SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Propuesta de diseño de una red de datos móviles con la solución WiFi Offload complementaria a las redes UMTS y LTE, que permita brindar servicio de internet a usuarios móviles a través de un acceso WiFi

AUTOR:

Ing. Christian Xavier Ferigra Orellana

Trabajo de titulación previo a la obtención del grado de Magister en Telecomunicaciones

TUTOR:

Ing. Romero Paz Manuel de Jesús, MSc.

Guayaquil, a los 21 días del mes de junio año 2017

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por Christian Xavier Ferigra Orellana como requerimiento parcial para la obtención del Título de Magíster en Telecomunicaciones.

TUTOR

_____

MSc. Manuel Romero Paz

DIRECTOR DEL PROGRAMA

_____

MSc. Manuel Romero Paz

Guayaquil, a los 21 días del mes de junio año 2017

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, CHRISTIAN XAVIER FERIGRA ORELLANA

DECLARÓ QUE:

El trabajo de Titulación "**Propuesta de diseño de una red de datos móviles con la solución WiFi Offload complementaria a las redes UMTS y LTE, que permita brindar servicio de internet a usuarios móviles a través de un acceso WiFi**" **previa** a la obtención del Título de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 21 días del mes de junio año 2017

EL AUTOR

_____

Ing. Christian Xavier Ferigra Orellana

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

YO, CHRISTIAN XAVIER FERIGRA ORELLANA

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación**, en la biblioteca de la institución del Trabajo de Titulación de Titulación, "**Propuesta de diseño de una red de datos móviles con la solución WiFi Offload complementaria a las redes UMTS y LTE, que permita brindar servicio de internet a usuarios móviles a través de un acceso WiFi**" **cuyo** contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

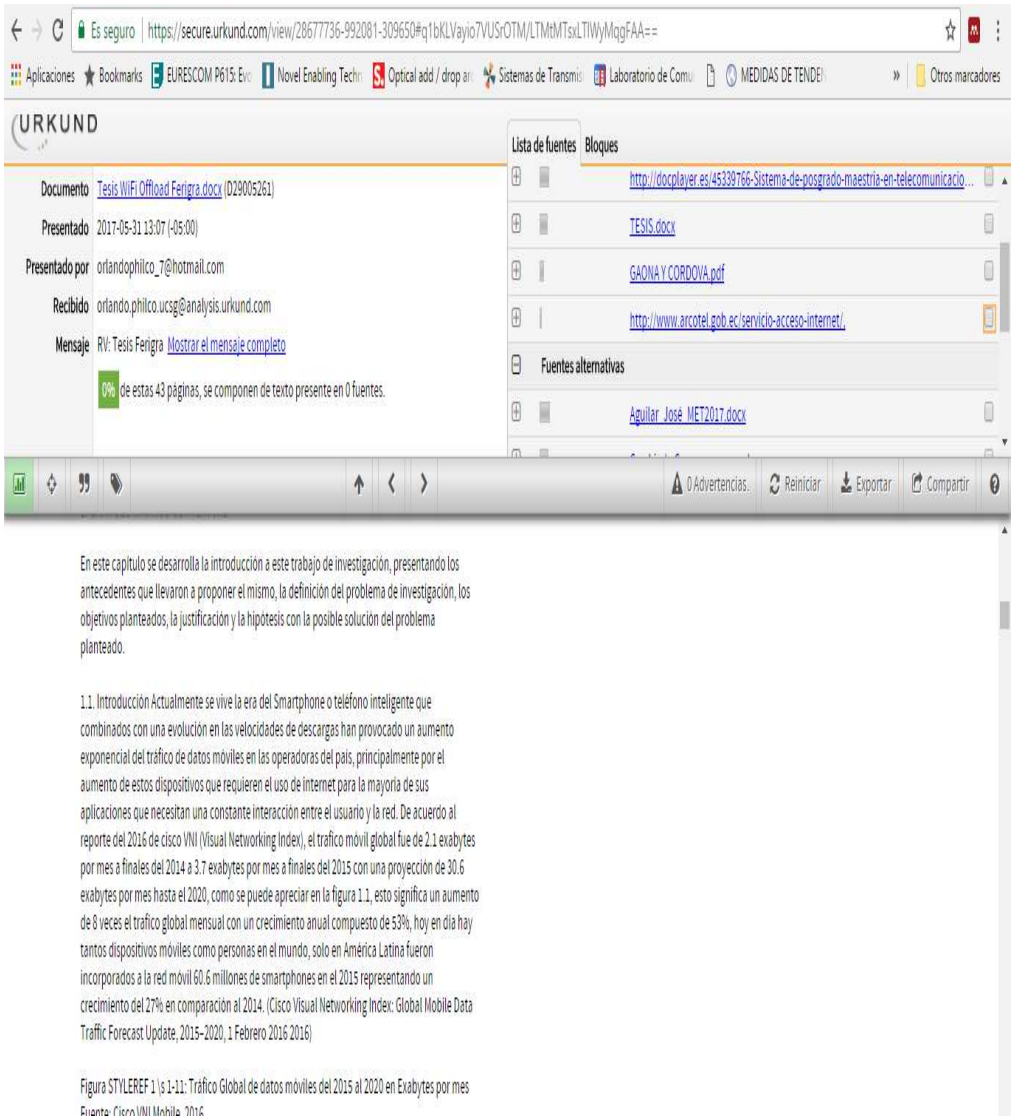
Guayaquil, a los 21 días del mes de junio año 2017

EL AUTOR

_____

Ing. Christian Xavier Ferigra Orellana

REPORTE DE URKUND



Reporte Urkund TT “Propuesta de diseño de una red de datos móviles con la solución WiFi Offload complementaria a las redes UMTS y LTE” del ing. Christian Ferigra al 0% de coincidencias.

Agradecimientos

Por sobre todo a Dios por la fortaleza, salud y sabiduría para seguir adelante en cada proyecto trazado. A mi padre Luis Humberto Ferigra que desde el cielo me bendice y guía en cada paso y quien fue mi motor de impulso para iniciar este posgrado, a mi amada esposa Ana Julia Gabela Gallardo por su amor y apoyo incondicional, mi madre Mirian Orellana Parreño por su infinito amor, dedicación y entrega; mis hermanos Luis Eduardo Ferigra y Juan José Ferigra por ser mi apoyo moral y motivación y mi sobrina Victoria Ferigra por ser la luz de la familia. Un agradecimiento especial a mi maestro y director de Tesis el Ing. Manuel Romero Paz.

Christian Ferigra Orellana.

Dedicatoria

Dedicado a mi padre Luis Humberto Ferigra por haber sido mi ejemplo a seguir, mi mejor amigo y apoyo incondicional, por ser ese padre ejemplar y luchador del cual siempre estaré orgulloso. Por haber sido la persona que me motivó a iniciar este proyecto y aunque se nos adelantó de esta vida terrenal sé que está muy orgulloso de mí.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ROMERO PAZ MANUEL DE JESÚS

TUTOR

f. _____

CÓRDOVA RIVADENEIRA, LUIS SILVIO

REVISOR

f. _____

PHILCO ASQUI ORLANDO

REVISOR

f. _____

ROMERO PAZ MANUEL DE JESÚS

DIRECTOR DEL PROGRAMA

INDICE

INDICE FIGURAS

Capítulo 1: Marco Contextual

Capítulo 2: Redes UMTS y LTE

Capítulo 3: Solución WiFi Offload

INDICE DE TABLAS

Capítulo 1: Marco Contextual

Capítulo 3: Solución WiFi Offload

Resumen

Este proyecto de tesis consiste en proponer el diseño de una red móvil de datos con la solución WiFi Offload para poder proporcionar el servicio de datos móviles a través de una red de acceso no 3GPP como WiFi como una alternativa tecnológica para mejorar el rendimiento general de la red, solventar los problemas de cobertura indoor y mejorar la experiencia de navegación del usuario con velocidades y calidad de servicio que superan a 3G e igualan y mejoran 4G a menor precio el Mbps. Se analizó la mejor propuesta basado en los últimos estándares propuestos por 3GPP y basados en la tecnología de un proveedor de telecomunicación como Huawei. Se describe las arquitecturas existentes UMTS/LTE y la arquitectura final luego de la implementación de la solución con sus respectivos protocolos e interfaces lógicas, así como el detalle del flujo de señalización que debe seguir un usuario para poder acceder al servicio de datos móviles a través de una red de acceso WiFi con un servicio continuo permitiendo handover entre diferentes tecnologías de acceso (WiFi a Celular y viceversa) y entre las mismas tecnologías como (WiFi a WiFi).

Palabras Claves:

UMTS, LTE, WLAN, WiFi Offload, SaMOG,

Abstract

This thesis proposes a mobile data network design with WiFi Offload solution in order to provide data mobile service using WiFi as an alternative non-3GPP access network technology to improve the overall network system performance, to solve the indoor coverage problem and improve the user service experience providing higher bandwidth and sufficient level of QoS than 3G, equal and even better than 4G with lowest data traffic cost. The best proposal based on the latest standards of 3GPP and based on the technology of a telecommunication provider like Huawei was analyzed. The existing UMTS/LTE network architecture are described and the final architecture with WiFi Offload solution with the protocols and logical interfaces and the users signaling traffic flow through non-3GPP access (WiFi), seamlessly handoff between different RANs technologies (WiFi to Cellular) and the same technologies (WiFi to WiFi).

Key words:

UMTS, LTE, WLAN, WiFi Offload, SaMOG,

1. CAPÍTULO I: MARCO CONTEXTUAL

En este capítulo se desarrolla la introducción a este trabajo de investigación, presentando los antecedentes que llevaron a proponer el mismo, la definición del problema de investigación, los objetivos planteados, la justificación y la hipótesis con la posible solución del problema planteado.

1.1.Introducción

Actualmente se vive la era del Smartphone o teléfono inteligente que combinados con una evolución en las velocidades de descargas han provocado un aumento exponencial del tráfico de datos móviles en las operadoras del país, principalmente por el aumento de estos dispositivos que requieren el uso de internet para la mayoría de sus aplicaciones que necesitan una constante interacción entre el usuario y la red. De acuerdo al reporte del 2016 de cisco VNI (*Visual Networking Index*), el trafico móvil global fue de 2.1 exabytes por mes a finales del 2014 a 3.7 exabytes por mes a finales del 2015 con una proyección de 30.6 exabytes por mes hasta el 2020, como se puede apreciar en la figura 1.1, esto significa un aumento de 8 veces el trafico global mensual con un crecimiento anual compuesto de 53%, hoy en día hay tantos dispositivos móviles como personas en el mundo, solo en América Latina fueron incorporados a la red móvil 60.6 millones de smartphones en el 2015 representando un crecimiento del 27% en comparación al 2014. (Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020, 1 Febrero 2016 2016)

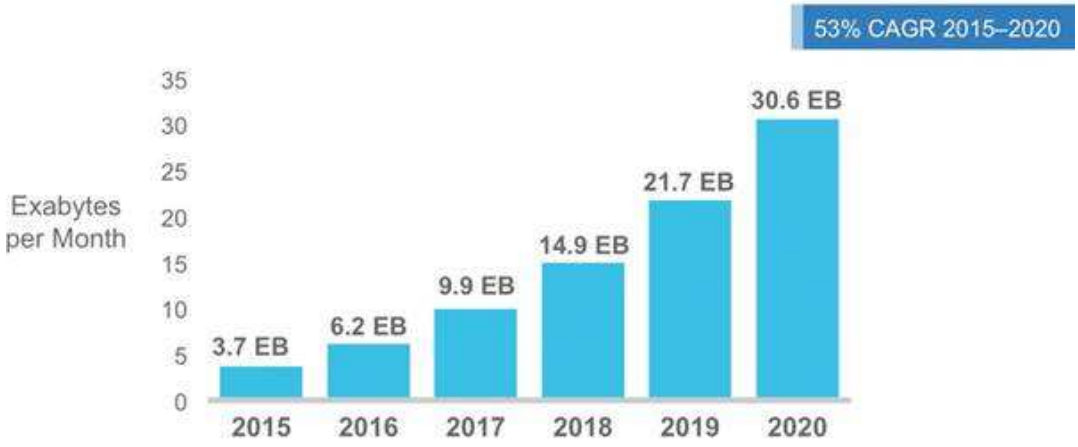


Figura 1-1: Tráfico Global de datos móviles del 2015 al 2020 en Exabytes por mes

Fuente: Cisco VNI Mobile, 2016

En términos de generación de tráfico de datos móviles, Cisco prevé que la región Asia-Pacífico generará la mayor parte del tráfico de datos móviles en el mundo. A continuación se muestra cómo cada una de las regiones se clasifica en términos de generación de tráfico de datos móviles esperada para el 2020:

1. Asia-Pacífico: 13,7 exabytes por mes en 2020
2. América del Norte: 3,25 exabytes por mes en 2020
3. Europa occidental: 2,85 exabytes por mes en 2020
4. Europa del Este y Central: 4,4 exabytes por mes en 2020
5. El Oriente Medio y África: 4,3 exabytes por mes en 2020
6. América Latina: 2,1 exabytes por mes en 2020

La infraestructura desplegada en la actualidad por los operadores del país permite tener acceso a internet móvil en la mayoría de lugares de desplazamiento diario, gracias al aumento en la capacidad de acceso a internet el comportamiento de los usuarios ha ido cambiando el uso de ancho de banda móvil, la tendencia en el uso de redes sociales como Facebook, instagram, twitter o servicios de streaming como Youtube o Netflix, hacen que sea un verdadero reto soportar el incremento de tráfico en las redes móviles por lo que es necesario buscar una solución que prometa resultados favorables tanto para la empresa como el usuario, según Ericsson en su reporte del 2015 a nivel global un smartphone en el 2014 generó 1.0 gigabytes al mes en promedio, en el 2015 fue 1,4 gigabytes al mes y podría alcanzar 8,5 gigabytes al mes en el 2021 solo en América Latina será de 6.0 gigabytes en el 2021. (Ericsson-Mobility-Report-Nov-2015.pdf n.d.)

Una solución a este incremento de tráfico es descargar los datos móviles a redes auxiliares o tecnologías complementarias con una técnica conocida como *Offloading* la cual se podría definir como el porcentaje de bytes descargados a otro canal como Wi-Fi en comparación al total de bytes generados por los usuarios móviles que originalmente son dirigidos a una red de acceso celular, las principales tecnologías de redes complementarias para descarga de datos son Femtoceldas o Wi-Fi.

Wi-Fi Offload es una estrategia importante que ofrece descarga de datos móviles acoplando o integrando una red celular basada en estándares 3GPP (*3rd Generation Partnership Project*) con una red fija no 3GPP, reduciendo los costos elevados que representa implementar una red de acceso celular en los que incluyen gastos de mantenimiento, operación, renovación de licencias de frecuencias que cada vez son más escasas y se hace más difícil la ubicación de macro-celdas en áreas urbanas de alto tráfico, mientras que los costos de una de red de acceso Wi-Fi son mucho menores incluso que el de las femtoceldas y su espectro es libre.

1.2. Justificación

Los dispositivos móviles como smartphone o tablets cada vez tienen un rol más significativo en la vida diaria de los usuarios debido a los múltiples usos y beneficios que representan, esto ha ocasionado que las empresas de telefonía celular tengan la necesidad de buscar soluciones viables que alivien la fuerte inversión que representa la infraestructura de acceso móvil para poder cubrir la necesidad que cada vez es mayor de ancho de banda y movilidad requeridas por los usuarios. Por tal razón se plantea como una opción para la descarga de datos móviles a través de una técnica conocida como WiFi Offload manteniendo una alta QoE (*Quality of Experience*) de una manera rentable.

Wi-Fi es una tecnología posicionada a nivel mundial que podría evitar el estrangulamiento de internet móvil, la mayoría de tráfico de datos proviene de interiores ya sea en las casas o en las oficinas, se puede apreciar que ya las redes Wi-Fi reducen significativamente el tráfico de datos celular, una solución que los operadores han comenzado a adoptar es que cuando un usuario se encuentre en una zona con acceso Wi-Fi al alcance ya sean hotspots públicos o residenciales, el dispositivo móvil reconduzca la transmisión de datos hacia esa vía sin que el usuario sea consciente de ello, la descarga la hacen los dispositivos móviles que soportan conexiones celulares y Wi-Fi. De esta manera se descongestionaría parte del tráfico de las redes celulares que sería desviado a través de redes fijas. Como se puede apreciar en la figura 2.1 cisco pronostica que en el 2020 el 55% del tráfico de datos generado por dispositivos móviles será descargado a redes complementarias.

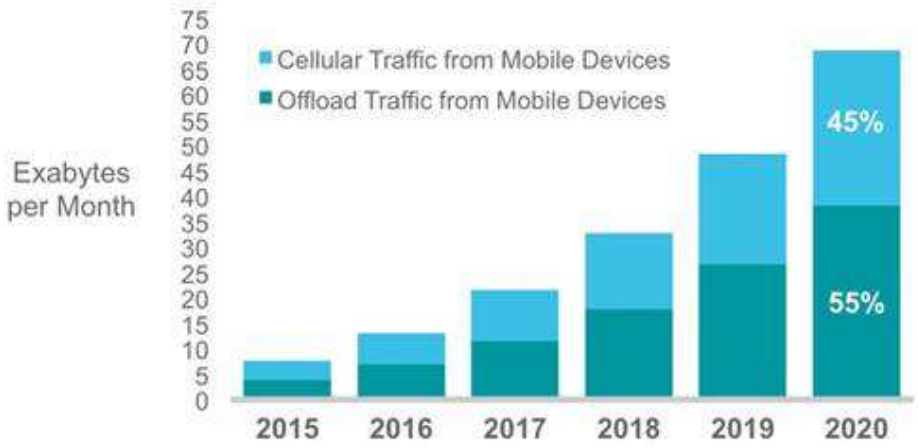


Figura 1-2: En 2020, el 55 por ciento del total del tráfico de datos móviles se descargará

Fuente: Cisco VNI Mobile, 2016

Según cisco el tráfico de datos móviles creció 3 veces más rápido que el tráfico de internet fijo en América Latina en el 2015, con la tecnología de descarga de datos se está tratando de buscar soluciones a este problema y que les permita a los usuarios una conexión transparente a las redes Wi-Fi cuando lleguen a sitios públicos o privados, de esta manera la eficacia de la descarga de tráfico a través de Wi-Fi será mucho mayor, dejando cantidad de frecuencias de móviles libres para hacer llamadas o para personas que por diferentes razones, no se puedan conectar a la solución Wi-Fi Offload. Por lo que será necesario garantizar una movilidad automatizada entre las diferentes redes de acceso siendo la clave para alcanzar una alta calidad de experiencia del usuario.

