UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

Estudio descriptivo de los elementos de un sistema LTE que permiten integrar equipos WI-FI en su red

Trabajo Monográfico para optar al título de
Ingeniero en Telecomunicaciones

Elaborado por:

- Br. Joe Farhat Amador Martínez.
  2007-22729
- Br. Esvalle Darién Salgado Ulmos.
  2007-22717

Tutor:

Ing. Juan Manuel Martínez Toribio
Profesor Titular de la facultad de electrotecnia y computación (FEC)

Managua, Nicaragua
Julio 2015

Dedicatoria

*A **Dios** creador de todo cuanto existe, quien nos brindó la salud, sabiduría e inteligencia necesarias para concluir nuestra tesis.*

*A **mis padres**, pilares fundamentales en mi vida quienes con amor, esfuerzo y dedicación me han apoyado incondicionalmente en cada etapa de mi vida.*

*A **mis familiares, amigos y seres queridos** quienes de una u otra manera me alentaron para alcanzar mis metas, siempre creyeron en mí y cuyas palabras me impulsaron a seguir adelante.*

Joe Farhat Amador Martínez.

Le dedico este trabajo monográfico a mi madre:

Ana Ulmos Vado.

Tengo el gozo de poder compartir con ella, una persona recta, admirable, intachable y con una visión singular del mundo. Me siento afortunado y privilegiado de contar con su amor y apoyo incondicional.

Esvalle Darién Salgado Ulmos.

Abreviaciones

0-9	
3GPP	Third Generation Partnership Project
A	
AF	Application Function
AH	Authentication Header
AMPS	Advanced Mobile Phone System
ANDSF	Access Network Discovery and Selection Function
ANQP	Access Network Query Protocol
API	Application Program Interface
APN0	Access Point Name
AS	Application Server
B	
BA	Biding Acknowledgement
BBERF	Bearer Binding and Event Report Function
BGCF	Breakout Gateway Control Function
BS	Base Station
BSC	Base Station Controller
BSS	Basic Service Set
BU	Biding Update
C	
CCK	Complementary Code Key
CDMA	Code Division Multiple Access
CN	Core Network
CoA	Care of Address
CSCF	Call Session Control Function
D	
DNS	Domain Name System
DRB	Data Radio Bearer
DSL	Digital Subscriber Line
DSMIPv6	Dual Stack Mobile IPv6
DSSS	Direct Sequence Spread Spectrum
E	
EAP	Extensible Authentication Protocol
EAP-SIM	Extensible Authentication Protocol- Subscriber Identity Module
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EDGE	Enhanced Data Rates for GSM Evolution
EIR	Equipment Identity Register
eNB	Evolved Node B
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway

EPS	Evolved Packet System
ESP	Encapsulated Security Payload
ESS	Extended Service Set
E-UTRAN	Evolved-Universal Terrestrial Access Network
F	
FDD	Frequency Division Duplex
G	
GAS	Generic Advertise Service
GBA	Generic Bootstapping Architecture
GERAN	GSM/Edge Radio Access Network
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communications
GTP	GPRS Tunneling Protocol
GUTI	Globally Unique Temporary Identity
H	
HA	Home Agent
HeNB	Home e-Node
HESS	Homogeneous ESS
HetNet	Heterogeneous Networks
HLR	Home Location Register
HoA	Home of Address
HS2.0	HotSpot 2.0
HSB	Home Base Station
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
I	
I-CSCF	Interrogating-CSCF
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force,
IFOM	IP Flow Mobility
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	IP Security
ISMP	Inter-System Mobility Policy
ISP	Internet Service Provider
ISRP	Inter-System Routing Policy
L	
LIPA	Local IP Access
LMA	Local Mobility Anchor
LTE	Long-Term Evolution
M	
MAG	Mobile Access Gateway

MAPCON	Multiple Access PDNs Connectivity
ME	Mobile Equipment
MGCF	Media Gateway Controller Function
MGW	Media Gateway
MIP	Mobile IP
MME	Mobility Management Entity
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber Integrated Services Digital Network
N	
NB	NodeB
O	
OCS	Online Charging System
OFCS	Offline Charging System
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frecuency Division Multiple Access
OMA-DM	Open Mobile Alliance Device Management
OSI	Open System Interconnection
OSFP	Open Shortest Path First protocol
P	
PBA	Proxy Biding Acknowledgement
PBU	Proxy Biding Update
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy-CSCF
PDN	Packet Data Network
PDN GW	Packet Data Network Gateway
PGW	Packet Data Network Gateway
PLMN	Public Land Mobile Network
Q	
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
QoS	Quality of Service
R	
RA	Routing Advertisement
RIP	Routing Information Protocol
RNC	Radio Network Controller
S	
SA	Security Association
SAE	System Architecture Evolution
SC-FDMA	Single Carrier FDMA
S-CSCF	Server-CSCF
SDM	Space Division Multiplexing
SDF	Service Data Flow
S-GW	Serving Gateway
SIP	Session Initiation Protocol

SPR	Subscription Profile Repository
SSH	Secured Shell
STA	Station
T	
TDD	Time-Division Duplexing
TIC	Tecnologías de la Información y la Comunicación
TLS	Transport Layer Security
U	
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Access Network
V	
VLR	Visitor Location Register
W	
WAG	WLAN Access Gateway
WBA	Wireless Broadband Alliance
WiMAx	Worldwide Interoperability for Microwave Access.
WLAN	Wireless Local Area Network
WPA	Wireless Protected Accesss

Resumen

Este trabajo monográfico es una investigación teórica que presenta los conceptos de la arquitectura del sistema de comunicaciones inalámbrica celular LTE que permiten que la tecnología de acceso inalámbrica Wi-Fi se integre para formar una red heterogénea.

Dado que es el núcleo del sistema LTE que permite la interoperabilidad entre las tecnologías de acceso, se definen los conceptos que sirven de base para los análisis posteriores. Estos conceptos se encargan de introducir a la arquitectura de LTE, es por eso que se abarcan los elementos básicos y principales que están presente en este sistema, la manera de abordar los elementos es basándose a la función en los procesos de interoperabilidad con la tecnología Wi-Fi a pesar que el elemento no interactúe directamente en ciertos casos.

El análisis de la arquitectura LTE con Wi-Fi integrado está basado en los documentos publicados por la 3GPP por lo que en este caso los elementos son específicamente relacionados con la interoperabilidad de LTE con otras tecnologías, dado que la tecnología que se aborda es Wi-Fi, las variantes de la arquitectura y elementos presentados son solamente los que permitan la interoperabilidad con esta.

La 3GPP define una serie de procedimientos para los accesos y movilidad cuando se utilizan otras tecnologías de acceso, es por eso que en este documento se define un escenario en los cuales se hicieron las consideraciones pertinentes que sirve de guía para la elección de estos procedimientos y crear un contexto a todos los conceptos que son definidos en este documento.

Este estudio adquiere una importancia dado que ambas tecnologías aquí expuestas (LTE y Wi-Fi) son fundamentales en el desarrollo de las telecomunicaciones a nivel mundial, se han redactados múltiples investigaciones y documentos similares lo cual reafirma la tendencia y la anuencia a no solo aplicar estas tecnologías sino también a integrarlas.

El eje principal de este estudio es; aportar al mundo de las TICs en Nicaragua a través de investigaciones de tecnologías trascendentes que puedan ayudar a Nicaragua a competir en la región, por lo cual se discuten una serie de temas para enriquecer la investigación y contextualizar ciertos aspectos que son muy importantes para los objetivos de esta.

Las conclusiones demuestran que la integración de la tecnología Wi-Fi en el sistema LTE es compleja y existen muchas variables en el proceso de interoperabilidad lo cual generan un debate inminente, de si los proveedores de servicio móvil de Nicaragua que, aún no han implementado de manera comercial LTE, les sea rentable y útil contar e invertir en una red heterogénea de este tipo. Por lo que ofrece la investigación se puede concluir que se ofrece grandes bondades y las bases están sentadas para que las integraciones entre tecnologías inalámbricas sigan mejorando.

Índice

Introducción

Las telecomunicaciones avanzan a un paso desmesurado hace un poco de más de diez años éramos testigos de la increíble utilidad y casi futurística tecnología celular y como esta en tan poco tiempo ha evolucionado hasta multiplicar su rendimiento por centenas, esto en gran medida por el gran avance en el procesamiento digital y la ley de Moore donde cada día se desarrollan dispositivos más rápidos, más eficientes y más baratos [1].

LTE (*Long Term Evolution,* Evolución a Largo Plazo) en el presente, ha sido la respuesta lógica a las crecientes demandas que se habían venido dando por un consumidor que empezó a asociar las cualidades y prestaciones de un servicio de banda ancha, que pudiese tener en su casa o trabajo por medio de fibra, DSL *(Digital Subscriber Line,* Línea de Subscriptor Digital*)*, o cable módem con un dispositivo móvil que no dependiera de estar conectado a un cable o al corto alcance de un punto de acceso Wi-Fi.

LTE implementa el protocolo IP *(Internet Protocol,* Protocolo de Internet*)* [Figura 6.1.1] en su sistema de principio a fin, lo que le permite acoplarse mejor a las redes externas ya que la mayoría funciona con este mismo protocolo, así como también facilitar el acceso a otras tecnologías.

Siendo una nueva generación presenta nuevas características y aplicaciones. La implementación y la propia arquitectura del sistema LTE han marcado la tendencia de integrarse con otras tecnologías tales como anteriores generaciones y tecnologías ajenas a la telefonía celular como es el caso de Wi-Fi.

Contar con las tecnologías Wi-Fi ya sea de respaldo o complemento a una infraestructura de naturaleza muy versátil permite tener una red más escalable, pensada para las aplicaciones actuales y más longevas.

El presente trabajo ofrece una visión clara de cómo la tecnología Wi-Fi, que hace poco menos de una década era considerada de área local y de corto alcance, es capaz de integrarse a un sistema LTE que está diseñado para dar servicio a gran escala, generando lo que hoy en día se conoce como red heterogénea.

Los detalles están presentes en el sistema LTE, término que hace referencia a los estándares y conceptos definidos por sus creadores 3GPP *(3rd Generation Partnership Project, Proyecto de la Asociación de Tercera Generación)*, que trabajan con base en *releases* (publicaciones), se le empezó a llamar LTE desde el *release* 8 hasta la fecha se han publicado hasta el *release* 12 .

Hay que destacar que muchos de los conceptos y temas abarcados fueron definidos desde el *release* 8 sin embargo nuevas funcionalidades han sido definidas sobre todo en el tema de interoperabilidad y flexibilidad de red es por eso que esta investigación considera *releases* posteriores.

Objetivos

Principal

- Presentar un estudio descriptivo de la parte de la arquitectura de un sistema LTE basado en el *release* 8 que permite a dispositivos Wi-Fi obtener servicio a través de la infraestructura del sistema LTE.

Específicos

- Identificar los puntos claves de la arquitectura del sistema LTE que se correlacionen con la integración de Wi-Fi con este sistema.

- Describir de forma general los estándares, entidades de red, interfaces y protocolos que sirvan como base para el estudio.

- Abstraer los puntos de correlación entre la tecnología de acceso de red LTE y Wi-Fi.

- Crear diagramas de red del sistema LTE que presente una red heterogénea Wi-Fi /LTE con base en criterios congruentes a la posibilidad de implementación en Nicaragua.

- Discutir el futuro de estas tecnologías y lo que representan para un país en vías de desarrollo como Nicaragua, haciendo uso de las tendencias regionales y globales de proveedores que ya han implementado tales redes.

Justificación

Las comunidades científica y académica del país por sus naturalezas están ligadas al estudio, desarrollo e investigación de las tecnologías que rompen cada vez más frecuentemente en el mundo de hoy.

Es importante que las investigaciones estén a tono con la situación y agenda de Nicaragua, que ha mostrado un gran interés en fomentar el sector de las TIC (Tecnologías de la Información y la Comunicación) otorgando licitaciones para la explotación del espectro con fines comerciales de telefonía celular, internet de banda ancha inalámbrico e incluso planea invertir capital propio al lanzar el primer satélite de la región.

En Nicaragua las pocas empresas que ofrecen telefonía celular, internet móvil o convencional no hacen estudios públicos acerca de las tecnologías que han, están o planean implementar, lo cual dificulta estudiar o evaluar estas tecnologías aplicadas en Nicaragua.

La mayor fuente de información se genera a través de los desarrolladores y empresas de telecomunicaciones extranjeras que publican estudios e investigaciones propias, así como también organizaciones internacionales que recogen datos de los diferentes países.

Es imperativo que existan investigaciones que abarquen el estudio de las tecnologías en el país así como toma igual valor estudios de nuevas tecnologías que están en fase de implementación y puedan significar un cambio radical.

El presente abarca la temática del sistema celular LTE que ha tenido una gran aceptación y ha incidido positivamente en la región. En el caso de Nicaragua no hay redes LTE desplegadas por el momento ya que están en fase de pruebas y diseño, sin embargo contar con un estudio de este tipo aporta a la dinámica global creando un soporte científico del cual sectores económicos, científicos y académicos pueden hacer uso, retroalimentarse y dar base a investigaciones posteriores más profundas sobre el tema.

El estudio comprende las partes del sistema LTE que permiten que una tecnología ajena a este ecosistema como lo es Wi-Fi pueda operar bajo la misma infraestructura. Por lo antes expresado la intención de esta investigación es brindar un documento que sirva de referencia a las personas que estudien sistemas de nueva generación relacionados a las telecomunicaciones y sea la base del diseño de una red heterogénea de este tipo o estudie su impacto en Nicaragua.

El poder estudiar estas tecnologías lleva al lector a comprender mejor hacia donde se dirigen las tecnologías de nueva generación, ya que es la base para poder hacer un bueno uso de ellas repercutiendo positivamente en el avance de la sociedad Nicaragüense.

1. Marco Teórico

1.1. Redes heterogéneas

El termino redes heterogéneas no es un estándar o un término definido por algún fabricante u organización, y es usado comúnmente en comunicaciones inalámbricas basadas en tecnologías celulares.

En telefonía celular cuando hablamos de macro-celdas (Áreas de cobertura entre 1 a 20 km) comúnmente se consideran redes homogéneas por utilizar el mismo tipo de acceso de radio a una determinada potencia que puede variar en el uso de la frecuencia asignada de acuerdo con el planeamiento del despliegue de la red y técnicas de reusó, como su nombre lo indica, ésta abraca una gran área de cobertura.

Sin embargo debido a las diferentes generaciones de tecnologías de telefonía celular y su longevidad, es común encontrar múltiples macro-celdas de diferentes tecnologías cubriendo la misma área y a los mismos usuarios, en dado caso tendríamos una red similar al concepto de red heterogénea.

Para llegar a un concepto concreto hay que considerar las *smallcells* que son consideradas como estaciones base de menor tamaño y potencia respecto a una macro-celda, dentro de este rango de celdas de menor tamaño encontramos a las femto-celdas, pico-celdas y micro-celdas. Este tipo de celdas son capaces de utilizar la misma tecnología que la macro-celda (LTE, HSDA+, WCDMA, etc.) o tecnologías alternativas como Wi-Fi.

Habiendo expuesto lo anterior, la red heterogénea a estudiar está compuesta por dos niveles:

1) Macro-Celdas
2) Smallcells

El término de redes heterogéneas a grandes rasgos es una red con múltiples niveles de diferentes tamaños de celdas y/o múltiples tecnologías de redes de acceso [1].

El nivel con que estas redes se integran se define en 4 tipos de acoplamientos:

1) **Sin acoplamiento**: las redes operan independientemente y la decisión recae en el dispositivo.
2) **Acoplamiento ligero**: en esta se comparten credenciales y autentificación pero la información viaja en núcleos diferentes.
3) **Acoplamiento estrecho**: ya en esta el tráfico es manejado completamente por el núcleo de red del operador.
4) **Acoplamiento muy estrecho**: en este las dos tecnologías de acceso de red se comunican entre sí para coordinar la comunicación.

Para cumplir con los objetivos de la investigación, abordaremos la red heterogénea enfocada en *smallcells* que empleen Wi-Fi como tecnología de acceso, este tipo de tecnología no se diseña basado en celdas si no por área de cobertura y a esta se le domina *hotspot.*

Al hablar de estas dos tecnologías de acceso que trabajan en las primeras dos capas del modelo de referencia OSI *(Open System Interconnection,* Modelo de Interconexión de Sistemas Abiertos*)*; Wi-Fi y LTE, podremos definir un concepto más específico de la red heterogénea a estudiar:

Un sistema de comunicación celular LTE que pueda integrarse con *smallcells* (*hotspot)* que trabajen con tecnología Wi-Fi, brindando acceso al equipo indistintamente de la tecnología de red de acceso (LTE o Wi-Fi), haciendo uso de cierto elementos de una misma infraestructuras. Aquí definimos una red heterogénea que puntualiza diferentes tamaños de celdas, múltiples redes de acceso y de acoplamiento.

A continuación estudiaremos las dos tecnologías ya antes mencionadas primeramente la tecnología Wi-Fi y posteriormente la tecnología celular LTE que sirve como infraestructura de la red heterogénea ya antes definida.

1.2. Wi-Fi

El termino Wi-Fi es una marca registrada, propiedad de Wi-Fi *Alliance* que lo definió como cualquier tipo de red de área local inalámbrico que se base en los estándares IEEE 802.11 del Instituto de ingenieros eléctricos y electrónico (*Institute of Electrical and Electronics Engineers*, IEEE).

IEEE 802.11:

Este estándar se definió con el propósito de proveer conectividad inalámbrica tanto a estaciones móviles, portables o fijas. También ofrece un medio de normalización de acceso a una o más bandas de frecuencia con el propósito de establecer comunicación en un área local [2].

Cada cierto tiempo la organización lanza una nueva versión del estándar, hasta la fecha ha publicado 3 (1999, 2007, 2012) en donde incluye oficialmente *Amendments* (modificaciones) que son desarrollados posteriormente a la publicación del anterior estándar, estos se distinguen de este por estar seguido de una o más letras en minúsculas; 802.11a y 802.11b son ejemplos concretos de estos, probablemente son los términos más conocidos en el mundo de las redes inalámbricas de área local.

Su arquitectura básica se puede observar el Figura 1.1.1 y está compuesta por:

- **BSS *(Basic Service Set,* Conjunto de Servicios Básico*)*:** este es el diagrama base en el que las estaciones se conectan a un punto centralizado normalmente un punto de acceso.

- **BSS *(ad-hoc)*:** este es un diagrama con la variante que la comunicación sucede entre STA
- **STA *(Station,* Estación*)***: estas son las estaciones o dispositivos capaces de trabajar con la tecnología Wi-Fi normalmente tienen la connotación de clientes o terminales.
- **AP *(Access Point,* Punto de Acceso*)*:** estos son los puntos de acceso encargados de interactuar con los múltiples STA y es la encargada de manejar la BSS
- **ESS *(Extended Service Set,* Conjunto de Servicios Extendido*)*:** es cuando se unen o se solapan múltiples AP trabajando juntos para dar una mayor cobertura.

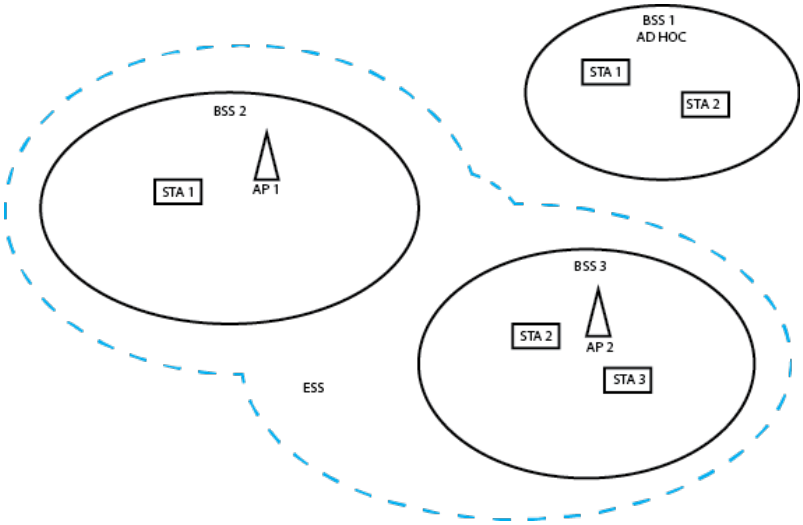

Figura 1.1.1: Arquitectura de red de 802.11

Cabe mencionar que el protocolo 802.11 se define a nivel de capa 1 y de la subcapa MAC (*Media Access control*, Control de Acceso al Medio) que pertenece a la capa 2 del modelo de referencia OSI, sin embargo la subcapa MAC se mantiene inalterada en la mayoría de las revisiones o *Amendments,* siendo la capa física la que varía. La tabla 1.2.1 muestra las características generales de las llamadas 5 generaciones de Wi-Fi y de su versión original.

Se definen otras revisiones que realizan otras funciones más que dar acceso destacándose 2 en particular:

- **802.11i:** este define unas series de medidas y protocolos para brindar seguridad por medio de autenticación.

- **802.11u:** este define mecanismos que permiten que las tecnologías IEEE 802.11 puedan interrelacionarse con redes externas tales como núcleos de redes celulares o líneas fijas.

	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac
Tecnología	DSSS	DSSS/CCK	OFDM	OFDM DSSS/CCK	SDM/OFDM	OFDM
Tasa de trasferencia (Mbps)	1, 2 s	5.5, 11	6-54	1-54	6.5-600	6.5-6933.3
Banda de frecuencia (GHz)	2.4	2.4	5	2.4	2.4, 5	5
Separación de canal (MHz)	25	25	25	25	20 y 40	20, 40 ,80 y 160

Tabla 1.2.1: Características físicas.
Extraída de [3]

1.3. Sistema LTE.

Este sistema formalmente definido como EPS *(Evolved Packet System,* Sistema de Paquetes Evolucionado*)* es un sistema muy robusto en muchos sentidos, sin embargo su gran avance es como su nombre lo indica; trabajar con paquetes, término que hace referencia a la capa internet del modelo TCP/IP donde se define el protocolo IP, EPS trabaja con este protocolo de principio a fin.

EPS fue definido por la organización 3GPP motivada por las múltiples demandas en el mundo de las comunicaciones celulares, esta organización lanza una serie de documentos que contienen toda la información correspondiente a las especificaciones de las tecnologías celulares por medio de TS (*Technical Specifications,* Especificaciones Técnicas*)* que se organizan por las diferentes partes y funciones de la red, la organización se reúne y revisa estas serie de documentos y los actualiza por medios de *releases* para definir mejoras o nuevas características.

La primera red LTE que se comercializo fue del *release* 8 y 9, los *releases* posteriores son conocidos como *LTE-Advanced.*

EPS está integrado por:

- **UE *(User Equipment,* Equipo de Usuario*)*** como estación móvil.

- **LTE/E-UTRAN *(evolved UMTS Terrestrial Radio Access,* Acceso de Radio Terrestre UMTS Evolucionado*)*** como acceso de radio.

- **SAE *(System Architecture Evolution,* Evolución de la Arquitectura del Sistema*)* /EPC *(Evolved Packet Core,* Núcleo de Paquetes Evolucionado*)*** como núcleo de red.

1.3.1. LTE/E-UTRAN

La organización 3GPP publica los documentos (TS 36.xxx), estas son conocidas comúnmente como LTE o E-UTRAN, como su nombre lo indica estos documentos definen la red de acceso de EPS.

El Principal elemento que se define es el eNB *(Evolved Node B,* Nodo B evolucionado*)* este tiene dos funciones [4]:

1. Trasmisiones de radio haciendo uso del procesamiento de señal tanto analógico como digital de la interfaz de radio de LTE.
2. Un control de operación de bajo nivel mandando mensajes de señalización como indicaciones de traspaso correspondiente a esas comunicaciones de radio.

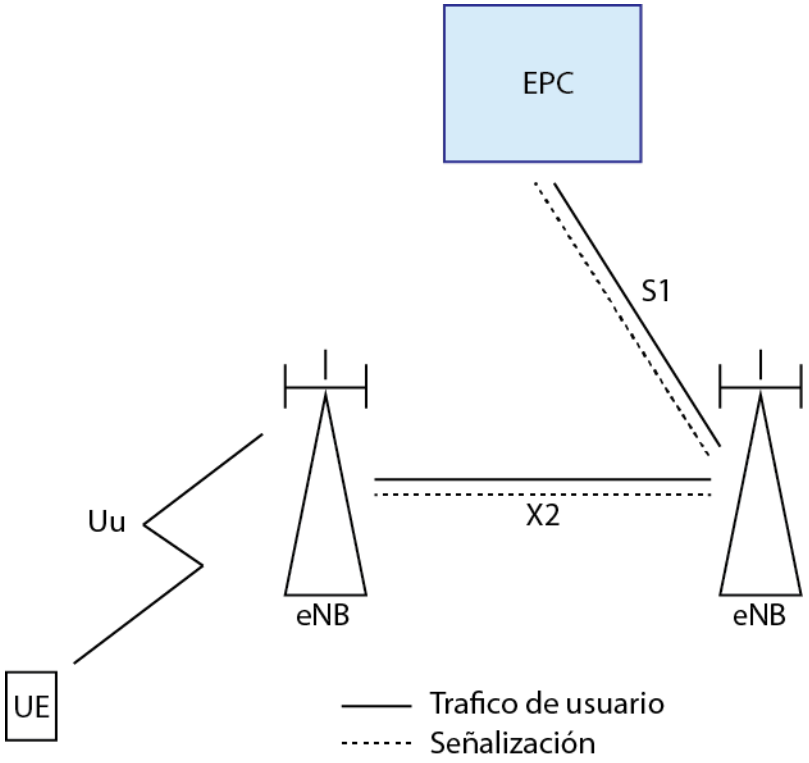

Figura 1.3.1: Arquitectura de E-UTRAN.

Como se puede ver en la *figura 1.3.1* el eNB se comunica a través de 3 interfaces:

Interfaz S1: conecta uno o más eNB al EPC (interfaz se define con más detalle en página 14).

Interfaz X2: Esta interfaz se utiliza para interconectar eNB entre sí utilizando los mismos protocolos que la interfaz S1-U (interfaz se define en página 21), además de también ser una interfaz basada en el protocolo UDP, otra similitud con la interfaz S1 es la división de su funcionamiento tanto en el plano de usuario como en el plano de control:

- Plano de usuario: La transferencia de datos de usuarios entre eNB se realiza únicamente durante los procesos de traspaso en el que los paquetes de usuarios almacenados en el eNB antiguo se transfieren al eNB nuevo [5]
- Plano de control: dentro del plano de control la interfaz X2 realiza las funciones de soporte de mecanismos de traspaso entre eNB e indicación del estado de carga al eNB.

Interfaz Uu: esta interfaz está encargada de comunicar al eNB con el UE a pesar que no se muestra en la gráfica esta interfaz es usada tanto para control como para tráfico de usuario.

Plano de control: Se utiliza para hacer *broadcast* (difusión) para que los UE reciban la información tanto de la red de acceso como también de la red troncal, por medio de estos mensajes *broadcast* también se le puede indicar al equipo ciertas acciones para restablecer conexión o hacerlo en dado caso que no lo haya hecho previamente, cabe destacar que esta interfaz permite el manejo de la señalización.

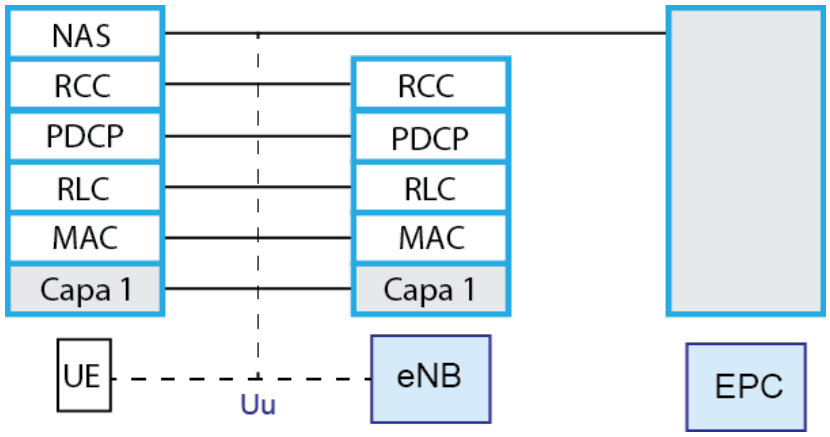

Figura 1.3.2: Protocolos de la interfaz Uu (plano de control)

Como se puede observar en Figura 1.3.2 la comunicación se realiza utilizando los siguientes protocolos:

- **Protocolo RRC (*Radio Resource Control*, Control de Recursos de Radio):** Es un protocolo definido por la 3GPP en su TS 36.331, encargado de controlar el móvil cuando se encuentra en un estado de conexión o si este se encuentra en modo *idle* (inactivo) [5]. Las principales funciones de RRC son:

  - Difusión de la información del sistema: mensajes de señalización NAS y AS.
  - Conexión de control RRC: control de establecimiento, modificación y liberación de los servicios portadores de radio y datos, funciones de movilidad que abarcan traspasos de intra e inter *handover* (traspasos), avisos *paging* (paginación), activación de seguridad inicial, recuperación en caso de fallo de enlace).
  - Medición, configuración y reportes.
  - Soporte de auto-configuración y auto-optimización

- **Protocolo PDCP (*Packet Data Convergence Protocol,* Protocolo de Convergencia de Paquetes de Datos):** Es un protocolo definido por la 3GPP en el TS 36.323 que se encarga de la compresión de cabecera de los paquetes IP [6]. Este protocolo es responsable del cifrado del plano de control, integridad y protección de la transferencia de datos, así como también la entrega ordenada de paquetes y remueve los paquetes duplicados generados debido a los traspasos, sus principales funciones se resumen en:

  - Transferencias de datos del plano de control y de usuario.
  - Mantenimiento de los números de secuencia de PDCP.
  - Descarte de paquetes por expirado de tiempo.

- **Protocolo RLC (*Radio Link Control*, Control de Radio Enlace):** Es un protocolo de la 3GPP definido en TS 36.322 y TS 25.322, se encarga de transportar los paquetes PDCP [7], sus principales funciones son:

  - Concatenación.
  - *Padding* (relleno).
  - Control de flujo.
  - Transferencia de datos de usuario.
  - Corrección de errores.
  - Detección de duplicados.
  - Cifrado.

- **Protocolo MAC (*Medium Access Control*, Acceso de Control al Medio):** El protocolo MAC fue definido por la 3GPP en el TS 36.321 y TS 25.321. Se encarga de brindar un conjunto de canales lógicos a la sub-capa RLC [7], sus principales funciones son:

  - Brinda servicios de transferencia de datos y ubicación de recursos a capas superiores.
  - Provee servicios de transferencia de datos a la capa física.
  - Señalización para peticiones de *scheduling* (asignación dinámica de recursos).
  - Mediciones.

Plano de usuario: Este se encarga de entregar los paquetes, como se puede observar en la figura 1.3.3 es muy similar al plano de control sin embargo nos encontramos con el protocolo IP y la capa de aplicación.

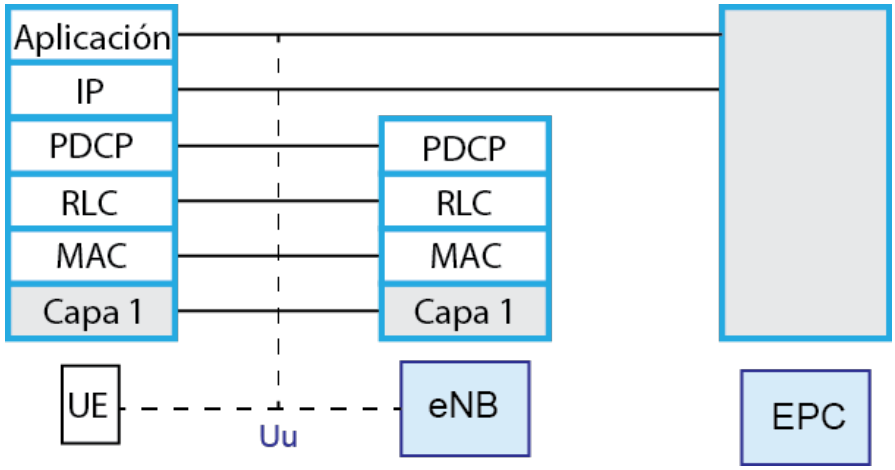

Figura 1.3.3 Interfaz Uu (plano de usuario)

En tabla 1.3.1 se muestra un resumen de las especificaciones de la capa física o capa 1.

		LTE	LTE-Advanced.
Ancho de Banda.		1.25-20 MHz	40-100 MHz
Modos de transmisión		FDD, TDD, Half Duplex FDD	FDD, TDD.
Latencia		10-15 ms	10 ms
Acceso de Radio	Downlink	OFDMA	OFDMA
	Uplink	SC-FDMA	SC-FDMA
Técnicas MIMO	Downlink	2x2, 4x2, 4x4	8x8
	Uplink	1x2, 1x4	4x4
Velocidades Pico a 20MHz	Downlink	173Mbps (2x2), 326Mbps (4x4) a 20 MHz	1 Gbps (8x8 64QAM)
	Uplink	75Mbps (1x2) a 10 MHz	500 Mbps (4x4)
Modulación Adaptativa		QPSK, 16QAM y 64AM	QPSK, 16QAM y 64AM

Tabla 1.3.1: Características Técnicas de LTE y LTE-Advanced
Extraída de [4]

Las velocidades respecto a las transferencias de datos pueden variar en dependencia de factores como la carga de la red, las condiciones de propagación del medio y los niveles en la intensidad de la señal transmitida. Los distintos tipos de accesos se utilizan con el fin de permitir la flexibilidad en el uso de las bandas de frecuencias.

Una de las grandes ambiciones de 3gpp no solo era brindar una evolución en la interfaz de radio si no también evolucionar su red troncal o núcleo a una que trabajara exclusivamente con paquetes utilizando el protocolo IP como característica principal es así como nace EPC.

1.3.2. EPC

Este se conforma por múltiples entidades de red que definen las funcionalidades para proporcionar un servicio de conectividad IP [8], este está pensado para aprovechar LTE/E-UTRAN, así como mejoras e incluso otras tecnologías, ya que su diseño se basa en una arquitectura plana, donde el tráfico de usuario es procesado por la menor cantidad de entidades de red o nodos.

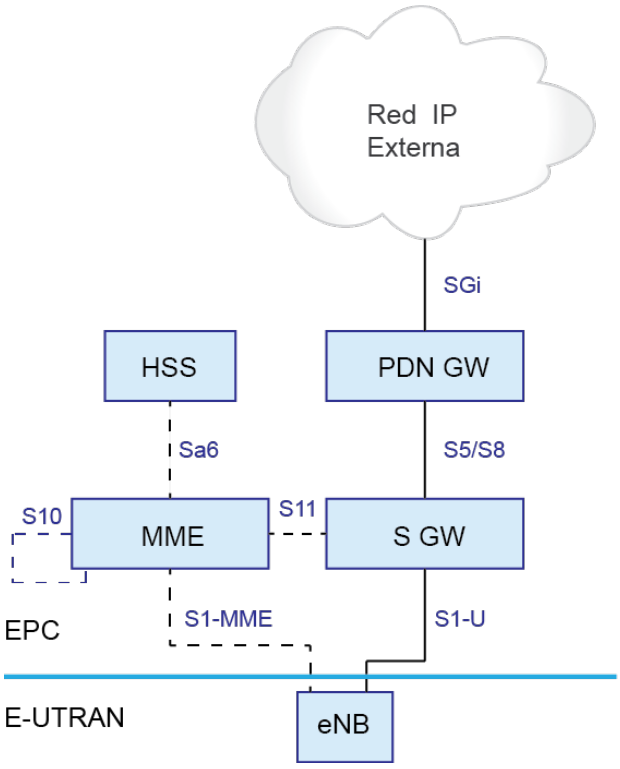

Figura 1.3.4: Arquitectura básica EPC para LTE

Como se muestra en la figura 1.3.4 nos encontramos con entidades de red que representan entidades lógicas que cubre una funcionalidad perfectamente delimitada. Por tanto, una entidad de red es una entidad funcional [5], estas se comunican a través de interfaces, ambas hace uso de protocolos definidos, tanto por la 3GPP y por otras organizaciones.

A continuación se definen entidades e interfaces de la arquitectura básica de EPC:

MME (*Mobility Management Entity*, Entidad de Manejo de Movilidad)

Esta entidad está encargada de todas las funciones relacionadas con el plano de control y señalización entre UE y el EPC para gestionar el acceso de los terminales a través de E-UTRAN. Todo usuario que se encuentre registrado en la red LTE y sea accesible a través de E-UTRAN, tiene una sola entidad MME asignada que sirve a un conjunto de eNB dependiendo de la ubicación en que se encuentre [5].

La MME es responsable de la autenticación de usuario así como también del manejo de los terminales que se encuentran en estado *idle* y del envío de mensajes *paging.*

En redes de mayor tamaño podemos encontrar más de una MME para cumplir requerimientos de señalización, cada MME se encuentra asignada a una determinada área geográfica.

Como lo muestra la gráfica le entidad MME se conecta a otras entidades de red usando las siguientes interfaces:

Interfaz S1-MME: Esta es una interfaz que se maneja en el plano de control y sirve para conectar el eNB con la MME y brindar un conjunto de funciones y procedimientos de control entre estas entidades.

Procedimientos de control realizado por la interfaz S1-MME:

- Procedimiento para el establecimiento, modificación, y liberación de recursos de los servicios portadores o *bearers* tanto de la interfaz de radio (radio *bearers*) como de la interfaz S1 (S1 *Bearer,* servicios portadores S1).
- Procedimientos de traspasos entre eNBs.
- Procedimientos de *paging.*

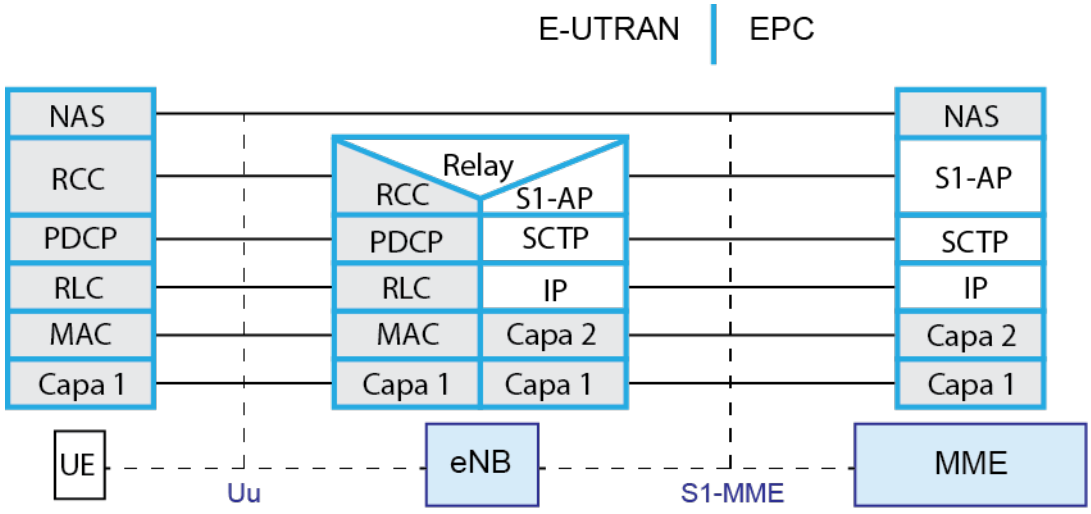

Figura 1.3.5: pila de protocolos de la interfaz S1-MME

Como se pude apreciar en la figura 1.3.5 hace uso de los siguientes protocolos:

- **SCTP (*Stream Control Transmission Protocol,* Protocolo de Control de Transmision de Flujo de datos)*:*** Desarrollado por un grupo de trabajo conocido como SIGTRAN (*Signaling Transport*, Señalización y Transporte), perteneciente a la IETF (*Internet Engineering Task Force,* Grupo de Trabajo de Ingeniería de Internet), con el objetivo de crear un protocolo capaz de transportar mensajes de señalización SS7 (*Signaling System number* 7, Sistema de Señalización número 7) de redes telefónicas sobre redes IP.

El protocolo SCTP es un protocolo de transporte que provee un servicio confiable asegurando que los datos sean transportados en la red sin errores y entregados en orden. Por ser un protocolo de transporte, el protocolo SCTP comparte características similares a los protocolos UDP y TCP, dentro de estas similitudes con TCP tenemos que el protocolo SCTP es orientado a la conexión, esto significa que todos los datos enviados entre dos extremos SCTP son transferidos como parte de una sesión o asociación a como se le conoce dentro del marco del protocolo SCTP [8].

Al igual que TCP, el protocolo SCTP es capaz de utilizar una tasa de transmisión adaptativa que podrá incrementar o disminuir dependiendo de las condiciones de tráfico de la red.

En comparación con el protocolo TCP, SCTP también es un protocolo orientado al envío de mensajes contrastando con UDP que es orientado al envió de bytes, en otras palabras el protocolo SCTP es capaz de enviar distintos mensajes en un mismo *stream* (flujo) de datos, estableciendo límites de donde empieza y termina cada mensaje, a diferencia de UDP que mezclaría el contenido de los mensajes sin saber diferenciar entre los distintos mensajes enviados.

El protocolo de transporte SCTP también ha introducido nuevas funcionalidades que lo hacen un protocolo más robusto y tolerante a fallas en comparación a TCP y UDP. Dentro de las nuevas funcionalidades introducidas por SCTP encontramos en [5] que el protocolo SCTP incorpora soporte para *Multihoming* (lo que quiere decir que las asociaciones SCTP soportan la transferencia a través de múltiples caminos entre los nodos participantes, es decir, los nodos participantes pueden disponer de múltiples direcciones IP), *Multi-Streaming* (permite que múltiples mensajes puedan enviarse en paralelo).

Dentro del núcleo EPC el protocolo SCTP es usado como el protocolo de transporte en varias interfaces, como por ejemplo en la interfaz S1-MME donde se encarga del transporte del protocolo S1-AP o en la interfaz X2 donde actúa como el protocolo de transporte del protocolo X2-AP, entre otras interfaces.

- **S1-AP:** Es un protocolo definido por la 3GPP en su TS 36.413, encargado del plano de control entre el eNB y la entidad MME. Provee servicios de señalización como el establecimiento de los servicios portadores S1 entre el eNB y la MME [9].

  Dentro de las principales funciones que ejecuta el protocolo S1-AP destacan las siguientes:

  - Establecimiento, modificación y liberación de servicios portadores de radio.
  - Creación de información de contexto inicial del UE en el eNB.
  - Brindar información acerca de las especificaciones técnicas del UE a la entidad MME.
  - Funciones *paging.*

- Transporte de los mensajes de señalización NAS entre el UE y la entidad MME.
- Reporte de localización del UE.
- Funciones de movilidad.
- Modificación de la información de contexto del UE.

El protocolo S1-AP hace uso del protocolo SCTP para él envió confiable de los mensajes de señalización que se llevan a cabo entre el eNB y la entidad MME [8]

Interfaz S10: Se encarga de interconectar entidades MME entre si además de brindar soporte al mecanismo de reubicación de la entidad MME cuando sea necesario, por ejemplo, en el caso de que una entidad MME que controla un UE deba cambiarse (debido a fallas, a la movilidad del UE, etc.), a través de la interfaz S10 se realiza la transferencia de la información del contexto de usuario entre MMEs.

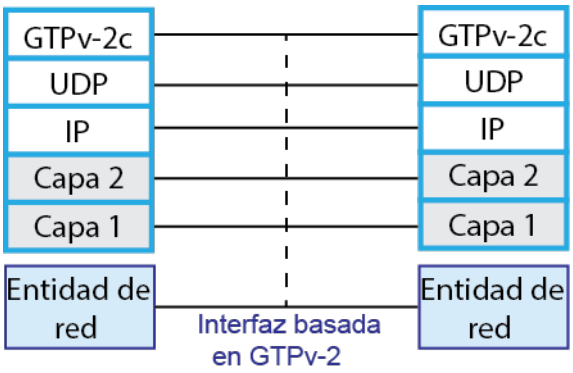

Figura 1.3.6: Pila de protocolos de interfaces basadas en GTPv-2

Como se puede observar en la Figura 1.3.6 además de los protocolos IP y UDP se define:

- **GTP-C:** La 3GPP ha definido distintas versiones para el protocolo GTP (*GPRS Tunneling Protocol,* Protocolo de Túnel GPRS) dentro del plano de control siendo GTPv2-C definido en el TS 29.247 la versión implementada por EPC, esto debido a que la versión GTPv2-C da lugar a un manejo más flexible de los distintos servicios portadores que se utilizan en el núcleo EPC, favorece a la de unificación de los distintos elementos de EPC de una manera más simple, brinda soporte a las funciones de movilidad cuando se brinda acceso al núcleo EPC a través de redes de acceso no-3GPP así como también mejoras en cuanto a la rapidez en la restauración y recuperación de elementos de red tales como MME, S-GW, P-GW, etc.

  Los mensajes de señalización y control de GTP-C incluyen funciones relacionadas con:

  - Gestiones de Movilidad.
  - Control y manejo de los servicios portadores.
  - Gestión de localización.
  - Reportes acerca del estado del terminal

Interfaz S11: Controla el plano de control en la red troncal EPC desde la entidad de red MME hacia el nodo S-GW. Esta interfaz permite la creación, modificación, eliminación y cambio de los servicios portadores EPS que los terminales tienen establecidos a través de EPC. La interfaz S11 también se encarga de dar soporte al proceso de reubicación de la entidad S-GW asociada a un terminal mediante la transferencia de información de contexto (información relacionada al plano de control) del terminal desde la entidad S-GW antigua hacia la nueva entidad S-GW.

Al igual que la interfaz S10 está basada en GTPv-2c [Figura 1.3.6]

Interfaz S6a: Permite la transferencia de información entre la base de datos HSS y la entidad MME.

A través de la interfaz S6a se le da soporte a las siguientes funciones [8]:

- Mantenimiento de información de gestión de la localización.
- Autorización de acceso a la red LTE.
- Autenticación de los usuarios.
- Notificación y descarga del módulo P-GW que utiliza un usuario en una conexión.
- Intercambiar información acerca de la localización del UE.

Esta interfaz también es capaz de brindar soporte en casos de *Roaming* (Itinerancia) donde una entidad MME de la red de un operador pueda acceder a la base de datos HSS de otro operador.

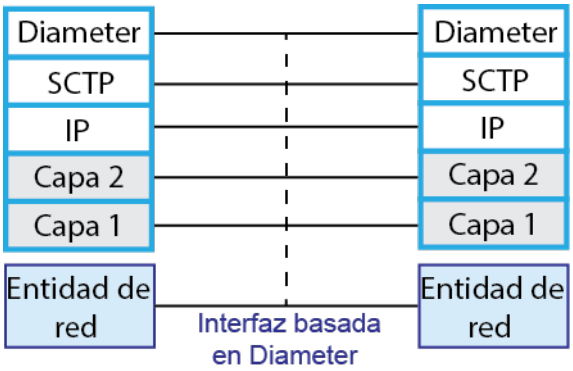

Figura 1.3.7: Pila de protocolos de interfaces basadas en Diameter

Además de los protocolos IP y SCTP se utiliza:

- ***Diameter*:** Es un protocolo diseñado para brindar soporte a funciones AAA *(Authentication, Authorization and Accounting,* Autenticación, Autorización y Contabilidad*)*. El protocolo *Diameter* brinda soporte AAA a aplicaciones que involucran acceso a redes IP móviles. Debido a la importancia de los servicios AAA el protocolo *Diameter* realiza la transferencia de sus mensajes a través de los protocolos TCP o STCP en lugar de UDP.

El protocolo *Diameter* fue definido por la IETF (RFC 3588) como un protocolo base que la mayor parte del tiempo no se utiliza solo, a menos que se use para funciones de *accounting* ya que las demás funciones (autenticación y autorización) son consideradas como aplicaciones que soportan las funcionalidades básicas del protocolo. Estas aplicaciones son extensiones adicionales que se pueden ir agregando conforme sea necesario dependiendo del uso que se le vaya a dar. Es importante destacar que dentro del marco del protocolo *Diameter,* una aplicación no representa un programa en si, sino un protocolo basado en *Diameter*.

Dentro de las redes de comunicación inalámbricas, el protocolo *Diameter* es usado para la transferencia de información relacionada con el perfil del subscriptor que puede contener datos ligados a parámetros de autenticación, tarificación, QoS (*Quality of Service,* Calidad de Servicio) y movilidad. Esta información es transferida entre los distintos nodos de la red a través de las interfaces basadas en el protocolo *Diameter* dentro del núcleo EPC ya sea de manera local o en modo *roaming.*

De una manera general podríamos agrupar las funciones de estas interfaces en:

- Autenticación, registro, autorización.
- QoS relacionado al ancho de banda.
- Tarificación.
- Localización.

El protocolo *Diameter* es considerado como un protocolo *peer-to-peer* (par a par) donde cada nodo o entidad que utilice el protocolo puede realizar las funciones de cliente, agente o servidor [10].

- Cliente: Aquellas entidades que generan los mensajes *Diameter* solicitando información (MME, P-GW).
- Servidores: Las entidades que se encargan de responder las solicitudes de los clientes (HSS, OCS, PCRF).
- Agente: Quien se encarga de direccionar los mensajes entre el cliente y servidor (una entidad que realice funciones de *Home Agent*).

S-GW (*Serving Gateway*, Puerta de enlace de Servicio)

Esta encargado del enrutamiento y envió de paquetes de datos entre el eNB y el P-GW, también actúa como punto de anclaje en el plano de usuario durante un inter-eNB *handover* (de un eNB a otro eNB), lo que quiere decir que los datos enviados a un UE específico son enrutados hacia el nodo S-GW sin importar el eNB al que el UE esté conectado.

