiciones de redes definidas por software. También se analizará los métodos que se utilizan para el correcto funcionamiento de una red 4G, desglosando los parámetros más relevantes, los mismos principios que ayudara a determinar el correcto funcionamiento del aplicativo final. La teoría de comunicaciones y la virtualización de funciones de red se consideran fundamental para realizar la virtualización posterior.

1 MARCO TEÓRICO

1.1 Introducción a las Redes Móviles

Un sistema de redes de comunicaciones móviles se lo puede definir como el grupo de redes, servicios y aplicaciones que permiten a los usuarios enviar o recibir voz y datos entre ellos, además permite la movilidad de los usuarios sin perder conectividad con la red. Entre los principales objetivos de las redes móviles está proporcionar acceso a las redes de telecomunicaciones, facilitar la movilidad de los usuarios, brindar un servicio en todas las zonas de cobertura y proporcionar un nivel de servicio aceptable (Pérez et al., 2019).

En principio los sistemas de comunicaciones móviles eran centralizados, los cuales tenían muchos defectos y causaban problemas, debido a esto nacen los sistemas móviles celulares. Esta definición estructura las redes móviles con una perspectiva diferente, se reemplaza el único y potente transmisor por múltiples transmisores menos potentes a largo del área de cobertura. Estos transmisores están diseñados para brindar cobertura a un área pequeña alrededor de ellos, llamada célula. Este diseño tiene algunos beneficios, uno de ellos es que los usuarios de celdas aledañas usan frecuencias diferentes, logrando una mayor calidad y capacidad con un espectro menor. Además, el área de cobertura de la estación base es un rango relativamente pequeño con lo que los terminales móviles deben emitir una potencia menor (Pérez et al., 2019).

En el capítulo I se describe la arquitectura de un sistema de comunicaciones móviles basadas en las especificaciones de un sistema 4G. Parta ello, se presenta la arquitectura genérica de toda la

familia de sistemas especificadas por 3GPP. Esto permite identificar de forma clara cuales son, y a que criterios esenciales de diseño obedecen, las entidades del sistema LTE. En este apartado se detalla la arquitectura genérica de redes móviles y la arquitectura genérica de una red 3GGP. Una vez identificados los componentes y entidades de más alto nivel que conforman parte del sistema 4G, en apartados siguientes se realiza una descripción más detallada de cada uno de ellos en base a las entidades de red e interfaces asociadas en su estructura interna. De cada una de las entidades de red se detalla sus funciones más relevantes. Respecto a las interfaces entre las entidades de red, conjuntamente con la descripción de su funcionalidad se describen los distintos protocolos que sustentan las interfaces.

1.1.1 Arquitectura Genérica de las Redes Móviles

En la Figura 1-1 se ilustra una arquitectura generalizada de un sistema de comunicaciones móviles celular. Esta arquitectura representa un modelo de la red a muy alto nivel donde se reconoce a tres componentes básicos (Comes, 2010):

- Equipo de usuario, dispositivo electrónico que hace posible que un usuario pueda acceder a los servicios y recursos de la red. El equipo de usuario contempla una tarjeta inteligente llamada Universal Integrated Circuit Card, UICC, la misma que contiene la información necesaria para autenticarse en la red. El UE accede a la red mediante la interfaz radio.
- Red de acceso, cumple la función de sustentar la transmisión radio con los UE de cara a brindar la conectividad necesaria entre éstos y los equipos de la red troncal. Los servicios de transmisión ofrecidos por la red de acceso para transportar la información de los usuarios (tanto información de datos como señalización) hacia y desde la red troncal son servicios portadores, es decir, servicios cuya finalidad última es provisionar una cierta capacidad de transmisión. La red de acceso es la encargada de administrar el uso de los recursos radio disponibles para la provisión de servicios portadores de manera eficaz.
- Red troncal, parte del sistema encargado de aspectos tales como, control de acceso a los usuarios, movilidad de UE, conexión con otras redes 3GPP y no 3GPP, etc. Aquí se forman equipos que cumplen funciones de conmutación de circuitos, enrutamiento de paquetes, bases de datos, etc.

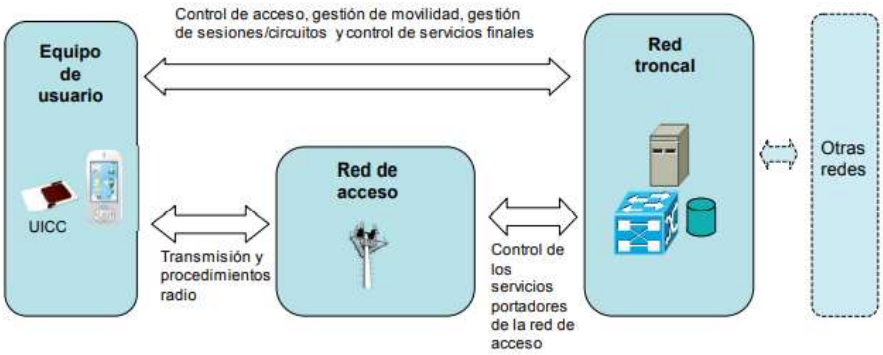


Figura 1-1: Arquitectura genérica de un sistema celular

Fuente: (Comes, 2010)

1.1.2 Arquitectura Genérica de las Redes 3GPP

Las arquitecturas de red contenidas en la familia de sistemas especificados por 3GPP se amoldan a la arquitectura genérica descrita anteriormente. Como se muestra en la Figura 2-1, los sistemas 3GPP contienen la especificación del equipo de usuario llamado User Equipment (UE) y de una infraestructura de red, la misma que se separa de forma lógica en dos, una para la infraestructura de red troncal (Core Network, CN) y la otra para la red de acceso (Access Network, AN) (3GPP, 2019).

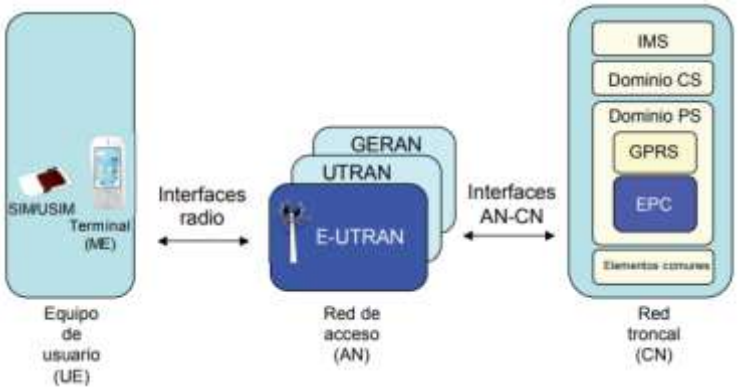


Figura 2-1: Arquitectura de alto nivel de los sistemas 3GPP

Fuente: (Jiménez, 2013)

El UE en el estándar 3GPP está conformado por dos elementos básicos: el dispositivo móvil o terminal (Mobile Equipment ME) y una tarjeta UICC. La tarjeta UICC, también llamadas SIM (Subscriber Identity Module) en GSM y USIM (Universal SIM) en UMTS y LTE, es la que contiene la información y sustenta los procedimientos que tienen que ver con la subscripción del usuario a los servicios de la red. La separación entre terminal móvil y tarjeta hace que el usuario (identificado a través de la SIM/USIM) pueda utilizar diversos terminales para autenticarse en la red.

Para la red de acceso, 3GPP específica y estandariza 3 tipos de redes de acceso: GERAN, UTRAN y E-UTRAN. E-UTRAN es la red de acceso definida para los sistemas 4G. La red de acceso define su propia interfaz radio para la comunicación con los equipos de usuario (UE): E-UTRAN utiliza la tecnología OFDMA.

La red troncal EPC, se divide de forma lógica en un dominio de circuitos (Circuit Swiched, CS, Domain), un dominio de paquetes (Packet Switched, PS, Domain) y por último el llamado subsistema IP Multimedia (IP Multimedia Subsystem, IMS). En adelante, estas tres entidades se llamarán dominio CS, dominio PS y subsistema IMS, respectivamente.

El dominio CS contempla a todas las entidades de EPC que tienen la función de brindar servicios de telecomunicación basados en conmutación de circuitos, es decir, servicios a los que se les da recursos de forma dedicada (circuitos) en el instante en que se establece la conexión, hasta la finalización del servicio (Jimenez & Rizo, 2013).

El dominio PS contiene a las entidades de EPC que brindan servicios de telecomunicación que se basan en conmutación de paquetes: la información de usuario se encapsula en paquetes de datos que se encaminan y distribuyen por los distintos elementos y enlaces de la red. Específicamente el dominio PS proporciona un servicio de conectividad a redes de paquetes (e.j., redes IP y X.25). Para el dominio PS existen dos implementaciones diferentes: GPRS y EPC. EPC es la especificación del dominio PS desarrollada para el sistema 4G. La red troncal está estructurada para soportar conectividad IP, indistintamente si es tecnología 3GPP o 3GPP (Jimenez & Rizo, 2013).

El subsistema IMS contempla los servicios IP multimedia que se basan en el protocolo SIP (Session Initiation Protocol) de IETF (Internet Engineering Task Force). El subsistema IMS es el que se encarga de la señalización relacionada a los servicios multimedia y utiliza como mecanismo de transporte los servicios de transferencia de datos proporcionados por el dominio PS. El subsistema IMS constituye el plano de control por lo cual queda claramente separado de las funciones relacionadas al transporte del tráfico de usuario.

1.2 Redes Móviles 4G

Con la llegada de LTE se empezaron a comercializar las redes de comunicaciones de cuarta generación. A partir de la Release 8 publicada por 3GPP, se estableció el estándar de LTE promovido por diversas necesidades como la alta demanda de datos, la complejidad de los sistemas móviles de tercera generación o elevados costes que incentivaron la aparición del 4G,

convirtiéndose en el estándar de comunicaciones que ha marcado los pasos a seguir en el futuro (Remy & Letamendia, 2014).

Su principal objetivo era conseguir simplificar la red móvil heredada de tercera generación y diferenciar de manera clara la parte RAN de la parte del núcleo de la red CN. Por lo que la RAN evolucionó hacia la conocida como E-UTRAN que implementaba nuevas tecnologías de acceso radio y el núcleo de la red pasó de una arquitectura basada en conmutación de circuitos a una arquitectura basada en TCP/IP que se llamó EPC (Dahlman et al.,2011).

Pero además este nuevo diseño de la arquitectura de 4G, conocido como EPS quería optimizar el tráfico de datos desde y hacia los usuarios. Bajo esta premisa, la reducción del número de nodos que están implicados en la conmutación de paquetes fue la solución y la arquitectura de 4G pasó a ser conocida como plana (Abdrabou et al., 2015).

De esta forma, E-UTRAN es el responsable de toda la funcionalidad relacionada con la parte radio de la red general, que incluye los protocolos de retransmisión, codificación y gestión de recursos radio. Y el EPC que, aunque no se encarga de las funciones de la interfaz radio, proporciona una red de banda ancha móvil completa, que facilita la autenticación y la configuración de las conexiones extremo a extremo.

Como se ve en la figura 3-1, el UE puede alcanzar el EPC usando E-UTRAN, sin embargo, esta no es la única tecnología de acceso admitida. 3GPP especificó el soporte de múltiples tecnologías de acceso y también el traspaso entre estos accesos. La idea era lograr la convergencia utilizando una red central única que proporciona varios servicios basados en IP a través de tecnologías de acceso múltiple. Se admiten las redes de acceso por radio 3GPP existentes. Las especificaciones 3GPP definen cómo se logra el interfuncionamiento entre una E-UTRAN (LTE y LTE-Advanced), GERAN (red de acceso por radio de GSM / GPRS) y UTRAN (red de acceso por radio de tecnologías basadas en UMTS WCDMA y HSPA) (Jimenez & Rizo, 2013).

El EPS también permite que las tecnologías no 3GPP interconecten el UE y el EPC. No 3GPP significa que estos accesos no se especificaron en el 3GPP. Estas tecnologías incluyen, por ejemplo, WiMAX, cdma2000, WLAN o redes fijas. Los accesos que no son 3GPP se pueden dividir en dos categorías: los "confiables" y los "no confiables":

- Los accesos confiables que no son 3GPP pueden interactuar directamente con el EPC.
- Los accesos que no son 3GPP no confiables interactúan con el EPC a través de una entidad de red llamada ePDG (para Evolved Packet Data Gateway). La función principal

del ePDG es proporcionar mecanismos de seguridad como el túnel IPsec de las conexiones con el UE a través de un acceso que no es de confianza y que no es 3GPP.

3GPP no especifica qué tecnologías que no son 3GPP deben considerarse confiables o no confiables. Esta decisión la toma el operador (Firmin, 2018).

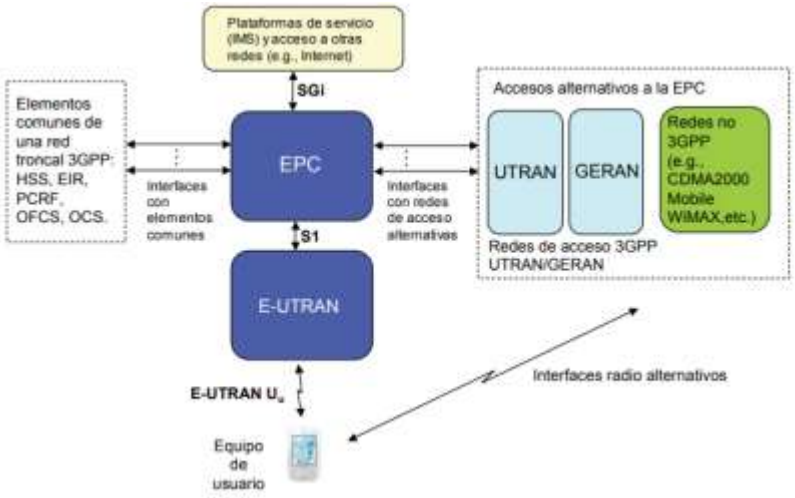


Figura 3-1: Arquitectura del sistema LTE

Fuente: (Jiménez, 2013)

A continuación, se resume las principales características de LTE release 8 (Xiang et al, 2018):

- Uso del espectro: 900 / 1800 / 2000 / 2600 MHz (y otras).
- Flexibilidad de ancho de banda: 1, 4 / 3 / 5 / 10 / 15 / 20 MHz.
- Tasas de 100 Mbit/s en DL y 50 Mbit/s en UL.
- Retardos reducidos en establecimiento y transmisión (latencia inferior a 10 ms).
- Modos dúplex FDD yTDD.
- Multiacceso OFDMA en DL y DFTS-OFDM (SC-FDMA) en UL.
- Modulaciones QPSK, 16QAM y 64 QAM.
- Técnicas multiantena: diversidad, conformación de haces (beamforming) y MIMO.
- Técnicas de protección frente a las variaciones del canal: rate control, channel dependent scheduling, hybridARQ with soft combining.
- Coordinación de interferencia (ICIC, Inter-Cell Interference Coordination).
- Compatibilidad con otras tecnologías de 3GPP.

1.2.1 Arquitectura de E-UTRAN

La arquitectura de E-UTRAN está compuesta por una sola entidad de red llamada evolved NodeB (eNB) la misma que constituye la estación base. La estación base realiza todas las funciones de

la red de acceso. Los estándares de la arquitectura de E-UTRAN se encuentra en 3GPP TS 36.300 y TS 36.401. Como se puede observar en la figura 4-1 los eNBs funcionan de intermediarios entre los equipos de usuarios y la red troncal. Para la conectividad del eNB con los elementos del sistema se definen las interfaces S1, X2 y UTRAN Uu.

El eNodeB es el que se encarga de todas las funciones relacionadas con la interfaz radio en una o varias celdas. Es importante tener en cuenta que un eNodeB es un nodo lógico y no una implementación física. La implementación común de un eNodeB es un sitio de tres sectores, en la cual una estación base está manejando transmisiones en tres celdas, aunque también se pueden encontrar otras implementaciones, como una unidad de procesamiento de banda base a la que se conectan varios cabezales de radio remotos (Dahlman et al.,2011).

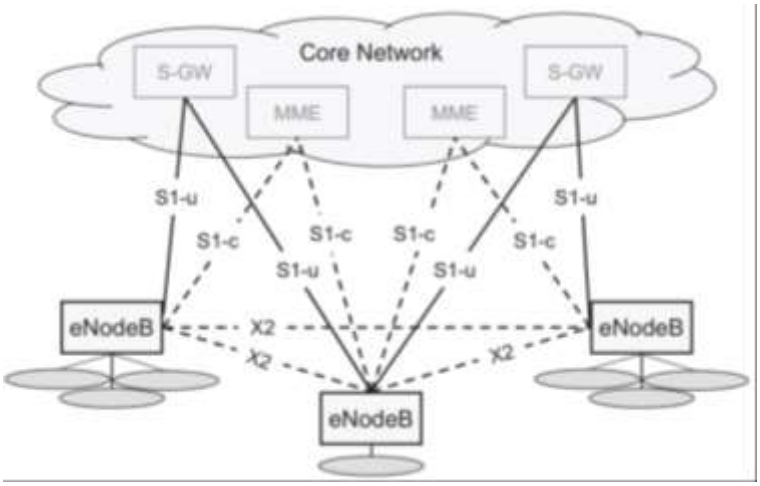


Figura 4-1: Red de acceso E-UTRAN

Fuente: (Dahlman et al., 2013)

Para que el equipo de usuario pueda conectarse a la red se define la interfaz E-UTRAN Uu, la cual hace posible enviar/recibir datos por el canal radio. El eNB contempla todas las acciones y protocolos necesarios para la realización del envío o recepción de paquetes de datos y paquetes de control a través de la interfaz E-UTRAN Uu.

La conectividad entre el eNB y el EPC es a través de la interfaz S1, la cual en realidad se divide en: S1-MME para sustentar el plano de control y S1-U como soporte del plano de usuario. El plano de usuario se refiere a la pila de protocolos empleada para la transmisión de tráfico de usuario a través de dicha interfaz (paquetes IP del usuario de voz o datos). El plano de control se refiere a la pila de protocolos necesaria para sustentar las funciones y procedimientos en la gestión de la operación de dicha interfaz o de la entidad correspondiente (paquetes IP de señalización). Al separar el plano de usuario y plano de control en la interfaz S1, permite que el eNB se conecte

con dos entidades diferentes entidades de EPC. Así, el eNB se comunica con MME mediante la interfaz S1-MME, ya que MME es la encargada de gestionar las funciones relacionadas con el plano de control de usuario. En cambio, con la interfaz S1-U, el eNB se comunica con la entidad S-GW que se encargada de procesar los datos del usuario (Comes, 2010).

1.2.2 Arquitectura de EPC

El núcleo EPC está diseñado para soportar una conectividad IP, junto con una estructura de red que utilice todas las funciones diseñadas y estandarizadas en E-UTRAN. Además, otro factor que resalta en la arquitectura EPC es que tiene interconectividad e interoperabilidad con tecnologías 3GPP (UTRAN y GERAN) o tecnologías no 3GPP (cdma2000, WiMAX, 802.11). La descripción completa de la red troncal EPC se recoge en los documentos 3GPP TS 23.401 y 3GPP TS 23.402. En particular, en la especificación TS 23.401 se cubre la arquitectura de la red troncal EPC cuando la red de acceso es E-UTRAN, así como la utilización de redes de acceso 3GPP alternativas o complementarias como UTRAN y GERAN. Por otro lado, la especificación TS 23.402 extiende la arquitectura de la red troncal EPC para soportar el acceso a través de otras redes no 3GPP.

Dos principios fundamentales han estado guiando el diseño de la arquitectura. En primer lugar, el fuerte deseo para optimizar el manejo de tráfico de datos del usuario en sí, mediante designaciones a una arquitectura "plana". Una arquitectura plana en este contexto significa que está involucrado el menor número de nodos posibles en el procesamiento del tráfico de datos del usuario (Olsson et al., 2009: pp. 37-49).

La primera motivación para esto fue el permitir un costo eficiente escalable de la infraestructura operativa sobre el tráfico de datos del usuario en sí, un argumento cada vez más importante como el volumen de tráfico de datos móviles que está creciendo rápidamente y se espera que crezca aún más rápido en el futuro con la introducción de nuevos servicios que se basan en IP, así como nuevas tecnologías tal como LTE y 5G.

La segunda guía principal fue la separación del manejo del plano de señalización del tráfico de datos del usuario. Esto fue motivado por diversos factores. La necesidad de permitir una independencia escalable de las funciones de control y del plano de usuario, fueron vistas como importantes desde que la señalización del control de datos tiende a escalar con el número de usuarios, mientras que el volumen da datos de usuarios puede escalar más dependiendo de nuevos servicios y aplicaciones al igual que las capacidades en términos de dispositivos (Olsson et al., 2009: pp. 37-49).

La arquitectura en la Figura 5-1 contiene únicamente las entidades de red que conforman parte del núcleo EPC los cuales hacen posible brindar los servicios de conectividad basados en IP mediante E-UTRAN, control de calidad de servicio QoS, mecanismos de autenticación, etc. Es importante recalcar que las entidades de red en base a las cuales se realiza la descripción de la estructura de EPC son entidades funcionales, es decir una entidad de red en 3GPP se describe como una entidad "lógica" que cubre una funcionalidad perfectamente delimitada. Por tanto, una implementación concreta de la red troncal EPC admite que diferentes entidades funcionales puedan estar en el mismo equipo físico.

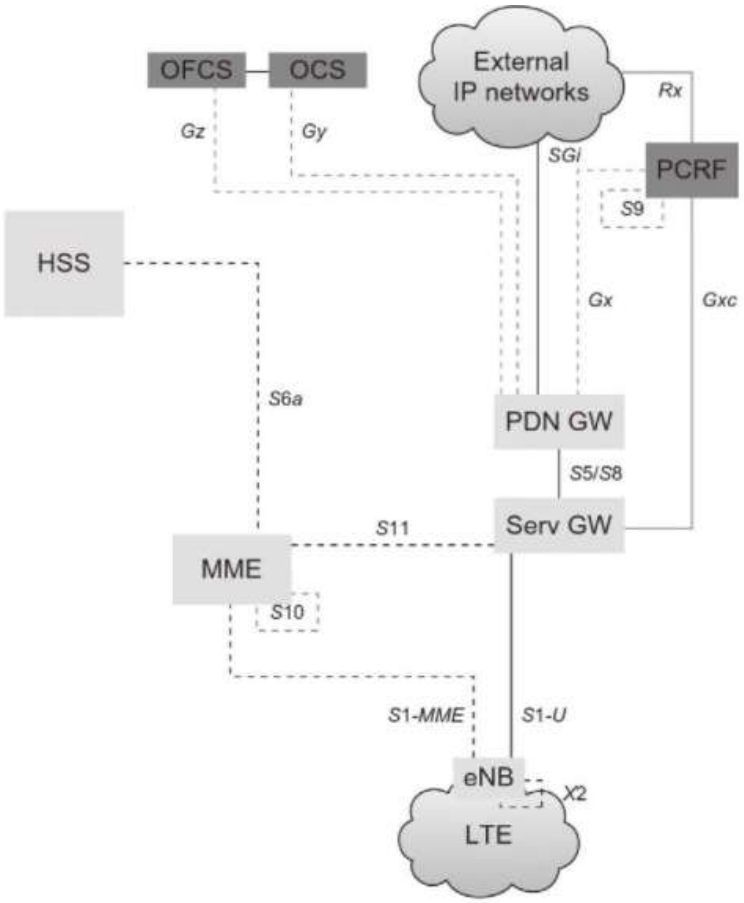


Figura 5-1: Arquitectura básica de la red troncal EPC

Fuente: (Olsson et al., 2009: pp. 37-49).

En la Figura 5-1 se puede apreciar que el núcleo está conformado por tres entidades de red principales: MME (Mobility Management Entity), Serving Gateway (S-GW) y Packet Data Network Gateway (P-GW). Además, junto con la base de datos denominada HSS (Home Subscriber Server), forman los elementos básicos para el funcionamiento de una central 4G. Las funciones asociadas con el plano de usuario son realizadas por S-GW y P-GW, en cambio MME lleva a cabo las funciones en el plano de control (Comes, 2010).

La interfaz S1 sirve de pasarela de comunicación entre EPC y E-UTRAN, esta interfaz S1 se subdivide en dos, para el plano de control la interfaz S1-MME se conecta con la entidad del núcleo llamada MME, mientras que en el plano de usuario se conecta a través de la interfaz S1-U a la entidad S-GW. Para que un equipo de usuario UE pueda conectarse a la red debe proceder a autenticarse, para ello la entidad MME es la encarga de realizar este procedimiento mediante los protocolos NAS. Finalmente, tal como puede observarse en la Figura 5-1, las entidades MME tienen la posibilidad de intercambiar información mediante la interfaz S10 (Comes, 2010).

El intercambio de información del plano de usuario en EPC se realiza por la entidad S-GW mediante la interfaz S1U. Por esta pasarela se encamina todo el tráfico de voz y datos que genera el usuario al enviar o recibir llamadas, documentos, archivos, etc. Esta entidad S-GW envía todo el tráfico generado por el usuario a la pasarela P-GW con la ayuda de la interfaz S5, cuando el mismo operador es dueño de ambas pasarelas, y mediante S8, cuando éstas son de operadores diferentes y se está brindando el servicio conocido como roaming o itinerancia. La interconexión con redes externas o plataformas de servicio como plataformas IMS es a través de P-GW (Comes, 2010).

En la Tabla 2-1 se resumen las entidades de red e interfaces propias de EPC. En la tabla también se indican las especificaciones del 3GPP más relevantes relacionadas con cada una de ellas.

Tabla 1-1: Entidades de red e interfaces de EPC para el acceso desde E-UTRAN

	Nombre	**Estándar en 3GPP**
Entidades de red EPC	MME	TS 23.401
	S-GW	TS 23.401
	P-GW	TS 23.401
Entidades comunes a las redes 3GPP	**Nombre**	**Estándar en 3GPP**
	HSS	TS 23.002 TS 23.008
	PCRF	TS 23.203
	OCS	TS 23.203

		TS 32.240
	OFCS	TS 23.203 TS 32.240
Interfaces	**Nombre**	**Estándar**
	S1-MME	Documentos TS 36.41x
	S1-U	TS 29.281
	SGi	TS 29.061
	S6a	TS 29.272
	S5/S8	TS 29.274 (opción GTP) TS 23.275 (opción PMIPv6)
	S11	TS 29.274
	S10	TS 29.274
	Señalización NAS	TS 24.301
	Rx	TS 29.214
	S9	TS 29.215
	Gx/Gxc	TS 29.212
	Gz/Gy	Documentos TS 32.2xx

Fuente: (Comes, 2010)

Realizado por: (Henry Yugsin, 2022)

1.2.2.1 MME (Mobility Management Entity)

En el plano de control de una red LTE la entidad MME es parte fundamental ya que cumple la función de gestionar el acceso de todos los equipos de usuarios que se encuentren registrados en la red LTE. El MME se selecciona de acuerdo a la ubicación del UE y los criterios de balanceo de cargas que se realiza a través de la interfaz S1. Este MME debe almacenar diversos datos claves del usuario como las claves de seguridad, conexiones y servicios portadores EPS activos, etc. Un usuario puede cambiar de entidad MME asignada, esto debido a la capacidad que tiene el usuario para movilizarse en la red. MME tiene las siguientes funciones principales (Comes, 2010):

- Identificación, autenticación y autorización. El HSS entrega los datos necesarios a la entidad MME (mediante la interfaz S6a) para que este lleve a cabo el proceso de controlar el acceso mediante un proceso AAA.
- Gestión de los servicios portadores EPS. Gestionar la señalización requerida para establecer, liberar, modificar y mantener los servicios portadores EPS sobre los cuales se están intercambiando los paquetes IP.
- Gestión de movilidad de equipos de usuario en modo idle (equipos de usuarios que no están conectados a la red E-UTRAN, es decir están inactivos). Esta gestión es conocida específicamente como gestión de localización y consiste básicamente en que la entidad MME dentro del área de servicio realiza constantemente una geolocalización.
- Terminación de los protocolos de señalización NAS.

1.2.2.2 Serving Gateway (S-GW)

La entidad S-GW cumple la función de pasarela del plano de usuario entre el EPC y E-UTRAN. A la par que MME, a un usuario registrado en la red LTE se le asigna una entidad S-GW y mediante ella pasa su plano de usuario. Las principales características del S-GW (Comes, 2010):

- Esta entidad brinda un punto de anclaje en la red troncal con respecto a la movilidad del UE entre eNBs. Esto ayuda al momento de realizar el proceso de handover entre eNBs.
- Gestión de movilidad con las otras redes de acceso 3GPP, para ello también se aplica la funcionalidad de punto de anclaje que brinda S-GW. De esta forma, los usuarios pueden enviar trafico basado en IP hacia otras redes no 3GPP o 3GPP.
- En caso de que los usuarios se encuentren en modo idle, la entidad S-GW puede almacenar temporalmente los paquetes IP de dicho usuario.
- Enrutamiento del tráfico de usuario. Esta pasarela cumple la función de un conmutador de paquetes ya que envía los paquetes IP del plano de usuario a la entidad encargada en este caso a P-GW.

1.2.2.3 PDN Gateway (P-GW)

La entidad P-GW se encarga de proporcionar conectividad entre la red LTE y redes externas. Es decir, P-GW hace posible que un usuario sea "visible" en la red IP externa. Por tanto, los paquetes IP que se generan en el UE son inyectados en la red externa mediante el enrutador P-GW y, viceversa. P-GW tiene las siguientes características principales (Koodli & Perkins, 2007):

- Controla ciertas funciones que forman parte del marco PCC como el control de tarificación que se dan en los servicios portadores del usuario y aplicación de las reglas de uso.
- Asignación de dirección IP al equipo de usuario. Una vez que el usuario es autenticado correctamente por el MME la pasarela P-GW tiene el deber de asignarle una dirección IPv4 o IPv6. El UE recibe esta dirección IP con la ayuda de los protocolos NAS y la P-GW utiliza el mecanismo DHCP para asignar dichas IP.
- P-GW sirve como pasarela de comunicación entre la red 4G y otras redes 3GPP o no 3GPP.

1.2.2.4 HSS (Home Subscriber Server)

En HSS se almacena la información de los usuarios de la red, ya que esta entidad es la base de datos principal del sistema LTE. Aquí se almacena la información del usuario es decir el perfil de suscripción y la información necesaria para el correcto funcionamiento de la red. Es una base de datos relacional ya que puede ser consultada, modificada y escrita desde las entidades con autorización como el MME, SGSN. El HSS guarda tanto información permanente, como información que está en constante modificación debido a la propia operación del sistema (geolocalización del UE). En esta base de datos la información primordial de un usuario es la IMSI, ISDN, MSISDN, vectores de autenticación, identificador de MME e información de los servicios pagados por el usuario establecidas en el contrato de suscripción. (Comes, 2010).

La entidad HSS se estandarizó en 3GPP R5. A continuación, se pueden destacar algunas de sus funciones principales:

- El subgrupo de funciones de las entidades AuC/HLR esencial para el correcto funcionamiento del dominio de paquetes en el núcleo EPC, así como GPRS. Esta entidad se comunica mediante la interfaz S6a.
- El subconjunto de funciones de las entidades AuC/HLR necesarias para el funcionamiento del dominio CS.
- Funciones de apoyo asociadas a las funciones de control del subsistema IMS como gestionar la información relativa a la subscripción de servicios IMS y el almacenamiento de perfiles de usuario asociados a servicios IMS.

La información almacenada en el HSS se detalla en la especificación 3GPP TS 23.008 (3GPP, 2015).

1.2.3 Interfaces de comunicación

1.2.3.1 Interfaz Radio

Existen básicamente tres tipos de mecanismos de transferencia de la información que soporta la interfaz radio: envió de paquetes IP, difusión de señalización de control y transferencia de señalización de control dedicada entre un equipo de usuario y el eNB. Se los observa en la Figura 6-1 y se describen a continuación (Comes, 2010):

- Difusión (broadcast) de control de señalización en la zona de cobertura de la celda. La información transmitida hace posible que el equipo de usuario pueda detectar la presencia del eNB.
- Transferencia de paquetes IP de los equipos de usuarios mediante el canal radio.
- La señalización de control se realiza mediante esta interfaz entre el UE y el eNB.

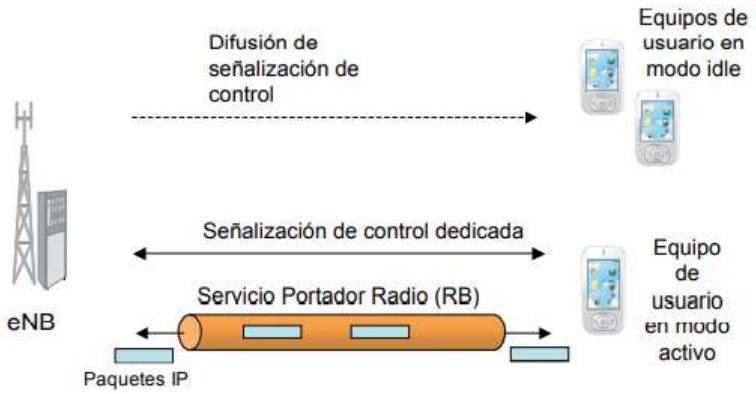


Figura 6-1: Ilustración de los mecanismos de transferencia de información en la interfaz radio

Fuente: (Peñuelas et al., 2012)

1.2.3.2 Interfaz eNB-EPC (S1)

La interfaz S1 es la que conecta los eNodeB con el EPC. Esta interfaz se divide en dos partes, una para el plano de usuario (la S1-U hacia la S-GW) y otra para el plano de control (la S1-MME hacia la MME). La capa física y la de enlace de datos no están especificadas en el estándar para ninguno de los planos. Por el contrario, la capa inmediatamente superior es IP en ambos casos. Tanto los eNodeB como las MME deben soportar IPv6/IPv4. A partir de este punto la pila de protocolos es distinta para cada plano (Peñuelas et al., 2012).

El llamado S1-U, transfiere la información del usuario entre eNB y S-GW pero no asegura que la información va a llegar a su destino (basado en UDP). Este toma el nombre de servicio portador S1 (S1 bearer). El plano de control, llamado S1-MME o también S1-C, se utiliza para soportar un

conjunto de procedimientos y funciones de control entre eNBs y la entidad MME de la red troncal. En la Figura 7-1 se ilustra dicho control del plano de usuario por parte de la entidad MME (Peñuelas et al., 2012).

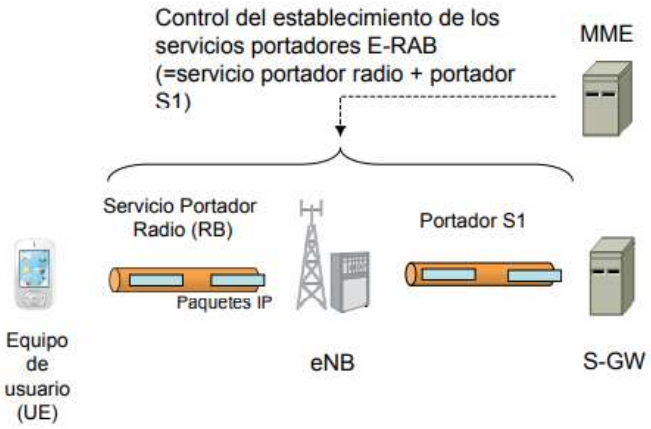


Figura 7-1: Control de los servicios portadores radio y S1 a través de la interfaz S1-MME

Fuente: (Peñuelas et al., 2012)

1.2.3.3 Interfaz eNB – eNB (X2)

La interfaz X2, que conecta los eNodeB entre sí, se utiliza principalmente para admitir la movilidad en modo activo. Esta interfaz también se puede utilizar para funciones de gestión de recursos de radio (RRM) de varias celdas, como la coordinación de interferencias entre celdas (ICIC). La interfaz X2 también se usa para admitir la movilidad sin pérdidas entre células mediante el reenvío de paquetes. El plano de usuario de X2 se encapsula en UDP al igual que S1 por lo que proporciona un servicio de transferencia de datos de usuario entre eNBs pero no garantiza que los paquetes de datos llegaran completos a su destino, además no tiene soporte de mecanismo de control de errores y de control de flujo. Únicamente en el proceso de handover se da la transferencia de datos del usuario entre eNBs (Dahlman et al., 2013).

1.2.3.4 Interfaz P-GW Redes Externas (SGi)

Mediante la interfaz SGi se realiza la conexión de la entidad P-GW de la red LTE con redes externas IP. La red externa puede ser tanto una red pública (Internet) o privada (intranet corporativa, red de un ISP, red interna del propio operador, etc). La interfaz SGi es equivalente a la interfaz Gi especificada para la interconexión de la pasarela GGSN del dominio GPRS con redes externas (Kaaranen et al., 2005: pp. 47-68).

La interfaz SGi está diseñada para soportar trafico IPv4 como IPv6. Vista desde otra perspectiva, P-GW es como un router IP convencional. Existen dos maneras básicas de interconexión de la red 4G con redes externas: acceso transparente y acceso no transparente. Estas maneras de conectividad se ilustran en la Figura 8-1 y se describen a continuación.

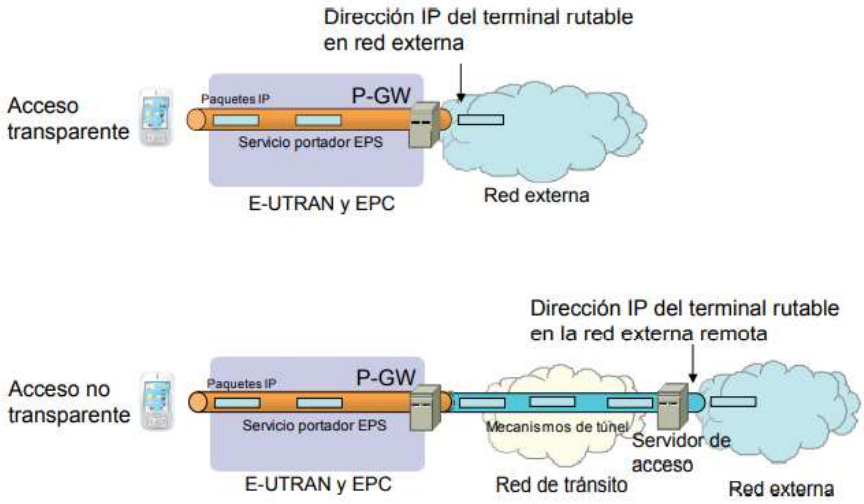


Figura 8-1: Tipos de interconexión a través de SGi

Fuente: (Peñuelas et al., 2012: pp. 124-137)

Con el modelo de interconexión transparente, el equipo de usuario resulta "visible" para la red externa, esto se debe a que la dirección IP asignada al terminal es convalida en SGi y en la red externa, la misma que es accesible mediante la pasarela SGi. En cambio, en el modelo no transparente, la red LTE ofrece un acceso a una red externa de forma que el espacio de direcciones utilizado por los terminales pertenece al espacio de direcciones de la red externa remota. La interfaz SGi y los diferentes tipos de acceso a la red externa se especifican en 3GPP TS 29.061 (3GPP, 2015).

1.2.3.5 Interfaz MME S-GW (S11)

La interfaz S11 es la interconexión entre la entidad MME y S-GW esto con la finalidad de controlar el plano de usuario desde la entidad MME. Así, los procedimientos soportados en esta interfaz permiten la creación, eliminación, modificación y cambio de los servicios portadores que los equipos de usuario tienen establecidos a través de la red troncal LTE. La funcionalidad de esta interfaz se recoge en 3GPP TS 23.401 (3GPP, 2015) y el protocolo GTPv2-C que da soporte a esta interfaz se especifica en TS 29.274 (3GPP, 2015).

1.2.3.6 Interfaz MME MME (S10)

Para unir dos entidades MME se define a la interfaz S10. Tiene como objetivo soportar el mecanismo de reubicación de la entidad MME. De esta forma, cuando la entidad MME que controla a un determinado usuario debe cambiarse (debido, por ejemplo, a su movilidad), a través de la interfaz S10 se realiza la transferencia de la información entre MMEs. La funcionalidad de esta interfaz se recoge en 3GPP TS 23.401 (3GPP, 2015) y el protocolo GTPv2-C que da soporte a esta interfaz se especifica en TS 29.274 (3GPP, 2015).

1.2.3.7 Interfaz HSS MME (S6a)

Para la interconectividad entre la base de datos HSS y la entidad MME se defina la interfaz S6a. S6a cumple con los siguientes criterios de diseño (Comes, 2010):

- Mantenimiento de información de gestión de la localización.
- Autorización de acceso a la red LTE.
- Autenticación de los usuarios.
- Notificación y descarga de la información correspondiente a la identidad de P-GW que utiliza un equipo de usuario en una conexión.

La interfaz S6a además soporta escenarios de itinerancia donde una entidad MME de un operador puede acceder a la base de datos de otro operador. La interfaz S6a se basa en el protocolo Diameter. La funcionalidad de la interfaz se recoge en TS 23.401 (3GPP, 2015) y la especificación de la extensión (Diameter application) del protocolo se aborda en TS 29.272 (3GPP, 2015).

1.2.4 Protocolos de Comunicación

1.2.4.1 Protocolos en la Interfaz Radio

Él envió de paquetes IP entre un equipo de usuario UE y el eNB es mediante la interfaz radio, la misma que se sustenta en una torre de protocolos formados a nivel de la capa de enlace (capa 2) y una capa física (capa 1). La pila de protocolos utilizados se muestra en la Figura 9-1. La capa de enlace se divide en tres subcapas: Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC) y Medium Access Control (MAC). Cada subcapa se encarga de un conjunto de funciones. A continuación, se describen las principales características de cada una (Morfa, 2013):

- Packet Data Convergence Protocol (PDCP). La capa PDCP se encarga de comprimir y descomprimir las cabeceras IP a través de ROHC (RObust Header Compression - RFC 3095), y también realiza el cifrado de datos en el plano de usuario y en el plano de control.
- Radio Link Control (RLC). La capa RLC realiza las funciones de segmentación/concatenación/reensamblaje de las Unidades de Datos de Servicio (SDU) RLC, reordenación de SDU, entrega secuencial y corrección de errores a través del

mecanismo ARQ. La capa RLC puede operar en uno de los tres modos de confiabilidad: el modo de reconocimiento (AM - Modo reconocido), el modo no reconocido (UM - Modo no reconocido) o el modo transparente (TM - Modo transparente). El modo UM admite segmentación/reensamblaje, entrega secuencial, no admite retransmisiones y es adecuado para servicios en tiempo real como VoIP. El modo AM, por otro lado, admite retransmisiones y es adecuado para servicios que no se transmiten en tiempo real, como archivos descargables. El modo TM es completamente transparente, no admite retransmisiones, segmentación/reensamblaje ni entrega secuencial.