1.3. Antecedentes

La telefonía celular desde sus inicios con la primera generación 1G, era limitada solo a servicios de voz, no fue hasta la llegada de 2G (Segunda Generación) con la tecnología GSM (*Global System for Mobile communications)* en la década de los 90´s que se consiguieron los primeros avances en transmisión de datos aunque solo tenían acceso a servicios muy básicos, se contaban con tasas teóricas de hasta 14,4 kbps DL (*Downlink*), las siguientes tecnologías de 2G como GPRS (*General Packet Radio Service*) ofrecía velocidades de descargas máximas teóricas de 171,2 kbps y EDGE (*Enhanced Data Rates for GSM Evolution)* velocidades teóricas hasta de 473,6 kbps DL, con estas tecnologías se podían ofrecer servicios como:

- Mensajes de texto SMS (*Short Message Service*).
- Correo electrónico.
- MMS (*Multimedia Messaging Service*).
- WAP (Wireless Application Protocol).
- Transferencias de paquetes pequeños
- Navegación lenta a internet

En la década de los 90´s los móviles eran principalmente usados para hablar, pero la llegada del nuevo milenio marcó el inicio de 3G (tercera Generación) en el que se integraban la transmisión de voz y datos en un mismo sistema y dispositivo, con tecnologías como EV-DO/CDMA2000 (*Evolution – Data Optimized / Code Division Multiple Access*) o WCDMA/UMTS (*Wideband Code Division Multiple Access / Universal Mobile Telecommunication System*) estas tecnologías con sus respectivos estándares alcanzaban velocidades máximas teóricas de descarga de 2 Mbps y de carga o Uplink de 474 Kbps, permitiendo ofrecer servicios de alta transmisión como:

- Video o streaming.
- Transferencia de paquetes más grandes.
- Browser o navegación.
- Video llamadas o video conferencias.
- Juegos en Línea.
- Acceso a todo tipo de redes sociales
- Descargas de APP móviles (Aplicaciones de Software).

Los requerimientos de más altas velocidades de transmisión de datos eran cada vez mayores, las siguientes tecnologías como HSPA (High Speed Packet Access) son consideradas tecnologías 3.5G con velocidades máxima de descargas de datos de 7 a 14 Mbps y velocidades de carga de 5.76 Mbps permitiendo así cumplir las necesidades de los clientes, la siguiente tecnología fue considerada 3.75G HSPA+ con velocidades máxima de descarga de 21 a 42 Mbps y velocidades de carga de 7.2 Mbps, la última tecnología es 4G o LTE (Long Term Evolution) con velocidades máximas teóricas de 100 Mbps DL y 50 Mbps UL(*Uplink*), en Ecuador

los primeros servicios LTE fueron ofrecidos por la Corporación Nacional de Telecomunicaciones (CNT EP) desde el 2014, a partir del 2015 ya los ofrecían las otras 2 empresas del país OTECEL (Operadora de Telefonía Celular Sociedad Anónima) y CONECEL (Consorcio Ecuatoriano de Telecomunicaciones). Todas estas tecnologías de telefonía móvil están gestionadas o estandarizadas por la organización 3GPP. (Qualcomm, 2014)

La evolución de la telefonía celular en Ecuador comenzó siendo un servicio muy costoso que solo era utilizado para llamadas y estaba al alcance de pocos, hoy en día el teléfono móvil es considerado un servicio básico y una herramienta fundamental para el desarrollo diario en la vida de las personas ya que se tiene acceso a todo tipo de información desde un solo dispositivo por lo que es necesario que esté conectado a internet en todo momento, según el ente regulador de las telecomunicaciones en ecuador ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones), el crecimiento de las líneas con internet móvil ha sido considerable en los últimos 6 años como se puede ver en la tabla 1.1 y en la figura 1.3, en diciembre del 2010 se tenían 331.662 líneas representando el 2,35% por cada 100 habitantes y en marzo del 2016 ya son 5.991.107 líneas con un 36,66% por cada 100 habitantes.(ARCOTEL 2016)

Tabla 1-1: Cuentas del servicio de acceso a internet móvil

Año	Usuarios	Población	Usuarios Internet Móvil por cada 100 habitantes
dic-10	331.662	14.111.640	2,35%
dic-11	1.513.107	14.443.679	10,48%
dic-12	3.300.480	14.899.214	22,15%
dic-13	4.205.577	15.774.749	26,66%
dic-14	4.934.076	16.027.466	30,79%
dic-15	5.693.268	16.278.844	34,97%
mar-16	5.991.107	16.341.316	36,66%

Fuente: Arcotel – Ecuador, 2016

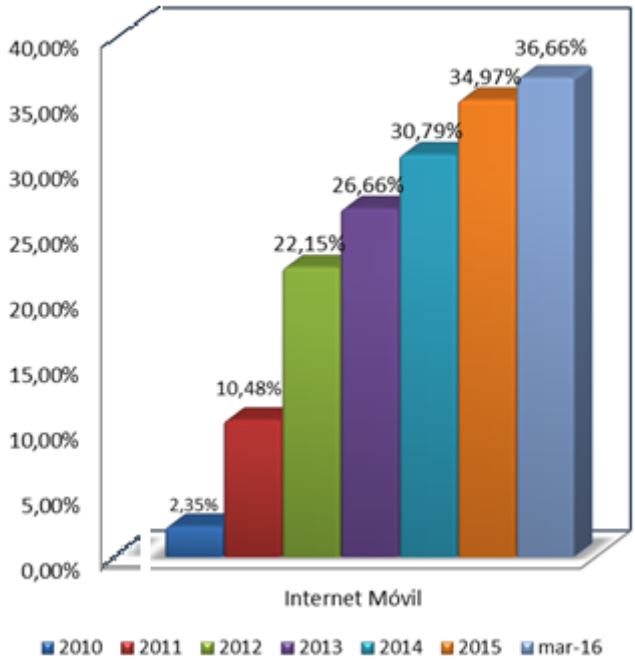


Figura 1-3: Usuarios internet móvil en Ecuador 2010 – 2016, por cada 100 habitantes

Fuente: Arcotel – Ecuador, 2016

Por otra parte se ve que el internet fijo a presentado una rápida expansión en el país, según los datos de ARCOTEL como se observa en la tabla 1.2 y figura 1.4, en el 2010 en Ecuador existían 472.429 cuentas de internet fijo que daban servicio a unos 3 .495.498 usuarios y a marzo del 2016 ya existen 3.495.498 cuentas que ofrecen internet a 11.772.507 usuarios en todo país.

Tabla 1-2: Cuentas del servicio de acceso a internet Fijo

Año	Cuentas	Usuarios	Población	Usuarios Internet Fijo por cada 100 habitantes	Cuentas Internet Fijo por cada 100 habitantes
dic-10	472.429	3.495.498	14.111.640	24,77%	3,35%
dic-11	645.822	3.986.086	14.443.679	27,60%	4,47%
dic-12	890.276	5.710.625	14.899.214	38,33%	5,98%
dic-13	1.084.535	6.880.205	15.774.749	43,62%	6,88%
dic-14	1.322.802	7.924.291	16.027.466	49,44%	8,25%
dic-15	1.491.405	11.027.782	16.278.844	67,74%	9,16%
mar-16	1.511.964	11.772.507	16.341.316	72,04%	9,25%

Fuente: Arcotel – Ecuador, 2016

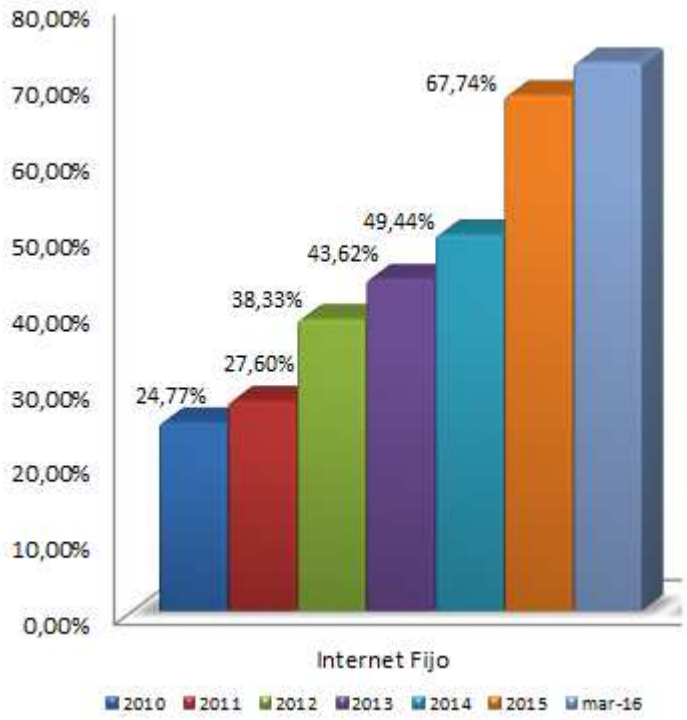


Figura 1-4: Usuarios internet fijo en Ecuador 2010 – 2016, por cada 100 habitantes

Fuente: Arcotel – Ecuador, 2016

Con estos datos es posible ver que en los últimos años el internet fijo y móvil se ha convertido en un servicio de primera necesidad, dentro de los inicios de Wi-Fi Offload la organización 3GPP en el 2002 con el Realese 6 estandarizó por primera vez la interacción entre una red WLAN (Wireless Local Area Network) con un sistema 3GPP denominada I-WLAN (Interworking WLAN) que hace referencia a extender los servicios y funciones de 3GPP a través de una red de acceso WLAN transfiriendo paquetes IP entre un dispositivo celular y el Core Network de un operador móvil a través de una red de acceso WLAN. Ofrece servicio de acceso a internet móvil con autenticación, facturación y seguridad unificada en los siguientes capítulos podremos ver la evolución de esta tecnología con sus respectivos estándares.

1.4. Planteamiento del Problema

El gran incremento del volumen de tráfico de datos móviles y señalización debido a la popularidad de los teléfonos inteligentes que requieren interacción entre el usuario e internet para la mayoría de sus aplicaciones, conduce a una enorme

inversión de las operadoras móviles en infraestructura de redes de acceso, Core, necesidad de canales de radio y licencias de frecuencias la cual no es proporcional al crecimiento de la rentabilidad provocando uno de los mayores obstáculos que tienen que afrontar las empresas que ofrecen este servicio.

Las operadoras móviles tienen la necesidad de buscar soluciones que generen beneficios desde su perspectiva de empresa como proporcionar calidad de servicio a los clientes con menores gastos de inversión y gastos operacionales; desde la perspectiva del usuario que comprende la experiencia en el uso de ancho de banda desde su dispositivo móvil.

Proveer cobertura de telefonía celular en interiores es un desafío para las empresas de telecomunicaciones , debido a la degradación o pérdida de la intensidad de señal en los edificios o casas la cobertura es menor en relación a los exteriores, los mecanismos actuales son muy costosos y poco rentables, el tráfico que proviene de interiores representa un gran porcentaje de la totalidad del tráfico generado por los usuarios móviles por lo que Wi-Fi Offload se presenta como una solución más económica para solventar este problema.

1.5.Definición del problema

Uno de los mayores retos que las operadoras móviles tienen que afrontar es la efectividad en la tasa de descarga de datos móviles (*Mobile Data Offloading*) utilizando mecanismos prometedores como femtoceldas o través de una red de acceso Wi-Fi que ofrecen descongestionar la cantidad de datos generados por los usuarios móviles.

1.6. Objetivos

Los objetivos planteados para este proyecto son los siguientes:

1.6.1 Objetivo General

Proponer el diseño de una red de datos móviles con la solución Wi-Fi Offload complementaria a las redes de datos UMTS y LTE que permita descongestionar el

tráfico generado por los usuarios de telefonía celular redireccionando la descarga de datos móviles a través de una red de acceso WiFi.

1.6.2 Objetivos Específicos

- Detallar el proceso de autenticación y autorización de un usuario móvil en una red de acceso 3GPP y no 3GPP para acceder a los servicios de datos móviles.
- Definir el proceso de señalización y el flujo de tráfico de datos de carga y descarga en una red WLAN/3GPP.
- Proponer el diseño de una solución WiFi offload complementaria a las arquitecturas de redes UMTS y LTE.

1.7. Hipótesis

Un dispositivo celular puede reconducir la señalización y transmisión de datos Uplink y Downlink que tiene a través de una red de acceso móvil a una red de acceso fija como Wi-Fi, manteniendo los mismos procesos de core móvil de autenticación y facturación, levantando y finalizando contextos y sesiones. Permitiendo así a los operadores celulares descongestionar parte del tráfico total generado por los dispositivos móviles en la actualidad sin necesidad de hacer grandes inversiones en licencias de frecuencias e infraestructura de acceso móvil, ya que Wi-Fi funciona con espectro libre y la inversión es considerablemente menor.

Con Wi-Fi Offload también se podrá mejorar la cobertura en interiores que ha sido un problema debido a los altos precios que representaban los mecanismos actuales como femtoceldas.

1.8. Metodología

Este trabajo de investigación es exploratorio porque es necesario recopilar e indagar información y al ser escasa es necesario hacerlo de forma analítica, estudiando cada una de las partes que componen esta tecnología de forma individual para poder

luego sintetizarlas y evaluarla de forma integral. Para lograrlo es necesario ser positivista y cualitativos recolectando datos sin mediciones numéricas pero que permitan resolver las dudas sobre esta tecnología.

2. CAPITULO II: Redes UMTS y LTE

En este capítulo se presenta un estudio por separado de la estructura, principales procesos y funciones del Core Móvil de Datos 3G, 4G y una red WLAN

2.1. Introducción

las tecnologías de telefonía móvil de voz y datos son estandarizadas y regularizadas por la organización 3GPP, en sus diferentes Releases muestra la evolución de la telefonía celular, como podemos observar en la figura 2.1 para la Tercera Generación 3G se estandarizó la tecnología UMTS (*Universal Mobile Telecommunications System*) a partir del Release R99 en el año 2000, que heredó las funciones y servicios de 2G (GSM y GPRS), originalmente fue basado en WCDMA con una tasa de transferencia de 384 Kbit/s. En el Release R4 iniciando el 2001 principalmente se distingue por la separación del plano de control o señalización del plano de usuario o tráfico, 3GPP mejoró WCDMA a través de HSPA en el Reléase R5 y R6 a finales del año 2002 y 2005 respectivamente; HSPA+ con el Release R7 en el año 2007 presenta como principal novedad la conexión de los nodos a través de una red IP.

A partir del Release R8 en el 2009 es estandarizada por primera vez LTE y posteriormente en el año 2011 el Release R10 la Cuarta Generación 4G de tecnología móvil celular (LTE-Advanced).(3GPP R.99 2010)

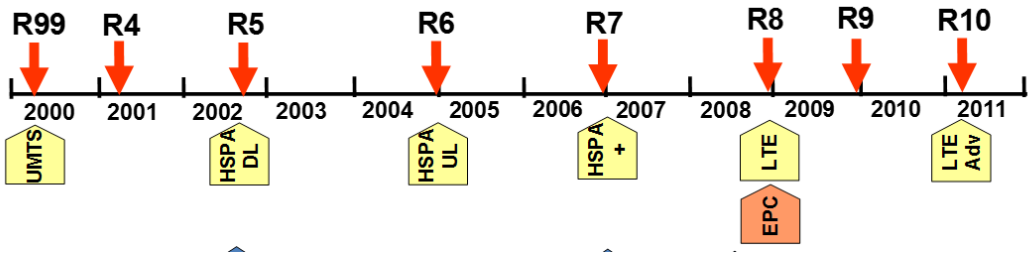


Figura 2-1: 3GPP Release Timeline

Fuente: (3GPP, 2015)

2.2. Estructura de red de datos 3G UMTS

La arquitectura de red del sistema UMTS está conformado por una nueva red de acceso UTRAN (*UMTS Terrestrial Radio Access Network*) y el CN (*Core Network*), la red de acceso UTRAN como podemos ver en la Figura 2.2 provee la conexión entre el UE (*User Equipment*) o equipo de usuario y el Core Móvil; está conformada por el NodoB y RNC (*Radio Network Controler*).

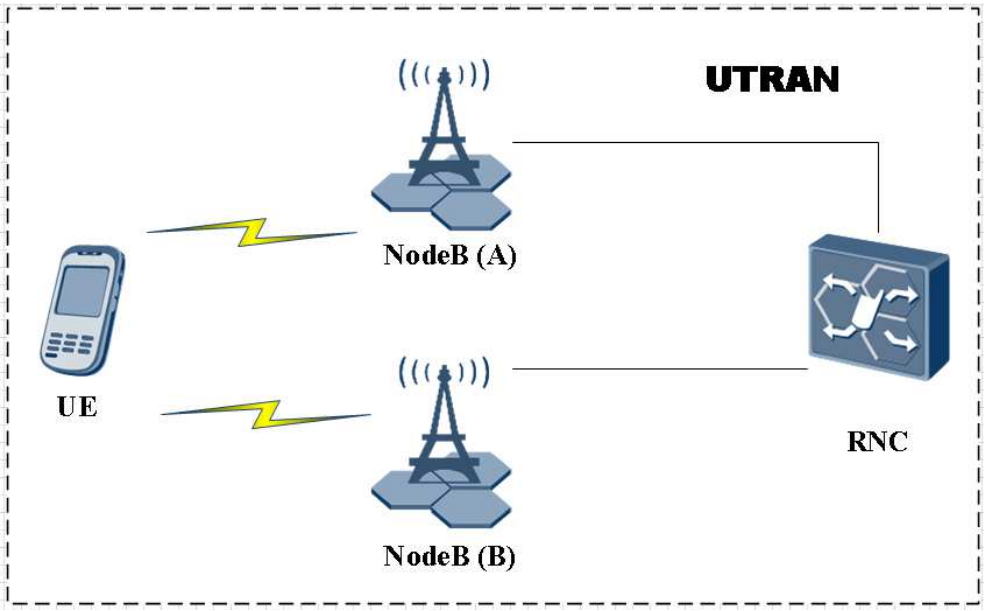


Figura 2-2: UTRAN

Elaborado por: Autor

El core network está constituido de un dominio CS (*Circuit Switched*) un dominio PS (*Packet Switched*), el dominio CS se refiere al conjunto de entidades de core que ofrecen el servicio de tráfico de voz y el dominio PS al conjunto de entidades de core que ofrecen el servicio de tráfico de datos transportando la señalización para el plano de control y los paquetes en el plano de usuario; los componentes del Core Móvil de datos como podemos ver en la figura 2.3 son el SGSN (*Serving GPRS Support Node*), GGSN (*Gateway GPRS Support Node*), DNS *(Domain Name System*), equipos que son en común para el dominio CS y PS están: HLR/ AuC (*Home Location Register / Authentication Center*), EIR *(Equipment Identity Register*), MSC *(Mobile Switching Center*), CG (*Charging Gateway*), OCS (*Online Charging System*). (3GPP R.99 2010)

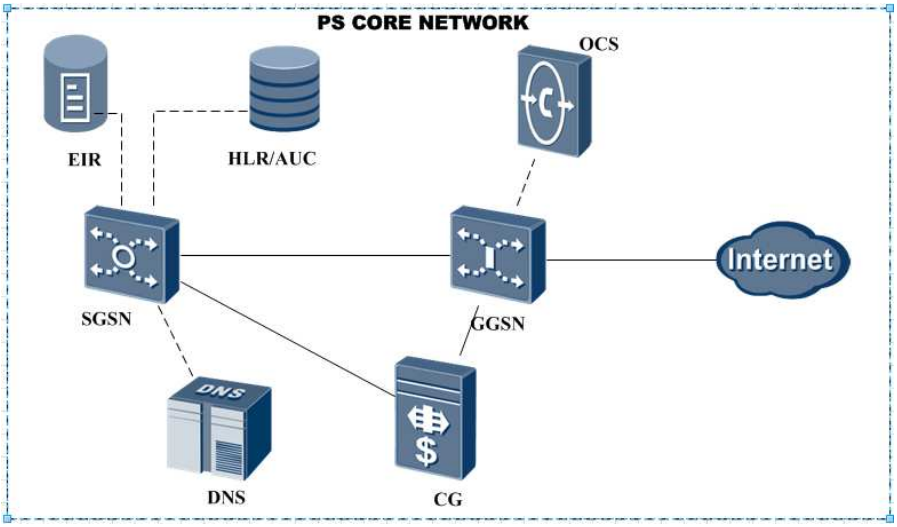


Figura 2-3: PS CORE NETWORK

Elaborado por: Autor

2.2.1 User Equipment

El UE o equipo de Usuario permite el acceso a los servicios de la red y está conformado por:

- El ME (*Mobile Equipment*) o dispositivo móvil usado por el usuario final para poder comunicarse, abarca una variedad de tipo de equipos con diferentes niveles de funcionalidades como un teléfono celular, una Tablet, relojes inteligentes o cualquier equipo terminal compatible con interfaces de acceso para transmisión y recepción de radio. El ME comprende el MT (*Mobile Termination*) que dependiendo de la aplicación y los servicios puede soportar varias combinaciones de TA (*Terminal Adapter*) y grupos de funciones TE (*Terminal Equipment*).