En la arquitectura típica de una red LTE podemos encontrar varios nodos S-GW atendiendo una determinada zona geográfica, pero un único nodo S-GW es asignado al

terminal móvil al igual que una sola entidad MME es asignada a un UE. La asignación del S-GW corresponde a criterios geográficos así como al balanceo de cargas [5].

Una función sobresaliente del nodo S-GW es que permite el enlace de una red LTE en su totalidad con redes de diferentes tecnologías, especialmente otras versiones 3GPP como UTRAN (*UMTS Terrestrial Radio Access,* Acceso de Radio Terrestre UMTS) o GERAN (*GSM/Edge Radio Access Network,* Red de Acceso de Radio GSM/EDGE). También almacena todos los paquetes IP dirigidos a un usuario mientras este se encuentra fuera de servicio o en estado *idle*. Así, cuando el UE pasa a un estado activo, recibe sus paquetes enviados desde el S-GW.

Otra función importante del S-GW es el manejo de los túneles a través de los cuales se envían los paquetes entre el eNB y el P-GW, la creación y modificación de estos túneles es controlada por la MME que envía comandos de control hacia el S-GW

Al igual que la entidad MME, la entidad S-GW utiliza interfaces para comunicarse a nivel de plano de control y de usuario, comparte la interfaz S11 y se definen otras:

Interfaz S5/S8: Proporciona soporte para la transmisión de paquetes de usuario entre el S-GW y el P-GW. En el caso de que ambos módulos pertenezcan a la misma red se utiliza la interfaz S5, lo opuesto seria con la interfaz S8 que es utilizada en casos de itinerancia donde el S-GW pertenezca a la red visitada (*Visited* PLMN [*Public Land Mobile Network*, Red Pública Móvil Terrestre]) y el P-GW pertenezca a la red matriz o local (*Home* PLMN).

Es importante mencionar que ambas interfaces S5/S8 admiten dos implementaciones diferentes, la primera basada en el protocolo de encapsulación GTP y la segunda implementación utiliza el protocolo PMIPv6.

- S5/S8 sobre GTP [figura 1.3.9]: Provee funcionalidades asociadas con la creación, modificación, eliminación o cambio de los servicios portadores EPS para un determinado UE dentro del EPC [11].

- S5/S8 sobre PMIPv6: Provee el manejo del encapsulamiento *(tunneling)* de los paquetes IP entre el S-GW y el P-GW figura 1.3.8.

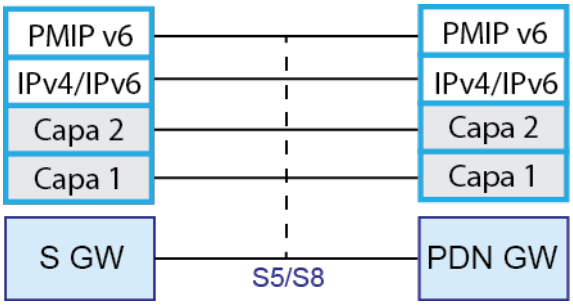

Figura 1.3.8: Pila de protocolos de la interfaz S5/S8 utilizando PMIPv6

- **PMIPv6 (Proxy Mobile IPv6)**: Es un protocolo definido por la IETF en su RFC 5213 cuya función principal es brindar soporte de movilidad a nivel de la capa de red con la finalidad de mantener la continuidad de las sesiones IP en caso de haber un cambio de red de acceso.

  Las interfaces del núcleo EPC que operan usando el protocolo PMIP utilizan la versión PMIPv6 [4] cuando trabaja con redes no-3GPP ya que normalmente para redes de acceso 3GPP se utiliza el protocolo GTP.

  Para determinar la localización del UE el protocolo PMIP define las siguientes entidades de red:

  - **MAG (*Mobile Access Gateway*, puerta de enlace de acceso móvil):** Esta entidad se comporta como un agente de movilidad que actúa como un cliente MIP (Mobile IP) en lugar del UE. Tiene la responsabilidad de detectar cualquier cambio de movimiento del UE dentro de su punto de conexión o red de acceso y así dar inicio al envió de los mensajes de señalización [8].
    Esta entidad está localizada dentro de lo que consideramos en el protocolo MIP como red visitada (nuevo punto de conexión del UE).

  - **LMA (*Local Mobility Anchor*, punto de anclaje de movilidad local):** Realiza funciones similares a un HA (*Home Agent*) ya que también se encarga de un proceso similar al *biding update* (actualización de vinculación) entre las direcciones HoA (*home of address*) y CoA (*care of adress*).
    Es considerado como un punto de anclaje a la red local del UE ya que se encuentra topológicamente localizado dentro de la misma red.

Interfaz S1-U: Proporciona un servicio de transferencia de datos de usuario entre el eNB y el S-GW sin garantías de entrega y no soporta mecanismos de control de errores ni de control de flujo ya que esta interfaz se basa en el protocolo UDP (*User Datagram Protocol,* Protocolo de Datos de Usuario) [5]. Además de UDP utiliza protocolos como IP y GTP. Al servicio de transferencia de datos realizado a través de la interfaz S1-U se le conoce como servicio portador S1.

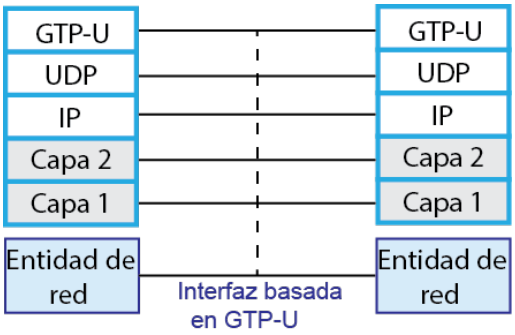

Figura 1.3.9: Pila de protocolos de Interfaces basadas en GTP-U

Como se pude observar en la gráfica 1.3.9 esta interfaz hace uso de una pila de protocolos similares a los de la figura 1.3.6 sin embargo el protocolo GTP varia debido a que ahora lleva a cabo funciones relacionadas con el plano de usuario.

- **GTP-U:** La versión de GTP-U que utiliza EPC es la versión GTPv1-U definida por la 3GPP en su TS 29.281 la función principal de GTPv1-U es encargarse del transporte de los paquetes de datos (generados en el plano de usuarios) utilizando mecanismos que describen la creación de túneles a través de las distintas interfaces basadas en GTP por donde transcurre toda la información relacionada al plano de usuario. La señalización necesaria para establecer el túnel se realiza a través del protocolo S1-AP (entre MME y eNB) y GTPv2-C (entre las demás entidades del núcleo EPC).

  Los mensajes enviados a través del protocolo GTPv1-U tienen como principal objetivo proveer un manejo fluido de los paquetes tanto en el enlace ascendente como en el enlace descendente. Es importante mencionar que los túneles GTP-U y GTP-C están asociados entre ellos para un mismo usuario, ya que su papel principal es el de establecer conexiones a través de la red para que el usuario pueda enviar y recibir datos [8]. Tanto el protocolo GTPv2-C como el protocolo GTPv1-U utilizan el protocolo UDP como protocolo de transporte.

P-GW *(Packet Data Network Gateway,* Puerta de enlace de la red de paquete de datos)

Es un módulo del núcleo EPC que ha sido definido como un punto de contacto con redes externas (IMS, Internet, Intranet, etc.) sirviendo como punto de salida y de entrada para manejar el tráfico del UE. Cada UE es asignado por defecto a un P-GW cuando se conecta a la red LTE, para tener conectividad con una o varias PDNs (*Packet Data Network,* Redes de paquetes de datos) externas como por ejemplo Internet, cada PDN es identificada por un APN (*Access Point Name,* Nombre de punto de acceso), un operador puede tener varios APN por ejemplo definir un APN para sus servidores y uno para Internet (opcional).

En caso de ser necesario a un UE se le pueden asignar múltiples P-GWs si se desea conectar con redes externas adicionales (Redes Privadas, IMS), cada P-GW se mantiene asignado al UE hasta finalizar la conexión establecida [4]. Es importante destacar que aunque existan múltiples P-GWs asignados a un UE, únicamente un nodo S-GW será el encargado de enrutar los datos provenientes de los múltiples P-GW hacia el UE.

Entre las funciones del nodo P-GW encontramos las siguientes:

- Asignar direcciones IP a los terminales móviles.
- Filtrado del contenido de los paquetes de usuario.
- Aplicación de las reglas de uso y tarificación de la red (Reglas PCC).
- Realiza funciones de HA.

Comparte la interfaz S5/S8 con S-GW además de usar la interfaz SGi:

Interfaz SGi: A través de esta interfaz se realiza la interconexión del módulo P-GW con redes IP o PDN externas, Como se puede observar en la figura 1.3.10 la interfaz SGi trabaja a nivel de la capa de aplicación directamente con el equipo.

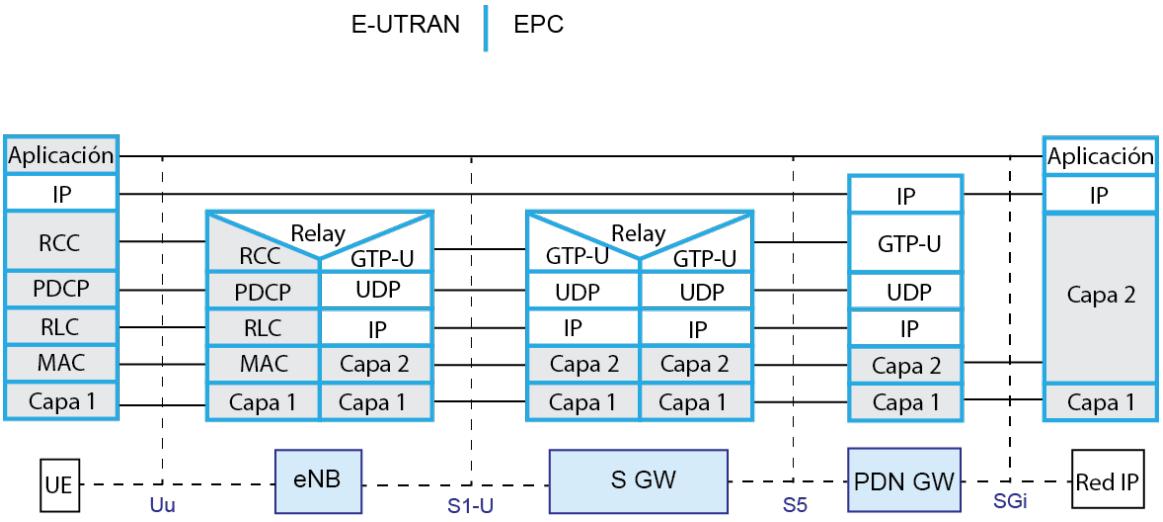

Figura 1.3.10: Pila de protocolos de interfaces desde el UE hasta una red de paquetes

HSS *(Home Subscriber Server*, Servidor de Suscriptores Locales)

Es una base de datos que contiene información acerca de los subscriptores de una red LTE [4]. La información contenida en el HSS abarca tanto información relativa a la subscripción del usuario como información necesaria para la operatividad de la red

Es importante mencionar que esta información contenida por el HSS puede ser de carácter permanente que únicamente puede ser cambiada por procesos administrativos, así como también información de carácter temporal que cambia como consecuencia de la operación del sistema.

Dentro de la información que almacena el HSS se encuentra lo siguiente:

- Identificador universal IMSI (*International Mobile Subscriber Identity,* Identidad Universal del Subscriptor Móvil) es un número único para identificar a un usuario en cualquier red.
- El número telefónico del subscriptor conocido como MSISDN (*Mobile Subscriber Integrated Services Digital Network,* Subscriptor Móvil de la Red Digital de Servicios Integrados)
- Información de autenticación de usuarios.
- La lista de *APNs* que el usuario tiene permitido acceder.
- Información de seguridad y cifrado.
- Localización del usuario en la red.
- Información necesaria para la provisión de servicios de acuerdo con las condiciones establecidas por el operador.

1.3.3. Subsistema PCC *(Policy and Charging Control,* Políticas de Tarificación y Control)

El subsistema PCC es un conjunto de elementos o entidades de red que se encargan de ejecutar funciones relacionadas con el control y admisión del flujo de paquetes de datos *(gating)*, autorización de QoS, mediciones relacionadas al uso de los recursos de la red, tarificación *(charging)*, entre otras funciones que forman parte de un conjunto de reglas conocidas dentro de EPS como Reglas PCC. El concepto de PCC fue diseñado con el objetivo de habilitar un método de control de políticas de acceso y tarificación para cada flujo de datos o SDF *(Service Data Flow,* Flujo de Servicios de Datos) que transiten a través del núcleo EPC.

La arquitectura del subsistema PCC de EPS es considerada como una evolución de la arquitectura PCC definida en el *release 7* de la 3GPP. Con el pasar del tiempo, la arquitectura del subsistema PCC ha recibido mejoras con el fin de proveer nuevas funcionalidades que faciliten la interacción de distintas redes de acceso no-3GPP. La meta de la 3GPP ha sido crear una arquitectura que sirva como marco para definir las políticas de control de acceso y QoS que sean indiferentes al tipo de tecnología de acceso que utilice el usuario final (E-UTRAN, UTRAN, GERAN, WiMAX, WLAN, etc.) [8].

Información obtenida de [5], describe que, a través del subsistema PCC se articula la interacción del servicio de conectividad proporcionado por LTE con las plataformas que sustentan los servicios finales (IMS, Internet, Intranet, etc.). Esto explica por qué los servicios portadores EPS son afines con las necesidades de transmisión de los servicios finales, ya que gracias a esta interacción, se podrán realizar cambios en los servicios portadores establecidos o modificar las reglas PCC definidas por la red en caso de que el servicio final así lo requiera y que la red LTE lo permita .

Modelo QoS.

El subsistema PCC está estrechamente ligado al concepto de QoS, es por eso que consideramos necesario hacer mención que la arquitectura del subsistema PCC opera bajo un modelo QoS conocido como "*Modelo de QoS iniciado por la red"*, donde la red hace uso de mecanismos propios para determinar las necesidades de QoS que las aplicaciones requieran y así establecer los servicios portadores adecuados.

Existe otro modelo QoS conocido como "*Modelo QoS iniciado por el móvil"*, este modelo conlleva al uso de una API *(Application Program Interface,* Interfaz de Programación de Aplicaciones) a través de la cual las aplicaciones puedan solicitar a la red el nivel de QoS que requieren, las redes del tipo GPRS hacen uso de este modelo.

Habiendo especificado el tipo de modelo QoS que utiliza la arquitectura del subsistema PCC, procederemos a definir brevemente ciertos conceptos básicos pero indispensables ya que sobre estos se fundamenta la calidad de servicio o QoS dentro de una red LTE. Dentro de los conceptos que definiremos tenemos los siguientes:

- **SDF:** Constituye la unidad mínima de agregación de tráfico sobre la que se aplican las políticas de uso y tarificación del subsistema PCC [8], Cada SDF está asociado con una regla PCC que define sus parámetros de políticas de control de acceso y tarificación.
- ***Gating*:** Es un procedimiento mediante el cual se controla y autoriza el acceso de los paquetes provenientes de redes externas y que serán enviados a través de un SDF. El procedimiento de *gating* se realiza en el nodo PCEF (en breve describiremos estos nodos y sus funciones).
- **Tarificación:** Determinan como los paquetes en un SDF serán tarificados. Este parámetro también se encarga de definir el método de tarificación a utilizar, método que puede ser de dos tipos: *Offline Charging* (para usuarios con servicios post-pago) y *Online Charging* (para usuarios con servicios pre-pago). Dentro de la arquitectura PCC el elemento encargado de la tarificación es el nodo PCEF.

Además de ser parte fundamental de QoS, estos conceptos también ayudan a determinar como la red va a manejar un servicio portador EPS en particular.

Reglas PCC.

Dentro del subsistema PCC se definen dos tipos de reglas PCC que se encargaran de determinar el trato de QoS y tarificación (entre otros parámetros) que se le brindara a los flujos SDF que transiten a través del núcleo EPC, estos dos tipos de reglas se clasifican en:

- **Reglas PCC Predefinidas:** Son reglas que la red LTE ha predefinido con anterioridad y que se almacenan en el nodo PCRF y normalmente son utilizadas cuando se requiera un nivel de QoS estándar, estas reglas PCC están ligadas al establecimiento de servicios portadores por defecto donde no se requiere un trato especial de QoS.
- **Reglas PCC Dinámicas:** A diferencia de las reglas PCC predefinidas, las reglas dinámicas se elaboran basándose en los requerimientos QoS de los servicios finales que pueda ofrecer una PDN externa. Como mencionábamos anteriormente la interacción del subsistema PCC con las plataformas que sustentan los servicios finales, permite el intercambio de información para verificar si un determinado servicio requiere un distinto nivel de QoS superior al que pudiese recibir en caso de utilizar las reglas PCC predefinidas por la red LTE.

Arquitectura del Subsistema PCC.

La arquitectura del subsistema PCC véase figura 1.3.11 está compuesta por elementos o entidades de red que se encuentran ubicados dentro del núcleo EPC como nodos independientes (nodo PCRF, nodo SPR) o como extensiones lógicas que agregan funciones adicionales a las que ejecutan los nodos básicos de EPC, tal es el caso de los nodos S-GW y P-GW que ejecutan funciones indispensables dentro del marco PCC con la singularidad de un cambio en el nombre de estos elementos por definición de la 3GPP y para una mejor comprensión de la arquitectura PCC.

La siguiente imagen es una representación gráfica de la arquitectura del subsistema PCC que nos ayudara a identificar de una manera más clara los elementos o entidades de red que definiremos a continuación.

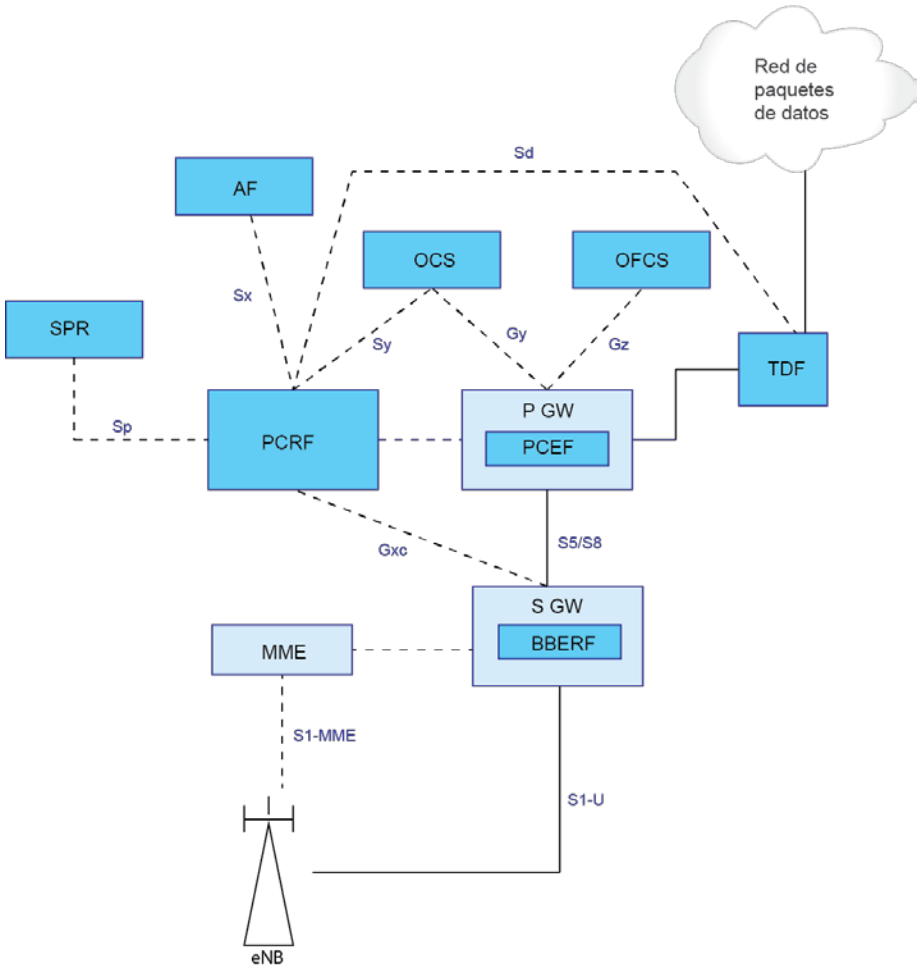

Figura 1.3.11: Arquitectura del Subsistema PCC.

Nodo PCRF *(Policy and Charging Rules Function,* Función de Políticas y Reglas de Tarificación)

Es considerado como el elemento más importante del subsistema PCC, el nodo PCRF es el encargado de suministrar las políticas o reglas PCC predefinidas por la red o de definir las reglas PCC dinámicas en caso de ser necesario. Una vez que las reglas PCC hayan sido definidas, el nodo PCRF podrá enviar estas reglas al nodo PCEF o BBERF para que se apliquen a los flujos de datos o SDFs. Como mencionábamos anteriormente cada SDF está asociado a reglas PCC predefinidas o dinámicas, las políticas indican cual será el perfil de QoS autorizado y los parámetros necesarios para el control de tarificación de cada SDF.

Para el establecimiento de reglas PCC dinámicas, el nodo PCRF interactúa con una entidad perteneciente a la red PDN externa, conocida como AF (*Applicaction Function*,

Función de Aplicación, abordado en breve), el objetivo de esta interacción consiste en el intercambio de información que suministra el nodo AF a el nodo PCRF, acerca de los requerimientos QoS de los servicios finales en dependencia del tipo de servicio al que acceda el usuario teniendo en consideración políticas de control de acceso y QoS así como también el tipo de subscripción del usuario.

Dentro de las funciones que realiza el nodo PCRF tenemos las siguientes:

- Servicio de detección de paquetes basado en el flujo de datos.
- Control de *acceso (Gating).*
- Autorización de QoS.
- Tarificación basada en el flujo de datos en el nodo PCEF [7].

Otra función del nodo PCRF es reportar a los nodos PCEF (P-GW), BBERF (S-GW) y AF acerca de eventualidades o cambios que puedan estar relacionados con variaciones en las reglas PCC, modificación o terminación de las sesiones IP o cambios en el tipo de red de acceso que utilice el UE (cambio de una red de acceso LTE a una red de acceso WLAN, WiMAX, UMTS, etc.) [8].

Nodo AF *(Applicaction Function*, Función de Aplicación*)*

El nodo AF representa cualquier entidad de la plataforma de los servicios finales que interactúe con el nodo PCRF mediante la interfaz Rx [5]. El termino AF es utilizado dentro del marco PCC, en la práctica las funcionalidades del nodo AF están contenidas dentro de un elemento específico en dependencia de la plataforma de servicios a la que se esté accediendo (por ejemplo, en el caso de que la plataforma de servicios sea IMS, las funciones de nodo AF están contenidas dentro de la entidad P-CSCF).

Nodo SPR *(Subscription Profile Repository,* Almacén del Perfil del Subscriptor)

El nodo SPR es una base de datos que fue introducida como parte de la arquitectura PCC en el *release 7* y que se ha mantenido en *releases* posteriores como un nodo independiente. La función principal del nodo SPR consiste en almacenar información relativa a las políticas de uso de la red que contempla la subscripción de un usuario.

La base de datos SPR puede indicar que servicios finales tiene autorizado un usuario en una determinada red PDN, los parámetros de QoS autorizados, categoría del UE, etc, [5].

En el caso de que el nodo PCRF carezca de algún tipo de información relacionada a las reglas PCC que han sido definidas para un usuario, podrá obtener esos datos accediendo a la base de datos SPR por medio de la interfaz Sp.

La base de datos SPR es considerada como una entidad funcional diferente de la base de datos HSS y, en la versión inicial de las especificaciones del sistema LTE *release 8* no se contempla ninguna interacción entre ambas.

Nodo PCEF *(Policy and Charging Enforcement Function,* Función de Ejecución de las Políticas y Tarificación*)*

El nodo PCEF se encarga aplicar el conjunto de reglas PCC que recibe del nodo PCRF mediante la interfaz Gx, estas reglas PCC deberán ser aplicadas a todos los flujos SDFs que han sido autorizados para transitar el núcleo EPC.

Dentro de la arquitectura general del núcleo EPC, el nodo P-GW realiza las tareas de PCEF. Dentro de las funciones que realiza podemos mencionar las siguientes:

- Control del tráfico del Plano de usuario y QoS.
- Análisis y medición de los flujos SDFs.
- Interactúa con el nodo OCS (*Online Charging System*, tarificación pre-pago) para el manejo del crédito o saldo que posee el usuario.
- Reporta la utilización de los recursos de la red (volumen del tráfico del plano de usuario, duración de una sesión) al nodo OFCS (*Offline Charging System*, tarificación post-pago).
- Ejecuta los parámetros relacionados con QoS y control de accesos en dependencia de las reglas PCC establecidas por el nodo PCRF.
- Reporta cambios en los flujos SDFs al nodo PCRF.
- Proporciona información al nodo PCRF relativa al usuario y el tipo de red de acceso utilizada (E-UTRAN o redes de acceso alternativas).

Nodo BBERF (*Bearer Binding and Event Report Function*, Función de Reporte de Eventos y Vinculación de los Servicios Portadores.)

Este nodo realiza funciones similares al nodo PCEF exceptuando las funciones de tarificación que siempre se ejecutan en el nodo PCEF.

Las funciones de BBERF se encuentran ubicadas en el nodo S-GW de EPC, en el caso de utilizar una red de acceso alternativa por ejemplo Wi-Fi, las funciones de BBERF las realizara la compuerta que brinde acceso a la red (en Wi-Fi según el *release 8* será la compuerta conocida como WAG, *WLAN Access Gateway,* Compuerta de Acceso WLAN).

La utilización de este nodo es necesaria únicamente cuando la gestión de los servicios portadores EPS no se realiza en el nodo P-GW [5], normalmente esto ocurre cuando la interfaz S5/S8 emplea el protocolo PMIPv6 en lugar del protocolo GTP o en el caso de que se acceda al nodo P-GW a través de las interfaces S2a/b/c contempladas en la interconexión con otras redes de acceso no 3GPP.El nodo BBERF se comunica con el nodo PCRF a través de la interfaz Gx.

1.3.3. IMS *(IP Multimedia Subsystem,* Subsistema Multimedia IP*)*

IMS es un subsistema que opera dentro de la arquitectura de una red móvil, este al igual que la arquitectura EPC consiste de un número de entidades lógicas que se encuentran conectadas entre sí a través de interfaces estandarizadas [8].

IMS fue desarrollado por la 3GPP y presentado oficialmente en el *release 5* y posteriormente refinado en los *release* 6 y 7, originalmente fue desarrollado con el objetivo de permitir servicios multimedia IP sobre redes GSM y CDMA, pero con el tiempo el tipo de redes de acceso se expandió hasta el punto que IMS se utiliza como una forma rentable para la entrega de servicios como la voz y SMS en una red LTE.

IMS utiliza el protocolo SIP (*Session Initiation Protocol*, Protocolo de Inicio de Sesiones) RFC 3261 como protocolo base para la señalización asociada al subsistema IMS, además de SIP, IMS emplea protocolos como Diameter y H.248.

En cuanto al desarrollo y aplicación de IMS tenemos que se ha extendido tanto a redes móviles que no forman parte de la 3GPP (redes 3GPP2, Mobile WiMAX) así como también a redes fijas (ADSL, cable, etc.).

Modelo de provisión de servicios del subsistema IMS

Según [5] el modelo de provisión de servicios del subsistema IMS está estructurado en 3 capas:

- Capa de transporte: representa la infraestructura de la red IP que proporciona el encaminamiento de los flujos IP entre terminales móviles y los demás elementos de la red, esta infraestructura podría ser una red LTE, UMTS, GSM, WiMAX, etc.
- Capa de control: se ubican los elementos especializados en la gestión de sesiones, este es el caso de los servidores de señalización SIP (o entidades CSCF que abordaremos posteriormente), así como otros elementos para la interacción con redes que utilicen la conmutación de circuitos (este es el caso de los *Media Gateways,* Compuerta de Acceso a Medios).
- Capa de aplicación: residen los servidores que albergan la lógica y datos asociados a los diferentes servicios proporcionados a través de IMS (mensajería instantánea, VoIP, etc.).

Arquitectura IMS

La arquitectura del subsistema IMS véase 1.3.12 se ubica dentro de la capa de control del modelo de provisión de servicios, las principales entidades lógicas que componen al subsistema IMS se conocen como CSCF *(Call Session Control Function,* Función de Control de las Sesiones de Llamadas*)* de los cuales existen tres tipos y varían en cuanto a su funcionamiento:

S-CSCF (Servidor CSCF): Se encarga del control de los terminales móviles de una manera similar a la MME del núcleo EPC [4]. Cada terminal se encuentra registrado a un servidor CSCF el cual se encarga del establecimiento de las llamadas con otros terminales móviles, así como también de notificar al terminal móvil cuando exista una llamada entrante.

Esta entidad también es capaz de funcionar como un nodo central de señalización en sesiones IMS.

Los servidores CSCF tienen acceso a la base de datos HSS donde también se almacena información necesaria para soportar sesiones multimedia sobre IMS.

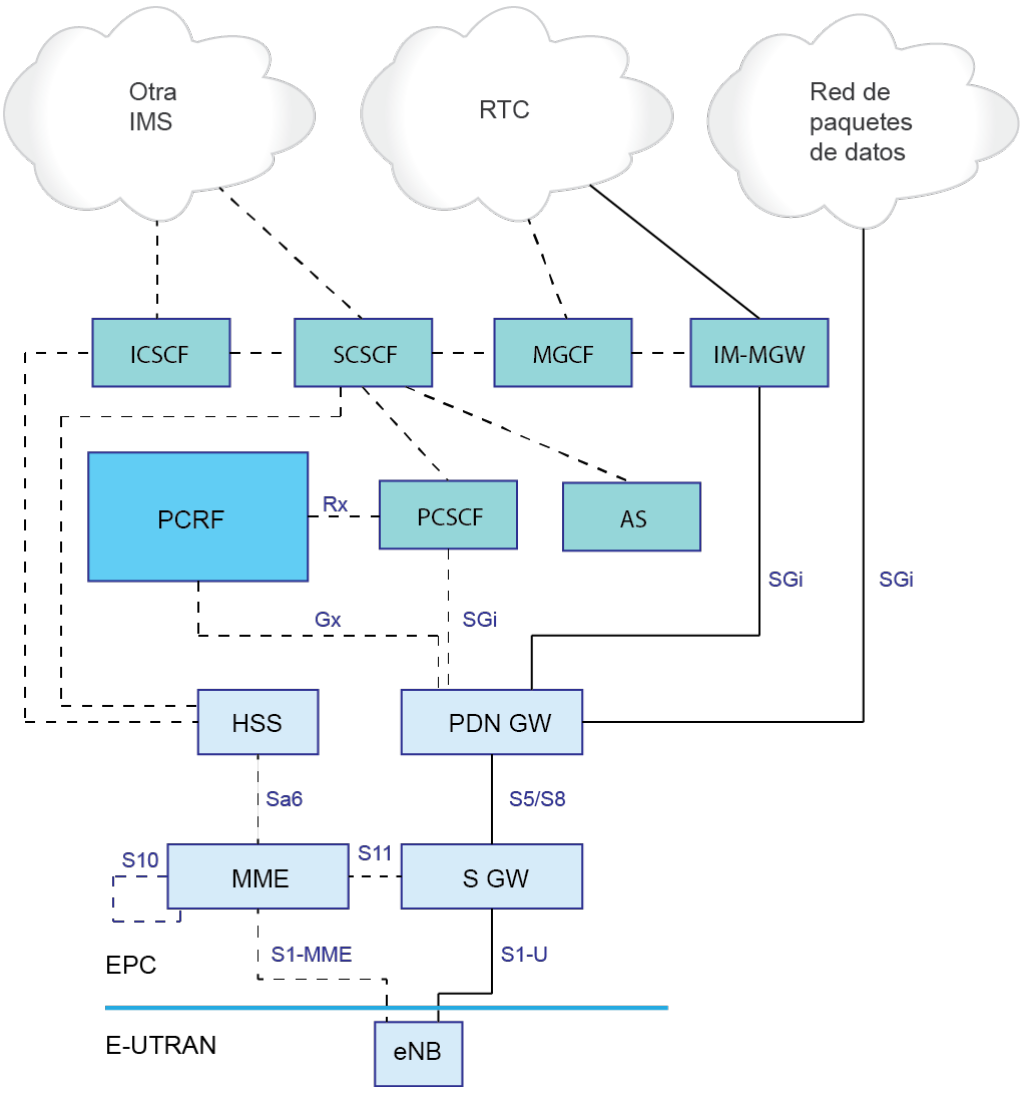

Figura 1.3.12: Arquitectura del subsistema IMS operando en conjunto con el núcleo EPC.

P-CSCF (Proxy CSCF): Esta entidad actúa como compuerta de entrada al subsistema IMS desde la red que proporciona la conectividad IP (LTE, UMTS, GSM, WiMAX, etc.) por lo que toda la señalización SIP entre los terminales y el subsistema IMS transcurre a través de esta entidad [5].

Una función importante que realiza esta entidad, es la compresión de los mensajes de señalización que el terminal móvil intercambia con IMS, esto ayuda a reducir la carga de transporte de la red que brinda el servicio de conectividad IP.

El P-CSCF es el elemento que interacciona con las funciones PCC de la red de conectividad LTE (a través del nodo PCRF). A través de P-CSCF, el subsistema IMS puede controlar la operativa de la capa de transporte (por ejemplo, servicios portadores EPS en el caso de una red LTE).

I-CSCF (*Interrogating* CSCF, Interrogador CSCF).

Se encarga de recibir los mensajes de señalización recibidos de otros subsistemas IMS externos. La entidad I-CSCF interactúa con el nodo HSS para asignar una entidad S-CSCF que maneje las sesiones SIP de los usuarios.

Por ser entidades lógicas, los tres distintos tipos de CSCF se pueden encontrar físicamente en un mismo dispositivo de hardware.

AS (*Application Server*, Servidor de Aplicación).

Es el servidor que provee al usuario el servicio final al cual desea tener acceso (puede ser un servicio de mensajería instantánea, *streaming* de video, cualquier servicio multimedia, VoIP etc.).

2. Análisis del sistema LTE integrado con la tecnología de acceso Wi-Fi

Este análisis comprende los elementos cruciales que se identificaron en una red heterogénea LTE/Wi-Fi, se aborda de manera genérica y con bases en especificaciones propias de la 3GPP y de otras organizaciones involucradas con estas tecnologías.

2.1. Interoperabilidad Wi-Fi con el sistema LTE *(release* 8**)**

EPC es un núcleo robusto fue pensado para aprovechar no solo las nuevas tecnologías sino que también es capaz de trabajar con tecnologías predecesoras de 3GPP, añadiendo ciertas entidades a la arquitectura.

3GPP fue más allá y también definió la arquitectura cuando el acceso de radio no es parte de las tecnologías de la organización a pesar que no estandariza ninguna en particular, Wi-Fi es una de las tecnologías que la 3GPP ha considerado desde *release* anteriores al 8 y siempre ha tratado de promover e integrarlo a su sistema, es por eso que EPS ofrece muchas facilidades para diseñar una red heterogénea.

Para esto, 3GPP definió en TS 33.402 dos maneras de abordar esta integración:

2.1.1 Redes no 3GPP confiables *(Trusted* non-3GPP*)*

Cuando todas las características y políticas de seguridad se consideran lo suficientemente seguras por el operador de la red celular, las redes de acceso no-3GPP son identificados como redes no-3GPP confiables, porque así lo ha considerado el operador. Estas redes de acceso no-3GPP confiables se conectan directamente con el núcleo EPC.

Cabe destacar que por la naturaleza de la tecnología Wi-Fi esta no era considera una tecnología que pudiera llegar a ser confiable debido a muchos potenciales riesgos de seguridad sin embargo en los recientes *releases* esto ha cambiado, la arquitectura definida a continuación sigue siendo muy similar al tipo de red de acceso no-3GPP confiable si se deseara implementar Wi-Fi

En la figura 1.4.1 observamos entidades ya definidas, también aparecen nuevas y por ende nuevas interfaces para comunicarse.

P-GW definido en el Apartado 1.3 se comunica utilizando las siguientes interfaces:

S2a: comunica al P-GW con la red de acceso no-3gpp confiable. Esta se utiliza de manera similar a la interfaz S5 para la trasmisión de datos del plano de control y usuario en las figuras 1.4.2 y figura 1.4.3 se pueden observar los protocolos que utiliza tanto en plano de control como plano de usuario.

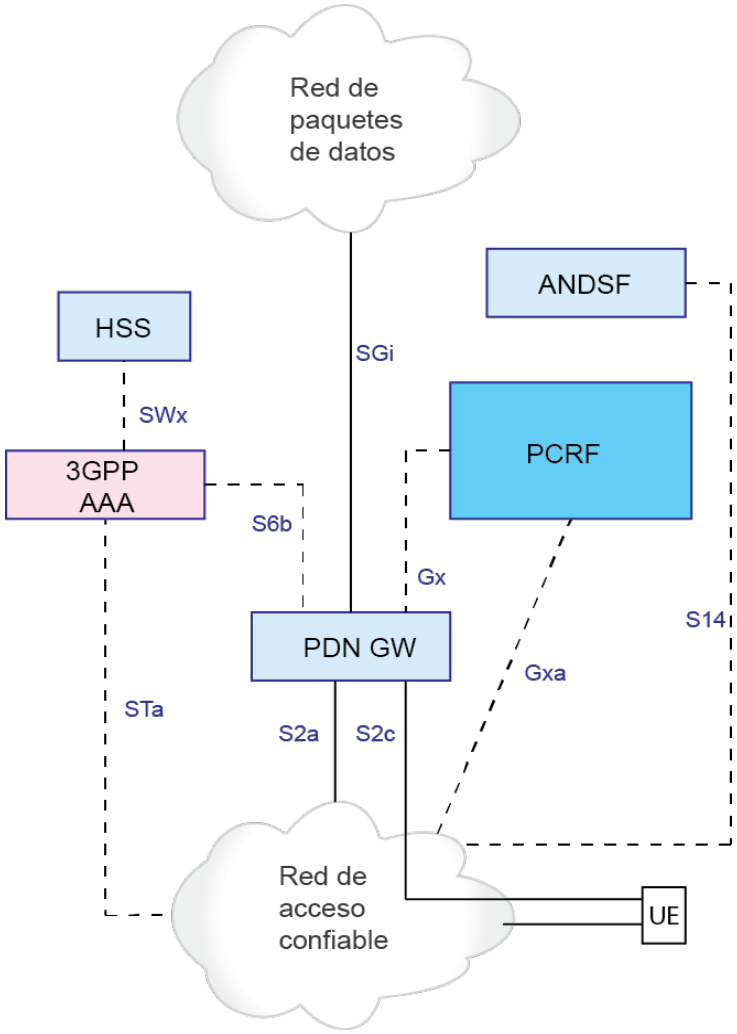

Figura 1.4.1: Arquitectura básica para una red de acceso no-3GPP confiable.

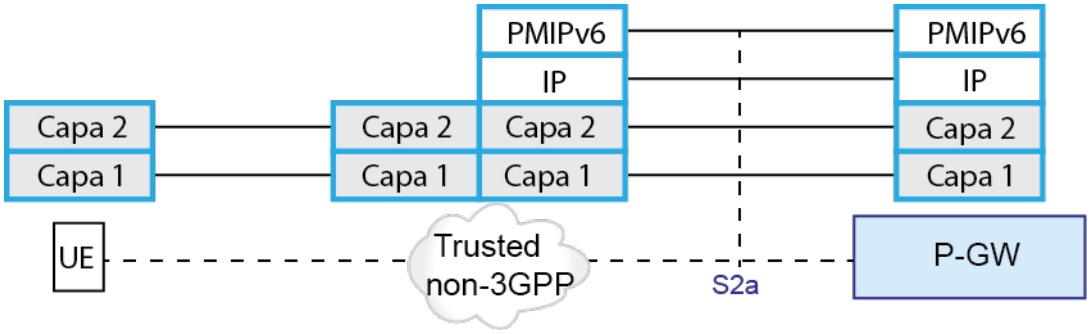

Figura 1.4.2: pila de protocolos de la interfaz S2a (Plano de control)

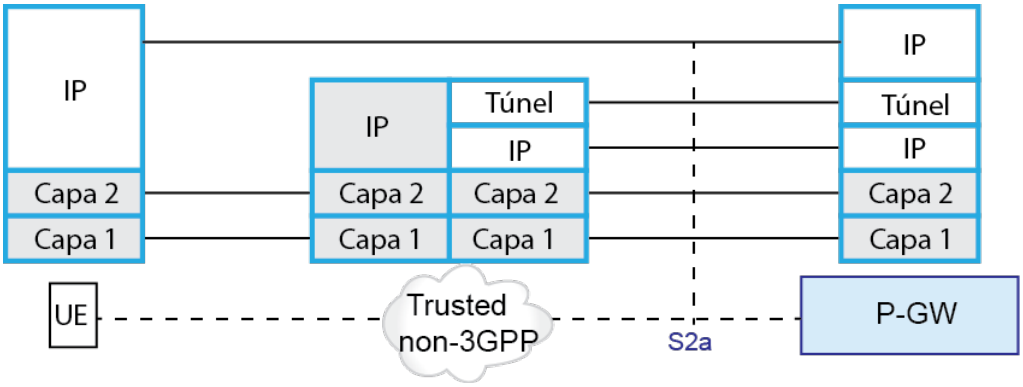

Figura 1.4.3: pila de protocolos de la interfaz S2a (plano usuario)

Como se puede observar en la *figura 1.4.3* hay un túnel que se crea entre la red de acceso no-3GPP confiable y el P-GW esto se realiza a través del siguiente protocolo:

- **Protocolo GRE *(Generic Routing Encapsulation,* Encapsulación de Enrutamiento Genérico*):*** define un método para transportar los paquetes creados por un protocolo de la capa de red (modelos TCP-IP) dentro de otro protocolo de la capa de red esto con el fin de enviar paquetes IP sobre redes donde no exista una compatibilidad nativa entre el paquete y la red (ej: un paquete IPv6 que tenga que ser enviado sobre una red IPv4 o viceversa).

  El paquete original es conocido como *payload packet* (contiene los datos a ser enviados) este ya ha sido encapsulado por un protocolo de la capa de red (IPv6 o IPv4 etc.) pero para ser enviado hacia su destino final necesita ser encapsulado dentro de un paquete GRE el cual le agregara un nuevo encabezado con la información sobre la ruta o túnel que se ha establecido para el envió de los paquetes, el paquete GRE será nuevamente encapsulado usando un protocolo de la capa 3 compatible con el tipo de red sobre la cual se enviara el paquete, una vez que el paquete es enviado y llega al punto final del túnel GRE, el encapsulamiento del protocolo de capa de red y del protocolo GRE es removido y se procede a reenviar el paquete a su destino final.

Interfaz S2c: Comunica al UE con el P-GW esta se utiliza para la trasmisión de datos del plan de control y usuario los protocolos que utiliza se observan en la figura 1.4.4 y figura 1.4.5.

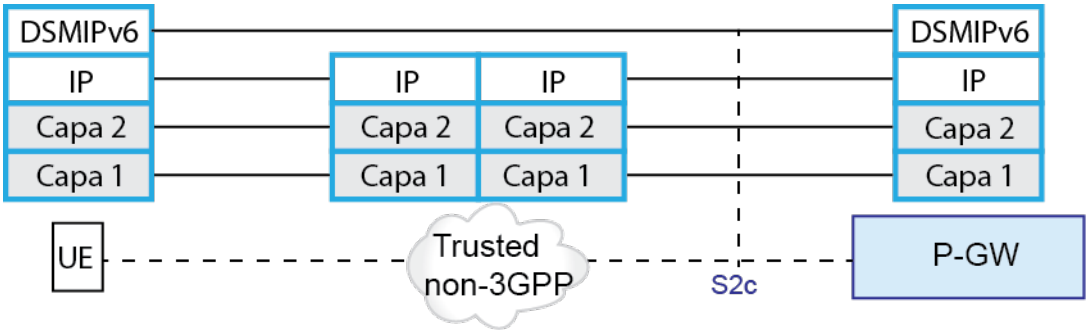

Figura 1.4.4: pila de protocolos de la interfaz S2c (Plano de control)

- **DSMIPv6 (*Dual Stack Mobile IPv6*, IPv6 móvil de pila doble):** fue definido por la IETF en el RFC 5555 con el objetivo de facilitar el uso de los protocolos de movilidad en escenarios donde coexistan redes IPv4 e IPv6.

  DSMIPv6 es considerado como una extensión del protocolo MIPv6 que permite el transporte de paquetes tanto del tipo IPv4 como IPv6 dentro del túnel que se crea entre el HA y la red que se considera como red visitada. Esta extensión permite que el dispositivo pueda moverse libremente entre redes IPv4 e IPv6 sin problema alguno.

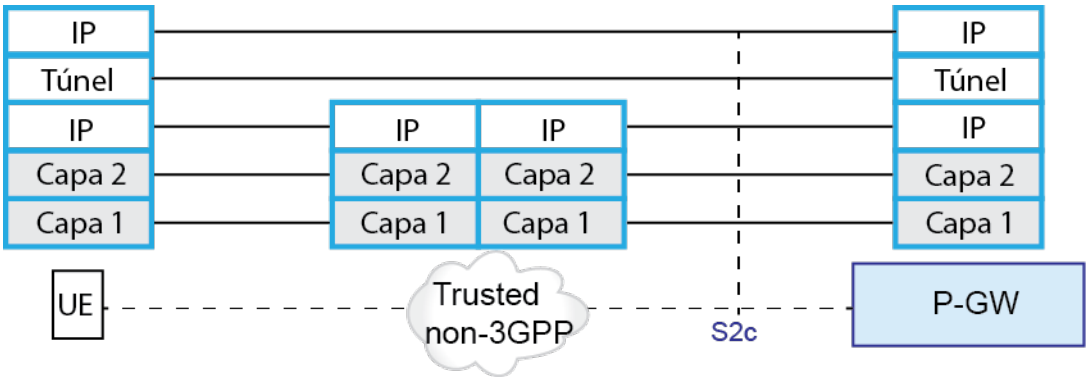

Figura 1.4.5: pila de protocolos de la interfaz S2c (Plano de usuario)

El túnel en el caso de S2c pude ser creado por:

- **Protocolo IPsec (*IP Security*, Seguridad IP):** Desarrollado por la IETF (RFC 4301), fue creado con el objetivo de brindar soporte de seguridad al intercambio de paquetes IP que viajan sobre una red IP.

  Al trabajar con paquetes IP podemos ubicar al protocolo IPsec dentro de la capa 3 del modelo de referencia OSI a diferencia de otros protocolos de seguridad como TLS *(Transport Layer Security)* y SSH *(Secured Shell)* que funcionan en capas superiores.

  En EPC es usado para asegurar las comunicaciones en varias interfaces que puedan conectar nodos de la red LTE entre sí o en interfaces que conectan al UE con el núcleo EPC.

  Para una mejor comprensión del funcionamiento del protocolo IPsec podemos dividir este proceso en dos fases que serán:

  1. Encriptación de los datos.

  Dentro de la fase de encriptación de datos tenemos que el protocolo IPsec dispone de dos protocolos capaces de realizar esta función y así brindar protección los datos:

1) ESP (*Encapsulated Security Payload*, Carga de Seguridad Encapsulada) definida en RFC 4303, Provee las funciones de autenticación, integridad y confidencialidad de los datos transmitidos a través de IPsec, el protocolo ESP protege únicamente el contenido del paquete IP (además de encabezado y tráiler ESP)
2) AH (*Authentication Header*, Cabecera de Autenticación) definida den RFC 4302. El protocolo AH provee únicamente funciones de integridad a los paquetes que se transmiten usando IPsec pero protege por completo el paquete IP (cabecera IP y cabecera AH).

Los datos generados por ambos protocolos podrán ser transmitidos usando los protocolos de transporte TCP o UDP, de igual manera ambos protocolos podrán ser utilizados tanto en modo túnel como en modo de transporte (en breves definiremos estos modos de funcionamiento).

2. El establecimiento y mantenimiento de las asociaciones de seguridad (*Security Association*, SA).

La segunda fase nos describe un procedimiento a través del cual los nodos que se comunicaran entre si comparten parámetros relacionados con claves de seguridad o algoritmos de encriptación. Para el manejo de estos parámetros de seguridad y autenticación, se crea una asociación bidireccional entre los nodos que establecen la comunicación, esta asociación se encarga de definir como los nodos se comunicaran entre si utilizando IPsec. El protocolo que utiliza IPsec para establecer y mantener una SA es el protocolo IKE (*Internet Key Exchange*) ya sea en su versión IKEv1 o IKEv2.

- **Protocolo IKE *(Internet Key Exchange, Intercambio de Claves en Internet)*:** Como ya mencionábamos anteriormente para que dos elementos de red puedan comunicarse haciendo uso del protocolo IPsec, será necesario establecer una asociación de seguridad (SA) como también una autenticación mutua entre los nodos que desean comunicarse, es aquí donde entre en juego el protocolo IKE. El protocolo IKE se encargara de negociar, establecer y mantener las respectivas SA. La finalidad de las SA consiste en que los elementos que procederán a usar el protocolo IPsec deberán de acordar de alguna manera los tipos de cifrado (AH o ESP) y algoritmos de autenticación para poder iniciar la conexión de forma segura. El protocolo IKE no solo está presente en IPsec también se le encuentra en el protocolo OSFP *(Open Shortest Path First protocol,* protocolo abierto de camino más corto*)* o el protocolo RIP *(Routing Information Protocol,* protocolo de información de enrutamiento*)*.

  Existen dos versiones del protocolo IKE: IKE versión 1 (IKEv1) e IKE versión 2 (IKEv2), siendo IKEv2 la versión utilizada por EPC al momento de establecer las asociaciones de seguridad previo a la creación de un túnel IPsec. Según [8] tenemos que la versión 2 del protocolo IKE brinda soporte para el uso del protocolo de autenticación EAP lo que se traduce en un mayor rango de credenciales de autenticación por ejemplo el uso de tarjetas SIM.