- Medium Access Control (MAC). La subcapa MAC realiza la programación de recursos de canales compartidos. En el enlace descendente, el programador eNodeB decide sobre el UE particular y el SRB/DRB particular del UE desde el cual multiplexar las PDU RLC en el TB que transmite. En el enlace ascendente, el programador eNodeB decide a qué UE asignar los recursos PUSCH, y el UE decide el SRB/DRB particular desde el cual multiplexar las PDU RLC en el TB. Las entidades MAC en los lados de transmisión y recepción transmiten TB utilizando HARQ, y el lado de recepción extrae la PDU RLC del TB y la transfiere a la entidad RLC.
- Capa física. Es la capa que tiene como función la transmisión propiamente dicha a través del canal radio (emitir y recibir la onda electromagnética). En el enlace descendente, el esquema de transmisión es OFDMA. Se les conoce como canales de transporte a los servicios de transferencia de la capa MAC. Solo existe una única entidad de capa física por cada celda

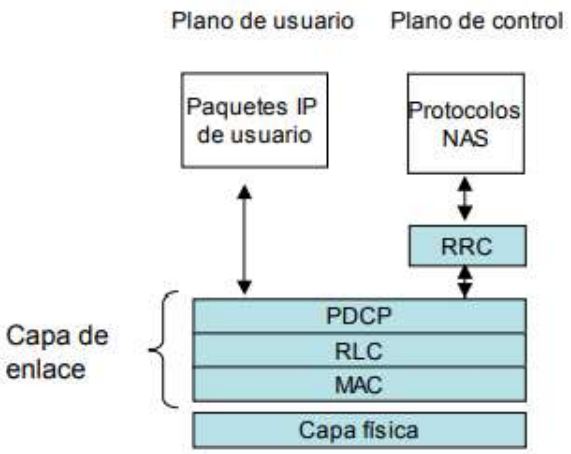


Figura 9-1: Protocolos de la interfaz radio de E-UTRAN

Fuente: (3GPP, 2015)

Respecto al plano de control entre el usuario y la red LTE, éste plano de control se soporta sobre la misma capa de enlace (protocolos PDCP, RLC, MAC) y la misma capa física utilizada en el plano de usuario. Los protocolos de nivel de red específicos de este plano de control son:

- Radio Resource Control (RRC). Esta capa hace posible establecer una conexión de control entre el eNB y el usuario mediante la cual se llevan a cabo un número importante de funciones relacionadas con la gestión de la operativa de la interfaz radio. Entre dichas funciones de la capa RRC destacan los mecanismos de gestión de los servicios portadores radio, el soporte de funciones de movilidad (señalización de handover), la difusión (broadcast) de parámetros de sistema y funciones de aviso de los terminales que no disponen de una conexión RRC establecida (envío de avisos a través del canal de paging). Se denomina servicio portador de señalización (Signalling Radio Bearer, SRB) a los servicios de transferencia que ofrece la capa PDCP para el envió de los mensajes de señalización del protocolo RRC (Morfa, 2013).
- Señalización de los protocolos NAS. Estos protocolos NAS se extienden entre la entidad MME en la red troncal y el usuario. Los mensajes de estos protocolos se transportan de forma transparente en la interfaz radio encapsulados dentro de la parte de datos de los mensajes RRC.

1.2.4.2 Protocolos en las Interfaces S1 y X2

Para soporta las interfaces S1 y X2 de E-UTRAN la estructura de protocolos establece una división entre la capa de red de transporte (Transport Network Layer, TNL) y la capa de red radio (Radio Network Layer, RNL). Esta partición tiene como objetivo separar las funciones que son específicas del sistema de comunicaciones móviles (LTE o UMTS), de otras que dependen de la tecnología de transporte utilizada (IP, ATM). Así, la capa RNL está constituida por protocolos específicos de la red de acceso radio, por otro lado, los protocolos utilizados para transportar la información de la capa RNL entre las entidades de red son los que conforman la capa TNL. En la Figura 10-1 se ilustra la arquitectura de protocolos de las interfaces S1 y X2. Los documentos de base del 3GPP que especifican la estructura de las interfaces S1 y X2 son, respectivamente, 3GPP TS 36.410 (3GPP, 2015) y TS 36.420 (3GPP, 2015).

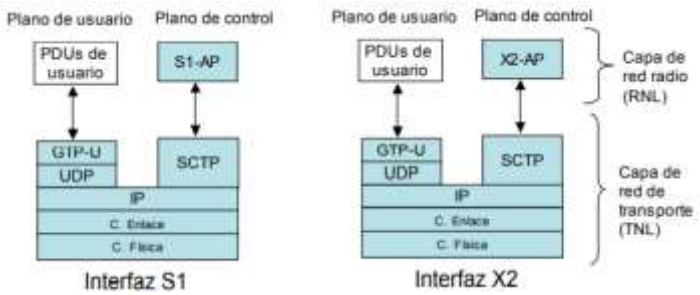


Figura 10-1: Protocolos en las interfaces S1 (izquierda) y X2 (derecha)

Fuente: (3GPP, 2015)

Para el plano de usuario tanto en la interfaz S1 (S1-U) como en la interfaz X2 se utiliza el protocolo de encapsulado GTP-U (GPRS Tunneling Protocol – User Plane) para la transmisión de paquetes IP de usuario. El protocolo GTP-U es un protocolo heredado de GPRS. En las interfaces S1-U y X2, el protocolo GTP-U se encapsula sobre UDP/IP y fundamentalmente se utiliza para multiplexar los paquetes IP de múltiples usuarios (se le asigna un identificador de túnel único a cada servicio portador). Por último, es importante recalcar que los planos de usuario de ambas interfaces no contemplan mecanismos de entrega garantizada para la transferencia de los paquetes de usuario, ni tampoco mecanismos de control de errores o control de flujo, esto se debe a que se encapsulan en UDP.

La interfaz S1 (S1-MME o S1-C) contiene el plano de control, para este la capa de red radio se basa en el protocolo S1-AP (S1 - Application Part). Este protocolo es el que hace posible los procedimientos soportados en la interfaz S1 (establecimiento de servicios portadores en el eNB, control del handover, paging, etc.). La especificación del protocolo se realiza en el documento 3GPP TS 36.413 (3GPP, 2015). La transferencia de los mensajes de señalización del protocolo S1-AP entre eNBs y MMEs se realiza mediante el servicio de transferencia fiable que ofrece el protocolo de transporte Stream Control Transmission Protocol (SCTP).

SCTP es un protocolo de comunicaciones de la capa de transporte (similar a TCP y UDP) de propósito general el mismo que está definido en el estándar IETF en la RFC4960 (IETF, 2015) que originalmente fue diseñado para el envío de señalización de redes telefónicas sobre redes IP. SCTP hereda muchas de las funciones que tiene el protocolo TCP a la vez que introduce importantes mejoras encaminadas a proporcionar mayor robustez y versatilidad en la transferencia de diferentes tipos de información. En particular, existen mecanismos idénticos entre TCP y SCTP como el mecanismo de control de flujo y de congestión en la conexión, denominada asociación en SCTP. Por otro lado, SCTP añade soporte para multihoming (las asociaciones soportan la transferencia a través de múltiples caminos entre los nodos participantes), multi-streaming y el envío de la información se estructura en base a mensajes. Estas nuevas capacidades son las que hicieron que en 3GPP se decidiera por la utilización de este protocolo, en lugar de TCP, para implementar el plano de control de las interfaces S1 y X2 de E-UTRAN.

En la interfaz X2 para el plano de control, el protocolo que se utiliza para sustentar los procedimientos se denomina X2-AP (X2 Application Part) y se especifica en 3GPP TS 36.423 (3GPP, 2015).

1.2.4.3 Plano de usuario entre UE y EPC

En la Figura 11-1 se ilustra el plano de usuario completo de E-UTRAN para el envío de paquetes IP entre el equipo de usuario (UE) y la red troncal (la entidad S-GW). Los paquetes IP llevan en ellos la información correspondiente al servicio que el usuario está utilizando (voz, video, datos) así como la señalización a nivel de aplicación (protocolos SIP, RTCP, etc.). El eNB debe realizar funciones de "relay" entre la pila de protocolos PDCP, RLC, MAC, PHY de la interfaz radio y la pila de protocolos de la interfaz S1-U. Es importante recalcar que el eNB no toma ninguna decisión de encaminamiento o enrutamiento a partir de la información contenida en las cabeceras IP de los paquetes de usuario, sino que simplemente cumple la función de transferir los datos entre las dos interfaces cumpliendo asi los requerimientos de los servicios portadores definidos, es como una pasarela. (Morfa, 2013).

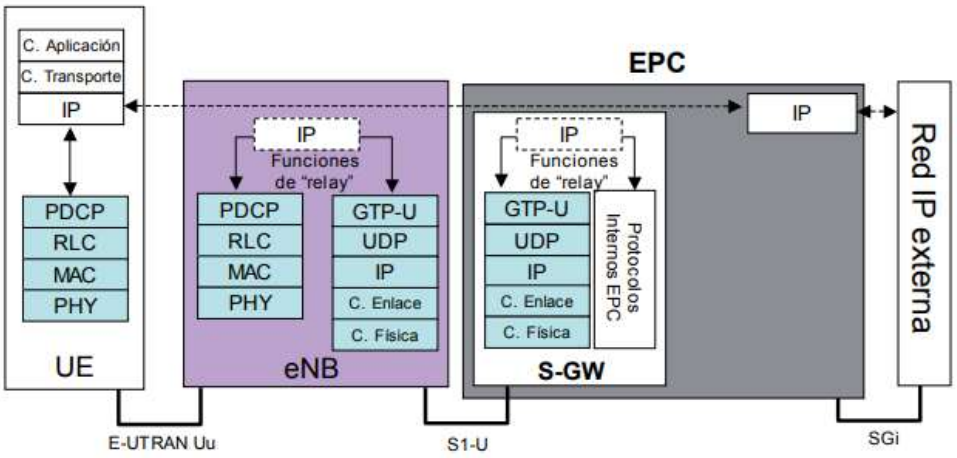


Figura 11-1: Protocolos del plano de usuario en E-UTRAN

Fuente: (Morfa, 2013)

1.2.4.4 Plano de control entre UE y EPC

En la Figura 12-1 se ilustra la pila de protocolos del plano de control para el envío de señalización NAS entre el equipo de usuario (UE) y la red troncal (EPC). Los protocolos NAS se transportan encapsulados (de forma transparente) dentro de mensajes RRC en la interfaz radio y en mensajes S1-AP en la interfaz S1-MME. El eNB realiza las funciones de "relay" necesarias entre ambas torres de protocolos (Morfa, 2013).

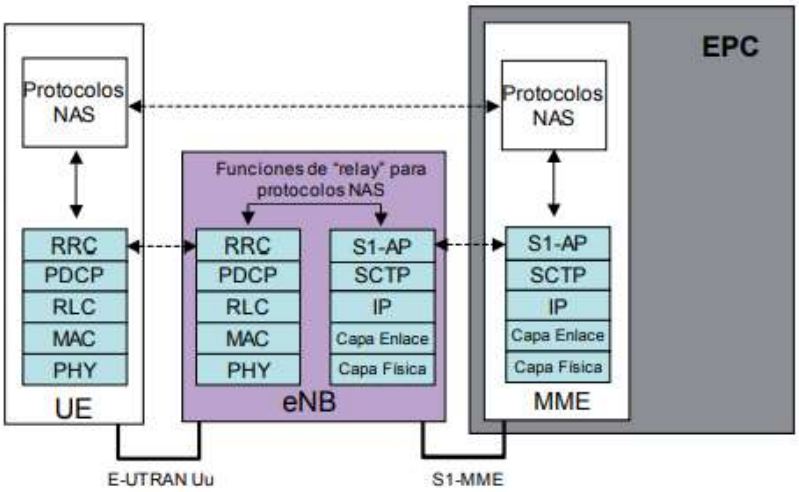
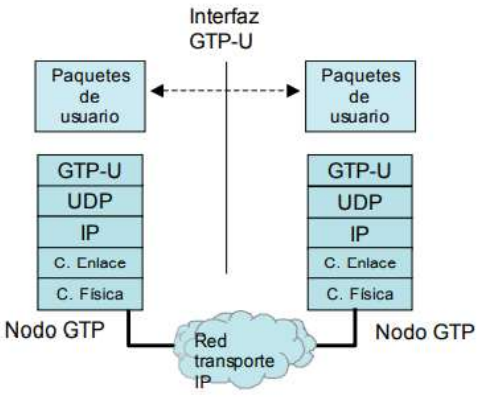


Figura 12-1: Protocolos del plano de control en E-UTRAN

Fuente: (Morfa, 2013)

1.2.4.5 Interfaces basadas en GTP-U

El protocolo GTP-U está diseñado para soportar el transporte de información del plano de usuario entre las diferentes entidades de la red troncal EPC a través de todas las interfaces de la red, excepto la variante de la interfaz S5/S8 basada en PMIPv6. La pila de protocolos utilizada en las interfaces basadas en GTP-U y el listado de dichas interfaces se proporciona en la Figura 13-1. Nótese que en la tabla ilustrada en la figura se indica el uso de GTP-U también sobre las interfaces S4 y S12. GTP-U además se utiliza en el plano de usuario de las interfaces internas de E-UTRAN, S1-U y X2-U, tal como se ha visto en apartado anteriores.



Interfaces	Nodos
S1-U	S-GW ↔eNB
S5/S8	S-GW ↔P-GW
S4	S-GW ↔SGSN
S12	RNC ↔SGSN
X2-U	eNB ↔eNB

Figura 13-1: Interfaces basadas en GTP-U

Fuente: (Comes, 2010)

Para poder dar respuesta a la implementación del servicio GPRS, 3GPP desarrolla el protocolo GTP-U. En este sentido, el plano de usuario entre los nodos de red del dominio GPRS así como el plano de usuario de la interfaz S1 de UTRAN se soportan también sobre dicho protocolo.

GTP-U brinda un mecanismo de encapsulado para la transmisión de paquetes IP de usuario entre nodos de una red IP. Los paquetes que corresponden a un mismo servicio portador EPS son transportados con un identificador de túnel único denominado TEID (Tunnel Endpoint Identifier). Esto se ilustra, en la Figura 14-1 que representa la implementación de un túnel entre las entidades S-GW y P-GW (interfaz S5/S8) mediante GTP-U. En la figura se observa que los paquetes IP del equipo de usuario llegan a la entidad S-GW a través de los servicios portadores radio y la interfaz S1. Las direcciones IP origen y destino de los paquetes de usuario recibidos en el S-GW contienen, respectivamente, la dirección asignada al terminal móvil y la dirección del equipo de la red externa al que vaya dirigido el paquete IP. Cabe recalcar que estas direcciones IP no tienen por qué pertenecer al rango de direcciones IP utilizado en la red de transporte que une las pasarelas S-GW y P-SW, de ahí la necesidad de establecer el túnel. Así, para proceder al envío de estos paquetes IP de usuario hacia P-GW, el nodo S-GW los encapsula mediante el protocolo GTP-U.

La cabecera del protocolo GTP-U está compuesta por un mínimo de 6 bytes y contiene el identificador de túnel TEID, junto con otros campos tales como identificadores de secuencia y longitud del paquete. El paquete GTP resultante tiene como dirección IP origen la dirección de S-GW y como dirección destino la dirección IP de P-GW. De esta forma, el paquete GTP puede ser enrutado en la red de transporte IP que une a ambas entidades. Una vez el paquete GTP llega a la pasarela P-GW, ésta extrae el paquete IP del usuario y lo inyecta en la red externa.

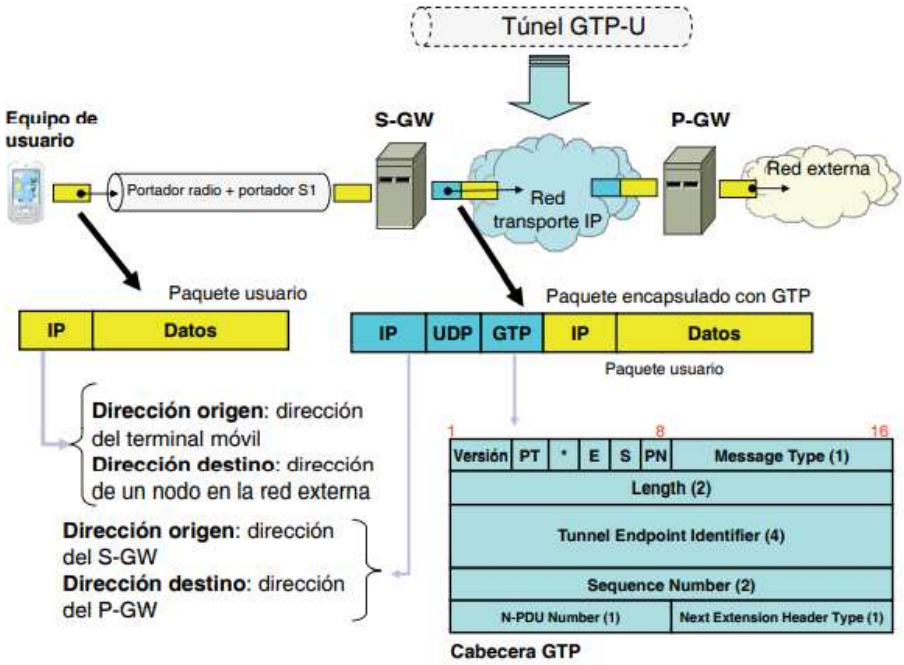


Figura 14-1: Ilustración del funcionamiento de un túnel GTP-U

Fuente: (Comes, 2010)

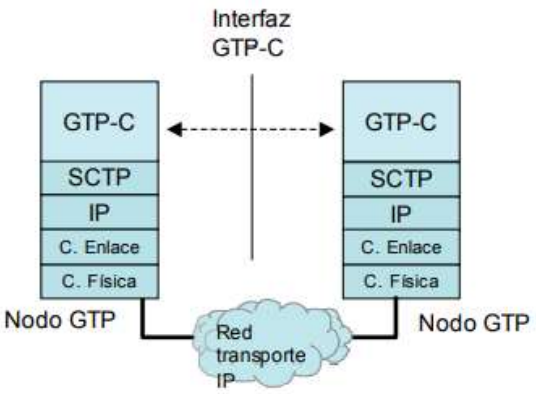
Para establecer un túnel GTP-U básicamente consiste en elegir el identificador TEID asociado a un determinado servicio portador EPS en ambos extremos del túnel. La señalización necesaria para establecer el túnel se realiza mediante otros protocolos como GTP-C o S1-MME. El protocolo GTP-U, y en particular su versión GTPv1-U, se utiliza tanto en LTE como en UMTS y se especifica en TS 29.281 (3GPP, 2015).

1.2.4.6 Interfaces basadas en GTP-C

El protocolo GTP-C soporta un conjunto de funciones que pueden clasificarse en torno a los siguientes aspectos:

- Gestión de sesiones. Mediante los procedimientos y mensajes de señalización que fueron diseñados para GTP-C, la red LTE administra la creación de nuevos túneles GTP-U entre las entidades de la red por donde transcurre el plano de usuario. Estos túneles forman parte de la propia gestión de sesiones en la red, mediante el establecimiento, mantenimiento, actualización y liberación de conexiones PDN y servicios portadores EPS.
- Gestión de movilidad. A través del protocolo GTP-C se llevan a cabo algunos de los procedimientos asociados con la gestión de movilidad tales como la transferencia de los contextos de información de los equipos de usuarios entre las entidades de red en casos de reubicación de las mismas.

En la Figura 15-1 se observa a la pila de protocolos de las interfaces que se basan en GTP-C y la relación de las interfaces con los nodos. En las interfaces S11, S5/S8, S10, S3, S4 y S16 por defecto y diseño se utiliza GTP-C. Nótese que no hay una correspondencia directa entre los interfaces que utilizan GTP-U en el plano de usuario (Figura 13-1) y GTP-C en el plano de control, ya que, tal como se ha mencionado, el protocolo GTP-C abarca otras funciones además de la gestión de túneles GTP-U. La versión del protocolo GTP-C utilizada en las interfaces de LTE, denominada como GTPv2-C, las cuales se especifican en TS 29.274 (3GPP, 2015).



Interfaces	Nodos
S11	S-GW ↔MME
S5/S8	S-GW ↔P-GW
S10	MME ↔MME
S3	MME ↔SGSN
S4	S-GW ↔SGSN
S16	SGSN ↔SGSN

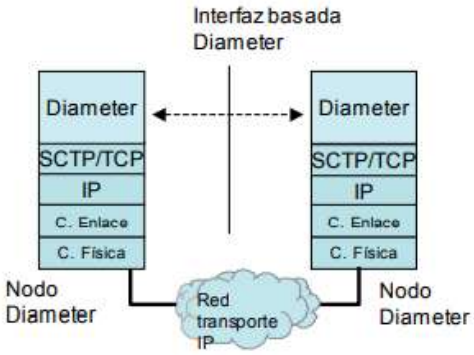
Figura 15-1: Interfaces basadas en GTP-C

Fuente: (3GPP, 2015)

1.2.4.7 Interfaces basadas en Diameter

El protocolo Diameter es inicialmente diseñado para sustentar funciones de Autenticación, Autorización y Accounting (AAA), este protocolo es una evolución del protocolo RADIUS. Diameter mejora las funciones de su antecesor RADIUS en aspectos tales como seguridad, robustez a pérdidas de mensajes, así como en su extensibilidad que permite el uso del protocolo para aplicaciones fuera del ámbito de AAA.

El protocolo Diameter se utiliza en un gran número de interfaces de la red LTE. La Figura 16-1 representa la pila de protocolos sobre la que se sustenta Diameter junto con una tabla donde se indican todas las interfaces del sistema LTE que utilizan este protocolo. La transferencia de los mensajes Diameter entre nodos se encapsula mediante un protocolo de transporte orientado a conexión como TCP o SCTP.



Interfaces	Nodos
S6a, S6d	HSS ↔MME,SGSN
SWx, STa, SWa, SWm, S6b, SWd	3GPP AAA Server ↔HSS, Red no-3GPP segura, Red no-3GPP no segura, ePDG, P-GW, 3GPP AAA Proxy
Gx, Gxa, Gxc, Rx, S9	PCRF ↔P-GW, S-GW, AF, PCRF
S13, S'13	EIR ↔MME, SGSN

Figura 16-1: Interfaces basadas en Diameter

Fuente: (3GPP, 2015)

El protocolo Diameter se estructura alrededor de un protocolo base (Diameter base standard definido en RFC 3588 (IETF, 2015)) y un número de extensiones llamadas aplicaciones. El protocolo de base aporta las funcionalidades comunes del protocolo Diameter: formatos de los mensajes y elementos de información genéricos (Attribute Value Pairs, AVPs), mecanismos de transferencia de mensajes, descubrimiento de capacidades de las entidades Diameter, aspectos de seguridad, etc. Las "aplicaciones" definen los mensajes adicionales y los procedimientos necesarios para adaptar el uso de Diameter al soporte de una determinada funcionalidad. Entre las aplicaciones de Diameter más sobresalientes y que están estandarizadas por IETF tenemos: Network Access Server Application (aplicación de Diameter para servicios AAA en el marco de control de acceso a redes, definido en RFC 4005 (IETF, 2015)) y Credit Control Application (aplicación de Diameter para la implementación de sistemas de tarificación on-line, como sistemas de pre-pago, definido en la RFC 4006 (IETF, 2015)). Además de IETF, otras entidades también pueden llevar a cabo la especificación de nuevas aplicaciones del protocolo, como es el caso de 3GPP. Estas aplicaciones de Diameter se denominan como "vendor-specific" y se les asigna un identificador unico de aplicación a través de IANA. Así pues, 3GPP ha definido distintas aplicaciones "vendor-specific" para la implementación de diferentes interfaces de la red LTE a través de extensiones del protocolo Diameter. Cada una estas aplicaciones de Diameter estan en un documento de especificación técnica del 3GPP. Por ejemplo, la aplicación de Diameter para la interfaz S6a/S6d se define en 3GPP TS 29.272 (3GPP, 2015).

1.2.4.8 Interfaces basadas en PMIPv6

En el RFC 5213 se define al protocolo PMIPv6 (Proxy MIPv6) el mismo que puede ser utilizado para administrar la movilidad a nivel de capa de red IP (capa 3). La entidad 3GPP adopto el protocolo PMIPv6 para su posible utilización en la interfaz S5/S8 entre las entidades S-GW y P-GW, como alternativa al uso del protocolo GTP. Al igual que la alternativa basada en GTP,

PMIPv6 proporciona una solución de movilidad de forma transparente al equipo de usuario, es decir, sin necesidad de que éste participe en la señalización pertinente. Este modelo de gestión de movilidad se lo denomina como gestión de movilidad "network-based", en contraposición al modelo "host-based" establecido por el protocolo MIP donde los nodos extremos (equipos de usuarios) participan en la gestión de movilidad (Koodli & Perkins, 2007). En la Figura 17-1 se observa el ámbito de utilización del protocolo de movilidad PMIPv6 junto con sus componentes funcionales. Este protocolo define una entidad llamada LMA (Local Mobility Anchor) que realiza labores similares a un Home Agent (HA) en MIP. Fundamentalmente el LMA mantiene una asociación entre la dirección IP que tiene asignada el equipo de usuario (y que no pertenece al rango de direcciones IP de la red de transporte IP que conecta el LMA y los MAGs) y la dirección IP hacia la que debe enviar los paquetes del usuario mediante un mecanismo de encapsulado de paquetes IP. De esta forma, en el caso de la interfaz S5/S8, todos los paquetes IP que llegan a P-GW (LMA) desde la red externa y que contienen como dirección destino la dirección IP asignada a un terminal, son encapsulados y enviados mediante un túnel PMIPv6 a S-GW correspondiente (MAG), y viceversa.

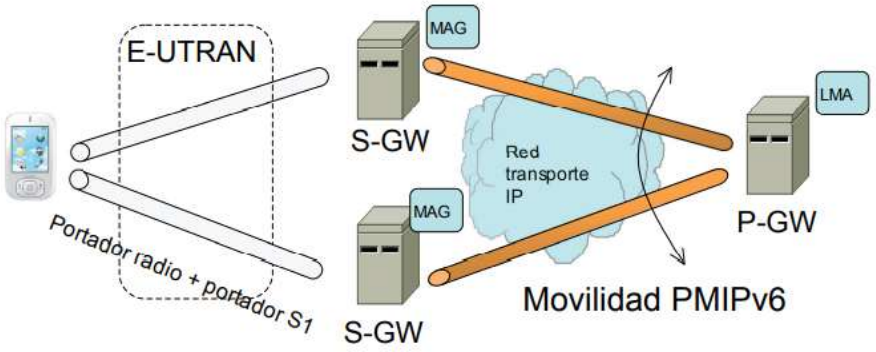
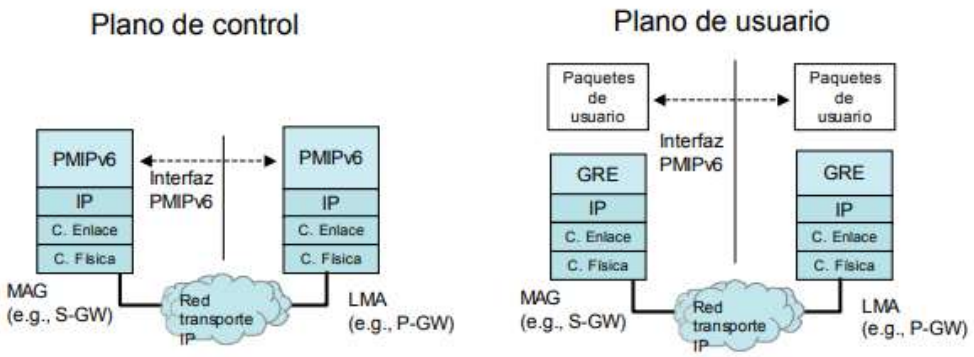


Figura 17-1: Ámbito y componentes del protocolo PMIPv6

Fuente: (Comes, 2010)

En la Figura 18-1 se observa los planos de control y de usuario del protocolo PMIPv6, junto con las interfaces que soportan este protocolo. El plano de control básicamente consiste en unos mensajes de señalización especificados en el protocolo que se envían en la parte de datos de los paquetes IP que se envían y reciben entre MAGs y LMA. El plano de usuario del protocolo se basa en el establecimiento de un túnel que permite enviar de forma transparente los paquetes IP de los usuarios (con direcciones IP de origen y destino pertenecientes al espacio de direcciones de la red externa) entre MAGs y LMA. Para ello, los paquetes IP de usuario se encapsulan dentro de la carga útil de paquetes IP mediante el protocolo GRE (Generic Routing Encapsulation). El protocolo GRE añade unas cabeceras al paquete IP de usuario que permiten asociar cada paquete con la conexión PDN a la que pertenece.



Interfaces	Nodos
S5/S8	S-GW ↔P-GW
S2a	P-GW ↔Red no 3GPP *trusted*
S2b	P-GW ↔ePDG

Figura 18-1: Interfaces basadas en PMIPv6

Fuente: (3GPP, 2015)

Aparte de la interfaz S5/S8, el protocolo PMIPv6 es uno de los protocolos especificados por 3GPP para el soporte de movilidad entre LTE y redes no 3GPP. En particular, las interfaces S2a y S2b están basadas en PMIPv6.

1.2.4.9 Protocolos NAS

El 3GPP desarrollo los protocolos NAS para llevar a cabo la gestión de movilidad de los equipos de usuario (EPS Mobility Managenement, EPM) y la gestión de las sesiones para el establecimiento de la conectividad entre el usuario y la pasarela P-GW (EPS Session Management, ESM). Los protocolos NAS se soportan entre el equipo de usuario y un nodo MME y se han desarrollado específicamente para E-UTRAN, aunque se mantienen muchas similitudes con los protocolos NAS utilizados en UMTS (Kaaranen et al., 2005: p. 47). En la Figura 19-1 se ilustra el alcance de los protocolos NAS en la red LTE.

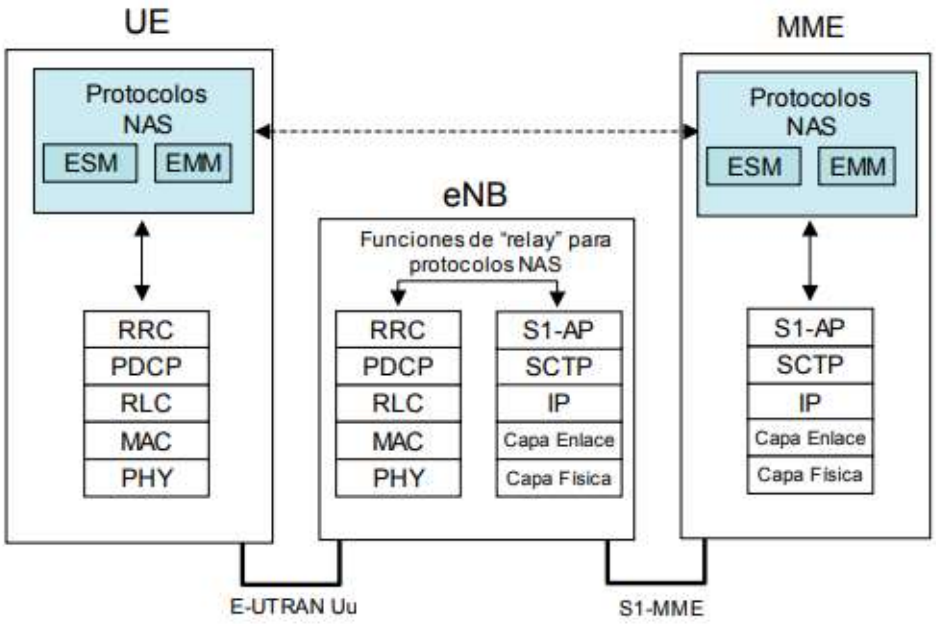


Figura 19-1: Protocolos NAS entre UE y MME

Fuente: (3GPP, 2015)

Protocolo NAS para la gestión de movilidad (EMM): El protocolo EMM brinda los procedimientos necesarios para el control de la movilidad de UE que utiliza E-UTRAN para el acceso a EPC. En particular, entre los procedimientos que soporta el protocolo EMM tenemos los mecanismos de "registro" y "cancelación de registro" del usuario en la red LTE (conocidos como Network Attach y Dettach) y la actualización del área de seguimiento (conocido como Tracking Area Update). Mediante estos procedimientos se gestiona y administra la accesibilidad a los servicios de la red LTE de los usuarios (la realización del registro en la red LTE es necesaria para que el usuario pueda iniciar o ser contactado para proceder a la activación de un servicio).

En el caso de equipos de usuarios que se encuentren en estado idle (modo inactivo), mediante el protocolo EMM se soporta el procedimiento de aviso (paging). En particular, el mensaje de aviso es un mensaje de señalización generado por el protocolo EMM que se distribuye a los equipos de usuarios mediante las funciones disponibles en la interfaz S1-MME. El procedimiento de aviso es utilizado por la red troncal EPC para forzar el re-establecimiento de la señalización de control con un equipo de usuario que se encuentre en modo idle. Asimismo, el protocolo EMM soporta un procedimiento de petición de servicio (llamado Service Request) por parte del usuario cuyo propósito es permitir "reactivar" el plano de usuario entre el S-GW y un usuario que se encuentre en modo idle. La petición del servicio la realiza el usuario cuando, por ejemplo, tiene paquetes IP pendientes de ser transmitidos.

El protocolo EMM también contiene funcionalidades que permiten a la red LTE interrogar al equipo de usuario para el envío de identificadores tales como el IMSI (International Mobile Subscriber Identity) o el IMEI (International Mobile Equipment Identity) y llevar a cabo la autenticación del usuario (procedimiento llamados EPS Authentication and Key Agreement, AKA). En particular el procedimiento EPS AKA permite la autenticación mutua entre el equipo de usuario y red LTE así como el establecimiento de una clave maestra a partir de la cual se derivan las claves de cifrado e integridad (Comes, 2010).

Finalmente, también cabe recalcar que es posible llevar a cabo el envío de información diversa entre el usuario y la red troncal EPC a través de un procedimiento de transporte sobre mensajes NAS soportado por el protocolo EMM. Mediante dicho procedimiento se puede soportar, por ejemplo, la transferencia de mensajes SMS a través de la red LTE. Los mensajes SMS se envían encapsulados en mensajes NAS EMM.

Protocolo NAS para la gestión de las sesiones (ESM): El protocolo ESM soporta los procedimientos necesarios entre el usuario y la red LTE para la gestión de los servicios portadores EPS cuando el usuario utiliza E-UTRAN.

Entre algunos de los procedimientos soportados por el protocolo ESM se encuentran los procedimientos de gestión (activación, desactivación, modificación) de los servicios portadores EPS. Además del servicio portador por defecto, pueden establecerse múltiples servicios portadores EPS dedicados que hacen posible aplicar un trato de QoS (calidad de servicio) específico a un determinado flujo de paquetes IP. Estos procedimientos pueden realizarse en cualquier instante de tiempo, una vez el equipo de usuario se encuentra registrado y tiene establecido el servicio portador por defecto. En cuanto a la activación del servicio portador por defecto, una característica importante de la red LTE, es que su activación puede realizarse de forma conjunta con el proceso de registro, reduciéndose por tanto la señalización necesaria. Durante la activación del servicio portador por defecto, mediante el protocolo ESM se puede llevar a cabo la asignación de la dirección IP al equipo de usuario, aunque es importante señalar que LTE también soporta la asignación de la dirección a través de protocolos IETF en lugar de utilizar la señalización NAS (Comes, 2010).

El protocolo ESM además contiene un procedimiento que permite que un equipo de usuario solicite a la red el establecimiento de la conexión a una red externa. En respuesta a dicha petición, la red LTE puede proceder a activar el servicio portador por defecto con dicha red externa. El protocolo soporta también un mecanismo de petición de asignación de recursos (denominado como UE requested bearer resource allocation procedure). Este mecanismo hace posible que el

equipo de usuario UE pueda notificar su necesidad de disponer de recursos que le permitan transferir paquetes IP de datos con unas determinadas características de calidad de servicio QoS. En el sistema LTE, el establecimiento de servicios portadores se controla siempre desde la red troncal EPC. Por tanto, este mecanismo permite disponer de una alternativa para que el equipo de usuario pueda solicitar el inicio de la activación del servicio portador, otorgando una mayor flexibilidad para el soporte de aplicaciones cuya señalización no se controle directamente a través de plataformas de servicios.

1.2.5 Equipo de Usuario UE

El equipo de usuario (UE) es cualquier dispositivo utilizado directamente por un usuario final para comunicarse. Puede ser un teléfono de mano, un ordenador portátil equipado con un adaptador de banda ancha móvil, o cualquier otro dispositivo el cual se conecta a una estación base o nodo eNB. Es considerado el dispositivo terminal de la red LTE. La arquitectura funcional de un UE de LTE está representada en la Figura 20-1. Son dos elementos básicos: un módulo de subscripción del usuario llamada SIM o USIM y el equipo móvil propiamente dicho denominado Mobile Equipment, ME. Adicionalmente, las funciones del equipo móvil se agrupan en dos entidades funcionales: la terminación móvil y el equipo terminal (Paulino, 2013).