- USIM (*Universal Subscriber Identity Module*), es una tarjeta inteligente, específicamente una tarjeta de circuitos integrados removible que puede ser usada en diferentes dispositivos 3G, almacena información confiable del usuario para ser identificado en la red.(3GPP R.99 2010)

2.2.2 Nodo B

El nodo B es un componente de red el cual representa una celda UTRAN, utiliza la tecnología WCDMA como interfaz de aire, contiene las frecuencias de transmisión y recepción para la comunicación directa con los dispositivos móviles, un nodo B dependiendo de la configuración y tipo de antena puede ser omnidireccional (360°), 3 sectores (3x120°) o 6 sectores (60° cada sector).

Adicional el Nodo B es un elemento de red que provee resultados de mediciones para calcular la posición estimada del usuario.

2.2.3 Radio Network Controller (RNC)

RNC es un equipo tiene la función principal de controlar uno o más nodos B, formando el sistema de red de radio RNS (*Radio Network System*) en sus funciones tiene gestionar los recursos de radio, controlar la variación en niveles de potencia para señalización UL y DL según la posición del usuario, cálculo de niveles de interferencia, gestiona la movilidad del UE basado en los requerimientos de nuevas ubicaciones, maneja un sistema de *broadcast* para posicionar a los usuarios en un nodeB especifico. La RNC conecta los UE con el CN.

2.2.4 Home Location Register/ Authentication Centre (HLR/AuC)

El HLR es una entidad funcional que se la utiliza tanto para el dominio CS como PS en la que se almacena la base de datos de todos los abonados móviles de la red, Contiene toda la información administrativa y de servicios de cada usuario que puede ser actualizada en cualquier momento, los datos principales son:

- Información de suscripción del abonado como: Perfil (prepago / postpago), servicios activos (SMS, voz / datos, *roaming*, buzón de voz, etc.) o servicios restringidos.
- Información de localización del usuario en la red.

- Información de identificación de un usuario como el IMSI *(International Mobile Station Identity)*, tiene el formato E.212 de la recomendación de la ITU (*Internationational Telecommunication Union*) que está formado por el MCC (*Mobile Country Code*) + MNC (*Mobile Network Code*) + MSIN (*Mobile Subscription Identification Number*), para nuestro país el MCC es 740 y el MNC varía según el operador para Movistar es 00, claro es 01 y CNT es 02, el MSISDN (*Mobile Station International Subscriber Directory Number*) tiene el formato E.164 de la recomendación de la ITU está formado por el CC (*Country Code*) + NDC (*Network Destination Code*) + SN (*Subscriber Number*) el CC para Ecuador es 593 juntos permiten identificar a un usuario móvil en la base de datos almacenada en el HLR.

El centro de Autenticación AuC es una entidad integrada en el HLR que comparten la base datos de los usuarios para manejar el proceso de autenticación y así permitir o denegar el acceso a los servicios de la red basados en el IMSI y otros códigos de seguridad que identifican las USIM. La autenticación debe ser mutua entre el UE y la red, los mensajes de señalización deben ser cifrados y encriptados por mayor seguridad del proceso.

2.2.5 Equipment Identity Register (EIR)

EL EIR es una entidad que se encarga de almacenar la información relacionada al estado del IMEI (*International Mobile Station Equipment Identities*), que es único por cada UE y es usado en el sistema UMTS para ayudar a determinar si el usuario está permitido a acceder a la red basado en el estado de su IMEI, detectar USIMs clonadas permitiendo vincular una USIM con uno o más UEs y al detectar que la USIM es ingresada en otro UE queda inhabilitada también permite detectar UEs clonados de la misma forma, los estados de un IMEI puede ser uno de los siguientes:

- *Whitelist*: El usuario está habilitado para acceder a la red.

- *Blacklist*: El usuario en la lista negra no está habilitado para acceder a la red.

El IMEI está formado por 15 dígitos los primeros 6 dígitos son el TAC (*Type Authorization Code*) que es asignado por un centro de autorización y son los códigos del país, los siguientes 2 dígitos el FAC (*Final Assemble Code*) indica el vendedor o fabricante del dispositivo, los próximos 6 dígitos el SRN (*Serial Number*) es el número de serie del teléfono y el digito final es SP (*Spare*) que es el número de reserva.

2.2.6 Charging Gateway Function (CGF)

Es la entidad encargada de recolectar en tiempo real los CDR *(Charging Data Record*) o datos de facturación para consolidarlos, clasificarnos y filtrarlos de acuerdo a su tipo, un CDR incluye datos como por ejemplo para el dominio CS tiempo de establecimiento, duración y finalización de la llamada y para el dominio PS la cantidad de paquetes transferidos, temporalmente los almacena, los pre-procesa y los envía a un centro de facturación.

Existen 2 tipos de mecanismos de facturación del tráfico de datos:

- *Offline Charging*: es un mecanismo de facturación que no afecta el servicio en tiempo real ya que los usuarios pueden hacer uso de los servicios de voz y datos sin limitaciones y al final del mes se le factura la totalidad del tráfico generado, se los conoce como usuarios Postpago.
- *Online Charging:* es un mecanismo en el que la información de facturación si influye en el servicio a tiempo real, el usuario al requerir un servicio primero se consulta su crédito para poder permitir o denegar el acceso al mismo en caso que se le acaba la cuota asignada ya no puede seguir usando los servicios, podemos considerar a los usuarios Postpago controlados que contratan una cuota mensual fija ya sea de saldo de voz o datos y los usuarios pre-pagos que cargan cuota de acuerdo a su necesidad, estos usuarios son controlados por la OCS a través del protocolo Diameter. (3GPP R8 n.d.)

2.2.7 Online Charging System (OCS)

Es la entidad encargada de controlar el crédito en cuota en tiempo real de los usuarios con el mecanismo de facturación Online Charging.
Se conecta al SGW y PGW a través de la interfaz Gy y utiliza el protocolo diameter, esta comunicación con la OCS le permite saber cuándo el usuario deja de tener cuota o balance en su cuenta y el operador debe tomar la decisión de bloquearle el servicio

2.2.8 Domain Name System (DNS)

El DNS se lo utiliza para resolver APN (*Access Point Name*) en diferentes procesos de señalización del Core Móvil, la estructura del APN es: APN-NI + APN-OI, un identificador de la Red NI (*Network ID*) y el identificador del operador OI (*Operator ID*), unas de las funciones del APN es poder identificar a los servicios que desea acceder en la red y junto al HLR determinar si puede acceder o no esos servicios, también se lo utiliza en el proceso de actualización de la ubicación.

2.2.9 Serving GPRS Support Node (SGSN)

El SGSN es uno de los equipos principales del CN, es el nodo encargado de las funciones de control de la señalización, dentro de sus funciones están:

- MM (*Mobility Management*) o gestión de movilidad, tiene como función mantener actualizada la ubicación de un UE dentro de la red al conocer datos como el nodo B, el área de enrutamiento que se encuentra específicamente o dentro de otra red visitante en caso de ser un Roaming. Se encarga controlar los procesos de *Attach* que consiste en el cambio de estado de los usuarios en la red que pueden ser CONNECTED, IDLE o DETACHED, la primera vez que hace el proceso de attach lo hace con el IMSI y se le asigna un P-TIMSI (*PS Temporary IMSI*), al estar en estado Idle y hacer un requerimiento de servicio lo hace con el P-TIMSI. También controla los procesos de RAU (*Routing Area Update*) para cambios de áreas de enrutamiento y RAU periódicos para las actualizaciones. El MM gestiona

los procesos de *paging* que consiste en buscar a un usuario en la red cuando está en estado idle, el paging es un mensaje de broadcast enviado a un grupo de nodos B.

- SM (*Session Managemente*) es la gestión de navegación y encaminamiento de los paquetes se basa en la creación y actualización de estructuras de datos denominados contextos en el UE y los nodos SGSN y GGSN concretamente un Contexto PDP (*Packet Data Protocol*) que es la Información que define una conexión 3G entre un teléfono móvil y la red. La activación del contexto PDP también representa la asignación de una dirección IP privada a un móvil, así como la activación de otros parámetros relativos al abonado. La petición de activar contexto PDP lleva información tal como un identificador de punto de acceso de servicio de capa de red (NSAPI), un tipo de PDP, un APN, un parámetro de QoS (calidad de servicio) demandada y un identificador de transacción (TI). El proceso de PDP Contex consiste en activación, modificación y desactivación.

- El SGSN también desarrolla el enrutamiento y transferencia de los paquetes o servicios de datos entre el UE y el GGSN.

2.2.10 Gateway GPRS Support Node (GGSN)

El GGSN es también un componente primario del Core Mobile, actúa como una interfaz y un router hacia la red externa, cumple funciones de DHCP (*Dynamic Host Configuration Protocol*) asignando una IP privada valida dentro de un pool de IP a los UE dependiendo del tipo de APN y servicio al que quiera acceder. Al contener información de enrutamiento les permite a los dispositivos reenviar paquetes hacia internet, después que el usuario levanto contexto PDP con el SGSN se crea un túnel en el plano de usuario entre el UE y el GGSN para la transferencia de paquetes hacia internet.

El GGSN ofrece servicios como la gestión de QoS soportando negociación de QoS, control de ancho de banda y diferenciador de servicio basado en un análisis de políticas de control y facturación al interactuar con equipos que cumplan la función

de PCC (*Policy & Charging Control*), permite el servicio de desvío del tráfico hacia *Web Proxy* o Captive Portal.

El GGSN cumple funciones de DPI (*Deep Packet Inspection*), realiza la inspección de paquetes ya sea a nivel de capa 3 o 4 del modelo OSI basado en la IP + Puerto o a través del tipo de protocolo ya sea TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*), GRE (*Generic Routing Encapsulation*), IPSEC (*Internet Protocol security*), etc.

También a nivel de capas superiores basadas en URL (*Uniform Resource Identifier)* o el tipo de protocolo de aplicación y servicio ya sea HTTP (*Hypertext Transfer Protocol),* WAP, FTP (*File Transfer Protocol*), DNS, etc.

El GGSN también permite generar reportes de servicio ofreciendo estadísticas sobre el tráfico transmitido ya sea basado protocolo, Web site, un servidor o un usuario especifico al cual se le podría hacer un análisis de desempeño.

2.3 Interfaces lógicas y protocolos de la arquitectura UMTS

En la figura 2.4 podemos observar las conexiones lógicas o las interfaces que conectan cada uno de los equipos del dominio PS en la arquitectura de red UMTS, en la tabla 2.1 se especifican la interfaz que corresponde a cada conexión con su respectivo protocolo ya sea para el plano de control o señalización o el plano de usuario para la transmisión de paquetes.

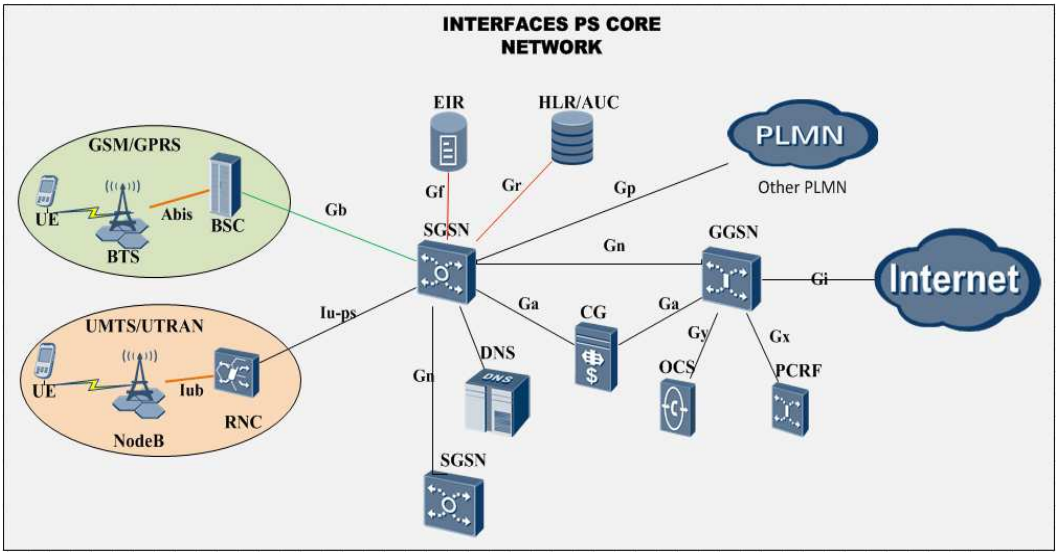


Figura 2-4: INTERFACES PS CORE NETWORK

Elaborado por: Autor

Para mencionar las principales interfaces con sus respectivos protocolos en la arquitectura UMTS:

- Iub es la interfaz lógica que conecta un nodo B con sus respectiva RNC es la encargada de llevar tráfico de señalización a través del protocolo NBAP (*Node B Application Part*) o tráfico de usuario tanto para el dominio CS y PS
- La Interfaz Iu-Ps en el conecta la red de acceso de con el CN específicamente es la interfaz entre una RNC y el SGSN también se divide en plano de control adoptando el protocolo RANAP (*Radio Access Network Aplication Protocol*) encargado de transportar y gestionar los mensajes de señalización para el servicio de acceso de un usuario a la red y así gestionar la asignación de recursos de radio para el plano de usuario que a través del protocolo GTP-U (*GPRS Tunneling Protocol – User plane*) se encargaría de la transferencia de datos.
- Gr, interfaz lógica que conecta el SGSN y el HLR, permite el acceso a la información de usuario que se encuentra almacenada en el HLR y realiza los procesos de autenticación y ubicación de los UE, lo hace a través del protocolo MAP (*Mobile Application Part*) es un protocolo del sistema S7

proporcionando funciones a nivel de capa de aplicación puede ser sobre TDM o IP.

- Gf es la Interfaz usada entre la SGSN y el EIR para intercambiar datos, para que el EIR pueda verificar el estado del IMEI del móvil adoptando el protocolo MAP.
- Gn, es la interfaz que permite la comunicación entre el SGSN y el GGSN o SGSN con otro SGSN de la misma red en caso de tener más de 1, en el plano de control provee mensajes de señalización lo hace atrás del protocolo GTP-C y para el plano de usuario el protocolo GTP-U. Para el caso de conexiones roaming la interfaz lógica que conecta el SGSN con el equipo de borde de otro operador es la interfaz Gp.
- Ga, interfaz que permite que el SGSN y el GGSN puedan generar y enviar CDR a un sistema central o Charging Gateway, el protocolo que utiliza es el GTP' (GTP prime) usa la misma estructura que GTP-C y GTP-U pero tiene la función diferente de transportar CDR.
- Gy, interfaz entre el GGSN y la OCS para la facturación online, utiliza el protocolo Diameter que es un protocolo de red que ofrece servicios AAA *(Authentication, Authorization, Accounting*) su desarrollo es basado en el protocolo RADIUS.
- Gx, es la interfaz entre el GGSN y el PCRF adopta el protocolo diameter, para proveer políticas de control y facturación.
- Gi es la interfaz entre el GGSN y el PDN (*Public Data Network*) directamente a internet

2.4 Arquitectura de red LTE

Previo a 4G, 3GPP estandarizó LTE en el Release R8 como una tecnología evolutiva hacia 4G, se describe la evolución del dominio PS 3GPP o también conocido como EPS (*Evolved Packet System*), optimizando la red de acceso para proveer conectividad IP usando E-UTRAN (*Evolved Universal Terrestrial Radio Access Network*) o LTE y simplificando el Core Network con EPC (*Evolved Packet Core*) o también conocido como SAE (*System Arquitecture Evolution*). La

combinación de E-UTRAN con EPC se conoce como EPS. Esta evolución continua de las tecnologías móviles se centraron principalmente en:

- Reducir latencias;
- Velocidades de navegación más altas;
- Mejoras en la capacidad del sistema y cobertura, y reduciendo los costos a los operadores;
- Reducción de costos del tráfico;
- Flexibilidad en el acoplamiento de tecnologías de acceso ya existentes y nuevas ofreciendo movilidad con una red basada en IP.