Servidor 3GPP AAA: brinda las debidas técnicas de autenticación, autorización y manejo de localización, para obtener acceso al EPS. También se encarga de coordinar la información requerida para permitir la movilidad entre redes de acceso 3GPP y no-3GPP, tales como la coordinación de información con el PGW. Interactúa con el HSS para mantener información consistente con dispositivos que son capaces de mantener la continuidad de la sesión entre 3GPP y no-3PP [12].

- **Protocolo EAP (*Extensible Authentication Protocol*, Protocolo de Autenticación Extensible)** utilizado por el servidor AAA para realizar las funciones de autentificación.

  Definido por la IETF en el RFC 3748 ha sido diseñado con el fin de proveer un marco de trabajo genérico sobre el cual se pueda definir un mecanismo específico de autenticación.
  El protocolo EAP en si no realiza el acto de autenticación, más bien se encarga de proveer un marco común a los dispositivos para que se lleve a cabo la negociación entre el terminal y el servidor de autenticación acerca del método específico de autenticación a utilizar [AAA and network sec]. El protocolo EAP se considera como un protocolo flexible y capaz de soportar múltiples métodos de autenticación de entre los cuales tenemos los siguientes mecanismos que han sido estandarizados por la IETF:

  - EAP-TLS (*Transport Layer Security*, Seguridad de la Capa de Transporte): Es un método basado en el protocolo TLS y define un método de autenticación mutua entre el terminal y el servidor de autenticación.
  - EAP-SIM (*Subscriber Identity Module*, Modulo de Identidad del Subscritor): Desarrollado como un método para autenticar subscriptores conectados a una red IP mediante el uso de una tarjeta SIM (GSM).
  - EAP-AKA (*Authentication and Key Agreement*, Autenticación y Acuerdo de Clave,): Fue creado como un mecanismo de autenticación basado en el uso de credenciales del tipo USIM (Universal Subscriber Identity Module, Modulo Universal de Identidad del Subscriptor, para redes UMTS y LTE) para autenticar a usuarios conectados a redes Wi-Fi.
  - EAP-AKA' (RFC 5448): Es una revisión al protocolo EAP-AKA que provee mejoras en cuanto al manejo de claves de seguridad.

  A través del protocolo EAP se brinda soporte para el transporte fiable de los distintos métodos de autenticación mencionados anteriormente [5].

  La estructura del protocolo EAP consta de tres elementos principales:

  - EAP Peer (par): Sera cualquier dispositivo que intente obtener acceso a la red (UE).
  - EAP *Authenticator* (autenticador): Es la compuerta de acceso (conocida como *Access Gateway*) que solicita la autenticación, esto es previo a permitir el acceso a la red (WAG o nodo ePDG).

- Servidor de Autenticación: Define el método particular de autenticación EAP que se utilizara, valida los credenciales EAP y brinda el acceso a la red (servidor AAA).

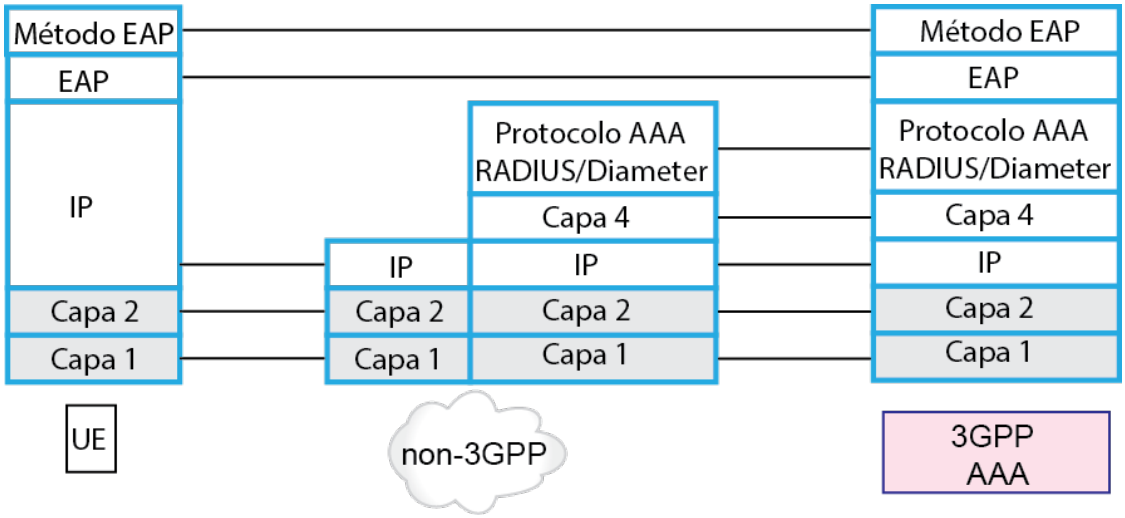

Figura 1.4.6 Estructura del protocolo EAP

Las interfaces que utiliza 3GPP AAA se basan en Diameter (*Figura 1.3.7*) y son las siguientes:

Interfaz STa: Sustenta ciertos procedimientos de control de acceso como la autenticación y autorización de los usuarios en la red no-3GPP.

A través de esta interfaz también se transporta información ligada a parámetros de movilidad en dependencia del tipo de protocolo de movilidad e interfaz a emplear en la arquitectura de la red no-3GPP confiable. Por ejemplo en el caso de utilizar la interfaz S2a y los protocolos PMIPv6 o MIPv4 los parámetros de movilidad podrían incluir información como la identidad o dirección IP del nodo P-GW y una lista de los APN con los cual el UE tiene una conexión establecida.

En el caso de la interfaz S2c y el protocolo DSMIPv6 la información relacionada con los parámetros de movilidad incluye envió de la dirección IP del HA desde el servidor AAA hasta la entidad WAG de la red no-3GPP confiable [8].

Interfaz SWx: La información que se comparte a través de la interfaz SWx está ligada a la subscripción del usuario además brinda acceso a las credenciales de autenticación USIM (*Universal Subscriber Identity Module*, Modulo Universal de Identidad de Subscriptor) para completar el proceso de autenticación del UE en el servidor AAA.

Interfaz S6b: La interfaz S6b transporta la información que el servidor AAA obtiene del nodo HSS mediante la interfaz SWx, esta información está relacionada con el perfil del

subscriptor y es enviada al nodo P-GW para gestionar el servicio de conectividad IP (por ejemplo el perfil QoS para redes no-3GPP).

Haciendo uso de esta misma interfaz, el nodo P-GW es capaz de indicar al servidor AAA su identidad o dirección IP así como también la identidad de las posibles redes externas a las que se encuentre conectado el UE información que es de vital importancia al momento de realizar el proceso de handover.

La entidad **PCRF** (*Apartado 1.3*) utiliza las siguientes interfaces basadas en Diameter (F*igura 1.3.7*):

Interfaz Gxa: Es una de las tantas interfaces relacionadas con el nodo PCRF, es a través de la interfaz Gxa que se aplican las políticas de control y QoS establecidas por el operador para garantizar una interoperabilidad que siga y cumpla con los niveles de QoS establecidos en la red 3GPP.

Interfaz Gx: Esta interfaz se utiliza para soportar el manejo de las reglas PCC ya sea instalación, modificación o eliminación de estas.

ANDSF (Access Network Discovery and Selection Function, Función de Descubrimiento y Selección de Redes de Acceso): Provee a equipos 3GPP con información acerca de las redes disponibles ya sea Wi-Fi u otra tecnología y las políticas del operador para seleccionar y usar dichas redes.

El servidor ANDSF contiene la gestión de datos y la funcionalidad de control necesarios para la detección y selección de redes. Su función primaria es seleccionar redes de acceso no-3GPP, particularmente redes basadas en 802.11 (WLAN) pero también con la capacidad de conectarse a redes como CDMA2000, WiMax, etc. Es considerado como un servicio de detección de redes móviles IP.

ANDSF fue diseñado con el propósito de proveer a los dispositivos móviles (UE) con información acerca de redes alternas para hacer cumplir las políticas para la selección y el uso de esas redes. ANDSF requiere soporte del protocolo OMA-DM *(Open Mobile Alliance Device Management)* en el dispositivo.

2.1.2 Redes no-3GPP no confiables *(non-3GPP untrusted).*

Cuando una o más de las características de seguridad no son consideradas lo suficientemente seguras por el operador local, las redes de acceso no-3GPP se consideran no confiables o como lo define la 3GPP en su TS 23.402: *non*-3GPP *untrusted*.

Este tipo de redes de acceso se pueden conectar al EPC a través de una entidad de red denominada ePDG *(Evolved Packet Data Gateway,* Puerta de enlace de Paquetes de Datos Evolucionada*).*

Como se puede ver en la *Figura 1.4.7* la entidad de red nueva que aparece es:

ePDG: Provee confidencialidad de la identidad (autenticación) del nodo móvil, además de encriptar los flujos de datos cuando el nodo está enviando información desde una red de acceso considerada como no confiable. La autenticación con este nodo es llevada a cabo usando el protocolo EAP-AKA.

El nodo ePDG utiliza las siguientes interfaces:

Interfaz SWn: Es a través de esta interfaz que se transporta la información del plano de control y del plano de usuario entre el núcleo EPC y un sistema no-3GPP no confiable [8]. El tráfico de señalización y del plano de usuario que genera la asociación lógica entre el UE y el nodo ePDG (interfaz SWu) es transferido siempre sobre la interfaz SWn

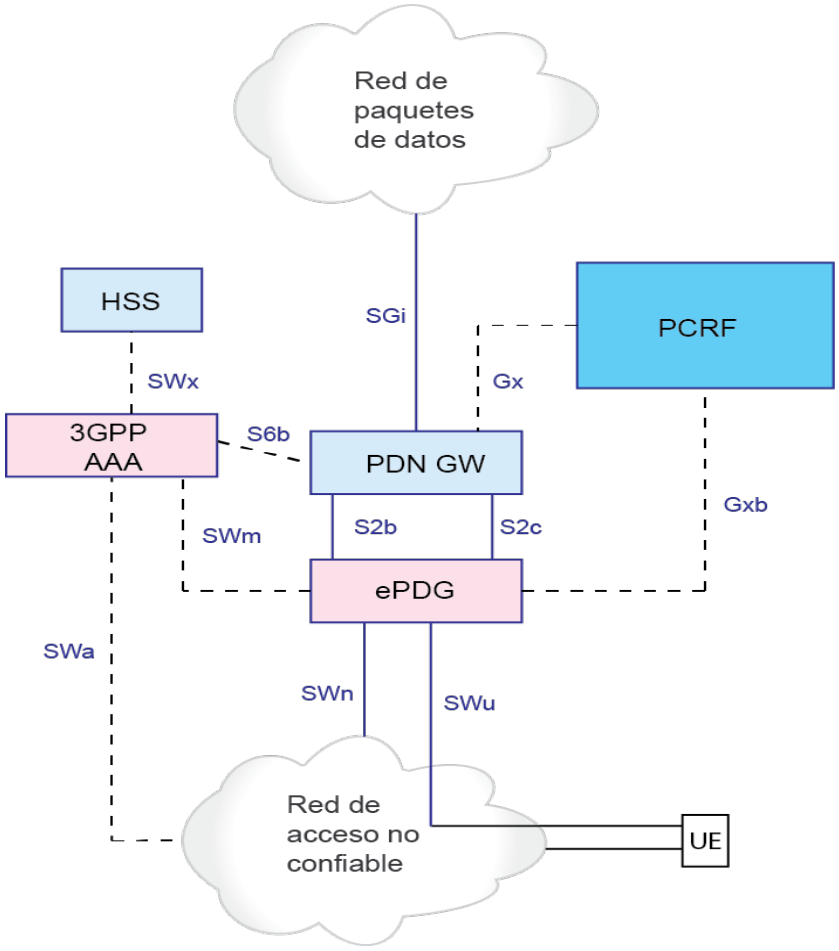

Figura 1.4.7: Arquitectura básica para una red de acceso no-3GPP no confiable.

Interfaz SWu: Brinda soporte para el establecimiento, modificación y liberación de túneles del tipo IPsec entre el UE y el nodo ePDG [8]. El UE y el nodo ePDG realizan una

asociación de seguridad haciendo uso del protocolo IKEv2 para luego proceder con el establecimiento del túnel IPsec y de esa manera garantizar un acceso seguro a los servicios del núcleo EPC.

Es importante mencionar que el establecimiento de los túneles IPsec es siempre iniciado por el UE mientras que la liberación de los mismos puede ser iniciada por el UE o por el nodo ePDG.

Tanto SWn y SWu utilizan la misma pila de protocolos véase figura 1.4.8 y figura 1.4.9:

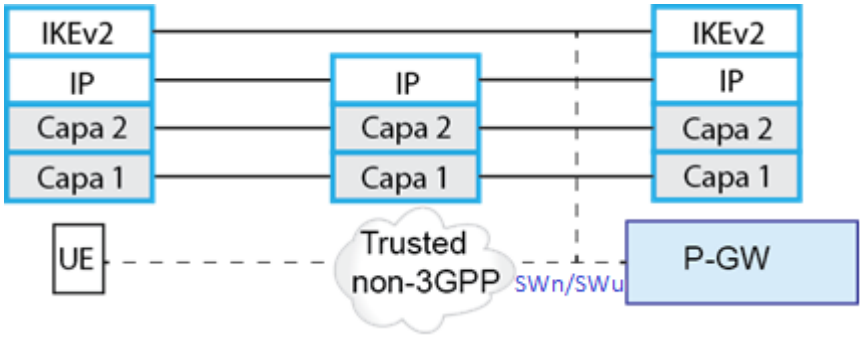

Figura 1.4.8 pila de protocolos de la interfaz SWn/SWu (plano de control)

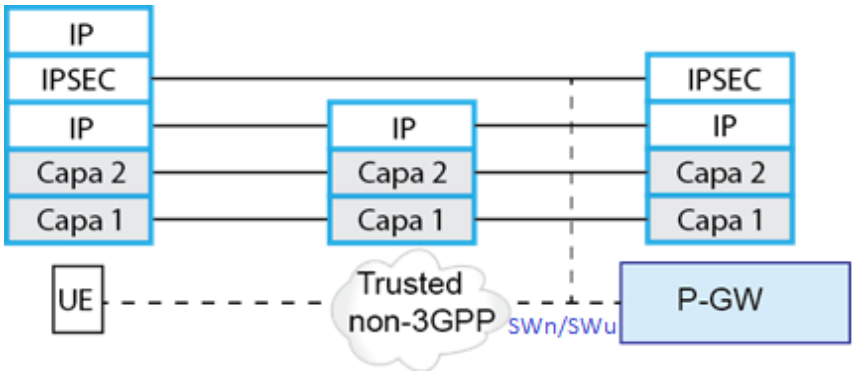

Figura 1.4.9 pila de protocolos de la interfaz SWn/SWu (plano de usuario)

En el caso de **3GPP AAA** utiliza interfaces ya definidas (SWx y S6b) y aparecen nuevas, todas basadas en Diameter (*Figura 1.3.7*):

Interfaz SWa: Esta interfaz es similar a la interfaz STa definida en el sistema para redes de acceso no-3GPP confiables ya que realiza las mismas funciones de autenticación y autorización, la diferencia radica en que ahora estos servicios se brindan a un sistema no-3GPP no confiable.

I**nterfaz SWm:** Esta interfaz se encarga de las siguientes funciones:

- Autenticar y autorizar al usuario al momento del establecimiento del túnel IPsec entre el UE y el nodo ePDG.

- Transportar la información relacionada al perfil del subscriptor desde el servidor AAA hasta el nodo ePDG.
- Transportar información relacionada al tipo de movilidad IP seleccionada (acerca de las funciones soportadas por el nodo ePDG) [8].

La interfaz SWm también comparte similitudes en cuanto a funcionamiento con la interfaz S6b del sistema no-3GPP confiable ya que también es capaz de transportar información relacionadas con ciertos parámetros de movilidad en dependencia de la interfaz y protocolo a utilizar (S2b y PMIPv6, S2c y DSMIPv6).

Como se puede observar la entidad **P-GW** mantiene las interfaces (S6b, Gx, Sgi, S2c) con la diferencia que S2c se comunican con el ePDG y no con la red de acceso *non*-3GPP y además se define una entidad nueva:

La interfaz S2b: Es homologa a la interfaz S2a ya que de manera similar hace uso tanto del mecanismo *network-based* como del protocolo PMIPv6 para brindar soporte de movilidad dentro de la capa de red. Otra similitud que comparte con la interfaz S2a es que se encarga de manejar el tráfico del plano de usuario haciendo uso del protocolo GRE para el establecimiento y manejo de túneles entre las entidades P-GW y ePDG.

La entidad **PCRF** mantiene su interface Gx pero también se comunica con el ePDG a través de:

Interfaz Gxb: Esta interfaz realiza la interconexión entre el nodo PCRF y la nueva entidad para redes de acceso no-3GPP no confiables, ePDG. Las funciones de la interfaz Gxb están relacionadas con la transferencia de las políticas de control y QoS de la red del operador hacia la entidad ePDG para que sean aplicadas al tráfico generado en un sistema de interoperabilidad.

2.2. Interoperabilidad Wi-Fi / LTE con *releases* posteriores

Release 9

En el *release 9* se introduce el concepto de LIPA *(Local IP Access,* Acceso IP Local*)* partiendo de las técnicas de interoperabilidad ya establecidas en el *release* 8 para redes de acceso no-3GPP. LIPA es un mecanismo mediante el cual un UE que se encuentre conectado a un *Home Node B* (3G) o *Home eNode B* (4G), es capaz de transferir datos a una red de área local (LAN) conectada al mismo HNB o HeNB sin necesidad de atravesar todo el núcleo EPC de la red LTE, este mecanismo aporta beneficios mínimos al núcleo de la red en términos de descarga de tráfico pero reduce considerablemente la latencia que el usuario experimentaría en el caso de que los datos viajasen a través de todo el núcleo EPC. El uso de LIPA se aplica únicamente a redes pequeñas que utilicen un HeNB o Femto-celda como fuente de acceso a los servicios de conectividad proporcionados por el operador.

Otra de las mejoras que se añadieron en el *release 9* que favorecen a la interoperabilidad con redes Wi-Fi es que se incrementan las capacidades y funciones del servidor ANDSF, el cual desde el *release 9* permite su operación en el caso de enfrentar un escenario *roaming* donde existirá una interacción entre un *Home*-ANDSF (para la red local) y un *Visited*-ANDSF (para la red visitada) [8].

Release 10

Los siguientes mecanismos que describiremos han sido publicados en el *release 10* de la 3GPP y contribuyen con la creación de una red heterogénea, la selección y descarga de tráfico y sobre todo la interoperabilidad con redes del tipo Wi-Fi a nivel macro y micro.

IFOM *(*IP *Flow Mobility,* Movilidad de Flujos IP*)*

Esta técnica de descarga y selección de tráfico permite al UE establecer varias sesiones de datos con una misma PDN de manera simultánea sobre una red LTE y Wi-Fi. Para que esta técnica se ejecute es necesario el uso del protocolo DSMIPv6 que permitirá al UE establecer sesiones tanto en redes IPv4 como en redes IPv6 o encapsular tráfico IPv6 para ser transportado sobre redes IPv4 o viceversa.

El UE será capaz de agregar o eliminar sesiones de datos usando cualquiera de las dos redes de acceso pero siempre guiándose bajo los parámetros técnicos que ha establecido el operador y que son enviados al UE haciendo uso de las políticas ISRP del servidor ANDSF, que nuevamente ha sido actualizado en este *release* para llevar a cabo esta y otras funciones esenciales en el manejo y descarga del tráfico de datos a redes de acceso alternativas.

MAPCON *(Multiple Access PDNs Connectivity,* Conectividad de Acceso Múltiples PDNs*)*

Como su nombre lo indica el mecanismo MAPCON provee al terminal móvil con la capacidad de establecer múltiples sesiones de datos con distintas PDNs haciendo uso de diferentes redes de acceso por ejemplo LTE y Wi-Fi.

Las conexiones entre las distintas PDNs son independientes una de la otra, esta es una técnica de selección y descarga de tráfico que ayuda al operador a liberar la carga de la red.

Un ejemplo que podemos citar es el de un usuario con una subscripción con el mismo operador que le permita acceder a ambas redes de acceso (LTE y Wi-Fi) donde el UE ha sido configurado a través de las políticas ISRP del servidor ANDSF para habilitar el modo MAPCON [8] y así seleccionar y enviar el flujo de datos que deberá fluir sobre LTE o sobre Wi-Fi.

Una característica importante del mecanismo MAPCON es que para lograr establecer estas sesiones de datos con distintas PDN, se hace uso de distintas direcciones IP en ambas redes de acceso que pueden ser intercambiables entre las mismas (LTE o Wi-Fi),

pero no modificadas. El uso de múltiples PDNs es controlado por el núcleo EPC y está basado en las políticas y condiciones que ha definido el operador en la subscripción del usuario.

Release 11

Como parte de las mejoras en términos de interoperabilidad de LTE con redes Wi-Fi dentro del *release* 11 se define el considerar las redes Wi-Fi como redes de acceso no-3GPP confiables, con el fin de mejorar la experiencia del usuario y proveer a los operadores con un modelo de interoperabilidad enfocado a un acoplamiento más estrecho entre las redes Wi-Fi y el núcleo EPC.

También se define formalmente el empleo de la interfaz S2a para un modelo de interoperabilidad con redes no-3GPP confiables haciendo uso de redes Wi-Fi, este modelo había sido detallado anteriormente en el *release 8* pero en ese momento el enfoque estaba dirigido a redes WiMAX o CDMA, además de esto se añade soporte para usar el protocolo GTP sobre la interfaz S2a.

Release 12

Según [13] en cuanto a interoperabilidad con redes Wi-Fi, el *release 12* se enfoca en mejoras que apuntan a un incrementos en la fluidez de procesos como; traspasos o *handover* donde el usuario final no resienta el cambio de red de acceso ya sea por degradación o interrupción de servicios, también se considera el despliegue y control de los puntos de accesos Wi-Fi por parte del operador de la red LTE.

El servidor ANDSF continuara jugando un papel importante en cuanto a la selección inteligente de los puntos de acceso para lo cual también se plantea la integración o colaboración del mismo en conjunto con *Hotspot 2.0* desarrollado por Wi-Fi Alliance.

2.3. WLAN

3GPP define métodos de interoperabilidad con redes de acceso que no son desarrolladas por ellos, en nuestro caso la tecnología Wi-Fi o WLAN.

Hay que destacar que WLAN se consideraba una tecnología no confiable en este caso se utilizan las entidades, interfaces y protocolos definido en el *capítulo 2.1*, WLAN en este caso sería similar al de la figura 2.2.1

WLAN depende del diseño, este puede variar mucho con respecto al de la figura 2.3.1, siempre va a estar en dependencia de las características deseadas y del fin que tenga esta red de acceso.

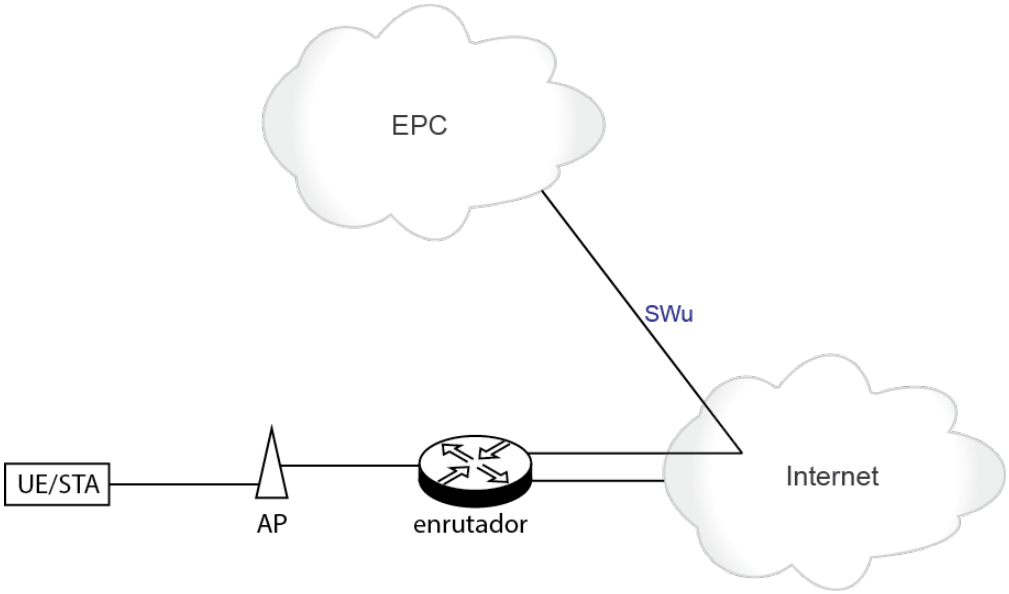

Figura 2.3.1: elementos de una WLAN básica

Entre las variantes nos encontramos con el tipo de AP:

- ***Autonomous* AP (AP autónomos):** es cuando el AP realiza todas las funciones relacionadas con IEEE 802.11 y se comunica a través de protocolos ya definidos para LAN como lo es 802.3 en este caso el AP de la figura 2.3.1 sería un AP autónomo.

  En este caso en particular cada AP autónomo es considerado una red aparte en todo caso un BSS y cada AP deberá ser configurado uno por uno, para poder contar con una ESS se depende de las configuraciones y capacidades del dispositivo como tal.

- **Thin AP (AP reducido):** estos son los AP de un modelo centralizado donde las funciones 802.11 son divididas entre los *thin* AP y un nodo central llamado controlador WLAN que tiene funciones de configuración, control y manejo, las funciones varían dependiendo de los equipos y sus características tanto para el controlador como para los *thin* AP

Estos son los dos tipos principales de AP sin embargo existe muchas variantes ya sean mezclas, tecnologías propietarias y nuevas tendencias, lo importante es que la red WLAN sea capaz de conectarse al EPC al trabajar con los protocolos de las interfaces correspondientes.

WLAN también puede ser utilizado como red de acceso no-3gpp confiable sin embargo la organización 3GPP ha hecho un gran esfuerzo al facilitar su adopción y ha añadido ciertos requerimientos en sus documentos dado que en el reléase 8 define redes tales como WIMAX, CDMA2000 etc..., sin embargo no habla nada de WLAN si no hasta el reléase 11 donde define requerimientos que se pueden observar en la Figura 2.3.2:

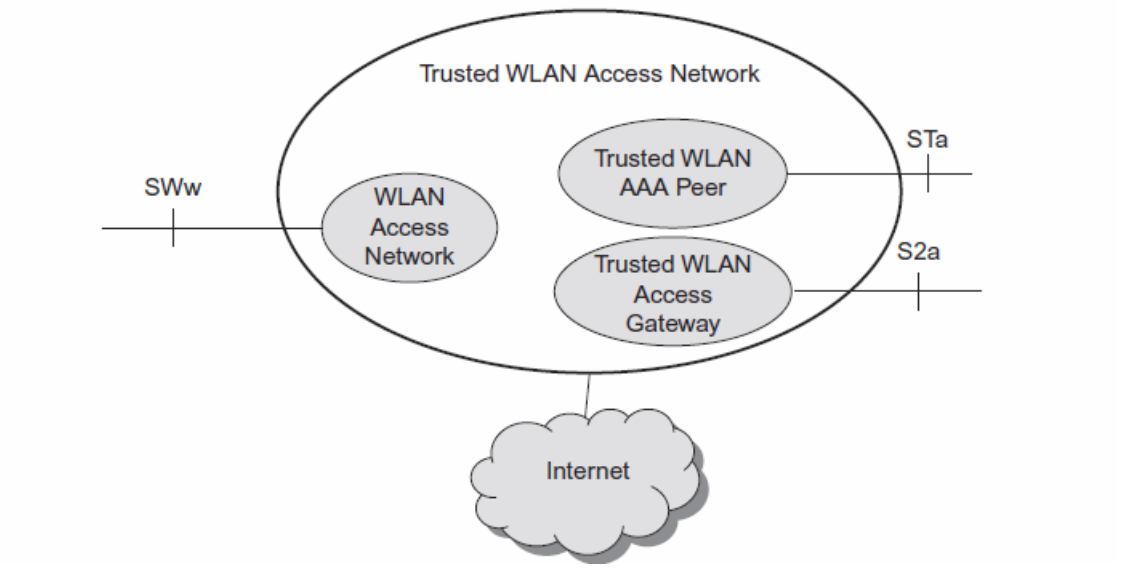

Figura 2.3.2: funcionalidad de una red de acceso WLAN confiable
Extraído de [8]

En la figura 2.3.2 observamos que la organización 3GPP define dos especies de entidades dentro de la red WLAN para terminar las interfaces que se conectan con el núcleo, esto indica cierto control o confiabilidad del operador hacia esta WLAN.

En la práctica la red WLAN confiable puede llegar a ser muy similar a la figura 2.3.1 dado que lo que varía es la capacidad del equipo físico y la decisión que tome el operador acerca de su interés de contar con una red WLAN confiable.

Tanto para WLAN confiables como para WLAN no confiables, es indispensable que los equipos ya sean puertas de enlace o AP sean capaces de trabajar con los protocolos de las interfaces correspondientes

2.3.1 HOTSPOT 2.0

También conocido como Wi-Fi *Certified Passpoint*, es un estándar desarrollado por la Wi-Fi Alliance y la WBA *(Wireless Broadband Alliance)* con el fin de permitir a los usuarios conectarse a redes Wi-Fi de manera automática y segura sin tener que emplear requerimientos adicionales de autenticación. En escenarios donde existan múltiples puntos de acceso Wi-Fi con soporte para Hostpot 2.0, el usuario podrá conectarse libremente a los distintos APs incluso al realizar un traspaso de un determinado AP hacia otro AP siempre y cuando existan acuerdos entre el propietario del punto de acceso y el operador de la red celular considerada como la red local del terminal móvil.

El principal objetivo de HS2.0 consiste en imitar un comportamiento similar al roaming de una red celular asegurándose que el usuario final pueda acceder a las redes Wi-Fi de varios proveedores (redes Wi-Fi de ISPs, redes públicas, redes privadas, etc) sin la intervención del usuario. Este estándar está basado en el protocolo 802.11u por tanto retoma el uso de los protocolos y servicios empleados en 802.11u tales como ANQP y GAS.

Funcionamiento: Primeramente tenemos que el punto de acceso se encuentra transmitiendo en su *beacon* que es un AP con soporte para HS2.0, adicional a esta información, el AP difunde información relacionada a los operadores que pueden acceder a ese AP en específico. El terminal móvil (que deberá soportar el uso de 802.11u) verifica si posee los credenciales pertenecientes a alguno de los operadores difundidos por el AP, en caso de poseer alguno de los credenciales autorizados, procede a autenticarse haciendo uso del protocolo 802.11X. Los credenciales soportados incluyen:

- SIM
- USIM
- Certificados X.509
- Nombre de usuario y contraseña
- Dirección MAC del terminal móvil

Estos credenciales podrán estar asociados a una de las variantes del protocolo de autenticación EAP.

2.3.2. 802.11u

Este *admentment* fue creado por la IEEE y titulado como *Interworking with External Networks* en febrero del año 2011.Este protocolo le permite a los puntos de acceso con soporte 802.11u, difundir en su *beacon* mayor cantidad de información o parámetros que en su mayoría están relacionados con la calidad de servicio, carga de la red, tipo de red, entre otros, en contraste con los puntos de acceso comunes que únicamente difunden en su *beacon* el SSID de la red Wi-Fi. Este protocolo es sumamente útil en lugares donde existen múltiples puntos de acceso Wi-Fi y donde el UE no cuenta con una manera de determinar que punto de acceso será conveniente utilizar (aquel que provea mejor servicio, que sea más rápido, que tenga mayor seguridad).

Este protocolo también es util en localidades donde el acceso Wi-Fi es provisto por varios APs relacionados entre ellos como parte de un ESS también conocido como *Homogeneous* ESS (HESS). 802.11u agrega los elementos de información necesarios para la interoperabilidad entre los APs tales como el identificador HESSID que permite a los terminales móviles el identificar que APs pertenecen al mismo HESS [14].

Otra de las bondades de este protocolo es que permite al UE determinar lo siguiente:

- Si el tipo de red Wi-Fi es pública o privada.
- El tipo de servicios autorizados por la red.
- Si el uso de la red Wi-Fi demanda un pago por el uso del servicio.
- Los servicios de emergencia disponibles.

Todo esto sin necesidad de que el equipo o terminal móvil haya realizado algún tipo de asociación con el AP. La capacidad de obtener este tipo de información sin que exista alguna asociación entre el terminal móvil y el AP es introducida por medio del protocolo ANQP *(Access Network Query Protocol)* que implementa el uso del servicio GAS (*Generic*

Advertise Service, Servicio Generico de Difusion) el cual le permite al terminal móvil ejecutar una sesión *query/response* con el AP sin tener que asociarse a este, esta sesión le permitirá al terminal móvil obtener información más detallada acerca del AP al cual desea asociarse.

Funcionamiento: El UE detecta la presencia de un dispositivo (AP) con soporte GAS por la información contenida en el *beacon* difundido por el mismo, el dispositivo procede con el envió de un mensaje GAS “Solicitud Inicial” al AP, el cual puede solicitar información adicional a un servidor de difusión. El AP tendrá cierto tiempo para responder el mensaje que recibió del UE (“Solicitud Inicial”) y responde con un mensaje GAS “Respuesta Inicial”. En caso de que la información envida por el AP en el mensaje GAS “Respuesta Inicial”, exceda el tamaño máximo de la PDU y por lo tanto no encaje en el mensaje GAS “Respuesta Inicial”, el dispositivo deberá enviar una o más solicitudes GAS “Repetir/Completar” para obtener la información restante, para finalizar con el proceso, se procede a la autenticación del equipo con el AP [14].

2.4. Dispositivo

EL dispositivo es un elemento vital para LTE y Wi-Fi, las redes presentan múltiples entidades componentes y protocolos, muchas de estas tienen que tener una contraparte en el proceso de comunicación con el equipo, es por eso que la percepción, rendimiento y calidad de la comunicación no solo está en dependencia de la red sino también del equipo que se utilice.

El dispositivo hasta el momento ha sido definido como:

- UE para EPS
- STA para IEEE 802.11

En la práctica este dispositivo es el mismo, valiéndose de hardware y software que le permite la interoperabilidad entre estas dos tecnologías, de hecho, incluso al mismo tiempo, entre los tipos de dispositivos nos podemos encontrar:

Sistemas de cómputo

- Teléfonos celulares
- Computadoras
- Tabletas
- Cualquier dispositivo que cuente con un procesador, sistema operativo e interfaces que le permitan operar con Wi-Fi y LTE.

Sistemas de monitoreo remoto

- Sistemas de control
- Sistemas de vigilancia

Existen dispositivos que su tarea es convertir de una tecnología a otra:

- **Router:** este no difiere mucho de las funciones de un enrutador, sin embargo tiene la capacidad de tomar la señal LTE y redistribuirla vía Wi-Fi, Ethernet, WAN o cualquier característica u otra tecnología definida por el fabricante.
- **Mi-Fi:** toman la señal celular en este caso LTE y la redistribuyen a través Wi-Fi para brindar acceso a internet a dispositivos compatibles.
- **Módems USB (*Universal serial bus*, bus universal serial):** toman la señal celular para brindar acceso a internet a una computadora a través de un enlace serial USB.

El dispositivo tiene que ser compatible con ambas tecnologías.

2.4.1. Dispositivo en LTE

Para esto diferentes fabricantes desarrollan tecnología específica para poder integrarse a los dispositivos, muchas veces estos son circuitos integrados que hacen uso del poder de procesamiento y de software para proporcionar un mejor funcionamiento así como nuevas características.

3GPP define los parámetros y técnicas que el equipo tiene que realizar, muchos de ellos se pueden encontrar en Tabla 1.3.1 así mismo las bandas en las que puede trabajar están definidas en la Tabla 2.4.1

3GPP ha designado categorías a los equipos de las cuales ciertos requisitos deben ser cumplidos esto indica al usuario la capacidad y el rendimiento que se puede esperar, las tablas 2.4.2 y 2.4.3 definen ciertos parámetros, en [Figura 6.2.2] se puede observar la categoría en las especificaciones técnicas de un equipo móvil celular.

Además de trabajar con las capas 1 y 2 como se pude observar en los gráficos de las interfaces en el apartado 1.3 el UE tiene que ser capaz de soportar todos los protocolos pertinentes.

UE Category	Maximum number of DL-SCH transport block bits received within a TTI	Maximum number of bits of a DL-SCH transport block received within a TTI	Total number of soft channel bits	Maximum number of supported layers for spatial multiplexing in DL
Category 1	10296	10296	250368	1
Category 2	51024	51024	1237248	2
Category 3	102048	75376	1237248	2
Category 4	150752	75376	1827072	2
Category 5	299552	149776	3667200	4

Tabla 2.4.2: valores de parámetros de capa 1 asignados a su categoría correspondiente
Extraído de: 3GPP TS 36.306 V8.9.0 (2013-03)

E-UTRA Operating Band	Uplink (UL) operating band BS receive UE transmit	Downlink (DL) operating band BS transmit UE receive	Duplex Mode
	F_{UL_low} – F_{UL_high}	F_{DL_low} – F_{DL_high}	
1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
4	1710 MHz – 1755 MHz	2110 MHz – 2155 MHz	FDD
5	824 MHz – 849 MHz	869 MHz – 894MHz	FDD
6	830 MHz – 840 MHz	875 MHz – 885 MHz	FDD
7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
9	1749.9 MHz – 1784.9 MHz	1844.9 MHz – 1879.9 MHz	FDD
10	1710 MHz – 1770 MHz	2110 MHz – 2170 MHz	FDD
11	1427.9 MHz – 1447.9 MHz	1475.9 MHz – 1495.9 MHz	FDD
12	699 MHz – 716 MHz	729 MHz – 746 MHz	FDD
13	777 MHz – 787 MHz	746 MHz – 756 MHz	FDD
14	788 MHz – 798 MHz	758 MHz – 768 MHz	FDD
17	704 MHz – 716 MHz	734 MHz – 746 MHz	FDD
...			
33	1900 MHz – 1920 MHz	1900 MHz – 1920 MHz	TDD
34	2010 MHz – 2025 MHz	2010 MHz – 2025 MHz	TDD
35	1850 MHz – 1910 MHz	1850 MHz – 1910 MHz	TDD
36	1930 MHz – 1990 MHz	1930 MHz – 1990 MHz	TDD
37	1910 MHz – 1930 MHz	1910 MHz – 1930 MHz	TDD
38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
39	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz	TDD
40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz	TDD

Tabla 2.4.1 Bandas de operación de LTE (Release 8)
Extraído de: 3GPP TS 36.101 V8.26.0 (2014-12)

UE Category	Total layer 2 buffer size [bytes]
Category 1	150 000
Category 2	700 000
Category 3	1 400 000
Category 4	1 900 000
Category 5	3 500 000

Tabla 2.4.3: tamaño total del buffer de capa 2 asignado a su categoría correspondiente
Extraído de: 3GPP TS 36.306 V8.9.0 (2013-03)

2.4.2. Dispositivo en Wi-Fi

Las redes de acceso WLAN tienen una gran ventaja y es que todo equipo que quiere implementar el protocolo 802.11 puede optar a que Wi-Fi *Alliance* lo certifique y esto asegura la operatividad de estos en un ambiente con equipos certificados, sin embargo esta certificación no obliga a dar soporte a todo lo especificado en el protocolo, aunque existen ciertas características obligatorias se puede por optar a dar soporte solo a ciertas características o *amendments* e incluso definir características propias.

Las principales características de la capa física de los diferentes *amendments* que fueron incluidos en 802.11 ya fueron definidos en el apartado 1.2 en este caso el equipo debe especificar en sus datos técnicos cuáles de ellos son soportado [Figura 6.2.2]

	802.11b	802.11a	802.11g	802.11n	802.11ac
802.11a		X			
802.11b	X		X		
802.11g					
802.11n	X		X	X	X
802.11ac		X		X	X

Tabla 2.4.4: Compatibilidad entre los diferentes Amendments de 802.11

Banda	Canal	Frecuencia GHz
2.4 GHz ISM	1	2.412
	2	2.417
	3	2.422
	4	2.227
	5	2.232
	6	2.237
	7	2.442
	8	2.447
	9	2.452
	10	2.457
	11	2.462
	12	2.467
	13	2.472
	14	2.484
U-NII-1	36	5.180
	40	5.200
	44	5.220
	48	5.240
U-NII-2	52	5.260
	56	5.380
	60	5.300
	64	5.320

Banda	Canal	Frecuencia GHz
U-NII-2 Extended	100	2.412
	104	2.417
	108	2.422
	112	2.227
	116	2.232
	120	2.237
	124	2.442
	128	2.447
	132	2.452
	136	2.457
	140	2.462
U-NII-3	149	5.180
	153	5.200
	157	5.220
	161	5.240

Tabla 2.4.5: Bandas de operación de 802.11

El equipo deberá ser capaz de funcionar en las bandas definidas por la IEEE no todos los países tienen estas bandas libres por lo que varía un poco dependiendo de la región, en la tabla 2.4.5 se observan estas bandas que corresponden a las bandas 2.4GHz y 5GHz de la tabla 1.2.1.

Hay que asegurarse que el AP y el dispositivo puedan operar en las bandas correctas, la banda de operación suele ser intercambiable es por eso que hay que asegurarse que el dispositivo pueda hacerlo en la banda elegida por el operario.

3. Análisis del escenario propuesto y de los procedimientos específicos.

En el siguiente análisis se define un escenario que se utiliza para indicar los procedimientos que han sido identificados como básicos, el apartado 2 sirve como base para este análisis.

Descripción del escenario:

- Una área de cobertura con un una sola frecuencia (banda).
- Un eNB.
- Una red inalámbrica LAN ESS representada por dos puntos de acceso.
- Un dispositivo compatible con LTE y WI-FI.
- El eNB está conectado al EPC.

Dado este escenario nos enfocaremos en 3 casos particulares:

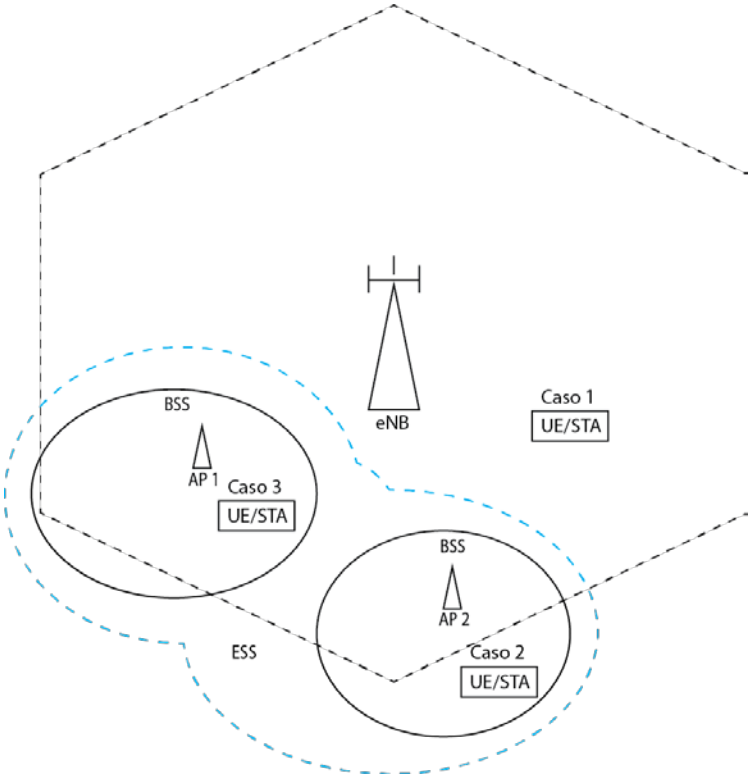

Figura 3.1: Escenario propuesto.

1. Cuando un UE solo tiene acceso a LTE donde no existe interoperabilidad con Wi-Fi- debido a no tener acceso a la cobertura de esta tecnología.
2. Cuando el equipo solo tiene acceso a la tecnología WI-FI.
3. Cuando el Equipo tiene conexión a ambas tecnologías.

Hay que destacar que una red funcional conlleva mucha más complejidad que el escenario planteado, así mismo existen muchísimas variantes, estos casos han sido elegidos debido a que engloban la funcionalidad y base de los procedimientos de interés.

3.1. Caso 1

El equipo del usuario solo tiene cobertura LTE de no haberlo hecho este tendrá que registrarse a la red:

El procedimiento de registro, es el primer procedimiento que realiza el terminal móvil al ser encendido por primera vez, tras recuperar cobertura en caso de salir de la zona de servicio o en caso de que el terminal haya estado haciendo uso de *roaming* y haya vuelto a registrarse a lo que se considera como su red local (donde originalmente recibe los servicios del operador móvil), este procedimiento es necesario para que se lleve a cabo la provisión de servicios por parte de la red LTE.

Oficialmente la 3GPP ha definido este proceso con el nombre de *Network Attachment* Figura 3.1.1. Durante este proceso se activan varios mecanismos que son necesarios para mantener una conectividad IP siempre activa (*always-on* IP por la 3GPP), ejemplo de estos mecanismos son:

- Establecimiento de al menos un servicio portador por defecto.
- La activación de las políticas PCC predefinidas o dinámicas, que almacena el nodo P-GW para aplicarlas a los servicios portadores por defecto.
- La asignación de una dirección IP.

El establecimiento de uno o múltiples servicios portadores dedicados (únicamente en el caso de ser necesario).

A continuación presentaremos una descripción paso a paso del proceso que atraviesa un UE al registrarse dentro de una red LTE extraído de TS 23.401:

Pasos 1 y 2: el UE envía un mensaje conocido como "*Attach Request"* (AR, Solicitud de Registro) al eNB para iniciar con el proceso de registro. Si el UE posee parámetros de seguridad válidos, el mensaje de solicitud de registro será íntegramente protegido dentro de los mensajes NAS-MAC para lograr la validación del UE en la entidad MME. El eNB verifica la identidad de la MME transferida en la capa RRC. Si el eNB tiene una conexión con le entidad MME en cuestión, reenvía le mensaje AR a esa entidad MME. En caso contrario, el eNB seleccionara una nueva MME y reenviara el mensaje AR hacia esa nueva entidad [8] (este mensaje es enviado como un mensaje de control a través de la interfaz S1-MME).

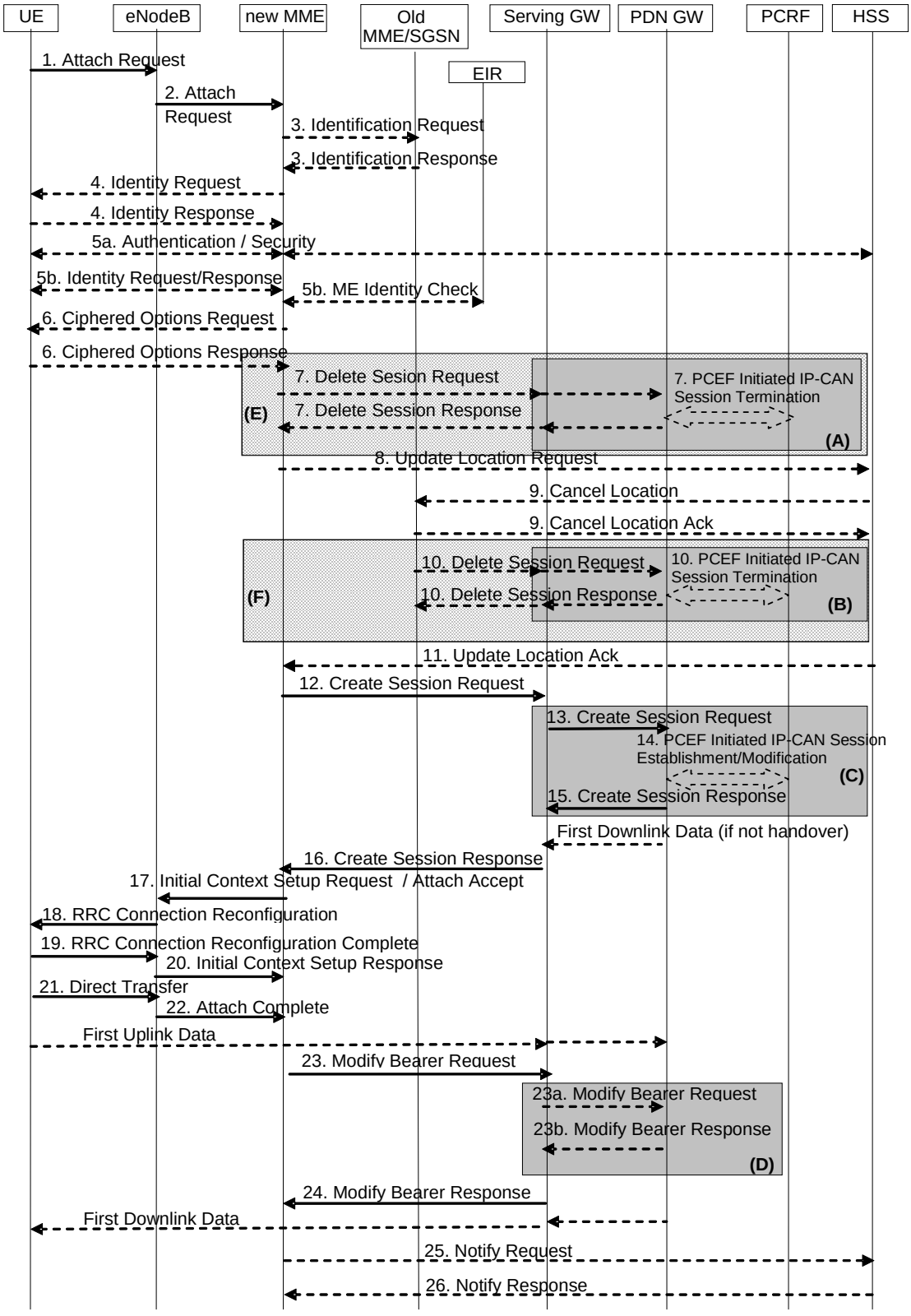

Figura 3.1.1: proceso de registro de un equipo a la red de acceso E-UTRAN
Extraído de TS 3GPP TS 23.401

Paso 3: parte del mensaje de solicitud de registro incluye el identificador GUTI *(Globally Unique Temporary Identity,* Identidad Temporal Única Global*)* el cual es asignado al terminal cada vez que el UE se registra a una MME [15]. En el caso de que el proceso de registro lo lleve a cabo una nueva entidad MME, esta hará uso del identificador GUTI para obtener la dirección de la MME antigua y así enviar un mensaje de "solicitud de identificación" con la finalidad de solicitar el identificador IMSI del UE. En el caso de que la antigua entidad MME esté disponible, esta verifica el mensaje de "solicitud de información" con el nodo EIR (*Equipment Identity Register,* Registrador de la Identidad del Equipo) para luego responder con un mensaje de "respuesta de identificación" o "MM *Context"* este mensaje contiene parámetros de seguridad, información relacionada al usuario y el numero IMSI.