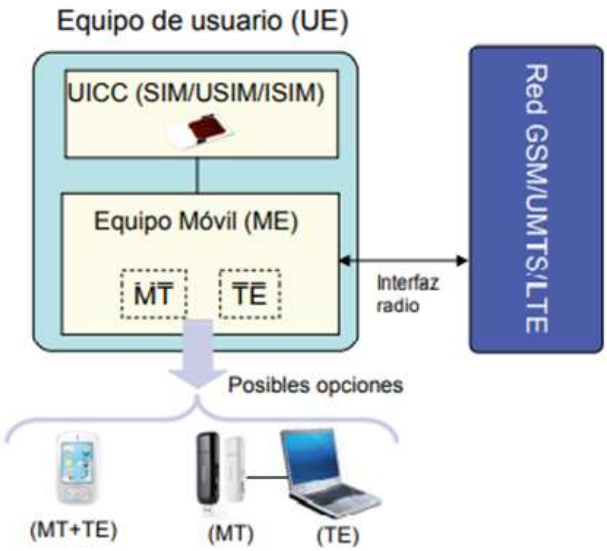


Figura 20-1: Equipo de Usuario

Fuente: (3GPP, 2015)

1.2.6 Autenticación LTE

Cuando un usuario solicita el acceso a una red LTE, se utiliza EPS AKA para autenticación mutua usuario/red. En la Figura 23-1 podemos ver el proceso de forma gráfica. El procedimiento de autenticación se puede apreciar en la Figura 21-1 es tal como sigue (Gualda, 2016):

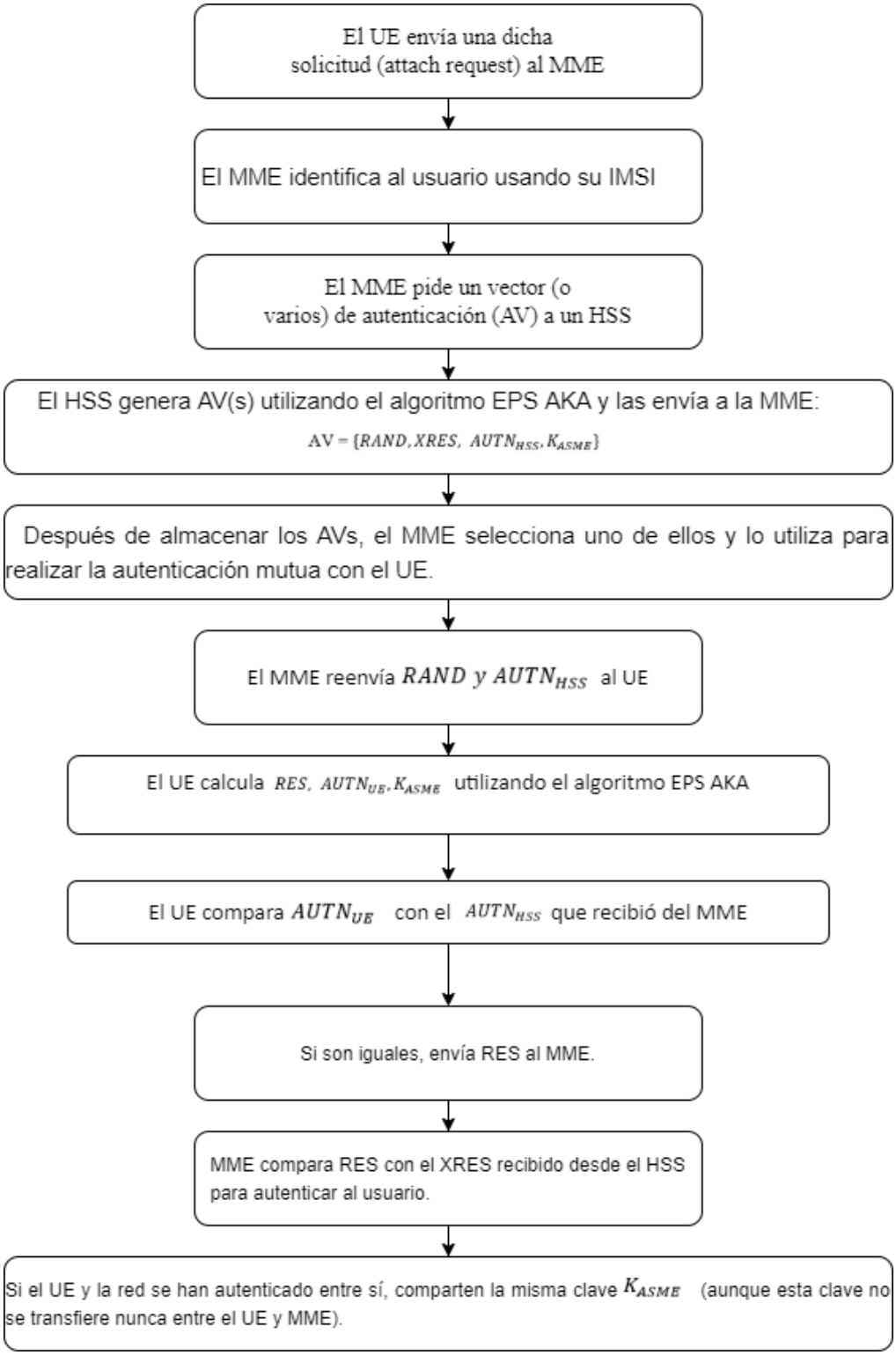


Figura 21-1: Orden en el proceso de autenticación UE

Realizado por: (Henry Yugsin, 2022)

La información que utiliza el HSS/AuC se puede observar en la figura 22-1:

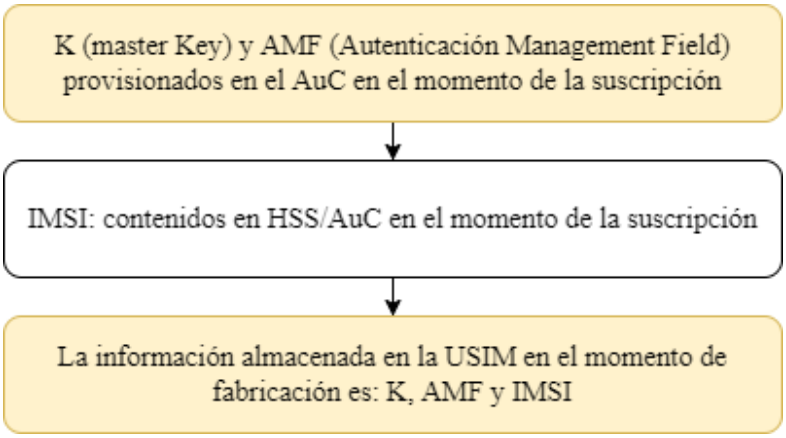


Figura 22-1: Información que utiliza el HSS/AuC

Realizado por: (Henry Yugsin, 2022)

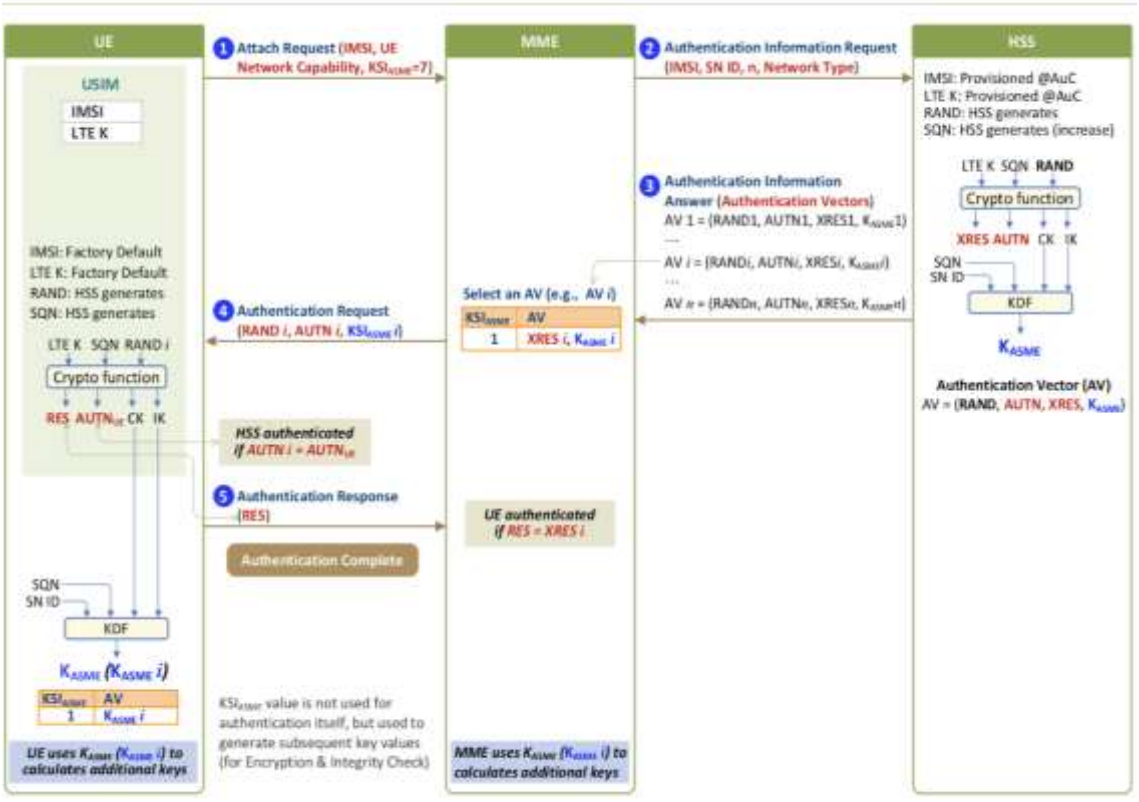


Figura 23-1: Proceso de autenticación UE

Fuente: (Gualda, 2016: pp. 39-47)

A continuación, se describe el proceso de autenticación en cada una de sus 5 etapas (Gualda, 2016):

UE-MME Attach Request

El UE envía un mensaje Attach Request a un MME con la información que se puede observar en la figura 24-1:

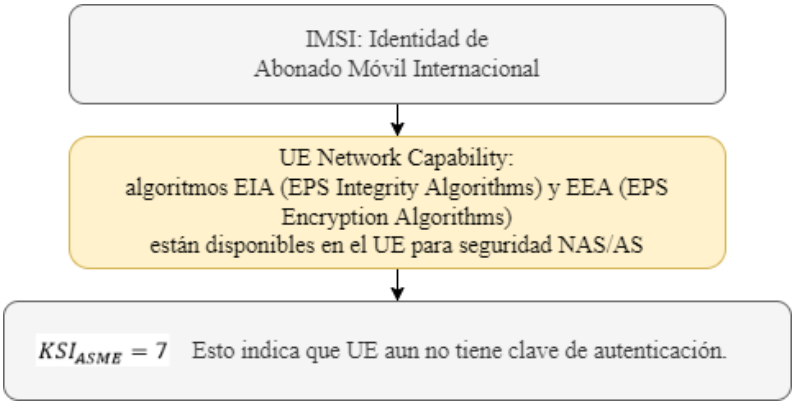


Figura 24-1: Información enviada en el mensaje Attach Request

Realizado por: (Henry Yugsin, 2022)

MME-HSS Authentication Information Request

- El MME envía un mensaje de Authenticacion Information Request (IMSI, SN ID, n, Network Type) al HSS:
  - SN ID (Serving Network ID): identifica a la red visitada por el usuario. Consta de Identificación PLMN (MCC+MNC).
  - n (número de vectores de autenticación): Numero de vectores de autenticación que solicita el MME.
  - Tipo de red: tipo de la red visitada por el UE (E-UTRAN para LTE).
- El HSS genera RAND (aleatorio) y SQN (número de secuencias se incrementa con re-autenticaciones).
- A partir de RAND, SQN, AMF y K unas funciones generadoras "f" generan los siguientes parámetros de seguridad:
  - IK (Integrity Key): Generado por HSS y USIM.
    $(K, RAND) \rightarrow f4 \rightarrow IK$
  - CK (Ciphering Key): Generado por HSS y USIM.
    $(K, RAND) \rightarrow f3 \rightarrow CK$
  - AK (Anonymity Key): Generado por HSS.
    $(K, RAND) \rightarrow f5 \rightarrow AK$
  - XRES (eXpected RESponse): Generado por HSS que debe coincidir con RES generado por el USIM.
    $(K, RAND) \rightarrow f2 \rightarrow XRES$
  - MAC (Message Authentication Code): Generado por HSS, el USIM debe generar XMAC.
    $(K, SQN, RAND, AMF) \rightarrow f1 \rightarrow MAC$
  - AUTN (Authentication Token): Generado por HSS.

$$AUTN = SQN \otimes AK||AMF||MAC$$

Ecuación 1-1: Autenticación Usuario con Token

- Mediante una función KDF se deriva K_{ASME}.

HSS-MME Authentication Information Answer

La información requerida se puede apreciar en la figura 25-1.

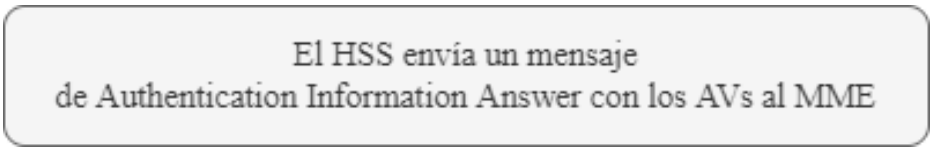


Figura 25-1: Información enviada en Authentication Information Answer

Realizado por: (Henry Yugsin, 2022)

MME-UE Authentication Request

Este procedimiento se puede apreciar en la figura 26-1.

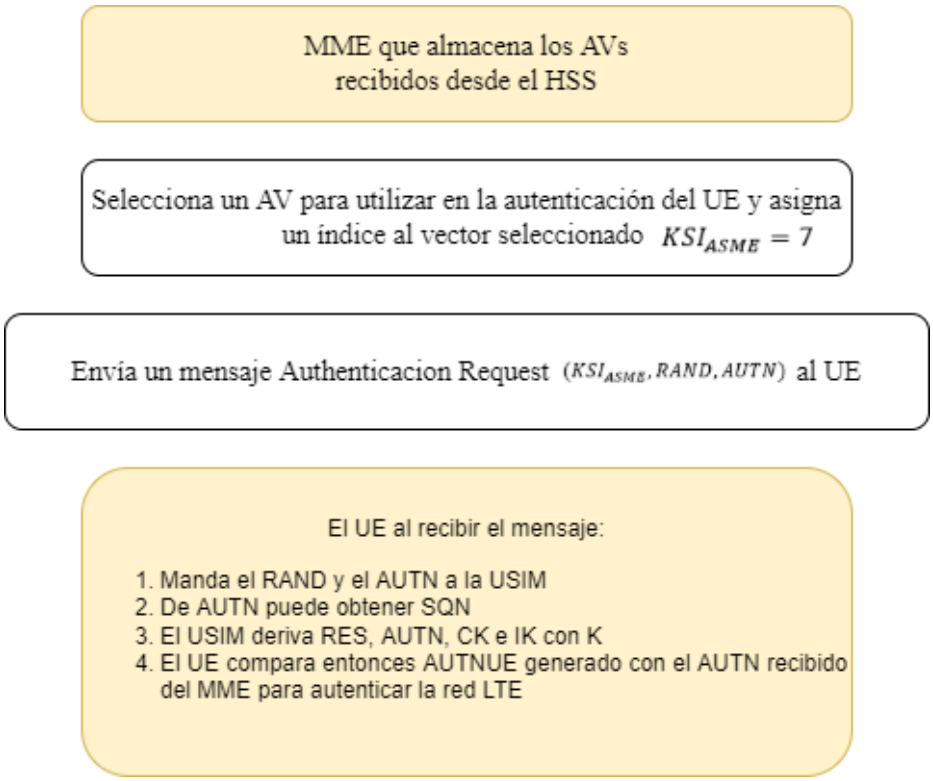


Figura 26-1: Proceso MME-UE Authentication Request

Realizado por: (Henry Yugsin, 2022)

UE-MME Authentication Response

Este procedimiento se puede apreciar en la figura 27-1.

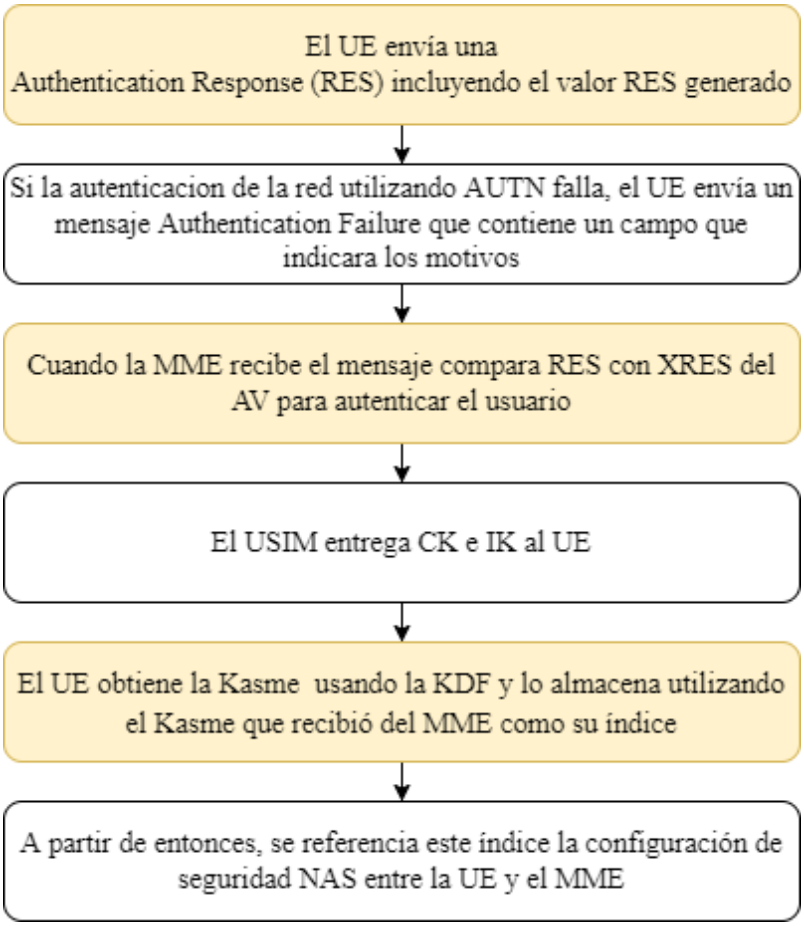


Figura 27-1: Proceso UE-MME Authentication Response

Realizado por: (Henry Yugsin, 2022)

1.2.7 Análisis del arte de las redes móviles 4G

Las redes de comunicaciones móviles 4G han sufrido una evolución desde la aparición de la tecnología LTE Release 8 la cual es considerada como el primer eslabón en una evolución de las redes 4G. Las principales características que se han ido mejorando en las diferentes versiones de LTE son la capacidad de transmisión de datos, agregación de portadoras, coordinación de la interferencia entre celdas, mejoras en la transmisión de múltiples antenas (MIMO) entre otras (Mendoza, 2019).

Para hablar de la evolución de las redes 4G debemos analizar el desarrollo de los Releases de 3GPP los cuales son utilizados para la estandarización de las redes móviles. En estos estándares tenemos tres fechas, fecha de comienzo, fecha de finalización y fecha de cierre, la diferencia entre la fecha de finalización y la de cierre es que en la primera los Releases todavía pueden sufrir alguna pequeña modificación mientras que después de la fecha de cierre ya no podrán ser

modificados. En relación con estas tres fechas podemos encontrar tres estados en los Releases. A partir de la fecha de comienzo el Release pasa a estar en estado open, en la fecha de finalización el Release pasa a estar en estado frozen y ya para la fecha de cierre el Release pasa a estado closed. En la tabla 3-1 podemos observar las fechas y estado de los diferentes Releases de 3GPP que existen hasta la actualidad, tomando en cuenta desde el Release 8 el cual es el primero en la evolución de las redes 4G y 5G.

Tabla 2-1: Estado de los Releases de 3GPP

Nombre	Estado	Fecha de Inicio	Fecha de Finalización	Fecha de cierre
Release 8	Frozen	2006-01-23	2009-03-12 (SA#43)	-
Release 9	Frozen	2008-03-06	2010-03-25 (SA#47)	-
Release 10	Frozen	2009-01-20	2011-06-08 (SA#52)	-
Release 11	Frozen	2010-01-22	2013-03-06 (SA#59)	-
Release 12	Frozen	2011-06-26	2015-03-13 (SA#67)	-
Release 13	Frozen	2012-09-30	2016-03-11 (SA#71)	-
Release 14	Frozen	2014-09-17	2017-06-09 (SA#76)	-
Release 15	Frozen	2016-06-01	2019-06-07 (SA#84)	-
Release 16	Frozen	2017-03-22	2020-07-03 (SA#88-e)	-
Release 17	Open	2018-06-15	2022-06-10 (SA#96)	-
Release 18	Open	2019-09-16	-	-

Realizado por: (Henry Yugsin, 2022)

A continuación, se realiza una explicación de las principales características de cada uno de los Releases antes mencionados.

Release 8 LTE. En este estándar se adopta la modulación OFDMA para el acceso múltiple. Además, la celda tiene la opción de utilizar un canal con mayor ancho de banda preferentemente en el enlace descendente. Con la ayuda de técnicas conjuntas como DC y 64QAM se puede lograr una capacidad del enlace descendente de hasta 84 Mbps. Fue la versión 8 de 3GPP en la cual se conoció el termino LTE por primera vez. Todos los lanzamientos siguientes fueron mejoraron la tecnología. Basado en la estandarización del Release 8, las siguientes son las principales características (3GPP, 2022):

- Velocidades de datos de alta velocidad: hasta 300 Mbps de velocidad en enlace descendente y hasta 75 Mbps de velocidad en enlace ascendente.
- Una eficiencia espectral alta.
- Múltiples anchos de banda: 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz y 20 MHz.
- Una arquitectura simplificada.
- Toda la red se basa en IP.
- Inclusión de tecnología MIMO.
- Multiplexacion en frecuencia (FDD) y multiplexacion en tiempo (TDD).

Release 9 (Enhancement to LTE). Este estándar introduce a la arquitectura de redes las femtoceldas, las cuales toman el nombre de Home eNodeB (HeNB). Además, se da soporte a los servicios multicast o broadcast multimedia MBMS (Multimedia Broadcast Multicast Services) y se realiza algunas mejoras en los servicios basados en la localización, LBS (Location Based Services). Las mejoras se detallan a continuación (Becvar et al., 2013: pp.11-12):

- PWS (Public Warning System): los usuarios siempre deben recibir alertas oportunas y precisas relacionadas con desastres naturales u otras situaciones críticas. El Sistema de Alerta Movil Comercial (CMAS) fue presentado en el lanzamiento de Release 9.
- Femto Cell: Femto cell es básicamente una celda de tamaño pequeño utilizada en oficinas u hogares, la cual se conecta a redes de proveedores a través de una conexión de banda ancha.
- eMBMS: con los servicios de multidifusión de transmisión multimedia (MBMS), los operadores tienen la capacidad de transmitir servicios a través de la red LTE. Para LTE, el canal MBMS ha sufrido una evolución desde la perspectiva de capacidad de datos y capacidad.
- Posicionamiento LTE: Los métodos de tres posiciones se especifican en la versión LTE 9, es decir, GPS asistido (A-GPS), diferencia de tiempo de llegada observada (OTDOA) e identificación de célula mejorada (ECID).

Release 10 (LTE Advanced). Esta versión es la primera norma 3GPP compatible con tecnología 4G. Se introducen algunas mejoras técnicas como la agregación de portadoras, mejoramiento en la tecnología MIMO. Asimismo, se definen técnicas avanzadas para la coordinación de la interferencia lo cual hace posible la implementación densa de femtoceldas. Las especificaciones LTE Advanced en la versión 10 incluyen características y mejoras significativas esto con la finalidad de cumplir con los requisitos ITU IMT-Advanced que establece velocidades más altas para UE que las especificadas en la versión 8 de 3GPP. Algunos de los requisitos principales establecidos por IMT-Advanced son los siguientes: 1 Gbps DL / 500 Mbps de rendimiento UL, Alta eficiencia espectral y Roaming mundial. Las siguientes son algunas mejoras importantes en la versión 10 (3GPP, 2013):

- Velocidad máxima de datos aumentada, DL 3 Gbps, UL 1,5 Gbps
- Mayor eficiencia espectral, desde un máximo de 16 bps/Hz en R8 a 30 bps/Hz en R10
- Mayor número de suscriptores activos simultáneamente.
- Acceso múltiple mejorado del enlace ascendente: esta versión introduce el SC-FDMA agrupado en el enlace ascendente. LTE-Advanced en la versión 10 tiene la opción de programación selectiva de frecuencia en el enlace ascendente.
- Mejoras MIMO: LTE Advanced permite hasta 64 MIMO en enlace descendente y en el equipo de usuario UE permite 4X4 en dirección de enlace ascendente.
- Nodos de retransmisión: para disminuir los agujeros de bucle de cobertura, los nodos de retransmisión son una de las características propuestas en la versión 10. Los nodos de retransmisión o los enbs de baja potencia extienden la cobertura del eNB principal en entornos de baja cobertura.
- Mejor coordinación de interferencia entre células (eICIC): eICIC se introdujo en la versión 10 de 3GPP para tratar problemas de interferencia en redes heterogéneas (HetNet). eICIC disminuye la interferencia en el tráfico y los canales de control. eICIC usa potencia, frecuencia y también dominio de tiempo para disminuir la interferencia intrafrecuencia en redes heterogéneas.
- Agregación de portadores (CA): La CA presentada en la versión 10 es una forma rentable para que los operadores utilicen su espectro fragmentado distribuido en diferentes o mismas bandas con el fin de mejorar el rendimiento del usuario final según lo requerido por IMT-Advanced.
- Soporte para redes heterogéneas: la combinación de macro células grandes con células pequeñas da como resultado redes heterogéneas. La versión 10 pretende diseñar la especificación de detalle para redes heterogéneas.

Release 11 (Enhancement to LTE Advanced). Esta nueva versión incrementa la agregación de portadoras y introduce la comunicación multipunto cooperativa Cooperative MultiPoint communication (CoMP), incrementa la eficiencia espectral, y mejora la eficiencia energética. La versión 11 incluye mejoras en LTE Funciones avanzadas estandarizadas en la versión 10. Algunas de las mejoras importantes son (Mendoza, 2019):

- Agregación de operadores: Múltiples avances de tiempo (TA) para la agregación de portadores de enlace ascendente, Agregación de portadoras intrabandas no contiguas, cambios de capa física para soporte de agregación de operador en TDD LTE.
- Transmisión y recepción multipunto coordinado (CoMP): con CoMP, el transmisor puede compartir carga de datos incluso si no están ubicados.
- ePDCCH: Nuevo PDCCH mejorado el introducido en la versión 11 de 3GPP para aumentar la capacidad del canal de control. ePDCCH utiliza recursos PDSCH para transmitir información de control a diferencia de la versión 8 PDCCH que solo puede usar la región de control de las subtramas.
- Minimización de la prueba de manejo (MDT): Las pruebas de manejo siempre son costosas. Para disminuir la dependencia en las pruebas de manejo, se introdujeron nuevas soluciones que son independientes de SON aunque muy relacionadas. MDT básicamente se basa en la información provista por la UE.
- Control de sobrecarga Ran para comunicación de tipo maquina: para dispositivos de tipo máquina, se ha especificado un nuevo mecanismo en la versión 11 donde la red en caso de comunicación masiva desde dispositivos puede bloquear algunos dispositivos para enviar solicitudes de conexión a la red.

Release 12 (Further enhancement to LTE Advanced). La versión 12, busca aumentar la capacidad. Algunas de las principales características (Mendoza, 2019):

- Mejoras de células pequeñas: Las células pequeñas fueron compatibles desde el comienzo con características como ICIC y eICIC en la versión 10. La versión 12 presenta la optimización y las mejoras para las células pequeñas, incluidas las implementaciones en áreas densas. La conectividad dual, es decir, la agregación de portadoras entre sitios entre macro y pequeñas células también es un área de enfoque.
- Mejoras en la agregación de operadores: La versión 12 ahora permite la agregación de operadores entre operadores TDD coubicados y FDD. Además de la agregación de

operadores entre TDD y FDD, ahora también hay tres agregaciones de operadores posibles para un total de 60 Mhz de espectro agregado.

- Comunicación de tipo de maquina (MTC): se espera un gran crecimiento en la comunicación de tipo de maquina en los próximos años, lo que puede ocasionar una tremenda señalización de red, problemas de capacidad. Para hacer frente a esto, se define una nueva categoría de UE para las operaciones optimizadas de MTC.
- Integración WiFi con LTE: Con la integración entre LTE y WiFi, los operadores tendrán más control sobre la gestión de sesiones WiFi. En la versión 12, la intención es especificar el mecanismo para dirigir el tráfico y la selección de red entre LTE y WiFi.
- LTE en espectro sin licencia: una operación LTE en espectro sin licencia es uno de los elementos de estudio en la versión 12. Las operaciones en ancho de banda del espectro sin licencia brindan muchos beneficios a los operadores como el aumento en la capacidad de red, carga y rendimiento.

Release 13 (Meeting the growing throughput demand). Su objetivo principal es satisfacer la creciente demanda de rendimiento (Mendoza, 2019).

- Mejoras en agregación de operadores: el objetivo en la versión 13 es admitir la agregación de operadores de hasta 32 CC (operadores de componentes) donde, como en la versión 10, la agregación de operadores se introdujo con soporte de solo 5 CC.
- Mejoras para la comunicación de tipo maquina (MTC): a partir de la versión 12, hay mejoras adicionales en MTC, se está definiendo una nueva categoría de UE de baja complejidad para proporcionar soporte para ancho de banda reducido, alimentación y soporte de larga duración de la batería.
- LTE en mejoras del espectro sin licencia: el enfoque en la versión 13 es la agregación de la celda primaria del espectro con licencia con una celda secundaria del espectro sin licencia para satisfacer la creciente demanda de tráfico.
- Posicionamiento en interiores: en el lanzamiento 13 se está trabajando para mejorar los métodos existentes de posicionamiento en interiores y también se están explorando nuevos métodos de posicionamiento para mejorar la precisión en interiores.
- Técnicas de transmisión multiusuario mejoradas: la versión 13 también cubre posibles mejoras para la transmisión multiusuario de enlace descendente utilizando la codificación de superposición.
- Mejoras MIMO: Hasta 8 sistemas MIMO de antena son compatibles actualmente, el nuevo estudio en esta versión buscar en sistemas MIMO de alto orden con hasta 64 puertos de antena.

Release 14. El comienzo de la estandarización 5G. La versión 14 marcar el inicio del trabajo de la comunicación móvil 5G en 3GPP. Además de la continua evolución de LTE, se estandariza una nueva tecnología de acceso por radio, y estas dos tecnologías juntas formaran un acceso de radio 5G. Mejorando los inconvenientes tecnológicos de los releases antecesores y sobre varias áreas clave: comunicación de baja latencia, flexibilidad de espectro, comunicación de tipo de máquina, técnicas de transmisión de múltiples antenas y sitios múltiples, y diseño ultra delgado, y como pueden ser parte del próximo trabajo 5G en 3GPP. 5G consistirá en la evolución de LTE junto con una nueva tecnología de acceso de radio, que llamamos "NX" a continuación. La evolución de LTE se enfocar en mejoras compatibles hacia atrás en el espectro existente hasta 6 GHz, mientras que NX se enfocar en un nuevo espectro, es decir, espectro donde LTE no está desplegado (Mendoza, 2019).

Release 15. Después de la entrega inicial a finales de 2017 de las nuevas especificaciones de radio NR 'Non-Stand-Alone' (NSA) para 5G, gran parte del esfuerzo se centró en 2018 en la finalización oportuna de la versión 15 de 3GPP, el primer conjunto completo de estándares 5G, y en el trabajo por aprobar. los primeros hitos para la presentación del 3GPP hacia las IMT-2020. Si bien las especificaciones iniciales permitieron sistemas de radio 5G no independientes integrados en redes LTE de generaciones anteriores, el alcance de la versión 15 se amplía para cubrir 5G "independiente", con un nuevo sistema de radio complementado con una red central de próxima generación. También incluye mejoras en LTE e, implícitamente, Evolved Packet Core (EPC). Este punto de referencia crucial permite a los proveedores avanzar rápidamente con el diseño de chips y la implementación inicial de la red durante 2019 (3GPP, 2019).

A medida que el trabajo de la versión 15 ha madurado y se acerca a su finalización, el enfoque del grupo ahora está cambiando a la primera etapa de la versión 16, a menudo denominada informalmente como "5G R15Phase 2". A finales de año, estaban en curso 83 estudios relacionados con la versión 16 más otros trece relacionados con la versión 17, que abarcaban temas tan diversos como el servicio de prioridad multimedia, los servicios de capa de aplicación Vehicle-to-everyment (V2X), el acceso satelital 5G , soporte de red de área local en 5G, convergencia inalámbrica y alámbrica para 5G, posicionamiento y ubicación de terminales, comunicaciones en dominios verticales y automatización de redes y nuevas técnicas de radio. Se iniciaron o avanzaron estudios adicionales sobre seguridad, códecs y servicios de transmisión, interfuncionamiento de LAN, división de redes e IoT (3GPP, 2019).

Otras actividades se centraron en ampliar la aplicabilidad de la tecnología 3GPP a los sistemas de acceso por radio no terrestres, desde satélites y estaciones base aerotransportadas hasta

aplicaciones marítimas. El trabajo también avanzó en la nueva funcionalidad de radio móvil profesional (PMR) para LTE, mejorando los servicios orientados al ferrocarril desarrollados originalmente con la tecnología de radio GSM que ahora se acerca al final de su vida útil (3GPP, 2019).

Release 16. La versión 16 es una versión importante para el proyecto, sobre todo porque lleva nuestra presentación IMT-2020, para un sistema 3GPP 5G completo inicial, a su finalización. Además de ese proceso formal, se ha avanzado en alrededor de 25 estudios de la versión 16, en una variedad de temas: servicio de prioridad multimedia, servicios de capa de aplicación Vehicle-to-everything (V2X), acceso satelital 5G, soporte de red de área local en 5G, convergencia inalámbrica y alámbrica para 5G, posicionamiento y ubicación de terminales, comunicaciones en dominios verticales y automatización de redes y nuevas técnicas de radio. Otros elementos que se están estudiando incluyen seguridad, códecs y servicios de transmisión, interfuncionamiento de redes de área local, división de redes e IoT (3GPP, 2020).

También se han desarrollado Informes Técnicos sobre la ampliación de la aplicabilidad de la tecnología 3GPP al acceso de radio no terrestre (inicialmente satélites, pero también se considerarán estaciones base aerotransportadas) y a aspectos marítimos (intrabuque, barco a tierra y barco a barco). El trabajo también avanza en la nueva funcionalidad PMR para LTE, mejorando los servicios orientados al ferrocarril desarrollados originalmente utilizando la tecnología de radio GSM que ahora está llegando al final de su vida útil (3GPP, 2020).

Como parte de la versión 16, los servicios de MC se amplían para abordar un sector empresarial más amplio que los servicios iniciales de seguridad pública y defensa civil bastante limitados para los que se habían desarrollado originalmente. Si se pueden usar estándares iguales o similares para aplicaciones comerciales (desde el despacho de taxis hasta la gestión del tráfico ferroviario y otros escenarios del sector vertical que se están investigando actualmente), esto brindaría una mayor confiabilidad a esos servicios de MC a través de una implementación más amplia y costos de implementación reducidos debido a economías de escala – en beneficio de todos los usuarios (3GPP, 2020).

Release 17. Varias de las funciones de Rel-17 están destinadas a mejorar el rendimiento de la red para los servicios y casos de uso existentes, mientras que otras abordan nuevos casos de uso y opciones de implementación. 5GAdvanced se basará en Rel-17, brindando soluciones de red inteligentes y cubriendo numerosos casos de uso nuevos además de casos de uso y opciones de implementación previamente definidos. Un componente clave de 5GAdvanced es el uso de inteligencia artificial (IA) basada en técnicas de aprendizaje automático (ML). Se espera que

AI/ML desencadene un cambio de paradigma en las futuras redes inalámbricas. Las soluciones basadas en AI/ML se utilizarán para introducir la gestión de red inteligente y resolver problemas de optimización multidimensional con respecto a la operación de red en tiempo real y no en tiempo real (Ericsson, 2021).

AI/ML también se utilizará para mejorar la interfaz de radio optimizando aún más el rendimiento de sistemas complejos de múltiples antenas, por ejemplo. Nuevos casos de uso como la realidad extendida (XR) comunicación utilizará redes inalámbricas para proporcionar experiencias inmersivas en entornos ciberfísicos y permiten interacciones hombre-máquina mediante dispositivos inalámbricos y prendas de vestir (Ericsson, 2021).

A continuación, se presenta algunas de las mejoras que plantea este Rel-17:

- Beamforming y entrada múltiple, salida múltiple (MIMO)
- Espectro compartido dinámico
- Ahorro de energía en el equipo del usuario
- Posicionamiento
- Comunicación ultra confiable y de baja latencia
- Transmisión de datos pequeños
- Redes no públicas
- Computación perimetral
- NR más allá de 52,6 GHz

Release 18. El equipo de estandarización de 3GPPRAN comenzó a discutir el alcance de Rel-18 en junio de 2021 en el Taller 3GPPRANRel-18 y tiene como objetivo la aprobación del alcance detallado para diciembre de 2021. De las más de 500 propuestas que se presentaron al taller, Ericsson identificó lo que consideramos los aspectos más destacados y los ubicó en tres categorías (Ericsson, 2021).

- Mejoras clave para los casos de e-MBBuse: Tres de las adiciones Rel-18 más notables para los casos de eMBBuse son la formación de haces/MIMO, las mejoras de movilidad y el ahorro de energía de la red.
- Mejoras clave para casos que no son de eMBBuse: Las mejoras más notables para aplicaciones que no son eMBB (como verticales nuevas o existentes) incluyen RedCap, XR y seguridad nacional y seguridad pública (NSPS)

- Funcionalidades de dominio cruzado para casos MBB y no MBBuse: También se debe destacar tres funcionalidades de dominio cruzado que se enfocan en casos de uso de MBB y no MBB: AI/ML para mejoras de capa física (PHY), AI/ML para mejoras de RAN y dúplex completo.

1.3 Virtualización de Funciones de Red (NFV)

La virtualización de las funciones de red (NFV) ha capturado el interés de la industria de telecomunicaciones durante varios años como una manera innovadora de mejorar la agilidad de los servicios, reducir los costos y crear mayor flexibilidad en el centro de datos de Telecomunicaciones. Las promesas y beneficios de la NFV son claros y se comprenden bien. La implementación inteligente y automatizada de las funciones de red virtualizada (VNF), sin embargo, aún presenta dificultades que la industria de las telecomunicaciones y los proveedores de NFV deben enfrentar (INTEL, 2021).

Las funciones de red, de entidades como Evolved Packet Core (EPC), los nodos inalámbricos 3G, Broadband Network Gateways (BNG), Provider Edge (PE), los routers, los firewalls, etc., tradicionalmente se han comercializado en dispositivos de hardware dedicados (de un único propósito). Sin embargo, el surgimiento reciente de las funciones de red virtualizada tiene como objetivo reemplazar este enfoque centrado en el hardware con dispositivos de software instanciados en un ambiente de virtualización apropiado para Telecomunicaciones con servidores basados en el procesador Intel Xeon que se comercializan actualmente. La industria de telecomunicaciones entiende y acepta este cambio que lleva a un enfoque de virtualización de funciones de red (NFV) como algo clave para conseguir que sus empresas sean más ágiles, sus redes más adaptables, y que se reduzcan sus costos totales de propiedad. Si bien el enfoque de NFV abre nuevas posibilidades tanto para las Telcos como para el creciente ecosistema de proveedores de dispositivos de VNF, los componentes de VNF son solo una parte de la solución. Implementar un servicio VNF apropiado para Telcos plantea nuevas dificultades que deben enfrentar tanto las Telcos como los proveedores (INTEL, 2021).

1.3.1 Modelo NFV ETSI

A continuación, se indican una serie de conceptos basado en el modelo ETSI para el ambiente NFV (Loza, 2019):

1. Función de red física (PNF): una PNF es la implementación de un bloque de funciones de red especializadas, con comportamiento e interfaces externas bien definidas. Hoy, un PNF hace referencia a un nodo de red o un dispositivo físico, ya que está estrechamente vinculado con el cumplimiento de un fin específico. Esta funcionalidad no presenta mayor variación con el tiempo, debido a que está ligado íntimamente al Hardware estático, donde en la mayoría de los casos sus cambios consisten en aumentar sus capacidades.
2. Infraestructura de virtualización de funciones de red (NFVI): NFVI brinda un entorno de red integrado por componentes de hardware y software, en el que se pueden implementar, gestionar y ejecutar VNF. Un NFVI puede atravesar diversos lugares geográficos, mientras que las conexiones entre estos diferentes lugares geográficos también se consideran parte de este NFVI.
3. Sistema de gestión de elementos (EMS): un EMS es un conjunto de Gestores de elementos (EM) individuales que gestionan las instancias de VNF en términos de creación de instancias, ejecución y despliegue durante sus ciclos de vida.
4. Gestión y orquestación (MANO): NFV introduce algunas capacidades nuevas en la red de comunicación, mientras que MANO es el elemento utilizado para gestionar y acomodar estas nuevas capacidades. En particular, MANO se puede dividir en tres entidades, es decir, Virtualized Infrastructure Manager (VIM), VNF Manager (VNFM) y NFV Orchestrator (NFVO), que son las encargadas de gestionar el NFVI, la asignación de recursos, la virtualización de funciones, etc.
5. Función de red virtual (VNF): Es la implementación de software de PNF, el cual debe proporcionar los mismos comportamientos funcionales e interfaces de operación externa que una función física (PNF). Una VNF puede estar compuesta por uno o más elementos. Por un lado, si se implementa una VNF en una sola Máquina Virtual (VM), se compone de un solo componente. Por otro lado, si se implementa un VNF en varias VM, se compone de múltiples componentes, donde cada VM aloja un componente. Tomando el EMS como ejemplo, en realidad es una VNF que consta de muchos componentes individuales (es decir, EM) que se distribuyen en diferentes máquinas virtuales.
6. Punto de presencia de red (N-PoP): N-PoP indica la ubicación donde se implementan la PNF y la VNF. Se puede acceder a los recursos correspondientes, como memoria y almacenamiento desde N-PoPs.

A continuación, en la Figura 28-1, y para una mejor visualización de la relación entre estos conceptos, se muestran en azul y diferenciados en una estructura de capas, donde SFC significa Service Function Chaining Working Group.

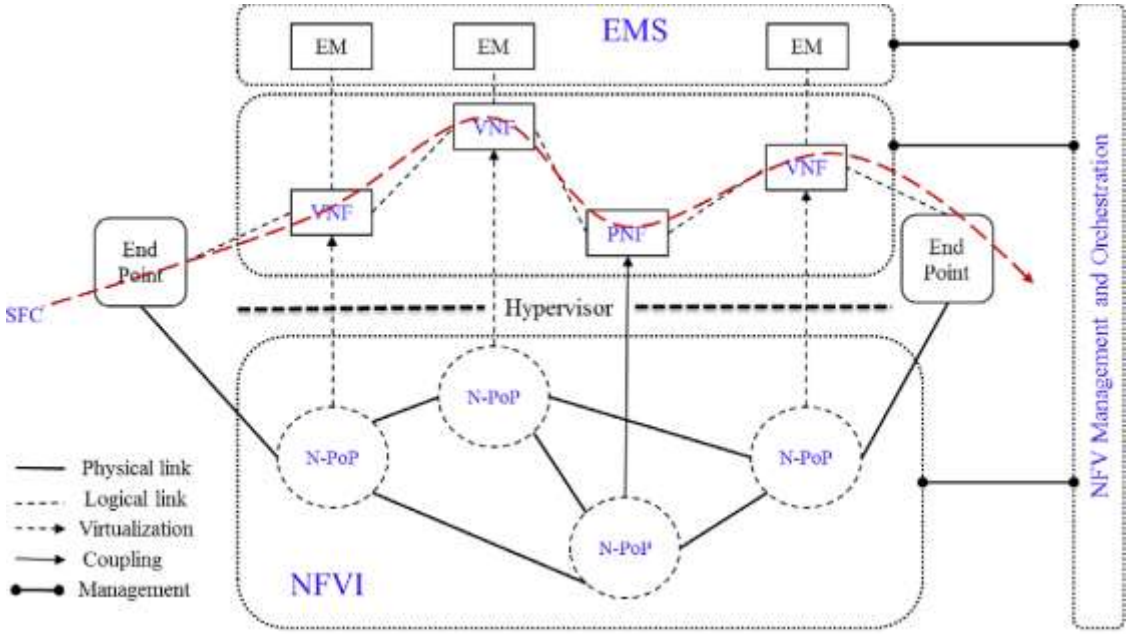


Figura 28-1: Relación en la terminología NFV con una visión se servicio end to end

Fuente: (Yi, 2018)

1.3.2 Arquitectura de NFV

La arquitectura general de referencia entregada por la ETSI, se puede apreciar en la Figura 29-1. En particular, la NFVI (Hardware/Infraestructura) corresponde al plano de datos, que reenvía datos y proporciona recursos para ejecutar servicios de red. MANO corresponde al plano de control, que es responsable de construir las conexiones entre varias VNF y orquestar recursos en NFVI. La capa VNF corresponde al plano de la aplicación (Software), que alberga varios tipos de VNF que pueden considerarse aplicaciones (Loza, 2019).