Dentro de los cambios en la red, la arquitectura SAE es optimizada en los siguientes aspectos:

- La estación base LTE está directamente conectada al EPC core network, las funciones independientes que cumplían BSC/RNC ahora están integradas en el EnodeB.
- El dominio PS es reestructurado, el plano de control y el plano de usuario del SGSN son separados, la función de señalización del SGSN es implementada por el MME (*Mobility Management Entity*) y la función de plano de usuario para el reenvío de paquetes del SGSN ahora es implementado por el S-GW (*Serving Gateway*).
- Las funciones del GGSN son implementadas por el P-GW (*PDN Gateway*).
- El S-GW y P-GW son implementados ya sea en un mismo nodo físico o por separado.
- Se actualiza el HLR como HSS (*Home Subscriber Server*) cumpliendo las mismas funciones

En la figura 2.5 podemos ver la estructura de red EPS

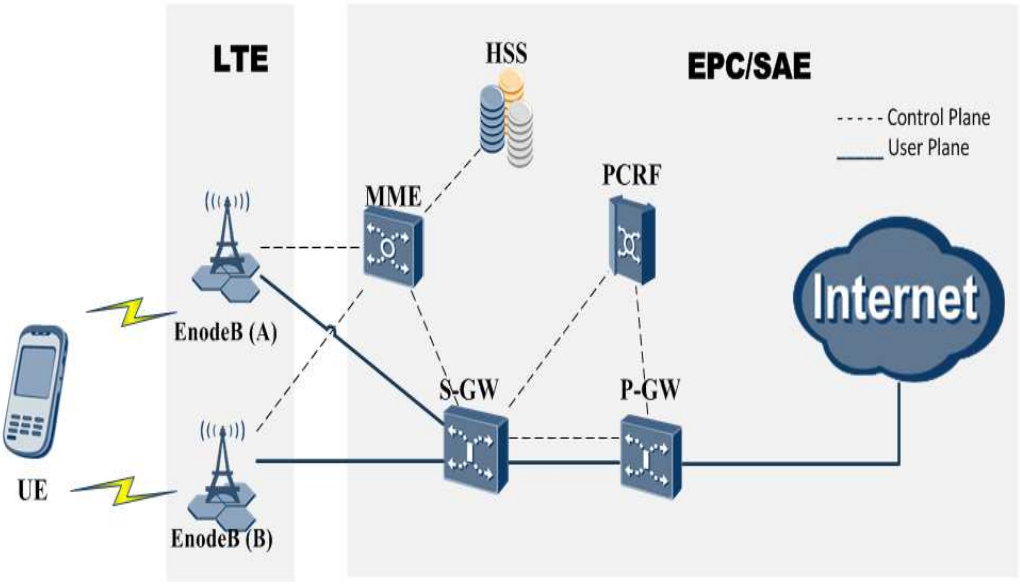


Figura 2-5: EPS Network Structure

Elaborado por: Autor

2.4.1 EnodeB

El EnodeB o su abreviatura eNB es la tecnología de acceso 3GPP, cumple las siguientes funciones:

- Gestionar los recursos de radio ya sea controlando el Radio Bearer, la admisión o asignando dinámicamente los recursos a los UEs para UL y DL.
- Encriptar el tráfico de datos de usuarios;
- Selección del MME en el proceso de attach utilizando la información que provee el UE;
- Enrutar los datos del plano de usuario hacia el S-GW;
- Transmisión de los mensajes de pagins originados desde el MME;
- Transmisión de información broadcast

Los eNBs son interconectados entre ellos a través de la interfaz X2 y se conectan al EPC por medio de la interfaz S1mas específicamente al MME por la interfaz S1-MME y hacia el S-GW por medio de la S1-U.(3GPP R8 TS 36.300 2009)

2.4.2 Mobility Management Entity (MME)

MME es el equipo encardado de gestionar el plano de control o señalización sus funciones incluyen:

- Señalización NAS (*Non-access Stratum*) como la selección de MME, EPS MM (EMM) el control de acceso del UE a las redes de acceso UTRAN y E-UTRAN;
- Gestión de seguridad, señalización NAS encriptanda como protección.
- Procesos de attach, detach, paging, RAU, requerimientos de servicio, reasignación de RNC, TAU (*Tracking Area Update*) y handover.
- Gestiona el proceso de autenticación entre el UE y el HSS;
- Gestión de bearer a través de la lista de TA (*Tracking Area*);
- Información de locación del UE basada en el TA;
- Selección del S-GW y P-GW;
- Gestiona la señalización en procesos de roaming;
- Identidad confidencial implementada a través de asignación de P-TIMSI para 3G y GUTI (*Globally Unique Temporary Identity*) para 4G. (3GPP R8 - TS 23401 2007)

2.4.3 Serving Gateway (S-GW)

El S-GW en la arquitectura EPS es la encargada del plano de usuario dentro de sus funciones principales están:

- Es el punto de anclaje local de movilidad para el handover entre eNB, también es el encargado de gestionar la movilidad entre LTE y 2G/3G;
- Cuando el UE está en estado IDLE, el S-GW implementa un buffer de paquetes DL hasta que se realice el procedimiento de service request a través del paging y pueda recibir los paquetes;
- Gestiona los contextos del UE;
- Es el encargado de generar y enviar CDRs hacia el charging Gateway, soportando facturación de paquetes UL y DL por usuario y QCI (*QoS class Identifier*).

2.4.4 PDN Gateway (P-GW)

El P-GW en la arquitectura SAE cumple las mismas funciones que el GGSN en UMTS de brindar la conectividad a los usuarios hacia internet siendo el punto de entrada y de salida del tráfico de datos, dentro sus principales funciones están:

- Es el punto de anclaje para el plano de usuario entre redes de acceso 3GPP y no 3GPP
- Asignación de IP address a los UE;
- Función de DPI;
- Filtrado de paquetes basada en subscriptores como por ejemplo SA (*Service Awareness*);
- Soporta prioridad en la transferencia de paquetes UL y DL etiquetando o marcando los paquetes;
- Servicio de facturación UL y DL basado sobre políticas y reglas de facturación en conjunto al PCRF y SA basado en políticas locales, Service Redirection;
- Direct Tunnel.

2.5 Interfaces lógicas y protocolos EPS

En la arquitectura de red EPS existen interfaces lógicas que conectan con los equipos de la red UMTS, la mayoría de proveedores tienen integrado en un mismo nodo físico el SGSN y MME por lo que la interfaz lógica se maneja internamente. Se puede ver en la figura 2.6 las interfaces de la red EPS y UMTS.

- S1-MME es la interfaz usada entre el MME y el eNodeB para el plano de control adoptando el protocolo de capa 7 S1-AP (*S1 Aplication Protocol*) utilizando como protocolo de transporte SCTP (*Stream Control Transmission Protocol*). Es utilizado para la creación, modificación y terminación del E-RAB (*E-UTRAN Radio Access Bearer*), transmitir señalización entre los UEs y la red para la transmisión de mensajería NAS asegurando una transmisión confiable sobre la red wireless.

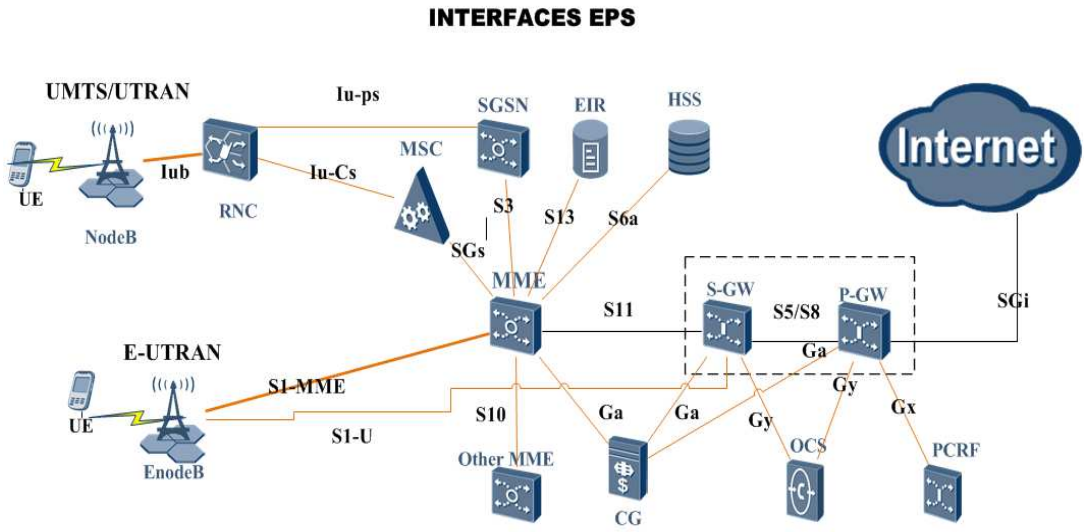


Figura 2-6: EPS Network Structure

Elaborado por: Autor

- S1-U es usada entre el S-GW y el eNodeB. El protocolo UDP es usado en la capa de transporte para transmitir los mensajes en el plano de usuario datos UL y DL adopta el protocolo GTP-U de capa superior.
- S6a es la interfaz usada entre el MME y HSS. Utiliza el protocolo de transporte SCTP transporte para transmitir los mensajes Diameter de capa superior. A través de esta interfaz se provee los servicios de autenticación de usuarios para acceder a la red y la gestión de datos de los subscriptores, en caso de ser usuarios con roaming utilizan la misma interfaz. También se encarga de la administración de localización permitiendo la actualización de la localización, borrado de los datos de suscripción *cancel location*, y el borrado de la información del usuario después del tiempo de purga.
- S10 es la interfaz usada entre MMEs del sistema EPC utiliza el protocolo GTP-C para reenviar información de contexto del suscriptor y señalización de traspaso durante el handover de MME.
- S11 es la interfaz entre el plano de control del MME y el S-GW adoptando el protocolo GTP-C, es usada para transmitir mensajes de establecimiento, actualización y borrado de bearer.
- S5/S8 son interfaces para el plano de control y plano de usuario entre el S-GW y el P-GW, sobre el plano de control son usadas para enviar mensajes

que permitan establecer el bearer para la transmisión de los datos y sobre el plano de usuario se usan para transmitir flujos de paquetes UL y DL entre el S-GW y P-GW, la interfaz S5 aplica en escenarios que no son roaming. Cuando el S-GW y el P-GW están integrados la interfaz S5 es una interfaz interna. la interfaz S8 es usadas en el S-GW y el P-GW en escenarios con roaming. Existen 2 tipos de interfaces S5/S8 la basada en GTP definida por 3GPP TS 23.401 para redes de acceso 3GPP en que utiliza GTPv2 para el plano de señalización y GTPv1 para el plano de usuario y el segundo tipo es la interfaz S5/S8 basado en PMIP (*Proxy Mobile IP)* es definido por 3GPP TS 23.402 para redes de acceso Non 3GPP como WLAN.

- S3 es una interfaz de plano de control usada entre el SGSN y el MME para soportar movilidad interna del sistema soportando el handover entre 3G y LTE.
- SGs es la interfaz entre el MME y MSC permitiendo enviar información den ambos sentidos para poder desarrollar CSFB (*Circuit Switched Fallback*).
- SGi es la interfaz entre el P-GW y la PDN para la salida de paquetes ya sea a internet o un servidor privado.

2.5.1 Protocolo GTP y Protocolo PMIP

El protocolo GTP involucra las funciones de gestión del path o camino y la gestión de los túneles entre nodos de la red UMTS/EPS. Dentro de las funciones está el establecer, actualizar o eliminar un túnel GTP que sirve transmitir datos entre: SGSN y SGW, MME y SGW, E-UTRAN y SGW y entre SGW y PGW. La función de gestión del path asegura que la conexión entre ambos nodos esté funcionando correctamente y así todos los mensajes o datos son transmitidos entre los nodos y en caso que falle dicha conexión desactiva todos los túneles asociados a ese path. En la figura 2.7 vemos la red móvil basada en el protocolo GTP.

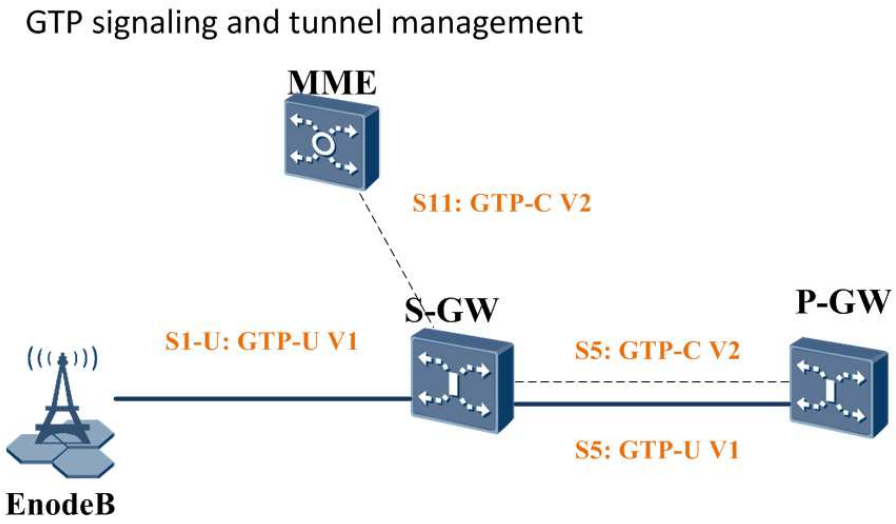


Figura 2-7: GTP signaling

Elaborado por: Autor

PMIP gestión de señalización involucra gestión de túnel y path, la función de gestión de túnel es el encargado de establecer un túnel PMIP para la transmisión de datos entre LMAs (Local Mobility Anchor) o entre MAGs (Mobile Access Gateway), se puede establecer, actualizar y eliminar un túnel y la función de gestión del path al igual que el protocolo GPT asegura que la conexión entre los nodos funcione correctamente. En la figura 2.8 vemos la red basada en el protocolo PMIP.

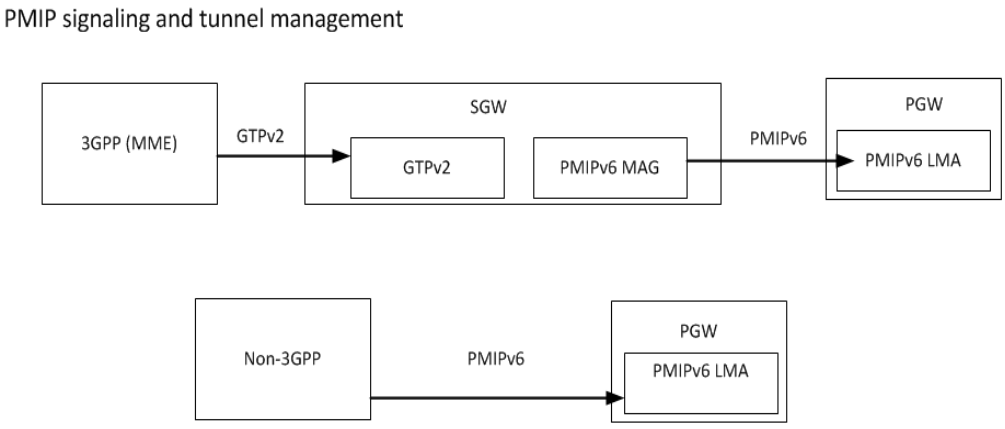


Figura 2-8: Evolución de la Red PS

Elaborado por: Autor

2.6 UMTS y EPS Bearer

En el dominio PS, 3GPP separa la transmisión de tráfico de señalización a través de plano de control con el protocolo GTP-C y la transmisión de paquetes de datos a través del plano de usuario con el protocolo GPT-U. Un túnel GTP es usado entre 2 entidades o nodos para que se puedan comunicar separando el tipo de tráfico en diferentes flujos. GTP-C provee un túnel para la transmisión de mensajes de señalización para UMTS entre RNC – SGSN – GGSN y para LTE entre EndoB – MME – SGW – PGW, GTP-U provee un túnel para la transmisión de paquetes UL y DL, hasta el Release R6 el túnel de plano de usuario se establecía para UMTS entre RNC – SGSN – GGSN pero 3GPP introdujo en el Release R7 *Direct Tunnel Solution* un túnel directo para el plano de usuario entre los nodos RNC y GGSN de esta manera el SGSN no necesita enviar datos de usuario. Como se puede ver en la figura 2.9 la evolución del plano de control y usuario en los diferentes Releases.

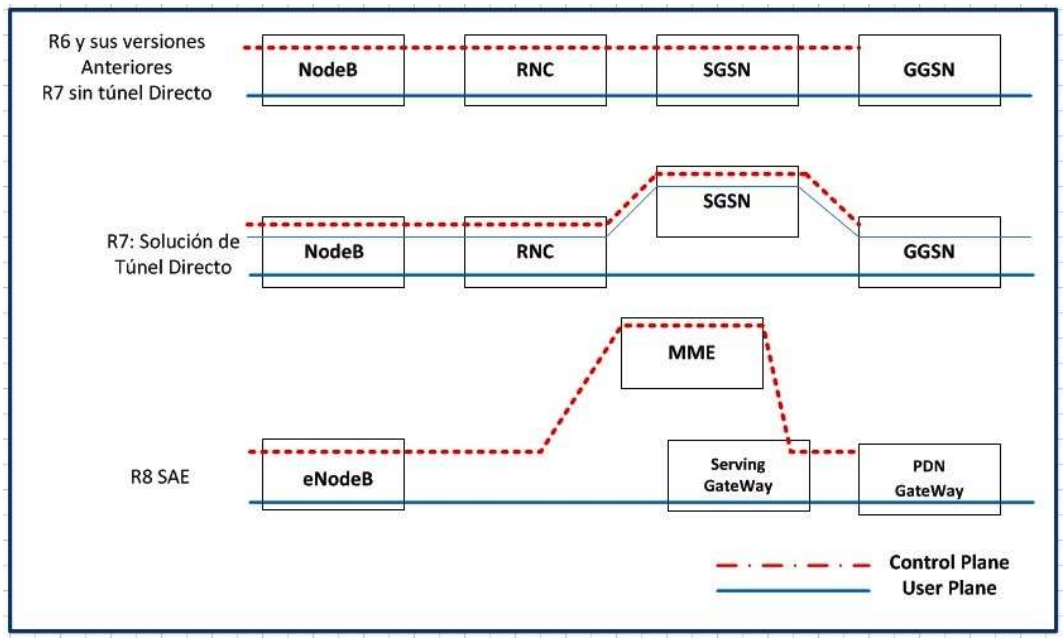


Figura 2-9: Evolución de la Red PS

Elaborado por: Autor

A partir del Release R7 en el dominio PS de la arquitectura UMTS, 3GPP establece un túnel directo GTP-U entre la RNC y GGSN, ahorrando recursos y de esta manera optimizando el plano de usuario en el dominio PS, reduciendo los tiempos de retardos o *delay* y mejorando la experiencia del usuario.

En la figura 2.10 se puede ver las diferentes portadoras o *Bearers* que se crean en el plano de usuario, cuando un UE hace un requerimiento de servicio de contexto lo hace en el plano de control, el SGSN determina habilitar la función de túnel directo basado en la configuración local, solicita se asigne recurso de radio al UE para formar el RAB (*Radio Access Bearer*) entre el UE y RNC y se levanta el túnel GTP-U entre la RNC y GGSN para que el UE pueda enviar paquetes UL transmitidos directamente por la RNC hacia el GGSN y los paquetes DL transmitidos directamente desde el GGSN a la RNC.

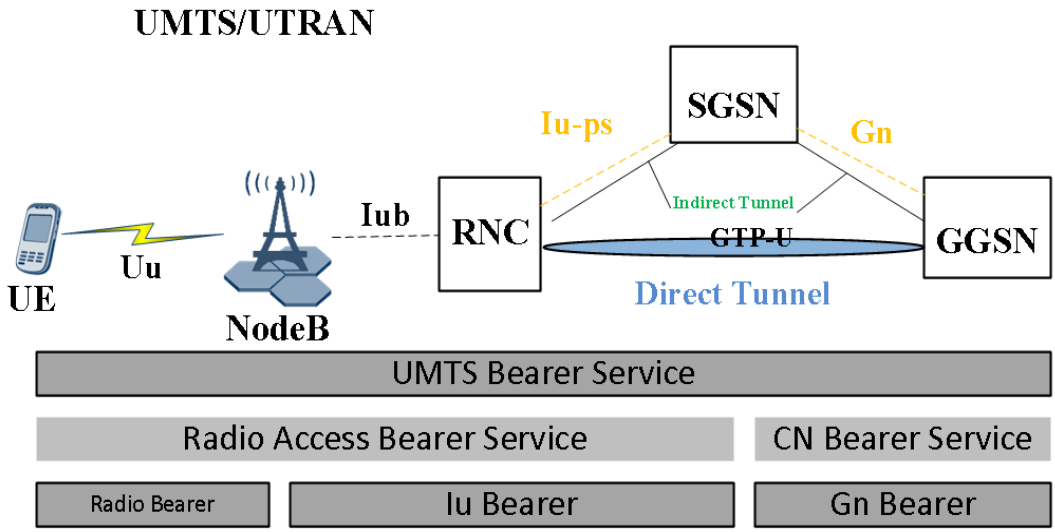


Figura 2-10: UMTS Bearers

Elaborado por: Autor

En la arquitectura SAE, la conexión IP entre el UE y un PDN es llamada sesión EPS, cada conexión PDN o sesión EPS es representada por una dirección IP de un UE con su respectivo APN. Una sesión EPS cuenta con varios Bearers para poder gestionar y entregar tráfico de usuario pero antes de entregar tráfico es necesario establecer el *Default bearer* entre el UE y el P-GW para que se le pueda asignar la IP al UE y pueda establecer la sesión con la PDN e intercambiar paquetes UL y DL de acuerdo a las reglas establecidas en el PCRF por el operador a cada usuario.