Paso 4: en el caso de que no se encuentre información acerca del UE en ninguna entidad MME (nueva MME y antigua MME), la nueva entidad MME enviara un mensaje de "solicitud de identidad" al UE, este procederá a responder con un mensaje de "respuesta de identidad" (Incluyendo el número IMSI entre otra información).

Paso 5a: en este paso se toman en cuenta las siguientes consideraciones:

- Si no existe ninguna información de contexto del UE en la red.
- Si el mensaje de solicitud de registro no fue íntegramente protegido (por NAS-MAC, paso 1).
- Si se falló en la tarea de validar el UE en la entidad MME (paso2).

Entonces será obligatoria la protección íntegra y cifrada de los menajes de autenticación y seguridad NAS. Caso contrario, esta medida de seguridad será opcional. Finalizado este paso 5a, todos los mensajes NAS deberán ser protegidos bajo las indicaciones de la entidad MME.

Paso 5b: la identidad ME (*Mobile Equipment*, Equipo Móvil) del equipo deberá ser obtenida del UE para luego ser encriptada y transferida por la entidad MME al EIR a través de un mensaje "validador de identidad del equipo móvil" o "ME identity Check", el EIR responderá a la MME con un mensaje conocido como "acuse de validador de identidad del equipo móvil" o *"Identity Check Ack"* y dependiendo del contenido de este mensaje la MME procederá a aceptar o rechazar la solicitud de registro del UE.

Paso 6: En el caso de que el UE haya establecido ciertas opciones de cifrado al momento de enviar el mensaje de solicitud de servicio, deberá enviar la información relacionada con las opciones de cifrado (estas opciones de cifrado se utilizan en el caso de que un UE establezca conexión con múltiples PDN y estas requieran un nombre de usuario y contraseña, este proceso es realizado de manera imperceptible al usuario final).

Paso 7: En caso de que existan servicios portadores activos en la nueva entidad MME que estén relacionados al UE que ha iniciado la solicitud de registro (por ejemplo en caso de que el UE se haya desconectado de manera incorrecta y registrado nuevamente a la

misma entidad MME), la nueva entidad MME se encargara de eliminar estos servicios portadores enviando un mensaje de “solicitud de cancelación de sesión” al nodo o nodos P-GW que brinden servicios de conectividad a los servicios portadores. De existir una sesión IP-CAN activa con un nodo PCRF, el nodo P-GW enviara un mensaje “terminación de sesión” para indicar que los recursos han sido liberados.

Paso 8: si las siguientes condiciones se cumplen:

- La entidad MME a la cual se conectó un UE anteriormente no es la misma.
- No existe información de contexto valida del UE en la nueva entidad MME.
- Si el UE provee un número IMSI o identificador GUTI que no corresponden a ninguna información de contexto valida existente en la entidad MME,

La entidad MME deberá enviar un mensaje de “actualización de ubicación” al nodo HSS. El servidor HSS almacenara la dirección de la nueva entidad MME [8].

Paso 9: el siguiente paso comprende la eliminación de cualquier información de contexto relacionada al UE que pudiese existir en una antigua entidad MME, para realizar esta acción, el servidor HSS envía un mensaje de “cancelación de ubicación” a la antigua entidad MME. La entidad MME antigua envía un mensaje “acuse de cancelación de localización” al servidor HSS y procede a eliminar la información de contexto relacionada al UE.

Paso 10: en el caso de que en la antigua entidad MME existan servicios portadores activos, se repite el proceso realizado en el paso 7 pero en este caso dirigido a la antigua entidad MME.

Paso 11: el servidor HSS envía un mensaje de acuse correspondiente al mensaje “actualización de ubicación” enviando un mensaje “acuse de actualización de ubicación” (este mensaje incluye el número IMSI e información del contexto de usuario) a la nueva entidad MME. La nueva entidad MME valida la presencia del UE en la nueva área de seguimiento.

Paso 12: una vez que se ha completado el paso anterior, la entidad MME procede con el proceso de establecimiento de sesión, este proceso resulta en la creación de un túnel a través del cual los paquetes IP del usuario pueden ser enviados [15] , este proceso lo inicia la nueva entidad MME con el envío de un mensaje de “solicitud de creación de sesión” al nodo S-GW.

Paso 13: el nodo S-GW procede a reenviar el mensaje “solicitud de creación de sesión” al nodo P-GW. Después de este paso, el nodo S-GW almacenara en buffer cualquier paquete procedente del nodo P-GW en el enlace descendente y no enviara un mensaje de notificación a la entidad MME hasta que reciba un mensaje de “solicitud de modificación del servicio portador” realizado en el paso 23 de este proceso de registro.

Paso 14: en el caso de que las reglas PCC sean del tipo dinámicas, el nodo P-GW dará inicio a la creación de una sesión IP-CAN y de ese modo obtendrá las reglas PCC por defecto establecidas para el UE. Caso contrario procederá con la aplicación de las reglas PCC predefinidas por el operador y almacenadas en el nodo P-GW.

Paso 15: una vez establecida la sesión IP-CAN, el nodo P-GW responde al nodo S-GW con un mensaje "respuesta de creación de sesión" que contiene la siguiente información:

- Dirección IP del plano de usuario.
- Identificador de túnel TEID del nodo P-GW para el plano de control y plano de usuario.
- Tipo de la red PDN externa.
- Dirección IP de la PDN externa.
- Identidad del servicio portador EPS.
- Nivel QoS del servicio portador EPS.
- Identificador de tarificación *(charging ID)*.
- Restricciones de APN.

Como parte de este paso, también tenemos que el nodo P-GW creara una nueva entrada dentro de la información del contexto del UE relacionada con la tarificación de los servicios a los que acceda el UE, esta entrada se conoce como "identificador de tarificación" y permite la tarificación de las PDUs provenientes de redes externas y enrutadas entre el nodo P-GW y el nodo S-GW.

Paso 16: a continuación el nodo S-GW envía un mensaje "respuesta de creación de sesión" a la entidad MME conteniendo la siguiente información:

- Tipo y dirección IP de la red PDN externa.
- Dirección IP del nodo S-GW para el plano de usuario.
- Identificador del túnel TEID del nodo S-GW para el plano de control y plano de usuario.
- Identidad del servicio portador EPS.
- Nivel de QoS del servicio portador EPS.
- Dirección IP del nodo P-GW.
- Identificadores de túnel TEID para el tráfico ascendente en el caso de usar el protocolo GTP en las interfaces S5/S8.
- Identificadores de túnel GRE en el caso de utilizar el protocolo PMIPv6 en las interfaces S5/S8.

Paso 17: la entidad MME envía al eNB un mensaje "solicitud de registro inicial" que a su vez incluye un mensaje "registro aceptado" con la siguiente información [15]:

- APN de la red PDN externa.
- Identificador GUTI.
- Tipo y dirección IP de la PDN externa.
- Identidad del servicio portador EPS.
- Numero de secuencia de números de los mensajes NAS.

- Identificador de túnel TEID del nodo S-GW para el plano de control y plano de usuario.

Este mensaje es enviado a través de la interfaz S1-MME entre la entidad MME y el eNB con la finalidad de iniciar el establecimiento de un túnel entre el nodo S-GW y el eNB para el envió de datos correspondientes al plano de usuario.

Paso 18: el eNB procede con el envío de un mensaje "reconfiguración de conexión RRC" al UE para establecer una conexión que se encargue del envió de los paquetes IP a través de la interfaz de aire. Para esto se establecerán dos nuevos servicios portadores de radio, el primero encargado del transporte de mensajes de señalización de baja prioridad y el segundo conocido como un DRB (*Data Radio Bearer*, servicio portador de radio que se encarga del transporte de los datos del plano de usuario en la interfaz de aire).
El envío de este mensaje "reconfiguración de conexión RRC" también incluye el envío de dos mensajes NAS adicionales que son "registro aceptado" y "activar servicio portador por defecto" [15]. En este paso también se le asigna una dirección IP al UE para que pueda comunicarse con redes PDNs externas o con un servidor DNS (las comunicaciones con PDNs externas se podrán llevar a cabo una vez que paso 22 del registro se haya completado).

Paso 19: el UE envía al eNB el mensaje "reconfiguración de conexión RRC completada".

Paso 20: el eNB envía un mensaje "respuesta de contexto inicial" a la MME. Este mensaje incluye el identificador de túnel TEID del eNB así como también la dirección IP del eNB usada para las comunicaciones en el enlace descendente en la interfaz S1-U.

Paso 21: a su vez el UE envía un mensaje directo al eNB que contiene un mensaje "registro completo" con la siguiente información: la identidad de los servicios portadores EPS y la secuencia de números de los mensajes NAS.

Paso 22: el eNB reenvía el mensaje "registro completo" a la entidad MME dentro de un mensaje de señalización NAS en el enlace ascendente. Después del envió del mensaje "registro completo" y una vez que el UE le ha sido asignada una dirección IP, este podrá enviar paquetes en el enlace ascendente hacia el eNB, paquetes que serán enrutados a través de los túneles creados entre el nodo S-GW y el nodo P-GW.

Paso 23: una vez que la MME ha recibido los mensajes "respuesta de contexto inicial" y "registro completo", procede a enviar un mensaje "solicitud de modificación de los servicios portadores" al nodo S-GW, este mensaje contiene la siguiente información:

- Identidad de los servicios portadores EPS.
- Dirección IP del eNB.
- Identificador de túnel TEID del eNB
- Indicador de *handover* (incluido en el mensaje únicamente cuando el proceso de registro se realice debido a un traspaso de redes de acceso no-3GPP hacia 3GPP).

Paso 23a: en el caso de que el mensaje "respuesta de contexto inicial" incluyera el parámetro *handover*, el nodo S-GW enviara un mensaje "solicitud de modificación de los servicios portadores (debido a *handover* o traspaso)" al nodo P-GW con motivo de orientar al P-GW a enviar todos los paquetes IP generados por y hacia una red de acceso no-3GPP hacia la red de acceso 3GPP, en este caso hacia el nodo S-GW perteneciente al núcleo EPC.

Paso 23b: continuando con el proceso de registro en el caso de ser ejecutado dentro de la red como consecuencia de un traspaso entre redes de acceso no-3GPP y 3GPP, el nodo P-GW enviara un mensaje 'respuesta de modificación de los servicios portadores" al nodo S-GW.

Paso 24: el nodo S-GW envía un mensaje "acuse de respuesta de modificación de los servicios portadores" a la MME. En esta parte del proceso de registro, el nodo S-GW almacena el identificador de túnel TEID del eNB para poder reenviar cualquier paquete entrante a través del túnel correcto hacia el eNB. El nodo S-GW ahora si podrá enviar cualquier paquete almacenado en *buffer* en el enlace descendente.

Paso 25: una vez que la entidad MME haya recibido el mensaje "acuse de respuesta de modificación de los servicios portadores" y en el caso de que se cumplan las siguientes condiciones:

- La solicitud de registro a la red no ha sido iniciada debido a un proceso de traspaso.
- Existe al menos un servicio portador EPS establecido.
- La información del perfil de subscripción indica que el usuario tiene permitido realizar traspasos con redes no-3GPP.
- Si la identidad de la entidad MME seleccionada y el nodo P-GW seleccionado, es diferente a los indicados en la información de contexto almacenada en el nodo HSS.

La entidad MME deberá enviar un mensaje de "solicitud de notificación" incluyendo la dirección APN de la red PDN externa y la identificación del nodo P-GW al servidor HSS para servicios de movilidad con redes de acceso no-3GPP.

Paso 26: El servidor HSS almacena la dirección APN de la red PDN externa y la identidad del nodo P-GW y envía un mensaje "respuesta de notificación" a la entidad MME.

Una vez registrado este podrá hacer uso de la red limitado por las políticas y calidad de servicio definidas por el operador en el subsistema PCC.

3.2. Caso 2

El equipo seguirá un proceso de registro utilizando una red de acceso Wi-Fi, este registro será con base en el modelo genérico de una red de acceso no-3GPP confiable o no confiable.

3.2.1. Procedimiento de registro a una red de acceso no-3GPP confiable utilizando la interfaz S2a basada en el modelo *network-based* y el protocolo PMIPv6

A continuación procederemos con la descripción del proceso de registro de un UE con una red de acceso no-3GPP confiable. Es importante hacer la salvedad que para realizar este proceso de registro el UE deberá de ser capaz de conectarse a redes del tipo WLAN o redes Wi-Fi. La solución de interoperabilidad que presentaremos a continuación se basa en el uso del protocolo PMIPv6 y el establecimiento de un túnel bidireccional usando el protocolo GRE a través de la interfaz S2a.

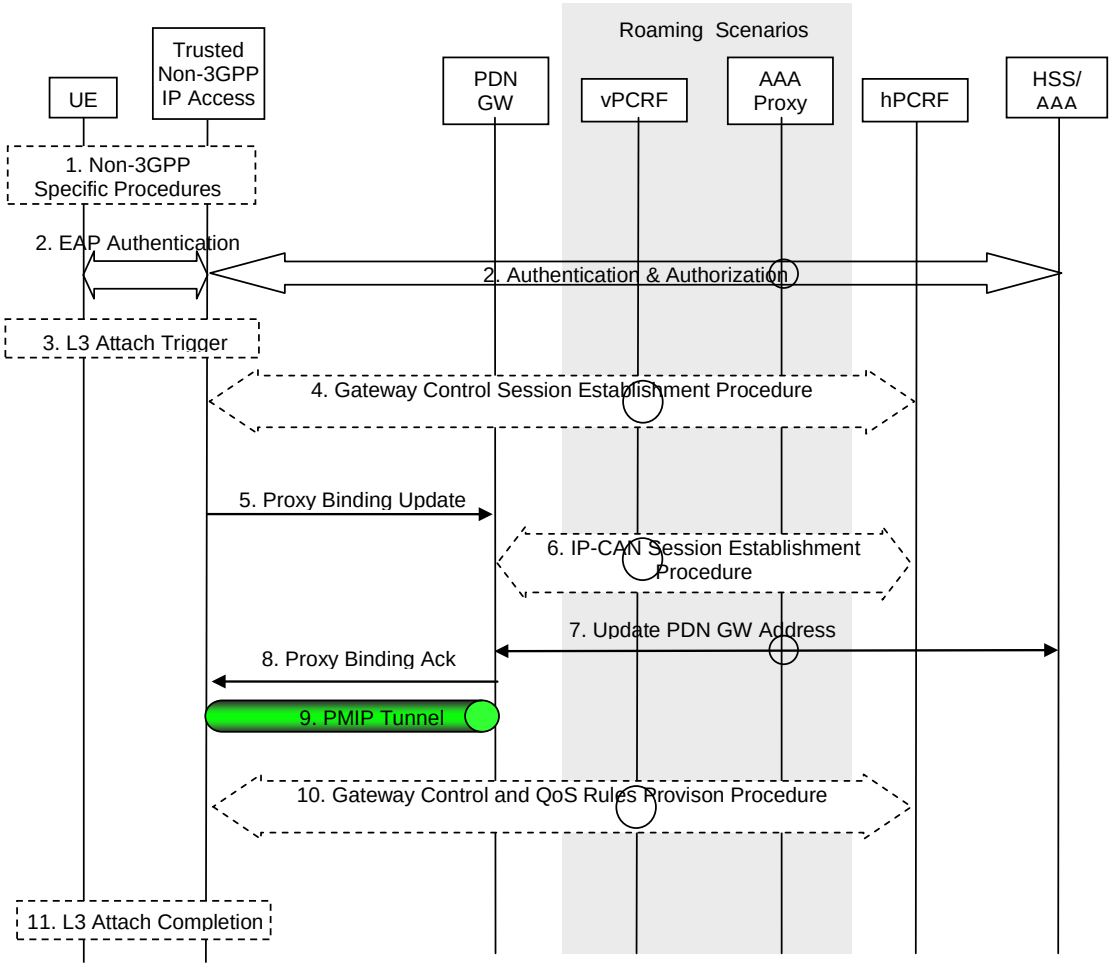

Figura 3.2.1: Proceso de registro de una red de acceso no-3GPP confiable, utilizando la interfaz S2a
Extraído de TS 3GPP TS 23.401

Para una mejor comprensión de este proceso de registro haremos un recorrido paso a paso del proceso de registro definido por la 3gpp en el TS 23.402 y se observa en la figura 3.2.1 de cómo se logra establecer una conexión entre el UE y la red de acceso no-3GPP confiable.

Paso 1: Como primer paso tenemos que el UE se conecta a la red de acceso no-3GPP confiable haciendo uso de la interfaz de radio conocida dentro del marco de la 3GPP como SWw o simplemente 802.11 por la IEEE, haciendo uso de los procesos normales para conectarse a una red WLAN.

Paso 2 y paso 3: Luego de establecer conexión con la red de acceso no-3GPP confiable se iniciara el proceso de autenticación del UE. Según la 3GPP en el proceso de autenticación involucra tanto a la red de acceso no-3GPP como a la red de acceso 3GPP en nuestro caso de estudio Wi-Fi y LTE respectivamente. La autenticación en redes Wi-Fi es soportada por el protocolo EAP para redes Wi-Fi con certificación WPA (*Wireless Protected Accesss*, Acceso Inalámbrico Protegido) [5], mientras que dentro de una red LTE la autenticación de los usuarios se realiza a través del protocolo AKA.

Dentro del sistema de interoperabilidad presentado la autenticación se realizará haciendo uso del protocolo EAP-AKA o su versión mejorada EAP-AKA' que permite que un terminal con una tarjeta USIM (LTE/UMTS) sea autenticado por el servidor AAA de la red troncal EPC mediante la señalización EAP intercambiada por la red de acceso no-3GPP confiable [5]. Durante el proceso de autenticación el servidor AAA comparte información relacionada al perfil del subscritor (vectores de autenticación, QoS y tarificación, direcciones PDN e IPs asignadas) por medio de la interfaz STa con la red de acceso no-3GPP para completar la autenticación del UE. La información que el servidor AAA comparte con la red de acceso no-3GPP confiable es obtenida de la base de datos HSS del núcleo EPC a través de la interfaz SWx.

Paso 4: Una vez que la autenticación ha sido completada de forma exitosa se procede con el establecimiento de una sesión de control entre el nodo PCRF del núcleo EPC y la entidad de la red de acceso no-3GPP confiable que desempeñe las funciones de BBERF de un subsistema PCC para tarificación y control de QoS, en nuestro caso de estudio el nodo WAG desempeñaría las funciones de BBERF. Cuando la sesión de control ha sido establecida a través de los mensajes de señalización enviados por medio de la interfaz Gxa, la red de acceso no-3GPP confiable procede a enviar información relacionada con el perfil del subscriptor (información que recibió del nodo HSS a través del servidor AAA) al nodo PCRF quien recibe la información y en respuesta envía las políticas de control y tarificación basándose en el perfil QoS del usuario para el control de los servicios portadores.

Paso 5: Luego que la sesión de control ha sido establecida, la red de acceso no-3GPP confiable inicia el proceso de asociación definido por el protocolo PMIPv6 y envía un mensaje conocido como PBU *(Proxy Biding Update)* hacia el nodo P-GW, la información contenida en este mensaje identifica al terminal móvil (dirección IP), dirección APN de la red externa a la que se brindara acceso y solicita el establecimiento de un túnel GRE a

través de la interfaz S2a. Anteriormente describíamos el funcionamiento del protocolo PMIPv6 que para lograr el envío de mensajes de asociación o *bidings* hace uso de dos entidades lógicas definidas como MAG y LMA. Dentro del modelo de interoperabilidad presentado la ubicación de estas entidades será la siguiente: la entidad que albergue las funciones MAG será la entidad WAG ubicada en la red de acceso no-3GPP confiable y la entidad que albergue las funciones de LMA será el nodo P-GW ubicado en el núcleo EPC.

Antes de responder al mensaje PBU se Asignara una dirección IP al terminal (IPv4/IPv6) y se realizaran los siguientes pasos:

Paso 6: la entidad P-GW Iniciará el establecimiento de una sesión IP-CAN necesaria para que el nodo P-GW sea capaz de configurar el nivel QoS de los servicios portadores establecidos por defecto *(defeault bearer)*. En el contexto de una sesión IP-CAN, la entidad PCRF envía a la red que proporciona el servicio de conectividad el conjunto de reglas PCC aplicables al usuario (QoS, tarificación, control de flujo de datos etc.)

Paso 7: Informará al servidor AAA acerca de su identidad y de la identidad de la red externa a la que se conectara el UE de esta manera el servidor AAA será capaz de almacenar esta información en la base de datos HSS que podrá ser utilizada en caso de futuros traspasos *(handovers).*

Paso 8 y paso 9: Una vez que realiza estas tareas el nodo P-GW responderá con un mensaje conocido como PBA *(Proxy Biding Acknowledgement)* que incluye la dirección IP asignada al UE además de la información necesaria (identificador de túnel) para completar la configuración del túnel GRE en ambos extremos.

Paso 10: en este paso se pueden incluir actualizaciones de las reglas de QoS en la red de acceso non-3GPP confiable iniciando un procedimiento de modificación de sesión de control

Paso 11: Finalmente una vez que la red de acceso no-3GPP confiable recibe este mensaje, mediante los mecanismos asignación de direcciones que disponga, procede a asignar la dirección IP enviada desde el nodo P-GW al UE.

3.2.2. Procedimiento de registro a una red de acceso no-3GPP confiable utilizando la interfaz S2c basada en el modelo *host-based* y el protocolo DSMIPv6

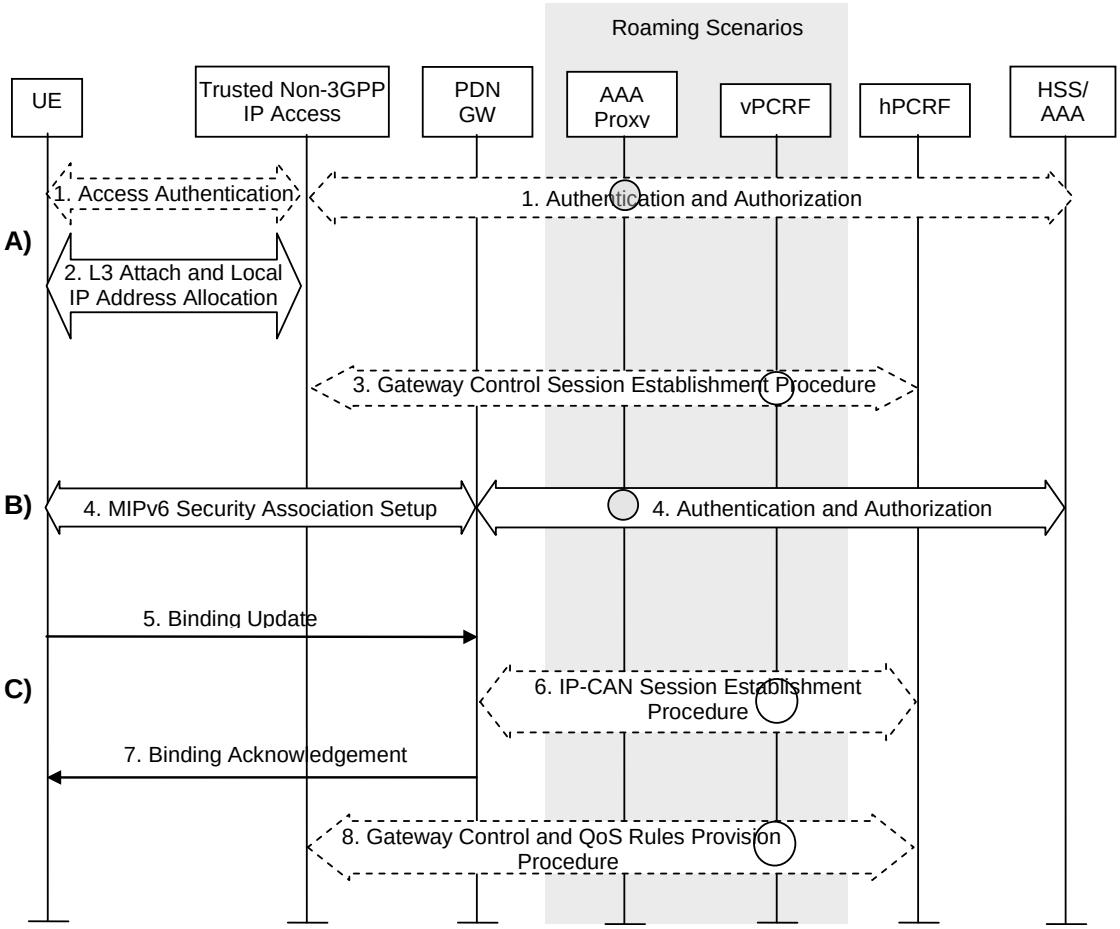

Figura 3.2.2: Proceso de registro de una red de acceso no-3GPP confiable, utilizando la interfaz S2c
Extraído de TS 3GPP TS 23.401

En el siguiente apartado describiremos el proceso mediante el cual un UE podrá registrarse y establecer conexión con una red de acceso no-3GPP confiable haciendo uso de la interfaz S2c y del protocolo DSMIPv6 para ejecutar los mecanismos de movilidad relacionados con un modelo *host-based* véase Figura 3.2.2. El proceso es similar al descrito anteriormente donde se hacía uso de la interfaz S2a y el protocolo PMIPv6 por lo cual presentaremos únicamente aquellos pasos en los que el proceso de registro difiere un modelo del otro.

Paso 2: Una vez que el usuario ha sido autenticado y autorizado recibe una dirección IP asignada por la red de acceso no-3GPP confiable, dentro del marco del protocolo DSMIPv6 a esta dirección se le conoce como dirección CoA, esta dirección le permite

tener acceso a los servicios de conectividad IP que proporciona la red de acceso así como también le permite establecer comunicación con el nodo P-GW del núcleo EPC.

Paso 3: Luego que la red de acceso no-3GPP confiable ha asignado una dirección IP al UE, se procede con el establecimiento de una sesión de control (sesión IP-CAN) con el nodo PCRF del núcleo EPC que a como describíamos anteriormente su finalidad es el compartir las políticas de control y QoS con la red de acceso no-3GPP confiable.

Paso 4: este proceso requiere de una asociación de seguridad entre el UE y el nodo P-GW para lo cual se hace uso del protocolo IPSec encargado de la creación de un túnel bidireccional entre ambos elementos involucrados y el protocolo IKEv2 que será el encargado de establecer y mantener la asociación de seguridad requerida entre el UE y el nodo P-GW. Cuando la asociación se completa satisfactoriamente, el nodo P-GW procede a interactuar con el servidor AAA en aras de autenticar al usuario. Es durante el intercambio de los mensajes de señalización entre el nodo P-GW y el servidor AAA que el terminal adquiere la dirección IP que utilizara como HoA.

Paso 5, paso 6 y paso 7: El terminal móvil o UE enviara un mensaje al nodo P-GW, este mensaje dentro del marco del protocolo DSMIPv6 es conocido como BU *(Biding Update*, similar al mensaje PBU del protocolo PMIPv6). Mediante el envió de este mensaje se vincula la dirección HoA asignada durante el establecimiento de la asociación de seguridad DSMIPv6, con la dirección CoA que dispone el terminal en la red de acceso no-3GPP confiable.

A continuación el nodo P-GW realizara las siguientes funciones:

- Iniciará una sesión IP-CAN con el nodo PCRF para aplicar las políticas de control, tarificación y QoS.
- Informará al servidor AAA su dirección IP y las direcciones IP de las posibles PDNs a las cual el dispositivo pueda estar conectado.
- Responderá al UE con un mensaje conocido como BA *(Biding Acknowledgement)* para completar la asociación DSMIPv6.
- Y finalmente para completar el proceso, tenemos que el túnel DSMIPv6 que transportara la información del plano de usuario, quedara establecido una vez que el UE reciba el mensaje BA.

En el siguiente apartado abordaremos un proceso similar a los descritos anteriormente en cuanto a modelos de interoperabilidad, entre las diferencias que encontramos con respecto a un sistema confiable resaltan la incorporación de una nueva entidad de red conocida como nodo ePDG (Apartado 2.1), además de nuevas interfaces lógicas para el transporte de los datos que en su mayoría realizan funciones similares a las que se ejecutan dentro de un modelo confiable, finalmente, en este modelo se da la intervención del nodo ePDG en las funciones de autenticación con el servidor AAA a través de la interfaz SWm.

Entre las similitudes en cuanto al proceso de registro que se ejecutan en ambos diseños de interoperabilidad (confiable y no confiable) tenemos las siguientes:

1. Las funciones de autenticación propias de la red de acceso no-3GPP no confiable y la autenticación del UE a través del servidor AAA (en conjunto con los demás nodos de la red, HSS, P-GW y ePDG) y la interfaz SWa (equivalente a la interfaz STa en el caso de un modelo confiable).
2. La movilidad y continuidad de los servicios IP entre redes de acceso que se garantiza gracias al uso del protocolo PMIPv6 en este caso empleado por la interfaz S2b (modelo *network-based*) y el protocolo DSMIPv6 empleado por la interfaz S2c (modelo *host-based*).
3. El soporte del subsistema PCC para el control de las políticas de uso y tarificación a través de la nueva interfaz Gxb.
4. Se emplea el mismo principio para las funciones de movilidad que consiste en considerar el nodo P-GW como un punto de anclaje para los servicios de conectividad.
5. Al momento de que se establece la asociación de seguridad (IKEv2) y el túnel IPSec entre el UE y el nodo ePDG, también ocurre una interacción entre el nodo ePDG con el servidor AAA para realizar parte del proceso de autenticación haciendo uso del protocolo EAP-AKA mediante la interfaz SWm. En el nodo ePDG se concentra todo el tráfico que viaja desde el núcleo EPC hacia la red de acceso no-3GPP no confiable y viceversa, lo que permite que también funcione como un filtro del tráfico de datos no autorizados [8].
6. El nodo ePDG desempeñara las funciones de MAG en el caso de usar un modelo *network-based*, en cuanto al subsistema PCC este nodo realizara las funciones de BBERF [4].

3.2.3. Procedimiento de registro a una red no-3GPP no confiable utilizando la interfaz S2b basada en el modelo *network-based* y el protocolo PMIPv6

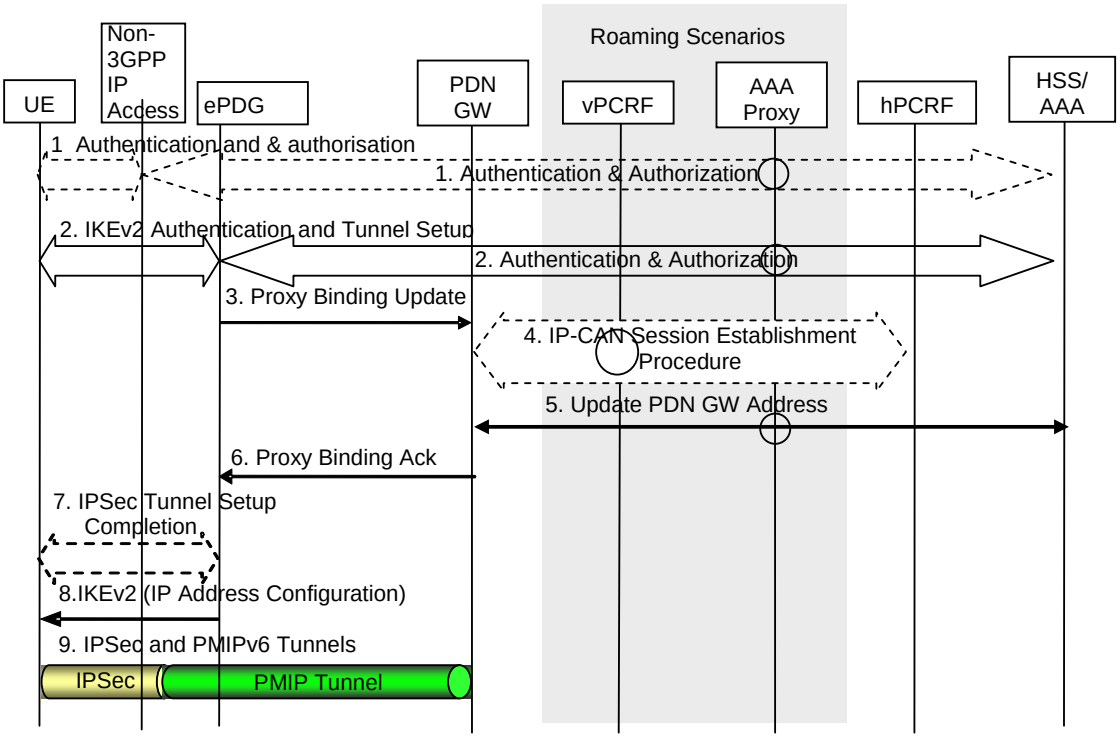

Figura 3.2.3: Proceso de registro de una red de acceso no-3GPP no confiable, utilizando la interfaz S2b
Extraído de TS 3GPP TS 23.401

El procedimiento de registro que que se puede observar en Figura 3.2.3 es muy similar al descrito anteriormente para un sistema de interoperabilidad con redes de acceso no-3GPP confiables haciendo uso de la interfaz S2a, por lo cual hemos decidido hacer mención únicamente de aquellos puntos en los cuales el proceso de registro difiere para un modelo confiable de uno no confiable.

Paso 1: La autenticación del usuario en la red de acceso no-3GPP no confiable es opcional y dependerá de la red de acceso en cuestión, la razón es que la mayor parte del tiempo estas redes de acceso no requieren de una autenticación de seguridad (WPA/WPA2) y se consideran redes abiertas o públicas (cafeterías, universidades, etc.) y por lo tanto la autenticación y autorización de acceso al servicio de conectividad se llevara a cabo al mismo tiempo en que el UE inicia una asociación de seguridad con el nodo ePDG haciendo uso del protocolo IKEv2. Es importante mencionar que para realizar la asociación de seguridad con IKEv2 el UE deberá obtener la dirección IP del nodo ePDG haciendo uso de DHCP (*Dynamic Host Configuration Protocol*, configuración dinámica del protocolo del terminal) [8].La autenticación del UE se basa en el protocolo EAP-AKA que ahora se ejecutará como parte de la asociación de seguridad IKEv2.

El establecimiento de conectividad con la red de acceso no-3GPP no confiable se realiza de manera previa a la señalización de PMIPv6 (antes del envió de un mensaje PBU), esto es debido a que el UE deberá disponer de una dirección IP validad para poder iniciar el establecimiento de la asociación de seguridad con el nodo ePDG. Esta dirección se conoce como dirección externa *(Outter Address)* del túnel IPSec [5].

Paso 2: Cuando la asociación de seguridad IKEv2 ha avanzado, el nodo ePDG recibe la dirección IP del nodo P-GW por parte del servidor AAA y en este punto es cuando el nodo ePDG puede proceder con el envió del mensaje PBU.

Paso 7: El UE recibirá la dirección HoA correspondiente al protocolo PMIPv6 una vez que se haya establecido el túnel IPSec .Esta dirección se conoce como dirección interna del túnel *(Inner Address)*.

Paso 8: El ePDG manda el mensaje IKEv2 final con la dirección IP, la identidad de la PDN asociado pero en caso que haya sido suministrado por el UE en pasos anteriores el ePDG no deberá cambiar este último.

Paso 9: La conexión IP esta lista, los paquetes enviados por el enlace ascendente son mandados por el UE a través de un túnel IPsec hasta el nodo ePDG, luego el nodo ePDG envía los paquetes a través de otro túnel hacia al nodo P-GW, desde ese punto el enrutamiento IP es normal. En términos del enlace descendente, los paquetes que tienen como destino el UE, llegan al nodo P-GW, luego de recibir los paquetes, el nodo P-GW los envía hacia el nodo ePDG a través de un túnel (tomando en cuenta las entradas almacenadas en *biding cache*), luego el nodo ePDG envía los paquetes a través de un túnel IPsec entre el nodo ePDG y el UE.

3.2.4. Procedimiento de registro a una red de acceso no-3GPP no confiable utilizando la interfaz S2c basada en el modelo *host-based* y el protocolo DSMIPv6

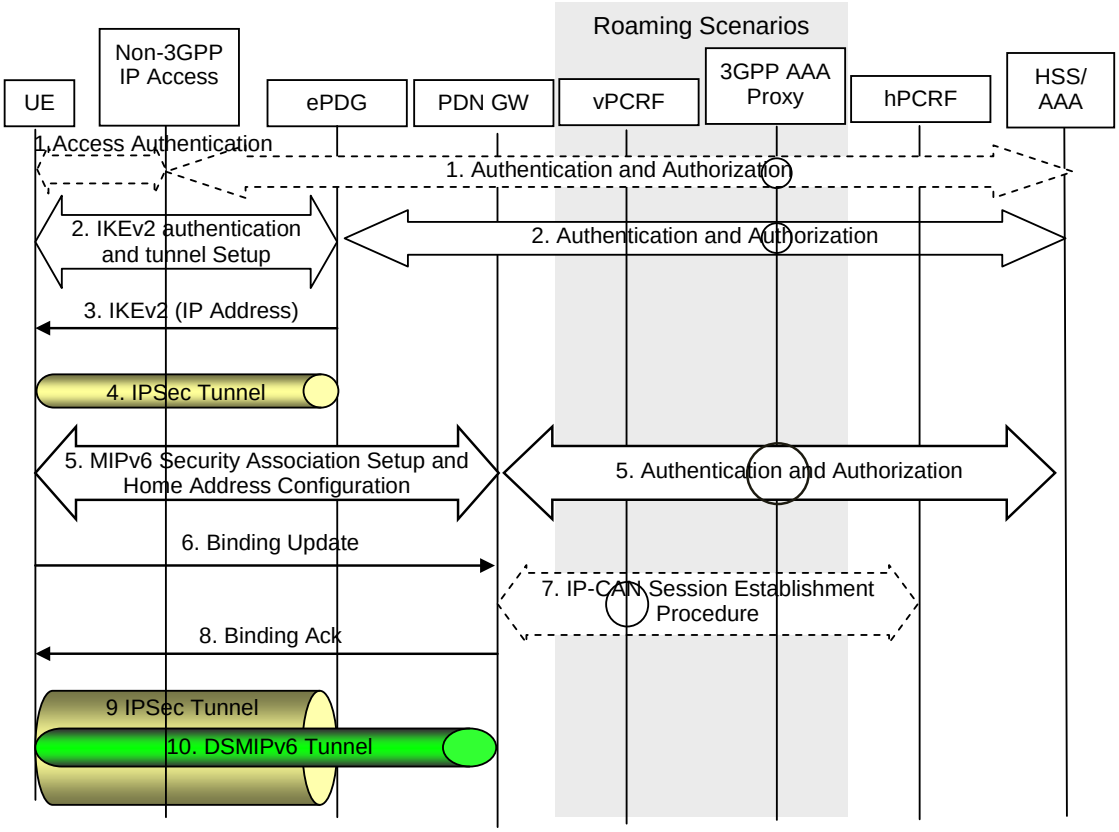

Figura 3.2.4: Proceso de registro de una red de acceso no-3GPP confiable, utilizando la interfaz S2c
Extraído de TS 3GPP TS 23.401

En cuanto a la interfaz S2c y el protocolo DSMIPv6 nos encontramos con una proceso un tanto semejante al descrito en el sistema *trusted* véase Figura 3.2.4 por lo cual haremos mención únicamente de aquellos pasos que sean diferentes en el sistema *untrusted* respecto al sistema *trusted*.

Paso 1: en cuanto a la autenticación realizada por la red de acceso no-3GPP no confiable es opcional por las razones que anteriormente explicábamos en referencia al sistema de interoperabilidad usando la interfaz S2b.

Paso 2: se da inicio al establecimiento de una asociación de seguridad entre el UE y el nodo ePDG, una vez establecida esta asociación de seguridad, se procede a autenticar al UE por medio de los nodos AAA y HSS del núcleo EPC.

Paso 3: El ePDG manda el mensaje IKEv2 final con la dirección IP que le ha sido asignada al UE.

Paso 4: se establece un túnel IPSec donde la dirección externa del túnel es la dirección que adquiere el terminal al momento de establecer conectividad con la red de acceso no-3GPP no confiable y la dirección interna del túnel será la que le asigne el nodo ePDG al UE en el siguiente paso, esta dirección tambien será la que el UE registrará como CoA en el nodo P-GW [5].

Paso 5, 6, 7, 8 y paso 9: Una vez que se ha establecido el túnel, el UE inicia el establecimiento de la asociación de seguridad y del *biding update* del protocolo DSMIPv6 de manera similar que las redes de acceso no-3GPP confiables, la diferencia radica en que ahora estos mensajes de señalización estarán protegidos por el protocolo IPSec.

3.3. Caso 3

En este caso el dispositivo tiene acceso a las dos redes depende mucho del equipo pero se realizaran ambos registros presentados en el caso 1 y caso 2.

3.4. Movilidad

La movilidad es el elemento esencial en una red inalámbrica, tanto LTE como Wi-Fi tienen sus propios mecanismos de movilidad sin embargo al combinar estas tecnologías la complejidad de dicho procesos incrementa, como se ha expuesto, el punto en común que facilita esto, es el dispositivo y los estándares (sobre todo el protocolo IP).

La 3GPP ha abordado la movilidad en su TS 23.402 donde conceptualizan los siguientes tipos de traspasos:

3.4.1. Traspasos genéricos entre redes LTE y redes de acceso no-3GPP.

Una red LTE es capaz de brindar soporte de movilidad entre distintos tipos de redes de acceso en caso de operar en conjunto como una red heterogénea, estas redes de acceso pueden ser consideradas como parte de la familia 3GPP (GSM, UMTS, HSPA) o simplemente como redes de acceso no-3GPP (Wi-Fi, WiMAX, CDMA200).

Se dice que los mecanismo de movilidad soportados por una red LTE son de carácter genérico por el hecho de no ser adaptados para un tipo de red de acceso no-3GPP en particular [8], equivale lo mismo el aplicar estos mecanismos a una red de acceso Wi-MAX así como a una red de acceso Wi-Fi, siempre y cuando la red soporte ciertos requerimientos básicos.

Dentro del marco del marco de la 3GPP a este tipo de mecanismos de movilidad o traspasos entre redes de acceso, se les conoce formalmente con el nombre de “Traspasos no Optimizados *(Non-optimized Handover)*”.

La finalidad principal de este tipo de traspasos se basa en la provisión de procedimientos eficientes que en los casos donde sea posible, se garantice la preservación de las sesiones IP que el usuario pudiese tener activas al momento del traspaso.

Características de un traspaso no optimizado entre LTE y redes no-3GPP.

Los traspasos no optimizados no realizan ningún tipo de interacción previa entre las redes de acceso (origen y destino), la red origen no realiza ningún tipo de mediciones en cuanto al desempeño o carga de tráfico de la red destino, debido al nivel de acoplamiento entre la red de acceso origen y la red de acceso destino. A diferencia de otro tipo de traspasos considerados como optimizados (traspasos entre redes de la misma familia 3GPP) donde existe una interacción previa entre ambas redes de acceso, la ejecución de comandos que den inicio al traspaso o la recolección de datos como QoS o carga de tráfico de la red destino, categoría del UE o terminal móvil, conexiones activas, entre otros.

Una característica principal en este tipo de traspasos es que la decisión de realizar el traspaso recae sobre el UE y en ciertos casos no existen mecanismos de coordinación entre las redes de acceso que faciliten este proceso. Existen ciertos factores que pueden conllevar al UE a realizar un traspaso:

- La selección manual del usuario al decidir establecer conexión con una distinta red de acceso.
- Propiciada por el UE al ejecutar mediciones en los niveles de intensidad de las señales de las redes de acceso disponibles.
- Propiciada por el operador de la red en caso de contar con mecanismos para la provisión de información relacionada con el tipo de redes de acceso disponibles a las cuales se pueda conectar el UE basándose en las políticas de acceso establecidas (en estos casos se podrá hacer uso del nodo ANDSF para proveer al UE con este tipo de información).

Esquemas de movilidad al momento de realizar un traspaso entre redes LTE y no-3GPP.

El núcleo EPC de una red LTE ha sido diseñado con la capacidad de coexistir con distintas redes de acceso basado en un concepto de heterogeneidad. Por lo tanto el núcleo EPC brinda soporte a los mecanismos de traspasos entre redes de acceso no 3GPP haciendo uso de dos esquemas de movilidad:

- ***Host-based:*** esquema que involucra la participación de UE en la detección de los movimientos o saltos del mismo así como el envío de los mensajes de señalización relacionados con movilidad [5]. El núcleo EPC es compatible con dos protocolos de movilidad basados en el esquema *host-based*: Protocolo DSMIPv6 y MIPv4.
- ***Network-Based:*** la señalización y detección de movilidad del UE es realizada directamente por la red la cual deberá de dar seguimiento a los movimientos del UE y encargarse de enviar los respectivos mensajes de señalización al núcleo de la red. Los protocolos GTP y PMIPv6 son soportados por el núcleo EPC en caso de emplear un esquema *network-based.*

En caso de utilizar el esquema de movilidad *host-based*, el UE deberá brindar soporte a la utilización de los protocolos DSMIPv6 y MIPv4 así como también de un cliente de

movilidad por software. En caso de emplearse un esquema *network-based*, la red deberá de ser compatible con el protocolo de movilidad a utilizar ya sea GTP o PMIPV6 y el UE deberá brindar soporte a la continuidad de las sesiones a nivel de la capa de red.

IPMS *(IP Mobility Mode Selection, Selección del Modo de movilidad IP).*

IPMS es una serie de reglas y mecanismos que permiten la selección apropiada de los protocolos de movilidad que deberá ejecutar un UE en conjunto con la red de acceso al momento de realizar un proceso de registro o traspaso entre redes de acceso (3GPP entre no-3GPP y viceversa).

Dentro del sistema EPS se hace necesaria la utilización de las reglas IPMS debido a las variantes en cuanto a los esquemas de movilidad que existen (*host-based* y *network-based*).

Las reglas IPSM se utilizan principalmente en los casos donde el proceso de registro o traspaso sea entre redes consideradas como no-3GPP puesto que dentro de las redes de acceso 3GPP se considera únicamente el esquema de movilidad *network-based* ya sea utilizando el protocolo PMIPv6 o GTP, la selección de cualquiera de los dos protocolo no tendrá ningún impacto en el terminal debido a que esta selección por parte de la red es transparente al UE [8].

Las reglas IPMS podrán ser aplicadas entre la red y el terminal en dos modos de operación:

- **Modo estático:** la red brinda soporte únicamente a un tipo de esquema de movilidad ya sea *host-based* o *network-based*. La correcta funcionalidad de este modo requiere que la red de acceso cuente con información en cuanto a las capacidades del UE, por ejemplo la red deberá determinar si el UE es capaz de brindar soporte a los clientes de movilidad DSMIPv6 o MIPv4.
- **Modo dinámico:** existe la posibilidad de seleccionar entre un esquema de movilidad *host-based* o un esquema de movilidad *network-based*. En el caso del modo dinámico, la selección del esquema de movilidad deberá realizarse al momento de registrar al UE dentro de la red o cuando este proceda a realizar un traspaso entre redes.

El UE hace uso de ciertos atributos pertenecientes a los protocolo de autenticación EAP-AKA y EAP-AKA' para informar a la red de acceso acerca de los protocolos de movilidad (PMIPv6, GTP, DSMIPv6, MIPv4) con los cuales es capaz de operar [8].

Con base en capacidades de la red y del UE, se determina el mecanismo de movilidad que se utilizara y en caso de que la red no cuente con información alguna acerca de las capacidades del UE, se utilizara el esquema *network-based* por defecto.

3.4.2. Traspasos Semi-Optimizados

Anteriormente definíamos el concepto de traspasos genéricos o no optimizados en el caso de que la red LTE no cuente con mecanismos de movilidad que asistan al UE al momento de seleccionar una red de acceso no-3GPP y realizar un traspaso a la misma. En el siguiente apartado presentaremos un elemento que se agrega a la red LTE con la finalidad de asistir en las labores de búsqueda, selección y orientación del tráfico IP en escenarios donde existan redes de acceso no-3GPP con las cuales el UE pueda establecer conexión, siempre asumiendo que esto sucede dentro del marco de una red heterogénea conformada por LTE y Wi-Fi como red de acceso no-3GPP.

Nodo ANDSF (*Access Network Discovery and Selection Function*)

La entidad ANDSF fue definida por la 3GPP en TS 23.402 y su función principal consiste en asistir al UE, en la búsqueda y selección de redes de acceso no-3GPP a través de la provisión de las políticas, preferencias y acuerdos que ha establecido el operador de la red.

La entidad ANDSF provee al UE con una lista de las redes de acceso no-3GPP disponibles en el área de ubicación del UE, los tipos de redes de acceso disponibles, identificación de las redes (SSID para redes Wi-Fi), entre otros datos.

Las políticas para la búsqueda y selección de las redes de acceso no-3GPP, pueden ser pre-configuradas en el terminal y luego podrán ser modificadas por la entidad ANDSF o podrán ser provistas directamente por esta entidad.