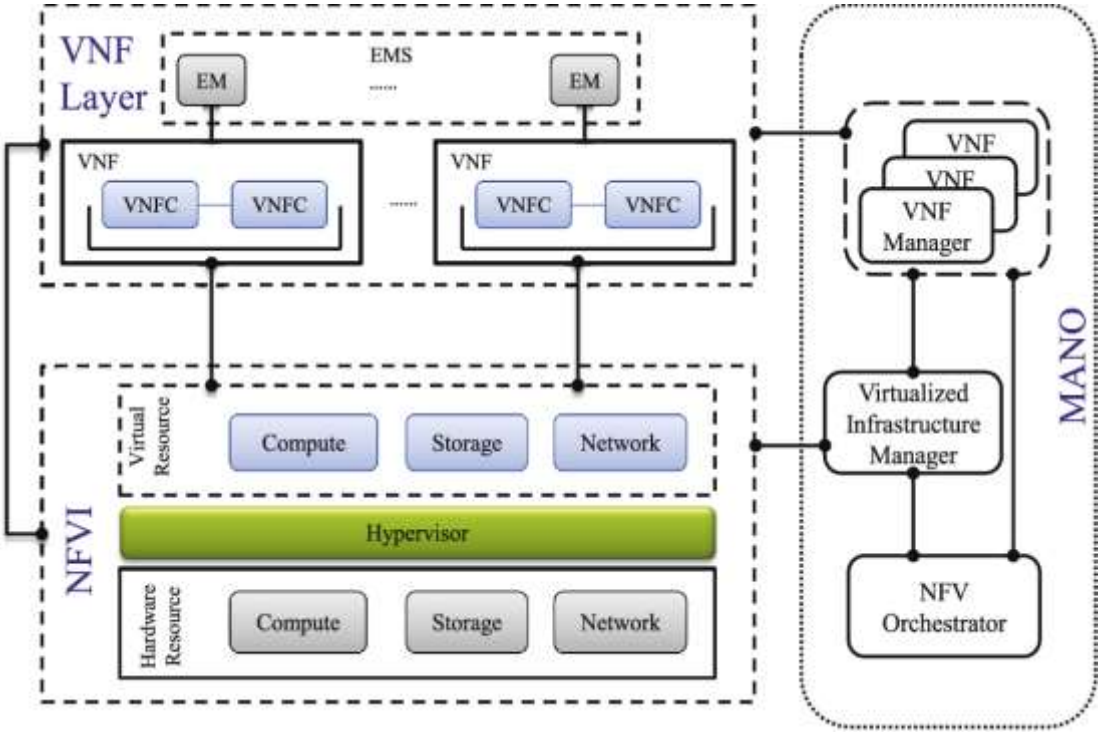


Figura 29-1: Arquitectura general de NFV

Fuente: (Yi, 2018)

1.3.2.1 Capa NFVI

La NFVI su principal función es, estando debajo de la capa de virtualización y sobre el Hardware, toma los recursos físicos como el cómputo, almacenamiento y tarjeta de red, y brinda con estos los recursos virtualizados de los mismos al resto del ambiente NFV. Al implementar un conjunto de dispositivos de red de propósito general en ubicaciones distribuidas, la NFVI puede satisfacer varios requisitos de servicio, como latencia y localidad, y reducir el costo de la red en CAPEX y OPEX, esto dado que se desliga del Hardware. Basado en el hardware de uso general, la NFVI también brinda un entorno de virtualización para la implementación y ejecución de las VNF. Aunque las arquitecturas de las NFVI actuales son generalmente las mismas entre ellas, sus implementaciones reales pueden diferir mucho. De acuerdo con la parte inferior de la Figura 29-1, la arquitectura de referencia de NFVI se divide en tres capas, es decir, infraestructura física, capa de virtualización e infraestructura virtual. Cada uno de ellos se presenta con sus funciones y características en las siguientes subsecciones (Loza, 2019).

Capa Física: La infraestructura física de NFVI es básicamente servidores de propósito general, los cuales proveen de cómputo y storage. En particular, los servidores que entregan computo, se les conoce como Nodo de Cómputo y a los dedicados a la memoria, se les llama Nodo de

Almacenamiento. Ellos se comunican entre sí a través de tarjetas de red con interfaces físicas (Loza, 2019).

El rendimiento de procesamiento de NFVI se puede mejorar si se utiliza los mecanismos de mejora de CPU, Storage y Networking, como, por ejemplo, el primero se puede cumplir conectando los aceleradores de hardware en los servidores estándar COTS para acelerar la velocidad de procesamiento de paquetes o admitiendo una gran página para reducir el tiempo de búsqueda. En las tarjetas de red se puede optimizar utilizando Network Interface Card (NIC) inteligentes para promediar la carga, o agregando otros coprocesadores (por ejemplo, FPGA) para acelerar el procesamiento de datos. También existen mecanismo de aceleración del procesamiento con cómputos en cola, o mecanismo de Hardware Offload.

- **CPU Hardware** (Loza, 2019)

  En el contexto NFV, cada nodo de cálculo se puede realizar en forma de un procesador de mono-núcleo o multi-núcleo. Actualmente, existe una gran diversidad de servidores que se pueden usar como nodos de cómputo de propósito general. De acuerdo a sus características se pueden dividir en cuatro tipos:

  - Tower Server: se refiere a una computadora independiente que está construida en un gabinete vertical conocido como la torre. Generalmente, los servidores de la torre se construyen con un cierto grado de robustez considerado para reducir el tiempo de inactividad del servicio y evitar posibles daños. Sin embargo, debido al gran volumen y peso del servidor de la torre, el espacio del piso puede ser una gran limitación para la expansión de NFVI.
  - Rack Server: En comparación con el servidor de la torre, una torre solo contiene un servidor, un rack puede contener múltiples servidores apilados uno sobre el otro, lo que no solo reduce el espacio requerido, sino que también consolida los recursos de la red.
  - Blade Server: Los servidores blade normalmente se colocan dentro de un receptáculo de cuchillas para formar un sistema de cuchillas que cumple con los estándares IEEE de unidades de bastidor. En comparación con los servidores de torre y rack, el servidor blade permite más potencia de procesamiento en menos espacio de rack, ya que comparte ciertos elementos de hardware entre los servidores blade dentro del mismo gabinete.
  - Hyper-converged Solution: Consolida los recursos informáticos, de almacenamiento y de red en un solo cuadro, logrando así una gran escalabilidad simplemente agregando o eliminando dinámicamente dichos cuadros. Aunque

este mecanismo ofrece muchos beneficios, como disponibilidad, seguridad y respaldo, reduce la flexibilidad del despliegue, la configuración, la escala y la mejora de la red debido a las características de alta convergencia, es decir se limita el dinamismo a lo que los cuadros puedan formar en sus distintas combinaciones, que a su vez pueden causar la ineficiente utilización del hardware afectando rendimiento.

- **Storage Hardware**

  Se considera Hardware de Storage, a los dispositivos capaces de guardar, de manera temporal y/o permanente, información. Muchos elementos de red funcionan en torno al Hardware de Almacenamiento, por ejemplo, el Video Streaming, donde la red debe ser capaz de mantener un caché (almacenamiento temporal) del video. En particular, estos dispositivos de almacenamiento se usan generalmente en los siguientes tres aspectos (Loza, 2019):

  - Direct Attached Storage (DAS): Indica el almacenamiento conectado de los servidores a través de una ruta de comunicación directa y el servidor directamente conectado solo puede acceder a dicho almacenamiento.
  - Network Attached Storage (NAS): Indica un dispositivo de almacenamiento que proporciona acceso a archivos a computadoras heterogéneas en la red, es decir, el archivo se comparte entre estas computadoras.
  - Storage Area Network (SAN): Similar a NAS, SAN también proporciona acceso a almacenamiento de datos compartidos. La diferencia es que SAN comparte los datos en la unidad de bloque en oposición a la unidad de archivo de NAS.

- **Networking Hardware**

  El formato de estos equipos es usualmente de los dispositivos de capa dos y tres del Modelo OSI (Capa de Enlace y Red), estos son switches o routers, aunque gradualmente están siendo remplazados por equipos que soporten solamente protocolos de ruteo estándar, o solo el protocolo OpenFlow, incluso ambos (Mckeown et al., 2008: pp.69-74).

Capa Virtualizada: Consiste en una capa de Software que administra al Hypervisor, el cual distribuye los recursos físicos de la capa inferior para asignarlos a unidades aisladas (por ejemplo, VM o contenedores), aunque estas unidades virtuales compartan la infraestructura, cada una tiene asignado los periféricos tanto físicos, como virtuales necesarios para sostenerse de manera independiente.

Durante el ciclo de vida de las funciones de red virtualizadas, hay varias rutinas que deben ser cubiertas por la capa virtualizada, como la activación de una VM, la eliminación, la migración en línea y el escalamiento dinámico de las mismas. Para esto, el Hypervisor puede ajustar de forma dinámica la asignación entre los recursos físicos y los recursos virtuales asignados a las máquinas virtuales, de modo que se pueda lograr una portabilidad de los recursos a alto nivel entre las distintas VMs (Yi, 2018).

En la actualidad los hipervisores utilizados en SDN, son similares a los utilizados en NFV, como es el caso de FlowVisor. Pero hay que tener en cuenta que el hipervisor en SDN reside entre el plano de datos y el plano de red, mientras que en NFV, reside entre la infraestructura física y el acceso virtual infraestructura.

Los Hipervisores de dividen en dos tipos según la forma que se ejecuta su software. Los Hipervisores de Tipo 1, también conocidos como nativos o de baremetal, son los que ejecutan su código directamente sobre el hardware en el que son instalados. Por contraparte, los de Tipo 2, o también conocidos como hosted, son los que entre su código de Software y el Hardware se instala un Sistema Operativo (llamado Host OS), por tanto, el Hipervisor funciona sobre un Sistema Operativo, lo cual vendría siendo una capa extra de Software (Yi, 2018).

Además de la tecnología del Hypervisor, está la opción de utilizar Contenedores. Las diferencias se pueden apreciar en la Figura 30-1, donde se puede ver que el contenedor no requiere separar el sistema operativo en GuestOS, esto puede ahorrar overhead de cómputo en comparación con un Hypervisor, ya que las aplicaciones corren directamente sobre el HostOS. Esta misma ventaja lleva implícito varios riesgos de seguridad, debido a la dependencia del HostOS.

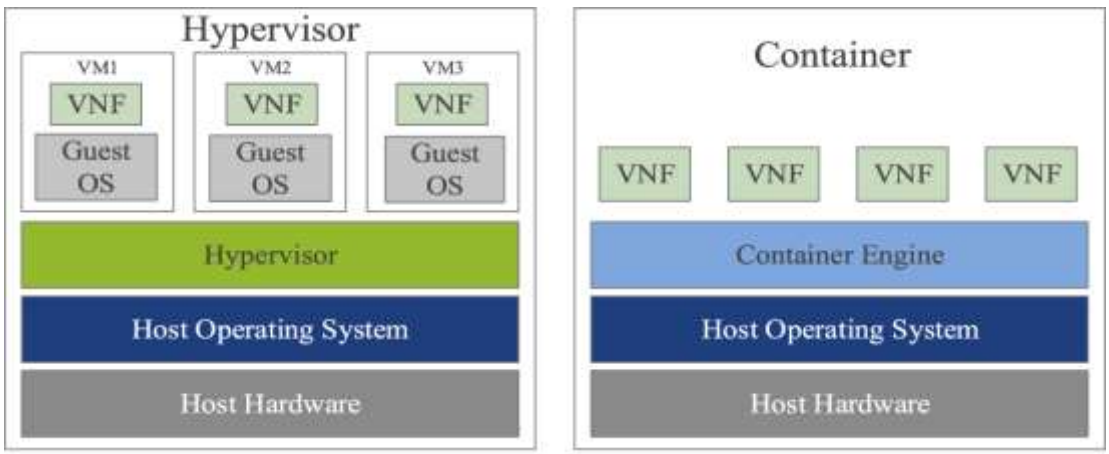


Figura 30-1: Comparación entre Hypervisor y Contenedor

Fuente: (Yi, 2018)

Capa de infraestructura Virtual: Como se puede apreciar en la Figura 30-1, la capa de infraestructura virtual abastecida de los recursos del Hardware, los convierte en elementos virtualizados (Virtual CPU, Storage y Networking) a través de Software como un Hypervisor, este nuevo tipo de recurso se explica a continuación (Yi, 2018).

- **Virtual CPU**

  El computo virtual, o vCPU proviene de la virtualización de elemento de cómputo en el hardware, como el CPU. Ésta es usualmente generada por el Hypervisor a través de APIs, que entrega una cierta capacidad que puede ser utilizado en el ambiente de las VNFs. También se puede dar como en SDC (Software Defined Compute), el cual pasa la capacidad de cómputo en una cloud, que puede ser compartido on-demand por una interfaz central.

- **Virtual Storage**

  La virtualización del almacenamiento separa su administración del hardware. Se constituye en forma de DAS, SAN y NAS (explicado anteriormente en el capítulo Storage Hardware). Esto permite la creación de depósitos de memoria compartibles, flexibles y escalables. También esto trae características como el snapshot y backup. Software Defined Storage (SDS) es otra forma de virtualizar almacenamiento, la cual crea memorias virtuales, y luego las conecta, de tal manera que parezca una sola unidad de storage virtualizado.

- **Virtual Networking**

  Las redes virtuales son similares a las redes tradicionales, pero estas permiten la interconexión de VMs, servidores virtuales, entre otros elementos, manteniéndose en un mismo ambiente virtualizado. Aunque se sigan los principios de redes físicas, las funcionalidades son controladas desde el software, por ejemplo, con adaptadores Ethernet virtuales o Switches virtuales. Otro aspecto importante a tener en cuenta, es que con elementos de red virtualizados, se puede tener una red de máquinas virtuales sin la necesidad de Hardware adicional dedicado a las redes, usando los mismos protocolos.

1.3.2.2 Capa de Funciones de Red Virtualizadas VNF

Las Virtual Network Function, son la abstracción final de las Physical Network Function (PNF), realizando la misma función, pero como software sobre un hardware compartido. Esta capa puede estar compuesta por varias VNF aisladas, cada una con sus respectivas componentes

controladoras (VNF Controller VNFC). Los Element Manager son las entidades administradoras de la VNF, los cuales arman el Element Management System (Yi, 2018).

La gran diversidad de VNFs hace que se puedan encontrar en toda la arquitectura de la NFV, como por ejemplo los vRouter puede estar en la capa de infraestructura virtual, otra VNF como OpenDaylight que es un software encargado de controlar, puede ser considerado dentro de la capa de Administración y Orquestación.

Actualmente las VNF se implementan de dos maneras distintas, como ambiente de Virtual Machine o como Contenedor (Container). Mientras el primero ofrece un ambiente aislado de la completitud de una computadora real, el contenedor se limita ejecutar los procesos esenciales, y tener las capas de computación necesarias para la VNF. Bajo estas dos visiones, se puede visualizar las siguientes posibilidades de implementación en la Figura 31-1. Existen combinaciones de ambas, donde por ejemplo un container se instala sobre una máquina virtual, esta combinación logra ejecutar con más simpleza que una VM al tener las características de un Container, a la vez también adquiere el aislamiento de una VM, aunque no logra la misma ligereza de un Container a secas propiamente tal. También hay intentos de Clear Linux por crear el "Clear Container", la cual es una idea similar a un Container dentro de una VM, pero con la diferencia clave de utilizar una VM con una reducción drástica en su ligereza, solo conservando las características esenciales, esto para tener un mejor rendimiento. Por último, Unikernel consiste en un tipo de container que solo se relacione con las librerías exclusivamente necesarias del Host OS (Bin/Libs) para esa VNF (Yi, 2018).

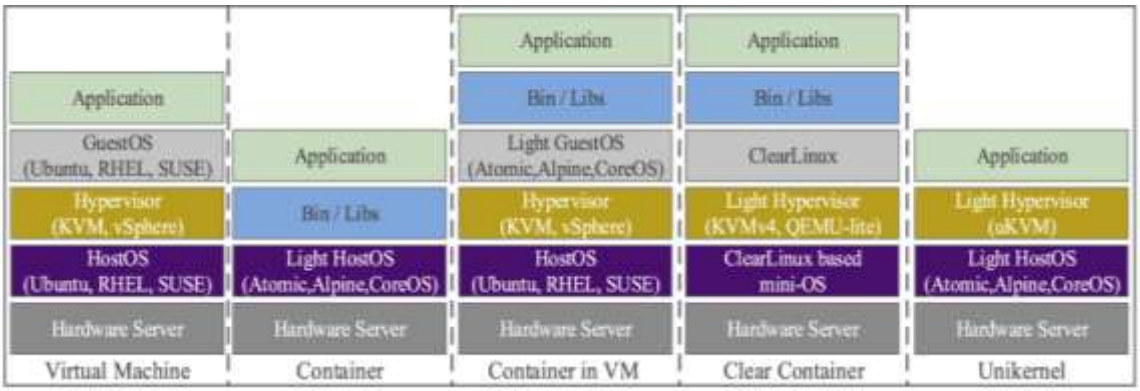


Figura 31-1: Ambientes de Virtualizacion para NFV

Fuente: (Yi, 2018)

1.3.2.3 Administración y Orquestación MANO

La principal responsabilidad del Management and Orchestration (MANO), es administrar el contexto virtualizado de la NFV. Esta responsabilidad se divide en tres áreas, como se aprecia en la Figura 32-1, y derivado del modelo ETSI se tiene particularmente el VIM, la NFVO y el VNFM.

En relación al despliegue de un servicio de red (Network Service NS), el NFVO administra globalmente los recursos, valida y autoriza los requerimientos de recursos de la NFVI, gestionando su ciclo de vida, administrando las políticas para las instancias de servicios de red e integrando las distintas VNFs para poder implementar el servicio final. Luego, el VNFM administra el ciclo de vida de las distintas VNFs instanciadas, además se establece que una VNF es administrada por una sola VNFM, pero una VNFM puede estar relacionadas a varias VNFs. El VIM administra y controla los recursos NFVI (cómputo, almacenamiento y red), aun cuando éste también puede ser configurado para manejar un tipo específico de recurso, por ejemplo, solamente cómputo (Loza, 2019).

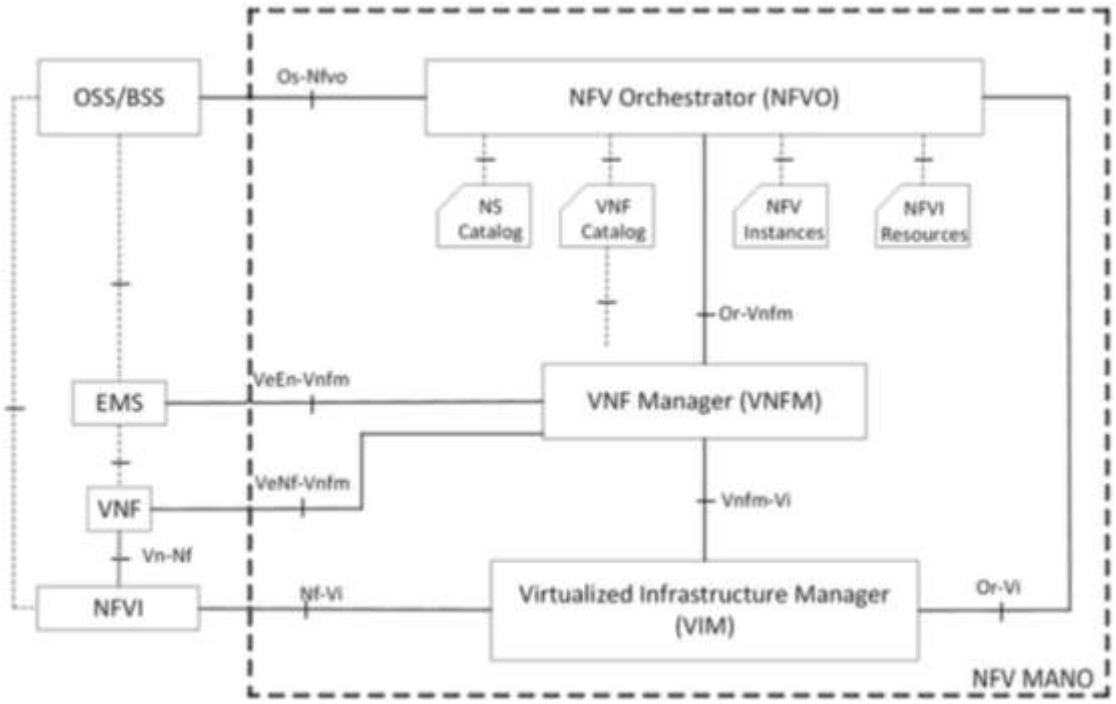


Figura 32-1: Componentes del MANO

Fuente: (Yi, 2018)

1.3.3 Software para VNF de LTE

1.3.3.1 OpenAirInterface OAI

OpenAirInterface OAI es una plataforma de código abierto, la cual fue desarrollada por OpenAirInterface Software Alliance (OSA) con la finalidad de implementar las especificaciones de LTE del 3GPP. Actualmente la plataforma de código abierto sigue en constante desarrollo/evolución por parte de la entidad OSA (OpenAirInterface, 2018).

Para el desarrollo de las redes LTE la plataforma OAI proporciona dos módulos, el primero contiene la funcionalidad del núcleo EPC y el segundo es la parte del acceso radio E-UTRAN.

- openair-cn: Este es el encargado de proporcionar el software para las entidades del núcleo HSS, MME y SPGW.
- openairinterface5g: Encargado de la parte de acceso radio, contiene software para la entidad eNB, gNB y UE.

A continuación, se tiene una lista de las principales características de OAI (OpenAirInterface, 2018):

- Compatible con el Release 8.6 de las especificaciones LTE del 3GPP. También implementa un subconjunto del Release 10. En versiones recientes implementa hasta el Release 14.
- Configuración FDD y TDD.
- Anchos de banda 5 MHz y 10 MHz (estable), 20 MHz (experimental).
- Permite la conexión de equipos de usuario simulados y comerciales, este proporciona su propio usuario simulado.
- Soporte para distintos eNB.
- Implementación de las capas MAC, RLC, PDCP y RRC.
- Posibilidad de capturar el trafico MAC LTE mediante wireshark.
- Configuración de la interfaz mediante ficheros de texto sencillos.
- Posibilidad de monitorización en tiempo real mediante un osciloscopio de software.
- Incluye un framework propio para la monitorización, llamado T Tracer. Este framework está constituido por un conjunto de herramientas que permiten entre otras funcionalidades monitorizar el eNB, capturar y reproducir el tráfico de red para su análisis posterior.
- Gestión de los usuarios y otros parámetros de la red en el HSS mediante MySQL y la interfaz Web phpMyAdmin.

OAI es una herramienta de software muy completa para el despliegue de redes LTE ya sean en máquinas físicas o mediante virtualizaciones. Gracias a que es de código abierto, posee una comunidad extensa de desarrolladores y probadores, por lo que la plataforma siempre se mantiene

actualizada en sus características y en correcciones de errores del propio software. Además, puede servir como base para futuras implementaciones de quinta generación 5G, por lo que esta entidad garantiza la inclusión de nuevas características y colaborar de manera activa en el desarrollo de las redes móviles del futuro.

1.3.3.2 OpenLTE

OpenLTE es un software de código abierto que implementa las especificaciones de LTE del 3GPP, el cual está desarrollado en los lenguajes de programación C++ y Python. Contiene las siguientes funcionalidades (Wojtowicz, 2017):

- Red de acceso radio E-UTRAN: Se basa principalmente en la transición y en la recepción del enlace descendente. Permite utilizar equipos de usuarios comerciales para probar el rendimiento y la funcionalidad de la red. Soporta el modo FDD con todos los anchos de banda definidos en las especificaciones y permite la captura de trafico LTE para los niveles MAC y también se puede utilizar Wireshark.
- Núcleo de red EPC simplificado: Implementa las funcionalidades del HSS y del MME, y una implementación sencilla del SWG y PGW.
- Además, contiene herramientas para pruebas y simulación de la parte radio.

1.3.3.3 Amari LTE 100

La compañía Amarisoft desarrollo una suite software llamada AMARI LTE 100 que tiene como objetivo la implementación de las especificaciones LTE del 3GPP. Se comercializa como un producto bajo licencia y por tanto es cerrado y de pago. El software contiene las siguientes funcionalidades (Amarisoft, 2018):

- Red de acceso radio E-UTRAN: Implementación completa de la red de acceso radio, compatible con el Release 14 de las especificaciones LTE del 3GPP. Entre otras características destacan el soporte FDD y TDD, la compatibilidad con varias plataformas SDR, la implementación de handover en las interfaces S1 y X2, la posibilidad de capturar tráfico en la capa MAC para su análisis mediante el wireshark, la posibilidad de monitorizar parámetros de nivel físico en tiempo real y la posibilidad de control remoto mediante un navegador Web mediante la API WebSocket.
- Núcleo de red EPC: Implementación completa del núcleo de red LTE, también compatible con el Release 14 de las especificaciones LTE del 3GPP. Entre otras características destacan el soporte para varios eNBs y la inclusión de un servidor IMS

con soporte para VoLTE, protocolo SIP, llamada de voz y video entre terminales, envió de SMS, etc.

- Emulador de equipo de usuario UE: Permite emular un amplio número de terminales de usuario que compartan el mismo espectro. Soporta el Release 8 de LTE con algunas características del Release 14. Entre otras características, destacan el soporte para los modos FDD y TDD con los anchos de banda definidos en las especificaciones.

1.3.3.4 srsLTE

Desarrollada por la compañía Software Radio Systems el software srsLTE implementa las especificaciones LTE del 3GPP. La implementación proporciona una librería LTE de alto rendimiento para aplicaciones SDR, que soporta tanto la red de acceso radio (eNB, UE) como el núcleo de la red EPC simplificado. La librería es modular y esta implementada en lenguaje C, está disponible tanto bajo licencia comercial como de código abierto. Incluye software de la implementación OpenLTE: partes relacionadas con funciones de seguridad y el análisis de mensajes RRC/NAS. El software incluye (SRS, 2018):

- Módulo srsUE: una aplicación completa que permite emular un terminal de usuario UE y que soporta todas las capacidades de red desde el nivel PHY hasta el nivel de red.
- Módulo srsENB: una aplicación completa para la creación del eNB.
- Módulo srsEPC: una implementación ligera y simplificada del núcleo de red EPC con HSS, MME y S/P-GW.
- Librerías adicionales para torres de protocolos: PHY, MAC, RLC, PDCP, RRC, NAS, S1AP.

A continuación, se realiza una tabla comparativa con las principales características de cada uno de los softwares mostrados anteriormente:

Tabla 3-1: Tabla comparativa de software para virtualizacion de LTE

	OpenAirInterface OAI	**Open LTE**	**Amari LTE 100**	**srsLTE**
Software de código abierto	Si (Licencia de código abierto)	Si (Licencia de código abierto)	No (Licencia cerrada y de paga)	Si (Licencia comercial o código abierto)

Entidad Propietaria	OpenAirInterface Software Alliance (OSA)	No especificado	Compañía Amarisoft	Compañía Software Radio Systems
Código de programación	C++ y Python	C++ y Python	Código cerrado	C++ y Python
Guías de Instalación y utilización	Cuenta con guías detallas en su página web, además de videos tutoriales.	No especificado	Junto con la licencia	Cuenta con guías detallas en su página web
Módulo EPC	Si	Si	Si	Si
Módulo eNB	Si	Si	Si	Si
Modulo UE	Si	No	Si	Si
Release implementados	Release 8-10-14	3GPP LTE	Release 9	LTE Release 10
Equipo SDR	USRP B2X0, USRP X300, Blade RF, LMS-SDR,	Utilización de GNU Radio	USRP N210	USRPB210, Raspberry Pi 4
Sistema Operativo	Ubuntu distribución de Linux	Ubuntu distribución de Linux	Fedora distribución GNU/Linux	Ubuntu distribución de Linux

Realizado por: (Henry Yugsin, 2022)

Se eligió el software OpenAirInterface de código abierto debido a diversas ventajas como lo es la compatibilidad con múltiples equipos SDR, principalmente la USRP B210 la cual se encuentra disponible en el laboratorio de comunicaciones de la FIE, otra característica importante es la posibilidad de implementar el software con distintos releases como 8-10-14, también la implementación de módulos EPC, eNB y UE por parte del software es una característica muy importante, por último la disponibilidad de guías para las implementación del software también resulta ser de mucha utilidad en el desarrollo del trabajo propuesto.

1.4 Radio Definido por Software

Existen diferentes conceptos de SDR basados en enfoques diferentes del problema que dependen, fundamentalmente, del campo de estudio de quien establece la definición. Wireless Innovation

Forum establece, en su sitio online, que un Radio Definido por Software es un "radio en el que algunas o todas las funciones de la capa física son definidas por software" (Garcia, 2011).

De acuerdo a Lee Pucker, el cual colabora con Wireless Innovation Forum, SDR se considera como una una tecnología aplicable en un amplio rango de áreas dentro la industria inalámbrica, capaz de proveer soluciones eficientes y comparativamente baratas a muchos problemas inherentes a arquitecturas de radio más tradicionales. En esencia, SDR es un término que se utiliza para describir una tecnología de radio donde algunas o todas las funciones de la capa física inalámbrica son definidas por software (Garcia, 2011).

Esta tecnología tiene amplias aplicaciones en el área de las comunicaciones inalámbricas pues brinda soluciones eficientes a problemas inherentes a las arquitecturas de radio tradicionales. También ofrece facilidades para una investigación menos costosa a través de simulación, permitiendo su experimentación y estudio a profundidad en entidades profesionales, comerciales y académicas.

1.4.1 Arquitectura de SDR

Con el fin de establecer una clasificación de los equipos de radio, el Wireless Innovation Forum ha definido 5 niveles de utilización de software dentro del radio para controlar o realizar funciones de la capa física, determinando la frontera entre hardware y software en el equipo:

- Nivel 0: Radio construido utilizando únicamente hardware, no puede cambiarse por software. En este nivel no hay software, ni en el control ni en la realización propia de las funciones de operación del radio.
- Nivel 1: Radio controlado por software con restricciones en cuanto a funciones que pueden ser controlables. Se controlan algunas como nivel de potencia, interconexiones, etc. pero nunca modo o frecuencia.
- Nivel 2: En este nivel una gran parte del radio es configurable por software. Normalmente se utiliza el término Radio Controlado por Software (SCR). Existe control de software de ciertos parámetros como frecuencia, modulación, generación/detección de forma de onda, seguridad, etc. La etapa de radio frecuencia RF permanece en hardware y no puede ser reconfigurada. Es importante destacar que el software en este tipo de radios sólo controla funciones que están implementadas de modo físico dentro del radio, a hardware únicamente (Garcia, 2011).
- Nivel 3: Este nivel alberga todos los radios en los que por lo menos una de sus funciones está definida por software, incluyendo la tecnologia Radio Definido por Software Ideal

(ISR) donde la frontera entre la parte configurable y la no configurable se encuentra muy cercana a la antena, y la etapa final de radio frecuencia RF es configurable. Se puede decir que el ISR es completamente programable.

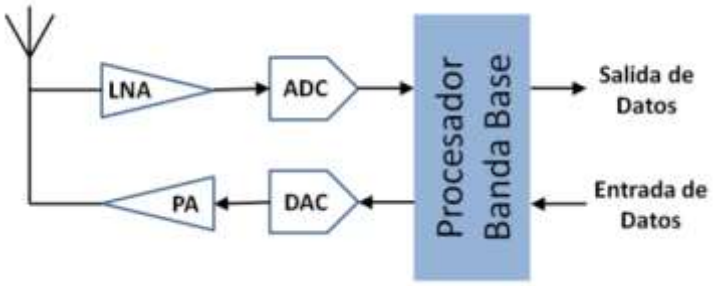


Figura 33-1: Diagrama en bloques simplificados de un SDR nivel 3

Fuente: (García, 2011)

- Nivel 4: Los equipos pertenecientes a este nivel se les conoce como Ultimate Software Radio (USR) y constituyen una etapa superior al ISR puesto que no solo son completamente programables, sino que además son capaces de soportar un amplio rango de funciones y frecuencias simultáneamente. Dentro de este nivel se encuentran los teléfonos celulares con soporte para varios estándares.

1.4.2 USRP B210

El USRP B210 proporciona una plataforma de periféricos de radio de software universal (USRP) de placa única totalmente integrada con cobertura de frecuencia continua de 70 MHz a 6 GHz. El USRP B210 proporciona una plataforma de periféricos de radio de software universal (USRP) de placa única totalmente integrada con cobertura de frecuencia continua de 70 MHz a 6 GHz. Diseñado para la experimentación de bajo costo, combina el transceptor de conversión directa RFIC AD9361 que proporciona hasta 56MHz de ancho de banda en tiempo real, un FPGA Spartan6 abierto y reprogramable y una rápida conectividad SuperSpeed USB 3.0 con una conveniente alimentación por bus. El soporte completo para el software USRP Hardware Driver (UHD) le permite comenzar a desarrollar inmediatamente con GNU Radio, crear un prototipo de su propia estación base GSM con OpenBTS y un código de transición sin problemas desde USRP B210 a plataformas USRP de mayor rendimiento y listas para la industria. Un kit de accesorios de caja está disponible para los usuarios de dispositivos PCB verdes (revisión 6 o posterior) para ensamblar una caja protectora de acero (Ettus, 2021).

Experimente con el USRP B210 en una amplia gama de aplicaciones que incluyen: transmisión de TV y FM, celular, GPS, WiFi, ISM y más. Los usuarios pueden comenzar inmediatamente a crear prototipos en GNURadio y participar en la comunidad SDR de código abierto. El soporte completo del software UHD permite la reutilización perfecta del código de los diseños existentes, la compatibilidad con aplicaciones de código abierto como HDSDR y OpenBTS, y una ruta de actualización a los sistemas USRP listos para la industria para cumplir con los requisitos de las aplicaciones. A continuación, se muestran algunos ejemplos de lo que puede hacer con un USRP B210 (Ettus, 2021).

La interfaz de RF integrada en el USRP B210 está diseñada con el nuevo Analog Devices AD9361, un transceptor de conversión directa de un solo chip, capaz de transmitir hasta 56 MHz de ancho de banda de RF en tiempo real. El B210 usa ambas cadenas de señales del AD9361, proporcionando una capacidad MIMO coherente. El procesamiento y control de la señal a bordo del AD9361 se realiza mediante un FPGA Spartan6 XC6SLX150 conectado a una PC host mediante SuperSpeed USB 3.0. El rendimiento en tiempo real de USRP B210 se compara con una cuadratura de 61,44 MS / s, lo que proporciona los 56 MHz de ancho de banda de RF instantáneo a la PC host para un procesamiento adicional mediante GNU Radio o aplicaciones que utilizan la API UHD. Para conocer las capacidades de rendimiento detalladas en varias configuraciones SISO y MIMO, consulte la tabla de referencia USRP B200 / B210 (Ettus, 2021).

CAPITULO II

2 MARCO METODOLÓGICO

En este capítulo se describirá la metodología utilizada, así como los tipos de investigación, métodos de investigación y técnicas de investigación que se utilizaron para el desarrollo del trabajo. Se detallará los requerimientos de los equipos y el desarrollo de la implementación de la central 4G virtual.

2.1 Metodología

Este apartado se desarrolló con el objetivo de obtener información necesaria acerca de las redes móviles 4G, la virtualización de funciones de red NFV y la utilización de equipos SDR, para así determinar los aspectos importantes para la virtualización de una central 4G en el laboratorio de comunicaciones de la FIE.

2.1.1 Tipo de Investigación

La investigación de este trabajo es de tipo aplicada ya que se busca obtener una correcta virtualización de una central EPC para que así las entidades como eNB o UE puedan acceder y utilizar todos los recursos que brinda este núcleo 4G.

2.1.2 Métodos de Investigación

El método de investigación utilizado es de tipo investigativo y aplicativo ya que se pretende virtualizar una central 4G con el fin de analizar los resultados obtenidos con pruebas de conectividad mediante la simulación de un eNB y un equipo de usuario UE.

2.1.3 Técnicas de Investigación

La principal técnica de investigación utilizada es la aplicada ya que se determinará el funcionamiento de la central 4G con la ayuda de la simulación de un equipo de usuario para así mediante capturas de trafico de paquetes IP determinar la correcta conectividad de UE con redes 3GPP o no 3GPP.

2.2 Implementación

2.2.1 Creación de las máquinas virtuales

Para empezar, se debe verificar que el hardware tenga la capacidad mínima necesaria para el correcto funcionamiento del software de virtualización, las máquinas virtuales deben tener las siguientes características mínimas en cuanto a capacidad de hardware:

- Memoria RAM: 4 GigaBytes (GB)
- Memoria ROM: 30 GigaBytes (GB)
- Procesadores: 4 Core (capacidad >=i5 de intel)
- Tarjetas de red: 1
- Puertos USB: 2

Una vez verificado la correcta disponibilidad del hardware, el primer paso es la instalación local del software de virtualización en este caso se utilizó VMware Workstation Pro 15, se recomienda instalar la última versión disponible. Una vez instalado correctamente el software de virtualización, pasamos a la creación de las máquinas virtuales, a las cuales se les ha proporcionado las siguientes características para que proporcionen un rendimiento eficiente al escenario de simulación:

Máquina para EPC

- Memoria RAM: 4 GigaBytes (GB)
- Memoria ROM: 50 GigaBytes (GB)
- Procesadores: 4 Core (2 físicos y 2 virtuales)
- Tarjetas de red: 2
- Sistema Operativo: Ubuntu 16.04 LTS

Máquina para OAISIM, eNB y UE

- Memoria RAM: 4 GigaBytes (GB)
- Memoria ROM: 50 GigaBytes (GB)
- Procesadores: 4 Core (2 físicos y 2 virtuales)
- Tarjetas de red: 1
- Puertos USB: 1
- Sistema Operativo: Ubuntu 14.04 LTS

Una vez creado las máquinas virtuales se debe tener en cuenta la configuración de sus tarjetas de red. Para la maquina EPC una tarjeta de red se ha utilizado para la conectividad hacia internet y la otra para conectividad con la maquina OAISIM. Mientras que para la maquina OAISIM se tarjeta de red se ha configurado para que tenga conectividad con la central EPC. A continuación, las especificaciones de las direcciones IP:

Tabla 1-2: Configuración de Red Maquina EPC

Maquina EPC	
Red para el acceso a internet	eth0
Dirección IP DHCP	172.25.203.78
Mascara de red	24
Dirección IP de broadcast	172.25.203.255
Red para la conexión con OAISIM	eth1
Dirección IP estática	10.0.0.1
Mascara de Red	24
Dirección IP de broadcast	10.0.0.255

Realizado por: (Henry Yugsin, 2022)

Tabla 2-2: Configuración de Red Maquina OAISIM

Maquina OAISIM	
Red para la conexión con EPC	eth0
Dirección IP estática	10.0.0.2
Mascara de red	24
Dirección IP de broadcast	10.0.0.255

Realizado por: (Henry Yugsin, 2022)

Una vez que se haya configurado las tarjetas de red correctamente, se debe realizar una prueba de conectividad entre la maquina EPC y OAISIM para verificar que tengan comunicación, para ello se ejecuta un comando de ping entre ambas máquinas.

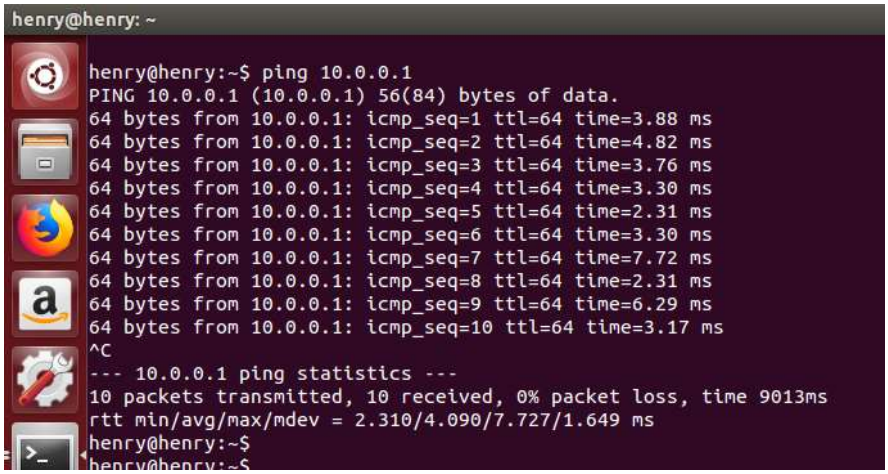


Figura 1-2: Conectividad EPC-OAISIM

Realizado por: (Henry Yugsin, 2022)

De igual manera se debe verificar que la maquina EPC tenga acceso a internet, lo cual se comprueba ejecutando un comando de ping hacia un servidor de Google:

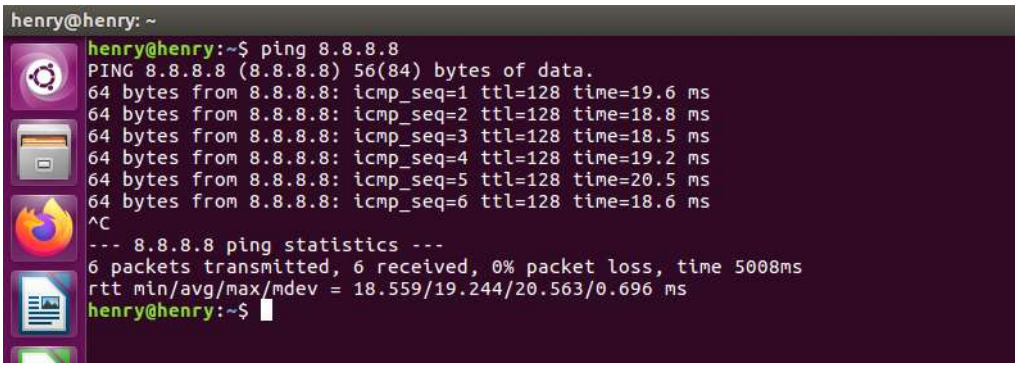


Figura 2-2: Conectividad EPC hacia Internet

Realizado por: (Henry Yugsin, 2022)

El esquema de conexión entre las máquinas EPC y OAISIM se muestra en la siguiente figura:

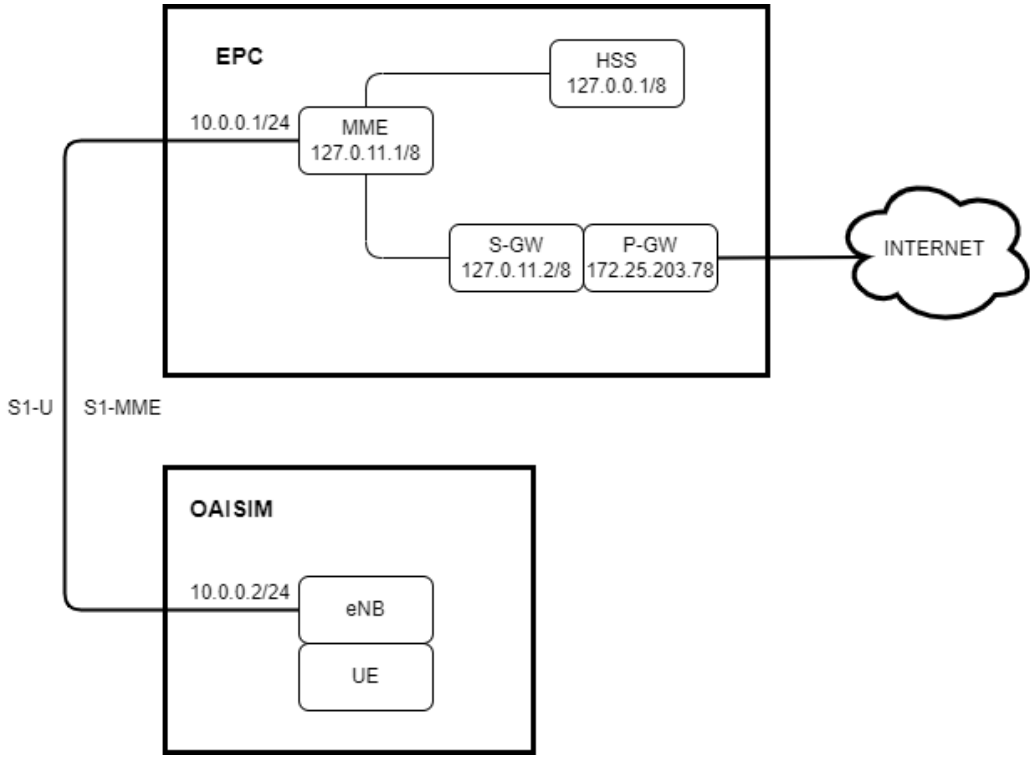


Figura 3-2: Esquema EPC-OAISIM Virtual - Escenario 1

Realizado por: (Henry Yugsin, 2022)

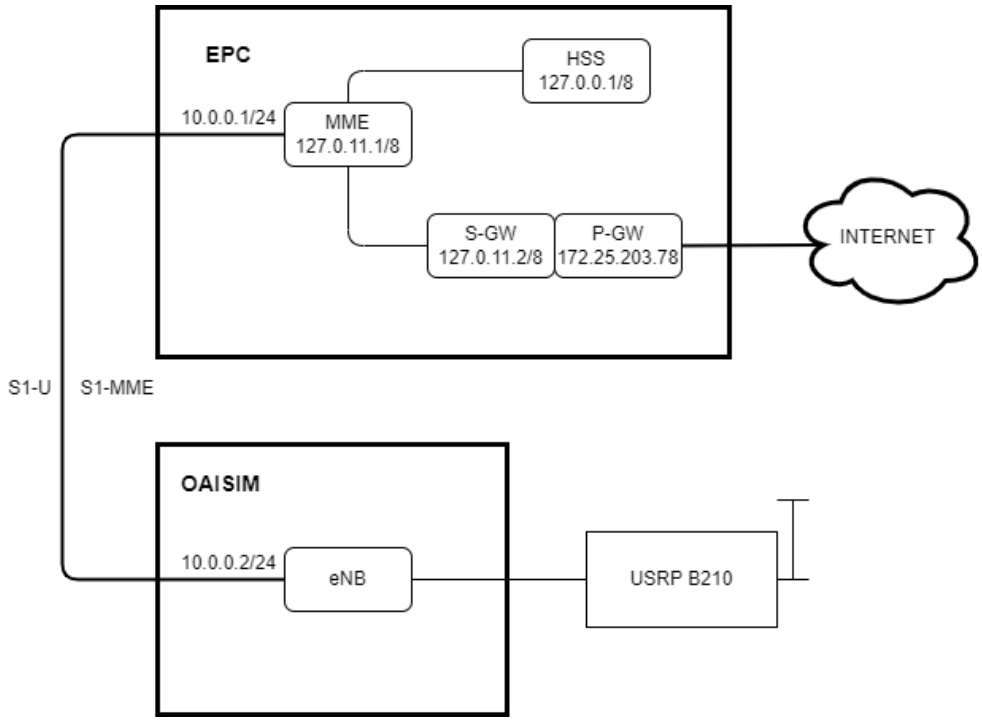


Figura 4-2: Esquema EPC-eNB con equipo SDR – Escenario 2

Realizado por: (Henry Yugsin, 2022)

2.2.2 Instalaciones previas

2.2.2.1 Instalación de kernel de baja latencia

Estas instalaciones previas se deben realizar para el correcto funcionamiento del software. Para el sistema operativo Ubuntu Linux, OpenAirInterface recomienda la instalación de un kernel de baja latencia. Para ello se utilizará la versión 3.19 del kernel del sistema operativo Ubuntu 14.04 LTS y la versión 4.10 del kernel del sistema operativo Ubuntu 16.04 LTS.