Un Bearer EPS o portadora EPS se lo podría definir como un tubo a través del cual se entregan los paquetes IP desde el UE hacia el P-GW que es el punto de entrada o salida hacia redes externas ya sean privadas o públicas, un solo UE puede tener

varias portadoras EPS al mismo tiempo. Como se puede ver en la figura 2.11 un EPS bearer está formado por las siguientes 3 portadoras:

- DRB (*Data Radio Bearer*): entre el UE y eNB es establecida sobre la interfaz LTE-Uu para poder entregar tráfico de usuarios.
- S1 Bearer: Entre el eNB y el S-GW se establece sobre la interfaz S1-U, el tráfico de usuario es entregado a través de un túnel GTP.
- S5 Bearer: entre S-GW y P-GW es establecida sobre la interfaz S5 y entrega tráfico de usuario a través de un túnel GTP.

E-RAB está formado técnicamente por un DBR y S1 Bearer y conecta un UE con el SGW.

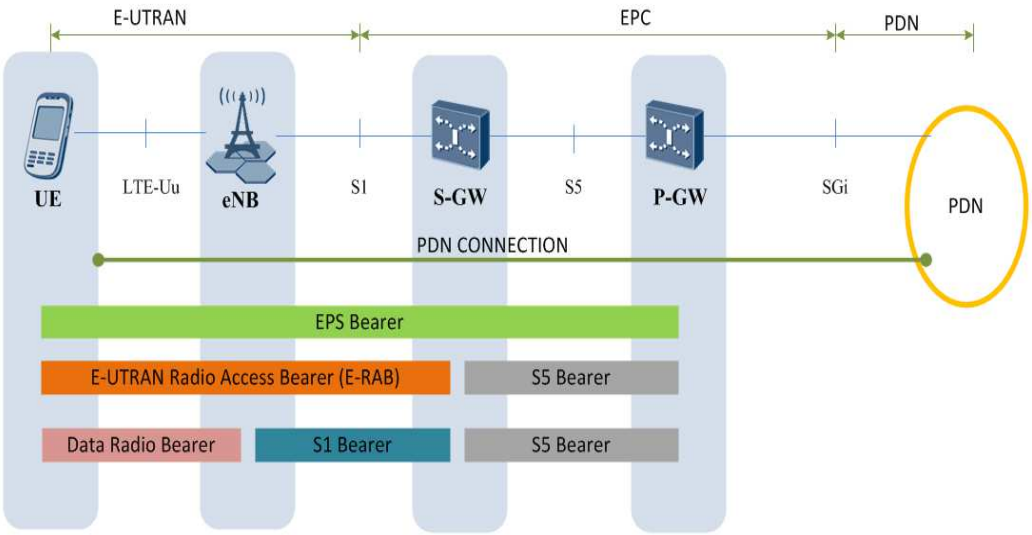


Figura 2-11: EPS Bearers

Elaborado por: Autor

Se puede definir dos tipos de portadoras o bearer: *default* y *dedicated*, una sesión EPS debe tener mínimo un default bearer y uno o varios *dedicated bearers* como se observa en la figura 2.12. Una vez que en el proceso de attach se establece el default bearer se le provee al usuario una conexión IP continua, se adicionan uno o más túneles dedicados para uno o más tráficos específicos ya sea VOIP, streaming, etc vinculándolos al default bearer establecido previamente.

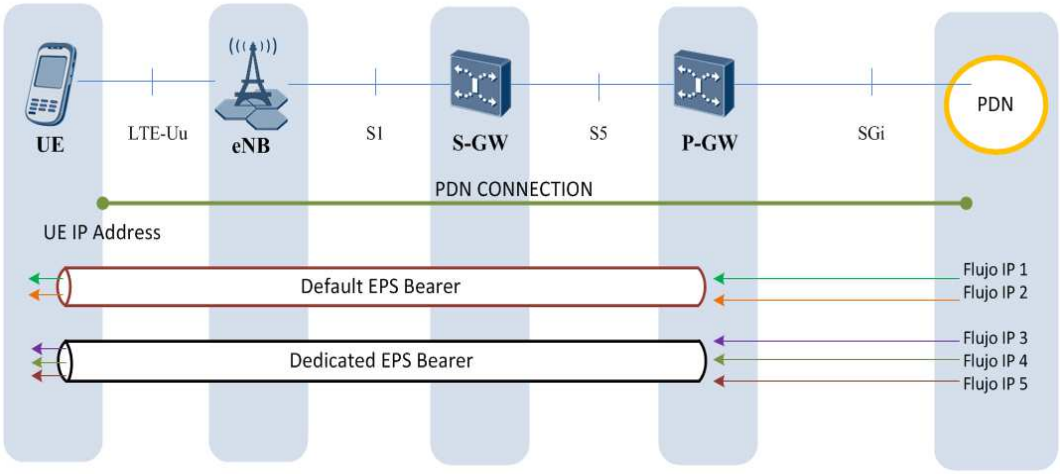


Figura 2-12: Default y dedicate bearer

Elaborado por: Autor

2.7 Mobility Management (SGSN/MME)

La gestión de movilidad en 3G es conocida como PMM (Packet Mobility Management) y en 4G seria EMM (EPS Mobility Management) ambos tienen como función controlar el acceso de un UE a la red e implementan los siguientes procedimientos:

- Attach
- Detach
- Paging
- Service Request
- handover
- Serving RNC relocation (interfaz IU)
- RAU (interfaz IU)
- TAU (interfaz S1)
- TA list management (interfaz S1)

De los procedimientos de MM como attach, RAU o TAU dan como resultado diferentes estados de los subscriptores en 3G se definen 3 estados PMM:

- PMM-CONNECTED
- PMM-IDLE
- PMM-DETACHED

En EPS se dividen los estados del subscriptor en EMM y ECM (EPS Connection Management). Los estados EMM son:

- **EMM – Deregistered** o estado Detach, este estado indica que el UE no está conectado a la red por lo tanto no tiene ningún tipo de recurso de red asignado, llegar a este estado puede ser de manera implícita cuando se vence un tiempo en el que el usuario no está haciendo uso de su dispositivo ya sea porque ha estado mucho tiempo en zonas sin cobertura de señal o le saco la batería, el MME o SGSN toman la decisión sin consultarle al usuario y la otra opción es la manera explícita cuando el usuario procede a apagar el dispositivo se envía una petición de detach al core.
- **EMM – Registered,** el Usuario entra en estado *registered* luego de un proceso de registración exitoso ya sea después del procedimiento de attach o TAU, en ese momento el MME conoce la ubicación del UE, este estado permite al UE desarrollar requerimientos de servicio ya sea iniciado por el MME en caso que necesite acceder al UE lo hace a través del paging o si quiere inicia un servicio que necesite enviar paquetes UL.

Los estados ECM son:

- **ECM - IDLE** un UE está en estado IDLE cuando se le borra el recurso de radio asignado entre el UE y el eNB y la conexión S1-MME y S1-U, los dispositivos pasan a estado Idle después que se expira un tiempo establecido por el operador en la mayoría son 20 segundos después el dispositivo no ha hecho requerimientos de navegación o servicio de esta manera cuando la red quiera acceder al UE debe enviar un paging para establecer nuevamente la conexión.
- **ECM – Connected,** un UE entra en estado connected cuando se restable el recurso de radio, la conexión S1-MME y S1-U ya sea porque la red desea

accede al Usuario a través de un paging o porque el Usuario hizo un requerimiento de servicio**.**

Cada operador maneja sus respectivos tiempos para mantener los diferentes bearer activos y cambiar los estados de cada UE para no tener recursos destinados a los usuarios cuando no hacen uso del servicio de datos por diferentes motivos.

2.8 Security Management (SGSN/MME)

La función de gestión de seguridad es usada para asegurar que solo usuarios legales puedan acceder a la red según su tipo de identificación es desarrollado en asociación con el MM. Asegura la confidencialidad e integridad de los datos de usuario y señalización a través de los canales de radio.

La función de seguridad está formada por:

- *Authentication*
  - La función de autenticación es usada para identificar un subscriptor y autenticar de manera bidireccional, la red autentica la USIM y viceversa.
- *UE Identity Confidentiality*
  - Es implementada a través de la asignación de P-TMSI/GUTI.
- *NAS Signaling Encryption and Integrity Protection*
  - Provee cifrado y protección integral para la señalización NAS, mejorando el Sistema de seguridad.
- *Identity Request*
  - Los usuarios pueden ser identificados por sus IMSI o IMEI.

2.8.1 Autenticación y Cifrado

Cada vez que un UE requiera establecer una conexión con el operador móvil para acceder a los servicios es necesario que se realice el proceso de autenticación y el cifrado de la señalización y los datos de usuario para asegurar su privacidad, la autenticación es en ambos sentidos; la red que autentique al usuario para prevenir accesos no autorizados y el usuario que autentique la red protegiéndolos de intercepciones ilegales y ataques, esta característica de seguridad es realizada con el uso de funciones criptográficas y algoritmos. Para la autenticación se utiliza el

método EAP (*Extensible Authentication Protocol*) que soporta diferentes variedades de autenticación, para usuarios GSM que utilizan SIM (*Subscriber Identity Module*), usuarios UMTS y LTE que utilizan USIM los métodos de autenticación de UE se tiene: EAP-SIM, EAP-AKA (*Extensible Authentication Protocol-Authentication and Key Agreement*) y EAP-AKA´ (EAP-AKA enhancement).

Los equipos que están involucrados en el proceso de autenticación y cifrado son la UE, SGSN/MME, HLR/AuC/HSS. Los principales parámetros de autenticación a considerar son los siguientes:

Quintupleta: considerados los vectores de autenticación.

- RAND: es un número generado por el AuC de forma aleatoria consta de 128 bits para el proceso de autenticación, es considerado un número inicial para conseguir un set de autenticación como XRES, IK, CK.
- RES o XRES: EL HSS genera el XRES mientras que RES es un valor esperado como respuesta del usuario, es un parámetro de un máximo de 128 bits y mínimo 32 bits.
- CK (*Ciphering Key*): es un parámetro para poder cifrar tráficos de datos de usuarios.
- IK (*Integrity Key*): es un parámetro de protección integral de señalización.
- AUTN: es un parámetro para que la USIM pueda validar la red.

Parámetros relacionados:

- AUTS: es un parámetro de 112 bits utilizado para la re-sincronización, provee información necesaria a la red para iniciar nuevamente el proceso de autenticación cuando existe una falla por sincronización.
- SQN: Numero de secuencia de 48 bits es usado para calcular el MAC (*Message Authentication Code*) y AUTN, este contador es almacenado por la USIM como SQNms y en el HSS como SQNhe. SQNhe es un contador individual de cada usuario y el SQNms denota el máximo número de secuencia recibido por la USIM.

- AMF (*Authentication and key Management Field)*: parámetro de 16 bits que indica el algoritmo y la clave de cifrado usada para generar cierto vector de autenticación, indica la máxima diferencia entre SQNms y SQN.
- K: es un valor de 128 bits usado para calcular parámetros de autenticación y es almacenado en la USIM y AuC.
- AK (*Anonymity Key*): es usado para encriptar el SQN contenido en el AUTN y se lo calcula basado en el RAND y K.
- *Operator Variant Algorithm Configuration Field* (OP): el mismo OP puede ser utilizado para todos los usuarios de un mismo operador para que se los pueda distinguir de otros operadores.
- OPC: es el valor producido después que el OP es encriptado.
- MAC-A (*Message Authentication Code*) con una longitud de 64 bits es usado para que la red autentique al usuario.
- MAC-S es el código de autenticación generado cuando una falla de sincronización y es necesario restablecer la misma.

Los datos almacenados en el HSS son: IMSI, K, K4, AMF, OP o OPC y SQNhe y los datos almacenados en el USIM son: IMSI, K, OP o OPC y SQNms, los algoritmos utilizados en el proceso de autenticación y cifrado son: f1, f2, f3, f4, f5, f1*, f5*, UIE y UIA. (3GPP R11 TS 33.102, 2013). El procedimiento consiste en compartir la información de autenticación entre el SGSN – HSS y SGSN – UE, cuando un UE hace un requerimiento de servicio al SGSN este nodo necesita autenticar al UE por lo que envía un *Authentication Request* al HSS mensaje que incluye el IMSI, el HSS debe generar los AV (*Authentication Vectors* / Vectores de autenticación) como se puede ver en la figura 2.13.

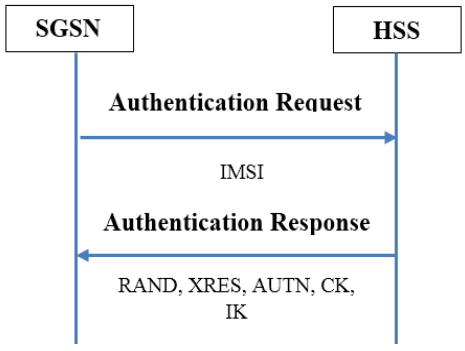


Figura 2-13 Autenticación desde SGSN al HSS

Elaborado por: Autor

2.8.2 Generación de los Vectores de autenticación

En la figura 2.14 vemos como se generan los vectores de autenticación por el HSS, la creación de los vectores o quintupletas está basada en el algoritmo MILENAGE. El HSS comienza generando un nuevo SQN que es un parámetro que va incrementando continuamente se utiliza para que la USIM pueda verificar la validez de los vectores de autenticación se lo conoce como SQNms y adicional genera un impredecible número aleatorio RAND, para cada usuario, el HSS registra un contador SQNhe. (3GPP R13 2016)

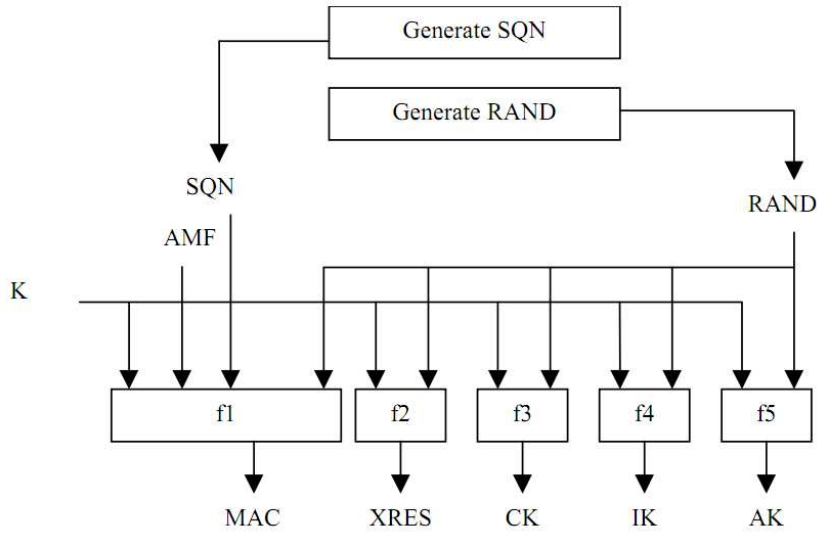


Figura 2-14 Generación de vectores de autenticación

Fuente: (3GPP, 2015)

f0 the random challenge generating function;

f1 the network authentication function;

f1* the re-synchronisation message authentication function;

f2 the user authentication function;

f3 the cipher key derivation function;

f4 the integrity key derivation function;

f5 the anonymity key derivation function.

f5* the anonymity key derivation function for the re-synchronisation message.

Cada uno de los algoritmos serán utilizados para proporcionar autenticación mutua entre ambas entidades HSS / USIM y así proteger la identidad del usuario. Dentro de los aspectos de implementación todas las funciones f0 a f5* se diseñaran de manera que puedan aplicarse sobre una tarjeta inteligente o chip equipada con microprocesador de 8-bits que funciona a 3.25 MHz con una ROM de 8 kbytes y 300 bytes de RAM produciendo AK, XMAC-A, RES, CK y IK con un tiempo de ejecución menor a 500 ms.(3GPP R13 2016)

Los criterios de diseño a considerar son los siguientes:

- Sin el conocimiento de las *Secrets Keys* o clave secretas K, las funciones f1, f1*, f2, f3, f4, f5 y f5* deben ser prácticamente imposible de determinar basado en las funciones aleatorias de entradas (RAND‖SQN ‖ AMF).
- Debe ser imposible determinar el valor del secret key K o del OP, al manipular las entradas o examinando las salidas del algoritmo.
- Los evento que tiendan a violar los criterios 1 y 2, deben considerarse insignificantes si se producen con una probabilidad aproximada de: 2^{-128} (o requiere aproximadamente 2^{128} operaciones) o menos.
- Los evento que tiendan a violar los criterios 1 y 2, deben ser examinados si ocurren con una probabilidad aproximada de 2^{-64} (o requiere aproximadamente 2^{64} operaciones) para asegurar que no tengan serias consecuencias.
- El diseño debe basarse en estructuras bien conocidas y evitar la complejidad innecesaria. Esto simplificará el análisis y evitará la necesidad de una evaluación externa formal.

Para generar los vectores del lado del HSS y USIM como se observa en la figura 2.13 y 2.14 respectivamente:

- La USIM utiliza la función f1 para calcular XMAC-A y el HSS para calcular MAC-A, utilizando la formula $f1_K$(SQN || RAND || AMF), en la que se concatenan los valores de SQN, RAND y AMF utilizando f1 en función del valor de K. Cada vez que la autenticación es exitosa la USIM almacena el SQNms en la memoria flash en este caso el SQNms es para el dominio PS,

la siguiente autenticación se requiere que el valor recibido de SQNms sea mayor al valor almacenado en la memoria flash, esto significa que la red va a generar nuevos vectores de autenticación y no serán repetidos.