El terminal móvil y el nodo ANDSF se conectan entre sí por medio de la interfaz S14, esta interfaz está basada en el protocolo IP y el protocolo desarrollado por la Open Mobile Alliance OMA-DM, por lo tanto el terminal móvil deberá brindar soporte al protocolo OMA-DM.

El UE será capaz de acceder al nodo ANDSF a través de una red de acceso no-3GPP que esté conectada al núcleo EPC mediante una conexión IP. La autenticación y seguridad de las comunicaciones entre el UE y el nodo ANDSF son basadas en la tecnología GBA (*Generic Bootstapping Architecture*, definida por la 3GPP en su TS 33.220) donde según información recopilada de [8] , GBA es usada como método de autenticación basado en las credenciales SIM y el numero IMSI del UE.

El nodo ANDSF cuenta con dos modos de operación para la entrega de las políticas de búsqueda, selección y preferencia de las redes de acceso no-3GPP:

- Modo *push*: el nodo ANSDF ejecuta este modo para enviar al UE las políticas del operador relacionadas con la búsqueda y selección de redes de acceso no-3GPP.
- Modo *pull*: es el modo que utiliza el UE para solicitar al nodo ANDSF las políticas del operador relacionadas con la búsqueda y selección de redes de acceso no-3GPP.

ANDSF MO *(Managment Object)*

Consiste en un mecanismo que permite el envió de parámetros relevantes y necesarios para el UE, estos parámetros tienen que ver con las políticas de movilidad entre sistemas (ISMP) además de las funciones de búsqueda y selección de redes de acceso que pueden ser manejadas por el nodo ANDSF TS 24.312. En otras palabras el ANDSF MO es el formato que se le da a la información que se intercambia entre el nodo ANDSF y el UE. Este mecanismo es compatible con el protocolo OMA DM (que mencionábamos anteriormente) desde la versión 1.2 en adelante, la tecnología DM le permite al nodo ANDSF la configuración remota de los parámetros enviados a través de MO por medio de la interfaz S14.

Dentro de este formato se puede almacenar información considerada de gran importancia tal como:

- Reglas ISMP *(Inter-System Mobility Policy)*.
- Información relacionada con la búsqueda y selección de las redes de acceso.
- Ubicación del UE.
- Reglas ISRP *(Inter-System Routing Policy)*.
- Perfil del UE

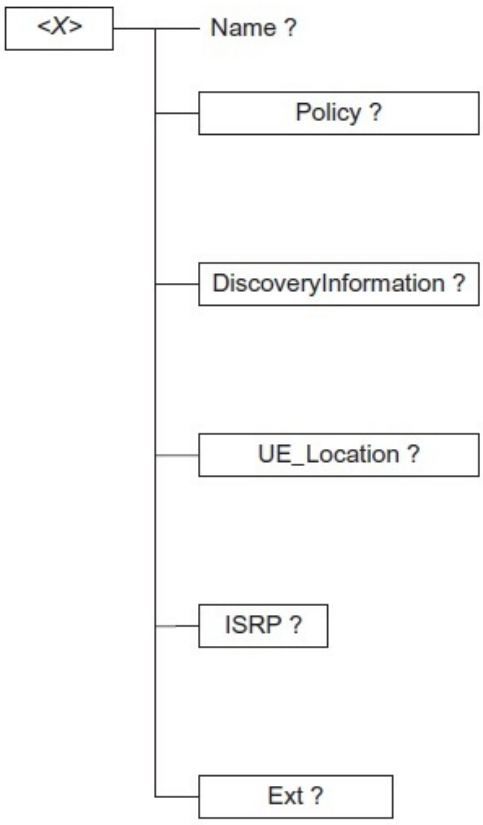

Figura 3.4.2.1 *Representación del formato MO.*

La Figura 3.4.2.1 es una representación gráfica de la estructura del formato MO, para obtener más información acerca del contenido de cada parámetro en la estructura del MO

El UE es capaz de proporcionar información al nodo ANDSF haciendo uso del formato OM dentro del parámetro conocido como perfil de usuario (UE_*Profile* por la 3GPP en TS 24.312), este parámetro contiene información como:

- Numero IMSI del UE.
- Ubicación (usando el sistema GPS del UE o según el código de las áreas de seguimiento del UE, identificador de celda).
- Información que el nodo ANDSF solicite al UE.
- Identificación o SSID de la red (en caso de tratarse de una red heterogénea con puntos de acceso Wi-Fi).
- Perfil del UE (capacidades del terminal, tipo de sistema operativo, etc.).

El nodo ANDSF podrá utilizar esta información para adaptar cada uno de los parámetros incluidos en el formato MO de acuerdo con las capacidades del UE, ubicación, puntos de accesos disponibles, etc.

Información que provee el nodo ANDSF al UE contenida en el formato OM: El nodo ANDSF provee al UE con información muy variada en cuanto a la búsqueda y selección de las redes de acceso no-3GPP, para mejor compresión de las funciones de este nodo y del tipo de información que provee al UE procederemos a detallar las mismas en este apartado.

Información relacionada con la búsqueda y selección de las redes de acceso: El contenido de esta información está relacionado con los tipos de redes de acceso disponibles en el área donde se encuentre ubicado el UE y generalmente recopila datos como [8] :

- Listado de las redes de acceso disponibles en el área de ubicación del UE (la lista puede incluir redes de acceso 3GPP así como no-3GPP).
- Identificadores de red.
- Condiciones establecidas para que el UE pueda tener acceso a la red.

El nodo ANDSF proveerá con al menos una red de acceso disponible dentro de la ubicación del UE y que será tarea del UE descartar aquellas redes con las cuales no pueda establecer conectividad. Si el UE descubre alguna red que no aparezca en el listado provisto por el nodo ANDSF, puede reportarlo al nodo ANDSF para investigar sobre esa red de acceso.

Reglas ISMP *(Inter-System Mobility Policy)*

Son un conjunto de reglas definidas por el operador que inciden al momento de llevarse a cabo un proceso de selección y traspaso hacia una red de acceso no-3GPP. Este tipo de reglas se utiliza en los casos donde el UE pueda utilizar una interfaz de radio a la vez para el manejo de los datos (en nuestro caso sería LTE o Wi-Fi).

Funciones de las reglas ISMP:

- Asistir al momento de decidir cuándo y bajo qué circunstancias (ubicación, hora del día, tipo de subscripción del usuario etc.) utilizar la red de acceso 3GPP o no-3GPP y viceversa.
- Asistir en la selección del tipo de redes de acceso no-3GPP que se va a utilizar (en caso de que existan distintas redes de acceso ya sean puntos de acceso Wi-Fi o redes WiMAX, etc.).
- Indicar cuando la movilidad o traspasos entre redes de acceso no-3GPP este permitida o se encuentre prohibida.
- En caso de existir distintos tipos de redes de acceso no-3GPP, las reglas ISMPs le indican al UE el nivel de preferencia y prioridad entre las redes de acceso (cuando preferir conectarse a Wi-Fi en lugar de a una red WiMAX, en el caso de múltiples APs Wi-Fi que red o determinado SSID tiene mayor prioridad sobre otro).

Reglas ISRP *(Inter-System Routing Policy)*

Son un conjunto de reglas creadas por el operador de la red LTE que se utilizan para indicar al UE acerca del tipo de tráfico (por ejemplo: VoIP, *Streaming* de video) que deberá ser enrutado sobre la red celular LTE y el tipo de tráfico (por ejemplo: Web, FTP) deberá ser enrutado sobre la red de acceso Wi-Fi.

Las reglas ISRP también le indican al UE acerca del tráfico IP que será enviado a través de la red de acceso Wi-Fi sin tener que ser enrutados por el núcleo EPC, con el fin de llevar a cabo una descarga de tráfico del núcleo EPC [8].

Este tipo de reglas se utiliza cuando se cuenta con un UE capaz de enrutar tráfico IP de manera simultánea utilizando distintas interfaces de radio (en el caso de nuestro estudio seria LTE y Wi-Fi de manera simultánea) [13].

Las reglas ISRP están divididas en 3 categorías:

1. Basada en el flujo de paquetes *(Flow Based)*: esta categoría se utiliza para crear una separación en el flujo de los paquetes IP correspondientes a una única conexión PDN con el fin de enviar ciertos paquetes a través de una red Wi-Fi por ejemplo, y la otra parte de los datos a través del núcleo EPC de una red LTE. Esta categoría ha sido diseñada para técnicas de descarga de tráfico tales como IFOM.

2. Basada en el servicio *(Service Based)*: esta categoría le permite al UE establecer conexión con múltiples redes PDNs externas utilizando distintas redes de acceso de manera simultánea, por ejemplo el UE podrá hacer uso de la interfaz de radio móvil para conectarse a la red E-UTRAN y acceder a servicios exclusivos del núcleo EPC, mientras hace uso de la interfaz de radio Wi-Fi para la navegación web.

3. Basada en la descarga de tráfico usando una red WLAN (WLAN *Offload*): el operador hace uso de este tipo de reglas ISRP para indicar el tipo de tráfico que será enviado a través de una red de acceso WLAN sin tener que atravesar el núcleo EPC.

CM *(Connection Manager)*

Es la aplicación que se ejecuta en el UE y que maneja la conectividad del mismo. Presenta información acerca de las distintas redes de acceso disponibles y se encarga de conectarse de manera automática a las redes de acceso teniendo en cuenta las políticas y preferencias del operador, preferencias del usuario, disponibilidad de las redes, condiciones de las redes, etc.

A continuación se presentan los procesos de traspasos con base en los casos antes expuestos definidos en el TS 23.402:

- **Traspaso de una red de acceso no-3GPP confiable a LTE utilizando la interfaz S2a y el protocolo PMIPv6 (Figura 3.4.2.2*)***

Paso 1: el UE se encuentra utilizando una red de acceso no-3GPP confiable y está siendo atendido por el nodo P-GW (quien a su vez se encuentra realizando funciones similares a las de un *home agent,*).

Paso 2: el UE descubre la red de acceso LTE y determina realizar un traspaso de las sesiones activas (que tiene dentro de la red de acceso no-3GPP confiable) hacia la red LTE que ha descubierto.

Paso 3: el UE inicia el proceso de registro en la red LTE y procede a enviar un mensaje de "solicitud de registro" a la MME.

Paso 4: la entidad MME contacta al servidor HSS y autentica al UE. Como parte del procedimiento de autenticación, la dirección IP del nodo P-GW a ser utilizado es enviada a la MME.

Paso 5: cuando la autenticación se ha completado satisfactoriamente, la entidad MME realiza el proceso de actualizar su ubicación con el servidor HSS a como se especifica en el paso 8 del registro de LTE (Apartado 3.1).

Paso 6: este paso equivale al paso 12 del registro del UE en la red LTE.

Paso 7: este paso equivale al paso 13 del registro del UE en la red LTE.

Paso 8: el nodo P-GW envía un mensaje de "modificación de la sesión IP-CAN" al nodo PCRF para obtener las reglas PCC requeridas por el P-GW y así funcionar como PCEF (entidad de la arquitectura PCC) para todas las sesiones que el UE haya establecido en la red de acceso no-3GPP confiable.

Paso 9: el nodo PRCF envía un mensaje "acuse de modificación de la sesión IP-CAN" al nodo P-GW. Este mensaje incluye los parámetros QoS y las políticas en cuanto a tarificación para que el nodo P-GW realice las funciones de PCEF.

Paso 10: este paso equivale al paso 15 del registro del UE en la red LTE. Es importante mencionar que en este paso, el mensaje de "respuesta de creación de sesión" incluirá la dirección IP local que le fue asignada al UE en la red de acceso no-3GPP confiable.

Paso 11: este paso equivale al paso 16 del registro del UE en la red LTE.

Paso 12: este paso equivale al paso 17 del registro del UE en la red LTE.

Paso 13: este paso equivale al paso 23a del registro del UE en la red LTE.

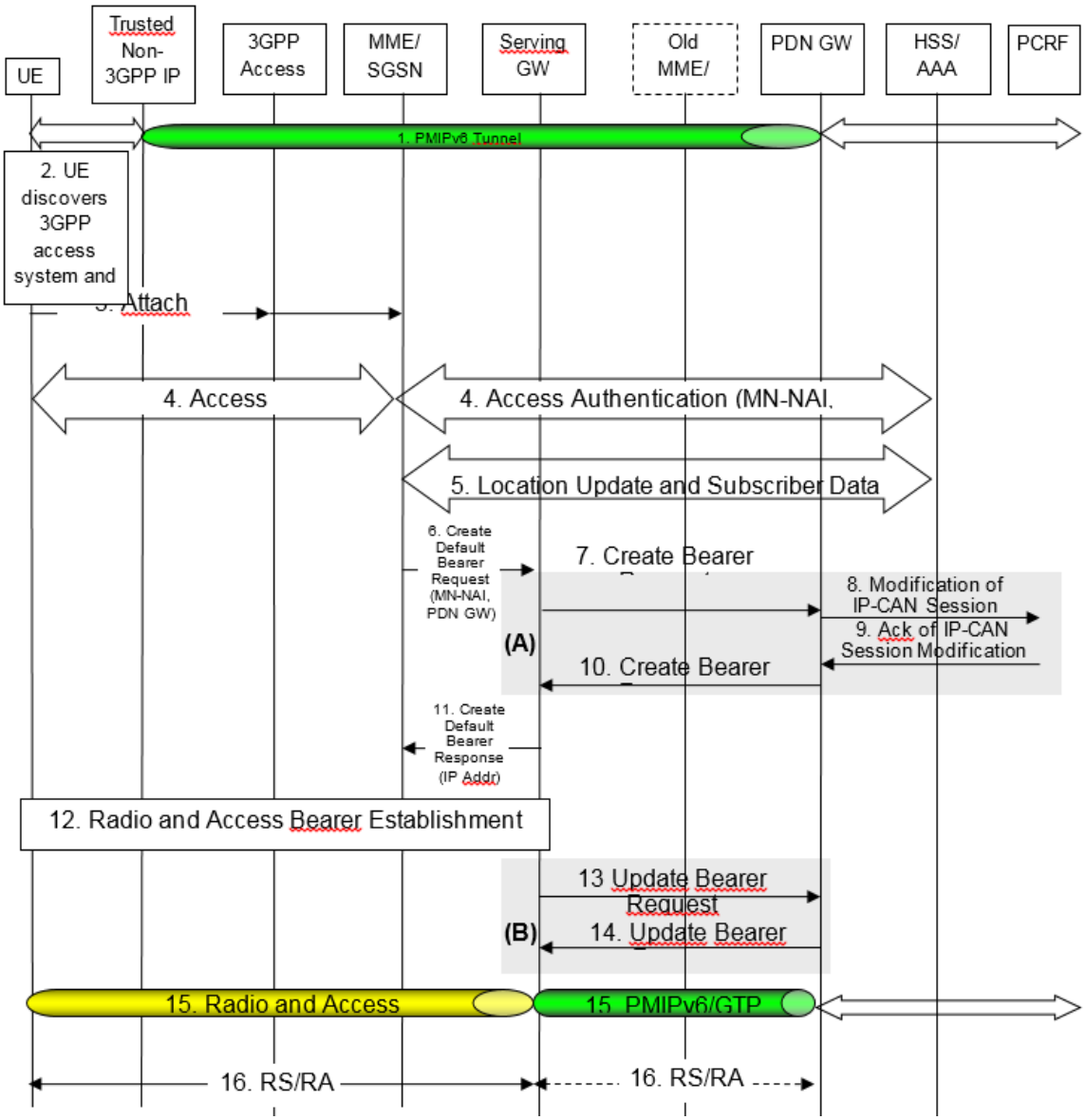

Figura 3.4.2.2: Traspaso de una red de acceso no-3GPP confiable a LTE utilizando la interfaz S2a
Extraído de 3GPP TS 23.402

Paso 14: El nodo P-GW envía un mensaje "acuse de respuesta de actualización de los servicios portadores" al nodo S-GW.

Paso 15: En este punto el UE podrá enviar y recibir datos haciendo uso de la red LTE.

Paso 16: en el caso de utilizar el protocolo GTP en la interfaz S5/S8, el nodo P-GW intercambiara mensajes del tipo RA *(Routing Advertisement)* con el UE. En caso de utilizar el protocolo PMIPv6 en la interfaz S5/S8 la entidad S-GW realiza el intercambio de este tipo de mensajes con el UE.

- **Traspaso de una red de acceso no-3GPP confiable a LTE utilizando la interfaz S2c y el protocolo DSMIPv6 (Figura 3.4.2.3)**

Paso 1: el UE se encuentra conectado a una red de acceso no-3GPP confiable y tiene establecido un túnel DSMIPv6 con el nodo P-GW del núcleo EPC.

Paso 2: el UE descubre una red de acceso 3GPP (LTE) y determina realizar un proceso de traspaso de la red de acceso no-3GPP confiable hacia la red 3GPP.

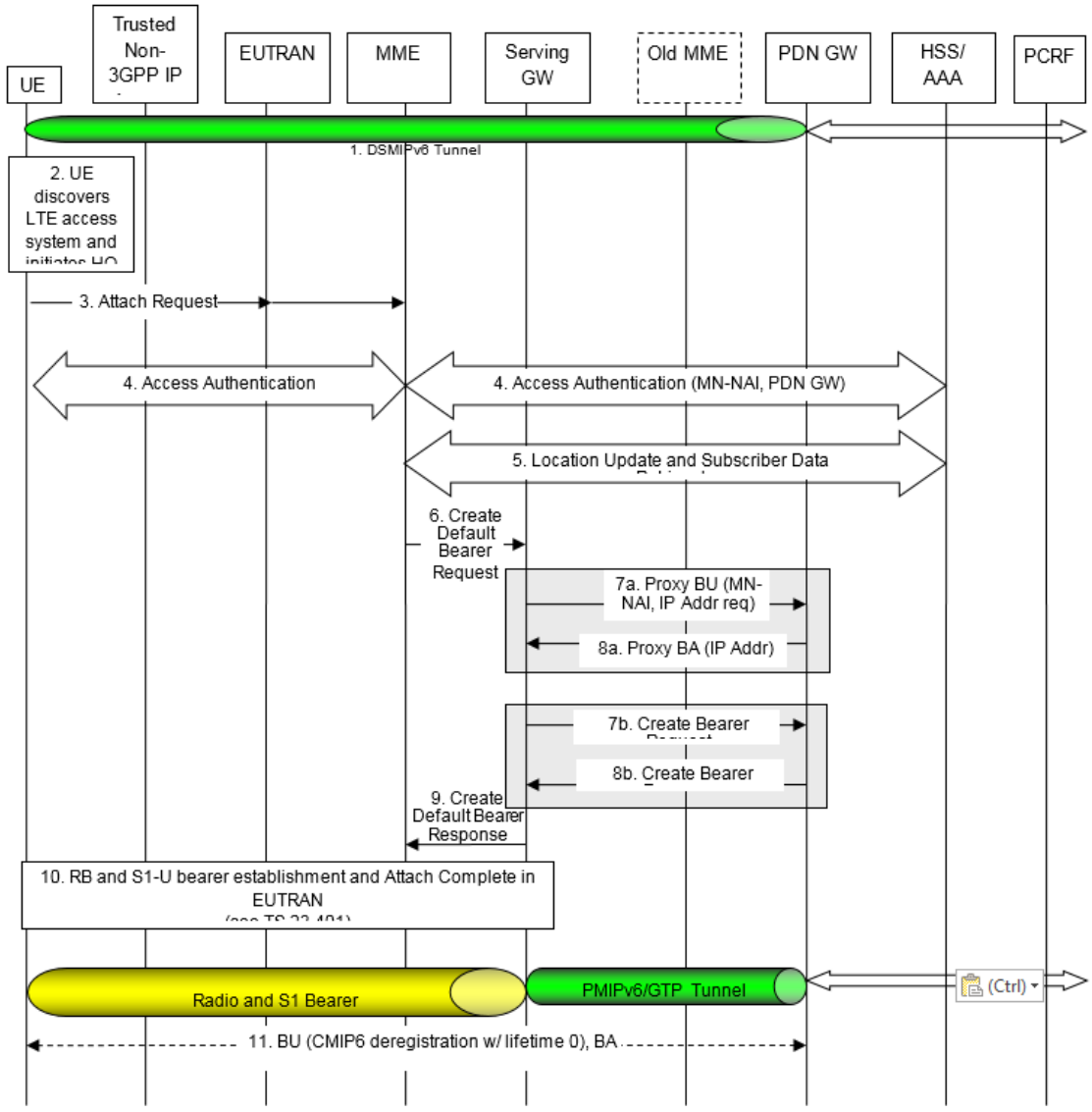

Figura 3.4.2.3. Traspaso de una red de acceso no-3GPP confiable a LTE utilizando la interfaz S2c

Extraído de 3GPP TS 23.402

Paso 3: el UE envía un mensaje de “solicitud de registro” a la entidad MME, este paso se describe en el paso 1 y 2 del proceso de registro de un UE dentro de una red LTE.

Paso 4: la entidad MME contacta al servidor HSS y al servidor AAA para autenticar al UE. Como parte del proceso de autenticación, la dirección IP del nodo P-GW que será utilizado dentro de la red de acceso 3GPP, es enviada a la entidad MME.

Paso 5: luego del proceso de autenticación, la entidad MME procede a enviar un mensaje "actualización de ubicación" al servidor HSS a como se especifica en el paso 8 del registro del UE en una red LTE.

Paso 6: este paso equivale al paso 12 del registro del UE en la red LTE.

Paso 7: este paso equivale al paso 13 del registro del UE en la red LTE.

Paso 8: este paso equivale al paso 15 del registro del UE en la red LTE. El mensaje de "respuesta de creación de sesión" incluirá la dirección IP local que le fue asignada al UE en la red de acceso no-3GPP confiable.

Paso 9: este paso equivale al paso 16 del registro del UE en la red LTE.

Paso 10: la entidad MME envía un mensaje "registro aceptado" al eNB (paso 17 del registro del UE). La red de acceso 3GPP inicia el establecimiento de los servicios portadores (paso 18 del registro del UE). La red de acceso 3GPP responde con un mensaje de "registro completo" (paso 21 del registro del UE).

Paso 11: el UE envía un mensaje BU *(Binding Update)* al nodo P-GW para desactivar el túnel DSMIPv6 que había sido creado mientras utilizaba la red de acceso no-3GPP confiable.

- **Traspaso de una red de acceso no-3GPP no confiable a LTE utilizando la interfaz S2b y el protocolo PMIPv6 (Figura 3.4.2.4)**

Paso 1: el UE se encuentra conectado a una red de acceso no-3GPP no confiable, existe un túnel IPsec entre el UE y el nodo ePDG y un túnel PMIPv6 adicional entre el nodo ePDG y el nodo P-GW.

Paso2: el UE se mueve de la zona de cobertura de la red y procede a iniciar un proceso de traspaso y registro a una red de acceso E-UTRAN.

Paso 3: el UE realiza el proceso de autenticación con la entidad MME. La entidad MME contacta al servidor HSS para autenticar al UE. Como parte de este procedimiento de autenticación, la dirección IP del nodo P-GW que se va a utilizar dentro de la red de acceso 3GPP, es enviada a la entidad MME.

Paso 4: luego del proceso de autenticación, la entidad MME procede a enviar un mensaje "actualización de ubicación" al servidor HSS a como se especifica en el paso 8 del registro del UE en una red LTE.

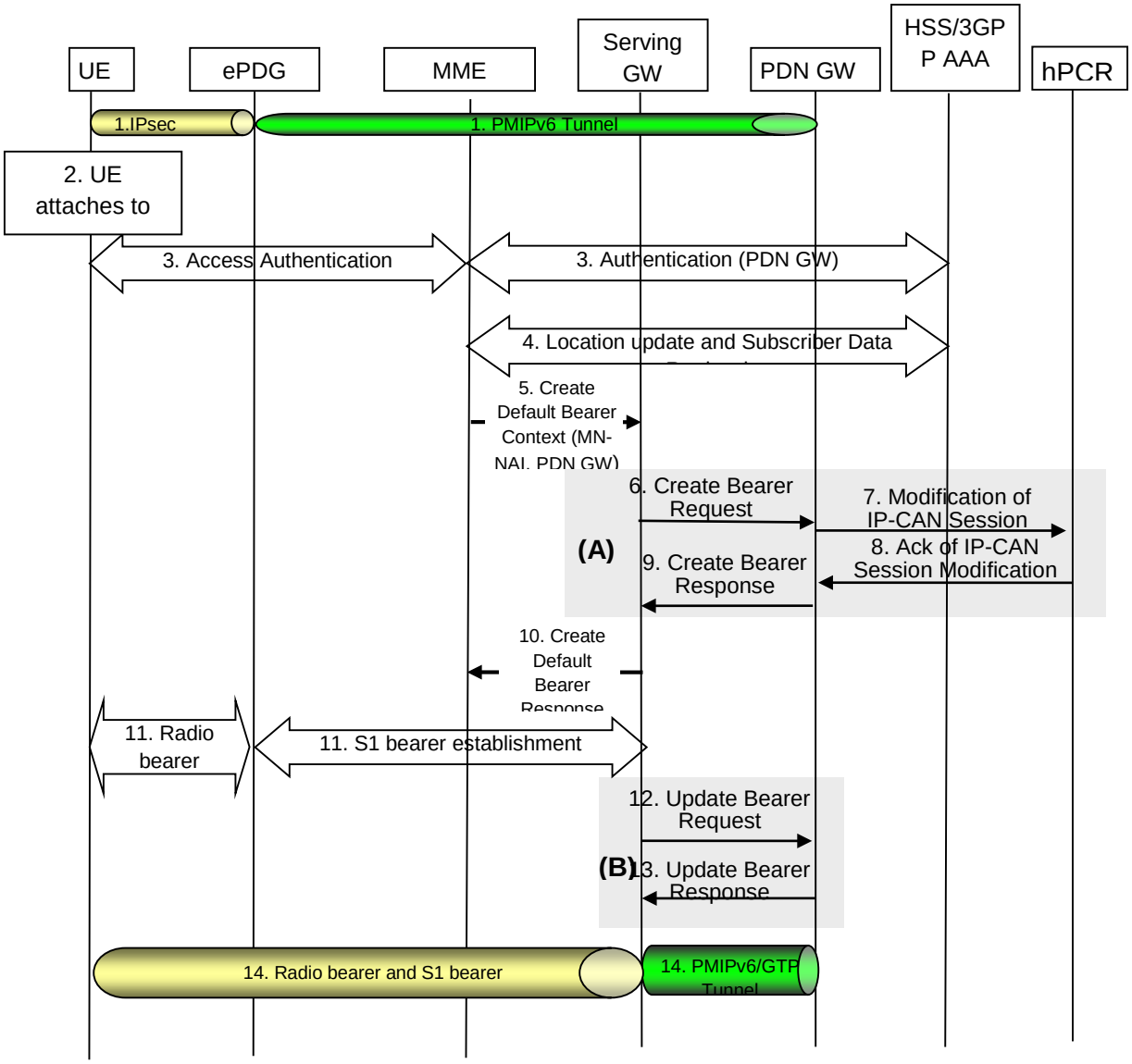

Figura 3.4.2.4: Traspaso de una red de acceso no-3GPP no confiable a LTE utilizando la interfaz S2b
Extraído de 3GPP TS 23.402

Paso 5: la entidad MME envía un mensaje de "solicitud de creación de sesión" al nodo S-GW. Este mensaje contiene un identificador del UE y la dirección del nodo P-GW que necesita ser utilizado.

Paso 6: el nodo S-GW reenvía el mensaje "solicitud de creación de sesión" al nodo P-GW.

Paso 7: en caso de que las reglas PCC sean soportadas (en la red de acceso no-3GPP no confiable), el nodo P-GW procederá a enviar un mensaje "modificación de la sesión IP-CAN" al nodo PCRF detallando que el proceso de registro se realiza debido a un

traspaso y de esta manera obtener los parámetros QoS y las reglas PCC relacionadas con políticas y tarificación.

Paso 8: si el paso 7 se lleva a cabo, el nodo PCRF envía un mensaje "acuse de modificación de la sesión IP-CAN" al nodo P-GW, este mensaje incluye los parámetros QoS y las reglas PCC en cuanto a políticas y tarificación.

Paso 9: este paso equivale al paso 15 del registro del UE en la red LTE. El mensaje de "respuesta de creación de sesión" incluirá la dirección IP local que le fue asignada al UE en la red de acceso no-3GPP no confiable.

Paso 10: el nodo S-GW envía un mensaje "respuesta de creación de servicio portador por defecto" a la entidad MME. El nodo S-GW incluye la dirección IP del UE en este mensaje.

Paso 11: se inicia el establecimiento de los servicios portadores de radio, de un servicio portador por defecto S1_U y de ser necesario se inicia el establecimiento de servicios portadores dedicados.

Paso 12: el nodo S-GW envía un mensaje "solicitud de modificación de los servicios portadores (debido a *handover* o traspaso)" al nodo P-GW. Con este mensaje el nodo S-GW le indica al nodo P-GW que a partir de este momento deberá enrutar los paquetes IP hacia el nodo S-GW dentro del núcleo EPC.

Paso 13: el nodo P-GW enviará un mensaje "respuesta de modificación de los servicios portadores" al nodo S-GW.

Paso 14: Al final del traspaso, existirá un servicio portador por defecto, ninguno o varios servicios portadores dedicados para el UE y se habrá establecido un túnel PMIPv6 o GTP entre el nodo S-GW y el nodo P-GW.

- **Traspaso de una red de acceso no-3GPP no confiable a LTE utilizando la interfaz S2c y el protocolo DSMIPv6 (Figura 3.4.2.5)**

Paso 1: el UE se encuentra conectado a una red de acceso no-3GPP no confiable y tiene un túnel IPsec/IKEv2 establecido con el nodo ePDG además de un túnel DSMIPv6 con el nodo P-GW ambos nodos pertenecientes al núcleo EPC.

Paso 2: el UE descubre una red de acceso LTE y determina realizar un proceso de traspaso de la red no-3GPP no confiable hacia la red 3GPP.

Paso3: el UE envía un mensaje de "solicitud de registro" a la entidad MME, este paso se describe en el paso 1 y 2 del proceso de registro de un UE dentro de una red LTE.

Paso 4: la entidad MME contacta al servidor HSS y al servidor AAA para autenticar al UE. Como parte del proceso de autenticación, la dirección IP del nodo P-GW que necesita ser utilizado dentro de la red de acceso 3GPP es enviada a la entidad MME.

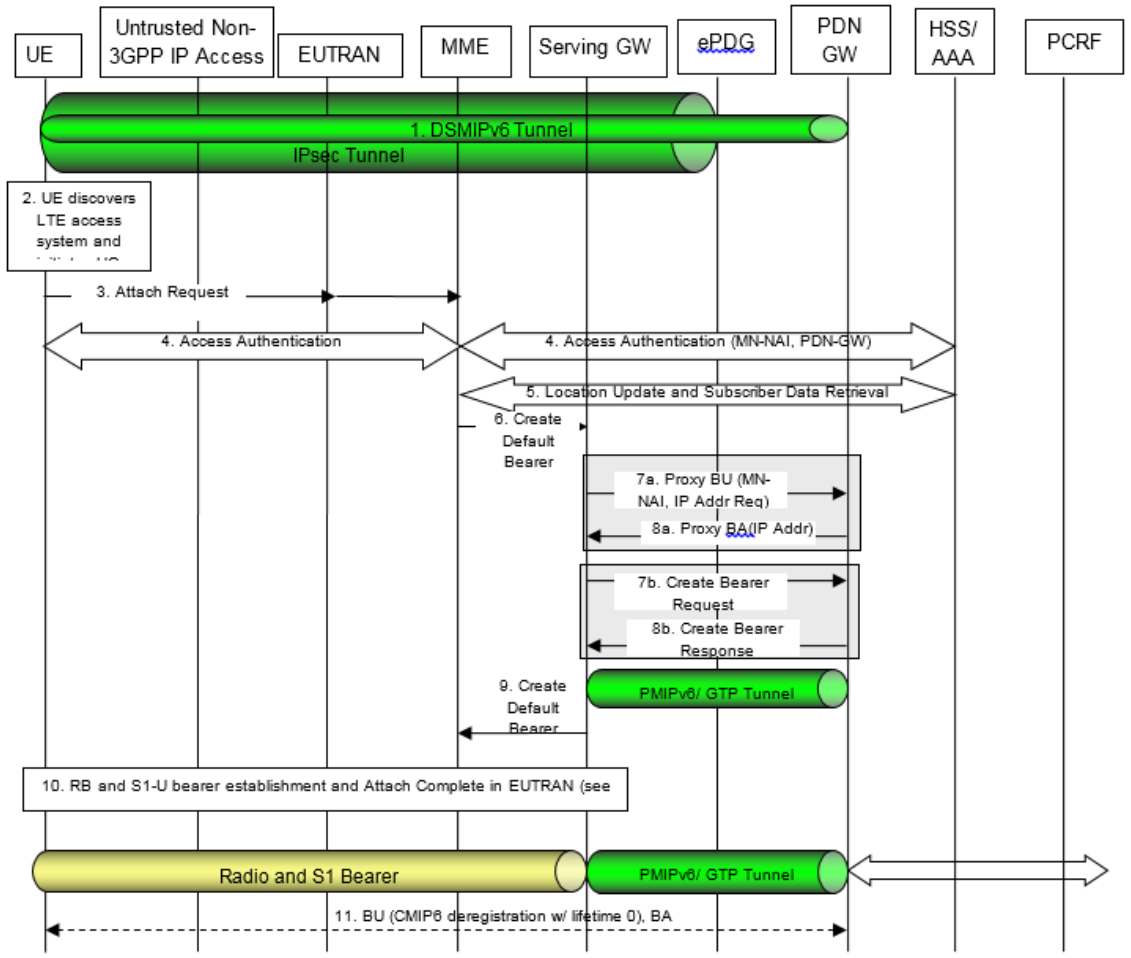

Figura 3.4.2.5: Traspaso de una red de acceso no-3GPP no confiable a LTE utilizando la interfaz S2c
Extraído de 3GPP TS 23.402

Paso 5: Luego de culminar con éxito el proceso de autenticación, la entidad MME procede a enviar un mensaje de actualización de ubicación al servidor HSS.

Paso 6: este paso equivale al paso 12 del registro del UE en la red LTE.

Paso 7: este paso equivale al paso 13 del registro del UE en la red LTE.

Paso 8: este paso equivale al paso 15 del registro del UE en la red LTE. El mensaje de "respuesta de creación de sesión" incluirá la dirección IP local que le fue asignada al UE en la red de acceso no-3GPP no confiable.

Paso 9: este paso equivale al paso 16 del registro del UE en la red LTE.

- **Traspaso de LTE a una red de acceso no-3GPP confiable utilizando la interfaz S2a y el protocolo PMIPv6 (Figura 3.4.2.6)**

Paso 1: el UE se encuentra conectado a una red de acceso 3GPP y existe un túnel PMIPv6 o GTP entre el nodo S-GW y el nodo P-GW del núcleo EPC.

Paso 2: el UE descubre una red de acceso no-3GPP y determina realizar un traspaso de las sesiones que ha establecido en la red 3GPP hacia la red de acceso no-3GPP. El nodo ANDSF podrá ser utilizado para asistir al UE en las funciones de búsqueda y selección de redes de acceso no-3GPP disponibles en el área de ubicación del UE.

Paso 3: en este paso el UE atraviesa por un proceso de autorización y autenticación en la red d acceso no-3GPP. Haciendo uso del protocolo EAP-AKA o EAP-AKA', el servidor AAA se encarga de autenticar al UE en la red de acceso no-3GPP. El servidor AAA se comunica con el servido HSS para solicitar la dirección IP del nodo P-GW que atiende al UE en la red de acceso 3GPP y enviarla a la red de acceso no-3GPP.

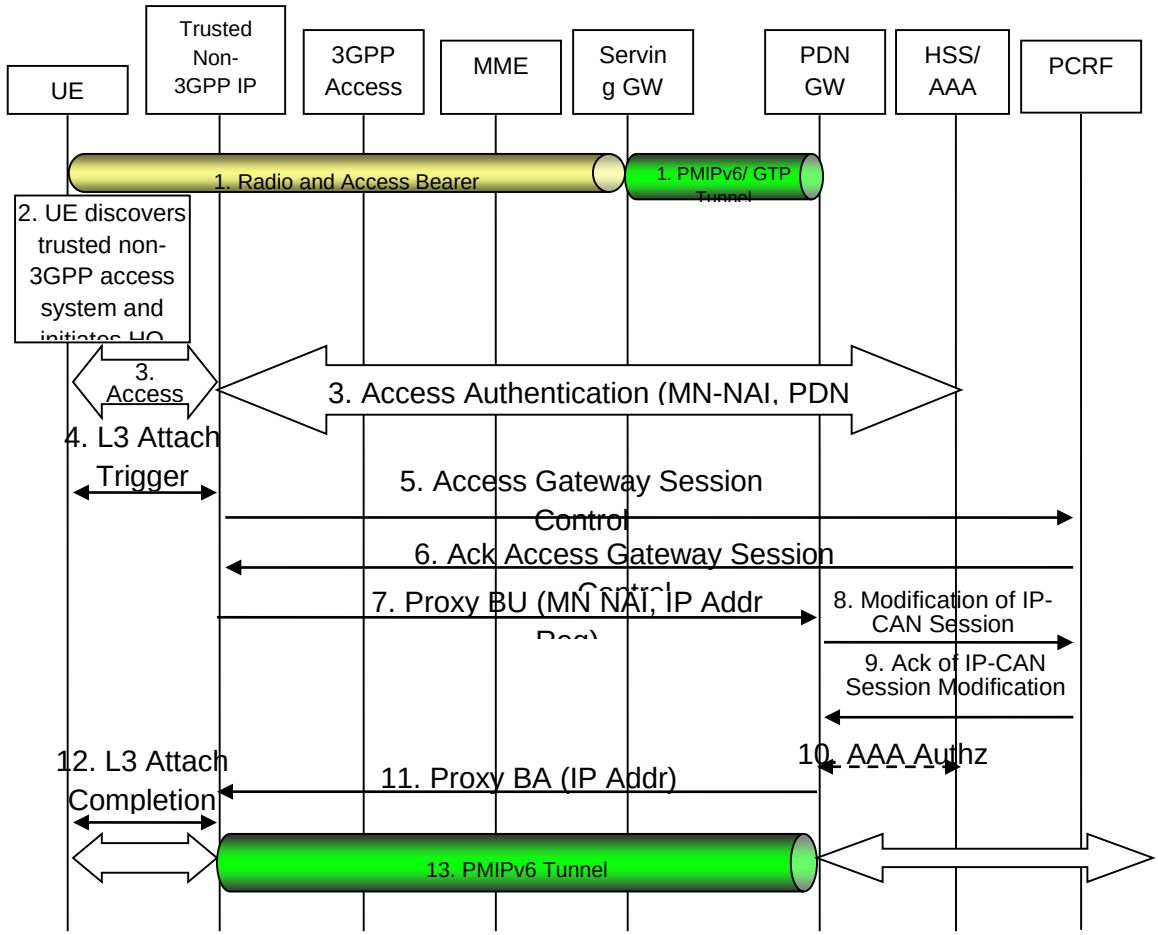

Figura 3.4.2.6: Traspaso de LTE a una red de acceso no-3GPP confiable utilizando la interfaz S2a
Extraído de 3GPP TS 23.402

Paso 4: una vez completada la autenticación y autorización, se da inicio al procedimiento de registro a nivel de capa 3 dentro de la red de acceso no-3GPP confiable.

Paso 5: la entidad que realice las funciones de BBERF (entidad de la arquitectura PCC y en nuestro caso el nodo WAG desempeñará estas funciones) procederá al envío de un mensaje "compuerta de control de sesiones" al nodo PCRF para obtener las reglas PCC requeridas en el nodo WAG de la red no-3GPP confiable para aplicarla el correcto trato de QoS a todas las sesiones activas que el UE haya establecido a causa del procedimiento de registro en la red de acceso no 3GPP. La dirección IP que el UE utilizaba en la red 3GPP, deberá ser compartida con la entidad WAG en la red de acceso no-3GPP.

Paso 6: el nodo PCRF envía un mensaje "acuse de compuerta de control de sesiones" a la entidad que realiza las funciones de BBERF. Este mensaje incluye los parámetros QoS para la red de acceso no-3GPP confiable.

Paso 7: la entidad en la red no-3GPP confiable que funciona como MAG (dispositivo WAG de una red Wi-Fi) envía un mensaje PBU *(Proxy Binding Update)* al nodo P-GW.

Paso 8: el nodo P-GW envía un mensaje de "modificación de la sesión IP-CAN" al nodo PCRF.

Paso 9: el nodo PCRF responde al nodo P-GW con un mensaje "acuse de modificación de la sesión IP-CAN". Este mensaje suministra al nodo P-GW con las reglas y políticas de tarificación predefinidas por el operador.

Paso 10: el nodo P-GW podrá interactuar con el servidor AAA en el caso de ser necesaria la autenticación de por ejemplo el nodo que desempeña las funciones de MAG (nodo WAG en una red Wi-Fi).

Paso 11: el nodo P-GW procesa el mensaje PBU y crea una nueva entrada en el cache de vinculación *(binding cahe)* para el UE. El nodo P-GW asigna la dirección IP del UE al enviar un mensaje PBA *(Proxy Binding Acknowledgement)* al nodo realizando las funciones de MAG en la red de acceso no-3GPP confiable.

Paso 12: el proceso de registro a nivel de capa 3 se ha completado en este punto y la dirección IP asignada por el nodo P-GW al UE le es enviada en este paso.

Paso 13: el túnel PMIPv6 ha sido establecido entre la red de acceso no-3GPP confiable y el nodo P-GW del núcleo EPC. En este punto el UE podrá enviar y recibir paquetes IP haciendo uso de la red de acceso no-3GPP confiable.

- **Traspaso de LTE a una red de acceso no-3GPP confiable utilizando la interfaz S2c y el protocolo DSMIPv6 (Figura 3.4.2.7)**

Paso 1: el UE se encuentra conectado a una red de acceso 3GPP y posee una dirección IP a través de la cual se conecta con el nodo P-GW por medio de la interfaz S5

Paso 2: en este paso el UE decide realizar un proceso de traspaso hacia una red de acceso no 3GPP confiable. El nodo ANDSF podrá ser utilizado para asistir al UE en las funciones de búsqueda y selección de redes de acceso no-3GPP disponibles en el área de ubicación del UE.

Paso 3: el UE inicia el proceso de autorización y autenticación dentro de la red de acceso no-3GPP confiable. El proceso de autorización y autenticación es realizado por el servidor AAA, una vez completado este proceso, el UE tiene acceso a la red de acceso no-3GPP confiable.

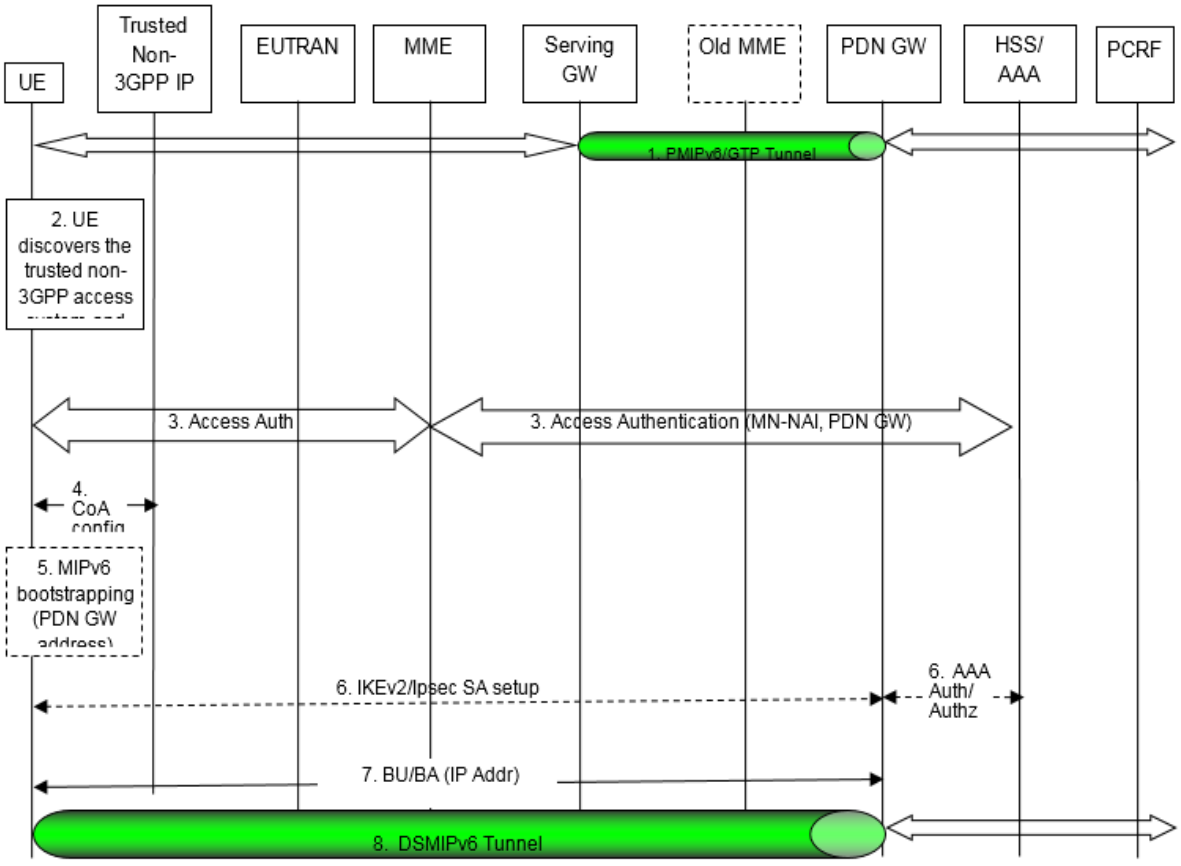

Figura 3.4.2.7: Traspaso de LTE a una red de acceso no-3GPP confiable utilizando la interfaz S2c
Extraído de 3GPP TS 23.402

Paso 4: el UE obtiene una dirección IP diferente a la dirección IP que utilizaba dentro de la red de acceso 3GPP, por lo tanto el UE en conjunto con la red, deberán iniciar los mecanismos de movilidad del protocolo DSMIPv6 para mantener las sesiones IP del UE.

Paso 5: el UE obtiene la dirección IP utilizando el procedimiento del protocolo MIPv6 llamado *bootstrapping.*

Paso 6: el UE podrá establecer una asociación de seguridad IKEv2 previo al establecimiento del túnel IPsec con el nodo P-GW. Esto sucede únicamente si se utiliza el RFC 4877 (la operación del protocolo MIPv6 con IKEv2) para el establecimiento de la asociación de seguridad entre el UE y el nodo P-GW. Este paso puede involucrar la autorización y autenticación del servidor AAA.

Paso 7: el UE envía un mensaje BU al nodo P-GW para registrar su dirección CoA. El nodo P-GW autentica y autoriza al UE y le envía un mensaje BA que incluye la dirección IP local que el UE utilizaba en la red de acceso 3GPP.

Paso 8: el UE continúa haciendo uso de los servicios IP utilizando la misma dirección IP de la red local 3GPP.

- **Traspaso de LTE a una red de acceso no-3GPP no confiable utilizando la interfaz S2b y el protocolo PMIPv6 (Figura 3.4.2.8)**

Paso 1: el UE se encuentra conectado a la red de acceso 3GPP E-UTRAN.

Paso 2: el UE se mueve de la zona de cobertura de la red y se conecta en una red de acceso no 3GPP no confiable*.*

Paso 3: el procedimiento de asociación de seguridad utilizando el protocolo IKEv2 es iniciado por el UE. La dirección IP del nodo ePDG con el cual el UE necesita establecer el túnel IPsec, puede ser provista por un servidor DNS o puede estar configurada de manera estática En este paso también se lleva a cabo la autorización y autenticación del UE, este proceso también involucra el envió de la información del nodo P-GW al nodo ePDG por medio del servidor AAA.

Paso 4: si las reglas PCC son soportadas dentro de la red de acceso no-3GPP no confiable, el nodo ePDG envía un mensaje “compuerta de control de sesiones” al nodo PCRF para informar acerca del proceso de traspaso y para obtener la información requerida en cuanto a los parámetros QoS.

Paso 5: si se lleva a cabo el paso 4, el nodo PCRF envía un mensaje “acuse de compuerta de control de sesiones” incluyendo la información relacionada con los parámetros QoS.

Paso 6: el nodo ePDG envía un mensaje PBU al nodo P-GW y solicita una dirección IP para el UE.

Paso 7: si las reglas PCC son soportadas dentro de la red de acceso no-3GPP no confiables, el nodo P-GW envía un mensaje de “modificación de la sesión IP-CAN” al nodo

PCRF para obtener cualquier tipo de cambio en cuanto los parámetros QoS y reglas PCC relacionadas con la sesión IP-CAN.

Paso 8: si se lleva a cabo el paso 7, el nodo PCRF envía un mensaje “acuse de modificación de la sesión IP-CAN” al nodo P-GW, este mensaje incluye información relacionada a cualquier posible cambio de los parámetros QoS o reglas PCC.

Paso 9: en este paso el nodo P-GW procesa el mensaje PBU que recibió del nodo ePDG y procede a crear una entrada en el cache de vinculación *(binding cache)* para el UE, luego responde con un mensaje PBA. El mensaje PBA incluye la dirección IP que el UE utilizaba en la red de acceso 3GPP. En este punto se ha establecido el túnel PMIPv6 entre el nodo P-GW y el nodo ePDG.

Paso 10: el nodo ePDG y el UE continúan el intercambio de información relacionada al protocolo IKEv2 y a la configuración de la dirección IP del UE.