Para empezar con la instalación lo primero es asegurarse que el sistema operativo este actualizado y funcionando correctamente sin ninguna dependencia faltante, para ello se ejecuta los siguientes comandos en el terminal del sistema:

```
$ sudo apt-get update
$ sudo apt-get upgrade
```

Una vez verificado que el sistema este actualizado y funcionando correctamente, se procede a la instalación del kernel, para ello se ejecuta el siguiente comando en el terminal:

```
$ sudo apt-get install linux-image-3.19.0-61-lowlatency linux-headers-3.19.0-
61-lowlatency
```

El gestor de paquetes se encargará de realizar la instalación del kernel. Una vez finalizado la instalación es necesario reiniciar la máquina para que los cambios se carguen correctamente al equipo. Para verificar que la instalación ha sido exitosa se debe ejecutar el siguiente comando:

```
$ uname –r
3.19.0-61-lowlatency
```

Con ello se verifica que el kernel deseado se encuentra instalado de manera satisfactoria, ya que el terminal muestra el parámetro 3.19.0-61-lowlatency.

2.2.2.2 Deshabilitado de los estados C del BIOS

Para el correcto funcionamiento del programa es necesario desactivar cualquier tecnología de gestión de potencia y energía, en la BIOS del sistema como en el sistema operativo. Para ello se debe deshabilitar los estados C y P del procesador. En primer lugar, procedemos a eliminar todas

las funciones de administración de energía de la BIOS conocidos como estados del sueño, particularmente C-states. Para ello se debe editar el fichero:

```
$ sudo nano /etc/default/grub
```

Este comando lanza a un editor de texto en el mismo terminal el cual permite modificar el fichero de configuración de arranque. Se debe localizar la línea GRUB_CMDLINE_LINUX_DEFAULT y se modifica con los siguientes parámetros:

```
GRUB_CMDLINE_LINUX_DEFAULT=”quiet splash intel_pstate=disable
processor.max_cstate=1 intel_idle.max_cstate=0 idle=poll net.ifnames=0
biosdevname=0”
```

Se debe guardar los cambios con las teclas ctrl+o y después salir con las teclas ctrl+x. Para que se hagan efectivo los cambios en el terminal se debe ejecutar el siguiente comando:

```
$ sudo update-grub
```

De igual manera se debe realizar otra modificación en el siguiente archivo:

```
$ sudo nano /etc/modprobe.d/blacklist.conf
```

En el final del archivo se debe agregar la siguiente línea:

```
blacklist intel_powerclamp
```

Para verificar que los cambios efectuados han sido exitosos, se instala la herramienta i7z, para lo cual se ejecuta el siguiente comando:

```
$ sudo apt-get install i7z
```

Para iniciar el programa se ejecuta el siguiente comando:

```
$ sudo i7z
```

Debemos comprobar que los procesadores no cambien su frecuencia en más de 1-2 MHz y no deben tener ningún estado C que no sea C0. Es necesario comprobar esto ya que caso contrario existirán futuros problemas de tiempo real con el eNB y UE. En la siguiente figura se puede apreciar que los cambios efectuados han sido exitosos.

2.2.2.3 Desactivación del escalado de frecuencia del CPU

De igual manera es importante desactivar el escalado de frecuencias del CPU, para lo cual se debe instalar la herramienta cpufrequtils, con el comando:

```
$ sudo apt-get install cpufrequtils
```

Posteriormente se debe editar el archivo /etc/default/cpufrequtils (en caso de no existir se debe crear el archivo). Se debe añadir la siguiente línea:

```
GOVERNOR=”performance”
```

Después de guardar el archivo se debe desactivar ondemand daemon, caso contrario una vez que reiniciemos todos estos cambios se desaparecerán, para desactivarlo se debe ejecutar los siguientes comandos:

```
$ sudo update-rc.d ondemand disable
$ sudo /etc/init.d/cpufrequtils restart
```

Para comprobar que todo esté bien ejecutamos el comando:

```
$ cpufreq-info
```

Una vez finalizado se debe reiniciar las máquinas virtuales y comprobar con el comando anterior que no se han modificado los parámetros.

2.2.3 Instalación

2.2.3.1 Instalación de EPC

Para poder descargar los repositorios desde gitlab es necesario descargar la herramienta de instalación git, para ello se ejecuta el siguiente comando:

```
$ sudo apt-get install subversion git
```

Procedemos a descargar openair-cn desde el repositorio de gitlab de eurecom, nos pedirá usuario y contraseña por lo que es necesario registrarse en gitlab para poder descargar, clonamos el repositorio de la siguiente manera:

```
$ git clone https://gitlab.eurecom.fr/oai/openair-cn.git
```

Una vez que hemos descargado el repositorio debemos especificar FQDM (Fully Qualified Domain Name). Para ello debemos editar el siguiente archivo:

```
$ sudo nano /etc/hosts
```

Este fichero permite establecer una relación entre direcciones IP y nombres de máquina. En OAI, los diferentes módulos se comunican a través de direcciones IP internas/locales (127.X.X.X) y en un puerto. Solo el MME y el HSS utilizaran los FQDM. En dicho archivo se debe incluir la configuración:

```
127.0.0.1 localhost
127.0.1.1 henry.openair4G.eur   henry
127.0.1.1 hss.openair4G.eur   hss
```

Para que los cambios se hagan efectivos es necesario reiniciar la máquina.
Se debe descargar todos los paquetes necesarios para las tres entidades del núcleo EPC, para ello se debe ingresar al siguiente directorio:

```
$ sudo ~/openair-cn/scripts
```

Y usamos los tres comandos para instalar los paquetes necesarios para EPC.

```
$ ./build_hss –i
$ ./build_mme –i
$ ./build_spgw –i
```

Con la utilización de la opción –i, se instala por primera vez todos los paquetes necesarios para la correcta compilación y ejecución de cada una de las entidades, por lo que es necesario ejecutarlo solo la primera vez.

Ya para finalizar se debe crear una carpeta en /usr/local/etc/oai y copiar algunos archivos que servirán para la configuración de las entidades de EPC posteriormente, para ello se ejecuta las siguientes líneas de comando:

```
$ sudo mkdir -p /usr/local/etc/oai/freeDiameter
$ sudo cp ~/openair-cn/ETC/hss.conf /usr/local/etc/oai
$ sudo cp ~/openair-cn/ETC/mme.conf /usr/local/etc/oai
$ sudo cp ~/openair-cn/ETC/spgw.conf /usr/local/etc/oai
$ sudo cp ~/openair-cn/ETC/acl.conf /usr/local/etc/oai/freeDiameter
$ sudo cp ~/openair-cn/ETC/hss_fd.conf /usr/local/etc/oai/freeDiameter
$ sudo cp ~/openair-cn/ETC/mme_fd.conf /usr/local/etc/oai/freeDiameter
```

Figura 5-2: Comandos para copiar los archivos de EPC en los ficheros de Ubuntu

Realizado por: (Henry Yugsin, 2022)

Con estas configuraciones se debe tener en cuenta que solamente se puede realizar una vez ya que se copian directamente en los ficheros raíz de nuestra maquina Ubuntu.

2.2.3.2 Instalación de OAISIM

Primero se debe descargar el repositorio de openairinterface5g desde gitlab, modulo correspondiente a la red de acceso radio (E-UTRAN, eNodeB y UE). Podemos descargarlo con el siguiente comando:

```
$ git clone https://gitlab.eurecom.fr/oai/openairinterface5g.git
```

Una vez culminado la descarga se debe proceder a actualizar los ficheros descargados a la versión master o estable de la implementación. Para lo cual se tiene los siguientes comandos:

```
$ cd openairinterface5g
$ git checkout master
$ git pull
```

Una vez actualizado ya se puede proceder a la instalación de todos los paquetes necesarios para el correcto funcionamiento de OAI. Para la instalación se ejecutan los siguientes comandos:

```
$ source oaienv
$ cd cmake_targets
$ ./build_oai –I --eNB -x –install-system-files -w USRP --T -tracer
```

La primera vez que se realiza la instalación es necesario especificar las siguientes opciones:

- -I: instala todos los paquetes de software requeridos.
- --eNB: especifica que se va a realizar la instalación del eNB.
- -x: instala un osciloscopio software que permite monitorizar el nivel físico.

- --install-system-files: instala los ejecutables de OAI en el sistema.
- -w: especifica la plataforma SDR que se va a utilizar, en este caso USRP.
- --T-tracer: habilita la utilización del framework de monitorización T Tracer de OAI.

Para la monitorización de paquetes es necesario instalar el framework de monitorización T Tracer. Para ello, se ejecutan los siguientes comandos:

```
$ sudo ~/openair-cn/common/utils/T/tracer
$ sudo apt-get install libxft-dev
$ make
```

2.2.4 Configuración

2.2.4.1 Configuración de EPC

En la central LTE se debe modificar los archivos de MME, HSS y PGWS, en los cuales se debe tener en cuenta sobre todo las IP, los puertos y los nombres de las interfaces, parámetros que deben estar configurados correctamente para que las entidades del núcleo puedan transmitir y recibir paquetes de datos sin ningún problema.

2.2.4.1.1 Configuración HSS

En esta sección configuraremos el HSS dentro de la máquina virtual, esta entidad funciona como la base de datos de EPC. El primer paso es la verificación de que la herramienta MySQL esté instalado correctamente. Esta herramienta se descarga automáticamente al momento que descargamos los ficheros necesarios para la entidad HSS en el apartado anterior, al momento de la descarga se debe ingresar un usuario y contraseña, el mismo que se debe tener en cuenta para editar los archivos de configuración de HSS. Con el siguiente comando se puede verificar que MySQL está instalado y funcionando correctamente:

```
$ mysql –u root -p
```

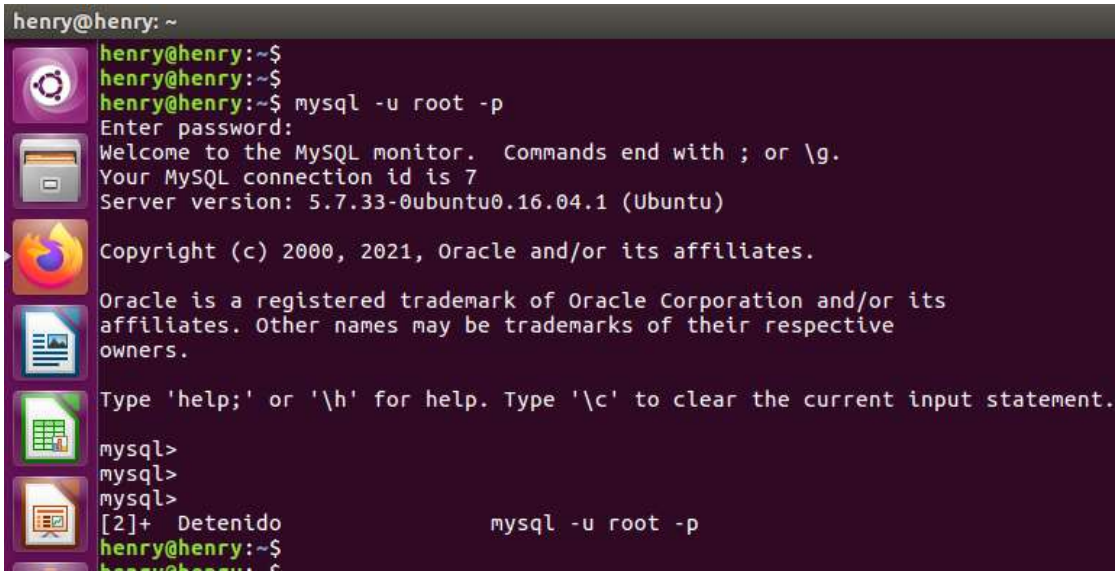


Figura 6-2: Correcto funcionamiento de MySQL

Realizado por: (Henry Yugsin, 2022)

En caso de encontrar problemas o no estar instalado MySQL se debe corregir los mismos ya que de lo contrario los eNBs y los UE no se podrán autenticar en la red y por ende se negarán los servicios que ofrece la central EPC.

Una vez que comprobemos el correcto funcionamiento de MySQL, se debe importar la base de datos de la herramienta OAI, la misma que está ubicada en /openair-cn/SRC/OAI_HSS/db/oai_db.sql. Para importar esta base de datos utilizamos la herramienta phpmyadmin que de igual manera se instala de manera automática con los paquetes de HSS, una vez dentro del gestor de base de datos phpmyadmin se debe crear una nueva base de datos con el nombre oai_db y en esta base de datos importar la base de datos de la herramienta OAI. Si el proceso fue exitoso se podrá observar lo siguiente:

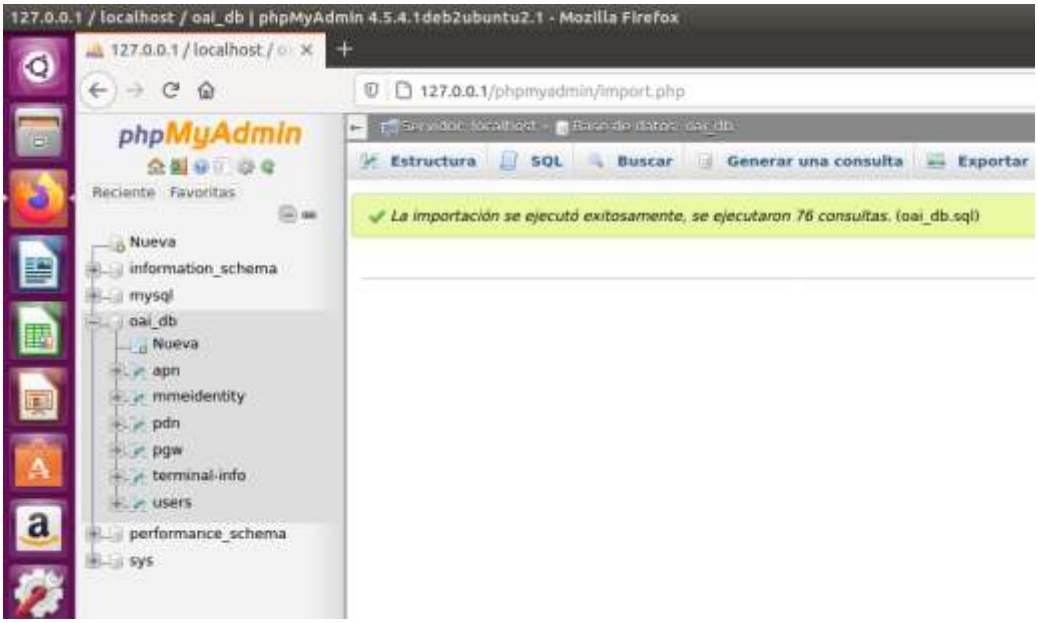


Figura 7-2: Correcta importación de la base de datos

Realizado por: (Henry Yugsin, 2022)

Esta base de datos contiene distintas tablas, de las cuales se deben tener en cuenta principalmente las siguientes:

- pdn

  Esta tabla contiene el APN y otros parámetros asignados a los IP Multimedia Subsystem (IMSI) de los usuarios. Los valores más importantes son el tipo de pdn, IMSI de cada identidad y sus umbrales de velocidad permitida tanto de subida como de bajada.

- apn

  En esta tabla se puede encontrar información sobre los nombres de los puntos de acceso.

- users

  Es la tabla utilizada para la autenticación de los usuarios, contiene información de todos los usuarios registrados en la red, esta tabla contiene campos como el IMSI, número de teléfono, International Mobile Equipment Identity (IMEI), mmeidentity_idmmeidentity, key (clave de cifrado usada), sqn (utilizada para sincronizar la tarjeta SIM con la red, autenticación), rand (valor aleatorio), OPc (parámetro usado por el operador para grabar los datos en la tarjeta SIM).

- mmeidentity

  Utilizada para configurar los nombres máquinas de las entidades mme y hss.

En la base de datos es necesario modificar dos campos en la tabla mmeidentity, en la cual se añade el nombre de los equipos involucrados y sus respectivos dominios:

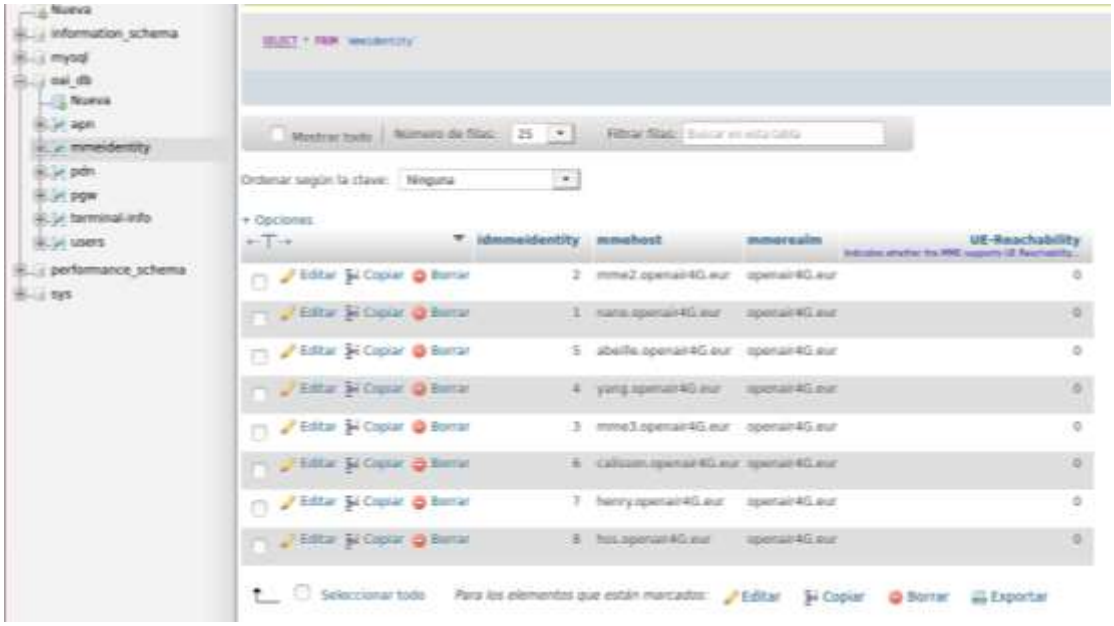


Figura 8-2: Modificación de tabla mmeidentity

Realizado por: (Henry Yugsin, 2022)

Posteriormente es necesario modificar el archivo /usr/local/etc/oai/hss.conf el mismo que se puede encontrar completo en los anexos, la mayoría de los campos quedan por defecto a excepción de los siguientes:

- MYSQL_server

  Indica la dirección IP (locales/internas) del servidor MySQL.

  Este tomara el valor IP de 127.0.0.1

- MYSQL_user

  Indica el nombre del usuario de la base de datos de MySQL (mismo valor que se configura en la instalación de MySQL).

  Este tomara el valor por defecto “root”.

- MYSQL_pass

  Indica la contraseña del usuario de la base de datos de MySQL (mismo valor que se configura en la instalación de MySQL).

  Este tomara el valor “root”.

- MYSQL_db

  Indica el nombre de la base de datos de MySQL (base de datos que fue importada anteriormente).

  Tomará el valor de oai_db.

También es necesario modificar el archivo /usr/local/etc/oai/freeDiameter/hss_fd.conf el mismo que se puede encontrar completo en los anexos, la mayoría de los campos quedan por defecto a excepción de los siguientes:

- Identity
  Tomará el valor de "hss.openair4G.eur"
- Realm
  Tomará el valor de "openair4G.eur"

2.2.4.1.2 Configuración MME

Para la configuración del MME es necesario cambiar los parámetros de dos archivos, el primero se encuentra en /usr/local/etc/oai/mme.conf, para ello se ejecuta el siguiente comando:

```
$ sudo nano /usr/local/etc/oai/mme.conf
```

En este archivo se debe modificar los siguientes parámetros:

- REALM
  Este parámetro indica el nombre del dominio. El cual toma el valor de "openair4G.eur".
- S6A_CONF
  Indica la ubicación del archivo de configuración de la interfaz S6A. Este tomara el valor de "/usr/local/etc/oai/freeDiameter/mme_fd.conf".
- HSS_HOSTNAME
  Contiene el nombre del equipo HSS. Tomará el valor de "hss".
- GUMMEI_LIST
  Esta lista contiene el identificador de entidad de administración móvil único a nivel mundial. Este contiene cuatro campos:
  - Mobile Country Code (MCC)
    Indica el código móvil del país. Se pondrá el valor "208".
  - Mobile Network Code (MNC)
    Indica el código de la red móvil. Toma el valor de "93".
  - MME_GID
    Indica el identificador de grupo de MME. Le daremos el valor de "4".
  - MME_CODE
    Indica el código de MME. Toma el valor de "1".
- TAI_LIST

Tracking Area Identifier List (TAI_LIST), esta lista contiene identidades de área de seguimiento. Contiene tres campos, MCC, MNC (debe ser el mismo que en GUMMEI_LIST), y el campo TAC (Technical Assistance Center) el mismo que es el código asociado de operador y le daremos el valor de 1.

- NETWORK_INTERFACES
  La configuración de red está compuesta de 5 campos que son:
  - MME_INTERFACE_NAME_FOR_S1_MME
    Da el nombre a S1 que conecta con la maquina OAISIM. Este tomara el valor de "eth0".
  - MME_IPV4_ADDRESS_FOR_S1_MME
    Da la IP a la tarjeta de red mediante la cual se conecta con la maquina OAISIM. Tomará el valor de "192.168.1.1/24".
  - MME_INTERFACE_NAME_FOR_S11_MME
    Da el nombre a S11 para utilizarse en la conexión con S/P-GW. La misma que será una dirección local ya que está dentro de la propia máquina. Le daremos el valor de "lo".
  - MME_IPV4_ADDRESS_FOR_S11_MME
    Dirección IP de S11, la cumple la función de conectar MME con el S/P-GW. Tomará el valor de "127.0.11.1/8".
  - MME_PORT_FOR_S11_MME
    Indica el puerto para la conexión con la interfaz S11. Tomará el valor de "2123".
- SGW_IPV4_ADDRESS_FOR_S11
  Indica la dirección IP del S-GW. Tomará el valor de "127.0.11.2/8".

Todos los demás campos se dejan los que vienen por defecto, de igual manera el archivo de configuración se puede encontrar en los anexos.

El siguiente archivo que se debe configurar se encuentra ubicado en /usr/local/etc/oai/freeDiameter/mme_fd.conf, para ello se ejecuta el siguiente comando:

```
$ sudo nano /usr/local/etc/oai/freeDiameter/mme_fd.conf
```

El archivo de configuración de igual manera se puede encontrar en los anexos, la mayoría de los campos se dejan con su valor por defecto a excepción de los siguientes:

- Identity
  Contiene la identidad dentro del dominio. Toma el valor de "henry.openair4G.eur".
- Realm

Indica el nombre del dominio. Toma el valor de “openair4G.eur”.

- Connect Peer

  Aquí se especifica el nombre del otro equipo al que estará conectado, para este caso es con el HSS. Para este se asigna el valor de “hss.openair4G.eur”. Esta parte contiene otros campos que deben tener los siguientes valores:

  - ConnectTo

    Indica la dirección IP del equipo HSS. Tomará el valor de “127.0.0.1”.

  - port

    Contiene el puerto de conexión con el equipo HSS. Tomará el valor de “3868”.

  - realm

    Indica el dominio en el que está el equipo HSS. Tomará el valor de “openair4G.eur”.

2.2.4.1.3 Configuración SPGW

En este apartado se realizará la configuración de SPGW, para esta entidad basta con modificar un solo archivo, este fue copiado en el directorio /usr/local/etc/oai/spgw.conf. La configuración completa se puede encontrar en los anexos. Para ingresar a este archivo se debe ejecutar el siguiente comando:

```
$ sudo nano /usr/local/etc/oai/spgw.conf
```

Aquí se debe identificar dos entidades, la primera es S-GW la cual sirve como pasarela de la red interna LTE y P-GW la cual funciona como pasarela de conexión a otras redes ya sea LTE o no. Los parámetros que se deben configurar son los siguientes:

- S-GW

  Contiene los parámetros asociados a las interfaces de red de S-GW.

  - SGW_INTERFACE_NAME_FOR_S11

    Es el nombre de S11 con la cual se conectará al MME. Tomará el valor de “lo”.

  - SGW_IPV4_ADDRESS_FOR_S11

    Dirección IP de la interfaz S11 mediante la cual se conecta al MME. Tomará el valor de “127.0.11.2/8”.

  - SGW_INT_NAME_FOR_S1U

    Interfaz mediante la cual se conectará al eNB. Le daremos el valor de “eth1”.

  - SGW_IP_ADD_FOR_S1U

    IPv4 que utilizara la interfaz para conectarse con el eNB. Tomará el valor de “192.168.1.1/24”.

- SGW_IPV4_PORT_FOR_S1U_S12_S4_UP
  Puerto de conexión al eNB. Le daremos el valor de “2152”.

- P-GW
  Contiene los parámetros asociados a las interfaces de red de P-GW. Se debe modificar los siguientes parámetros:
  - PGW_INTERFACE_NAME_FOR_SGI
    Indica el nombre de la interfaz de red mediante la cual tendremos salida hacia internet o hacia otras redes no LTE. Le daremos el valor de “eth0”.

2.2.4.2 Configuración de eNB

Para la configuración del eNB se debe tener en cuenta dos archivos de configuración, el primero sirve para el escenario totalmente virtual y el segundo para la utilización de SDR en este caso la USRP. El primer archivo se llama enb.band7.oaisim.conf (entorno totalmente virtual) y el segundo es enb.band7.tm1.usrpb210.conf (utilización de USRP). Los dos archivos contienen los mismos parámetros de configuración y para poder editarlos se debe ejecutar los siguientes comandos:

```
$ sudo nano /openairinterface5g/targets/PROJECTS/GENERIC-LTE-EPC/CONF/enb.band7.oaisim.conf
```

```
$ sudo nano /openairinterface5g/targets/PROJECTS/GENERIC-LTE-EPC/CONF/enb.band7.tm1.usrpb210.conf
```

Los archivos de configuración se pueden encontrar en los anexos. Los campos que se deben modificar son los siguientes:

- tracking_area_code
  Conocido como el código de área de seguimiento, este dato debe concordar con las configuraciones en EPC. Le daremos el valor de “1”.
- mobile_country_code
  Es el código móvil del país, de igual manera este campo debe concordar con las configuraciones de EPC. Tomará el valor de “208”.
- mobile_network_code
  Código de la red móvil, de igual manera este campo debe concordar con las configuraciones de EPC. Le daremos el valor de “92”.
- mme_ip_address

- ipv4

  Contiene la dirección IPv4 del mme. De igual manera este dato debe ser el mismo que el configurado en EPC. Le daremos el valor de “192.168.1.1”.
- ipv6

  Contiene la dirección IPv6 del mme. La versión IPv6 no la utilizaremos por lo que dejamos su valor por defecto.
- active

  Especifica si queremos que este activo el mme. Tomará el valor de “Yes”.
- preference

  Indica cuál de las versiones IP preferimos. En este caso será “IPv4”.

- NETWORK_INTERFACES

  Aquí se especifica las direcciones IP e interfaces del eNB, este contiene 5 campos a configurar:
  - ENB_INTERFACE_NAME_FOR_S1_MME

    Contiene el nombre de la interfaz S1 mediante la cual el eNB se conecta al MME. Esta tomara el valor de “eth0”.
  - ENB_IP_ADD_FOR_S1_MME

    IPv4 de la interfaz S1 = “192.168.1.2/24”.
  - ENB_INT_NAME_FOR_S1U

    Interfaz S1 mediante la cual se enviará el tráfico del usuario. Se le asigna el valor de “eth0”.
  - ENB_IP_ADDRESS_FOR_S1U

    IPv4 de S1, mediante esta se enviará los datos del usuario. Se asigna el valor de “192.168.1.2/24”.
  - ENB_PORT_FOR_S1U

    Especifica el número de puerto utilizado para la transmisión de los datos del usuario. Tomará el valor de “2152”.

2.2.4.3 Configuración de UE

Para la configuración del UE se debe tener en cuenta los siguientes parámetros asociados:

- IMSI International Mobile Subscriber Identity. Este es un código de identificación móvil único para cada dispositivo que esté conectado a las redes de telefonía. Permite su identificación en las redes GSM, UMTS y LTE.
- MSISDN Mobile Station Integrated Services Digital Network (Estación Móvil de la Red Digital de Servicios Integrados). Con este número es posible identificar a un equipo. Este

número no está atado al operador por lo que es factible migrar a otro operador. Es una entidad lógica y no se guarda en la SIM. Es posible asociar múltiples MSISDN a un solo SIM por lo que es posible localizar a un usuario a través de múltiples números con una sola SIM.

- IMEI International Mobile Station Equipment Identity (Identidad internacional del equipamiento móvil). Este número está inscrito en el propio móvil. No se utiliza para establecer conexión, pero sirve como seguridad en caso de robo del equipo móvil.
- IMEI SV similar a su homologo IMEI pero con especificación de SV "versión de software". Es decir, el mismo IMEI pero se añade los dos últimos dígitos la versión del software.
- KEY es la clave de la SIM y consiste en un valor de 32 dígitos en formato hexadecimal, este dato es proporcionado por el fabricante de las tarjetas SIM.
- OPc es el resultado del cálculo con clave OP (OP valor designado por el fabricante de la SIM). Este valor es calculado con la siguiente formula:

$$OPc = AES_{128}(K_i, OP) \oplus OP$$

Ecuación 2-2: Calculo de OPc

Estos valores de igual manera deben ser modificados en la tabla "users" de la entidad HSS, y los campos "key", "rand" y "OPc" deben cambiar su tipo de dato de varbinary a binary.

Para ingresar al archivo de configuración se debe ejecutar el siguiente comando:

```
$ sudo nano /openairinterface5g/targets/bin/ue_eurecom_test_sfr
```

En este archivo se debe editar los siguientes campos:

- IMEI
  Le daremos el valor de "35609204079301".
- MSIN
  Son los diez últimos números que conforman la IMSI. Le daremos el valor de "0000000001".
- USIM_API_K
  Es la clave. Tomará el valor de "8baf473f2f8fd09487cccbd7097c6862".
- OPC
  Es el valor calculado con la formula anterior. Este tomara el valor de "8e27b6af0e692e750f32667a3b14605d".
- MSISDN

Se le asigna el valor de "33638030001".

- HPLMN
  Junto con el MSIN confirman la IMSI, este compuesto de 5 números los 3 primeros corresponden a MCC y los dos restantes a MNC. Este tomara el valor de “20893”.

De igual manera el archivo de configuración puede encontrar en la parte de anexos.

2.2.5 Compilación y Ejecución del programa

2.2.5.1 Compilación y Ejecución de EPC

Una vez realizado la configuración de las entidades de EPC se debe compilar cada una de las entidades para verificar que todos los cambios estén correctos y listo para su posterior puesta en marcha. Para ello primero se ingresa al siguiente directorio:

```
$ sudo ~/openair-cn/scripts
```

Posteriormente se compila las tres entidades, donde la opción “c” es la que especifica que se trata de una compilación de las mismas.

```
$ ./build_hss –c
$ ./build_mme –c
$ ./build_spgw –c
```

Si las configuraciones de todas las entidades son correctas se debe apreciar los siguientes resultados:

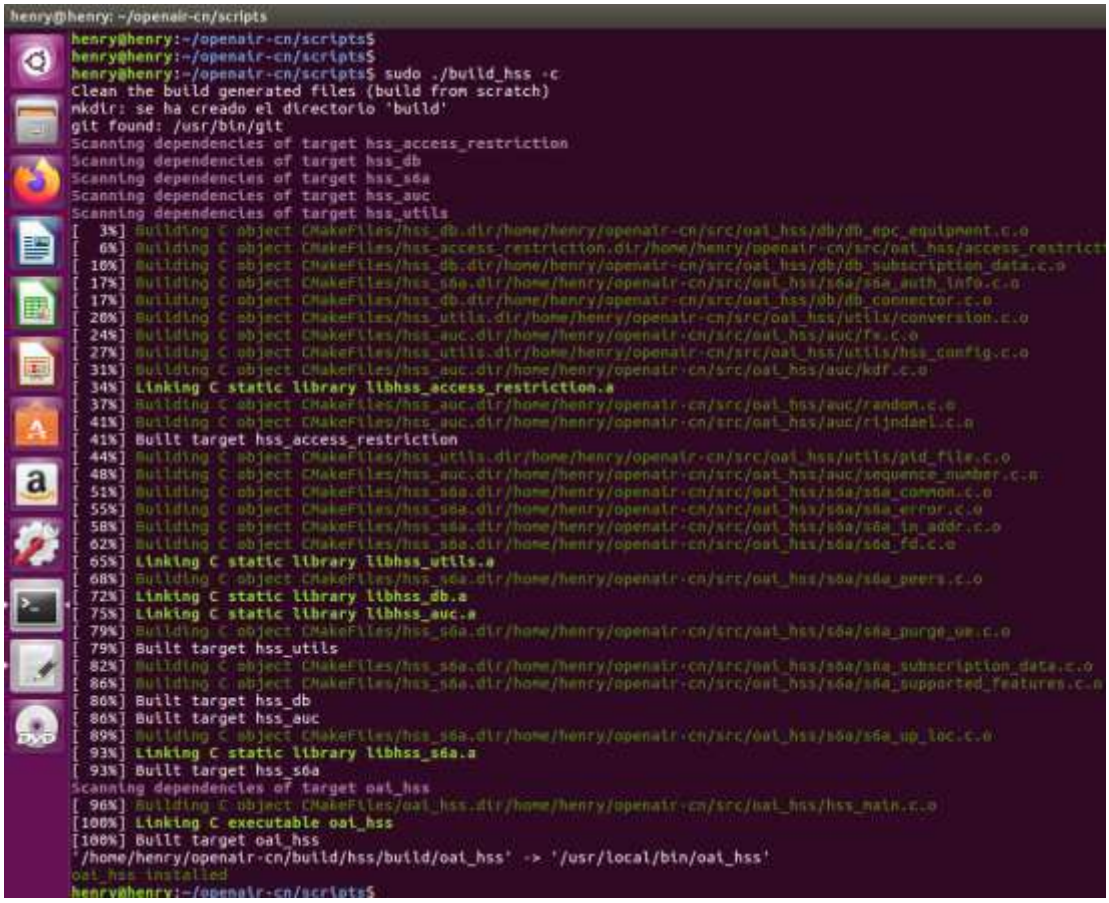


Figura 9-2: Compilación HSS

Realizado por: (Henry Yugsin, 2022)

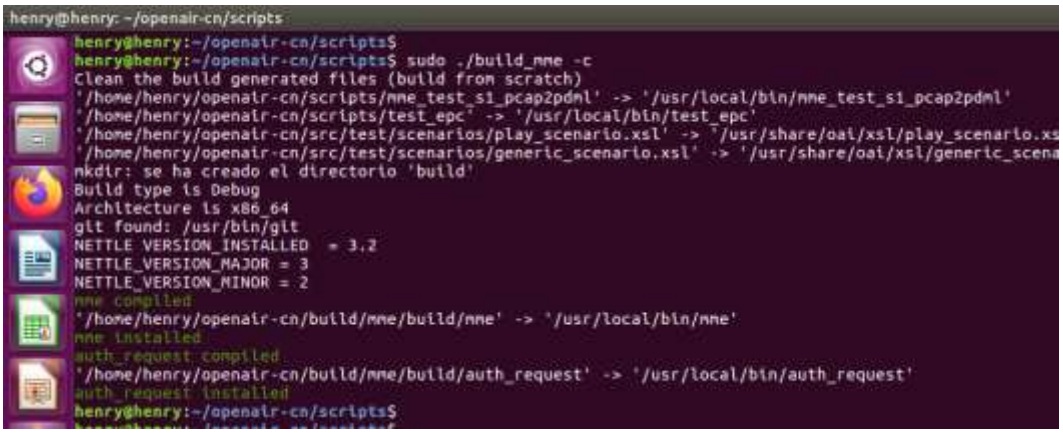


Figura 10-2: Compilación MME

Realizado por: (Henry Yugsin, 2022)

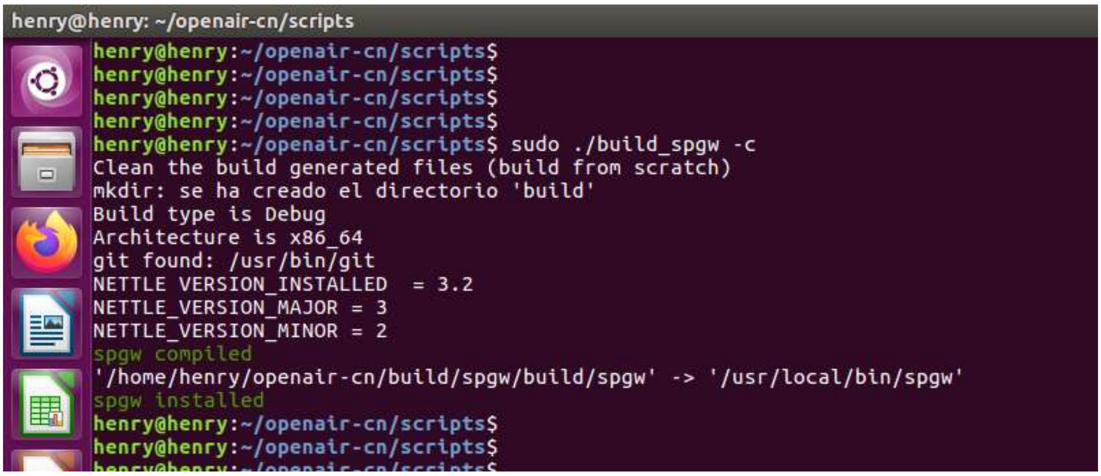


Figura 11-2: Compilación SPGW

Realizado por: (Henry Yugsin, 2022)

Una vez realizado esto, nuestro nucleo EPC está listo para ponerlo en marcha. La ejecución de las tres entidades HSS, MME y SPGW se lo realiza con los siguientes comandos:

```
$ ./run_hss
$ ./run_mme
$ ./run_spgw
```

Si la ejecución de las entidades ha sido exitosa se podrá apreciar lo siguiente en cada una de las ventanas de comandos:

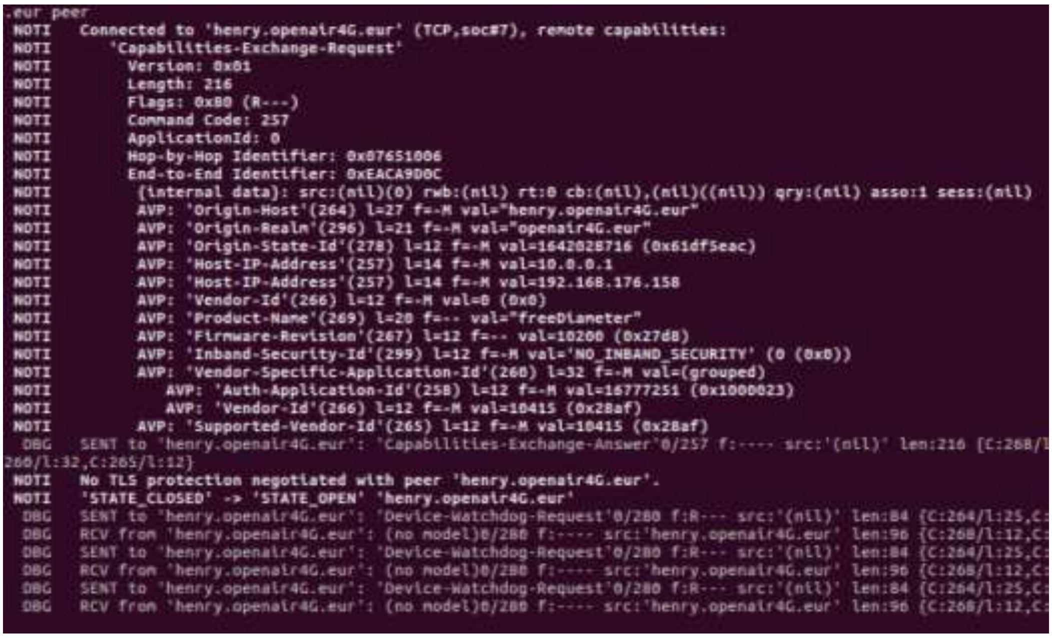


Figura 12-2: Correcta inicialización de la entidad HSS

Realizado por: (Henry Yugsin, 2022)

Figura 13-2: Correcta inicialización de la entidad MME

Realizado por: (Henry Yugsin, 2022)

Figura 14-2: Correcta inicialización de la entidad SPGW

Realizado por: (Henry Yugsin, 2022)

Si la ejecución de las cuatro entidades resulto exitosa, en las interfaces del sistema se deberá apreciar la aparición de una nueva interfaz llamada gtp0. Tal y como se puede observar en la figura 15-2.