- El valor de XRES en el HSS y RES en la USIM se genera con la formula $f2_K$(RAND).
- El parámetro *cipher key* CK = $f3_K$(RAND) y el parámetro *integrity key* IK = $f4_K$(RAND).
- Si el número de secuencia SQN va a ser encriptado el HSS y la USIM calculan el parámetro AK =$f5_K$(RAND) y encripta el valor de SQN con la operación lógica de disyunción exclusiva SQN ⊕ AK = SQN xor AK. Realizar este proceso es opcional en el HSS, para la USIM debe obligatorio el encriptado para calcular el valor de XMAC-A.
- Finalmente el HSS arma el *Autentication Token* AUTN concatenando los valores ya calculados de SQN encriptado, MAC-A y el valor de AMF quedando la formula AUTN = SQN [⊕ AK] || AMF || MAC-A de esta manera del lado del HSS los vectores de autenticación o quitupleta quedan definidos (RAND, XRES, CK, IK, AUTN) como se los puede observar en la figura 2.15. (3GPP R13 2016)

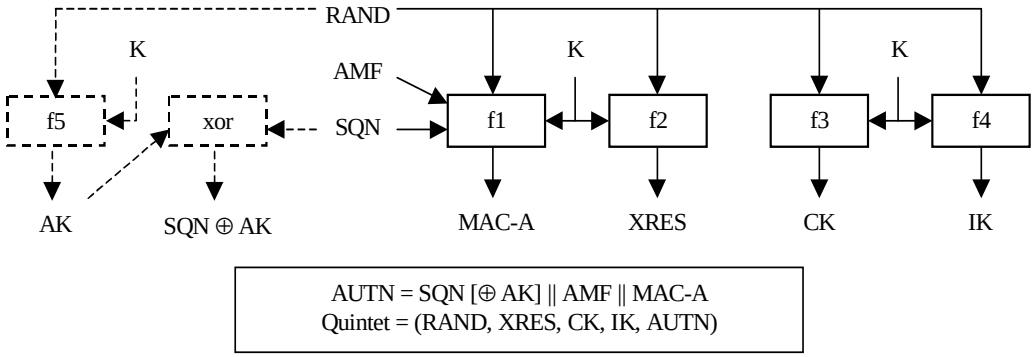


Figura 2-15 Generación de los vectores de autenticación del lado del HSS

Fuente: (3GPP, 2015)

Después de recibir los valores de RAND y AUTN la USIM actúa de la siguiente manera para generar los vectores como vemos en la figura 2.16:

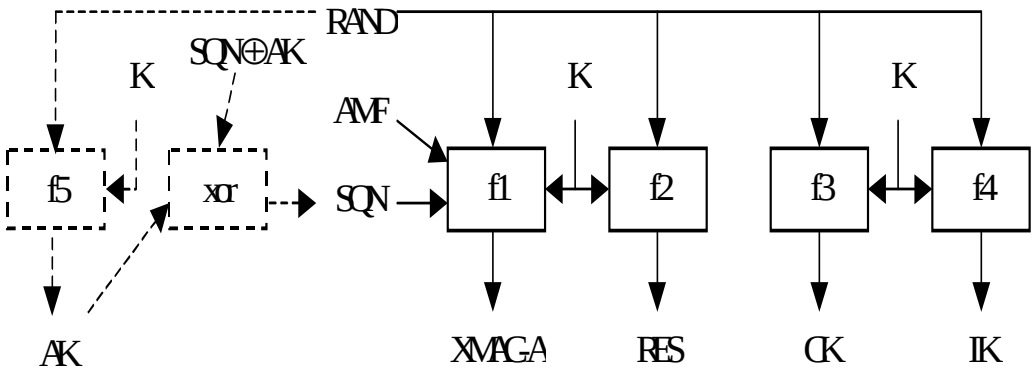


Figura 2-16 Generación de los vectores de autenticación del lado del USIM

Fuente: (3GPP, 2015)

2.8.3 Generación de Re-sincronización en la USIM y en el HSS

En el caso que se identifique una falla en la sincronización, la USIM inicia el proceso de Re-sincronización como se lo muestra a continuación en la figura 2.17 y se detalla a continuación:

- La USIM calcula el parámetro MAC-S = $f1*_K$(SQNms || RAND || AMF*), en la que se concatenan los valores de SQNms, RAND y AMF* utilizando f1* en función del valor de K y AMF* es el valor predeterminado usado en el re-sincronización.
- Si el número de secuencia SQNms va a ser encriptado con AK, la USIM calcula el parámetro AK =$f5*_K$(RAND) y encripta el valor de SQNms con la operación lógica de disyunción exclusiva SQNms ⊕ AK.
- Finalmente el *Re-synchronisation Token* AUTS es construido concatenando los valores ya calculados de SQNms encriptado y MAC-S quedando la formula AUTS = SQN [⊕ AK] || MAC-S.

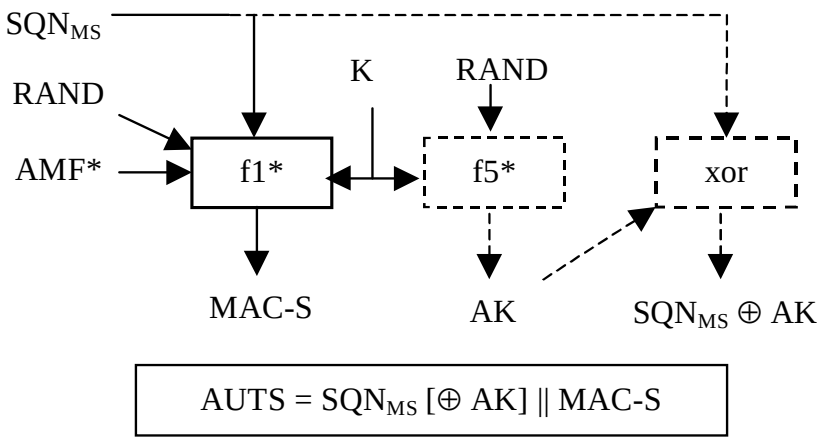


Figura 2-17 Generación del AUTS en la re-sincronización en la USIM

Fuente: (3GPP, 2015)

Al recibir una indicación de sincronismo fallido y los parámetros (AUTS y RAND) el HSS debe desarrollar las siguientes funciones criptográficas como se detalla a continuación y se muestra en la figura 2.18:

- Si el número de secuencia SQNms fue encriptado con AK, el HSS calcula el parámetro AK $= f5*_K$(RAND) y recupera el valor de SQNms con la operación (SQNms $\oplus$ AK) xor AK.
- Si el SQNhe generado no es aceptable el HSS calcula XMAC-S = $f1*_K$(SQNms || RAND || AMF*), y el luego el HSS verifica si el MAC-S incluido en el AUTS es igual al calculado XMAC-S, si el valor no es el mismo el HSS modifica el valor de SQNhe basado en SQNms del AUTS, luego el HSS calcula unos nuevos vectores de autenticación y se los envía al SGSN para iniciar el nuevo proceso de autenticación.

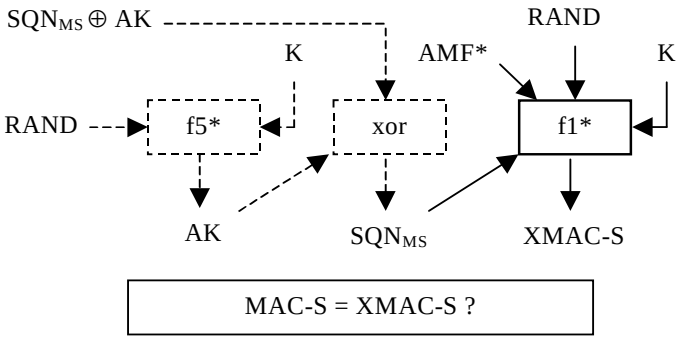


Figura 2-18 Re-sincronización en el HSS

Fuente: (3GPP, 2015)

2.8.4 Proceso de autenticación 3G

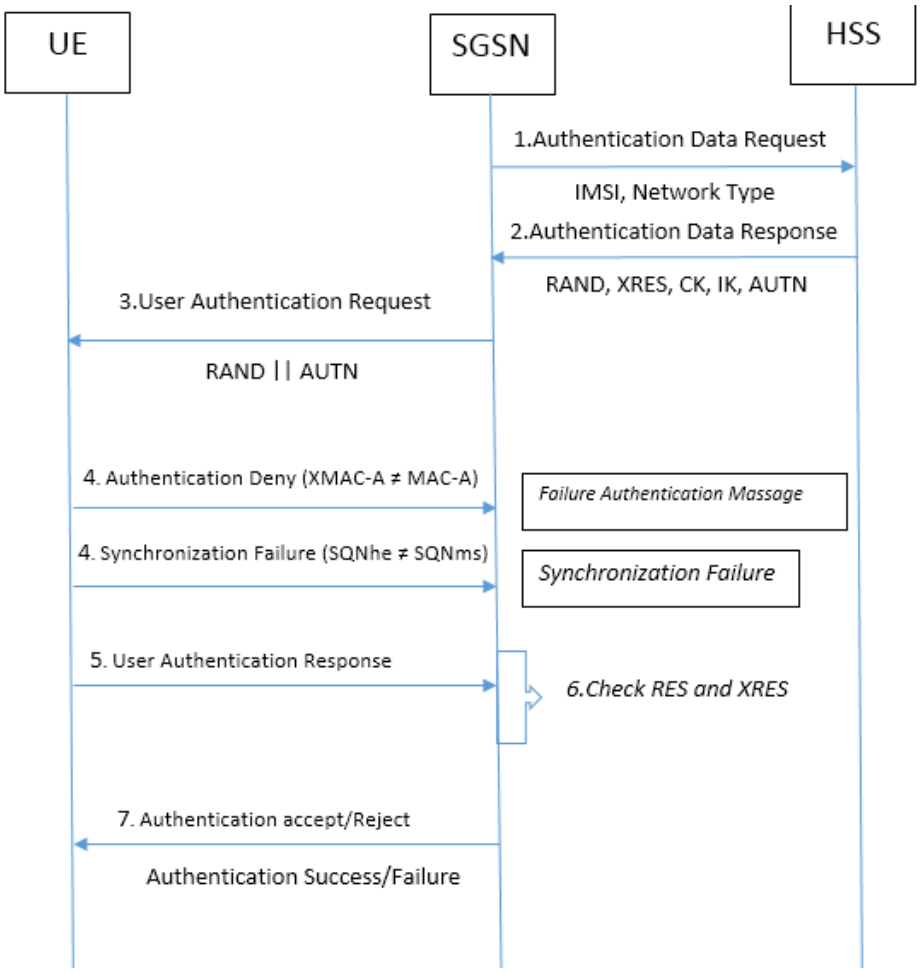


Figura 2-19 Autenticación 3G

Elaborado por: Autor

1. El SGSN inicia el procedimiento de autenticación requiriendo nuevos vectores enviando el mensaje *Authentication Data Request* al HSS en el que debe incluir el IMSI y el tipo de requerimiento si es para el dominio CS o PS.
2. Después de recibir el requerimiento desde el SGSN el HSS calcula los AV (RAND, XRES, CK, IK, AUTN) con el proceso descrito en (titulo 2.8.2 y figura 2.14) y se los envía al SGSN en el mensaje *Authentication Data Response.*
3. El SGSN inicia el proceso de autenticación con el UE con el mensaje *User Authentication Request* enviándole los parámetros RAND y AUTN, el propósito de este procedimiento es autenticar al usuario y establecer un

proceso de cifrado entre el SGSN y el UE. Como se lo describe en la figura 2.16

4. Después de recibir los parámetros RAND y AUTN el UE basado en AK recupera el valor de SQN enviado y calcula el valor de XMAC-A para compararlo con el parámetro MAC-A recibido en AUTN.
    - Si MAC-A y XMAC-A son diferentes se envía un mensaje de *Failure Authentication Massage* al SGSN con una identificación de la causa y que el UE abandono el proceso de autenticación así al notificarle al HSS se puede llevar un reporte de autenticaciones fallidas.
    - Luego basado en SQNms y SQNhe se verifica la validez de la red, chequeando si los valores recibidos de números de secuencia están dentro de los rangos correctos, si el UE considera que los valores de SQN no están dentro de los rangos correctos envía el mansaje *Synchronization Failure* al SGSN y el mensaje contiene el parámetro AUTS y se produce el proceso mostrado en el punto 2.8.3 figuras 2.17 y 2.18.
5. El UE calcula el parámetro RES basado en los valores recibidos de RAND y AUTN y luego lo envía al SGSN a través del mensaje *User Authentication Response.*
6. El SGSN compara el valor de RES recibido del UE con el valor de XRES calculado en el HSS.
    - Si los valores de RES y XRES no son los mismos el SGSN envía un mensaje al UE indicando que la autenticación fue rechazada, después de recibir el mensaje de rechazo el UE considera que el usuario no está autorizado y la autenticación es fallida.
    - Si los valores de RES y XRES si son los mismos indica que el UE si paso la autenticación. El SGSN envía un mensaje de respuesta al UE indicando que su requerimiento es aceptado.

3. CAPITULO III: Solución WiFi Offload

3.1 Introducción

Esta tesis direcciona a WiFi offload como una solución para el crecimiento del tráfico móvil de datos que continua evolucionando con el desarrollo de las redes UMTS y LTE, por lo que descargar tráfico Móvil a través de WiFi es considerada una alternativa tecnológica viable de acceso a redes EPC, puesto que existe un espectro WiFi sin licencias y gran cantidad de dispositivos compatibles de los que pueden hacer uso los operadores.

Wireless Fidelity (WiFi) es una tecnología inalámbrica de distancia corta que permite el acceso a internet, cumple con el estándar IEEE 802.11 y tiene como objetivo resolver grandes problemas de altos costos de implementación, siendo un medio eficaz para última milla. La IEEE permite servicios de red de área local a través del aire en su estándar 802.11, siendo un conjunto de parámetros para implementar un sistema LAN de comunicación inalámbrica WLAN en un espectro libre en las bandas de frecuencia 2.4, 3.6 y 5GHz.

El protocolo 802.11 a, g y n utilizan el esquema OFDM (*Orthogonal Frequency Division Multiplexing),* 802.11a y 802.11g trabajan en la frecuencia de 5 GHz y 2.4 GHZ respectivamente con una velocidad máxima de 54 Mbps, 802.11n trabaja en ambas frecuencias 2.4 o 5 GHz y a una velocidad máxima de datos de 600 Mbps (teórica), mientras que 802.11b usa el esquema DSSS (*Direct Sequence Spread Spectrum*) alcanza una velocidad de 11 Mbps, 802.11CA trabaja en la frecuencia de 5 GHz su señal es 256 QAM (*Quadrature amplitude modulation*) y alcanza una velocidad máxima de 1.3Gbps. Además 802.11n permite el uso de MIMO (*Multiple Input Multiple Output*), esta tecnología es usada para instalaciones internas y externas. Tanto WLANs, 3G y 4G son capaces de proporcionar conexiones *wireless* más veloces, WLAN puede cubrir solo áreas pequeñas debido a que opera con altas frecuencias y tiene poca penetración, pero provee una mejor transferencia de datos, un mecanismo que descargue datos de 3G/4G a WiFi es muy interesante para los operadores móviles que quieren balancear el costo de tráfico de datos y optimizar el uso de la red, la principal idea es que al tener un Access Point WLAN habilitado,

parte o la totalidad del tráfico sea enrutado a través de esa tecnología de acceso. La descarga debe ser controlada por el operador, por ejemplo el operador de la red móvil debe ser capaz de controlar que tipo de tráfico es enrutado a través de WLAN y cual se mantiene en 3G/4G. Se puede determinar que cierto flujo IP como por ejemplo VoIP se mantenga sobre 3G/4G para cumplir con los requerimientos QoS, mientras que flujos IP relacionados *streaming* sean descargados a WLAN.

Con la nueva generación de tecnología móvil LTE, las operadoras móviles cambian sus redes hacia la nueva generación All-IP (todo IP) eliminando las diferencias entre redes fijas y móviles conocido como FMC (*Fixed Mobile Convergence*), y así un dispositivo móvil pueda interactuar entre redes locales como WiFi y redes Wide-área como una red celular.

3.2 WiFi Offloading

Es un dominio de negocios emergente que promete ser la evolución del tráfico datos móvil combinando diferentes tecnologías de acceso ya existentes, acoplando las redes de acceso celulares 3GPP como son UMTS y LTE con la red de acceso no 3GPP como es WiFi al ser una tecnología de WLAN. Como resultado de esta evolución las nuevas generaciones de dispositivos móviles son integradas con múltiples interfaces de redes y así los usuarios puedan disfrutar de conexión a internet en todo momento y diferentes lugares. WiFi Offload ofrece mejorar la experiencia de navegación de usuarios 3G al tener velocidades de descarga iguales e incluso mejores que LTE y para usuarios 4G les ofrece navegar en internet a velocidades similares o superiores a LTE pero a un menor costo.
Existen dos maneras diferentes de interacción entre una red de acceso no 3GPP y el core EPC 3GPP, ya sea como un acceso no confiable (*Untrusted*) o como uno de confianza (*Trusted*). Los estándares 3GPP que definen la migración de WLAN y redes GPRS, UMTS y EPS:

- A partir del Release 6 3GPP TS 23.234 del 2004 describe por primera vez un acceso WLAN untrusted sobre una red GPRS y UMTS con la tecnología denominada I-WLAN, que ofrecía servicios PS con autenticación, políticas de facturación y seguridad unificada.

- En el Release 8 3GPP TS 23.402 del 2007 se describe un acceso WLAN untrusted a la red EPC. En el mismo Release 8 pero TS 23.327 del año 2008 ya se estandarizaba movilidad sobre servicio entre redes 3GPP-WLAN untrusted y se daban estudios sobre servicio continuo entre ambas tecnologías.
- En el Release 10 3GPP TS 23.261 del año 2011 se incluyen conceptos como IFOM (*IP Flow Mobility and Seamless WLAN offload*) para ofrecer un servicio continuo y descargas de tráfico dinámicos, hasta el momento cuando el UE detecta la presencia de una red de acceso alternar como WiFi AP (*Access Point*) termina el radio bearer que tiene con red de acceso 3GPP e inicia una nueva conexión a través de un acceso WLAN, como no hay interacción el usuario pierde la sesión activa y restablece otra. IFOM proporciona una conexión simultánea a las 2 alternativas de redes de acceso e intercambiar diferentes flujos IP pertenecientes a la misma conexión PDN como se ve en la figura 3.1. Otro concepto que se incluye es de MAPCON (Multi Access PDN Connectivity) esto quiere decir que un UE soporta acceso a múltiples PDNs, cuando el UE está conectado a través de una red de acceso 3GPP y una no 3GPP es controlado por el mismo core UMTS o EPC y puede acceder a diferentes PDNs.
- En el Release 11 3GPP TS 23.402 del año 2012 se incluyen los avances sobre SaMOG (*S2a Mobility based On GTP)* para acceso WLAN confiable o trusted a la red EPC sobre GTP. Soporta BBAI (*Broadband Forum Access Interworking*) y LOBSTER (*Location-Based Selection of gateways for WLAN*).
- En el Release 12 se especifican mejoras en SaMOG sobre el acceso confiable WLAN a redes EPC, se analiza el impacto de SaMOG en los UE. Estudios sobre la interacción radio WLAN/3GPP.