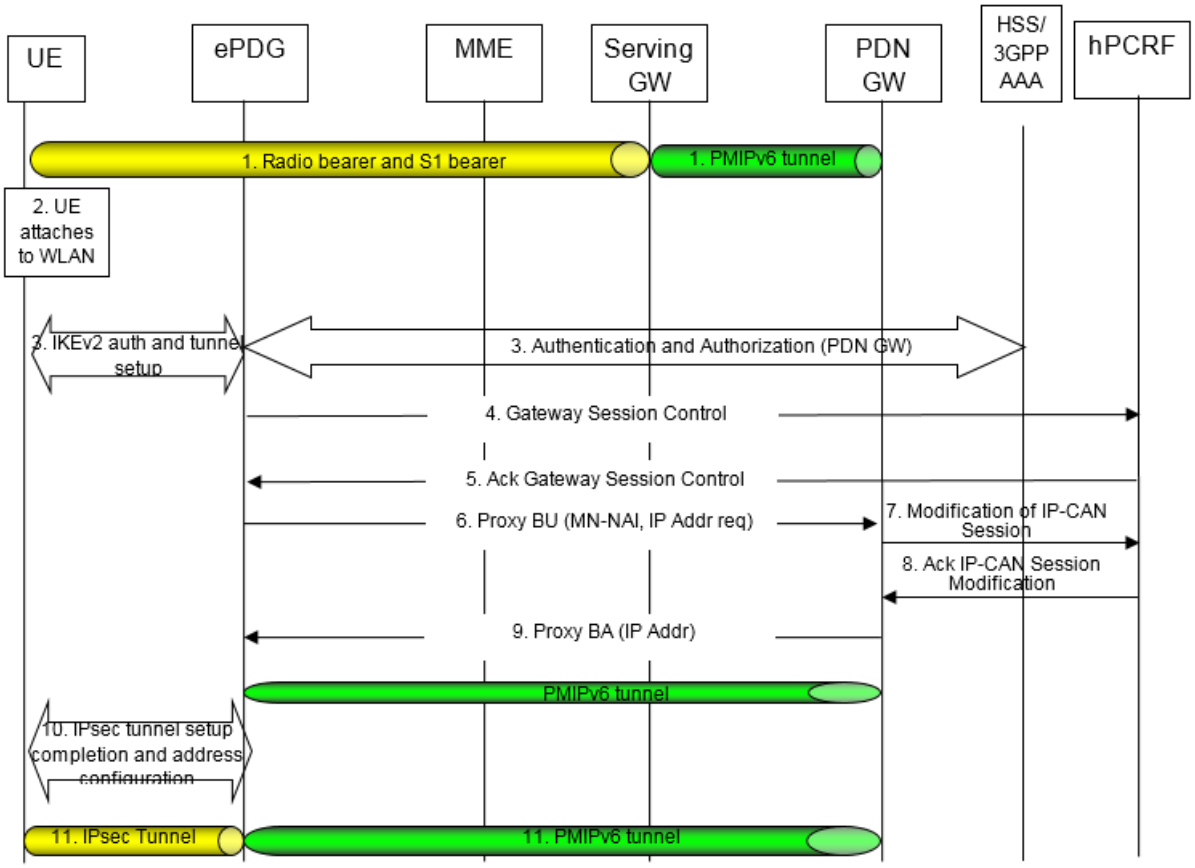

Figura 3.4.2.8: Traspaso de LTE a una red de acceso no-3GPP no confiable utilizando la interfaz S2b
Extraído de 3GPP TS 23.402

Paso 11: al final del proceso de traspaso, existe un servicio portador por defecto para el UE conformado por un túnel IPsec entre el UE y el nodo ePDG además del túnel PMIPv6 entre el nodo ePDG y el nodo P-GW.

- **Traspaso de LTE a una red de acceso no-3GPP no confiable utilizando la interfaz S2c y el protocolo DSMIPv6 (Figura 3.4.2.9)**

Paso 1: el UE se encuentra conectado a una red de acceso 3GPP y posee una dirección IP a través de la cual se conecta con el nodo P-GW por medio de la interfaz S5.

Paso 2: en este paso el UE decide realizar un proceso de traspaso hacia una red de acceso no 3GPP no confiable. El nodo ANDSF podrá ser utilizado para asistir al UE en las funciones de búsqueda y selección de redes de acceso no-3GPP disponibles en el área de ubicación del UE.

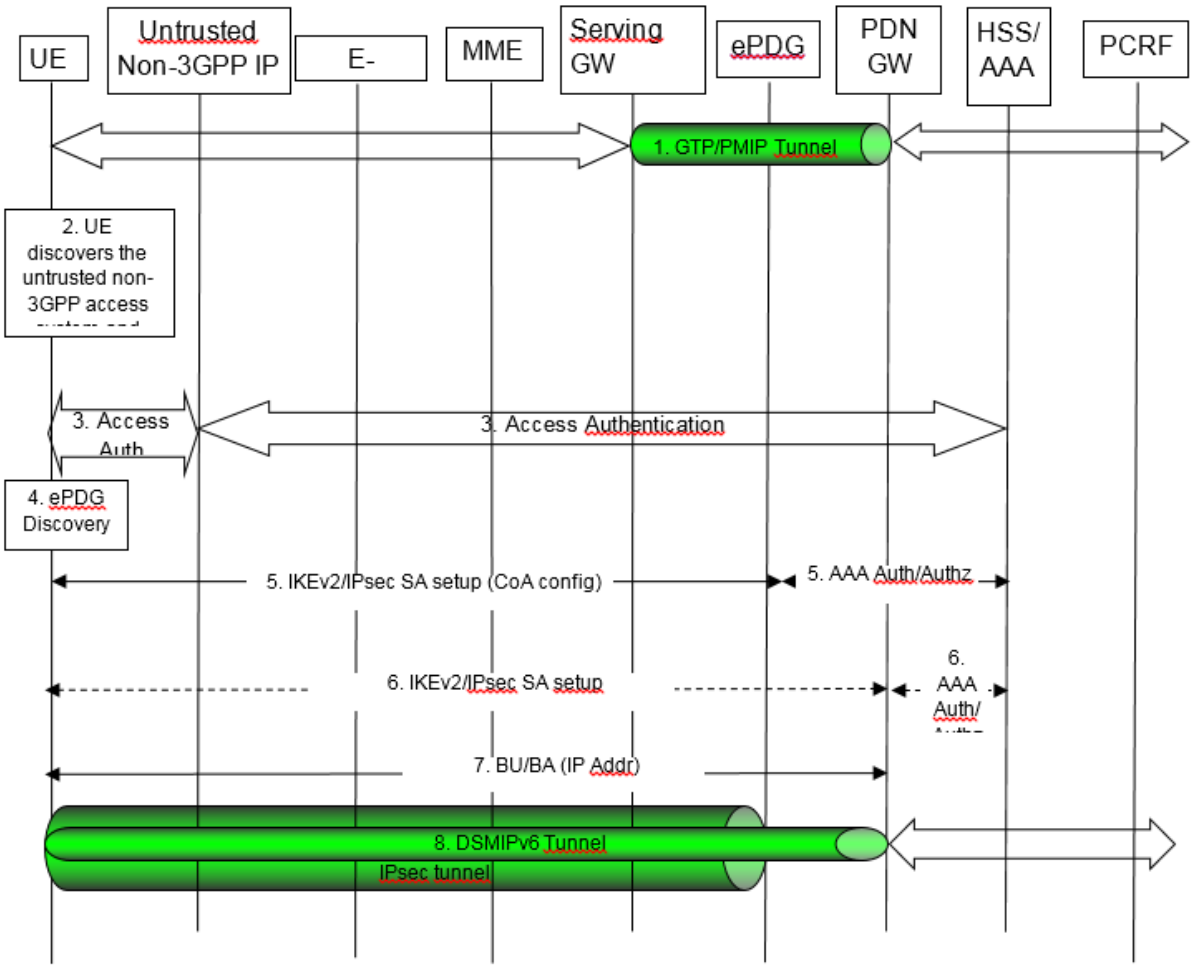

Figura 3.4.2.9: Traspaso de LTE a una red de acceso no-3GPP no confiable utilizando la interfaz S2c
Extraído de 3GPP TS 23.402

Paso 3: el UE inicia el proceso de autorización y autenticación dentro de la red de acceso no-3GPP no confiable. El proceso de autorización y autenticación se lleva a cabo entre los servidores AAA y HSS, una vez completado este proceso, el UE tiene acceso a la red de acceso no-3GPP no confiable.

Paso 4: el UE descubre la dirección IP del nodo ePDG (en caso de que no lo haya hecho con anterioridad).

Paso 5: el UE inicia las respectivas asociaciones de seguridad IKEv2 previas al establecimiento del túnel IPsec con el nodo ePDG que descubrió en el paso 4. En este paso el UE recibe una dirección IP por parte del nodo ePDG e inicia el procedimiento DSMIPv6 para mantener sus sesiones IP.

Paso 6: el UE podrá establecer una asociación de seguridad IKEv2 previo al túnel IPsec con el nodo P-GW. Esto sucede si se utiliza el RFC 4877 (la operación del protocolo MIPv6 con IKEv2) para el establecimiento de la asociación de seguridad entre el UE y el nodo P-GW. Este paso puede involucrar la autorización y autenticación del servidor AAA.

Paso 7: el UE envía un mensaje BU al nodo P-GW para registrar su dirección CoA. El nodo P-GW autentica y autoriza al UE y le envía un mensaje BA que incluye la dirección IP local que el UE utilizaba en la red de acceso 3GPP.

Paso 8: el UE continúa haciendo uso de los servicios IP utilizando la misma dirección IP de la red local 3GPP.

- **Caso especial: Traspaso entre dos redes de acceso no-3GPP no confiables conectadas al mismo nodo ePDG que utilizan la interfaz S2b y el protocolo PMIPv6 (Figura 3.4.2.10)**

Paso 1: el UE se encuentra conectado al nodo ePDG a través de un túnel IPsec, el nodo ePDG ha establecido un túnel PMIPv6 con el nodo P-GW.

Paso 2: el UE se desconecta a nivel de capa 2 de la red de acceso no-3GPP no confiable, para un mejor entendimiento, se le denomina a esta red como red de acceso 1.

Paso 3: el UE establece una conexión a nivel de capa 2 con otra red de acceso no-3GPP no confiable a la cual se le denomina como red de acceso 2.

Paso 4: se inicia la configuración de una dirección IP local en la red de acceso no-3GPP (red de acceso 2) no confiable.

Paso 5: haciendo uso del protocolo MOBIKE, se actualiza la dirección IP del UE con el nodo ePDG.

Paso 6: a través del envío de mensajes MOBIKE, el nodo ePDG realiza un proceso de verificación de la dirección IP del UE.

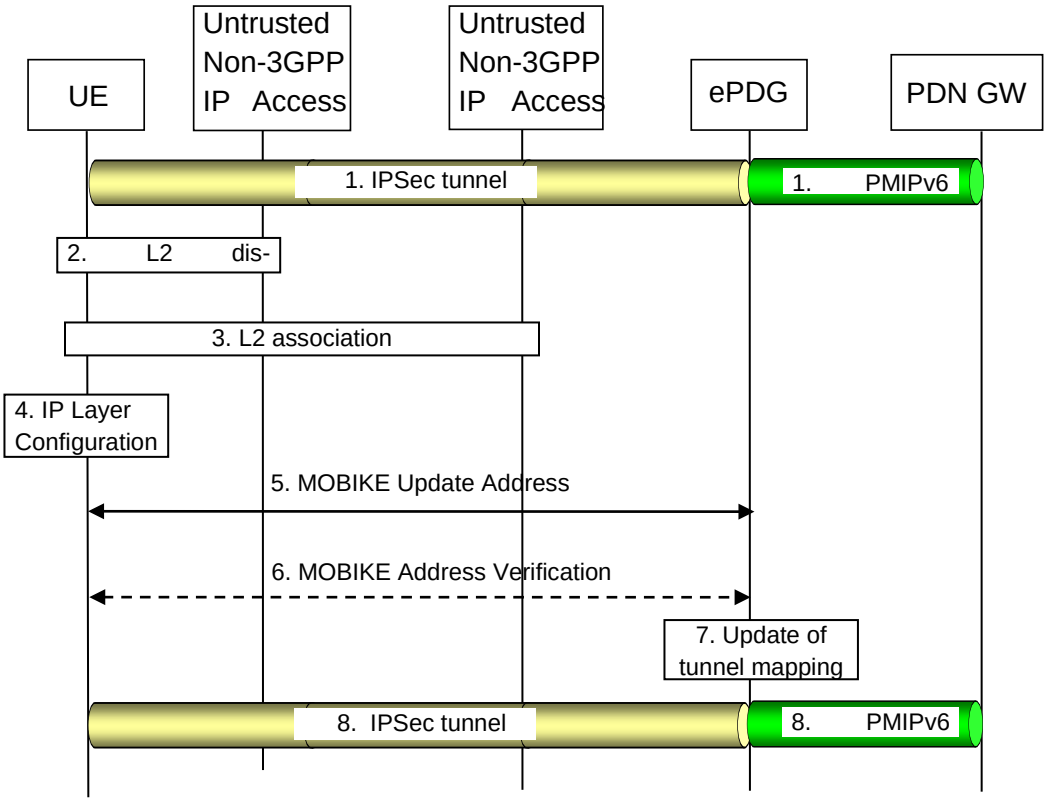

Figura 3.4.2.10: Traspaso dos redes de acceso no-3GPP no confiables utilizando la interfaz S2b
Extraído de 3GPP TS 23.402

Paso 7: se actualiza el mapeo del túnel IPsec con el túnel PMIPv6.

Paso 8: el túnel IPsec se encuentra funcionando en este paso.

- **Caso especial: Traspaso de una red de acceso no-3GPP no confiable que utiliza la interfaz S2b y el protocolo PMIPv6, a una red de acceso no-3GPP confiable que utiliza la interfaz S2a y el protocolo PMIPv6 (Figura 3.4.2.11)**

Paso 1: el UE se encuentra conectado a una red de acceso no-3GPP no confiable. Existe un túnel IPsec entre el UE y el nodo ePDG además de un túnel PMIPv6 entre el nodo ePDG y el nodo P-GW del núcleo EPC.

Paso 2: el UE inicia el proceso de traspaso hacia una red de acceso no-3GPP confiable.

Paso 3: en este paso se autoriza el acceso del UE a la red de acceso no-3GPP confiable.

Paso 4: se da inicio al procedimiento de autenticación basado en el protocolo EAP, este procedimiento involucra la interacción de la red de acceso no-3GPP confiable, del UE y del servidor AAA. Información acerca del nodo P-GW (la dirección IP por ejemplo) que será utilizado, es compartida con el nodo que realiza las funciones de MAG en la red de acceso no-3GPP confiable.

Paso 5: una vez completado el proceso de autenticación, se inicia el proceso de registro del UE dentro de la red de acceso no-3GPP confiable.

Paso 6: la entidad que realiza las funciones de MAG en la red de acceso no-3GPP confiable envía un mensaje PBU al nodo P-GW.

Paso 7: en este paso el nodo P-GW procesa el mensaje PBU que recibió de la entidad que realiza las funciones de MAG dentro de la red de acceso no-3GPP confiable y procede a crear una entrada en el cache de vinculación para el UE. Posteriormente el nodo P-GW envía un mensaje PBA a la entidad que realiza las funciones de MAG, este mensaje incluye la dirección IP que le será asignada al UE, esta dirección deberá ser la misma que le fue asignada al UE dentro de la red de acceso no-3GPP no confiable.

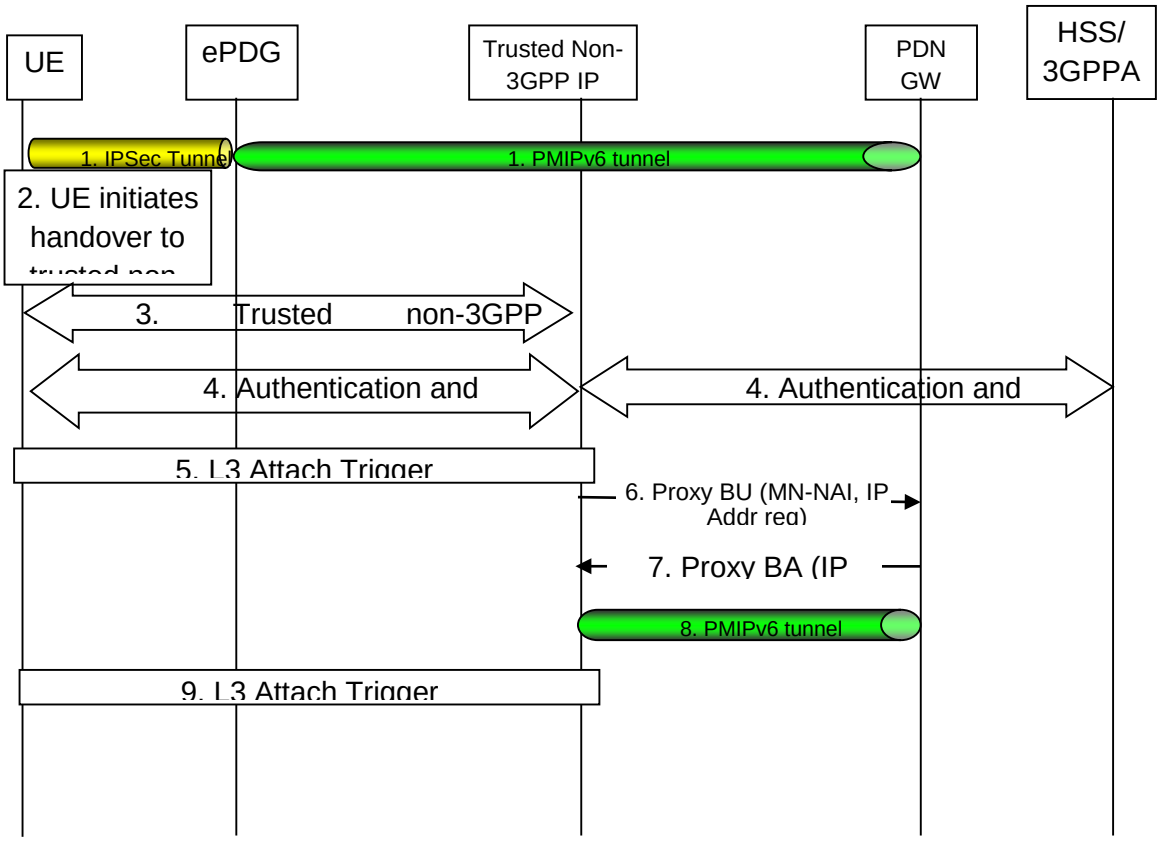

Figura 3.4.2.11: Traspaso de una red de acceso no-3GPP no confiable que utiliza la interfaz S2b y el protocolo PMIPv6, a una red de acceso no-3GPP confiable que utiliza la interfaz S2a y el protocolo PMIPv6
Extraído de 3GPP TS 23.402

Paso 8: se establece el túnel PMIPv6 entre la red de acceso no-3GPP confiable y el nodo P-GW del núcleo EPC.

Paso 9: el proceso de registro a nivel de capa 3 ha sido completado. La conectividad IP ha sido establecida entre el UE y el nodo P-GW tanto en el enlace ascendente como en el enlace descendente a través de la red de acceso no-3GPP confiable.

4. Discusiones y proyecciones.

4.1 Ventajas y retos de este tipo de red

Con base en los análisis previos se pueden discutir ciertas ventajas y desventajas que se identificaron cuando se decide tener este tipo de red.

Ventajas

- La ventaja principal que se identificó, es el desahogo de la red, una de las grandes preocupaciones de los operadores es la demanda de altas tasas de transferencias por parte de los usuarios, es el mismo motivo que impulso el desarrollo de LTE y de las mejoras posteriores, al añadir Wi-Fi básicamente se añade una opción al equipo por donde acceder a los servicios del proveedor.

- Al añadir una red de acceso Wi-Fi la infraestructura se convierte en un red más escalable y modular dado que ahora facilita su modificación en función de la carga de tráfico ya sea agregando nuevos *hotspot* o habilitando nuevos puertos en situaciones donde la red de acceso LTE este saturada o cualquier otra situación que le convenga al operador.

- Al añadir otra acceso a la red no solo se brinda una alternativa a LTE, sino también se incrementa la cobertura de servicio, Wi-Fi no depende de LTE basta con un acceso a internet, por lo que perfectamente puede ser empleado en ubicaciones donde haya poca o nula cobertura LTE.

- Otra de las ventajas principales es el uso de la tecnología Wi-Fi o el estándar 802.11, este ha revolucionado las redes de computadoras inalámbricas y su acogida ha sido masiva hasta tal punto que en la práctica los celulares inteligente o dispositivos móviles incorporan la tecnología Wi-Fi como norma, Lo cual abarata los costos de los equipos y facilita su implementación que además se aprovecha que en la mayor parte del mundo las bandas de frecuencias de operación de Wi-Fi son libres lo cual también aporta a que las redes de acceso sean implementadas con poca o ninguna regulación y sin necesidad de iniciar e invertir en procesos de licitación.

- Wi-Fi ofrece un gran rendimiento, hay que destacar que las velocidades o tasas de transferencias teóricas de los *amendments* del protocolo 802.11 (2012) son adecuadas para que el usuario mantenga o supere la calidad de su servicio en comparación con LTE. También aprovecha que el uso de IP, lo que le permite ofrecer movilidad (entre el mismo Wi-Fi como con LTE) con cierto o ningún esfuerzo del usuario.

Retos

- Las redes de acceso LTE y Wi-Fi son complejas tanto en diseño, implementación y mantenimiento, al mezclarlas se incrementa la complejidad de estos tres aspectos; la red de acceso Wi-Fi necesita infraestructura IP y como se ha expuesto también necesita ciertas entidades extras para poder conectarse al núcleo del sistema LTE, al tener una red mayor y con diferentes tecnologías los posibles puntos de fallos incrementan y esto incurre en mayor riesgo en la seguridad del sistema.

- Dado los procedimientos y precauciones requeridas por los riesgos de seguridad, se añade carga en el plan de control al núcleo de LTE que muchas veces se trata de evitar ya que estos pueden saturar la red.

- A pesar que Wi-Fi opere en bandas libres sea una ventaja como fue señalado, también significa una desventaja, ya que su uso no está controlado, lo que significa que mientras cumpla los requisitos cualquiera puede desplegar esta tecnología y podría causar interferencia y degradación del servicio.

- No todos los equipos que sean certificados Wi-Fi son compatibles con todos los *amendments* del estándar 802.11 y a pesar que lo sean, los procesos para conectarse al núcleo de LTE necesitan de protocolos adicionales, lo que reduce la cantidad de equipos que puedan hacer uso de esta red.

- La integración no es perfecta existen muchos problemas de selección de la red, muchas veces la red de acceso Wi-Fi puede estar más saturada que LTE sin que el equipo pueda darse cuenta.

- Movilidad presenta el mayor reto de la integración, pasar de una tecnología a otra y seguir manteniendo la conexión sería lo ideal sin embargo en la práctica estos procesos tienden a fallar y llegan a repercutir en el servicio e incluso pueden terminar las sesiones de conexión.

Según estudios realizados por la *4G Americas*, se han identificado los siguientes problemas de operación al momento de integrar una red LTE con Wi-Fi:

- Selección prematura de la red de acceso Wi-Fi: el terminal se conecta a una red Wi-Fi de manera prematura sin tener información alguna acerca del rendimiento de la red Wi-Fi en comparación con la red celular, lo que podría causar un impacto negativo en la experiencia del usuario en caso de haber degradación de los servicios debido a este traspaso a la red Wi-Fi.
- Elección inadecuada: El UE recibe la indicación de conectarse a una red de acceso Wi-Fi (con alto nivel de intensidad en la señal) pero esta se encuentra saturada. Esto conlleva a una degradación de los servicios y a causar un impacto negativo en la experiencia de usuario, en contraste con establecer conexión con

una red LTE (con carga de tráfico moderada) al borde de la celda de la cual se podría obtener un mejor desempeño que la red Wi-Fi congestionada.

- Elección de una red bajo desempeño de *backhaul*: El UE se conecta a un punto de acceso Wi-Fi que ofrece un bajo desempeño debido al ancho de banda provisto a través del *backhaul* de la red, en contraste al desempeño del *backhaul* de la red LTE.
- Ping-Pong: Este fenómeno ocurre en casos donde el UE se encuentre ubicado en zonas donde se cuente con múltiples puntos de acceso Wi-Fi y pocas áreas de solapamiento, el UE podrá encontrarse ejecutando varios ciclos de registro y traspaso generando un proceso repetitivo que afecte la experiencia del usuario.

4.3. Consideraciones a la hora de diseñar e implementar Wi-Fi sobre LTE para crear una red heterogénea

Como todo proyecto se necesita un plan de negocios, este cuenta con tres componentes principales [11]:

- El plan de mercado.
- El plan de ingeniería.
- El plan financiero.

A continuación describiremos cada una de estos planes de manera más detallada.

El plan de mercado

Este plan es indispensable para poder definir la oferta del producto y su aceptación por el mercado, deberá comprender el análisis de varios factores como son:

Evaluación socioeconómica de la región donde se pretende implementar la red, esto implica el estudio de la ubicación geográfica, un análisis de la población y de la economía de la región en cuestión.

Un estudio de la situación actual del mercado de la telefónica móvil así como también una proyección de esta en unos años en el futuro.

Un estudio acerca del comportamiento de los usuarios frente al uso de nuevas tecnologías, competencia y oferta del mercado, que llevara a definir cuál es el potencial del mercado.

Plan de ingeniería

Este plan se basa en el plan de mercado para definir su diseño y de esta manera cumplir con las condiciones determinadas por el plan de mercado.

A través de este plan se determinan los requerimientos para la implementación de la red, por consiguiente existen muchos factores a considerar:

- El modelo a seguir.
- Cantidad de equipos.
- Selección de los canales a utilizar para minimizar interferencias.
- Elección de los protocolos.
- Elección de los lugares donde se ubicaran los puntos de acceso Wi-Fi
- Cantidad de tráfico estimado que se pueda soportar.

Estos factores interactúan el uno con el otro y no pueden ser tratados separadamente. Al momento de crear un plan de ingeniería para el diseño de una red LTE también se toman en cuenta estos pasos adicionales:

Diseño de la red de acceso (RAN) en la zona geográfica elegida.

Para el diseño de la red de acceso se deben tomar en cuenta los siguientes pasos:

- Definir la banda de frecuencia de operación a utilizar, esto depende en gran manera del marco regulatorio del país y en los casos donde el operador posea bandas de operación previamente asignadas será conveniente usar las mismas o un rango entre esas bandas.
- En dependencia del modelo de propagación escogido, se deberán de realizar los cálculos que permitan definir la distancia de cobertura de los puntos de acceso por lo cual también se necesitan datos relacionados con la potencia de los transmisores usados.
- Determinar la capacidad y número de puntos de acceso que se utilizarán.
- Definir la topología de la red de acceso.

Diseño del núcleo EPC de la red LTE.

El núcleo de LTE como se pudo observar en el capítulo 2 varia un poco cuando se involucran otras tecnologías, para incorporar Wi-Fi se deberán configurar las interfaces pertinentes además de las entidades involucradas, se añade una nueva entidad básica para el funcionamiento en este caso ePDG.

A la hora de la selección y compra de los equipos que forman el núcleo EPC (nodo S-GW, nodo P-GW y la entidad MME) así como también la selección de un proveedor en específico del amplio portafolio de proveedores disponibles que brindan múltiples soluciones de núcleo tales como Ericsson, Alcatel-Lucent, Huawei, Qualcomm, por mencionar algunos, todas estas características vienen integradas de no ser así se deberá adquirir nuevos equipos.

En anexos podemos encontrar una solución propuesta por Alcatel-Lucent donde se aprecia el tipo de hardware que ofrece el proveedor para cada nodo de la red LTE.

Diseño de la red de transporte (*backbone*).

Por las características técnicas de LTE y Wi-Fi como su alto nivel en cuanto a las velocidades de transferencia y baja latencia, se requieren medios que soporten altas tasas de transmisión, la fibra óptica se considera como un medio ideal para este trabajo.

Esta parte también abarca la parte de la infraestructura y subsistemas presentes en las estaciones base:

- Uso de equipos auto-soportadas.
- Sistema de puesta a tierra.
- Pararrayos.
- Banco de baterías de respaldo.
- Sistemas de alarmas en caso de fallas (fallas al sistema de energía, sistema de ventilación, sistema de seguridad).

Cabe destacar que en este capítulo se considera al proveedor de servicio LTE como el que implementa la red de acceso Wi-Fi de no ser así muchos de los pasos anteriores no aplican ya que solo se deberá modificar el núcleo y interconectar si es necesario las dos redes.

Plan financiero

Este plan analiza la posibilidad de un riesgo financiero. Actualmente existen paquetes de software especializados que permiten generar un plan financiero con base en la tecnología que se va a utilizar para el despliegue de la red. Este plan se desarrolla a la par con el plan de mercado y el plan de ingeniería [11].

Este plan considera los siguientes factores:

CAPEX *(Capital Expenditure)*: es la inversión de capital que se realiza por año. Los puntos a considerar son: adquisición del espectro, infraestructura (torres, baterías, etc.), equipos de la estación base, equipos del núcleo y el *backhaul* de la red.

OPEX *(Operational Expenditure)*: son los gastos operacionales tales como rentas, costos de operación y mantenimiento, arrendamientos, costos de interconexión (con otros operadores, con la telefonía fija), costos por mantenimiento de *backhaul*, costos de facturación, costos de los equipos, costos de acceso a internet, entre otros

Normalmente existe una gran inversión en el despliegue de una red LTE y siendo una red de 4ta. Generación se asume que será suficiente para dar abasto a un mercado pequeño como Nicaragua y que genere ganancias, deberá existir anuencia de parte del operador para crear un valor agregado al usuario que este tipo de red pueda generar.

4.2 Contexto Nicaragüense

TELCOR (Instituto de telecomunicaciones y correos de Nicaragua)

Las telecomunicaciones están reguladas por la ley No. 200 que establece como objetivo principal lo siguiente:

“La presente Ley tiene por objeto la regulación de los servicios de telecomunicaciones y servicios postales, y establecer los derechos y deberes de los usuarios y de las operadoras, en condiciones de calidad, equidad, seguridad, y el desarrollo planificado y sostenido de las telecomunicaciones y servicios postales. La normación, regulación, planificación, supervisión, aplicación y el control del cumplimiento de las normas que rigen las telecomunicaciones y servicios postales corresponde al Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR), como Ente Regulador”.

TELCOR fue creado en 1982 por el decreto de ley No. 1053 no solo con la finalidad de regular las telecomunicaciones en el país sino también para fomentarlas como establece la constitución política de Nicaragua. En el Art 3 de la ley orgánica de TELCOR se atribuye la siguiente facultad:

“Controlar todo lo relativo a las actividades en las ramas telefónicas, telegráficas, postal facsímil, radiofoto, datos telefrecuencias, filatelias, o cualquier otro servicio relativo conocido o por conocerse en el campo de las telecomunicaciones, para lo cual tendrá que participar en actividades d planificación y ejecución de proyectos, en todos estos campo o en cualquier otra actividad mencionada con sus objetivos”

Proveedores de servicio:

Nicaragua cuenta únicamente con 3 proveedores de servicio de telefonía celular:

- **Movistar:** Es un operador con licencia para ofrecer Servicio de telefonía celular y acceso a internet cuenta con más del 40% del mercado de telefonía celular según cifras de TELCOR

  Tiene desplegado GSM, UMTS y HDSPA en la banda 850 MHz y 1900 MHz

  Actualmente movistar ofrece los siguientes servicios de telefonía celular:

  - Llamadas de voz nacionales e internacionales.
  - Mensajes de texto
  - Acceso a internet por medio de tecnología celular.

- **Claro:** Es un operador con licencia para ofrecer Servicios de telefonía fija, telefonía celular, trasmisiones de punto a punto, trasmisiones de datos, acceso a internet, televisión por suscripción.

Tiene desplegado GSM, UMTS, HDSPA, y HDSPA+ en las bandas 850 MHz y 1900 MHz

Actualmente claro ofrece los siguientes servicios de telefonía celular:

- Llamadas de voz nacionales e internacionales.
- Mensajes de texto
- Acceso a internet por medio de tecnología celular.

- **Xinwei Telecom Technology**: Es un operador con licencia para ofrecer Servicios de telefónica celular, acceso a internet entre otros.

Actualmente no ofrece ningún servicio a nivel de usuario.

También existen compañías que ofrecen el servicio de acceso a internet inalámbrico:

- **Yota:** Es un operador con licencia para ofrecer el servicio de telefonía fija, acceso a internet y trasmisión de datos.

Tiene desplegado Wi-Max en la banda 2.5 GHz

Actualmente Yota ofrece acceso a internet por medio de la tecnología Wi-Max

- **IBW:** Es un operador con licencia para ofrecer acceso a internet y lo hace al igual que Yota por medio de Wi-Max

Wi-Fi

El uso de Wi-Fi es libre, Telcor a través del acuerdo administrativo 001-2006 como lo recomienda la UIT define ciertas bandas de frecuencia para uso ICM (Industrial, científico, medico) que abarca Wi-fi.

Nicaragua no produce equipos de este tipo y se tienen que importar de mercados extranjero siendo, la mayoría de estos productos viene de Asia.

Nicaragua tiene procesos de homologación y controla todos los equipos de telecomunicaciones que entren al país incluyendo Wi-Fi

LTE

LTE ha sido una gran apuesta para la región tanto en Latinoamérica y en CA sin embargo Nicaragua no cuenta con red LTE desplegada hasta la fecha de entrega de este documento, de las empresas que listamos con anterioridad según informes de 4gamericas.com las empresas claro en la banda 700 al igual que movistar están en fases de pruebas y Xinwei en la banda 2600.

La banda 700 esta listada por Telcor para radiodifusión televisiva.

La banda 2600 esta listada para conexiones de punto a punto o televisión por suscripción.

De igual manera TELCOR puede habilitar las frecuencias para que las empresas prueben y diseñen las redes, sin embargo como lo establece la ley 200 a las empresas que querrán brindar servicio deberán pasar por los procedimientos establecidos para que se les otorgue una licencia para operar en las bandas deseadas.

4.5 Posibilidad de implementación en Nicaragua

La posibilidad de que se implemente una red heterogénea de este tipo radica principalmente en la comercialización de LTE por parte de los proveedores de servicios de telecomunicaciones del país.

También el gobierno a través de TELCOR debe incentivar el campo de las telecomunicaciones para que el usuario tenga mejores servicios, se deberá facilitar licencias y permisos para que los proveedores miren atractivo ofertar Wi-Fi como tecnología secundaria en sus redes LTE

4.5.1 Móldelo basado en posible implementación en Nicaragua.

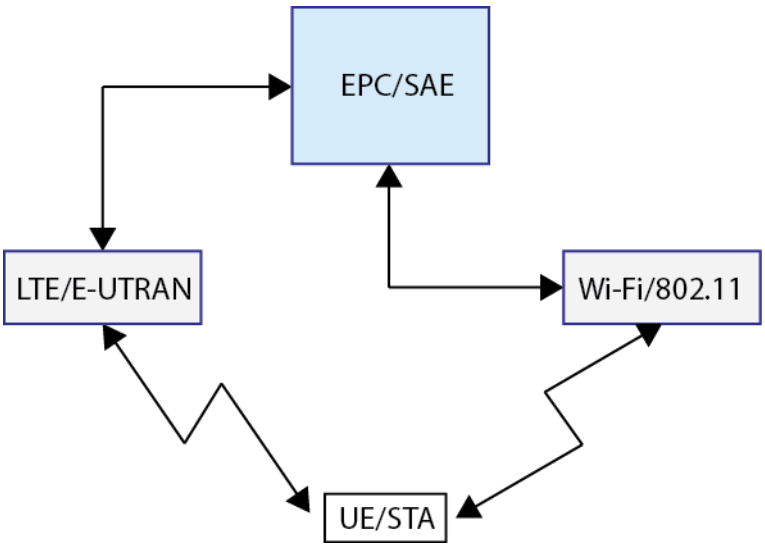

Figura 4.5.1: Esquema de red LTE/Wi-Fi básico de posible implementación en Nicaragua.

La Figura 4.5.1 representa en forma general el esquema básico de la integración y de la forma que interactúan los elementos de una red heterogénea LTE/Wi-Fi.

Hay que considerar que Nicaragua no cuenta con la red LTE desplegada hasta la fecha. Dado que la integración de la Figura 1.4.1 no es considerada práctica con Wi-Fi sino hasta *releases* posteriores al 11 se deberá considerar la red Wi-Fi como una red no confiable

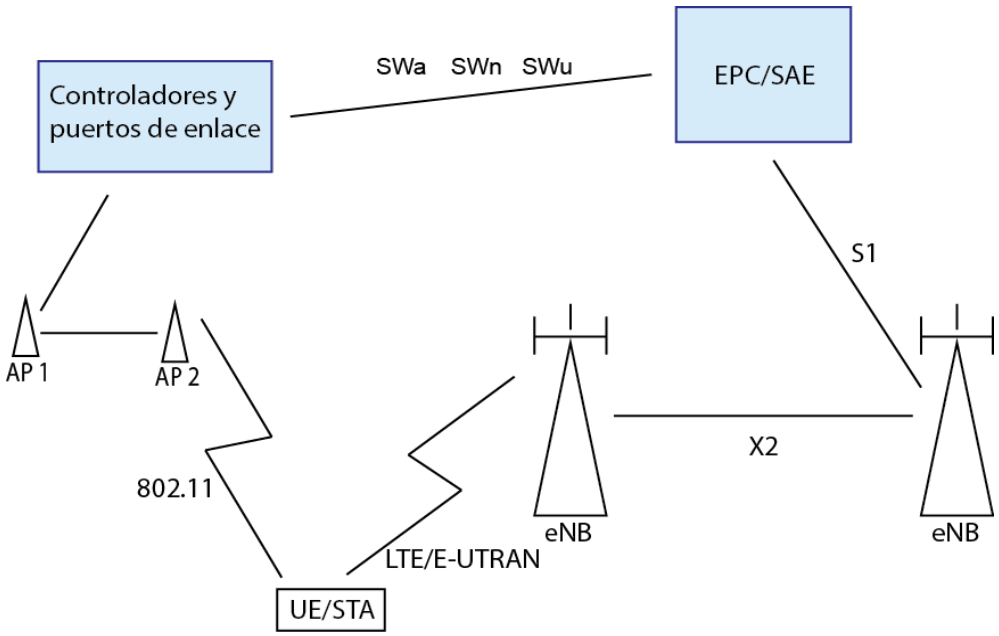

Figura 4.5.2: Esquema de red LTE con Wi-Fi considerada como no confiable

La Figura 1.4.6 muestra la red heterogénea considerando la red Wi-Fi como no confiable, la arquitectura es la misma que se muestra la Figura 1.4.6.

La infraestructura de la red de acceso Wi-Fi se considera en primera instancia sea desplegada y mantenida por los proveedores.

4.5.2 Oportunidad

Las telecomunicaciones han demostrado ser un mercado muy activo sobre todo en tecnologías de acceso de banda ancha, la demanda de mejores tecnologías y servicio por parte de los consumidores han empujado a los desarrolladores y empresas a buscar respuestas adecuadas.

Las redes de nueva generación basadas en el protocolo IP han sido la apuesta del mercado lo cual genera un soporte de la comunidad científica y del sector comercial permitiendo la rentabilidad y prolongando el tiempo de uso de las redes desplegadas.

Así mismo implementar estas tecnologías en una red heterogénea fomentaría al desarrollo de las TICs dado que existiría una retroalimentación entre Wi-Fi y LTE que se toma en cuenta en futuros desarrollos.

Los países subdesarrollados necesitan invertir en infraestructura para la creación e incremento del capital, además de generar por si misma también se crea un soporte a las demás industrias lo que se traduce en más competitividad en la región, que ha visto en

LTE la oportunidad de crecer tecnológicamente, esto se evidencia ya que muchos países de Centroamérica y el Caribe cuentan con red desplegada según datos de la 4Gamericas.com

Contar con redes de banda ancha como LTE abre un nuevo abanico de servicios que antes no eran posibles o se miraban limitados con las redes de generación anterior así mismo Wi-Fi se integra para ofrecer estos servicios manera más integral.

Cloud (Nube): este servicio se divide en dos; infraestructura y software como servicio, y pueden existir tanto de forma privada como pública. En estos nuevos modelos se accede a estos recursos deseados a través de internet o alguna conexión privada es por eso que las tecnologías de banda ancha son requeridas para poder explotar de manera correcta estos servicios, las redes de nueva generación y redes heterogéneas por sus velocidades y movilidad son perfectas para acceder a estos servicios.

Multimedia: Este es uno de los servicios que ha impulsado a la tecnología, el consumo de contenido multimedia requiere tasas de transferencias altas que las tecnologías anteriores a la 3generacion no podían brindar.

Entre los principales medios consumidos están música y videos estos tanto en descarga como en *streaming*, la capacidad de los dispositivos y de los proveedores de servicios para reproducir contenido en alta calidad ha creado una gran demanda, este tipo de servicios se puede ver muy beneficiado de redes heterogéneas y no saturar la red LTE.

VoIP (*Voice over IP*, Voz sobre IP): Este servicio se encarga de enviar las llamadas de voz haciendo uso de paquetes IP en lugar de la conmutación de circuitos, para lograr que la transmisión de la voz a través de paquetes IP sea exitosa se hace uso del protocolo H.323 que fue diseñado con la finalidad de enviar voz y video a través de redes públicas como el internet o redes privadas como una intranet.

Siendo LTE una red basada en IP de principio a fin al igual que Wi-Fi, la implementación de este servicio dentro de las redes heterogéneas se vuelve una realidad cada vez más latente.

VoWi-Fi (*Voice over Wi-Fi*, Voz sobre Wi-Fi): Este es un servicio que recientemente ha captado la atención de muchos operadores a nivel mundial y en especial por aquellos que cuentan con redes Wi-Fi propias y desplegadas en lugares estratégicos o con poca cobertura por parte de la red celular.

A inicios del año 2014 los operadores T-Mobile y Sprint (en EE.UU) comenzaron a implementar el servicio VoWi-Fi y a esta lista de operadores se han sumado AT&T, Verizon, Vodafone UK, O2 entre otros.

Este servicio se ve como una alternativa más viable y rentable que el empleo de femto-celdas para usos de interiores en lugares donde se tiene pobre o nula cobertura por parte de la red celular lo que dificulta el establecimiento de cualquier tipo de comunicación ya sea voz o datos.

Video llamadas: Similar al consumo multimedia, las video llamadas dependen de la trasmisión de video y audio en tiempo real, lo cual requiere altas tasas de trasferencias y latencia mínima, el contar con una red heterogénea amplia la oportunidad de encontrar estas características en la red.

Itinerancia: Esta es uno de los grandes potenciales debido a la gran compatibilidad que goza Wi-Fi, cosa que no se puede decir lo mismo de LTE, debido a distintas regulaciones como se ha presentado, LTE puede operar en múltiples bandas si el equipo que visita un red LTE no es compatible con la banda no tendrá servicio.

Los dispositivos usualmente integran Wi-Fi, y les facilita poder conectarse al sistema LTE visitado a través de este, y utilizar todo los servicios que el operador local haya negociado con el operador visitado.

5. Conclusiones y recomendaciones

5.1 conclusiones

Las redes de nueva generación se han decantado por el protocolo IP y este ha permitido que la integración con diferentes tecnologías se lleve a cabo de una manera más simple y sacándole más provecho a estas.

Tanto LTE como Wi-Fi son tecnologías que utilizan el protocolo IP sin embargo estas tecnologías son muy diferentes en sí; LTE utiliza distintos protocolos para poder realizar muchas tareas y características que no están presentes en redes inalámbricas Wi-Fi y viceversa.

Como conclusiones tomamos dos aspectos:

1. **Acceso**

   El acceso de Wi-Fi a la red LTE conlleva agregar y configurar entidades a la arquitectura de red, todo lo expuesto en esta investigación nos lleva a concluir que las redes heterogéneas no son fáciles de implementar, hay que tomar consideraciones que recaen en el operador según la manera que se quiera desplegar esta red.

   En el caso de la red LTE/Wi-Fi presenta ciertas variables que se debe tomar en cuenta y las decisiones tomadas pueden incluso variar los diagramas que son presentados en esta investigación.

   El operador principalmente deberá elegir que tanto confía en la red de acceso Wi-Fi ya que esta decisión cambiara la arquitectura de la red LTE de diferente manera tanto si la considera como confiable como no confiable.

   La red de acceso inalámbrica Wi-Fi presenta cierta libertad en su diseño sin embargo siempre debe de llevar los elementos necesarios para poder integrarse con el sistema LTE según la arquitectura que haya elegido el operador, cabe destacar que la red Wi-Fi no es necesariamente propiedad del operador aunque en muchos casos lo sea, si la red de acceso no es del operador tiene que tener ciertos aspectos necesarios para conectarse al sistema LTE y la práctica común es destinar este tipo de redes ya sea de públicas o privadas como no confiables.

   Como conclusión en este aspecto de la interoperabilidad, independiente de cómo se considere la red de acceso Wi-Fi, los elementos principales son las interfaces que permiten la interoperabilidad, estas utilizan una serie de protocolos de diferentes capas para poder realizar las funciones necesarias para el intercambio tanto en plano de control como de usuario tomando mayor valor los protocolos que permiten crear túneles hacia la entidad deseada.

2. Movilidad

El acceso a una red no es suficiente, la interoperabilidad en una red inalámbrica requiere que el dispositivo pueda desplazarse entre las redes de acceso y mantener cierto nivel de calidad en el servicio.

La movilidad por todos los procesos que se presentaron es lo que presenta mayor reto ya que un proceso de traspaso requiere protocolos de movilidad presentes en las dos redes de acceso y además en el equipo.

Todas las soluciones de movilidad dependen del protocolo IP que sirve como un punto de anclaje para poder retomar las conexiones pendientes, como se puede observar en los procesos presentados la mayoría son genéricos Wi-Fi y LTE no están optimizados para el traspaso de sesiones aunque en releases posteriores al 8 se han hecho ciertos avances sobre todo en el nodo ANDSF.

Este estudio descriptivo tiene como principal fuente la documentación de la 3GPP como fuente primaria, en conclusión es vital, ya que presenta la interoperabilidad y hace referencia a protocolos y estándares definidos no solo por ellos sino por otras organizaciones como la IEEE, ISO, IETF, entre otros.

La búsqueda para integrar Wi-Fi a LTE o tecnologías 3GPP se puede observar en las definiciones de los *releases* que incluso en tecnologías pasadas les dedicaron especificaciones técnicas a esta, en el caso de LTE ha ido de manera genérica hasta dar respuesta a problemas específicos de la integración con Wi-Fi en los últimos *releases* publicados.

El estudio comprende las funciones, protocolos, elementos y las diferentes arquitecturas en la red LTE sin embargo la red física es diferente, la mayoría las empresas desarrolladoras de equipo vende paquetes que en su mayoría utilizan software y hardware propietario para realizar las funciones definidas por las organizaciones además de integrar múltiples entidades en un solo equipo físico.

También se debe entender que todas las arquitecturas presentadas dependen de una red física de transporte IP, servidores DNS, DHCP etc., que son fundamentales para el funcionamiento de los procesos presentados en esta tesis.

La interoperabilidad aquí presentada es funcional y ha sido implementada en muchas partes del mundo, presenta grandes ventajas y abre nuevas oportunidades, las redes heterogéneas son el resultado de los procesos de estandarizaciones y grupos de trabajo que en las últimas décadas han desarrollado tecnologías que den respuestas a las necesidades del mercado de las telecomunicaciones.

Las redes heterogéneas promueven el desarrollo de las tecnologías involucradas no solo en el aspecto de interoperabilidad y competencia sino también en la evolución de ellas mismas.

5.2 Recomendaciones

Las tecnologías celulares son definidas de manera amplia por las organizaciones como la 3GPP sin embargo existen muchas limitantes a la hora del análisis, incluso fuentes secundarias que son propios análisis de estas tecnologías no son aptas por el idioma, contexto, y accesibilidad.

Es necesario que la comunidad científica de Nicaragua se involucre en el desarrollo de los estudios para retroalimentarse y crear recursos académicos que sean fuentes y soporte a los futuros estudios.

La investigación presentada por su naturaleza genera ciertos aspectos los cuales queda pendiente ampliar más:

- **Interferencia Wi-Fi/LTE:** Para una mejor armonía en cuanto al funcionamiento de LTE y Wi-Fi como tecnologías implementadas en conjunto para formar una red heterogénea, se deberá estudiar el impacto de la interferencia que se podría generar al momento de seleccionar las frecuencias de operación en las cuales vaya a funcionar la red LTE debido a que bandas de frecuencia como la 40, 7, 38 y 41, son cercanas a las bandas de frecuencia que opera Wi-Fi además del análisis de tecnología adicionales como filtros para minimizar la interferencia y lograr una mejor coexistencia entre Wi-Fi y LTE.
- **Administrador de conexiones:** El administrador de conexiones integrado en el UE jugara un papel clave en cuanto al mejor aprovechamiento de los recursos que brinde la red heterogénea, las soluciones hasta la fecha son muy básicas y presenta un potencial que se debe explotar y estudiar más.
- **ANDSF:** Este nodo es fundamental para el desarrollo de las redes heterogéneas de LTE, ha sido definido en forma básica desde el *release* 8 sin embargo se ha desarrollado mucho en los *releases* posteriores, al igual que el administrador de conexiones la implementación es muy básica, sin embargo esta es la solución para que la integración sea invisible para el usuario.
- **Reordenamiento de espectro:** uno de los temas más discutidos en el mundo de las telecomunicaciones y es necesario que Nicaragua haga estudios basados en investigaciones para reordenar el espectro disponible a tecnologías que beneficien al país como lo es el caso de LTE y Wi-Fi.

El tema propuesto delimita la red heterogénea a Wi-Fi/LTE sin embargo LTE permite la interoperabilidad con muchas otras tecnologías se recomienda que se estudien estas otras posibilidades.

En este estudio también se recomienda que se realice una investigación de carácter similar cuando se cuente con la tecnología LTE desplegada en Nicaragua que genere datos más certeros a un posible diseño y estudio de viabilidad de una red heterogénea LTE/Wi-Fi.