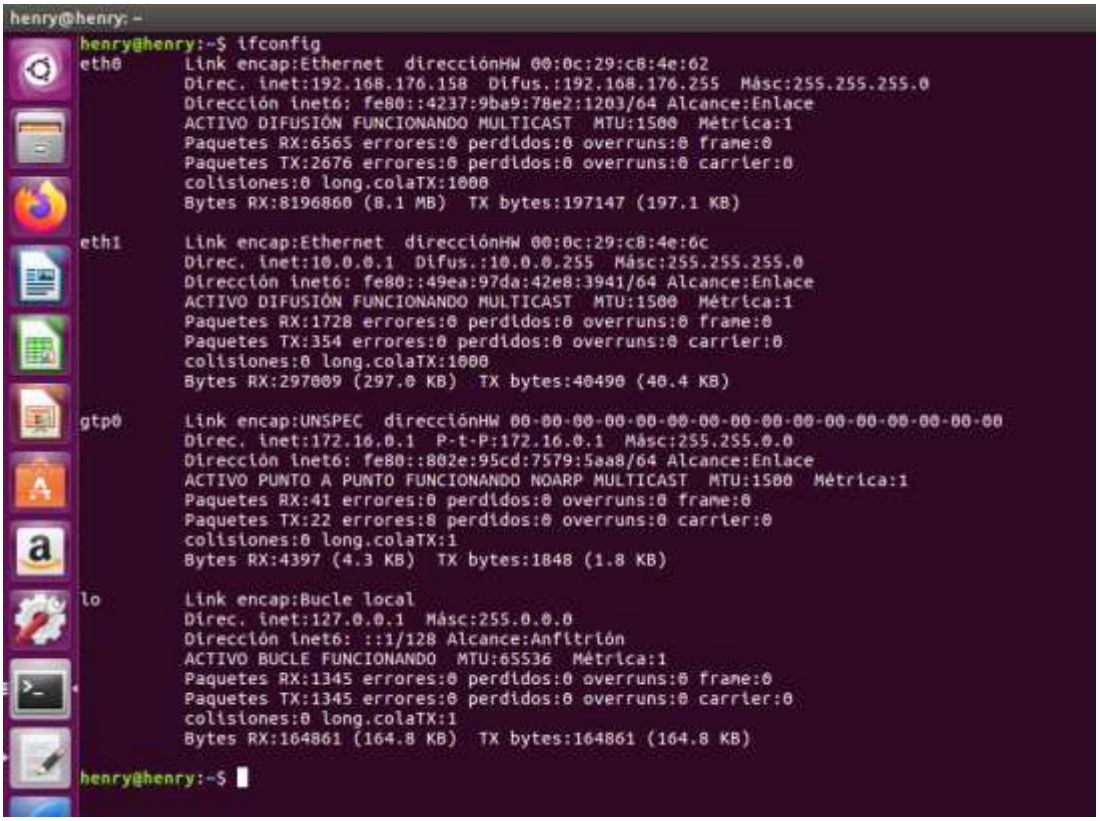


Figura 15-2: Levantamiento de la interfaz de túnel gtp0

Realizado por: (Henry Yugsin, 2022)

Con una ejecución exitosa nuestra central EPC de LTE está lista para conectarse con los eNBs, autenticar usuarios, direccionar el tráfico de usuarios hacia otras redes como el internet. La entidad que administra todos los dispositivos conectados a la central EPC es el MME y en la ventana de conexión del mismo se puede ver un menú en el cual se detalla la cantidad de eNBs, usuarios, y las interfaces que se han conectado o desconectado. Posteriormente se podrá verificar la conexión exitosa con los eNBs y los usuarios de OAISIM y OAI.

2.2.5.2 Compilación y Ejecución de OAISIM

La parte de OAISIM hace referencia a una virtualización total, es decir el eNB y el usuario UE va a estar virtualizado y literalmente no se realiza ninguna transmisión por interfaz aire, aunque la simulación cumple con el intercambio de todos los protocolos de autenticación y control reales de la red LTE. Para la compilación de esta entidad se debe ejecutar el siguiente comando:

```
$ sudo ~/openairinterface5g/cmake_targets
$ ./build_oai -c --oaisim --UE -x
```

- -c es la opción que especifica la compilación
- --oaisim crea un simulador de OAISIM. El hardware está definido como ninguno por defecto.
- --UE crea las partes específicas de UE.
- -x agrega una función de osciloscopio de software a los binarios producidos.

Si la compilación de estas partes ha sido exitosa se tendrá lo siguiente en la ventana de comandos:

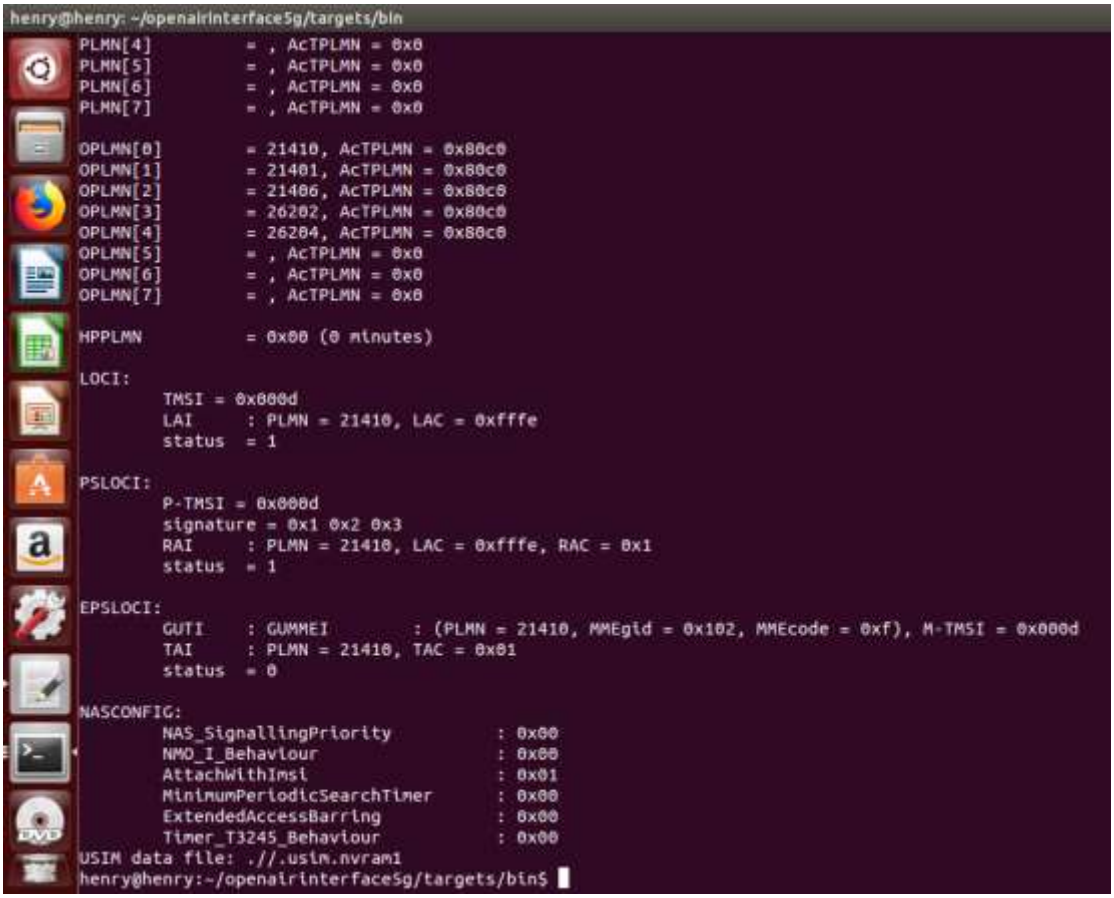


Figura 16-2: Compilación de OAISIM

Realizado por: (Henry Yugsin, 2022)

Una vez realizado la compilación se debe realizar unas configuraciones "adicionales" para que la interfaz del UE pueda crearse en la máquina virtual durante la ejecución de OAISIM.

```
$ sudo ~/openairinterface5g/targets/bin
$ sudo ifconfig oip0 up
$ sudo insmod ue_ip.ko
$ sudo ip route flush cache
$ sleep 1
$ sudo sysctl –w net.ipv4.conf.all.log_martians=1
$ sudo echo “Disabling reverse path filtering”
$ sudo sysctl –w net.ipv4.conf.all.rp_filter=0
$ sudo ip route flush cache
$ sudo fgrep lte /etc/iproute2/rt_tables >/dev/null
if [$? –ne 0 ]; then
echo “200 lte” >>/etc/iproute2/rt_tables
$ sudo ip rule add fwmark 1 table lte
$ sudo ip route add default dev $LTEIF table lte
```

Una vez realizado todas estas configuraciones, la entidad OAISIM está lista para su puesta en marcha, para lo cual se ejecuta el siguiente comando:

```
$ sudo ~/openairinterface5g/cmake_targets
$ sudo –E ./run_enb_ue_virt_s1
```

Una vez puesto en marcha el programa podemos ver que su ejecución ha sido exitosa comprobando las interfaces de red disponibles en la máquina virtual, se debe crear una nueva interfaz llamada oip1, la misma que debe tener una dirección IP acorde al DHCP configurado en la central EPC específicamente en la entidad SPGW. Dado que nuestro usuario virtual se ha creado correctamente y de igual manera se ha conectado correctamente a la central EPC, la virtualización de nuestra red LTE se ha llevado con éxito y en el próximo capítulo se realizará las pruebas de conectividad y el análisis de los protocolos de inicio de sesión exitosos.

2.2.5.3 Compilación y Ejecución de eNB

En este apartado se detalla la compilación y ejecución del eNB con el SDR para nuestro caso se utilizará un equipo USRP. Para la compilación de la entidad se debe ejecutar el siguiente comando:

```
$ cd ~/openairinterface5g/cmake_targets
$ ./build_oai –c --eNB -w USRP
```

Si la compilación ha sido exitosa se podrá observar en la ventana de comando lo siguiente:

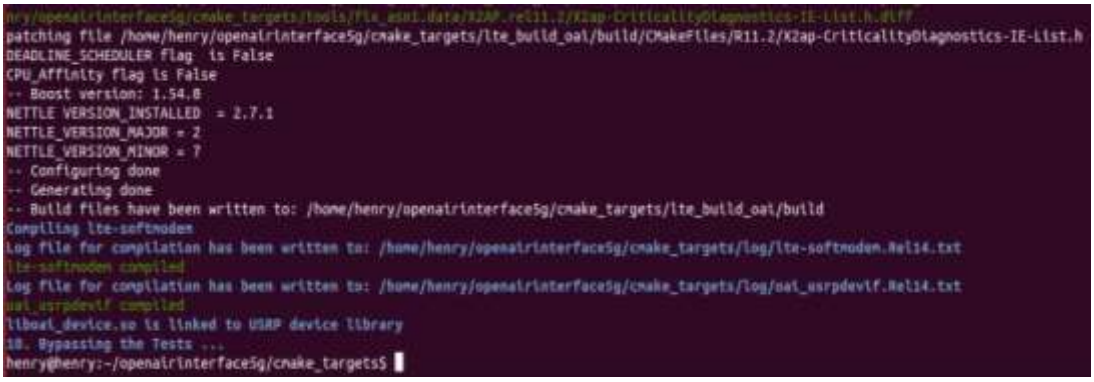


Figura 17-2: Compilación eNB con USRP

Realizado por: (Henry Yugsin, 2022)

Ya para la puesta en marcha de la entidad eNB, el primer paso es verificar que la USRP esté conectada a la CPU de nuestra máquina ya que de lo contrario saldrá un error en la ejecución de la entidad. Para ello se debe ejecutar el siguiente comando:

```
$ cd ~/openairinterface5g
$ sudo –E ./targets/bin/lte-softmodem –O ./targets/PROJECTS/GENERIC-LTE-EPC/CONF/enb.band7.tm1.usrpb210.conf
```

Si la ejecución del eNB ha sido exitosa se podrá observar lo siguiente en la ventana de comandos:

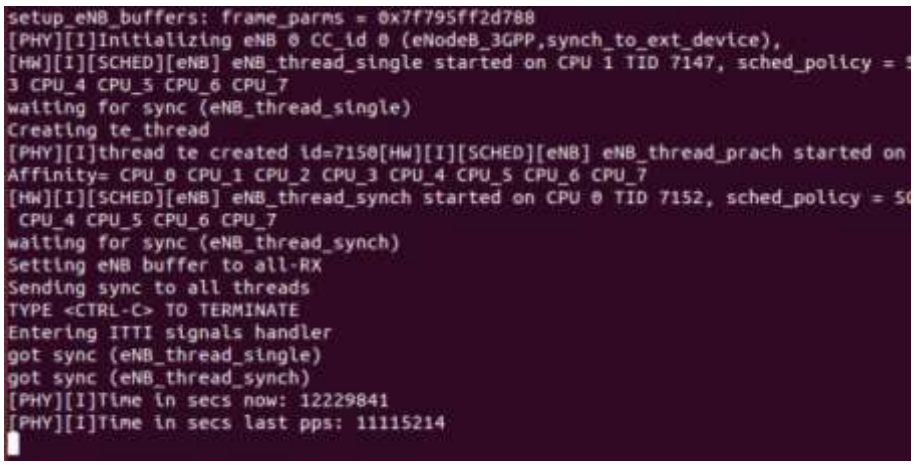


Figura 18-2: Ejecución del eNB con USRP

Realizado por: (Henry Yugsin, 2022)

Con esto la red LTE está lista para que los usuarios se puedan conectar a ella y acceder a sus servicios. En el capítulo siguiente se realizará el análisis de los parámetros de transmisión y recepción del eNB.

CAPITULO III

3 ANALISIS DE RESULTADOS

En el presente capítulo se comprobará los resultados obtenidos en las simulaciones realizadas. Para ello se realizará pruebas de conexión, verificación y medición de datos. Dado que tenemos dos escenarios de implementación se realizarán diferentes pruebas para cada uno de ellos.

3.1 Esquema EPC-OAISIM

Para el primer escenario que corresponde a un entorno totalmente virtual el mismo que se detalla en el capítulo 2, se comprobara que el usuario virtual se conecte exitosamente a la red LTE y pueda enviar/recibir paquetes hacia otras redes tanto internas como externas (internet), para validar el correcto funcionamiento de este escenario se seguirán los siguientes pasos:

- Analizar los paquetes transmitidos entre UE-eNB-EPC con la ayuda de la herramienta wireshark.
- Verificar el proceso de autenticación en la central LTE.
- Comprobación de la correcta asignación de la IP al usuario virtual.
- Prueba de ping del usuario virtual hacia redes internas y externas (internet).

A continuación, en la Figura 1-3 se muestra el escenario con las maquinas físicas y todo el equipo que se implementó en el laboratorio de comunicaciones de la FIE para el desarrollo de este escenario.

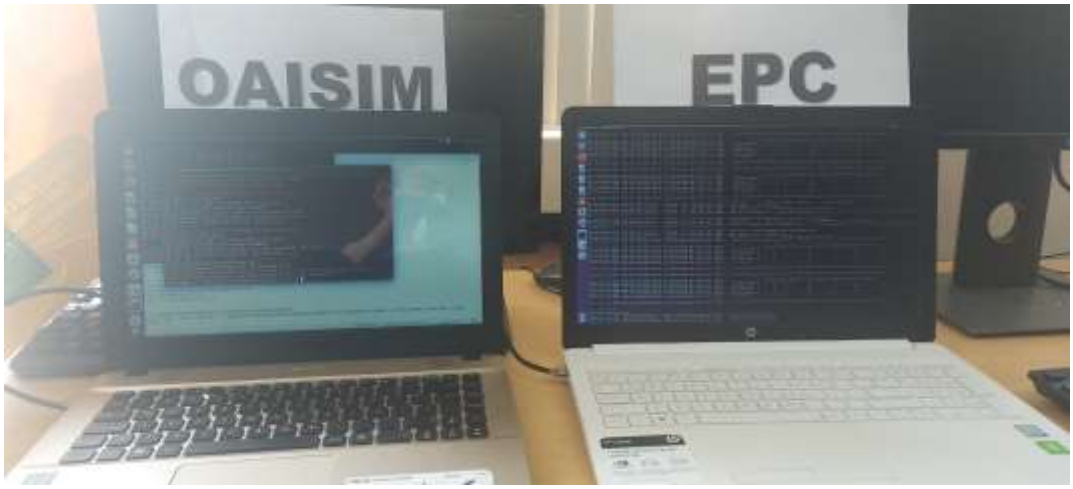


Figura 1-3: Fotografía de la Implementación del Escenario 1

Realizado por: (Henry Yugsin, 2022)

3.1.1 Análisis de paquetes de autenticación con wireshark

En el capítulo I en la sección 1.2.6 se detalla el proceso de autenticación de un usuario en la red LTE. En la figura 2-3 se puede apreciar todos los paquetes intercambiados entre la maquina EPC y OAISIM que corresponden a la autenticación tanto del eNB como la del usuario UE. La figura 3.1 puede ser analizada en las siguientes tres partes: Autenticación eNB con la central LTE, Autenticación usuario con la central LTE, EPS Bearer entre el UE y la central LTE.

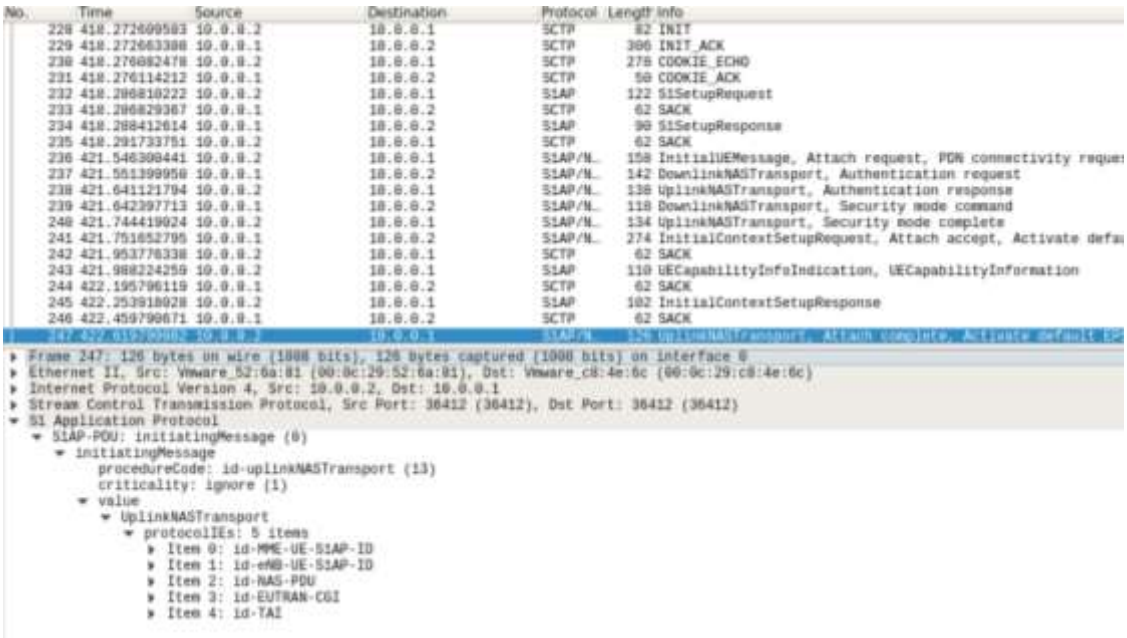


Figura 2-3: Autenticación del Usuario

Realizado por: (Henry Yugsin, 2022)

Como se puede apreciar en la figura 2-3, desde el número de paquete 228 hasta el paquete número 235 corresponde a la autenticación del eNB con la central LTE. En este intercambio de mensajes el eNB inicia enviando un mensaje llamado INIT con parámetros básicos para su identificación (MCC, MNC, TAI). Si los parámetros son iguales a los configurados en nuestra entidad MME el eNB se conectará sin mayor problema a la central EPC (Estos parámetros fueron configurados en los apartados 2.2.4.1.2 y 2.2.4.2). La autenticación finaliza con el mensaje COOKIE_ACK todos estos mensajes se encapsulan en el protocolo SCTP. Al mismo tiempo se debe levantar la capa S1AP que es la encargada de los mensajes de control entre el eNB y el MME a través de la interfaz S1-MME.

Posteriormente continua la autenticación del usuario el cual se puede observar en la Figura 2-3 desde el paquete número 236 hasta 240, en el apartado 1.2.6 se detalló todo el procedimiento que

la red LTE debe cumplir para que el UE se conecte a la central sin ningún problema. El paquete número 238 lleva el mensaje Authentication Response lo que nos dice que la autenticación del UE se realizó de manera exitosa. Después de esto la red LTE debe verificar la seguridad de los datos del usuario por lo que entre en proceso el levantamiento de seguridad NAS para ello el MME envía el paquete con los parámetros de seguridad NAS estos deben ser leídos por el equipo de usuario y una vez aceptados se reenviara un mensaje llamado Security mode complete (paquete número 240).

Por ultimo queda la conexión EPS Bearer que es establecida entre el UE y el P-GW para entregar trafico IP. Los bearer se identifican con el EPS Bearer ID. Los EPS Bearer ID son asignados por el MME. De igual manera la entidad MME envía el mensaje al usuario con todos los parámetros requeridos para el EPS Bearer ID, el UE los registra y reenvía un mensaje de aceptación como se puede apreciar en la Figura 2-3 (paquete numero 247) una vez finalizado este proceso el UE está listo para poder enviar/recibir información.

3.1.2 Autenticación en el núcleo EPC

El procedimiento de autenticación del UE también se puede apreciar desde la interfaz de las entidades HSS, MME y SPGW de la central EPC, a continuación, analizaremos cada una de ellas. Primero está la entidad HSS que como se define en el apartado 1.2.6 es la base de datos encargada de dar la información del usuario que sea solicitado por la entidad MME. La entidad HSS genera los vectores de autenticación (AVs) del usuario o usuarios solicitados y los envía a la MME. En la figura 3-3 se puede observar como HSS genera y envía los valores de AV $\{RAND, XRES, AUTN_{HSS}, K_{ASME}\}$ hacia MME del usuario requerido en este caso es el usuario "208930000000001".

Figura 3-3: Proceso de autenticación del usuario en la entidad HSS

Realizado por: (Henry Yugsin, 2022)

En la entidad MME cuenta con un cuadro estadístico que muestra la cantidad de eNB y UE conectados a la central LTE. Como se puede apreciar en el Anexo H existe 1 eNB y 1 UE que se conectaron correctamente a la red. De igual manera se puede apreciar en el Anexo H como el estado EMM-FSM del usuario "208930000000001" cambia de modo "DEREGISTERED" a "REGISTERED" esto nos dice que el usuario se autenticado sin ningún inconveniente a la red y que además cuenta con todos los permisos necesarios para utilizar los diferentes recursos de la red LTE.

Por ultimo esta la entidad S-PGW que es la encargada de los Bearers los mismos que son necesarios para él envió de trafico IP. Una vez que la entidad MME termina con el proceso de autenticación del UE envía un mensaje a S-PGW para que este le asigne una IP al usuario que se acaba de conectar a la red. Dependiendo de la configuración de DHCP en la entidad este asignara una IP al usuario en dicha red. En el Anexo I se puede apreciar cómo se levanta la sesión de Bearers y como el "SGI_UPDATE_ENDPOINT_RESPONSE" (el cual es un campo de Bearer ID) cambia su estado a "REQUEST ACCEPTED" esto nos quiere decir que ya se le asignó una IP al usuario con su correspondiente identificar de Bearer ("túnel ID"), con todo esto el usuario está listo para enviar/recibir información.

3.1.3 Comprobación de asignación de IP

Una vez realizado todo el proceso en la maquina OAISIM en la figura 4-3 se puede apreciar que se ha creado una nueva interfaz de red llamada oip1, la misma que tiene la IP asignada por la entidad S-PGW durante el procedimiento de autenticación, es importante verificar que esta interfaz esta levantada ya que por ahí se envía/recibe todos los paquetes de tráfico del usuario virtual.

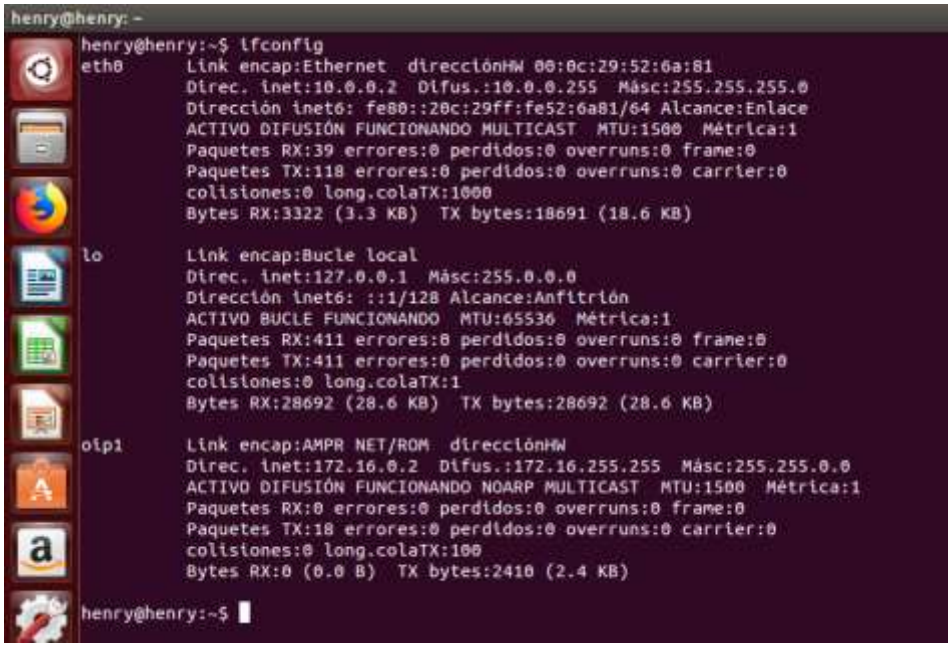


Figura 4-3: Comprobación de asignación de IP al usuario virtual.

Realizado por: (Henry Yugsin, 2022)

3.1.4 Prueba de conectividad del usuario

El escenario está listo para realizar las pruebas de conectividad, las mismas que se basan en enviar y recibir trafico IP a redes internas (a la propia central LTE) y hacia redes externas (internet). En la figura 5-3 se puede observar la correcta conectividad hacia la propia red (ping hacia 172.16.0.1) y conectividad hacia redes externas (ping 8.8.8.8). Esto nos indica que la implementación fue un éxito y que toda la red LTE tanto núcleo como parte radio esta funcionado según lo planificado. Además, cabe recalcar que el tráfico del usuario se encapsula en el protocolo GTP-U tal y como se lo había mencionado en el capítulo I.

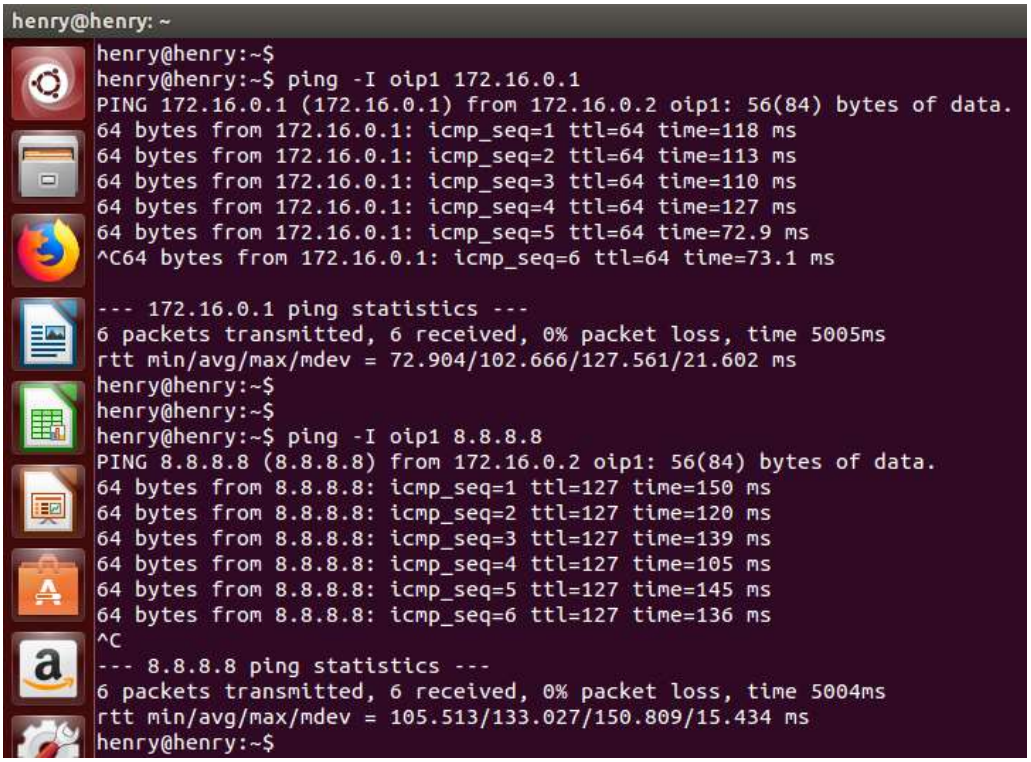


Figura 5-3: Prueba de conectividad del usuario virtual.

Realizado por: (Henry Yugsin, 2022)

En esta parte resulta importante analizar el flujo del trafico IP mediante la captura de wireshark, porque en la misma se puede evidenciar el encapsulamiento del tráfico del usuario mediante el protocolo de túnel de GPRS.

Primero analizaremos el trafico ICMP que fluye desde el usuario hasta su puerta de enlace, es decir hasta la entidad S-GW. En la figura 6-3 podemos observar que el paquete IP que envía y recibe el usuario está totalmente encapsulado con sus protocolos correspondientes, como se detalló en el capítulo I en la utilización de los protocolos de comunicación para el tráfico de usuario, este debe ser encapsulado en el protocolo de túnel GPRS (GTP), para que así el tráfico de usuario fluya a través de la red LTE sin ningún inconveniente.

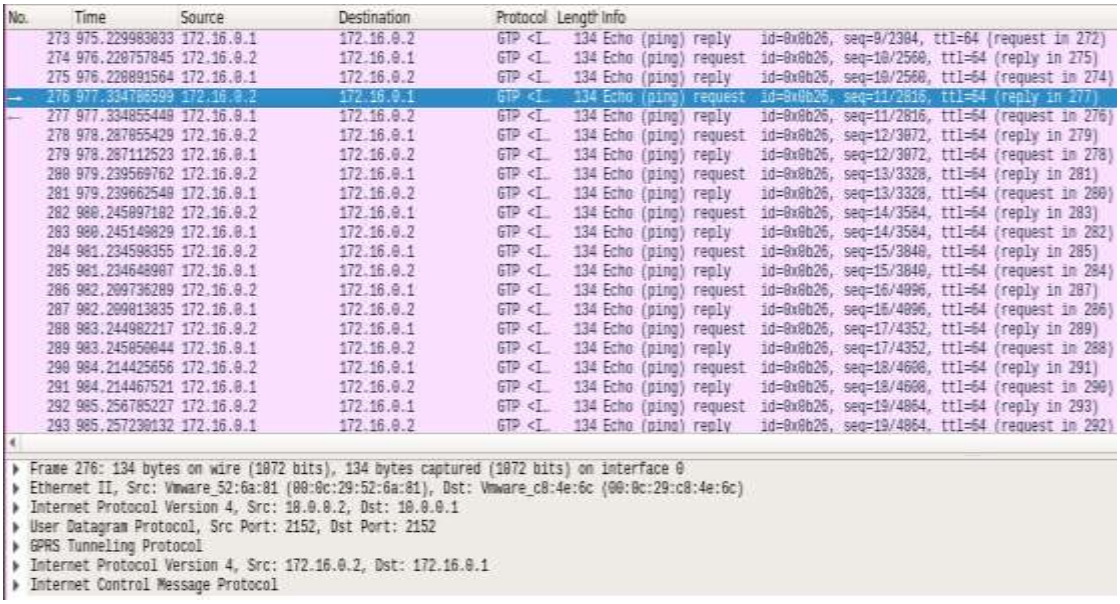


Figura 6-3: Encapsulación de paquetes IP del usuario hacia su puerta de enlace

Realizado por: (Henry Yugsin, 2022)

Después este tráfico debe pasar por la entidad que realiza el túnel dentro de la central 4G es decir la entidad S-GW, para ello este tráfico debe pasar por la interfaz de túnel gtp0 que está en la central, en la figura 7-3 se puede observar el trafico ICMP del usuario que fluye correctamente a través de la interfaz de túnel gtp0, la cual genera la conectividad entre el S-GW y el UE. Se puede observar a que este tráfico ya no está encapsulado mediante GTP sino más bien es netamente IP de usuario y IP de S-GW.

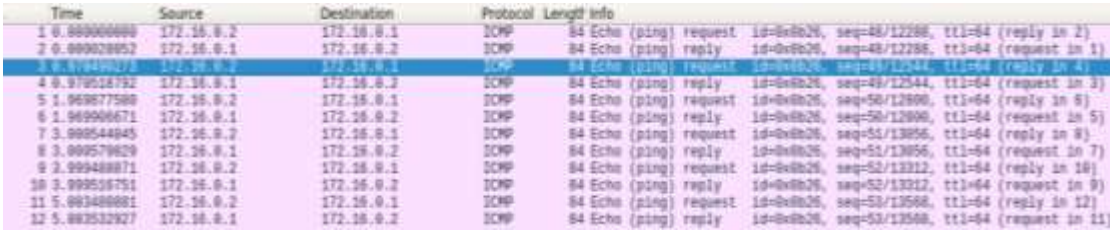


Figura 7-3: Flujo de paquetes IP del usuario hacia su puerta de enlace a través de la interfaz gtp0.

Realizado por: (Henry Yugsin, 2022)

Ahora analizaremos el trafico ICMP del usuario hacia el internet, como se puede observar en la figura 8-3 el tráfico del usuario esta encapsulado con el protocolo GPRS, ya que caso contrario este tráfico no podría circular a través de la red 4G. Otro dato a recalcar es que el protocolo GPRS se encapsula en UDP tal como se detalló en la revisión bibliográfica de las redes 4G en el capítulo I y además para el protocolo UDP se utilizando el puerto 2152 el mismo que se configuro para cada una de las entidades en el capítulo II.

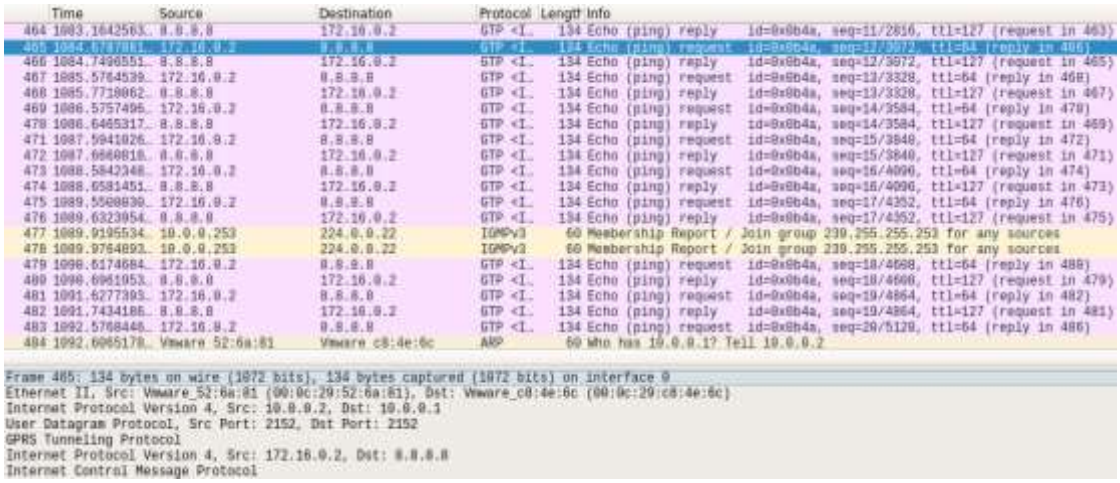


Figura 8-3: Flujo de paquetes IP del usuario hacia Internet

Realizado por: (Henry Yugsin, 2022)

Después el trafico pasa a través de la interfaz gtp0 la cual es la encargada de la conectividad con la entidad S-GW, en la figura 9-3 se puede apreciar como fluye el tráfico del usuario hacia el internet a través de la interfaz gtp0.

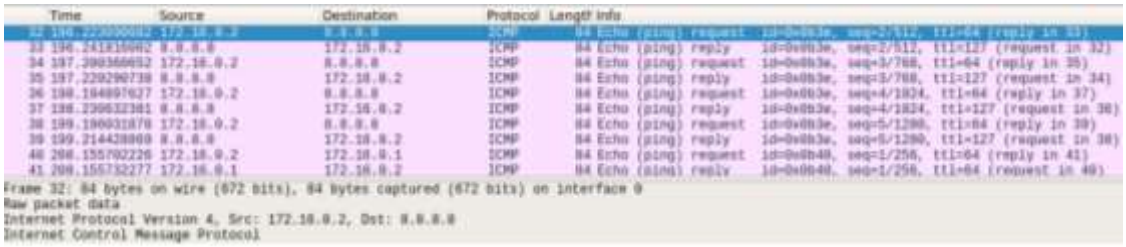


Figura 9-3: Flujo de paquetes IP del usuario hacia Internet a través de la interfaz gtp0

Realizado por: (Henry Yugsin, 2022)

Ya por último la entidad P-GW que es la entidad encargada de conectar a la red 4G con redes 3GPP y redes no 3GPP como internet, esta entidad realiza la acción de NAT para que el usuario de la red LTE sea reconocido por las redes externas. Tal y como se puede observar en la figura 10-3 la dirección IP del usuario se le ha aplicado NAT y ahora es la IP de nuestra máquina virtual.

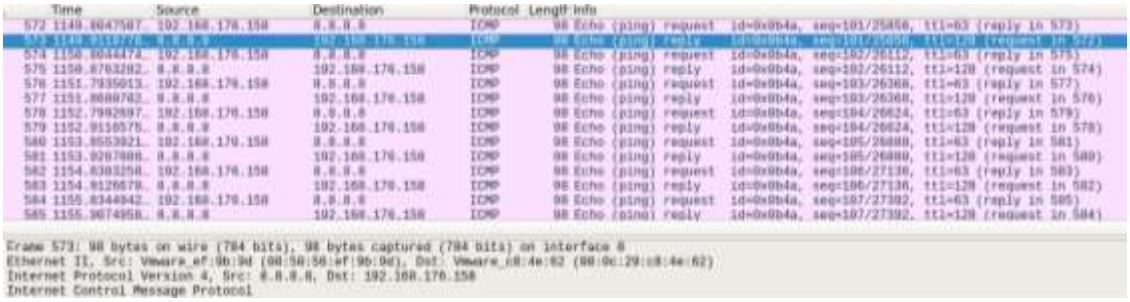


Figura 10-3: Flujo de paquetes IP del usuario hacia Internet

Realizado por: (Henry Yugsin, 2022)

3.2 Esquema EPC-eNB con equipo SDR

En este apartado se detallará y analizará los resultados obtenidos de la simulación de la red LTE con el equipo SDR, el cual corresponde al escenario de implementación número 2 que se especifica en el capítulo 2. Para ello se utilizará el analizador de espectro E8600B el cual sirve para analizar los canales de transmisión de LTE-FDD. Para poder verificar que la implementación del escenario número 2 se ha dado con éxito se debe:

- Comprobar la correcta conexión eNB-EPC-SDR
- Analizar el canal downlink del eNB y así verificar que dicho canal este habilitado para la transmisión/recepción de datos.

A continuación, en la Figura 11-3 se muestra la implementación de este escenario con todos los equipos y materiales requeridos, el mismo que fue realizado en el laboratorio de comunicaciones de la FIE.

Figura 11-3: Fotografía de la Implementación del Escenario 2

Realizado por: (Henry Yugsin, 2022)

3.2.1 Comprobación de conectividad eNB-EPC-SDR

Para comprobar que nuestra entidad eNB se ha conectado exitosamente a la central EPC, utilizaremos wireshark y así podemos observar los paquetes transmitidos durante el proceso de conexión y autenticación. En la figura 12-3 se puede apreciar la cantidad de paquetes que se intercambiaron entre el eNB y EPC para que se conecten sin ningún inconveniente. El paquete número 179 indica que la autenticación ha sido exitosa y que la entidad eNB ya puede acceder a los recursos de la central LTE, este proceso no es muy complejo ya que aquí se intercambian parámetros básicos de autenticación como el MCC, MNC y TAI, mismos parámetros que fueron configurados en las secciones 2.2.4.2 y 2.2.4.1.2 respectivamente. Todo este proceso de

autenticación se realiza con la ayuda del protocolo SCTP, mientras que para la habilitación de canales para el usuario se utiliza el protocolo S1AP, de igual manera en la figura 12-3 se puede apreciar cómo se habilita la utilización del protocolo S1AP entre el eNB y el núcleo de la red LTE.