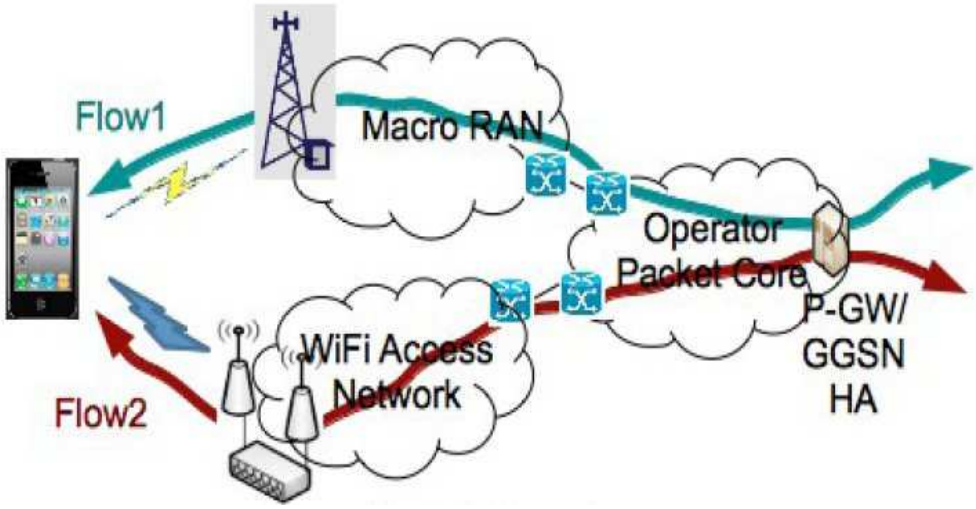


Figura 3-1 Enrutamiento de diferentes Flujos IP a través de diferentes redes de acceso

Fuente: (3g4g, 2010)

3.3 Movilidad y servicio continuo

EL principal objetico de EPC es proveer un servicio de internet continuo e ininterrumpido para dispositivos móviles con capacidad para múltiples tecnologías de acceso que les permita moverse de una red a otra garantizando que la transmisión de paquetes no se pierda y así poder soportar aplicaciones en tiempo real. Esto se puede conseguir conservando la dirección IP original, los 2 esquemas utilizados para conseguirlo son:

- Protocolos de movilidad basados en host HBM (Host Based Mobility) son los protocolos MIP (Mobile IP) tanto para IPv4 e IPv6 y DSMIPv6 (*Dual Stack Mobile IPv6*) , estos protocolos tiene como característica gestionar la movilidad a través del dispositivo móvil el cual tendrá la necesidad de actualizar la posición de su ubicación en la red mediante señalización con el core. Esta señalización en el proceso de actualización o handover genera un aumento en la señalización de la red provocando un problema de alta latencia para las aplicaciones de tiempo real.
- Protocolos de movilidad basados en red NBM (Netrwork Base Mobility) son los protocolo GTP y PMIP (Proxy Mobile IP) tanto para IPv4 e IPv6, este esquema permite gestionar movilidad y conservar la IP sin involucrar

al dispositivo móvil y así reduciendo tráfico de señalización en la movilidad y handover entre diferentes tecnologías de acceso. (3GPP R11 - TS 23.402 2012)

Cuando se utiliza el mecanismo NBM para establecer conexión con una red de acceso no 3GPP durante la movilidad del UE y con conservación de la IP para tener un servicio continuo, basándose en la información de la capacidad que tiene el UE para soportar NBM esta información es entregada de forma explícita por el UE a la Red. HBM puede tomar lugar si la red conoce la capacidad del UE para soportar ya sea el protocolo DSMIPv6 o MIP, esa información puede ser indicada desde el HSS/AAA a la red de acceso no 3GPP o de manera explícita del UE al core.

Cuando el objetivo de un UE es un acceso no 3GPP trusted o untrusted se le provee una nueva dirección IP local para acceder a la red si se selecciona el protocolo DSMIPv6, en ese caso para preservar la IP para una sesión continua. Esta dirección IP debe ser usada como un CoA (Care of Address) para DSMIPv6 sobre la interfaz S2c. Si el protocolo de gestión de movilidad seleccionado es MIPv4 la dirección provista al UE la red de acceso no 3GPP es una FACoA (Foreign Agent Care-of Address) y la IP se mantiene desarrollando el procedimiento MIPv4 FACoA sobre la interfaz S2a. Al seleccionar el protocolo basado en red PMIP para un acceso no 3GPP trusted lo hace sobre la interfaz S2a y para un acceso no 3GPP untrusted sobre la interfaz S2b. (3GPP R11 - TS 23.402 2012)

La selección del mecanismo de movilidad es desarrollada en los siguientes escenarios:

- En el proceso de attach inicial ya sea a una red no 3GPP en modo trusted o untrusted, la selección se desarrolla para decidir cómo establecer la conectividad IP para el UE.
- En el proceso de handover de una red de acceso 3GPP a una red de acceso no 3GPP, se desarrolla la selección del mecanismo de movilidad para establecer la conexión IP para el usuario.
- En el proceso de cambio entre dos redes de acceso no 3GPP si utilizan un protocolo basado en red.

El protocolo de movilidad IP que se utilizara para el attach inicial o para el handover se determina en el proceso de autenticación del UE.(3GPP R11 - TS 23.402 2012:11)

3.4 Redes de acceso Trusted y Untrusted

Para poder tener acceso a internar móvil 3GPP a través de una red de acceso WiFi no 3 GPP. El estándar 3GPP define dos tipos de acceso no 3GPP: Trusted (confiable) y Untrusted (no confiable) son redes de acceso IP que usan tecnología cuyas especificaciones están fuera del alcance de 3GPP. Si una red de acceso no 3GPP es considerada confiable o no confiable, no depende de la características de la red de acceso, es una decisión del operador terminar cuál de los dos utilizar.

3.4.1 Acceso WiFi 3GPP Untrusted

En el modo de acceso Untrusted la autenticación no es obligatorio y para que una red de acceso WLAN untrusted pueda interactuar con el Core móvil es necesario un equipo denominado ePDG (Evolved Pacjet Data Gateway) es un equipo de borde sobre el core que permite establecer un camino de comunicación entre una de acceso no 3GPP con el core móvil 3GPP este camino es un túnel IPSec. Es conocido que este modelo de acceso no ofrece suficiente seguridad como autenticación y encriptar la señalización.

3.4.2 Acceso WiFi 3GPP Trusted

Un acceso trusted o confiable debe cumplir parámetros de seguridad mínimos establecidos por el operador, es obligatorio en este tipo de acceso que los UEs sean autenticados a través de la SIM/USIM y la señalización entre la red de acceso y el Core móvil sea encriptado. 3GPP especifica que un acceso trusted WLAN se debe aplicar solo en redes que soporten autenticación EAP-SIM/EAP-AKA y debe utilizar los protocolos Diameter/Radius (*Remote Authentication Dial In User Service*), para la comunicación con el servidor AAA y HSS/HLR. Por lo tanto un acceso trusted no es posible con dispositivos móviles sin tecnología SIMs cards o USIMs cards.

Con la tecnología SaMOG utilizada para acceso WLAN trusted en la que se tiene movilidad basada en el protocolo GTP sobre la interfaz S2a introducido a partir del Release 11 3GPP, no es necesario establecer túneles IPsec con el UE. La autenticación la hace utilizando EAP y el proceso de encriptar es bajo el estándar 802.11i para WiFi, remplazando la función que tenía IPsec. Autenticación EAP soporta EAP-AKA y EAP-AKA´ que son utilizados para usuarios con tarjetas USIM para poder acceder al dominio de servicio PS a través de WLAN, esta autenticación registra en las USIM y en el HSS las KI o llaves de encriptación, para que sean utilizadas en cada proceso de autenticación necesario en la seguridad de la red y del usuario.

A WLAN trusted access network consiste de los siguientes módulos de funciones:

- AN (*WLAN Access Network*): incluye uno o más AP (*Access Points*) y el AC/BRAS (*Access Controller / broadband remote access server*).
- TWAP (*Trusted WLAN AAA Peer*): reenviar mensajes entre WLAN AN y el servidor AAA a través de la interfaz STa.
- TWAG (*Trusted WLAN Access Gateway*): Usa la interfaz S2a para conectar a la red EPC.

En esta tesis utilizaremos el equipo Huawei TGW (*Trusted Gateway*) que desarrolla las funciones de TWAG y TWAP, otros proveedores como Cisco tienen equipos separados para cada función.

3.5 Descubrir y seleccionar una red de Acceso

Cuando un usuario se registra en red propia o Home PLMN y tiene habilitado para conectarse al core móvil PS ya sea por una red de acceso 3GPP o no 3GPP, es necesario que el core le provea asistencia basado en reglas y políticas para poder determinar qué tipo de tecnología de acceso utilizar, esta asistencia se la obtiene a través de una funcionalidad conocida como ANDSF (*Access Network Discovery and Selection Function).* EL ANDSF es una nueva entidad EPC, con funciones de gestión y control de datos que proporciona asistencia al UE para escanear redes de acceso dentro de la vecindad del UE, seleccionar una red habilitada en el HPLMN y handover según las políticas del operador.

Debido a la movilidad que tienen los terminales dentro de una red heterogénea, constantemente el dispositivo está escaneando otros nodos de acceso disponibles ya sean de la misma tecnología de radio o diferentes dentro de la vecindad del UE la información del escaneo que incluye calidad de la señal y cobertura del nodo al que en ese momento está enganchado y la cobertura y señal de los nodos vecinos son enviadas al core móvil para que el operador pueda tomar la decisión basado en los umbrales configurados y así mantener al UE dentro de esa área de servicio o cambiarlo ya sea de nodo o de tecnología. Cuando un terminal está usando una tecnología de acceso 3GPP como 2G, 3G o 4G necesita descubrir cuando una red de acceso no 3GPP esté disponible para poder realizar un handover y descargar los datos a través de WiFi si esta tecnología esta predefinida como primera prioridad del usuario este cambio se lo realiza basado en las políticas del operador o en el caso que la señal de radio de un nodo 3GPP se esté degradando y la señal de WiFi sea mejor, esta movilidad entre sistemas o tecnologías debe ser sin que el usuario perciba el cambio y no pierda servicio ni continuidad. Cada celda o nodo debe estar dentro de una lista de difusión, esta lista de difusión puede incluir celdas con la misma tecnología de radio dentro de un área específica para poder hacer handover, cada nodo declara dentro de sus datos los nodos vecinos a los que un UE puede realizar handover.(3GPP R11 - TS 23.402 2012)

La interacción entre el UE y el ANDSF para requerimientos directos lo hace a través de la interfaz S14 sobre tecnologías de acceso 3GPP o no 3GPP como se puede apreciar en la figura 3.2, esta interfaz permite proporcionar información de forma dinámica al UE para el proceso de descubrir y seleccionar una red para ambas tecnologías. Esta asistencia es proporcionada solo si la comunicación es establecida de forma segura como se especifica en el documento 3GPP TS 33.402, esta información proporcionada dinámicamente es soportada vía Pull (el UE inicia la sesión) o vía Push (el ANDSF inicia la sesión). La red EPS permite al operador influenciar al UE a realizar handover en la red de acceso si está en modo ACTIVO/CONNECTED o hacer una reelección si está en modo IDLE.

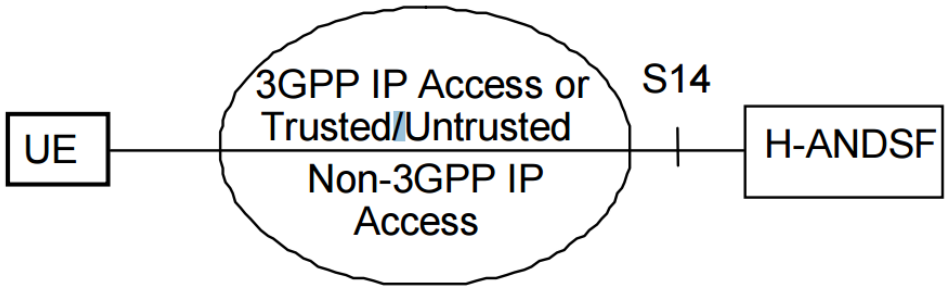


Figura 3-2 Arquitectura No Roaming para ANDSF

Fuente: (3GPP, 2015)

El dispositivo móvil puede escanear o descubrir redes de acceso (celdas o nodos) dentro de su vecindad de la manera más simple sin la asistencia de la red, esto lo hace periódicamente escaneando redes acceso disponibles sin requerir modificaciones en la red, pero presenta varios problemas como:

- El consumo de la batería aumenta considerablemente y más cuando requiere un escaneo de redes de alta velocidad.
- La información que recibe de los nodos de acceso es limitada.
- El dispositivo necesita tener dos receptores trabajando en paralelo uno para explorar o escanear nuevas redes y otro para las comunicaciones en curso.

Estos problemas impulsan la necesidad que la red asista el UE con el proceso de descubrir y seleccionar la mejor opción de red de acceso, porque ANDSF provee ventajas o beneficios como construir dinámicamente una base de datos con la función de guardar información dentro de un repositorio, determina qué tipo de información es necesaria recolectar y proveer al UE e incluso indica si la información proporcionada es válida o no.

El ANDSF incluye las siguientes tres categorías para proporcionar información de las redes de acceso al UE basados en la configuración del operador:

- ISMP (*Inter-System Mobility Policy*)

  ISMP es un conjunto de reglas y preferencias definidas por el operador para un UE con solo una conexión red de acceso activa ya sea UMTS/LTE o WiFi. Esto

quiere decir que el UE usa ISMP cuando puede enrutar trafico IP solo sobre una interfaz de radio en un determinado tiempo (no soporta IFOM o esta deshabilitado). En este caso ANDSF es capaz de transmitir indicaciones de Handover para preparar la ejecución del mismo, optimizando el procedimiento con la reducción del tiempo ya que conoce la red de origen y la red de destino del UE. La información que provee el ANDSF contiene políticas de movilidad entre sistemas ISMP y datos específicos de redes de acceso para asistir al dispositivo móvil con la decisión para realizar handover entre sistemas, por ejemplo ISMP puede indicar que es preferible seleccionar WLAN en lugar de UTRAN para acceder a EPS. ISMP se lo aprovisiona en el UE y puede ser actualizado por el ANDSF.

- ISRP (*Inter-System Routing Policy*)

ISRP es un conjunto de reglas definidas por el operador que determinan como el UE debe enrutar el trafico IP a través de múltiples interfaces de acceso de radio. El UE usa las reglas ISRP cuando puede enrutar trafico IP simultáneamente a través de múltiples interfaces de acceso de radio por ejemplo cuando IFOM o MAPCOM están habilitados. El propósito de estas reglas es decidir cuándo un tipo de tecnología de acceso de red es restringido para un específico flujo de tráfico IP o especifico APN o que tipo tecnología de acceso selecciona basada en el APN, flujo de IP o una aplicación específica.

- *Access Network Discovery Information*

  Luego que el UE hace una petición de request, el ANDSF puede proveer una lista de redes accesos disponibles en la vecindad del UE, la redes disponibles se determinan según la potencia mínima requerida por el UE en un área determinada. Dentro de la información específica que se le entrega al UE está el SSID (*Service Set Identifier*) en el caso de WLAN y para tecnologías de acceso 3GPP el Routing Area, tracking Área o Cell ID.

Para poder descubrir o llegar al ANDSF dentro de la red en un escenario de no Roaming, el H-ANDSF (*Home Access Network Discovery and Selection Function*)

es descubierto a través del DNS o a través de la función de un servidor DHCP para que le entregue la dirección IP del H-ANDSF al UE. (3GPP R11 - TS 23.402 2012)

3.6 Policy & Charging Control (PCC)

Los operadores móviles necesitan aplicar políticas de facturación y control, el operador puede desarrollar un control del tráfico de datos de los usuarios ya sea en términos de calidad de servicio (QoS) asignando un QCI o controlar consumos de los usuarios creando políticas, toma decisiones basado en políticas diferenciadas de cobro y asignación de ancho de banda por usuario o un grupo de usuarios, puede aumentar o disminuir el ancho de banda, limitar el acceso a ciertos sitios web bloqueando el acceso o re-direccionando a páginas de advertencia. El GGSN/PGW soporta la arquitectura PCC, en la interfaz S5 ya sea con el protocolo GTP o PMIP. Esta arquitectura PCC está conformada por el PCRF (*Policy and Charging Rules Function)* el PCEF (*Policy and Charging Enforcement Function*) y la OCS. WiFi Offload permite unificar este servicio a los usuarios que acceden a los servicios PS 3GPP a través de una red de acceso no 3GPP.

3.6.1 PCEF

El PCEF es el encargado de aplicar las políticas que se crean en el PCRF, antes que se apliquen las políticas el PCEF primero analiza mediante su función de DPI (*Deep Packet Inspection)* los paquetes de datos de sus interfaces, identifica que tipo de protocolo es y el origen de los paquetes (cliente que origina el tráfico). Asegura que los paquetes que son descartados como resultado de la aplicación de políticas son sean cobrados. El PCEF se conecta al PGW a través de radius, al PCRF a través de la interfaz lógica Gx y a la OCS a través de la interfaz lógica Gy.
El PCEF puede soportar diferentes tipos de políticas. De las principales se tiene:

- Charging: cuando se debe aplicar este tipo de política, al recibir la orden de hacer la consulta al OCS (usuarios prepago) o enviar los CDRs al CG (usuarios pospago).
- QoS: aplicación de la política para controlar el tráfico incrementando o disminuyendo el ancho de banda total o por flujos de tráfico específicos para

el usuario. Es posible administrar el consumo de ancho de banda al definir rangos de tiempos, el operador puede considerar que en horas pico a ciertos usuarios o ciertas localidades su consumo de ancho de banda tenga ciertas limitaciones.

- Access Control: limitar el acceso a ciertos sitios web bloqueando o re-direccionando los requests hacia páginas de advertencia. En este caso se puede negar el acceso a ciertas páginas de contenido de adultos para móviles que sean utilizados por menores de edad, limitar a ciertos usuarios que solo tengan acceso a redes sociales y no a ningún otro tipo de servicio cuando su crédito se acabe.
- FUP (*Fair Use Policy):* el PCRF lleva el conteo de una cuota en MB del consumo del servicio para cada usuario y envía diferentes políticas al llegar a niveles o al cumplirse la cuota mensual, siempre requiere la comunicación con el PCRF mediante el protocolo DIAMETER para informar de los consumos de ancho de banda realizados.

Es posible optimizar el ancho de banda, diferenciar paquetes de servicios, analizar tráfico, llevar un control de la conducta de consumos de un usuario o un grupo de usuarios. Implementa la función de SA (*Service Awareness*) como se muestra en la figura 3.3 que ayuda al operador identificar y diferenciar entre los requerimientos de servicio de los usuarios desarrollando las siguientes operaciones:

- Análisis de servicio: esta función proporciona información detallada y precisa del tráfico de datos al que el usuario está accediendo y lo clasifica basado en contenidos y puede ser cobrado a los subscriptores en diferentes tarifas. El requerimiento de servicio solicitado por el usuario puede identificado por información de capa 3 o capa 4 ya sea la dirección IP, Puerto o tipo de protocolo TCP, UDP, IPsec, etc. También en las capas superiores ya sea a través del URL, protocolo de aplicación como HTTP, WAP, DNS, etc. La librería de protocolos se definen en 3 niveles: Categoría, Protocolo y Sub-protocolo algunos ejemplos se pueden ver en la tabla 3.1.
- Control de servicio: basado en la inspección profunda de paquetes el operador lo clasifica dentro de una variedad de paquetes de servicio por

ejemplo el tráfico de redes sociales puede ser considerado en una tarifa 0 o que no se facture mientras que navegar en internet a través de browser o ver películas online si tengan una tarifa.