6. Bibliografía

[1] Rose Qingyang Hu; Yi Qjan, Heterogeneous cellular networks, Wiley, 2013.

[2] IEEE, "IEEE Std 802.11™-2012 (Revision of IEEE Std 802.11-2007)," The Institute of Electrical and Electronics Engineers, Inc., Nueva York, 2012.

[3] Eldad Perahia, Robert Stacey, Next Generation Wireless LANs, Segunda ed., Cambridge University Press, 2013.

[4] Christopher Cox, An Introduction to LTE, LTE –Advanced, SAE and 4G Mobile Communications, Wiley, 2012.

[5] Ramón Agusti, Francisco Bernardo, Fernando Casadevall, RamonFerrús, Jordi Pérez- Romero, Oriol Sallent, LTE: Nuevas Tendencias En Comunicaciones Móviles, Fundación Vodafone España, 2010.

[6] S. P. a. Erik Dahlman, 4G LTE/LTE-Advanced, Elsevier, 2011.

[7] T. Ali-Yahiya, Understanding LTE and its Performance, Springer New York Dordrecht Heidelberg London, 2011.

[8] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid, Catherine, Mulligan, EPC and 4G Packet Networks, Segunda ed., Elsevier, 2013.

[9] L. X. Chen Yangyang, Architecture and Protocols of EPC-LTE with relay, Telecom Bretagne.

[10] T. Z. Jyh-Cheng Chen, IP-Based Next-Generation, John Wiley & Sons, Inc, 2004.

[11] L. Korowajczuk, LTE, WIMAX AND WLAN NETWORK DESIGN,OPTIMIZATION AND PERFORMANCE ANALYSIS, John Wiley & Sons, Ltd, 2011.

[12] Shedman Tam , "Architectural Framework for the Non-3GPP Evolved Packet System (EPS) Access Tile," 2009. [Online]. Available: http://www.msforum.org/.

[13] 4G Americas, Integration of Cellular and Wi-Fi Networks, 2013.

[14] A. Schumacher / J. Schlienz, WLAN Traffic Offload in LTE, 2012.

[15] M. Sauter, FROM GSM TO LTE AN INTRODUCTION TO MOBILE NETWORKS AND MOBILE BROADBAND, John Wiley and Sons, Ltd, 2011.

[16] WNDW, Redes inalámbricas en los países en desarrollo, Cuarta ed., 2013.

[17] Zhang J. y de la Roche G., Technologies and Deployment, Wiley, 2010.

[18] 4G Americas, *Developing Integrating High Performance Het-Net,* (White Paper), 2012.

[19] Ahmed H. Hassanein, "New Authentication and Key Agreement Protocol for LTE-WLAN Interworking," 2013. [Online]. Available: www.ijcaonline.org.

[20] Jie Zhang, Guillaume de la Roche, Femtocells Technologies and Deployment, Wiley, 2011.

7. Anexos

7.1 Especificaciones técnicas de protocolos y tecnologías relacionadas

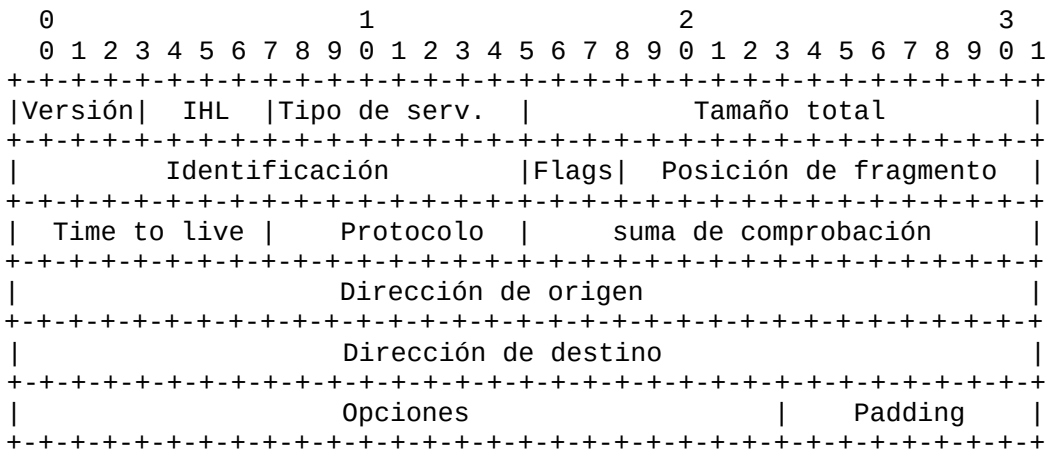

Figura 7.1.1. Cabecera IPv4
Extraído de RFC 791 [https://www.ietf.org]

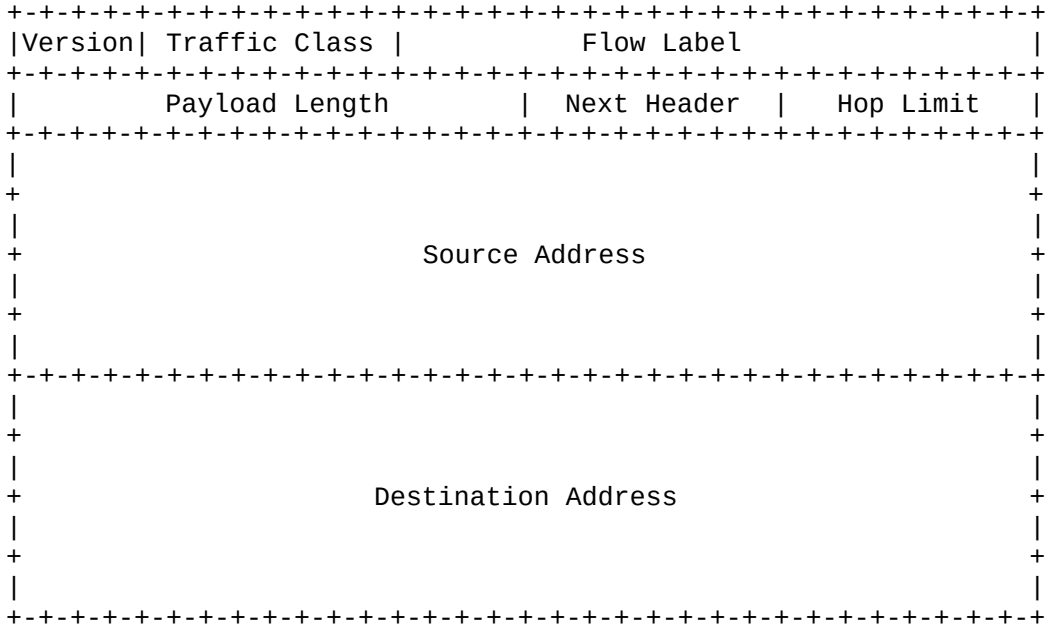

Figura 7.1.2. Cabecera IPv6
Extraído de RFC 2460 791 [https://www.ietf.org]

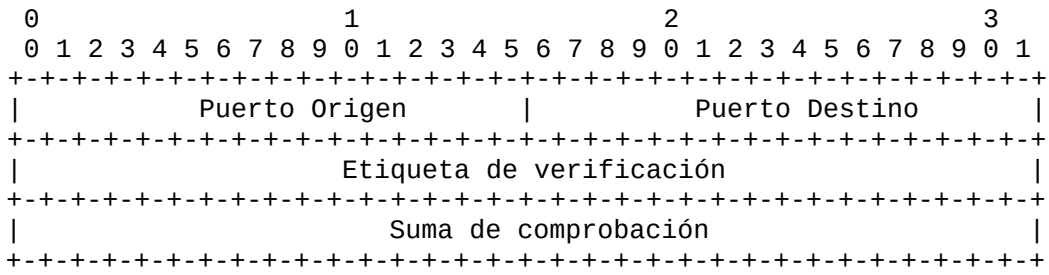

Figura 7.1.3. Cabecera Común de SCTP
Extraído de RFC 4960 [https://www.ietf.org]

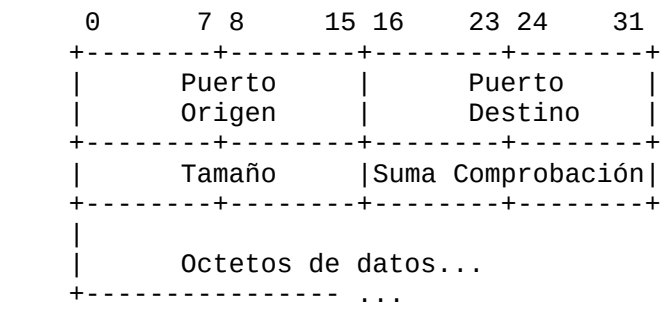

Figura 7.1.4. Cabecera UDP
Extraído de RFC 768 [https://www.ietf.org]

Bits

Octetos	8	7	6	5	4	3	2	1
1	Versión			P	T	Spare	Spare	Spare
2	Tipo de Mensaje							
3	Tamaño del Mensaje (1er Octeto)							
4	Tamaño del Mensaje (2do Octeto)							
m to k(m+3)	Si el parámetro T flag es 1, entonces el parámetro TEID se colocara en los octetos 5-8. En caso contrario el parámetro TEID no estará presente.							
n to (n+2)	Número de secuencia							
(n+3)	Spare							

Figura 7.1.5: Cabecera GTpv2 para el plano de control
Extraído de 3GPP TS 29.274 V8.11.0 (2011-12)

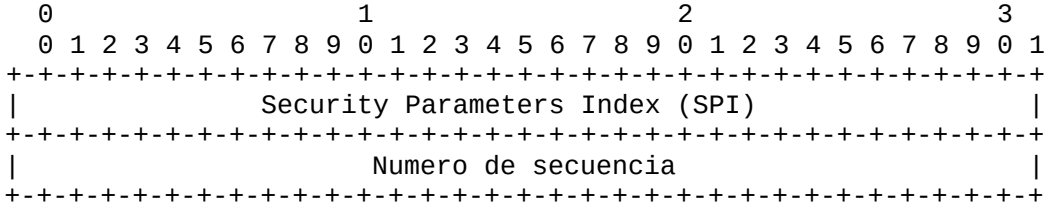

Figura 7.1.6. Cabecera ESP (IPsec)
Extraído de RFC 4303 [https://www.ietf.org]

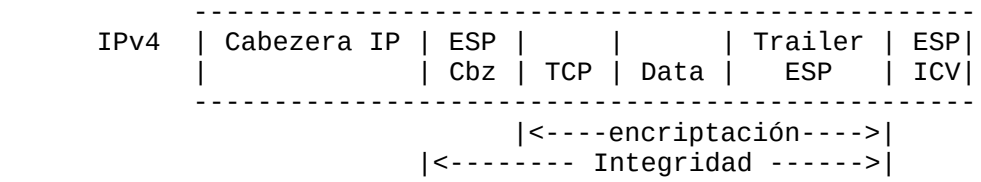

Figura 7.1.7. Paquete IPv4 después de agregar ESP
Extraído de RFC 4303 [https://www.ietf.org]

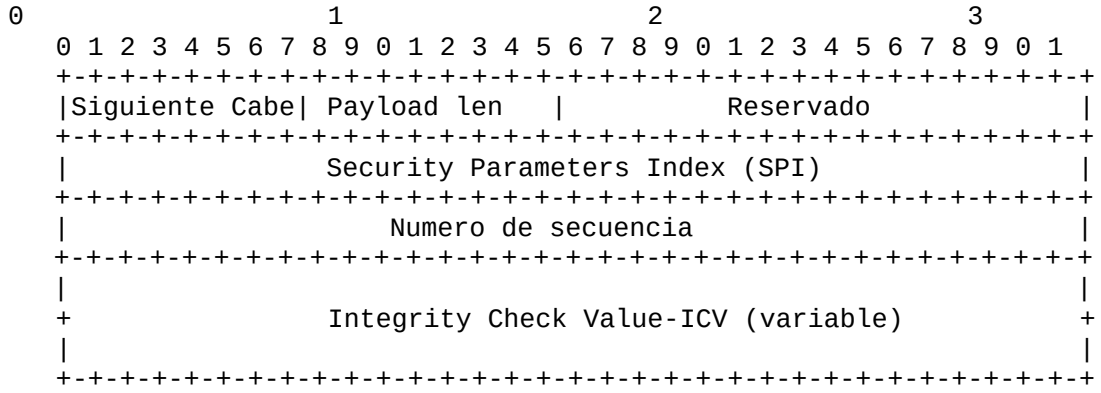

Figura 7.1.8 Cabecera AH (IPsec)
Extraído de RFC 4303 [https://www.ietf.org]

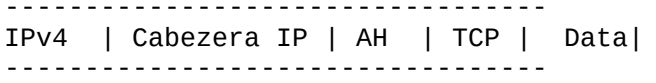

Figura 7.1.9. Paquete IPv4 después de agregar AH
Extraído de RFC 4303 [https://www.ietf.org]

	Bits							
Octetos	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Versión			PT	(*)	E	S	PN
2	Tipo de Mensaje							
3	Tamaño del Mensaje (1er Octeto)							
4	Tamaño del Mensaje (2do Octeto)							
5	Identificador del Extremo del tunel (1er Octeto)							
6	Tunnel Endpoint Identifier (2do Octeto)							
7	Tunnel Endpoint Identifier (3cer Octeto)							
8	Tunnel Endpoint Identifier (4to Octeto)							
9	Sequence Number (1er Octeto)[1) 4)]							
10	Sequence Number (2do Octeto)[1) 4)]							
11	Número N-PDU [2) 4)]							
12	Tipo de la Siguiente Extensión de Cabecera[3) 4)]							

Figura 7.1.10: Cabecera GTP-U
Extraído de 3GPP TS 29.281 V8.5.0 (2010-03)

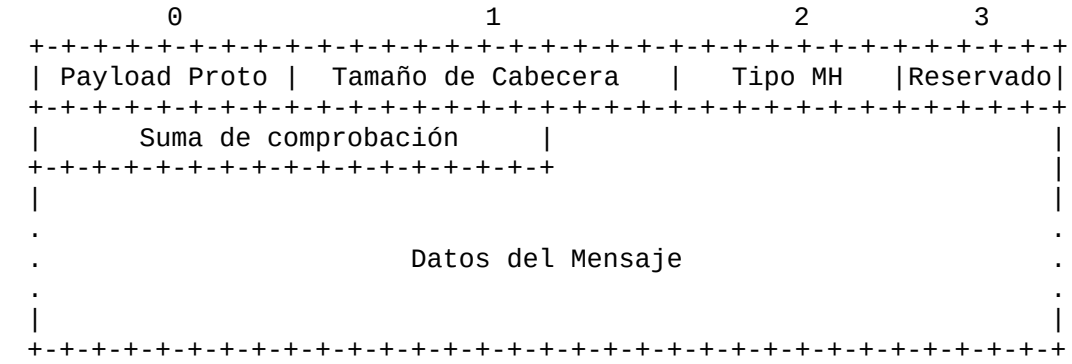

Figura 7.1.11. Cabecera MIPv6
Extraído de RFC 3775 [https://www.ietf.org]

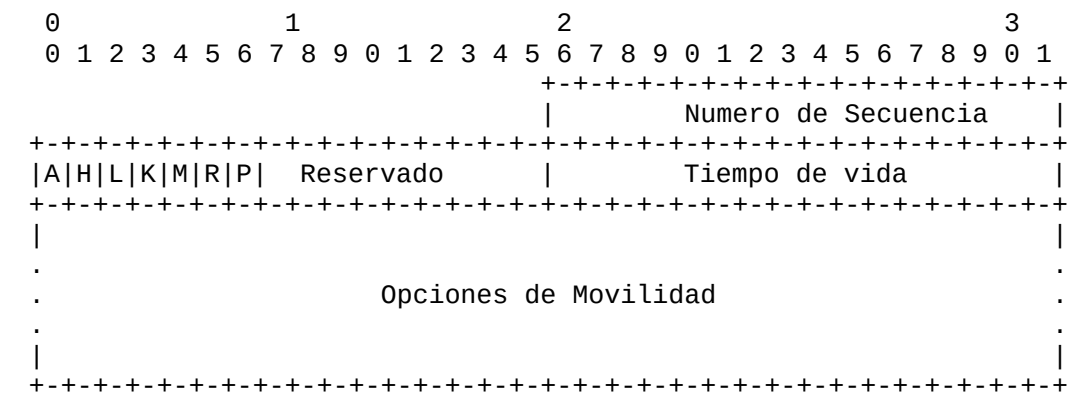

Figura 7.1.12 Mensaje Proxy Binding Update PMIPV6
Extraído de RFC 5213 [https://www.ietf.org]

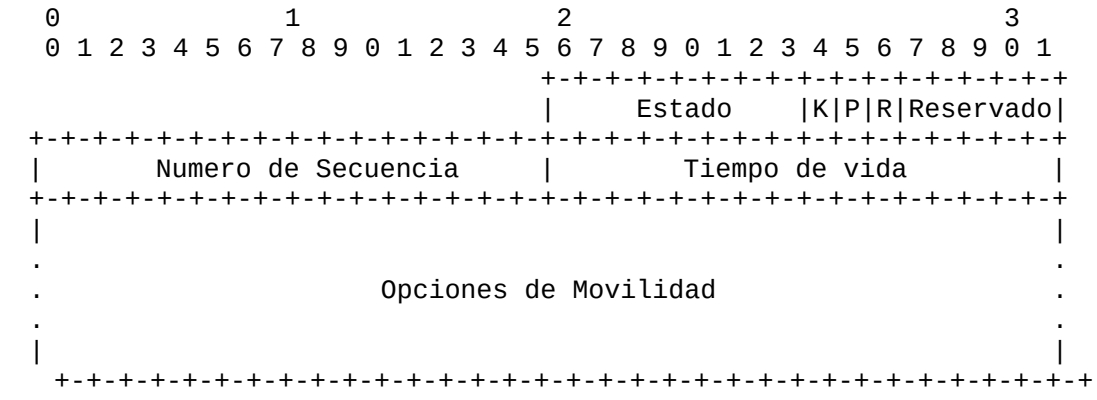

Figura 7.1.13. Mensaje Proxy Binding Acknowledgement
Extraído PMIPV6 de RFC 5213 [https://www.ietf.org]

E-UTRA Operating Band	Uplink (UL) operating band BS receive UE transmit	Downlink (DL) operating band BS transmit UE receive	Duplex Mode
	F_{UL_low} – F_{UL_high}	F_{DL_low} – F_{DL_high}	
1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
4	1710 MHz – 1755 MHz	2110 MHz – 2155 MHz	FDD
5	824 MHz – 849 MHz	869 MHz – 894MHz	FDD
6[1]	830 MHz – 840 MHz	875 MHz – 885 MHz	FDD
7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
9	1749.9 MHz – 1784.9 MHz	1844.9 MHz – 1879.9 MHz	FDD
10	1710 MHz – 1770 MHz	2110 MHz – 2170 MHz	FDD
11	1427.9 MHz – 1447.9 MHz	1475.9 MHz – 1495.9 MHz	FDD
12	699 MHz – 716 MHz	729 MHz – 746 MHz	FDD
13	777 MHz – 787 MHz	746 MHz – 756 MHz	FDD
14	788 MHz – 798 MHz	758 MHz – 768 MHz	FDD
15	Reserved	Reserved	FDD
16	Reserved	Reserved	FDD
17	704 MHz – 716 MHz	734 MHz – 746 MHz	FDD
18	815 MHz – 830 MHz	860 MHz – 875 MHz	FDD
19	830 MHz – 845 MHz	875 MHz – 890 MHz	FDD
20	832 MHz – 862 MHz	791 MHz – 821 MHz	FDD
21	1447.9 MHz – 1462.9 MHz	1495.9 MHz – 1510.9 MHz	FDD
22	3410 MHz – 3490 MHz	3510 MHz – 3590 MHz	FDD
23	2000 MHz – 2020 MHz	2180 MHz – 2200 MHz	FDD
24	1626.5 MHz – 1660.5 MHz	1525 MHz – 1559 MHz	FDD
25	1850 MHz – 1915 MHz	1930 MHz – 1995 MHz	FDD
26	814 MHz – 849 MHz	859 MHz – 894 MHz	FDD
27	807 MHz – 824 MHz	852 MHz – 869 MHz	FDD
28	703 MHz – 748 MHz	758 MHz – 803 MHz	FDD
29	N/A	717 MHz – 728 MHz	FDD[2]
30	2305 MHz – 2315 MHz	2350 MHz – 2360 MHz	FDD
31	452.5 MHz – 457.5 MHz	462.5 MHz – 467.5 MHz	FDD
32	N/A	1452 MHz – 1496 MHz	FDD[2]
33	1900 MHz – 1920 MHz	1900 MHz – 1920 MHz	TDD
34	2010 MHz – 2025 MHz	2010 MHz – 2025 MHz	TDD
35	1850 MHz – 1910 MHz	1850 MHz – 1910 MHz	TDD
36	1930 MHz – 1990 MHz	1930 MHz – 1990 MHz	TDD
37	1910 MHz – 1930 MHz	1910 MHz – 1930 MHz	TDD
38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
39	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz	TDD
40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz	TDD
41	2496 MHz 2690 MHz	2496 MHz 2690 MHz	TDD
42	3400 MHz – 3600 MHz	3400 MHz – 3600 MHz	TDD
43	3600 MHz – 3800 MHz	3600 MHz – 3800 MHz	TDD
44	703 MHz – 803 MHz	703 MHz – 803 MHz	TDD

NOTE 1: Band 6 is not applicable
NOTE 2: Restricted to E-UTRA operation when carrier aggregation is configured. The downlink operating band is paired with the uplink operating band (external) of the carrier aggregation configuration that is supporting the configured Pcell.

Tabla 7.1.1. Bandas de operación de LTE (Release 12)
Extraído de: 3GPP TS 36.101 V12.6.0 (2014-12)

UE Category	Maximum number of DL-SCH transport block bits received within a TTI (Note 1)	Maximum number of bits of a DL-SCH transport block received within a TTI	Total number of soft channel bits	Maximum number of supported layers for spatial multiplexing in DL
Category 0 (Note 2)	1000	1000	25344	1
Category 1	10296	10296	250368	1
Category 2	51024	51024	1237248	2
Category 3	102048	75376	1237248	2
Category 4	150752	75376	1827072	2
Category 5	299552	149776	3667200	4
Category 6	301504	149776 (4 layers) 75376 (2 layers)	3654144	2 or 4
Category 7	301504	149776 (4 layers) 75376 (2 layers)	3654144	2 or 4
Category 8	2998560	299856	35982720	8
Category 9	452256	149776 (4 layers) 75376 (2 layers)	5481216	2 or 4
Category 10	452256	149776 (4 layers) 75376 (2 layers)	5481216	2 or 4
Category 11	603008	149776 (4 layers, 64QAM) 195816 (4 layers, 256QAM) 75376 (2 layers, 64QAM) 97896 (2 layers, 256QAM)	7308288	2 or 4
Category 12	603008	149776 (4 layers, 64QAM) 195816 (4 layers, 256QAM) 75376 (2 layers, 64QAM) 97896 (2 layers, 256QAM)	7308288	2 or 4
Category 13	391632	195816 (4 layers) 97896 (2 layers)	3654144	2 or 4
Category 14	391632	195816 (4 layers) 97896 (2 layers)	3654144	2 or 4
Category 15	3916560	391656	47431680	8

NOTE 1: In carrier aggregation operation, the DL-SCH processing capability can be shared by the UE with that of MCH received from a serving cell. If the total eNB scheduling for DL-SCH and an MCH in one serving cell at a given TTI is larger than the defined processing capability, the prioritization between DL-SCH and MCH is left up to UE implementation.

NOTE 2: Within one TTI, a UE indicating category 0 shall be able to receive up to 1000 bits for a transport block associated with C-RNTI/Semi-Persistent Scheduling C-RNTI/P-RNTI/SI-RNTI/RA-RNTI and up to 2216 bits for another transport block associated with P-RNTI/SI-RNTI/RA-RNTI

Tabla 7.1.2. Categorías del UE LTE (Release 12)
Extraído de: 3GPP 3GPP TS 36.306 V12.3.0 (2014-12)

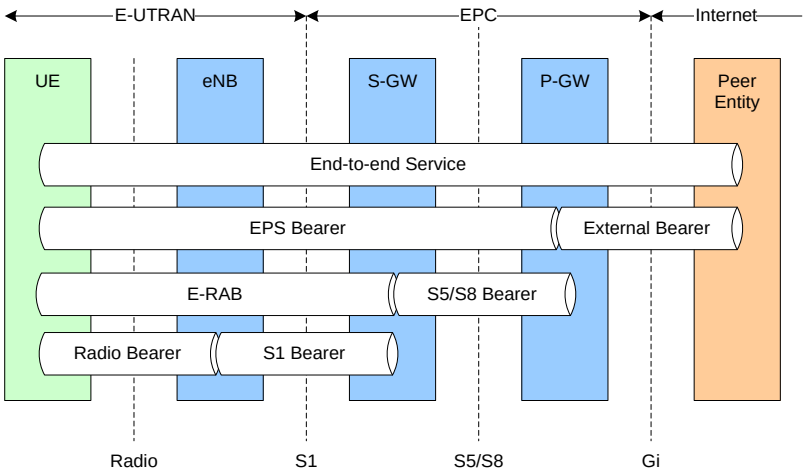

Figura 7.1.14. Arquitectura de los servicios portadores utilizados en LTE
Extraído de [3GPP TS 36.300 V8.12.0 (2010-03)]

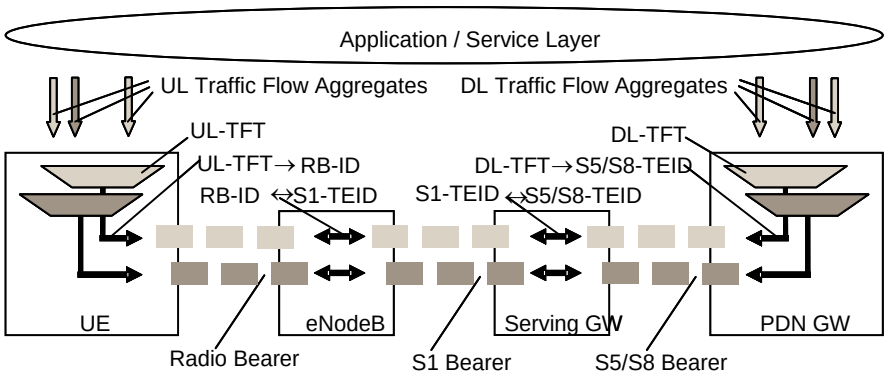

Figura 7.1.15. Implementación de túnel cuando se usa S5/S8 basados en GTP en dirección de bajada.
Extraído de [3GPP TS 23.401 V8.18.0 (2013-03)]

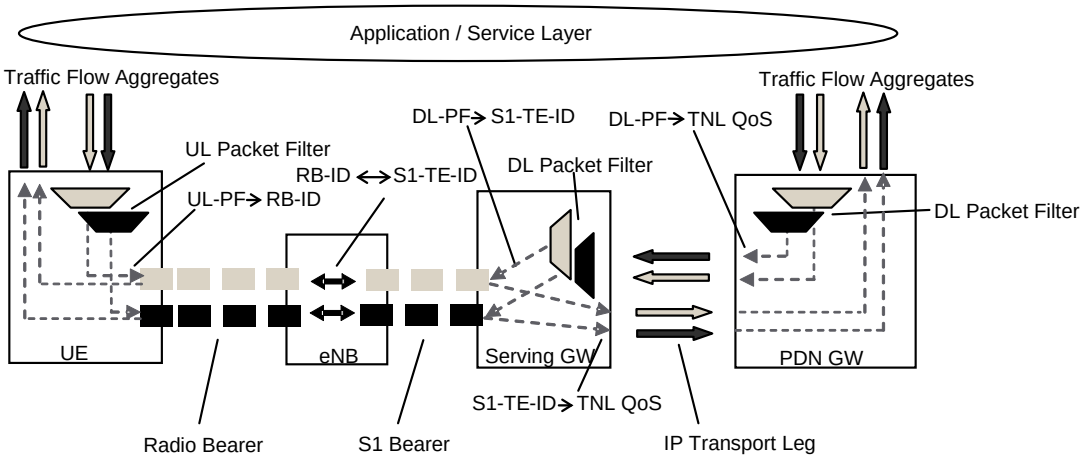

Figura 7.1.15. Implementación de túnel cuando se usa S5/S8 basados en PMIP en dirección de bajada.

Extraído de [3GPP TS 23.402 V8.18.0 (2013-03)]

Ubicación del UE	Hora del Día	Flujo de Datos por Aplicación	Regla para la Selección de la Red de Acceso	
			Prioridad	Tipo de Red de Acceso
Celda 1	N/D	YouTube, Tráfico HTTP Todo el tráfico enviado al servidor con la dirección IP X	1	WLAN (SSID=wlan1)
			2	WLAN (SSID=wlan2)
			3	3GPP
		Resto del Tráfico	1	3GPP
Celda 2	10: AM a 3:00 PM	Facebook	1	WLAN (SSID=wlan1)
			2	3GPP
	Cualquier otra hora	Facebook	1	3GPP
			2	WLAN (SSID=wlan1)
	N/D	Resto del Tráfico	1	WLAN (SSID=wlan2)
			2	3GPP

Tabla 7.1.3.Ejemplo de las políticas del nodo ANDSF
Extraído de [WLAN Traffic Offload in LTE, Rhode&Schwarz]

```
Scenario 2:
./ANDSF/Name = TeliaSonera
./ANDSF/Policy/Set_1/RulePriority = 1
./ANDSF/Policy/Set_1/PrioritizedAccess/1/AccessTechnology = WLAN
./ANDSF/Policy/Set_1/PrioritizedAccess/1/AccessID = HomeRun
./ANDSF/Policy/Set_1/PrioritizedAccess/1/AccessNetworkPriority=10
./ANDSF/Policy/Set_1/PrioritizedAccess/2/AccessTechnology = WLAN
./ANDSF/Policy/Set_1/PrioritizedAccess/2/AccessID = Other_SSID
./ANDSF/Policy/Set_1/PrioritizedAccess/2/AccessNetworkPriority=20
./ANDSF/Policy/Set_1/PrioritizedAccess/3/AccessTechnology = 3GPP
./ANDSF/Policy/Set_1/PrioritizedAccess/3/AccessNetworkPriority = 30
./ANDSF/Policy/Set_1/ValidityArea/3GPP_Location/1/LAC = 15
./ANDSF/Policy/Set_1/ValidityArea/3GPP_Location/2/LAC = 30
./ANDSF/Policy/Set_1/TimeOfDay/1/TimeStart = 0800
./ANDSF/Policy/Set_1/TimeOfDay/1/TimeStop = 1000
./ANDSF/Policy/Set_1/TimeOfDay/2/TimeStart = 1600
./ANDSF/Policy/Set_1/TimeOfDay/2/TimeStop = 1900
./ANDSF/Policy/Set_2/RulePriority = 2
./ANDSF/Policy/Set_2/PrioritizedAccess/1/AccessTechnology = WLAN
./ANDSF/Policy/Set_2/PrioritizedAccess/1/AccessID = HomeRun
./ANDSF/Policy/Set_2/PrioritizedAccess/1/AccessNetworkPriority=10
./ANDSF/Policy/Set_2/PrioritizedAccess/2/AccessTechnology = 3GPP
./ANDSF/Policy/Set_2/PrioritizedAccess/2/AccessNetworkPriority = 30
./ANDSF/Policy/Set_2/ValidityArea/3GPP_Location/1/PLMN = 24433
```

Figura 7.1.16. Ejemplo de una plantilla XML que contiene las políticas y preferencias de búsqueda y selección enviadas por el nodo ANDSF WLAN
Extraído de [WLAN Traffic Offload in LTE, Rhode&Schwarz]

```
<UE>
 <capabilities>
   <technologies>
    <supportedTechnology>
     <technology>LTE</technology>
     <bands>
      <band>
       <bandID>21</bandID>
<uplink><low>1447.9</low><high>1462.9</high></uplink>
<downlink><low>1495.9</low><high>1510.9</high></downlink>
       <duplex>FDD</duplex>
      </band>
     </bands>
     <category>5</category>
    </supportedTechnology>
    <supportedTechnology>
     <technology>WiMAX</technology>
     <bands>
      <band>
       <bandID>2</bandID>
<uplink><low>3527.5</low><high>3562.5</high></uplink>
<downlink><low>3527.5</low><high>3562.5</high></downlink>
       <duplex>TDD</duplex>
      </band>
     </bands>
     <category>1</category>
    </supportedTechnology>
   </technologies>
   <routingCapabilities>IFOM</routingCapabilities>
 </capabilities>
 <UELocation>
  <3GPPLocation>
   <location>
    <PLMN>28402</PLMN>
    <TAC>0xD34F</TAC>
    <EUTRA_CI>0xAF52D10<EUTRA_CI>
   </location>
  </3GPPLocation>
  <WiMAXLocation>
   <location>
    <NAP-ID>0xF4700A</NAP-ID>
    <BS-ID>0xCA9912</BS-ID>
   </location>
  </WiMAXLocation>
 </UELocation>
</UE>
```

Figura 7.1.17 Información que el UE envía al nodo ANDSF
Extraído de [WLAN Traffic Offload in LTE, Rhode&Schwarz]

Figura 7.1.18. Captura deSoftware WiROI para la creación del plan financiero
Extraído de [LTE, WiMAX and WLAN Network Design].

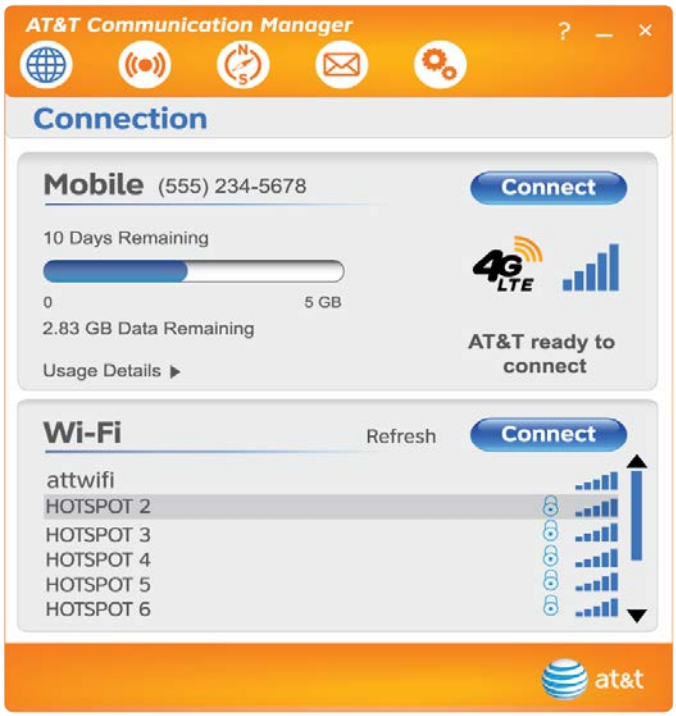

Figura 7.1.19. Captura de administrador de conexiones desarrollado por operador de telecomunicaciones AT&T de EE.U
Extraído de [https://wireless.att.com/businesscenter/solutions/wireless-laptop/communication-manager/index.jsp].

Figura 7.1.20 Foto de un teléfono con un administrador de Conexiones SAM (Smart Access Manager) desarrollado por InterDigital para dispositivos iOS y Android
Extraído de [InterDigital SAM Data Sheet]

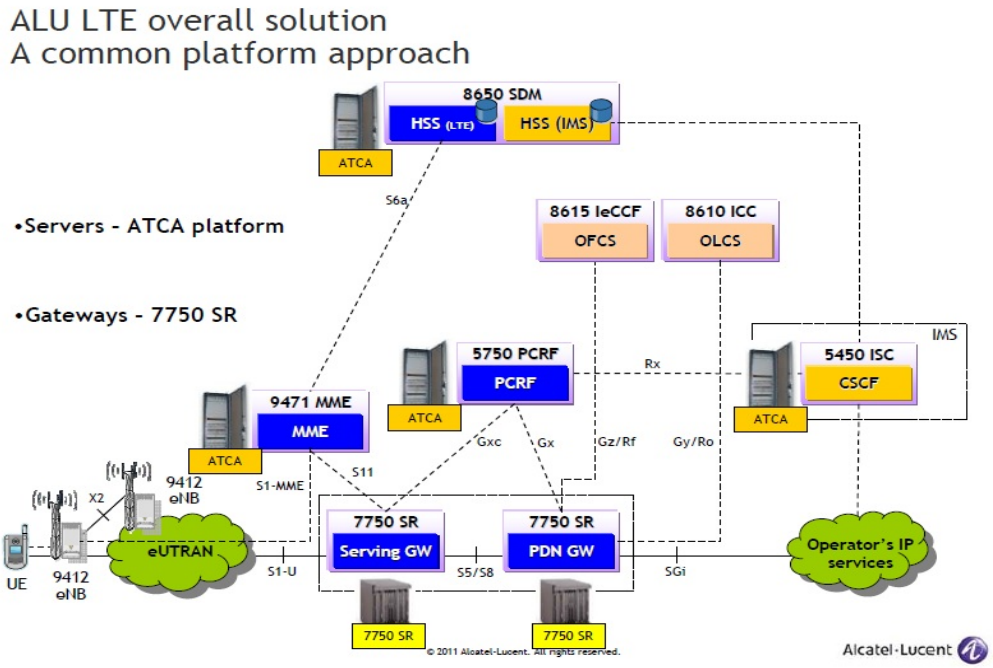

Figura 7.1.21. Propuesta de Alcatel-Lucent que muestra los diferentes nodos que conforman el núcleo EPC de una red LTE
Extraída de [Alcatel-Lucent Solution]

7.2 Especificaciones técnicas de equipos

Datos técnicos de dispositivos LTE.

Technical specifications

Dimensions and weight
- Length: 43.2 cm (17 in.)
- Depth: 42.5 cm (16.75 in.)
- Width: 3.6 cm (1.4 in.)
- Weight: 6.8 kg (15 lb)

Environmental specifications
- Operating temperature: 0°C to 40°C (32°F to 104°F)
- Relative humidity: 15% to 85% (operating), 5% to 90% (non-condensing)
- Altitude: 3048 m (10,000 ft)
- Power: 390 W

Regulatory specifications

Safety
- EN 60950-1
- IEC 60950-1 CB Scheme
- CSA/UL 60950-1 NRTL
- FDA CDRH 21-CFR 1040
- EN 60825-1
- EN 60825-2
- IEC 60825-1
- IEC 60825-2

EMC
- ICES-003 Class A
- FCC Part 15 Class A
- EN 300 386
- EN 1000-4-11
- EN 55022
- EN 55024
- EN 61000-4-2
- EN 61000-4-3
- EN 61000-4-4
- EN 61000-4-5
- EN 61000-4-6
- IEC CISPR22
- AS/NZS CISPR 22

Immunity
- EN 61000-3-2 Power Line

Harmonics
- EN 61000-3-3 Voltage Fluctuations and Flicker

- EN 61000-4-2 ESD
- EN 61000-4-3 Radiated Immunity
- EN 61000-4-4 EFT
- EN 61000-4-5 Surge
- EN 61000-4-6 Low Frequency

Common immunity
- EN 1000-4-11 Voltage Dips and Sags

Telecom
- Telcordia GR-253-CORE, Issue 3
- IEEE 802.3 (GE, Ethernet)
- ANSI T1.105
- ANSI T1.105.03
- ANSI T1.105.06
- ANSI T1.105.09
- ANSI T1.403 (DS1)
- ANSI T1.404 (DS3)
- ITU-T G.703
- ITU-T G.707
- ITU-T G.813
- ITU-T G.823
- ITU-T G.824
- ITU-T G.825
- ITU-T G.957

Environmental
- ETS 300 019-1-1, Storage Tests, Class 1.2
- ETS 300 019-1-2, Transportation Tests, Class 2.3
- ETS 300 019-1-3, Operational Tests, Class 3.2
- ETS 300 019-2-4, pr A 1 Seismic

Electronic equipment directives
- WEEE
- RoHS
- R&TTE
- China-CRoHS

Certifications
- NEBS level 3
- NE BS/Telcordia GR-1089-CORE, Issue 4, June 2006
- NE BS/Telcordia GR-63-CORE, Issue 3, March 2006
- ATT-TP-76200
- CE

Standards compliance
- 3GPP R8: TS 23.401, TS 23.402, TS 23.203, TS 23.060, TS 29.060, TS 29.061, TS 29.212, TS 29.213, TS 29.274, TS-29.275, TS 32.251, TS 29.281, TS 32.295, TS 32.297, TS 32.298, TS 32.299
- IETF: RFC 2131, RFC 3736, RFC 4862, RFC 3633, RFC 2865, RFC 2866, RFC 2868, RFC 2869, RFC 5176

Minimum platform requirements
- Alcatel-Lucent 7750 SR-7 or 7750 SR-12
- Alcatel-Lucent SR-OS-MG. EPC Gateway functions are release dependent

Ordering information
- 3HE04790AA Mobile Gateway Integrated Services Module

For detailed system specifications and IP capabilities, please check the Alcatel-Lucent 7750 Service Router Data Sheet.

Figura 7.2.1: Especificaciones técnicas de Alcatel-Lucent Mobile Gateway 7750
Extraido de *http://www.alcatel-lucent.com/products/7750-service-router-mobile-gateway*

Samsung GALAXY Note 4

Dimension
- 153.5 X 78.6 X 8.5 mm / 176g

Display
- 5.7" Quad HD Super AMOLED (2560 x1440)

AP
- 2.7GHz Quad Core Process
- 1.9GHz Octa Core (1.9GHz Quad + 1.3GHz Quad Core) Process

* May differ by country and carrier

Memory
- 3GB RAM + 32GB Internal memory
- Supports microSD up to 128GB

Network
- 2.5G (GSM/GPRS/EDGE) : 850/900/1800/1900 MHz
- 3G (HSPA+ 42Mbps): 850/900/1900/2100 MHz
- 4G (LTE Cat.4 150/50Mbps) or 4G (LTE Cat.6 300/50Mbps)

* May differ by country and carrier

Camera
- Front Camera 3.7MP + F1.9/ Selfie (90°), Wide selfie mode (120°)
- Rear Camera 16M+ Smart OIS/ Fast AF, Live HDR(Rich Tone)

OS
- Android 4.4 (Kitkat)

Connectivity
- Wi-Fi 802.11 a/b/g/n/ac (2X2 MIMO)
- Download Booster, NFC, Bluetooth® v 4.1 (BLE),ANT+, USB2.0, MHL 3.0
- IR LED (Remote Control)

Battery
- 3220mAh Fast Charging

Audio
- Codec: MP3, AAC/AAC+/eAAC+, WMA, AMR-NB/WB, Vorbis, FLAC
- Adapt Sound, Sound Alive, Wise Voice 2.0, Extra Volume 2.0
- 3 Mics (Directional Voice Recording)

S Pen
- 15g, Hovering 15mm, Pressure level 2,048

Sensor
- Gesture, Accelerometer, Geo-magnetic, Gyroscope, RGB ambient light, Proximity, Barometer, Hall Sensor, Finger Scanner, UV, HRM

Figura 7.2.2 Especificaciones técnicas de un teléfono celular Samsun Galaxy Note 4
Extraida de [www.samsung.com]

Figura 7.2.3. Imagen de dispositivo Cisco ASR 5500.
Extraído de [http://www.cisco.com]

Cisco ASR 5500 tiene la flexibilidad de cumplir la necesidad de los operadores, y permitir funciones para cambiar y mantener el balance correcto según los cambios de la red, a continuación hay algunas posibles funciones de Cisco ASR 550:

- LTE/EPC - Serving Gateway
- LTE/EPC - PDN Gateway
- UMTS/HSPA - Gateway GPRS Support Node
- CDMA/HRPD/eHRPD - Home Agent

Description	Specification
Logical Interfaces	• GSMA • GSM UMTS • SIGTRAN • IMS Ma, Mw, Mg, Mj, Mr, ISC, Cx, Sh • IETF SIP • H.248 • ECMP, IEEE 802.1q VLANs, IEEE 802.3ad link aggregation • MPLS LSPs, GRE interface tunnels • L2TP, IPSEC
Physical Dimensions	• Height: 93.3 cm (36.75 in,) • Width: 43.8 cm (17.25 in.) • Depth: 69.9 cm (27.5 in.) • Mounting weight (chassis): 51.25 kg (113 lb) • Total weight (fully loaded): 204.1 kg (450 lb)
Power	• Base 20-slot chassis: 256W • Fabric and storage card (up to 6 per chassis): 100W • System status card (up to 2 per chassis): 10W • Management I/O card (up to 6 per chassis): 900W • Data processing card (up to 8 per chassis): 1000W • Front fan tray (2 per chassis): 60W • Back fan tray (2 per chassis): 840W • Total power (fully loaded): 12,800W • 8 power feeds, capable of carrying 80A each • Operating voltage: -40.5 to -72V

Environmental	• Normal operating temperature: 0°C to 40°C (32°F to 104°F) • Storage temperature: -40°C to +70°C (-40°F to 158°F) • Normal operating humidity: 20% to 80% noncondensing • Storage humidity: 10% to 95% noncondensing • Normal operating altitude: 60m (197 ft) below to 4,000m (13,123 ft) above sea level (at 30°C) • Non-operating altitude: 60m (197 ft) below to 15,000m (49,212 ft) above sea level
GSM/UMTS (CS Domain)	• 3GPP TS 24.008, 48.006, 48.008, 25.413, 29.232, Q.1950, 23.003, 29.002, 23.039, 23.040, 23.401, 23.402, 24.011, 24.080, 24.081, 24.083, 24.084, 24.091, 24.173, 23.009, 49.008
IETF	• RFC 1035, 2046, 2387, 2617, 2782, 2915,2976, 2833, 3261(SIP), 3263(SIP), 3262, 3264, 3265(SIP), 3310, 3311, 3323, 3325, 3327(SIP), 3428, 3455, 3551, 3588, 3608(SIP), 3680, 3761, 3842, 3966, 4483, 4566
CDMA	• CDMA A.S0013-C v2.0, A.S0014-C v2.0, C.S0005-D v2.0

Tabla 7.2.1. Especificaciones de Cisco ASR 5500
Extraído de [http://www.cisco.com]

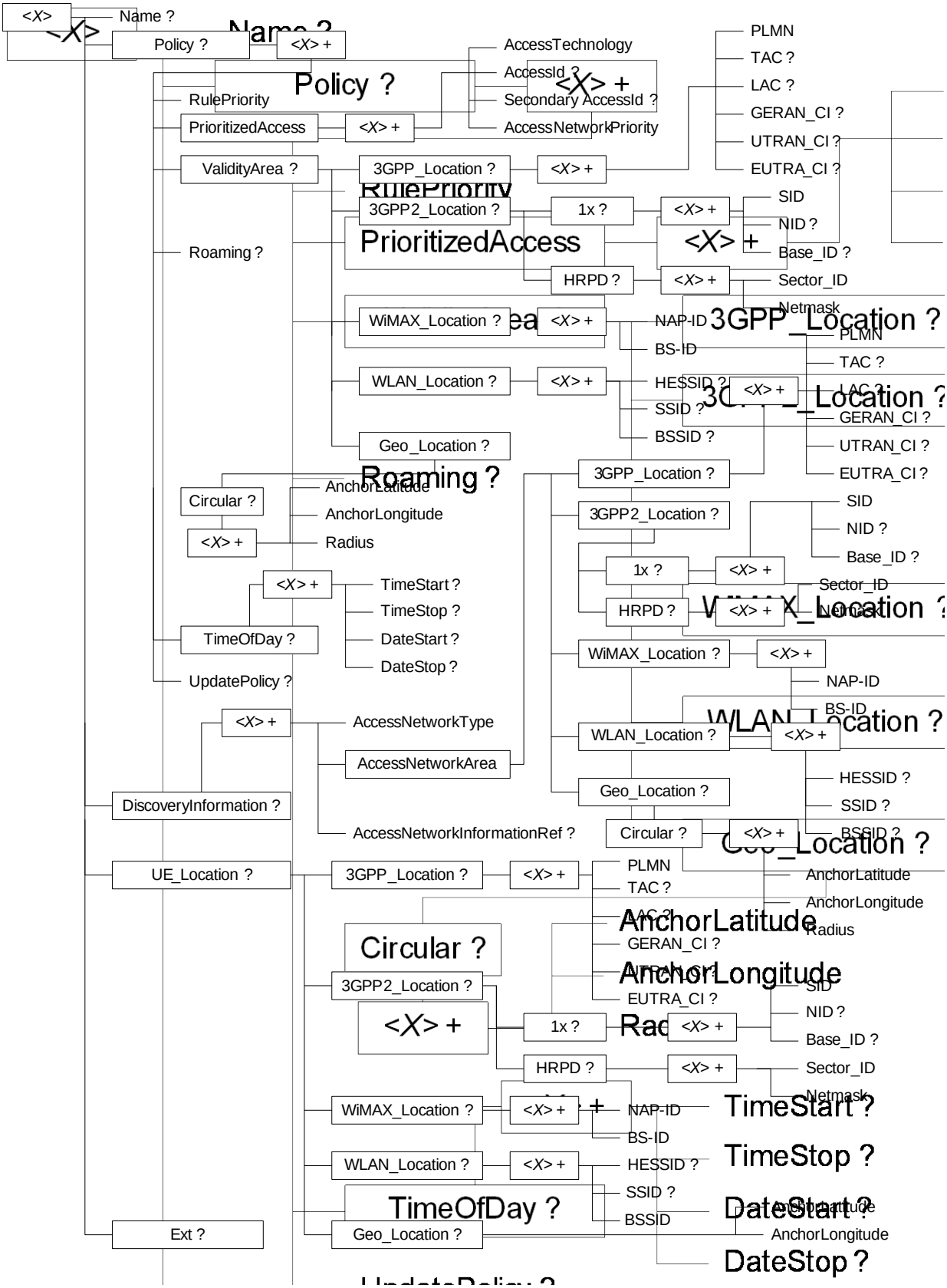

Figura 7.2.4: Representación del formato MO.