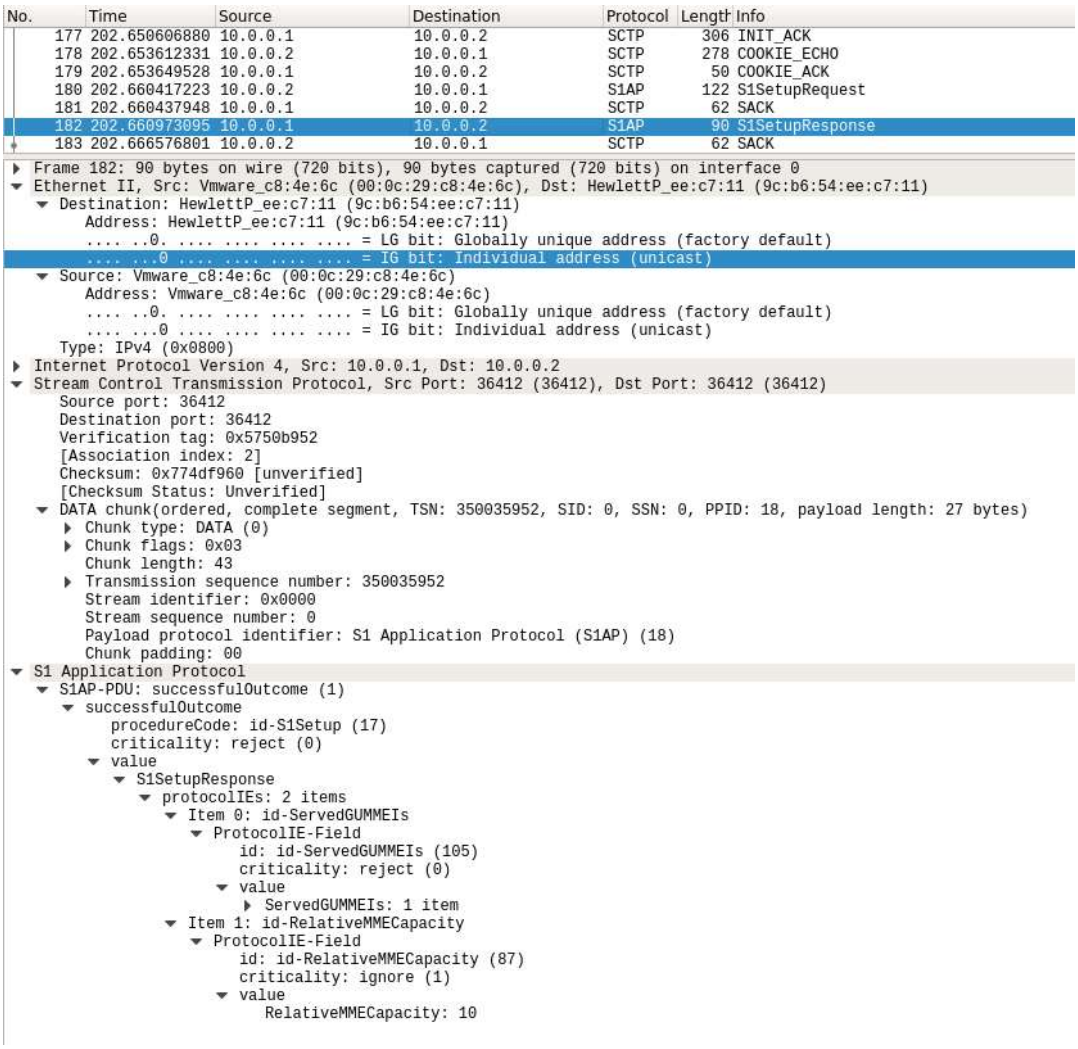


Figura 12-3: Autenticación eNB-EPC

Realizado por: (Henry Yugsin, 2022)

La conectividad con el equipo SDR (USRPB210) es parte fundamental en este escenario ya que la utilización de este equipo nos ayudara a implementar de una manera física la transmisión de datos por parte de la entidad eNB. Para ello se debe comprobar que nuestro equipo SDR (USRPB210) esté conectada a un puerto USB 3.0 de nuestra maquina eNB (Computadora con el software openairinterface5g). Posterior al proceso de autenticación del eNB con EPC en la ventana de comandos se podrá apreciar como la entidad eNB se conecta al equipo SDR y posteriormente carga las configuraciones a la USRPB210 para que este empiece a transmitir/recibir datos, realizando así la transmisión física de datos LTE por parte de la entidad

eNB. En la figura 13-3 se puede apreciar que la conexión entre el eNB y la USRPB210 fue exitosa. Por ende, nuestra entidad eNB está lista para la transmisión/recepción de datos de manera física (mediante la interfaz aire) lo mismo que será analizado a detalle a continuación.

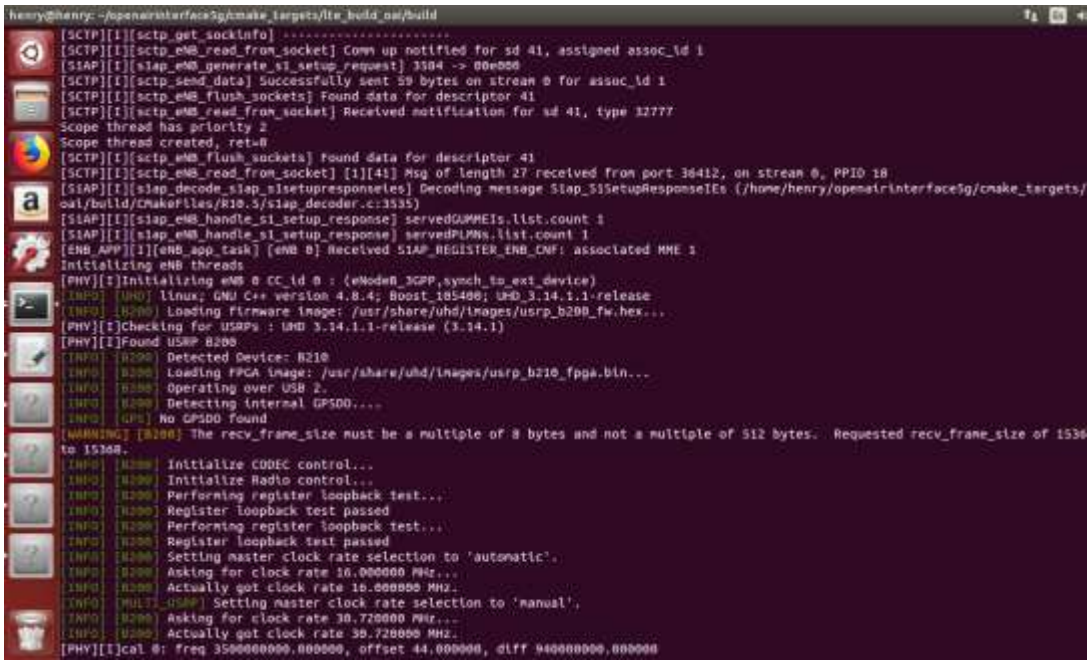


Figura 13-3: Conectividad eNB con equipo SDR (USRPB210)

Realizado por: (Henry Yugsin, 2022)

3.2.2 Análisis de canal uplink con Analizador de Espectro LTE

En este apartado se analizará los resultados obtenidos al medir nuestra red LTE con el analizador de espectros E8600B. Para la medición de los datos el analizador E8600B se colocó a 3m de distancia de la USRPB210 (equipo eNB) con una línea de vista directa tal y como se puede apreciar en la figura 14-3.

Figura 14-3: Escenario 2 con equipo de medición

Realizado por: (Henry Yugsin, 2022)

En la figura 15-3 podemos observar la frecuencia de transmisión de nuestro eNB la misma que tiene una frecuencia central de 2.68 GHz con una potencia de 50 dBm, este parámetro de potencia

es el primer indicador de que nuestra señal del eNB se está transmitiendo con éxito y en la banda de frecuencia establecidas en los archivos de configuración.

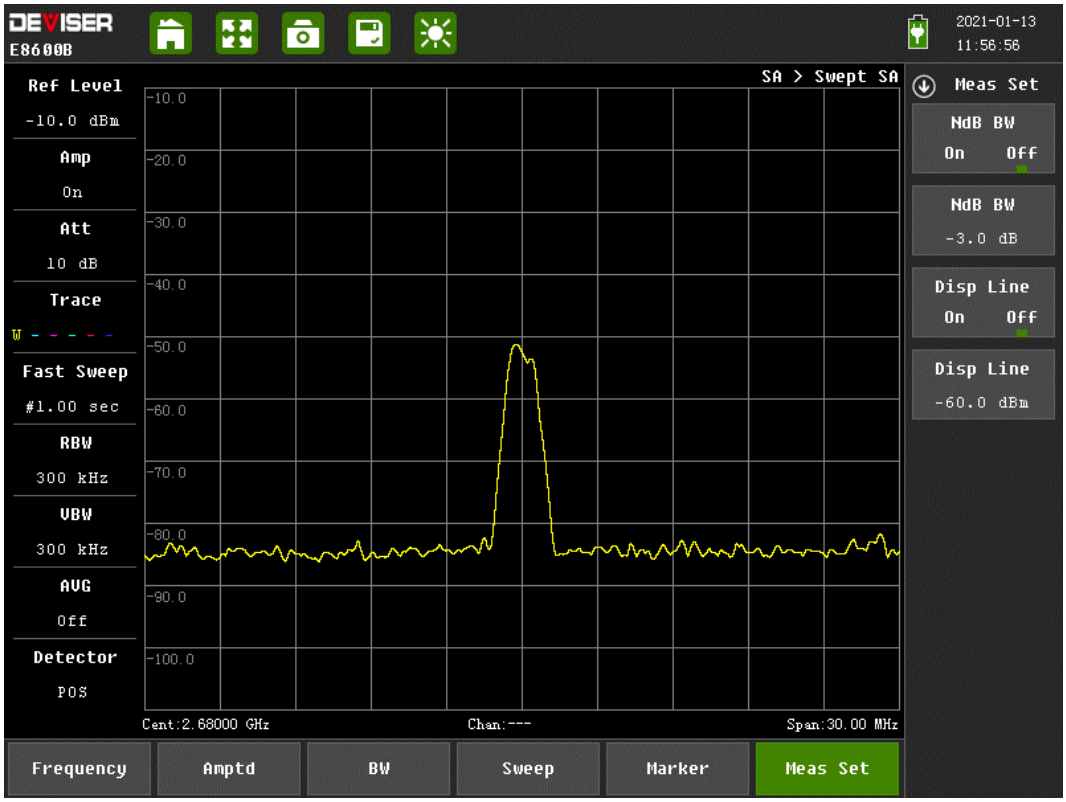


Figura 15-3: Frecuencia central de eNB

Autor: (Henry Yugsin, 2022)

Como segundo parámetro a analizar tenemos el ancho de banda BW, este ancho de banda puede variar en LTE (1.4MHz, 3MHz, 5MHz, 10MHz, 15MHz, 20MHz) dependiendo de la ocupación del mismo (cantidad de trafico), en este caso la ocupación del canal es mínimo ya que no existe ningún usuario conectado a nuestra red, el ancho de banda por defecto será 1.4 MHz. En la figura 16-3 podemos apreciar que nuestro canal LTE con una frecuencia central de 2.68GHz y una potencia de -60 dBm cuenta con un ancho de banda de 1.4MHz tal y como lo habíamos mencionado anteriormente.

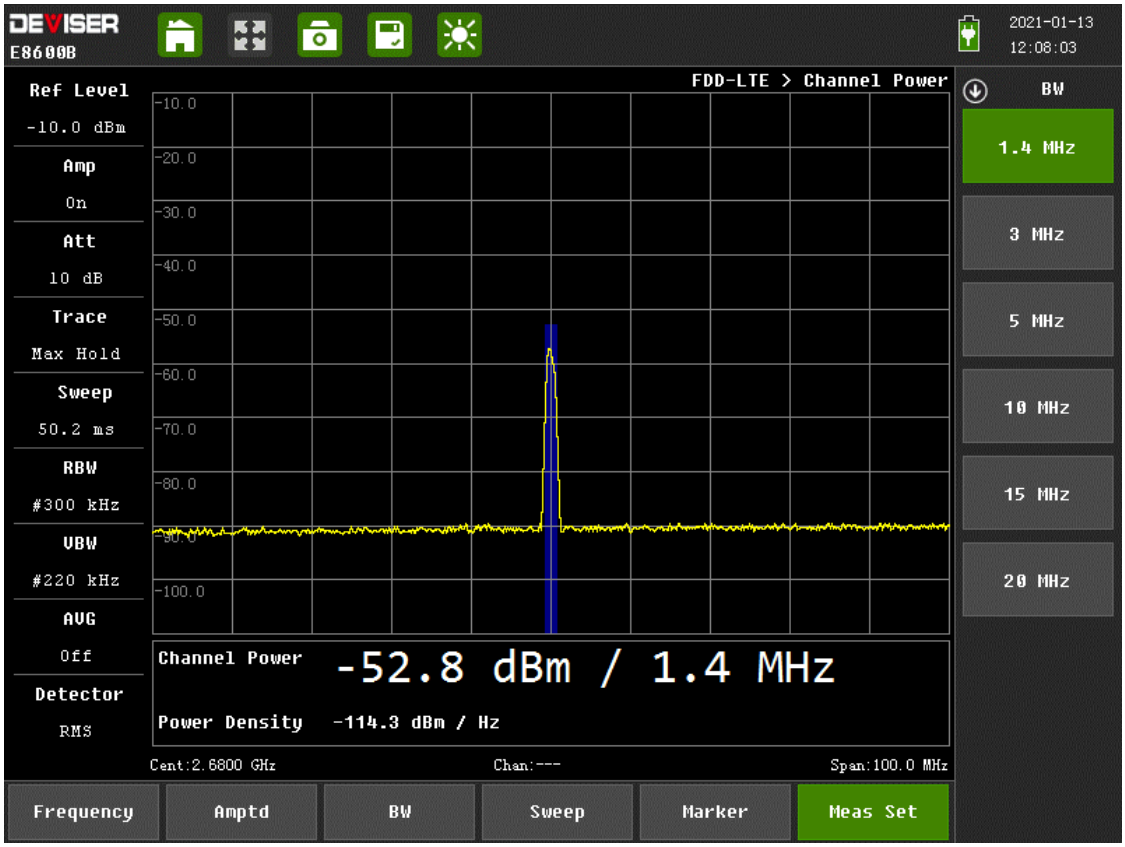


Figura 16-3: Ancho de banda utilizado por eNB

Autor: (Henry Yugsin, 2022)

En la figura 17-3 se puede observar las tramas emitidas por el eNB, estas tramas son paquetes de datos que se transmiten en cada slot asignado en el modo FDD, de igual manera se puede apreciar la cantidad de tramas en la frecuencia central 2.68 GHz y con el ancho de banda 1.4 MHz que son los correspondientes para el eNB. Estas tramas están emitiendo señales de control del eNB (señales utilizadas por un UE para poder conectarse a la red) las mismas que tienen una potencia alrededor de -70 dBm.

Figura 17-3: Tramas transmitidas por eNB

Autor: (Henry Yugsin, 2022)

Un parámetro que es importante para verificar que el canal LTE esté funcionando correctamente es la imagen de la constelación utilizada por LTE-FDD. En la figura 18-3 podemos apreciar que nuestro eNB está utilizando una modulación QPSK, cabe recalcar que esta imagen hace referencia a la representación gráfica de la transmisión de bits por medio del canal LTE, en este caso los bits que se aprecian en la figura son bits que llevan información de control del eNB.

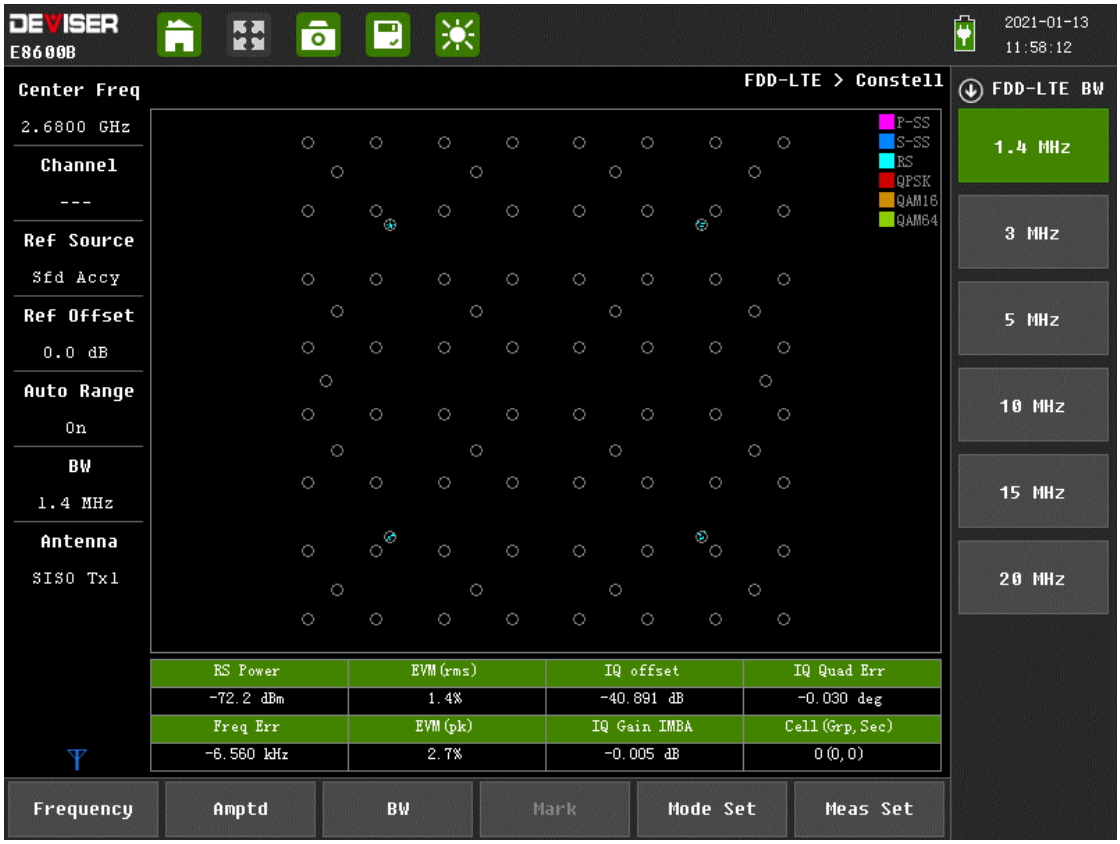


Figura 18-3: Modulación QPSK de eNB

Autor: (Henry Yugsin, 2022)

La relación de potencia de fuga del canal adyacente ACLR es una medida del rendimiento del transmisor que nos indica la potencia de fuga de nuestra señal (canal central) a canales contiguos/adyacentes. Es una medida de control de potencia que se utiliza para verificar que la señal no produzca una interferencia significativa en los canales adyacentes y así evitar inconvenientes en todas las redes LTE. En los estándares de 3GPP TS 36.104 se especifican requisitos mínimos de conformidad de este parámetro en E-UTRAN. En este caso debe tener un ACLR mínimo de -45 dBm. En la figura 19-3 se puede apreciar que nuestro eNB tiene un ACLR de -87.6 dBm por lo que se determina que la estación base esta no está generando interferencia en frecuencias vecinas.

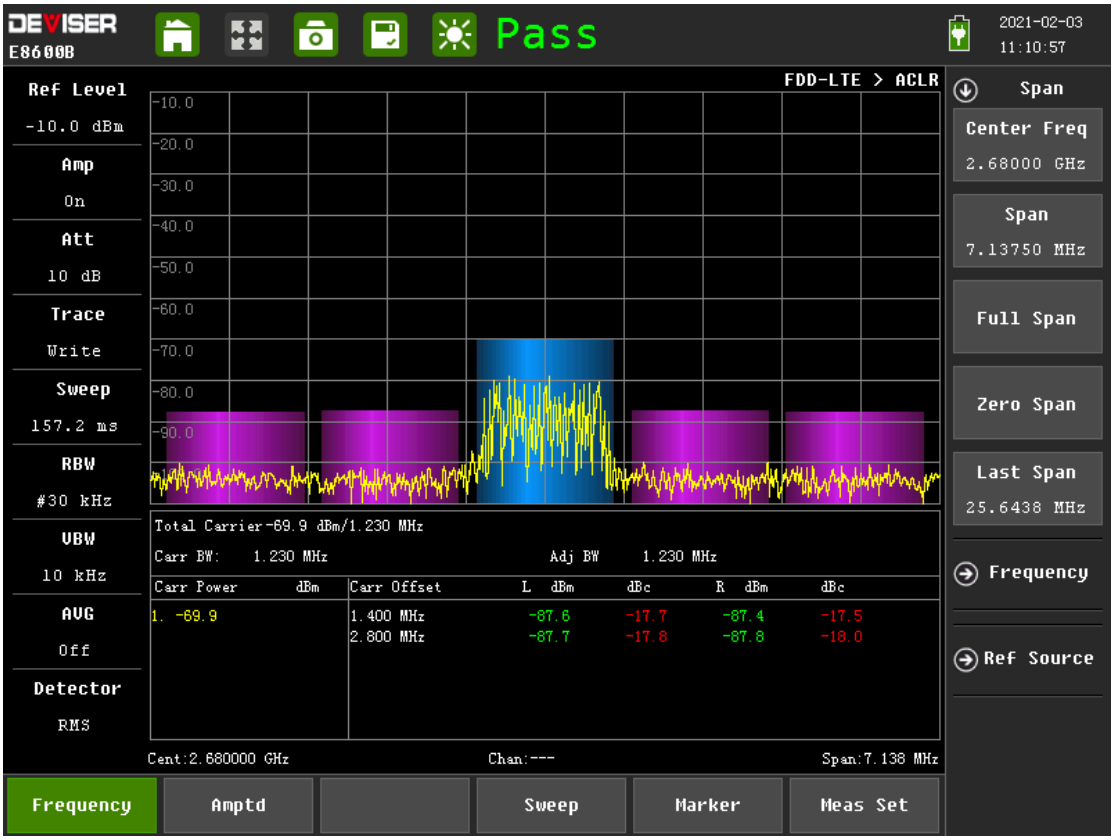


Figura 19-3: ACLR del eNB

Autor: (Henry Yugsin, 2022)

Siguiendo con el análisis del canal downlink del eNB en la figura 20-3 podemos apreciar la potencia con la que llegan cada una de las señales físicas y canales físicos de downlink. Tenemos tres señales físicas las cuales transportan información necesaria para la sincronización temporal de la célula servidora y estimación del canal. La primera llamada PSS (Primary Synchronization Signal) se transmite dos veces por trama, en el último símbolo-OFDM de los slots 0 y 10, sirve para identificar la temporización, el centro de la banda, y la identidad de la célula (una de las tres) dentro del grupo de identidades, vemos que esta tiene una potencia de -75.4 dBm. La segunda señal física es SSS (Secondary Synchronization Signal) se transmite dos veces por trama en el penúltimo símbolo OFDM de los slots 0 y 10 y en las mismas subportadoras que la PSS, sirve para identificar el grupo de identidades de célula, de los 168 posibles, vemos que esta señal llega con una potencia de -75.4 dBm. La tercera señal es RS (Reference signal) realiza la estimación función de transferencia del canal DL, la transmisión de estas señales identifica los puertos de antena, una vez adquirida la sincronización mediante las señales PSS y SSS, el UE puede evaluar la respuesta del canal, amplitud y fase, mediante las Reference Signals (RS) para esta señal tenemos una potencia de -101.1 dBm. Del mismo modo podemos analizar dos canales físicos de DL. El primer canal se llama PBCH (Physical Broadcast CHannel) este transporta en el llamado Master Information Block, MIB, la información básica del sistema: identificación de la red,

bandas de operación, longitud del prefijo cíclico, configuración MIMO, se transmite en las 72 subportadoras centrales y ocupa una modulación QPSK este canal tiene una potencia de -74.9 dBm. El otro canal es el PCFICH (Physical Control Format Indicator Channel) este indica el número de símbolos (formato) del PDCCH en la subtrama y se transmite en los mismos puertos que PBCH, este canal llega con una potencia de -81.4 dBm. La potencia que tiene cada uno de los canales es buena y suficiente para que un equipo de usuario pueda interpretar correctamente la información que lleva consigo todas estas señales y canales físicos.

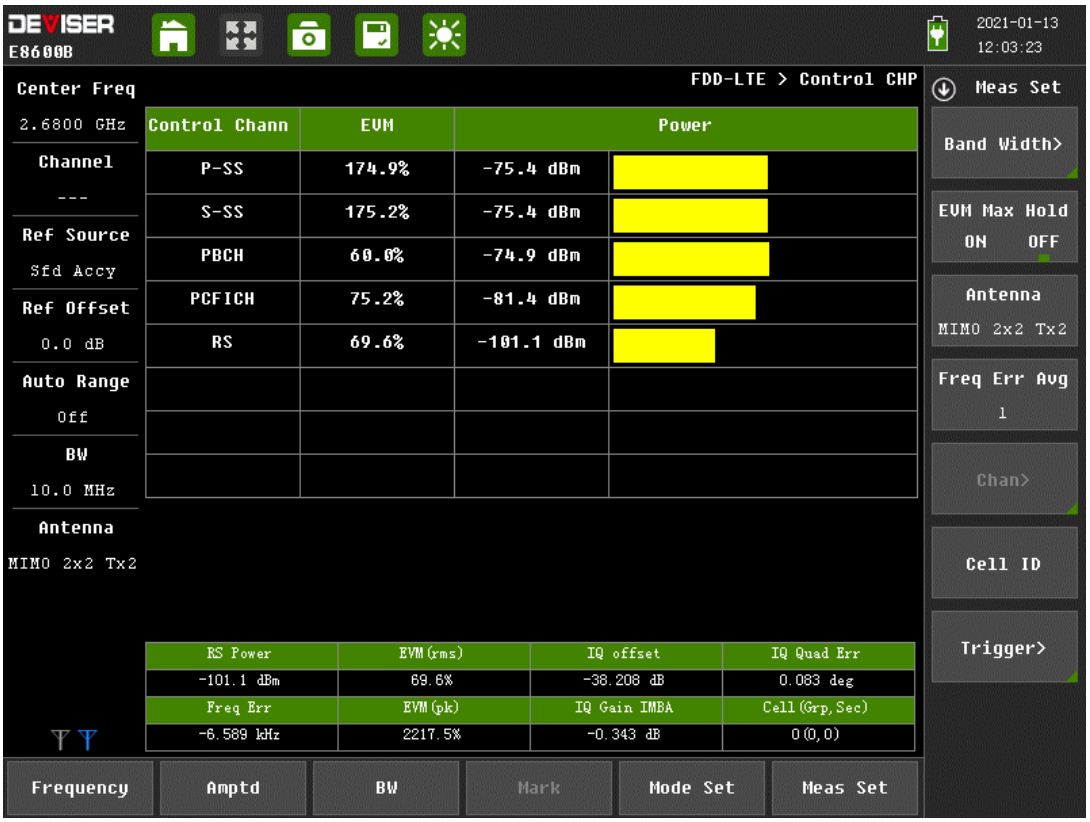


Figura 20-3: Control CHP del eNB

Autor: (Henry Yugsin, 2022)

La ocupación del ancho de banda en nuestra red es un parámetro que también se puede medir, tal y como se observa en la figura 21-3, la cual nos indica que el ancho de banda está disponible en un 99%, se tiene un ancho de banda real de 1.368 MHz con una potencia promedio de -54.5 dBm en la frecuencia central de 2.68 GHz.

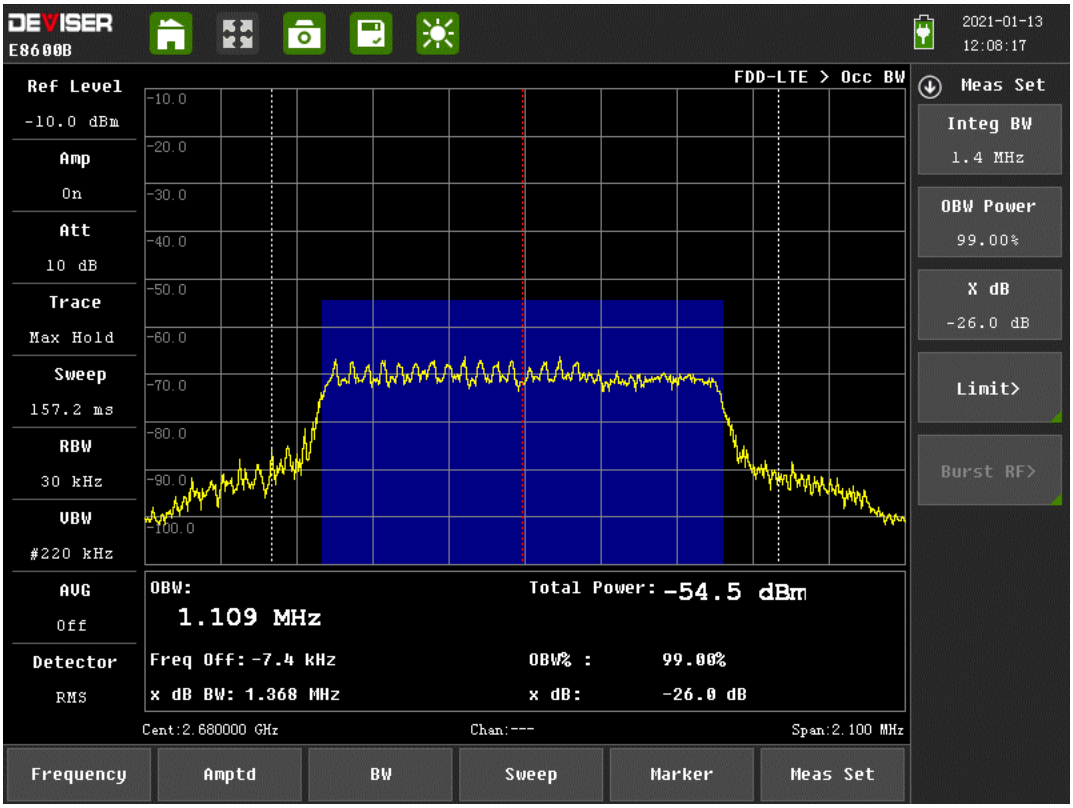


Figura 21-3: Ocupación del Ancho de Banda de eNB

Autor: (Henry Yugsin, 2022)

Todos estos resultados obtenidos al analizar el canal downlink de la parte E-UTRAN con el analizador de espectro de LTE-FDD indica que la entidad eNB está funcionando correctamente a la espera de un equipo de usuario UE.

CONCLUSIONES

Analizado el estado del arte de las redes móviles 4G se puede concluir que desde la aparición del primer estándar para LTE en el año 2008, la tecnología LTE se ha desarrollado y actualizado para cubrir la creciente demanda de las redes de comunicaciones móviles 4G y posteriormente para una coexistencia con redes móviles 5G. La tecnología LTE empieza con el Release 8 de 3GPP el cual tiene dos características principales, las redes pasan a ser totalmente IP y se distingue de una manera clara la parte de acceso radio y la parte del núcleo de la red, esto fue un avance significativo para el desarrollo de los nuevos sistemas de comunicaciones móviles ya que abre diferentes posibilidades como la interconectividad y la flexibilidad. El release 9 presenta algunas mejoras pero el siguiente punto de inflexión se observa en el release 10 de LTE el cual es el primero en cumplir todos los requisitos de una red 4G, en esta tecnología existen grandes diferencias en cuanto a capacidades con sus predecesoras reléase 8 y 9, con un incremento a 3 Gbps DL e 1,5 Gbps UL y diversas mejoras más, el release 10 de 3GPP es la primera tecnología 4G. Debido al exponencial crecimiento de la demanda de trafico de los usuarios la tecnología 4G sufrió mejoras constantes es por ello que se da el release 11 el cual tiene como principal característica que introdujo la comunicación multipunto cooperativa, en el release 12 se buscó aumentar la capacidad con células pequeñas, en el release 13 el satisfacer la creciente demanda de rendimiento fue su principal objetivo y el siguiente punto de inflexión se da en el release 14. El release 14 marca el inicio de la estandarización de 5G pero aun con la coexistencia con la red 4G, aquí se estandariza una nueva tecnología de acceso radio y se define parámetros importantes como una baja latencia, MIMO masivo entre otras. Después de esto se desarrolla el release 15 el cual define dos arquitecturas importantes como el Non-Stand-Alone ‘NSA’ y Stand-Alone ‘SA’, el NSA se basa en una central 4G como el EPC en el mismo que se agrega algunas mejoras. Posteriormente se desarrollan releases 16,17 y 18 los cuales ya son orientados completamente hacia las redes 5G. Una tecnología importante que nace en cuanto al crecimiento de las redes 4G y 5G es el de la virtualización de funciones de red, la cual brinda mejoras sobretodo en cuanto a costos de operación, flexibilidad y escalabilidad, aspectos importantes que han hecho que la tecnología de virtualización vaya tomando más fuerza al momento de desarrollar las redes de comunicaciones móviles actuales y futuras.

Existen diferentes herramientas de software ya sea de código abierto o código cerrado que sirven para la virtualización de funciones de redes móviles 4G, cada uno con características y capacidades diferentes, pero con el mismo objetivo. El software de código abierto OpenAirInterface tiene grandes ventajas como la implementación de los releases 8,10 y 14, capacidad de software para las entidades EPC, eNB y UE, software de código abierto y la compatibilidad con múltiples plataformas SDR. Otro aspecto que resulto muy útil fue que el

software y su entidad propietaria proporciona material de apoyo como tutoriales para la descarga e implementación de dicho software. En conclusión, esta herramienta de software resulta ideal para la virtualización de sistemas de comunicaciones móviles 4G.

La implementación del software para la virtualización de funciones de red 4G resulto exitosa, se pudo virtualizar la central 4G denominada EPC la cual contiene las principales entidades como HSS, MME, S-GW y P-GW. También se virtualizo con éxito la entidad eNB y un equipo de usuario UE, además de la utilización del equipo SDR específicamente la USRPB210.Siguiendo los pasos indicados en la página oficial de la entidad propietaria del software OpenAirInterface se instaló, configuro y ejecuto las entidades antes mencionadas con éxito. La utilización del sistema operativo Ubuntu en su versión 16 LTS resulta ser el indicado para el correcto funcionamiento de la central EPC, mientras que la utilización del sistema operativo Ubuntu en su versión 14 LTS resulta ser la indicada para las entidades eNB y UE, esto se debe principalmente a los requerimientos del propio software OpenAirInterface.

Las pruebas de conectividad desarrolladas en el capítulo III tuvieron como resultado la conectividad del usuario virtual a redes 3GPP (LTE) y redes no 3GPP (Internet), así también el análisis del canal downlink del eNB con el equipo SDR resulto en la correcta transmisión de las señales de control por parte de la entidad eNB mediante una interfaz aire. Para el escenario 1 la correcta conectividad del equipo de usuario virtual UE se comprobó con pruebas de ping a través de la interfaz del usuario oip1 hacia la propia red LTE y hacia el Internet, estas dieron como resultado paquetes ICMP Request e ICMP Reply con una latencia media de 118 ms y un TTL de 64 hacia la puerta de enlace de la central 4G, en cambio con una latencia media de 132 ms y un TTL de 127 hacia el internet, con esto se comprueba la funcionalidad del escenario 1. Para el escenario 2 se utilizó el analizador de espectro E8600B en el cual se comprobó la transmisión de la señal LTE del eNB en el canal downlink a una frecuencia de 2.68 GHz, un ancho de banda 1.4 MHz con potencia de canal de -52.8 dBm, una modulación QPSK, las potencias en los canales de control fueron en PBCH -74.9 dBm, en PCFICH -81.4 dBm, para las señales de control se tuvo en P-SS -75.4 dBm, S-SS -75.4 dBm, RS -101,1 dBm, y un valor de ACLR de -87.6 dBm el cual indica que no genera interferencia en frecuencias vecinas, todos estos valores nos indica que el canal downlink está funcionando correctamente por lo cual se concluye la correcta funcionalidad del escenario 2. Con todas estas pruebas se puede concluir que las implementaciones de los dos escenarios propuestos para el desarrollo de este trabajo de titulación resultaron ser exitosas.

RECOMENDACIONES

Para tener una idea clara del funcionamiento de las redes 4G se recomienda analizar el estado del arte de las mismas, investigar acerca de su estructura, sus interfaces de conexión y los protocolos que utilizan para su comunicación, esta es una parte muy importante que así se puede identificar errores y soluciones al momento de desarrollar los escenarios de virtualización. De igual manera se recomienda que toda la información recopilada sea de fuentes verificadas como libros, artículos científicos, pero sobretodo del mismo estándar de 3GPP ya que ahí se puede encontrar toda la información referente a las comunicaciones móviles 4G.

Al momento de indagar sobre la instalación, configuración y ejecución del software OpenAirInterface se recomienda guiarse en fuentes oficiales ya que así se tendrá certeza de que los pasos a seguir son los correctos. De igual manera se recomienda la utilización del software VMWare para la virtualización del sistema operativo Ubuntu ya que este resulta funcionar muy buen para la administración de capacidades de hardware. La utilización de dos computadoras resulta útil para en una de ellas virtualizar la entidad conocida como EPC y en la otra las entidades eNB o UE por lo que se recomienda la utilización de dos computadoras para que así las implementaciones, configuraciones y compilaciones resulten más sencillas y se puedan realizar independientemente una de otra. De igual manera se recomienda que en la maquina a virtualizar la entidad EPC se tenga como mínimo dos tarjetas de red ya que son necesarias para la implementación de cada uno de los escenarios.

Para la utilización del equipo SDR se recomienda que la conectividad sea mediante un USB 3.0 ya que así el equipo en conjunto con el software funcionara de una manera adecuada. De igual manera se recomienda revisar la correcta funcionalidad del equipo SDR mediante GNU ya que así se puede descartar diversos problemas futuros. Para la conectividad con la antena se debe utilizar un conector a 50 ohmios y se debe revisar que la antena trabaje dentro del rango de frecuencia de las bandas LTE. En configuraciones se recomienda utilizar la configuración en modo FDD-LTE ya que es la más utilizada, de igual forma se recomienda trabajar en una banda LTE con menor congestión posible ya que así no se tendrá problemas de interferencia, un parámetro importante es la ganancia de las antenas el cual se recomienda dejar el valor por defecto de los mismos ya que son los más óptimos para la utilización con equipos SDR.

Para trabajos futuros se recomienda tomar en cuenta la participación de SDN en la virtualización de funciones de red ya que son tecnologías que se complementan mutuamente y están diseñadas para funcionar en conjunto, mejorando así el rendimiento general de la red.

BIBLIOGRAFÍA

Abdrabou, Mohammed Aly; et al. "LTE authentication protocol (EPS-AKA) weaknesses solution". *En 2015 IEEE seventh international conference on intelligent computing and information systems (ICICIS)* [En línea], 2015, pp. 434-441. [Consulta: 20 agosto 2009]. Disponible en: https://ieeexplore.ieee.org/document/7397256

Amarisoft. *AMARI LTE 100 Software suite solutions* [blog]. 2018. [Consulta: 29 diciembre 2021]. Disponible en: https://www.amarisoft.com/software-enb-epc-ue-simulator/

Becvar, Zdenek; et al. *Redes móviles*. Redes móviles, 2013, pp. 11-12.

Comes, R. Agusti, et al. *LTE: Nuevas tendencias en comunicaciones móviles*. Fundación Vodafone España, 2010, pp. 55-302.

Dahlman, Erik; et al. *4G: LTE/LTE-advanced for mobile broadband*. Academic press, 2013.

ERICSSON. *Ericsson Mobility Report Inf tec* [En línea], 2020. [Consulta: 20 octubre 2021]. Disponible en: https://www.ericsson.com/en/mobility-report/reports/june-2020

ERICSSON. *5G EVOLUTION TOWARD 5G ADVANCED: An overview of 3GPP releases 17 and 18.* [En linea], 2021. [Consulta: 01 febrero 2022]. Disponible en: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-evolution-toward-5g-advanced

ETSI, GSNFV. *Network functions virtualisation (nfv): Architectural framework* [En linea]. ETsI Gs NFV, 2013. [Consulta: 20 octubre 2021]. Disponible en: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf

ETTUS. *USRP B210* [blog]. [Consulta: 30 noviembre 2021]. Disponible en: https://www.ettus.com/all-products/ub210-kit/

Firmin, F. *The Evolved Packet Core* [blog]. [Consulta: 25 diciembre 2021]. Disponible en: https://www.3gpp.org

Gualda Muñoz, Javier. Estudio de la arquitectura de protocolos de LTE [En línea] (Trabajo de titulación). Universidad Politécnica de Cataluña, Barcelona, España. 2016. pp. 39-47. [Consulta: 2021-12-20]. Disponible en: http://hdl.handle.net/2117/98231

García Algora, Carlos Manuel. Radio Definido por Software usando MATLAB. [En línea] (Trabajo de titulación). (Doctoral) Universidad Central " Marta Abreu" de Las Villas, Cuba. 2011. pp. 4-10. [Consulta: 2021-12-18]. Disponible en: https://dspace.uclv.edu.cu/handle/123456789/4729

INTEL, Brocade, Cyan, Red Hat, Telefónica. Implementación de la virtualización de funciones de red optimizada global. [En línea]. 2021. [Consulta: 15 noviembre 2021]. Disponible

en: intel.la/content/dam/www/public/lar/xl/es/documents/white-papers/end-to-end-optimized-nfv-paper-spa.pdf

IETF RFC4960, *Stream Control Transmission Protocol*. [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://datatracker.ietf.org/doc/html/rfc4960

IETF RFC 3588, *Diameter Base Protocol.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://datatracker.ietf.org/doc/html/rfc3588

IETF RFC 4005, *Diameter Network Access Server Application.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://datatracker.ietf.org/doc/html/rfc4005

IETF RFC 4006, *Diameter Credit-Control Application.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://datatracker.ietf.org/doc/html/rfc4006

Jiménez, Carlos Alberto Serra; & Rizo, Francisco Reinerio Marante. "Arquitectura general del sistema LTE". *Telemática* [En línea], 2013, vol. 12, pp. 81-90. [Consulta: 20 octubre 2021]. Disponible en: https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/106

Jaeger, Bernd. "Security orchestrator: Introducing a security orchestrator in the context of the etsi nfv reference architecture". *En 2015 IEEE Trustcom/BigDataSE/ISPA* [En línea], 2015. pp. 1255-1260. [Consulta: 25 octubre 2021]. Disponible en: https://ieeexplore.ieee.org/document/7345422

Koodli, Rajeev S.; Perkins, Charles E. *Mobile Inter-networking with IPv6: Concepts, principles and practices.* John Wiley & Sons, 2007, pp. 19-25.