7.3 Otros

Telcor
ENTE REGULADOR

ACUERDO ADMINISTRATIVO

No. 001 - 2006

La Directora General del Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR), en uso de sus facultades que le confiere el Decreto No. 1053, Ley Orgánica de TELCOR y sus reformas; el Decreto No. 128-2004, Reglamento General de la Ley Orgánica de TELCOR, publicado en la Gaceta No. 238 del 7 de Diciembre de 2004, la Ley No. 200, Ley General de Telecomunicaciones y Servicios Postales, publicada en la Gaceta No. 154, del 18 de Agosto de 1995 y el Decreto No. 19-96 y sus reformas en el decreto 131-2004 "Reforma al Decreto 19-96 Reglamento de la Ley General de Telecomunicaciones y Servicios Postales", publicado en la Gaceta No. 2 del 4 de enero del 2005.

CONSIDERANDO

I

Que la representación, dirección y administración de TELCOR está a cargo del Director General, quien es el Funcionario Ejecutivo Superior de la Institución, ostentando la representación legal y la responsabilidad de dirigir, coordinar, controlar y vigilar la actividad del Instituto Nicaragüense de Telecomunicaciones y Correos, de conformidad con la Ley y sus Reglamentos. (Art. 5 de la Ley Orgánica de TELCOR y sus reformas).

II

Que la Ley General de Telecomunicaciones y Servicios Postales se encuentra orientada dentro de sus tareas principales a garantizar un desarrollo planificado, sostenido, ordenado y eficiente de las telecomunicaciones y servicios postales (Art. 2 inciso 1 de la Ley General de Telecomunicaciones y Servicios Postales, Ley 200).

III

Que el Director General de TELCOR dentro de sus facultades tiene la de formular y aprobar los Reglamentos y Normas que sean necesarias para el cumplimiento de los objetivos y fines institucionales de TELCOR. (Art.12 numeral 3.1 del Reglamento General de la Ley Orgánica de TELCOR, Decreto 128-2004).

IV

Que es obligación de TELCOR garantizar el uso eficiente del Espectro Radioeléctrico mediante la emisión de Reglamentos y Normativas técnicas, para la prestación de Servicios de Telecomunicaciones que hacen uso de este recurso.

V

Que el Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR), tiene facultades para cancelar o cambiar una frecuencia autorizada siempre que sea factible para solucionar problemas de interferencias perjudiciales, para la aplicación de nuevas tecnologías o bien en cumplimiento a los acuerdos internacionales, suscrito y ratificados por el Gobierno de Nicaragua. (Art. 64, del Reglamento de la Ley No. 200 y sus reformas, decreto 131-2004).

25 ENE. 2006

Presidencia de la República

Director General

Páguese por 1 publicación(es) en el Diario Oficial la Gaceta la suma de C$ 2,220.00
Fecha: 19/1/06 Firma:

VI

Que la Unión Internacional de Telecomunicaciones UIT tiene atribuido a las aplicaciones Industriales Científicas y Médicas (ICM), para la Región 2 Américas, las bandas 902 a 928 MHz; 2 400 a 2 483.5 MHZ y de 5 725 a 5 825 MHz.

VII

Que a través del Acuerdo Administrativo No. 22 – 2000, Normativa Técnica NON-EE-001-2000, se atribuyeron diferentes bandas de radiofrecuencia, incluyendo las bandas ICM, para ser utilizadas en la prestación de servicios de Radiocomunicación haciendo uso de técnicas de Espectro Ensanchado.

VIII

Que existe una creciente demanda para prestar servicios de telecomunicaciones en las bandas ICM, debido a que estas bandas permiten la utilización de tecnologías de escala. TELCOR prevé que esta creciente demanda, no podrá ser satisfecha únicamente con las bandas ICM actualmente atribuidas para estos sistemas.

IX

Que para facilitar la introducción de los Sistemas de Acceso Inalámbrico, incluidas las redes radioeléctricas de área local, utilizando tecnologías de escala, es necesaria una armonización de las bandas de frecuencias actualmente atribuidas en el Acuerdo Administrativo No. 22 – 2000, en correspondencia con las Recomendaciones Internacionales.

X

Que la Conferencia Mundial de Radio 2003 "CMR-03", mediante resolución COM 5/16-CMR-03, acordó la utilización de las bandas 5 150-5 350 MHz y 5 470-5 725 MHz, para la implementación de sistemas de Acceso Inalámbrico, incluidas las Redes Radioeléctricas de Área Local (RLAN).

XI

Que es necesario la protección de los Servicios atribuidos a Título Primario en las bandas 5 150-5 350 MHz y 5 470-5 725 MHz.

XII

Que la banda 5 150-5 250 MHz esta atribuida mundialmente a Titulo Primario al Servicio Fijo por Satélite (FSS) (tierra-espacio) para su utilización con los enlaces de conexión de los sistemas no geoestacionarios del Servicio Móvil por Satélite (MSS).

XIII

Que el uso compartido de la banda 5 150-5 250 MHz entre Sistemas de Acceso Inalámbrico, incluidas las Redes Radioeléctricas de Área Local, y los FSS y MSS, es posible solo bajo condiciones especificas.

XIV

Que las bandas de frecuencia 5 250-5 350 MHz y 5 470-5 725 MHz están atribuidas a Título Primario al servicio de Radiolocalización. El uso compartido de las bandas 5 250-5 350 y 5 470-5 725, por los servicios de Radiolocalización y

los servicios de Acceso Inalámbrico, es posible solamente con la aplicación de técnicas de mitigación de interferencias, tales como Selección Dinámica de Frecuencia (DFS).

XV

Que de acuerdo a lo establecido en las Recomendaciones UIT-R serie F: 636, 595, 637, 748, 746 y 749, las bandas de frecuencia 14.4-15.35 GHz, 17.7-19.7 GHz, 21.2-23.6 GHz, 24.25-26.50 GHz, 27.50-31.30 GHz, 37.00-40.00 GHz y 36.0-40.5 GHz (mencionadas en el numeral 3 "bandas de frecuencias" de la normativa Técnica NON-EE-001-2000), están atribuidas a Título Primario al Servicio Fijo y a otros servicios, tales como Sistemas Inalámbricos Fijos para Circuitos Internacionales.

XVI

Que los derechos adquiridos por los titulares de Concesiones, licencias, permisos, registros o autorizaciones vigentes, deben ser respetados (Art. 22 de la Ley No. 200)

XVII

Que las concesiones, licencias, constancias de registro pueden ser renovadas, siempre y cuando sus titulares hayan cumplido con las condiciones establecidas en los mismos, lo soliciten con la anticipación prevista en el título habilitante y acepten las nuevas condiciones que la legislación vigente y TELCOR en su caso determinen. (Art. 22, del Reglamento de la Ley General de Telecomunicaciones y Servicios Postales, Decreto no. 19-96 y sus Reformas, Decreto 131-2004,).

POR TANTO;

ESTA AUTORIDAD REGULADORA

ACUERDA:

Art. 1º Emitir la Normativa Técnica contenida en el ANEXO I, "Normativa Técnica No. 001-2006, SISTEMAS DE ACCESO INALAMBRICO EN LAS BANDAS: 900 MHZ, 2.4 GHZ, 5 GHZ", la cual forma parte integra del presente Acuerdo Administrativo.

Art. 2º Las siguientes bandas de frecuencias quedan atribuidas a Titulo Primario para el Servicio Fijo y otros Servicios conforme al Cuadro de Atribución Nacional de Frecuencias de Nicaragua:

14 400 MHz	a	15 350 MHz
17 700 MHz	a	19 700 MHz
21 200 MHz	a	23 600 MHz
24 250 MHz	a	26 500 MHz
27 500 MHz	a	31 300 MHz
37 000 Mhz	a	40 000 Mhz

Art. 3º Modificar el Cuadro de Atribución Nacional de Frecuencias de Nicaragua en lo que corresponda.

Art. 4º Los operadores autorizados por TELCOR que hacen uso de las bandas 900 MHz, 2.4 GHz y 5 GHz deben, al momento de solicitar la renovación de su título habilitante, sujetarse a las condiciones establecidas en la presente

normativa. (arto. 22 del Reglamento de la Ley General de Telecomunicaciones y Servicios Postales, Reformado por el Decreto 131-2004).

Art. 5º Los operadores autorizados por TELCOR antes de la entrada en vigencia de esta normativa y que hacen uso de la banda 5 150 – 5 250 MHz, tendrán derecho a solicitar, dentro de los primeros 30 días de entrada en vigencia de esta Normativa, una moratoria por un período máximo de 3 años, para adecuarse a lo establecido en el Arto 4.4. del ANEXO I "Normativa Técnica No. 001-2006, SISTEMAS DE ACCESO INALAMBRICO EN LAS BANDAS: 900 MHZ, 2.4 GHZ, 5 GHZ", sin perjuicio de cesar transmisiones en caso de ocasionar cualquier tipo de Interferencia en el lapso de la moratoria otorgada.

Art. 6º Derogar el Acuerdo Administrativo No. 22 – 2000, emitido por TELCOR el trece de junio del año dos mil.

Art. 7º El presente Acuerdo administrativo entrará en vigencia a partir de la fecha de su firma, sin perjuicio de su posterior publicación en La Gaceta, Diario Oficial.

Dado en la ciudad de Managua, a las diez de la mañana del día dieciséis de Enero del dos mil seis.

Lic. Julia Marta Lugo Balcáceres
Directora General
TELCOR

2.4. Canal de Operación.

Una vez que un sistema de acceso inalámbrico que opera en las bandas de 5 GHz, comienza a operar en un "Canal Disponible", entonces este canal se convierte en un "Canal de Operación".

2.5. Canal Disponible

Es un canal de radiofrecuencia en el cual una "Verificación de Disponibilidad de Canal" no ha identificado la presencia de una señal de radar.

2.6. Control de Potencia Transmitida (TPC)

Característica que permite a un sistema de acceso inalámbrico que opera en las bandas de 5 GHz, cambiar dinámicamente entre varios niveles de potencia de transmisión en el proceso de la transmisión de datos.

2.7. Comunicación Punto a Punto

Comunicación proporcionada por un enlace, por ejemplo por medio de un radioenlace, entre dos estaciones situadas en unos puntos fijos determinados.

2.8. Comunicación Punto a Multipunto

Comunicación proporcionada por enlaces, por ejemplo por medio de un radioenlace, entre una estación situada en un punto fijo determinado y un número de estaciones situadas en unos puntos fijos determinados.

2.9. Verificación de Disponibilidad de Canal.

Es una verificación durante la cual un sistemas de acceso inalámbrico que opera en las bandas de 5 GHz, escucha sobre un canal de radiofrecuencia determinado con el fin de identificar si hay presencia de un radar operando en ese canal de radiofrecuencia.

2.10. Densidad Espectral de Potencia

Es la energía de salida total de un pulso o secuencia de pulsos por unidad de ancho de banda dividido por la duración total de los pulsos.

2.11. Densidad Espectral de Potencia Transmitida

Es la densidad espectral de potencia máxima, dentro del ancho de banda de medición especificado, en la banda de operación de un sistema de acceso inalámbrico que opera en las bandas de 5 GHz.

2.12. Emisión Fuera de Banda

Emisión en una o varias frecuencias situadas inmediatamente fuera de la anchura de banda necesaria, resultante del proceso de modulación, excluyendo las emisiones no esenciales.

2.13. Emisión no Esencial

Emisión en una o varias frecuencias situadas fuera de la anchura de banda necesaria, cuyo nivel puede reducirse sin influir en la transmisión de la información correspondiente. Las emisiones armónicas, las emisiones parásitas, los productos de intermodulación y los productos de la conversión de frecuencia están comprendidos en las emisiones no esenciales, pero están excluidas las emisiones fuera de banda.

2.14. Emisiones no Deseadas

Conjunto de las emisiones no esenciales y de las emisiones fuera de banda.

2.15. Máxima Potencia de Cresta de Salida Conducida

La potencia transmitida total entregada a todas las antenas y los elementos de antena promediados a través de todos los símbolos en el alfabeto de señal cuando el transmisor esta operando a su máximo nivel de control de potencia. El promedio no debe incluir ninguno de los intervalos de tiempo durante los cuales el transmisor esta apagado o esta transmitiendo a un nivel de potencia reducido. Si son posibles múltiples modos de operación (ej. Métodos de modulación alternativos), la "máxima Potencia de salida conducida" es la potencia de transmisión total mas alta que ocurre en cualquiera de los modos.

2.16. Modulación Digital

Proceso por el cual las características de una onda portadora son variadas entre un conjunto de valores discretos predeterminados de acuerdo con una función de modulación digital.

2.17. Periodo de No-ocupación.

Es el periodo requerido en el cual, una vez que se identifica que un canal contiene una señal de radar, este no será seleccionado como un "canal disponible".

2.18. Potencia Isotrópica Radiada Equivalente (EIRP).

Producto de la potencia suministrada a la antena por su ganancia con relación a una antena isótropa en una dirección dada (ganancia isótropa o absoluta).
Nota – La antena isótropa, cuando se alimenta con una potencia de 1 kW, se considera que proporciona una EIRP de 1 kW en todas las direcciones y produce una intensidad de campo de 173 mV/m a 1 km de distancia.

2.19. Potencia Promedio de la Envolvente de Símbolo

Es el promedio, tomado sobre todos los símbolos en el alfabeto de señal, de la potencia envolvente para cada símbolo

2.20. Selección Dinámica de Frecuencia (DFS)

Mecanismo que detecta dinámicamente señales de otros sistemas de radiocomunicación y evita la operación cocanal con estos sistemas, especialmente con sistemas de radar.

2.21. Sistema Híbrido

Combinación de las técnicas de Espectro Ensanchado por Salto De Frecuencia (FH) y Secuencia Directa (DS) o cualquier otro tipo de Modulación Digital.

2.22. Sistemas de Espectro Ensanchado (SS)

Es un sistema en el cual la energía media de la señal transmitida se dispersa sobre un ancho de banda mucho mayor que el de la información. En estos sistemas esencialmente se distribuye la potencia media de la información en un ancho de banda mayor que el mínimo requerido para su transmisión, resultando en una densidad espectral de potencia mas baja y un mayor rechazo a las señales interferentes. Los sistemas de Espectro Ensanchado emplean un código independiente al de los datos, ofreciendo

Director Ejecutivo

una capacidad de direccionamiento selectiva y la alternativa de compartir el espectro con otros sistemas de radiocomunicación. Las principales modalidades de funcionamiento de los sistemas de espectro ensanchado son: Secuencia Directa (Direct Sequence ,DS), Salto de Frecuencia (Frecuency Hopping, FH), e Híbridos (FH/DS).

2.23. Sistemas De Secuencia Directa (DS)

Técnica de transmisión en la cual, la potencia de la señal se expande sobre un ancho de banda de transmisión dado, lo cual se realiza multiplicando los datos binarios de información de banda base con un código de alta velocidad denominado Código de Pseudoruido o de dispersión; posteriormente, los datos compuestos se modulan para su transmisión. El receptor utiliza el mismo código utilizado en la transmisión para recuperar los datos binarios de información.

2.24. Sistemas Por Salto De Frecuencia (FH)

Técnica de transmisión en la cual se modulan los datos binarios de información empleando una portadora de banda estrecha, la cual "salta" de manera pseudoaleatoria de una frecuencia portadora a otra, en el tiempo, sobre determinada banda de transmisión. El receptor correspondiente realiza saltos de frecuencia en sincronismo con el código del transmisor para recuperar los datos binarios de información.

2.25. Tiempo de Desplazamiento de Canal.

Es el tiempo que necesita un sistema de acceso inalámbrico que opera en las bandas de 5 GHz para cesar todas las transmisiones en el canal en uso al detectar la presencia de una señal de radar a través del umbral de detección del DFS (TDFS)

2.26. Umbral De Detección De DFS (T_{DFS}).

Es el nivel de detección requerido, definido para detectar una Intensidad de Señal recibida (RSS) que es mayor que un umbral especificado, dentro del ancho de banda del canal utilizado por un sistema de acceso inalámbrico que opera en las bandas de 5 GHz. El umbral de detección se define en términos de dBm normalizado a la salida de una antena receptora a 0 dBi. Si el receptor utiliza ganancias de antena más elevadas, debe aumentarse el nivel T_{DFS} añadiendo la ganancia de antena.

3. BANDAS DE FRECUENCIAS

Se atribuyen en carácter Compartido y Secundario, para sistemas de acceso inalámbrico que utilizan tecnologías de Modulación Digital de banda ancha, incluyendo Espectro Ensanchado, las siguientes bandas de frecuencia:

902 MHz	a	928	MHz
2 400 MHz	a	2 498.5	MHz
5 150 MHz	a	5 250	MHz
5 250 MHz	a	5 350	MHz
5 470 MHz	a	5 725	MHz
5 725 MHz	a	5 850	MHz

4. CONDICIONES DE OPERACION

4.1 **Interferencias**: La operación del sistema está condicionada al cumplimiento de lo siguiente:

A. No deben causar interferencia perjudicial a las estaciones de Servicio Primario.

B. No pueden reclamar protección contra interferencias perjudiciales causadas por estaciones de un Servicio Primario.

C. Tienen derecho a la protección contra interferencias perjudiciales causadas por estaciones del mismo servicio que operen en las bandas de uso compartido establecido en esta normativa y otros servicios atribuidos a título Secundario en el Cuadro Nacional de Atribución de Frecuencias. Para estos casos se aplicará el derecho de precedencia una vez comprobado que el sistema afectado cumple con las normas de instalación así como las condiciones y parámetros de operación establecidos en la presente normativa.

D. El operador de radiadores incidentales que haya sido identificado como causante de una interferencia perjudicial debidamente comprobada, deberá suspender de inmediato su operación y no la reanudara hasta que no se hayan corregido las causas que originan o producen la interferencia perjudicial.

4.2 Las bandas 902 a 928 MHz; 2 400 a 2 498.5 MHZ; 5 470-5 725 MHz y 5 725 a 5 825 MHz pueden ser utilizadas tanto en Interiores como en Exteriores, para la implementación de sistemas de Acceso Inalámbrico, incluidas las Redes Radioeléctricas de Área Local.

4.3 Las bandas 902 a 928 MHz; 2 400 a 2 498.5 MHZ y de 5 725 a 5 825 MHz, puede ser utilizadas para las aplicaciones Industriales Científicas y Médicas (ICM). El nivel de la radiación de los dispositivos ICM, deberá ser tal que no cause interferencia perjudicial al Servicio de Radiocomunicación y en particular a los Servicios de Radionavegación o cualquier otro Servicio de Seguridad.

4.4 La banda 5 150-5 250 MHz debe ser utilizada únicamente en Interiores, para la implementación de sistemas de Acceso Inalámbrico, incluidas las Redes Radioeléctricas de Área Local, de conformidad con la resolución COM 5/16-CMR-03.

4.5 La banda 5 250-5 350 MHz puede ser utilizada tanto en Interiores como en Exteriores, para la implementación de sistemas de Acceso Inalámbrico, incluidas las Redes Radioeléctricas de Área Local.

4.6 Debido a que los Servicios de Radiolocalización y los servicios móviles comparten el uso de las bandas 5 250-5 350 y 5 470-5 725 MHz y con el fin de proteger los radares del Servicio de Radiolocalización que funcionan en dichas bandas, se deberán utilizar las técnicas de mitigación de interferencias referidas en el numeral 6.2.4 de la presente normativa.

4.7 En los sistemas por salto de frecuencia está permitido el empleo de inteligencia para posibilitar al sistema el reconocimiento de otros usuarios de la banda, de manera que de forma individual e independiente elijan y adapten sus saltos de frecuencia a fin de evitar la utilización de canales ocupados. En los sistemas por salto de frecuencia está prohibida cualquier otra forma de coordinación de

Director General

frecuencias que tengan el expreso propósito de evitar la ocupación simultánea de frecuencias de salto individuales por transmisores múltiples.

NOTA: Esta entidad reguladora hace énfasis en que las partes que utilicen dispositivos de telecomunicaciones en las bandas 5 150-5 250 MHz, 5 250-5 350 MHz y 5 470-5 725 MHz para proveer servicios considerados críticos deben determinar si existe un sistema de radar cercano que pueda afectar su operación, para lo cual podrán solicitar a la Dirección de Control y Monitoreo del Espectro Radioeléctrico mediante los procedimientos establecidos de solicitud de Radiotrayectos.

5. AUTORIZACIÓN

La autorización de los sistemas de acceso inalámbrico, incluidas las RLAN, está a cargo del Ente Regulador de las Telecomunicaciones.

5.1. CERTIFICACION DE LOS EQUIPOS Y ANTENAS

Los equipos y aparatos de telecomunicaciones, incluyendo el sistema de antenas, deberán contar con un certificado de homologación extendido por la Dirección de Titulación y Atención a Operadores y Usuarios, de conformidad con lo establecido en el decreto 128-2004. Solamente los equipos y aparatos de telecomunicaciones, incluyendo el sistema de antenas, certificados podrán ser instalados y operados en redes de Comunicaciones sujetas a esta normativa.

El uso de amplificadores de potencia de Radiofrecuencia externo o juego de amplificadores en los Sistemas de Acceso Inalámbrico en las bandas 900 MHz, 2.4 GHz y 5 GHz, estará sujeto a la autorización previa de TELCOR. Su utilización estará permitida sólo si se garantizan todos los parámetros técnicos establecidos en la presente normativa.

5.2. TIPOS DE ENLACES

Para la autorización de Sistemas de Acceso Inalámbrico fijos Punto a Punto se deberá cumplir con el procedimiento general vigente correspondiente emitido por el Ente Regulador y las condiciones contenidas en el numeral 6 de la presente normativa. Se excluye el uso de Sistemas de Acceso Inalámbrico en exteriores para enlaces que utilicen antenas omnidireccionales y el uso de múltiples antenas colocadas intencionalmente transmitiendo la misma información sobre múltiples sectores, según las condiciones contenidas en el numeral 6 de la presente normativa.

6. PARAMETROS DE OPERACIÓN

6.1. BANDAS 902 MHz a 928 MHz, 2 400 MHz a 2 498.5 MHz y 5 725 MHz a 5 850 MHz

6.1.1. SISTEMAS DE MODULACION DIGITAL, INCLUYENDO ESPECTRO ENSANCHADO DE SECUENCIA DIRECTA

Los sistemas de Modulación digital, incluyendo sistemas de Espectro Ensanchado de Secuencia Directa deben cumplir con los siguientes requerimientos:

Ancho de banda

El mínimo ancho de banda medido a 6dB de atenuación deberá ser al menos de 500 kHz.

Máxima Potencia de Cresta de Salida Conducida

1 Watt, con las limitaciones *impuestas en 6.1.4*

Densidad Espectral de Potencia transmitida

No debe exceder de 8 dBm en cualquier banda de 3 KHz, dentro del espectro de emisión y en cualquier intervalo de transmisión continua.

Nota: Para la banda 5 725 a 5 850 MHz puede certificarse de manera alternativa utilizando lo establecido en el numeral 6.2 de la presente normativa.

6.1.2. SISTEMAS POR SALTO DE FRECUENCIA

Los sistemas por salto de frecuencia deben utilizar canales de frecuencias portadoras separadas como mínimo el valor que resulte mayor entre 25kHz o el ancho de banda a 20 dB del canal de salto. El sistema debe saltar de manera pseudoaleatoria a través de una lista ordenada de frecuencias de salto a la razón de salto del sistema. Cada frecuencia debe ser utilizada igualmente, en promedio, por cada transmisor. Los receptores del sistema deberán hacer coincidir sus anchos de banda de entrada con los anchos de banda del canal de salto de sus transmisores correspondientes y deberán cambiar frecuencias en sincronización con las señales transmitidas.

De manera alternativa, los sistemas de FH que operan en la banda de 2400-2498.5 MHz pueden utilizar canales con frecuencias portadoras separadas como mínimo por el valor que resulte mayor entre 25kHz o dos tercios del ancho de banda a 20 dB del canal de salto, siempre que la potencia de salida no sea mayor a 125 mW.

Adicionalmente, los sistemas por salto de Frecuencia deben cumplir con los siguientes requerimientos:

6.1.2.1. Banda de 902 MHz a 928 MHz

Máxima Potencia de Cresta de Salida Conducida

1 W para sistemas con 50 ó más frecuencias de salto.
0,25 W para sistemas con 25 a 49 frecuencias de salto.

Anchura de banda del canal de salto

El ancho de banda máximo permitido, del canal de salto, a 20 dB es de 500 KHz.

Cantidad de frecuencias de salto y tiempo de permanencia en las mismas

Si el ancho de banda a 20 dB del canal de salto fuese menor a 250 KHz el sistema no utilizará menos de 50 frecuencias de salto y el tiempo de permanencia promedio no será mayor de 0,4 segundos dentro de un lapso de 20 segundos.

Si el ancho de banda a 20 dB del canal de salto fuese mayor o igual a 250 KHz el sistema no utilizará menos de 25 frecuencias de salto y el tiempo de permanencia promedio no será mayor de 0,4 segundos dentro de un lapso de 10 segundos.

6.1.2.2. Bandas de 2 400 MHz a 2 498.5 MHz y 5 725 MHz a 5 850 MHz

Máxima Potencia de Cresta de Salida Conducida

1 W, para sistemas de FH en la banda de 2 400-2 498.5 MHz con al menos 75 frecuencias de salto sin traslape y para todo sistema de FH en la banda de 5 725-5 850 MHz.

0.125 W, para otros sistemas de FH en la banda 2 400-2 498.5 MHz.

Anchura de banda del canal de salto

El ancho de banda a 20 dB del canal de salto no será mayor de 1 MHz.

Cantidad de frecuencias de salto y tiempo de permanencia en las mismas

Para 2 400 MHz a 2 498.5 MHz, el sistema debe utilizar al menos de 15 frecuencias de salto y el tiempo de permanencia promedio no será mayor de 0,4 segundos dentro de un periodo de 0.4 segundos multiplicado por el número de frecuencias de salto utilizadas.

Para 5 725-5 850 MHz, el sistema debe utilizar al menos de 75 frecuencias de salto y el tiempo de permanencia promedio no será mayor de 0,4 segundos dentro de un periodo de 30 segundos.

6.1.3. SISTEMAS HIBRIDOS

La operación de salto de frecuencia del sistema híbrido, con la operación en Secuencia Directa o Modulación Digital apagada, deberá tener un tiempo promedio de ocupación de cualquier frecuencia que no exceda 0.4 segundos dentro de un período de tiempo en segundos igual al número de frecuencias de salto empleadas multiplicado por 0.4. La operación en modulación digital del sistema híbrido, con la operación en salto de frecuencia apagada, deberá cumplir con los requerimientos de densidad de potencia del numeral 6.1.1 de esta normativa.

6.1.4. ANTENA

Con excepción a lo establecido en el numeral 6.1.4.1 de esta sección; si se emplean antenas de transmisión con ganancia direccional mayor a 6 dBi, la Máxima Potencia de Cresta de Salida Conducida debe ser reducida por debajo de los valores establecidos en los numerales 6.1.1, 6.1.2.1, 6.1.2.2 de esta normativa, en la cantidad en dB que la ganancia direccional de la antena exceda los 6 dBi.

6.1.4.1. OPERACIÓN CON ANTENAS DIRECCIONALES CON GANANCIA MAYOR A 6 dBi

(A) Operación Punto a Punto: La operación fija punto-a-punto excluye el uso de sistemas punto-a-multipunto, aplicaciones omnidireccionales, y transmisores múltiples co-localizados transmitiendo la misma información. El operador o el instalador del sistema es responsable de que el mismo sea utilizado exclusivamente para operación fija Punto a Punto.

Los sistemas utilizados exclusivamente para enlaces fijo Punto a Punto en:

Banda 2 400-2 498.5 MHz:

Pueden emplear antenas de transmisión con ganancia direccional mayor a 6dBi debiendo reducir la Máxima Potencia de Cresta de Salida Conducida en 1 dB por cada 3 dB que la ganancia direccional de la antena exceda 6dBi.

Banda 5 725-5 850 MHz

Pueden emplear antenas de transmisión con ganancia direccional mayor a 6dBi sin tener que reducir la Máxima Potencia de Cresta de Salida Conducida.

(B) Operación Multidireccional: Los sistemas de transmisión en la banda **2 400-2 498.5 MHz** que utilizan sistemas de antenas con haces direccionales múltiples, simultánea o secuencialmente, con el propósito de dirigir señales a receptores individuales o a grupos de receptores, deben cumplir lo siguiente:

a. La información transmitida a cada receptor debe ser diferente.

b. Si el transmisor emplea un sistema de antena que emite haces direccionales múltiples pero no de manera simultánea, la Máxima Potencia de Cresta de Salida Conducida al arreglo o arreglos de antena que componen el sistema (es decir la suma de la potencia suministrada a todas las antenas, elementos de antena, etc. y sumados a través de todas las portadoras o canales de frecuencia) no debe exceder el límite especificado en 6.1.1 ó 6.1.2 de esta normativa, según sea el caso. Sin embargo, la Máxima Potencia de Cresta de Salida Conducida debe ser reducida en 1 dB por cada 3 dB que la ganancia direccional del sistema de antena (o arreglo de antenas) exceda 6dBi. La ganancia direccional del sistema de antena debe ser calculada de la manera siguiente:

i) Como el resultado de la suma de la ganancia direccional del elemento de mayor ganancia en el arreglo mas 10 log(M) , donde M es el número de elementos del arreglo de antenas.

ii) Puede ser aceptado un valor menor al calculado en i) si se presenta suficiente evidencia que demuestre la precisión del mismo.

c. Si el transmisor emplea un sistema de antena que emite haces direccionales múltiples de manera simultánea utilizando los mismos o diferentes canales de frecuencia, la potencia suministrada a cada haz de emisión estará sujeta al límite de potencia especificado en el numeral B.b de esta sección. Si los haces transmitidos se traslapan, la potencia deberá reducirse para asegurar que la potencia agregada no excede el límite especificado en el numeral b de esta sección. Adicionalmente, la potencia agregada, transmitida simultáneamente en todos los haces no deberá exceder los limites especificados en el numeral B.b de esta sección por más de 8 dB.

d. Transmisores que emiten un solo haz direccional deberán operar bajo las condiciones establecidas en (A) de esta sección.

6.1.5. EMISIONES FUERA DE BANDA

Emisiones fuera de banda

La potencia en cualquier ancho de banda de 100 KHz fuera de la banda de operación del sistema debe ser atenuada por lo menos 20 dB con respecto al nivel máximo de potencia deseada en un ancho de banda de 100 KHz dentro de la banda de frecuencia de operación.

Emisiones no esenciales

Deberán ajustarse a lo establecido por el Reglamento de Radiocomunicaciones de la UIT-R en el Apéndice 3, EDICION 2001.

6.2. BANDAS 5 150 a 5 250 MHz, 5 250 a 5 350 MHz, 5 470 a 5 725 MHz y de 5 725 A 5 825 MHz

6.2.1. BANDA DE 5 150 A 5 250 MHZ

Máxima Potencia de Cresta de Salida Conducida:

No debe exceder el menor valor entre 50 mW ó 4 dBm + 10 log*B*, donde *B* es el ancho de banda de emisión en MHz a 26 dB.

Densidad Espectral de Potencia Transmitida:

La densidad espectral de potencia no debe exceder 4 dBm en cualquier banda de 1 MHz.

6.2.2. BANDAS 5 250 A 5 350 Y DE 5 470 A 5 725 MHZ

Máxima Potencia de Cresta de Salida Conducida:

La potencia de transmisión sobre la banda de frecuencia de operación no debe exceder el menor valor entre 250 mW ó 11 dBm + 10 log*B*, donde *B* es el ancho de banda de emisión en MHz a 26 dB.

Densidad Espectral de Potencia Transmitida:

La densidad espectral de potencia no debe exceder 11 dBm en cualquier banda de 1 MHz.

6.2.3. BANDA DE 5 725 A 5 825 MHz

Máxima Potencia de Cresta de Salida Conducida:

No debe exceder el menor valor entre 1 W ó 17 dBm + 10 log*B*, donde *B* es el ancho de banda de emisión en MHz a 26 dB.

Densidad Espectral de Potencia Transmitida:

La densidad espectral de potencia no debe exceder 17 dBm en cualquier banda de 1 MHz.

6.2.4. TÉCNICAS DE MITIGACIÓN DE INTERFERENCIAS PARA LAS BANDAS 5 250-5 350 Y 5 470-5 725 GHZ:

6.2.4.1. Control de Potencia Transmitida (TPC):

Los sistemas de acceso inalámbrico que operan en estas bandas, deben tener la capacidad para operar al menos 6 dB por debajo del valor EIRP medio de 30 dBm. No se requiere mecanismo de TPC para sistemas con una EIRP menor a 500 mW.

6.2.4.2. Selección dinámica de frecuencias (DFS):

Los sistemas de acceso inalámbrico deben satisfacer los siguientes requisitos:

A. El Umbral Mínimo de Detección de DFS para dispositivos con una EIRP entre 200 mW a 1 W es de -64 dBm. Para los equipos que operan con menos de 200 mW de EIRP, el Umbral Mínimo de Detección es – 62 dBm, promediada durante un 1 μs. El proceso DFS debe proveer una dispersión uniforme de la carga sobre todos los canales disponibles.

B. Tiempo de Verificación de Disponibilidad de Canal. Todo sistemas de acceso inalámbrico deberá realizar una verificación de disponibilidad de canal para comprobar si existe un sistema de radar operando en el canal de radiofrecuencia, antes de iniciar transmisión en dicho canal de radiofrecuencia, el mismo proceso aplica cuando tenga que trasladarse a un nuevo canal de radiofrecuencia. El sistema de acceso inalámbrico, puede comenzar a usar el canal si no se detecta señal de radar con un nivel de potencia mayor que los valores de umbral de interferencia establecidos en el numeral 6.2.2, durante 60 segundos.

Los sistemas de acceso inalámbrico deben realizar una Comprobación Técnica en Servicio para comprobar o verificar que en el canal de operación, ningún radar cocanal se ha desplazado o ha iniciado su funcionamiento dentro del alcance del sistema.

Si el sistema de acceso inalámbrico no ha estado previamente en funcionamiento o no ha realizado una Comprobación Técnica en Servicio continua, no debe iniciar la transmisión en ningún canal antes de completar la verificación de disponibilidad de canal.

C. Período de No-Ocupación. Un canal en el que se ha determinado que contiene una señal de radar, ya sea por Verificación de Disponibilidad de Canal o por comprobación técnica en servicio, está sujeto a un período de no-ocupación de por lo menos 30 minutos durante el cual no puede ser utilizado por el sistema de acceso inalámbrico, a fin de proteger los sistemas de radar. El Período de No-Ocupación debe iniciarse en el instante en que se detecta la señal de radar.

Adicionalmente, en la banda 5 600-5 650 MHz, si se ha determinado que un canal contiene una señal de radar, es necesario realizar una comprobación técnica continua de 10 min en dicho canal antes de utilizarlo. De no ser así, sería preciso emplear otros métodos adecuados tales como el de exclusión de canal.

D. El Tiempo de Desplazamiento de Canal no debe ser mayor de 10 s. Las transmisiones durante este periodo consistirán en tráfico normal por un máximo de 200 ms después de la detección de la señal de radar. Además, durante el tiempo restante pueden enviarse señales de control y gestión intermitentes para facilitar la liberación del canal de funcionamiento.

En el siguiente Cuadro se muestra un resumen de los requisitos descritos anteriormente.

CUADRO 1

Parámetro	Valor
Umbral de detección DFS	−62 dBm para dispositivos con una máxima EIRP. inferior de 200 mW y −64 dBm para dispositivos con una máxima EIRP de 200 mW a 1W promediada a lo largo de 1 µs
Tiempo de verificación de disponibilidad de canal	60 s
Periodo de no ocupación	30 min
Tiempo de desplazamiento del canal	≤ 10 s

6.2.5. ANTENAS

6.2.5.1. Bandas *5 150 a 5 250 MHz* , 5 250 a 5350 y 5 470 a 5725 MHz

Para antenas de transmisión de ganancia direccional mayor a 6 dBi, la potencia de transmisión pico y la densidad espectral de potencia pico deberán ser reducidas en la cantidad de dB que la ganancia direccional de la antena exceda los 6 dBi.

6.2.5.2. BANDA DE 5 725 A 5 825 MHz

Si son utilizadas antenas de transmisión de ganancia direccional mayor a 6 dBi, la potencia de transmisión pico y la densidad espectral de potencia pico deberán ser reducidas en la cantidad de dB que la ganancia direccional de la antena exceda los 6 dBi. Sin embargo, los dispositivos en operación fija punto-a-punto en esta banda pueden emplear antenas de transmisión con ganancia direccional hasta de 23 dBi sin la correspondiente reducción de la potencia de salida pico del transmisor, ni en la densidad espectral de potencia pico.

Para transmisión fija punto-a-punto empleando una ganancia direccional de la antena mayor a 23 dBi, se debe reducir la Máxima Potencia de Cresta de Salida Conducida y la Densidad Espectral de Potencia en 1 dB por cada dB que la ganancia de la antena exceda los 23 dBi. La operación fija punto-a-punto excluye el uso de sistemas punto-a-multipunto, aplicaciones omnidireccionales, y transmisores múltiples co-localizados transmitiendo la misma información. El operador o instalador de un dispositivo, es responsable de asegurar que los sistemas que emplean antenas con alta ganancia direccional sean utilizados exclusivamente para operaciones fijas punto-a-punto.

6.2.6. LÍMITES DE EMISIONES NO DESEADAS

Las emisiones pico fuera de las bandas de frecuencia de operación deberán ser atenuadas de acuerdo con los siguientes límites:

A. Para transmisores que operen en la banda de 5 150 a 5 250 MHz:

   Todas las emisiones fuera de la banda de 5 150 a 5 350 MHz no deberán exceder una EIRP de -27 dBm/MHz.

B. Para transmisores que operen en la banda de 5 250 a 5 350 MHz:

   Todas las emisiones fuera de la banda de 5 150 a 5 350 MHz no deberán exceder una EIRP de -27 dBm/MHz. Dispositivos que operen en la banda de 5 250 a 5 350 MHz que generen

Director General

emisiones en la banda de 5 150 a 5 250 MHz deben cumplir todos los requerimientos técnicos aplicables para la operación en la banda de 5 150 a 5 250 MHz (incluyendo el uso en interiores o recintos cerrados) o como alternativa, cumplir con una EIRP límite de emisión fuera de banda de -27 dBm/MHz en la banda de 5 150 a 5 250 MHz.

C. Para transmisores que operen en la banda de 5 470 a 5 725 MHz:

Todas las emisiones fuera de la banda de 5 470 a 5 725 MHz no deberán exceder una EIRP de -27 dBm/MHz.

D. Para transmisores que operen en la banda de 5 725 a 5 825 MHz:

Todas las emisiones dentro del rango de frecuencia comprendido desde el borde de la banda hasta 10 MHz por encima o por debajo del borde de la banda, no deberán exceder una EIRP de -17 dBm/MHz; para frecuencias 10 MHz o más, por encima o por debajo del límite de la banda, las emisiones no deberán exceder una EIRP de -27 dBm/MHz.

Director General

ACUERDO ADMINISTRATIVO
006-2012

IMPLEMENTACION DE TELECOMUNICACIONES INALÁMBRICAS AVANZADAS

El Presidente Ejecutivo del Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR), en uso de las facultades y atribuciones que le confieren los Artículos 5 y 7 de la Ley Orgánica de TELCOR, publicada en La Gaceta, Diario Oficial No. 137 del 12 de Junio de 1982; Artículos 1, 12 y 13, del Reglamento del mismo cuerpo de Ley, Decreto No. 128-2004, publicado en La Gaceta, Diario Oficial No. 238, del 7 de Diciembre del 2004; Artículos 1, 4 y 5 de la Ley General de Telecomunicaciones y Servicios Postales (Ley No. 200), publicada en La Gaceta, Diario Oficial No. 154 del 18 de Agosto de 1995; Artículos 2, 59, 61 y 64 del Reglamento de la Ley No. 200, Decreto No. 19-96, publicado en La Gaceta, Diario Oficial No. 177 del 19 de Septiembre de 1996 y sus reformas vigentes.

CONSIDERANDO

I

Que de conformidad con el arto. 102 de la Constitución Política de la República, los recursos naturales son parte del patrimonio nacional.

II

Que el Espectro Radioeléctrico es un recurso natural limitado y un bien del dominio público sujeto al control del Estado, correspondiendo a TELCOR la planificación, administración, control y regulación de este recurso para garantizar su uso eficiente, fomentando la libre y leal competencia en la prestación de los servicios de telecomunicaciones.

III

Que TELCOR está facultado para modificar la disposición de frecuencias radioeléctricas, siempre que sea factible, cuando el interés público lo exija para la prestación de servicios prioritarios o estratégicos, para la aplicación de nuevas tecnologías o bien, para el cumplimiento de acuerdos internacionales suscritos y ratificados por el Gobierno de Nicaragua.

IV

Que la rápida evolución de las tecnologías de la información y comunicación demanda la disponibilidad de nuevas bandas de frecuencias que permitan la introducción de tecnologías y servicios avanzados y el aumento decidido de la cobertura y de la disponibilidad de servicios de telecomunicaciones en todo el territorio nacional, especialmente en las zonas rurales desatendidas.

V

Que el Cuadro de Atribución Nacional de Frecuencias establece que el segmento de frecuencias 1775 – 1815 MHz está atribuido a los servicios FIJO y MÓVIL con carácter primario. En la actualidad, este segmento de frecuencias no está en uso en el territorio nacional.

Instituto Nicaragüense de Telecomunicaciones y Correos
TELCOR
Presidente Ejecutivo

VI

Que la Recomendación UIT-R M.1801-1 de abril del año dos mil diez identifica como interfaz radioeléctrica para sistemas de acceso inalámbrico de banda ancha, incluidas aplicaciones móviles y nómadas en el servicio móvil que funcionan por debajo de los 6 GHz, a la interfaz aérea de la norma Acceso Múltiple por División de Código (AMCD) síncrono que opera en el segmento de frecuencias 1775 – 1815 MHz.

VII

Que de conformidad con la Recomendación ITU-R M. 1801-1, los sistemas de acceso inalámbrico de banda ancha que cumplen con la norma de Acceso Múltiple por División de Código (AMCD) síncrono soportan servicios de datos bajo el esquema de mejor esfuerzo, datos multimedia en tiempo real, o voz y datos simultáneos. La interfaz radioeléctrica normalizada se ha optimizado para servicios de voz altamente eficientes, servicios de voz y datos con movilidad total, y para una elevada eficiencia en despliegues de frecuencia única.

VIII

Que TELCOR está tomando medidas pertinentes para asegurar la disponibilidad de espectro para la implementación en Nicaragua de interfaces radioeléctricas avanzadas.

POR TANTO;

ESTA AUTORIDAD REGULADORA

ACUERDA:

I

Modificar la Nota Nacional N97 del Cuadro de Atribución Nacional de Frecuencias, la que ya modificada deberá leerse de la siguiente manera:

"N97 Las bandas de frecuencias 824 – 849 MHz, 869 – 894 MHz, 1775 – 1815 MHz, 1850 – 1910 MHz, 1910 – 1930 MHz y 1930 – 1990 MHz se destinan al servicio de telefonía celular y otros servicios de radiocomunicaciones avanzados demandados por la sociedad."

II

Modificar los artículos 8, 9, 10, 11 y 12 del Reglamento del Servicio de Telefonía Celular, emitido mediante Acuerdo Administrativo No. 4-98, dictado por TELCOR el 30 de marzo de 1998 y publicado en La Gaceta, Diario Oficial No. 122 del primero de julio de 1998, artículos que fueron reformados por el Acuerdo Administrativo No. 40-2000, emitido por TELCOR el veinticuatro de agosto de año dos mil y por el Acuerdo Administrativo No. 054-2004, emitido por TELCOR el primero de octubre de 2004. Los textos de los antedichos artículos ya modificados deberán leerse de la siguiente manera:

Artículo 8.- Norma Técnica de Operación

El Servicio de Telefonía Celular deberá operar en las bandas atribuidas y destinadas a este servicio en el Cuadro de Atribución Nacional de Frecuencias, debiendo los operadores introducir tecnologías digitales modernas que mejoren continuamente la eficiencia del espectro asignado y la calidad de los servicios prestados.

Artículo 9.- Atribución de Frecuencias

En correspondencia con el Cuadro de Atribución Nacional de Frecuencias, las bandas de frecuencias 824 – 849 MHz, 869 – 894 MHz, 1775 – 1815 MHz, 1850 – 1910 MHz, 1910 – 1930 MHz y 1930 – 1990 MHz han sido destinadas por TELCOR para ser utilizadas por los servicios fijo y móvil terrestres con carácter primario, incluyendo el Servicio de Telefonía Celular, conforme el Plan de Frecuencias establecido en el siguiente artículo.

Artículo 10.- Plan de Frecuencias

El Plan de Frecuencias adoptado por TELCOR para la prestación del servicio de Telefonía Celular es el siguiente:

Bandas de frecuencias 824 – 849 MHz y 869 – 894 MHz

Bloque	Transmisión desde la Estación Terminal (TS) (MHz)	Transmisión desde la Estación Base (BS) (MHz)	Número de Canales	Modo de Operación
A´´	824.0 – 825.0	869.0 – 870.0	66	FDD
A	825.0 – 835.0	870.0 – 880.0	666	FDD
B	835.0 – 845.0	880.0 – 890.0	666	FDD
A´	845.0 – 846.5	890.0 – 891.5	100	FDD
B´	846.5 – 849.0	891.5 – 894.0	166	FDD

Bandas de frecuencias 1850 – 1910 MHz, 1910 – 1930 MHz y 1930 – 1990 MHz

Bloque	Transmisión desde la Estación Terminal (TS) (MHz)	Transmisión desde la Estación Base (BS) (MHz)	Número de Canales	Modo de Operación
A	1850 –1865	1930 –1945	1000	FDD
D	1865 – 1870	1945 – 1950	333	FDD
B	1870 – 1885	1950 –1965	1000	FDD
E	1885 – 1890	1965 – 1970	333	FDD
F	1890 – 1895	1970 – 1975	333	FDD
C	1895 – 1910	1975 – 1990	1000	FDD
G	1910 – 1920		333	TDD
H	1920 – 1930		333	TDD

Banda 1775 – 1815 MHz

Bloque	Transmisión desde la Estación Terminal (TS) (MHz)	Transmisión desde la Estación Base (BS) (MHz)	Número de Canales	Modo de Operación
A	1775 – 1785		333	TDD
B	1785 – 1805		666	TDD
C	1805 – 1815		333	TDD

El Número de Canales de cada bloque de frecuencias corresponde al cálculo de canales RF con separación adyacente de 30 KHz de ancho de banda. Esta canalización ha sido establecida únicamente para propósitos de cálculo de las tasas anuales por uso del espectro radioeléctrico. El ancho de banda real de las portadoras RF en cada banda estará determinado por el plan de

frecuencias y la tecnología que cada Operador implemente en su sistema, asegurando el cumplimiento de los niveles de calidad requeridos.

A fin de prevenir interferencias perjudiciales entre operadores de Telefonía Celular que utilicen canales adyacentes con modos de operación FDD-TDD o TDD-FDD, TELCOR analizará y definirá una banda de guarda u otra alternativa tecnológica que será asumida por el operador entrante al momento de la asignación. Las interferencias perjudiciales que resulten durante la operación de los sistemas de los operadores serán resueltas conforme las disposiciones de la Ley General de Telecomunicaciones y Servicios Postales y su Reglamento.

Artículo 11.- Parámetros Técnicos de Operación, Conformidad e Interoperabilidad

Los Parámetros Técnicos de Operación de las Redes y los Servicios de Telefonía Celular estarán determinados en las Normas Técnicas y los correspondientes Títulos Habilitantes que emita TELCOR, y en su defecto por lo dispuesto en las Recomendaciones de la UIT que sean aplicables. La altura de las antenas, la ubicación de las mismas y los demás requerimientos técnicos asociados están determinados por las normativas de las dependencias estatales involucradas y los Parámetros Técnicos de Operación emitidos por TELCOR.

Para un funcionamiento óptimo de las redes de telecomunicaciones, los Operadores e importadores de equipos en general deben cumplir las normas emitidas por TELCOR sobre homologación de equipos y aparatos de telecomunicaciones y las disposiciones sobre Conformidad e Interoperabilidad de Redes de la UIT que sean ratificadas por Nicaragua.

Artículo 12.- Emisiones Radioeléctricas

La Potencia Efectiva Radiada de las instalaciones o dispositivos de las redes celulares y la ubicación de los elementos radiantes deben ser definidos por los Operadores conforme los Límites de Exposición a campos electromagnéticos de radiofrecuencia establecidos en las recomendaciones de la Comisión Internacional de Protección contra las Radiaciones No Ionizantes (ICNIRP) con respecto a las Restricciones Básicas y Niveles de Referencia, mientras no exista una disposición nacional. En particular, las emisiones radioeléctricas de las Estaciones Base deben estar dentro de los Límites, independientemente de las tecnologías que se utilicen.

Asimismo, las emisiones radioeléctricas del equipo terminal deben estar dentro de los límites establecidos para la exposición de las personas a las radiaciones no ionizantes especificadas en la tasa de absorción específica (conocida como SAR o Specific Absorption Rate). Con este propósito, todos los terminales que sean importados a Nicaragua, o los fabricados o ensamblados en el país deben especificar su SAR para propósitos de verificación del cumplimiento de esta disposición.

III

El presente Acuerdo Administrativo entrará en vigencia a partir de la fecha de su publicación en La Gaceta, Diario Oficial.

Dado en la ciudad de Managua a los veintitrés días del mes de agosto del año dos mil doce.

Instituto Nicaragüense de Telecomunicaciones y Correos TELCOR Presidente Ejecutivo

ORLANDO JOSÉ CASTILLO CASTILLO
Presidente Ejecutivo
TELCOR