Kaaranen, Heikki, et al. *UMTS networks: architecture, mobility and services*. John Wiley & Sons, 2005, pp. 47-68.

Loza Valenzuela, Pablo Ignacio. Diseño y trial test de un sistema de monitoreo sobre el Evolved Packet Core virtualizado. [En línea] (Trabajo de titulación). Universidad de Chile, Santiago de Chile, Chile. 2019. pp. 14-35. [Consulta: 2021-11-06]. Disponible en: https://repositorio.uchile.cl/handle/2250/170763

Mckeown, Nick, et al. "OpenFlow: enabling innovation in campus networks". *ACM SIGCOMM computer communication review* [En línea], 2008, vol. 38, pp. 69-74. [Consulta: 12 noviembre 2021]. Disponible en: https://www.sigcomm.org/publications/computer-communication-review

Markus, M. Lynne; Robey, Daniel. "Information technology and organizational change: Causal structure in theory and research". *Management science* [En línea], 1988, vol. 34, pp. 583-598. [Consulta: 14 noviembre 2021]. Disponible en: https://www.jstor.org/stable/2632080

Moya, José Manuel Huidobro. *Comunicaciones Móviles. Sistemas GSM, UMTS y LTE*. Grupo Editorial RA-MA, 2013, pp. 54-59.

Morfa, Camilo Nuñez. "Protocolos de usuario en E-UTRAN". *Telemática* [En línea], 2013, vol. 12, pp. 32-40. [Consulta: 18 noviembre 2021]. Disponible en: https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/117/113

Mendoza Garcia, Jesus Deymer. Estudio del estado del arte de la telefonía móvil [En línea] (Trabajo de titulación). Universidad Nacional de Piura, Piura, Perú. 2019. pp. 71-108. [Consulta: 2021-12-02]. Disponible en: https://repositorio.unp.edu.pe/handle/UNP/1756

Olsson, Magnus, et al. *SAE and the Evolved Packet Core: Driving the mobile broadband revolution*. Academic Press, 2009, pp. 37-49.

OpenAirInterface. OpenAirInterface 5G software Alliance for democratising Wireless innovation. [En línea]. 2018. [Consulta: 29 diciembre 2021]. Disponible en: http://www.openairinterface.org/

Pérez Trigo, Javier, et al. *Introducción a los sistemas móviles de comunicaciones* [En línea]. Ediciones Universidad de Salamanca, 2019. [Consulta: 20 noviembre 2021]. Disponible en: https://gredos.usal.es/bitstream/handle/10366/139636/BISITE_P%c3%a9rezTrigoJ_Sistemasm%c3%b3viles.pdf?sequence=1&isAllowed=y

Peñuelas, Jorge Cabrejas, et al. *3GPP LTE: Hacia la 4G móvil*. Marcombo, 2012, pp. 124-137.

Paulino Johnson, Gabriel Enrique. Planificación de una red de cuarta generación móvil LTE en la Región de Murcia con la herramienta Radiogis [En línea] (Trabajo de titulación). (Maestría) Universidad Politécnica de Cartagena, Murcia, España. 2013. pp. 10-23. [Consulta: 2021-11-04]. Disponible en: https://repositorio.upct.es/handle/10317/3760

Remy, Jean-Gabriel; Letamendia, Charlotte. *LTE standards and architecture*. LTE standards, 2014, pp. 1-112.

SRS, Software Radio Systems, "Products". 2018. [En línea]. [Consulta: 29 diciembre 2021]. Disponible en: http://www.softwareradiosystems.com/products/#srslte

Wojtowicz, B. OpenLTE is an open source implementation of the 3GPP LTE specification OpenLTE. 2017. [En línea]. [Consulta: 29 diciembre 2021]. Disponible en: http://openlte.sourceforge.net/

Xiang, Xueyan, et al. Estudio de plataformas SDR para LTE-5G [En línea] (Trabajo de titulación). Universidad de Cantabria, Cantabria, España. 2018. pp. 16-32. [Consulta: 2021-11-04]. Disponible en: https://repositorio.unican.es/xmlui/handle/10902/14603

YI, Bo, et al. "A comprehensive survey of network function virtualization". *Computer Networks* [En línea], 2018, vol. 133, pp. 212-262. [Consulta: 05 diciembre 2021]. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S1389128618300306

3GPP, 2019. *Directory Listing.* [En línea]. 2015. [Consulta: 11 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/38_series.

3GPP TS 23.008. *Organization of subscriber data.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/23_series/23.008/

3GPP TS 29.061. *Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN).* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/29_series/29.061/

3GPP TS 23.401. *General Packet Radio Service (GPRS).* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/23_series/23.401/

3GPP TS 23.402. *Architecture enhancements for non-3GPP accesses.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/23_series/23.402/

3GPP TS 29.274. *3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3*. [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/29_series/29.274/

3GPP TS 23.275. *Proxy Mobile IPv6 (PMIPv6) protocolos de túneles y movilidad basados; Etapa 3.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/23_series/23.725/

3GPP 36.401. *Red Universal de Acceso Radio Terrestre Evolucionada (E-UTRAN); Descripción de la arquitectura*. [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/36_series/36.401/

3GPP TS 29.272. *Sistema de paquetes evolucionado (EPS); Interfaces relacionadas con la Entidad de gestión de movilidad (MME) y el Nodo de soporte de servicio GPRS (SGSN) basadas en el protocolo Diameter*. [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/29_series/29.272/

3GPP TS 36.410. *S1 General Aspects and Principles.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/36_series/36.410/

3GPP TS 36.420. *X2 General Aspects and Principles.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/36_series/36.420/

3GPP TS 36.413. *S1 Protocol Specification.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/36_series/36.413/

3GPP TS 36.423. *X2 Protocol Specifiation.* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/36_series/36.423/

3GPP TS 29.281. *General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U).* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/29_series/29.281/

3GPP TS 31.102. *Características de la Aplicación del Módulo de Identidad de Suscriptor Universal (USIM)*. [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/31_series/31.102/

3GPP TS 27.007. *AT command set for User Equipment (UE).* [En línea]. 2015. [Consulta: 15 noviembre 2021]. Disponible en: https://www.3gpp.org/ftp/Specs/archive/27_series/27.007/

3GPP. *Release 18*. [En línea]. 2022. [Consulta: 01 febrero 2022]. Disponible en: https://www.3gpp.org/specifications/releases/72-release-8

3GPP. *Release 10*. [En línea]. 2013. [Consulta: 01 febrero 2022]. Disponible en: https://www.3gpp.org/specifications/releases/70-release-10

3GPP. *Release 15*. [En línea]. 2019. [Consulta: 01 febrero 2022]. Disponible en: https://www.3gpp.org/release-15#:~:text=After%20initial%20delivery%20in%20late,3GPP%20submission%20towards%20IMT%2D2020.

3GPP. *Release 16*. [En línea]. 2020. [Consulta: 01 febrero 2022]. Disponible en: https://www.3gpp.org/release-16

ANEXOS

ANEXO A: Fichero de configuración de hss.conf

```
################################################################################
# Licensed to the OpenAirInterface (OAI) Software Alliance under one or more
# contributor license agreements.  See the NOTICE file distributed with
# this work for additional information regarding copyright ownership.
# The OpenAirInterface Software Alliance licenses this file to You under
# the Apache License, Version 2.0  (the "License"); you may not use this file
# except in compliance with the License.
# You may obtain a copy of the License at
# http://www.apache.org/licenses/LICENSE-2.0
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
# For more information about the OpenAirInterface (OAI) Software Alliance:
#      contact@openairinterface.org
################################################################################
HSS :
{
## MySQL mandatory options
MYSQL_server = "127.0.0.1";     # HSS S6a bind address
MYSQL_user   = "root";  # Database server login
MYSQL_pass   = "root";  # Database server password
MYSQL_db     = "oai_db";        # Your database name
## HSS options
#OPERATOR_key = "1006020f0a478bf6b699f15c062e42b3"; # OP key matching your database
OPERATOR_key = "11111111111111111111111111111111"; # OP key matching your database
RANDOM = "true";                        # True random or only pseudo random (for subscriber
vector generation)
## Freediameter options
FD_conf = "/usr/local/etc/oai/freeDiameter/hss_fd.conf";
};
```

ANEXO B: Fichero de configuración de hss_fd.conf

```
# -------- Local ---------
# The first parameter in this section is Identity, which will be used to
# identify this peer in the Diameter network. The Diameter protocol mandates
# that the Identity used is a valid FQDN for the peer. This parameter can be
# omitted, in that case the framework will attempt to use system default value
# (as returned by hostname --fqdn).
Identity = "hss.openair4G.eur";
# In Diameter, all peers also belong to a Realm. If the realm is not specified,
# the framework uses the part of the Identity after the first dot.
Realm = "openair4G.eur";
# This parameter is mandatory, even if it is possible to disable TLS for peers
# connections. A valid certificate for this Diameter Identity is expected.
TLS_Cred = "/usr/local/etc/oai/freeDiameter/hss.cert.pem",
"/usr/local/etc/oai/freeDiameter/hss.key.pem";
TLS_CA = "/usr/local/etc/oai/freeDiameter/hss.cacert.pem";
# Disable use of TCP protocol (only listen and connect in SCTP)
# Default : TCP enabled
No_SCTP;
# This option is ignored if freeDiameter is compiled with DISABLE_SCTP option.
# Prefer TCP instead of SCTP for establishing new connections.
# This setting may be overwritten per peer in peer configuration blocs.
# Default : SCTP is attempted first.
Prefer_TCP;
# Disable use of IPv6 addresses (only IP)
# Default : IPv6 enabled
No_IPv6;
# Overwrite the number of SCTP streams. This value should be kept low,
# especially if you are using TLS over SCTP, because it consumes a lot of
# resources in that case. See tickets 19 and 27 for some additional details on
# this.
# Limit the number of SCTP streams
SCTP_streams = 3;
# By default, freeDiameter acts as a Diameter Relay Agent by forwarding all
# messages it cannot handle locally. This parameter disables this behavior.
NoRelay;
```

```
# Use RFC3588 method for TLS protection, where TLS is negociated after CER/CEA exchange is completed
# on the unsecure connection. The alternative is RFC6733 mechanism, where TLS protects also
# CER/CEA exchange on a dedicated secure port.
# This parameter only affects outgoing connections.
# The setting can be also defined per-peer (see Peers configuration section).
# Default: use RFC6733 method with separate port for TLS.
#TLS_old_method;
# Number of parallel threads that will handle incoming application messages.
# This parameter may be deprecated later in favor of a dynamic number of threads
# depending on the load.
AppServThreads = 4;
# Specify the addresses on which to bind the listening server. This must be
# specified if the framework is unable to auto-detect these addresses, or if the
# auto-detected values are incorrect. Note that the list of addresses is sent
# in CER or CEA message, so one should pay attention to this parameter if some
# adresses should be kept hidden.
#ListenOn = "127.0.0.1";
Port = 3868;
SecPort = 5868;
# -------- Extensions ---------
# Uncomment (and create rtd.conf) to specify routing table for this peer.
#LoadExtension = "rt_default.fdx" : "rtd.conf";
# Uncomment (and create acl.conf) to allow incoming connections from other peers.
LoadExtension = "acl_wl.fdx" : "/usr/local/etc/oai/freeDiameter/acl.conf";
# Uncomment to display periodic state information
#LoadExtension = "dbg_monitor.fdx";
# Uncomment to enable an interactive Python interpreter session.
# (see doc/dbg_interactive.py.sample for more information)
#LoadExtension = "dbg_interactive.fdx";
# Load the RFC4005 dictionary objects
#LoadExtension = "dict_nasreq.fdx";
LoadExtension = "dict_nas_mipv6.fdx";
LoadExtension = "dict_s6a.fdx";
# Load RFC4072 dictionary objects
#LoadExtension = "dict_eap.fdx";
# Load the Diameter EAP server extension (requires diameap.conf)
```

```
#LoadExtension = "app_diameap.fdx" : "diameap.conf";
# Load the Accounting Server extension (requires app_acct.conf)
#LoadExtension = "app_acct.fdx" : "app_acct.conf";
# -------- Peers ---------
# The framework will actively attempt to establish and maintain a connection
# with the peers listed here.
# For only accepting incoming connections, see the acl_wl.fx extension.
#ConnectPeer = "ubuntu.localdomain" { ConnectTo = "127.0.0.1"; No_TLS; };
```

ANEXO C: Fichero de configuración de mme.conf

```
################################################################################
# Licensed to the OpenAirInterface (OAI) Software Alliance under one or more
# contributor license agreements.  See the NOTICE file distributed with
# this work for additional information regarding copyright ownership.
# The OpenAirInterface Software Alliance licenses this file to You under
# the Apache License, Version 2.0  (the "License"); you may not use this file
# except in compliance with the License.
# You may obtain a copy of the License at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#-------------------------------------------------------------------------------
# For more information about the OpenAirInterface (OAI) Software Alliance:
#      contact@openairinterface.org
################################################################################
MME :
{
   REALM                           = "openair4G.eur";            # YOUR REALM HERE
   PID_DIRECTORY                   = "/var/run";
   # Define the limits of the system in terms of served eNB and served UE.
   # When the limits will be reached, overload procedure will take place.
   MAXENB                           = 2;                    # power of 2
   MAXUE                           = 16;                   # power of 2
   RELATIVE_CAPACITY                = 10;
   EMERGENCY_ATTACH_SUPPORTED       = "yes";
   UNAUTHENTICATED_IMSI_SUPPORTED    = "yes";
   # EPS network feature support
   EPS_NETWORK_FEATURE_SUPPORT_IMS_VOICE_OVER_PS_SESSION_IN_S1      =
"yes";    # DO NOT CHANGE
```

```
EPS_NETWORK_FEATURE_SUPPORT_EMERGENCY_BEARER_SERVICES_IN_S1_MODE = "yes";    # DO NOT CHANGE
   EPS_NETWORK_FEATURE_SUPPORT_LOCATION_SERVICES_VIA_EPC                = "yes";    # DO NOT CHANGE
   EPS_NETWORK_FEATURE_SUPPORT_EXTENDED_SERVICE_REQUEST                 = "yes";    # DO NOT CHANGE
   # Display statistics about whole system (expressed in seconds)
   MME_STATISTIC_TIMER                     = 10;
   IP_CAPABILITY = "IPV4V6";                                            # UNUSED, TODO
   INTERTASK_INTERFACE :
   {
      # max queue size per task
      ITTI_QUEUE_SIZE           = 2000000;
   };
   S6A :
   {
      S6A_CONF                  = "/usr/local/etc/oai/freeDiameter/mme_fd.conf"; # YOUR MME freeDiameter config file path
      HSS_HOSTNAME              = "hss";                                # THE HSS HOSTNAME
   };
   # ------- SCTP definitions
   SCTP :
   {
      # Number of streams to use in input/output
      SCTP_INSTREAMS  = 8;
      SCTP_OUTSTREAMS = 8;
   };
   # ------- S1AP definitions
   S1AP :
   {
      # outcome drop timer value (seconds)
      S1AP_OUTCOME_TIMER = 10;
   };
   # ------- MME served GUMMEIs
   # MME code DEFAULT  size = 8 bits
   # MME GROUP ID size = 16 bits
```

```
    GUMMEI_LIST = (
        {MCC="208" ; MNC="93"; MME_GID="4" ; MME_CODE="1"; }                    # YOUR
GUMMEI CONFIG HERE
    );
    # ------- MME served TAIs
    # TA (mcc.mnc:tracking area code) DEFAULT = 208.34:1
    # max values = 999.999:65535
    # maximum of 16 TAIs, comma separated
    # !!! Actually use only one PLMN
    TAI_LIST = (
        {MCC="208" ; MNC="93";  TAC = "1"; }                                    # YOUR TAI CONFIG
HERE
    );
    NAS :
    {
        # 3GPP TS 33.401 section 7.2.4.3 Procedures for NAS algorithm selection
        # decreasing preference goes from left to right
        ORDERED_SUPPORTED_INTEGRITY_ALGORITHM_LIST = [ "EIA2" , "EIA1" ,
"EIA0" ];
        ORDERED_SUPPORTED_CIPHERING_ALGORITHM_LIST = [ "EEA0" , "EEA1" ,
"EEA2" ];
        # EMM TIMERS
        # T3402 start:
        # At attach failure and the attempt counter is equal to 5.
        # At tracking area updating failure and the attempt counter is equal to 5.
        # T3402 stop:
        # ATTACH REQUEST sent, TRACKING AREA REQUEST sent.
        # On expiry:
        # Initiation of the attach procedure, if still required or TAU procedure
        # attached for emergency bearer services.
        T3402                           =  1                    # in minutes (default is 12 minutes)
        # T3412 start:
        # In EMM-REGISTERED, when EMM-CONNECTED mode is left.
        # T3412 stop:
        # When entering state EMM-DEREGISTERED or when entering EMM-CONNECTED
mode.
        # On expiry:
```

```
    # Initiation of the periodic TAU procedure if the UE is not attached for
    # emergency bearer services. Implicit detach from network if the UE is
    # attached for emergency bearer services.
    T3412                   = 54                    # in minutes (default is 54 minutes, network dependent)
    # T3422 start: DETACH REQUEST sent
    # T3422 stop: DETACH ACCEPT received
    # ON THE 1st, 2nd, 3rd, 4th EXPIRY: Retransmission of DETACH REQUEST
    T3422                   = 6                     # in seconds (default is 6s)
    # T3450 start:
    # ATTACH ACCEPT sent, TRACKING AREA UPDATE ACCEPT sent with GUTI, TRACKING AREA UPDATE ACCEPT sent with TMSI,
    # GUTI REALLOCATION COMMAND sent
    # T3450 stop:
    # ATTACH COMPLETE received, TRACKING AREA UPDATE COMPLETE received, GUTI REALLOCATION COMPLETE received
    # ON THE 1st, 2nd, 3rd, 4th EXPIRY: Retransmission of the same message type
    T3450                   = 6                     # in seconds (default is 6s)
    # T3460 start: AUTHENTICATION REQUEST sent, SECURITY MODE COMMAND sent
    # T3460 stop:
    # AUTHENTICATION RESPONSE received, AUTHENTICATION FAILURE received,
    # SECURITY MODE COMPLETE received, SECURITY MODE REJECT received
    # ON THE 1st, 2nd, 3rd, 4th EXPIRY: Retransmission of the same message type
    T3460                   = 6                     # in seconds (default is 6s)
    # T3470 start: IDENTITY REQUEST sent
    # T3470 stop: IDENTITY RESPONSE received
    # ON THE 1st, 2nd, 3rd, 4th EXPIRY: Retransmission of IDENTITY REQUEST
    T3470                   = 6                     # in seconds (default is 6s)
    # ESM TIMERS
    T3485                   = 8                     # UNUSED in seconds (default is 8s)
    T3486                   = 8                     # UNUSED in seconds (default is 8s)
    T3489                   = 4                     # UNUSED in seconds (default is 4s)
    T3495                   = 8                     # UNUSED in seconds (default is 8s)
  };
  NETWORK_INTERFACES :
  {
```

```
    # MME binded interface for S1-C or S1-MME  communication (S1AP), can be ethernet interface, virtual ethernet interface, we don't advise wireless interfaces
    MME_INTERFACE_NAME_FOR_S1_MME         = "eth1";                 # YOUR NETWORK CONFIG HERE
    MME_IPV4_ADDRESS_FOR_S1_MME       = "10.0.0.1/24";        # YOUR NETWORK CONFIG HERE
    # MME binded interface for S11 communication (GTPV2-C)
    MME_INTERFACE_NAME_FOR_S11_MME        = "lo";                   # YOUR NETWORK CONFIG HERE
    MME_IPV4_ADDRESS_FOR_S11_MME          = "127.0.11.1/8";         # YOUR NETWORK CONFIG HERE
    MME_PORT_FOR_S11_MME                  = 2123;                   # YOUR NETWORK CONFIG HERE
  };
  LOGGING :
  {
    # OUTPUT choice in { "CONSOLE", "SYSLOG", `path to file`", "`IPv4@`:`TCP port num`"}
    # `path to file` must start with '.' or '/'
    # if TCP stream choice, then you can easily dump the traffic on the remote or local host: nc -l `TCP port num` > received.txt
    OUTPUT          = "CONSOLE";
    #OUTPUT          = "SYSLOG";
    #OUTPUT          = "/tmp/mme.log";
    #OUTPUT          = "127.0.0.1:5656";
    # THREAD_SAFE choice in { "yes", "no" } means use of thread safe intermediate buffer then a single thread pick each message log one
    # by one to flush it to the chosen output
    THREAD_SAFE     = "yes";
    # COLOR choice in { "yes", "no" } means use of ANSI styling codes or no
    COLOR           = "yes";
    # Log level choice in { "EMERGENCY", "ALERT", "CRITICAL", "ERROR", "WARNING", "NOTICE", "INFO", "DEBUG", "TRACE"}
    SCTP_LOG_LEVEL  = "TRACE";
    S11_LOG_LEVEL   = "TRACE";
    GTPV2C_LOG_LEVEL  = "TRACE";
    UDP_LOG_LEVEL   = "TRACE";
```

```
    S1AP_LOG_LEVEL    = "TRACE";
    NAS_LOG_LEVEL     = "TRACE";
    MME_APP_LOG_LEVEL = "TRACE";
    S6A_LOG_LEVEL     = "TRACE";
    UTIL_LOG_LEVEL    = "TRACE";
    MSC_LOG_LEVEL     = "ERROR";
    ITTI_LOG_LEVEL    = "ERROR";
    MME_SCENARIO_PLAYER_LOG_LEVEL = "TRACE";
    # ASN1 VERBOSITY: none, info, annoying
    # for S1AP protocol
    ASN1_VERBOSITY    = "none";
  };
  TESTING :
  {
    # file should be copied here from source tree by following command: run_mme --install-mme-files ...
    SCENARIO_FILE = "/usr/local/share/oai/test/mme/no_regression.xml";
  };
};
S-GW :
{
  # S-GW binded interface for S11 communication (GTPV2-C), if none selected the ITTI message interface is used
  SGW_IPV4_ADDRESS_FOR_S11        = "127.0.11.2/8";          # YOUR NETWORK CONFIG HERE
};
```

ANEXO D: Fichero de configuración de mme_fd.conf

```
# -------- Local ---------
# Uncomment if the framework cannot resolv it.
Identity = "henry.openair4G.eur";
Realm = "openair4G.eur";
# TLS configuration (see previous section)
TLS_Cred = "/usr/local/etc/oai/freeDiameter/mme.cert.pem",
        "/usr/local/etc/oai/freeDiameter/mme.key.pem";
TLS_CA   = "/usr/local/etc/oai/freeDiameter/mme.cacert.pem";
# Disable use of TCP protocol (only listen and connect in SCTP)
# Default : TCP enabled
No_SCTP;
# This option is ignored if freeDiameter is compiled with DISABLE_SCTP option.
# Prefer TCP instead of SCTP for establishing new connections.
# This setting may be overwritten per peer in peer configuration blocs.
# Default : SCTP is attempted first.
Prefer_TCP;
No_IPv6;
# Overwrite the number of SCTP streams. This value should be kept low,
# especially if you are using TLS over SCTP, because it consumes a lot of
# resources in that case. See tickets 19 and 27 for some additional details on
# this.
# Limit the number of SCTP streams
SCTP_streams = 3;
# By default, freeDiameter acts as a Diameter Relay Agent by forwarding all
# messages it cannot handle locally. This parameter disables this behavior.
NoRelay;
# Use RFC3588 method for TLS protection, where TLS is negociated after CER/CEA exchange is completed
# on the unsecure connection. The alternative is RFC6733 mechanism, where TLS protects also the
# CER/CEA exchange on a dedicated secure port.
# This parameter only affects outgoing connections.
# The setting can be also defined per-peer (see Peers configuration section).
# Default: use RFC6733 method with separate port for TLS.
```

```
#TLS_old_method;
AppServThreads = 4;
# Specify the addresses on which to bind the listening server. This must be
# specified if the framework is unable to auto-detect these addresses, or if the
# auto-detected values are incorrect. Note that the list of addresses is sent
# in CER or CEA message, so one should pay attention to this parameter if some
# adresses should be kept hidden.
#ListenOn = ;
Port = 3870;
SecPort = 5870;
# -------- Extensions ---------
# Uncomment (and create rtd.conf) to specify routing table for this peer.
#LoadExtension = "rt_default.fdx" : "rtd.conf";
# Uncomment (and create acl.conf) to allow incoming connections from other peers.
#LoadExtension = "acl_wl.fdx" : "acl.conf";
# Uncomment to display periodic state information
#LoadExtension = "dbg_monitor.fdx";
# Uncomment to enable an interactive Python interpreter session.
# (see doc/dbg_interactive.py.sample for more information)
#LoadExtension = "dbg_interactive.fdx";
# Load the RFC4005 dictionary objects
#LoadExtension = "dict_nasreq.fdx";
LoadExtension = "dict_nas_mipv6.fdx";
LoadExtension = "dict_s6a.fdx";
# Load RFC4072 dictionary objects
#LoadExtension = "dict_eap.fdx";
# Load the Diameter EAP server extension (requires diameap.conf)
#LoadExtension = "app_diameap.fdx" : "diameap.conf";
# Load the Accounting Server extension (requires app_acct.conf)
#LoadExtension = "app_acct.fdx" : "app_acct.conf";
# -------- Peers ---------
# The framework will actively attempt to establish and maintain a connection
# with the peers listed here.
# For only accepting incoming connections, see the acl_wl.fx extension.
# ConnectPeer
# Declare a remote peer to which this peer must maintain a connection.
# In addition, this allows specifying non-default parameters for this peer only
```

# (for example disable SCTP with this peer, or use RFC3588-flavour TLS).
# Note that by default, if a peer is not listed as a ConnectPeer entry, an
# incoming connection from this peer will be rejected. If you want to accept
# incoming connections from other peers, see the acl_wl.fdx? extension which
# allows exactly this.
ConnectPeer= "hss.openair4G.eur" { ConnectTo = "127.0.0.1"; No_SCTP ; No_IPv6; Prefer_TCP; No_TLS; port = 3868; realm = "openair4G.eur";};

ANEXO E: Fichero de configuración de spgw.conf

```
################################################################################
# Licensed to the OpenAirInterface (OAI) Software Alliance under one or more
# contributor license agreements.  See the NOTICE file distributed with
# this work for additional information regarding copyright ownership.
# The OpenAirInterface Software Alliance licenses this file to You under
# the Apache License, Version 2.0  (the "License"); you may not use this file
# except in compliance with the License.
# You may obtain a copy of the License at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#-------------------------------------------------------------------------------
# For more information about the OpenAirInterface (OAI) Software Alliance:
#      contact@openairinterface.org
################################################################################
S-GW :
{
   NETWORK_INTERFACES :
   {
      # S-GW binded interface for S11 communication (GTPV2-C), if none selected the ITTI message interface is used
      SGW_INTERFACE_NAME_FOR_S11            = "lo";                  # STRING, interface name, YOUR NETWORK CONFIG HERE
      SGW_IPV4_ADDRESS_FOR_S11              = "127.0.11.2/8";            # STRING, CIDR, YOUR NETWORK CONFIG HERE
      # S-GW binded interface for S1-U communication (GTPV1-U) can be ethernet interface, virtual ethernet interface, we don't advise wireless interfaces
      SGW_INTERFACE_NAME_FOR_S1U_S12_S4_UP    = "eth1";                  # STRING, interface name, YOUR NETWORK CONFIG HERE, USE "lo" if S-GW run on eNB host
```

```
    SGW_IPV4_ADDRESS_FOR_S1U_S12_S4_UP       = "10.0.0.1/24";            # STRING, CIDR, YOUR NETWORK CONFIG HERE
    SGW_IPV4_PORT_FOR_S1U_S12_S4_UP          = 2152;                     # INTEGER, port number, PREFER NOT CHANGE UNLESS YOU KNOW WHAT YOU ARE DOING
    # S-GW binded interface for S5 or S8 communication, not implemented, so leave it to none
    SGW_INTERFACE_NAME_FOR_S5_S8_UP          = "none";                   # STRING, interface name, DO NOT CHANGE (NOT IMPLEMENTED YET)
    SGW_IPV4_ADDRESS_FOR_S5_S8_UP            = "0.0.0.0/24";             # STRING, CIDR, DO NOT CHANGE (NOT IMPLEMENTED YET)
  };
  INTERTASK_INTERFACE :
  {
    # max queue size per task
    ITTI_QUEUE_SIZE            = 2000000;                    # INTEGER
  };
  LOGGING :
  {
    # OUTPUT choice in { "CONSOLE", "SYSLOG", `path to file`", "`IPv4@`:`TCP port num`"}
    # `path to file` must start with '.' or '/'
    # if TCP stream choice, then you can easily dump the traffic on the remote or local host: nc -l `TCP port num` > received.txt
    OUTPUT           = "CONSOLE";                                # see 3 lines above
    #OUTPUT           = "SYSLOG";                                # see 4 lines above
    #OUTPUT           = "/tmp/spgw.log";                         # see 5 lines above
    #OUTPUT           = "127.0.0.1:5656";                        # see 6 lines above
    # THREAD_SAFE choice in { "yes", "no" } means use of thread safe intermediate buffer then a single thread pick each message log one
    # by one to flush it to the chosen output
    THREAD_SAFE      = "no";
    # COLOR choice in { "yes", "no" } means use of ANSI styling codes or no
    COLOR            = "yes";
    # Log level choice in { "EMERGENCY", "ALERT", "CRITICAL", "ERROR", "WARNING", "NOTICE", "INFO", "DEBUG", "TRACE"}
    UDP_LOG_LEVEL     = "TRACE";
    GTPV1U_LOG_LEVEL   = "TRACE";
    GTPV2C_LOG_LEVEL   = "TRACE";
```

```
    SPGW_APP_LOG_LEVEL = "TRACE";
    S11_LOG_LEVEL      = "TRACE";
  };
};
P-GW =
{
  NETWORK_INTERFACES :
  {
    # P-GW binded interface for S5 or S8 communication, not implemented, so leave it to none
    PGW_INTERFACE_NAME_FOR_S5_S8          = "none";                 # STRING, interface name, DO NOT CHANGE (NOT IMPLEMENTED YET)
    # P-GW binded interface for SGI (egress/ingress internet traffic)
    PGW_INTERFACE_NAME_FOR_SGI            = "eth0";                 # STRING, YOUR NETWORK CONFIG HERE
    PGW_MASQUERADE_SGI                    = "yes";                  # STRING, {"yes", "no"}. YOUR NETWORK CONFIG HERE, will do NAT for you if you put "yes".
    UE_TCP_MSS_CLAMPING                   = "no";                   # STRING, {"yes", "no"}.
  };
  # Pool of UE assigned IP addresses
  # Do not make IP pools overlap
  # first IPv4 address X.Y.Z.1 is reserved for GTP network device on SPGW
  # Normally no more than 16 pools allowed, but since recent GTP kernel module use, only one pool allowed (TODO).
  IP_ADDRESS_POOL :
  {
    IPV4_LIST = (
                "172.16.0.0/16"                                 # STRING, CIDR, YOUR NETWORK CONFIG HERE.
              );
  };
  # DNS address communicated to UEs
  DEFAULT_DNS_IPV4_ADDRESS     = "8.8.4.4";                       # YOUR NETWORK CONFIG HERE
  DEFAULT_DNS_SEC_IPV4_ADDRESS = "8.8.8.8";                       # YOUR NETWORK CONFIG HERE
```

```
    # Non standard feature, normally should be set to "no", but you may need to set to yes for UE that do not explicitly request a PDN address through NAS signalling
    FORCE_PUSH_PROTOCOL_CONFIGURATION_OPTIONS = "no";                       # STRING, {"yes", "no"}.
    UE_MTU                          = 1500                  # INTEGER
};
```

ANEXO F: Fichero de configuración de enb.band7.oaisim.conf

```
Active_eNBs = ( "eNB_Eurecom_LTEBox");
# Asn1_verbosity, choice in: none, info, annoying
Asn1_verbosity = "none";
eNBs =
(
 {
   ////////// Identification parameters:
   eNB_ID    =  0xe00;
   cell_type =  "CELL_MACRO_ENB";
   eNB_name  =  "eNB_Eurecom_LTEBox";
   // Tracking area code, 0x0000 and 0xfffe are reserved values
   tracking_area_code  =  "1";
   mobile_country_code =  "208";
   mobile_network_code =  "93";
     ////////// Physical parameters:
   component_carriers = (
    {
        node_function                   = "eNodeB_3GPP";
        node_timing                     = "synch_to_ext_device";
        node_synch_ref                  = 0;
        frame_type                      = "FDD";
        tdd_config                          = 3;
        tdd_config_s                        = 0;
        prefix_type                         = "NORMAL";
        eutra_band                          = 7;
        downlink_frequency                  = 2680000000L;
        uplink_frequency_offset             = -120000000;
        Nid_cell                            = 0;
        N_RB_DL                             = 25;
        Nid_cell_mbsfn                      = 0;
        nb_antenna_ports                    = 2;
        nb_antennas_tx                      = 2;
        nb_antennas_rx                      = 2;
        tx_gain                 = 25;
         rx_gain                 = 20;
```

```
prach_root                                = 0;
prach_config_index                        = 0;
prach_high_speed                          = "DISABLE";
prach_zero_correlation                    = 1;
prach_freq_offset                         = 2;
pucch_delta_shift                         = 1;
pucch_nRB_CQI                             = 1;
pucch_nCS_AN                              = 0;
pucch_n1_AN                               = 32;
pdsch_referenceSignalPower                = 0;
pdsch_p_b                                 = 0;
pusch_n_SB                                = 1;
pusch_enable64QAM                         = "DISABLE";
pusch_hoppingMode                 = "interSubFrame";
pusch_hoppingOffset               = 0;
    pusch_groupHoppingEnabled                             = "ENABLE";
      pusch_groupAssignment                               = 0;
      pusch_sequenceHoppingEnabled                        = "DISABLE";
      pusch_nDMRS1                 = 0;
      phich_duration               = "NORMAL";
      phich_resource               = "ONESIXTH";
      srs_enable                   = "DISABLE";
      /*  srs_BandwidthConfig           =;
      srs_SubframeConfig                =;
      srs_ackNackST                     =;
      srs_MaxUpPts                      =;*/
      pusch_p0_Nominal                  = -108;
      pusch_alpha                       = "AL1";
      pucch_p0_Nominal                  = -108;
      msg3_delta_Preamble               = 6;
      pucch_deltaF_Format1              = "deltaF2";
      pucch_deltaF_Format1b              = "deltaF3";
      pucch_deltaF_Format2              = "deltaF0";
      pucch_deltaF_Format2a              = "deltaF0";
      pucch_deltaF_Format2b            = "deltaF0";
rach_numberOfRA_Preambles             = 64;
rach_preamblesGroupAConfig            = "DISABLE";
```

```
/*
        rach_sizeOfRA_PreamblesGroupA           = ;
        rach_messageSizeGroupA                  = ;
        rach_messagePowerOffsetGroupB           = ;
*/
        rach_powerRampingStep                   = 2;
        rach_preambleInitialReceivedTargetPower = -100;
        rach_preambleTransMax                   = 10;
        rach_raResponseWindowSize               = 10;
        rach_macContentionResolutionTimer       = 48;
        rach_maxHARQ_Msg3Tx                     = 4;
        pcch_default_PagingCycle                = 128;
        pcch_nB                                 = "oneT";
        bcch_modificationPeriodCoeff                = 2;
        ue_TimersAndConstants_t300                  = 1000;
        ue_TimersAndConstants_t301                  = 1000;
        ue_TimersAndConstants_t310                  = 1000;
        ue_TimersAndConstants_t311                  = 10000;
        ue_TimersAndConstants_n310                  = 20;
            ue_TimersAndConstants_n311                      = 1;
            ue_TransmissionMode                             = 2;
      }
   );
   srb1_parameters :
   {
      # timer_poll_retransmit = (ms) [5, 10, 15, 20,... 250, 300, 350, ... 500]
      timer_poll_retransmit    = 80;
      # timer_reordering = (ms) [0,5, ... 100, 110, 120, ... ,200]
      timer_reordering         = 35;
      # timer_reordering = (ms) [0,5, ... 250, 300, 350, ... ,500]
      timer_status_prohibit    = 0;
      # poll_pdu = [4, 8, 16, 32, 64, 128, 256, infinity(>10000)]
      poll_pdu              =  4;
      #                          poll_byte                          =                          (kB)
[25,50,75,100,125,250,375,500,750,1000,1250,1500,2000,3000,infinity(>10000)]
      poll_byte             =  99999;
```

```
   # max_retx_threshold = [1, 2, 3, 4 , 6, 8, 16, 32]
   max_retx_threshold       =  4;
}
# ------- SCTP definitions
SCTP :
{
   # Number of streams to use in input/output
   SCTP_INSTREAMS  = 2;
   SCTP_OUTSTREAMS = 2;
};
////////// MME parameters:
mme_ip_address      = ( { ipv4       = "10.0.1.2";
                          ipv6       = "192:168:30::17";
                          active     = "yes";
                          preference = "ipv4";
                        }
                      );
NETWORK_INTERFACES :
{
   ENB_INTERFACE_NAME_FOR_S1_MME           = "eth0";
   ENB_IPV4_ADDRESS_FOR_S1_MME             = "10.0.0.1/24";
   ENB_INTERFACE_NAME_FOR_S1U              = "eth0";
   ENB_IPV4_ADDRESS_FOR_S1U                = "10.0.0.1/24";
   ENB_PORT_FOR_S1U                        = 2152; # Spec 2152
};
log_config :
{
global_log_level                 ="trace";
global_log_verbosity               ="medium";
hw_log_level                    ="info";
hw_log_verbosity                  ="medium";
phy_log_level                   ="trace";
phy_log_verbosity                 ="medium";
mac_log_level                    ="trace";
mac_log_verbosity                  ="medium";
rlc_log_level                   ="trace";
rlc_log_verbosity                 ="medium";
```

```
    pdcp_log_level                  ="trace";
    pdcp_log_verbosity                ="medium";
    rrc_log_level                  ="trace";
    rrc_log_verbosity                ="medium";
    gtpu_log_level                  ="debug";
    gtpu_log_verbosity                ="medium";
    udp_log_level                  ="debug";
    udp_log_verbosity                ="medium";
    osa_log_level                  ="debug";
    osa_log_verbosity                ="low";
   };
  }
);
```

ANEXO G: Fichero de configuración de ue_eurecom_test_sfr

```
# List of known PLMNS
PLMN: {
   PLMN0: {
        FULLNAME="Test network";
        SHORTNAME="OAI4G";
        MNC="01";
        MCC="001";
   };
   PLMN1: {
        FULLNAME="SFR France";
        SHORTNAME="SFR";
        MNC="10";
        MCC="208";
   };
   PLMN2: {
        FULLNAME="SFR France";
        SHORTNAME="SFR";
        MNC="11";
        MCC="208";
   };
   PLMN3: {
        FULLNAME="SFR France";
        SHORTNAME="SFR";
        MNC="13";
        MCC="208";
   };
   PLMN4: {
        FULLNAME="OAI LTEBOX";
        SHORTNAME="OAIALU";
        MNC="93";
        MCC="208";
   };
   PLMN5: {
        FULLNAME="T-Mobile USA";
        SHORTNAME="T-Mobile";
```

```
        MNC="280";
        MCC="310";
    };
    PLMN6: {
        FULLNAME="FICTITIOUS USA";
        SHORTNAME="FICTITIO";
        MNC="028";
        MCC="310";
    };
    PLMN7: {
        FULLNAME="Vodafone Italia";
        SHORTNAME="VODAFONE";
        MNC="10";
        MCC="222";
    };
    PLMN8: {
        FULLNAME="Vodafone Spain";
        SHORTNAME="VODAFONE";
        MNC="01";
        MCC="214";
    };
    PLMN9: {
        FULLNAME="Vodafone Spain";
        SHORTNAME="VODAFONE";
        MNC="06";
        MCC="214";
    };
    PLMN10: {
        FULLNAME="Vodafone Germ";
        SHORTNAME="VODAFONE";
        MNC="02";
        MCC="262";
    };
    PLMN11: {
        FULLNAME="Vodafone Germ";
        SHORTNAME="VODAFONE";
        MNC="04";
```

```
        MCC="262";
    };
};
UE0:
{
    USER: {
        IMEI="35609204079301";
        MANUFACTURER="EURECOM";
        MODEL="LTE Android PC";
        PIN="0000";
    };
    SIM: {
        MSIN="0000000001";
        USIM_API_K="8baf473f2f8fd09487cccbd7097c6862";
        OPC="8e27b6af0e692e750f32667a3b14605d";
        MSISDN="33638030001";
    };
    # Home PLMN Selector with Access Technology
    HPLMN= "20893";
    # User controlled PLMN Selector with Access Technology
    UCPLMN_LIST = ();
    # Operator PLMN List
    OPLMN_LIST = ("00101", "20810", "20811", "20813", "20893", "310280", "310028");
    # Operator controlled PLMN Selector with Access Technology
    OCPLMN_LIST = ("22210", "21401", "21406", "26202", "26204");
    # Forbidden plmns
    FPLMN_LIST = ();
    # List of Equivalent HPLMNs
#TODO: UE does not connect if set, to be fixed in the UE
#    EHPLMN_LIST= ("20811", "20813");
    EHPLMN_LIST= ();
};
```

ANEXO H: Proceso de autenticación del usuario en la entidad MME

ANEXO I: Proceso de autenticación del usuario en la entidad S-PGW

espoch | Dirección de Bibliotecas y Recursos del Aprendizaje

UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 15 / 06 / 2022

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: HENRY EZEQUIEL YUGSIN SANCHEZ
INFORMACIÓN INSTITUCIONAL
Facultad: INFORMÁTICA Y ELECTRÓNICA
Carrera: TELECOMUNICACIONES
Título a optar: INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES
f. Analista de Biblioteca responsable: Lcdo. Holger Ramos, MSc.

0967-DBRA-UPT-2022