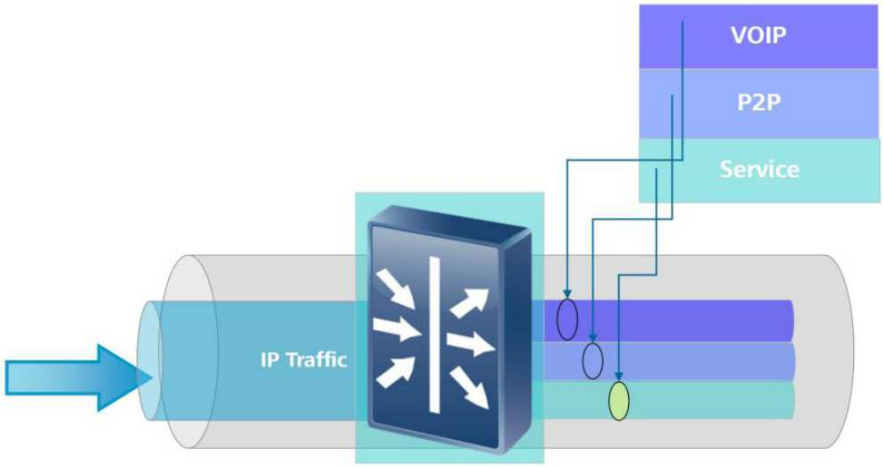


Figura 3-3 Service Awareness

Fuente: (Huawei, 2016)

Tabla 3-1 Protocolos y categorías

Categoría	Protocolo	Sub-protocolo
Web Browsing	HTTP	HTTP
	HTTPS	HTTPS
	WAP1	WAP1
Email	SMTP	Hotmail
	IMAP	IMAP
	MS_Exchange_Mailing_Protocols	NSPI
P2P	Bittorrent	BitTorrent_Data_TCP
	eDonkey_eDonkey2000	eDonkey_Detect_Function
VoIP	Skype_VoIP	Skype_PctoPhone
	GoogleTalk_VoIP	GoogleTalk_AudioData
	SIP	SIP_Control
Streaming	RTSP	RTSP_Control
	Microsoft_Media_Server	MMSP_Control_Data
	RealPlayer	RealPlayer_Stream

Elaborado por: Autor

3.6.2 PCRF

Es la plataforma encargada de crear las reglas de políticas de control y cobro por el uso de la red para cada usuario o grupo de usuarios que serán aplicadas por el PCEF, la interacción en el PCEF y PCRF es a través de la interfaz Gx usando el protocolo Diameter, que le permite al operador desarrollar un control dinámico de políticas de control y facturación estableciendo sesiones IP-CAN (*IP Connectivity Access Network*) ya sea para cualquier clase de 3GPP IP-CAN o acceso no 3GPP (UTRAN, EUTRAN o WLAN). Según la información proporcionada por el PCEF (Tipo de requerimiento inicio, modificación, fin, etc o tipo de IP-CAN) el PCRF toma la decisión de asignar una regla PCC específica a un usuario.

Dentro de las funcionalidades del PCRF podemos mencionar las políticas de tarifación clasificando a los subscriptores en postpago o prepago, el control de políticas basado en APN, grupo de subscriptores, utilización de servicios, localización del usuario, tipo de acceso a la red, etc.

Una regla está formada por: una condición, un objeto y una función. Una regla define como implementar una función específica sobre un objeto específico bajo una específica condición.

Dentro de los objetos podemos mencionar: URL, Socket, Browser Type, P2P service, las condiciones pueden ser: MSISDN, User Status, Date y las funciones: control de ancho de banda, notificaciones, comprimir textos etc. Un ejemplo podría ser que una condición de rango de MSISDN se le aplique la función de limitar el ancho de banda a 512 Kbps en un objeto ya sea cuando acceda a un servicio P2P.

3.6.3 Flujo de mensajes sobre la interfaz Gx

Cuando un usuario quiere acceder a internet por ejemplo visitar una página web el primer paso es que debe estar online, por lo que el usuario envía un requerimiento de activación de PDP CTX al PGW y el PGW envía un IP-CAN *Establish request* al PCEF que en este caso sería un *accounting start,* cuando ya no quiere seguir en la página web debe pasar a estado offline y se envía un requerimiento de desactivación de PDP CTX al PGW y el PGW envía al PCEF un IP-CAN *termination Request* un *accounting stop*. En la comunicación entre el PCEF y el PCRF se utilizan los mensajes diameter de control de crédito:

- CCRI (*Credit Control Request Initial)*, encargados de iniciar una sesión de control de crédito.
- CCAI (*Credit Control Answer Initial*) mensaje de respuesta al CCRI.
- CCRT (*Credit Control Request Terminate)*, encargada de finalizar la sesión establecida de control de crédito.
- CCRU (*Credit Control Request Update)*, contiene información para una sesión de control de crédito existente, son enviadas todo el tiempo para determinar el la asignación de cuota.

El flujo de mensajes diameter en la interfaz Gx la podemos apreciar en la figura 3.4.

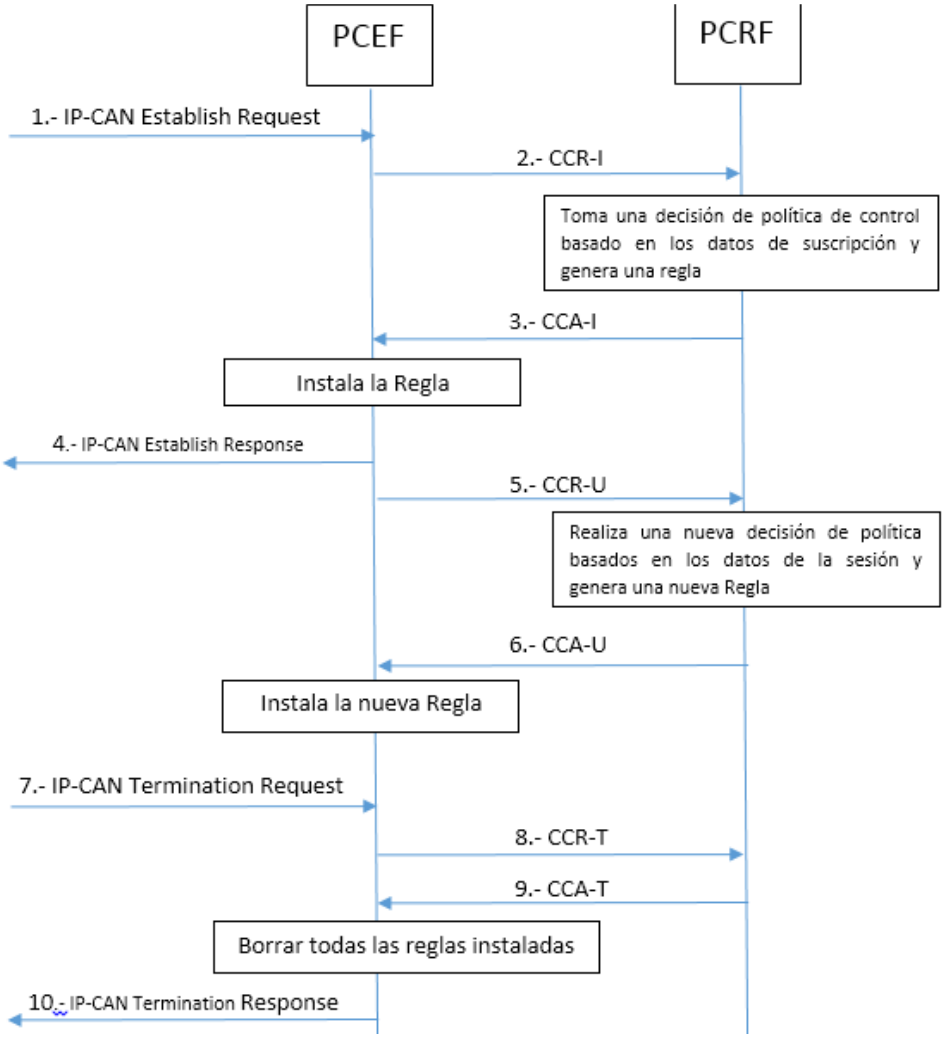


Figura 3-4 Flujo de mensajes en la interfaz Gx

Elaborado por: Autor

3.7 Elementos de red requeridos para una red WiFi Offload

Dentro de los elementos de red que se necesitan para poder acoplar una red WLAN a un core de datos móviles en modo confiable o trusted se tiene para WLAN AN el AP (*Access Point*) y AC/ BRAS (*Access Controller / broadband remote access server*) para el core un servidor Radius AAA y TGW.

Cada proveedor maneja sus propia tecnología por lo que se han establecido requisitos básicos que deben cumplir los equipos para que puedan interactuar usuarios móviles a través de una red de acceso WLAN.

3.7.1 UE

El equipo móvil y su USIM necesario para acceder a la red PS a través de una red acceso WLAN debe cumplir con los siguientes requisitos:

- Soportar Autenticación EAP SIM y EAP AKA.
- Interfaz para conexiones a WLANs
- Soportar protocolo de autenticación protegido PEAP (*Protected Extensible Authentication Protocol*).
- Soportar autenticación por portal en caso de ser requerido.
- Soportar autenticación por MAC
- Funciona como el cliente DHCP y obtiene las direcciones IP desde las redes WLAN utilizando la negociación DHCP.
- Operar en los estándares IEEE 802.11 a/b/g/n/ac.
- Soportar las frecuencias de operación Wi-Fi 2.4 GHz y/o 5 GHz, o ambas.
- Soportar los protocolos de seguridad Wi-Fi WPA2-Personal y WPA2-Enterprise.
- Soportar el modo de operación Dual Network, tanto para redes móviles celulares y redes Wi-Fi.
- Soportar mecanismos de handover entre redes 3GPP y redes Wi-Fi basados en ANDSF.
- Soportar los protocolos IPv4 e IPv6.

- Soportar WiFi Offload en base a los estándares 3GPP TS 24.312, TS 23.402, TS 31.102, TS 23.234, TS 23.261.

3.7.2 WLAN AN

Dentro de la red de acceso WLAN están los Access Point que son los encardados de convertir la señal de cable en señal de radio para proveer acceso WLAN, deben considerarse la frecuencia a la que trabaje según el estándar y si son para ambientes internos o externos; el tipo de Access Controller es el encargado de controlar y gestionar los APs de las WLANs interactúa con el servidor de autenticación para la seguridad de los subscritores WLAN, determinar qué tipo de AC utilizar dependerá de la cantidad de APs que maneje, dentro de los requisitos principales para WLAN AN se tiene:

- Soporta autenticación EAP-SIM / EAP-AKA.
- Soporta autenticación PEAP.
- Soporta autenticación por portal.
- Funciona como cliente RADIUS, encriptación de mensajes EAP o mensajes de autenticación por portal en mensajes RADIUS, y transmite los mensajes RADIUS al servidor AAA.
- Soporta facturación para los suscriptores WLAN.
- Soporta la asignación entre prioridad de usuario 802.11e/WMM y 802.1p/DSCP. (WMM (*Wi-Fi Multimedia*); DSCP (*Differentiated Services Code Point)*
- Soporta el método de establecimiento de un túnel SoftGRE de manera dinámica o estática y reenvío de paquetes de capa 2 a través del túnel SoftGRE en SoftGRE mode.
- Soporta reenvío de paquetes de servicios a través de un túnel GRE en modo IPoGRE (*IP sobre GRE*).
- Soporta el reenvío de paquetes de servicios Ethernet basados en etiquetas VLAN (*Virtual Local Area Network*).
- Asignación de dirección IP a usuarios WLAN.

3.7.3 Servidor AAA 3GPP

El servidor AAA es el encargado junto al HSS de la autenticación y autorización de los usuarios WLAN usa el protocolo Diameter y Radius para comunicación y debe cumplir los siguientes requisitos:

- Soporta autenticación EAP-SIM / EAP-AKA.
- Soporta autenticación PEAP.
- Soporta autenticación PORTAL.
- Soporta la interfaz D'/SWX y obtiene los datos de suscripción de los abonados que utilizan autenticación PEAP/MAC/ portal desde el HLR/HSS.
- Almacena y envía los datos de suscripción de servicios de red móvil.

3.7.4 TGW

El TGW funciona como un Trusted WLAN Gateway para proveer acceso a la red móvil para subscriptores que usan autenticación EAP-SIM/AKA, PEAP o por portal. El TGW es el responsable de enrutar los mensajes de autenticación hacia el Servidor AAA y de establecer el túnel GTP con el GGSN/PGW ya sea en la red propia o en usuarios roaming. Dentro de los requisitos se tiene:

- Soporta funciones de proxy RADIUS, transmite mensajes RADIUS entre el WLAN AN y el servidor 3GPP AAA.
- Soporta detección de link GTP.
- Soporta flujo de control basado en calidad de servicio (QoS), mapeo entre QoS y DSCP y DSCP re-marking en cabeceras IP de paquetes uplink GTP y paquetes downlink GRE.
- Configura la información de ubicación de abonado WLAN y lleva la información de ubicación de abonado WLAN en la información de ubicación de usuario ULI (*User Location Information*) incluido en un mensaje GTP activation request.
- Soporta asignación dinámica o estática de direcciones IP de la puerta de enlace predeterminada cuando el TGW interactúa con el P-GW en modo SoftGRE.

- Soporta método de establecimiento dinámico o estático para configurar un túnel SoftGRE y soporta el envío de paquetes de servicio Capa 2 a través de un túnel SoftGRE.
- Soporta reenvío de paquetes de servicios a través de un túnel GRE en modo IPoGRE.
- Soporta el envío de paquetes de servicios Ethernet basados en etiquetas VLAN.
- Posee funciones como servidor DHCP para procesar mensajes DHCP.
- Compatible con la traducción de direcciones de red NAT (*Network Address Translation*).

3.8 Tipos de Acceso WLAN trusted

El TGW es el punto de acceso unificado para los usuarios WLAN acceder al Core PS. Se pueden transmitir paquetes de capa 2 y capa 3, por lo tanto la comunicación entre la red de acceso WLAN y el TGW puede ser a través de un túnel IPoGRE (Capa 3), VLAN (Capa2) o SoftGRE (capa 2).

- IPoGRE utiliza el protocolo estandarizado GRE y provee encapsulación IP-in-IP, todos los paquetes IP enviados entre el WLAN AN y el TGW serán encapsulados en el protocolo GRE como se aprecia en la figura 3.6. En la figura 3.5 podemos ver 3 diferentes tipos de redes de acceso WLAN AN 1 con AP y AC, WLAN AN 2 incorpora un BRAS y WLAN AN 3 un FAT AP que integra en el mismo equipo AP y AC. En la figura 3.6 vemos el stack de protocolos para IPoGRE.

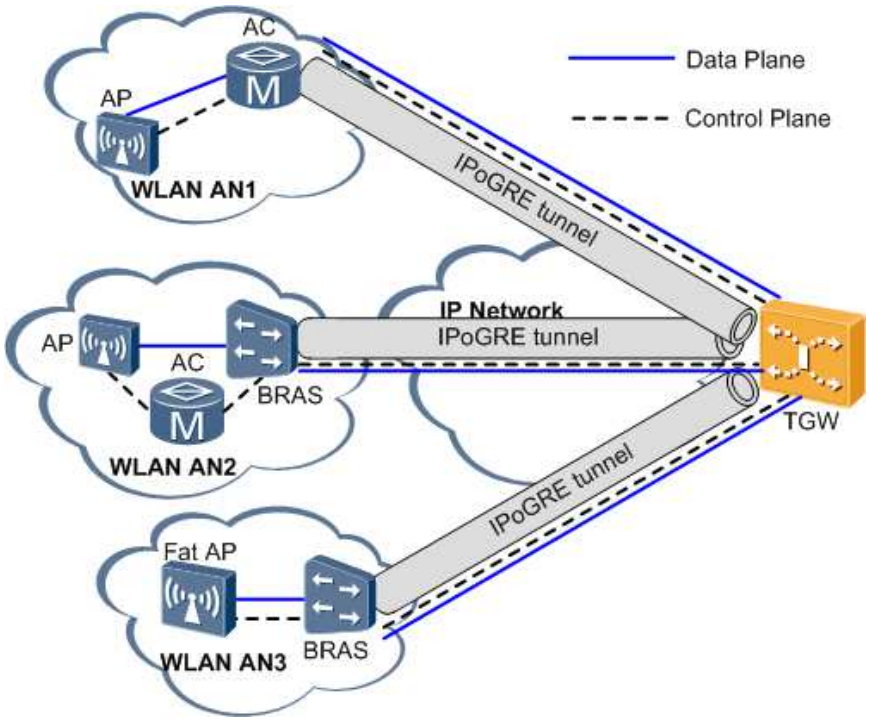


Figura 3-5 IPoGRE networkin mode

Fuente: (Huawei, WLAN Trusted Access, 2015)

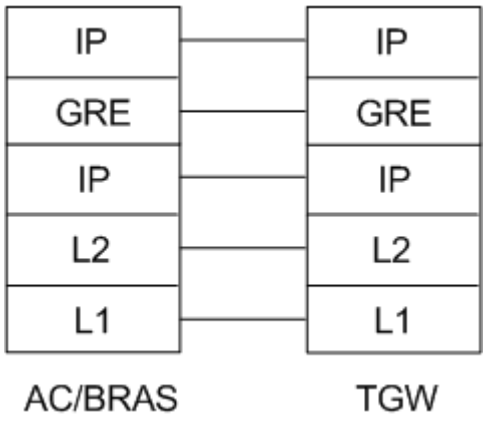


Figura 3-6 Stack de protocolos IPoGRE

Elaborada por: Autor

- SoftGRE Proporciona encapsulación Ethernet-in-IP, los paquetes Ethernet puede ser transmitidos sobre redes de capa 3 y tienen los diferentes tipos de redes de acceso como podemos ver en la figura 3.6. La WLAN AN1 basado en APs y AC establece un túnel SoftGRE entre el AC y el TGW para enviar paquetes de servicio Ethernet, WLAN AN2 también es basado en APs y AC pero el AP soporta envío directo de paquetes de servicio Ethernet a través del túnel SoftGRE y WLAN AN3 un FAT AP es desarrollado.

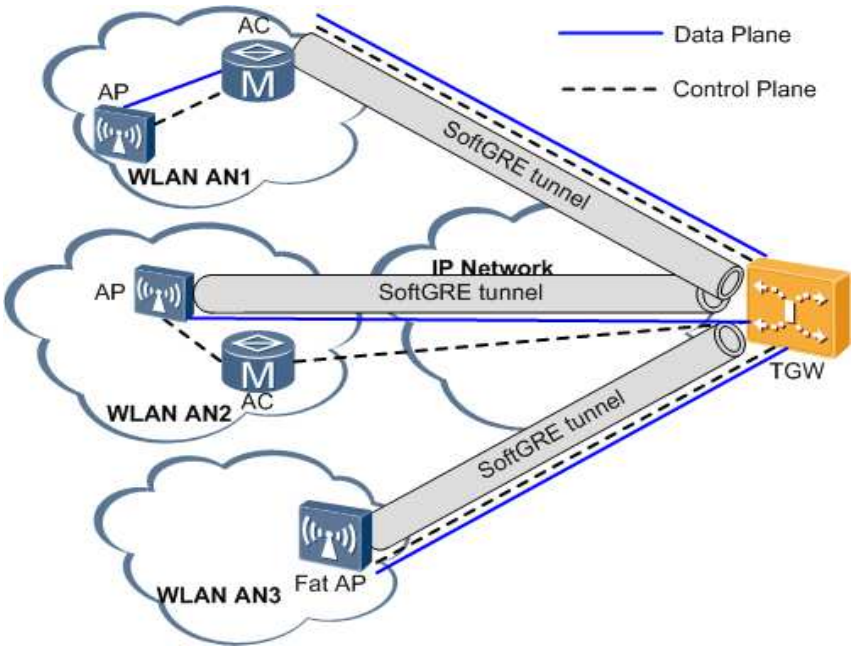


Figura 3-7: SoftGRE networkin mode

Fuente: (Huawei, WLAN Trusted Access, 2015)

- VLAN, los paquetes de servicios Ethernet son enviados basados a través del enlace capa 2 sobre VLAN tags y tiene los modos de acceso como se puede ver en la figura 3.7, WLAN AN1 el AC envía los paquetes de servicios con su respectiva VLAN, WLAN AN2 el AC soporta transmisión directa al TGW y el WLAN AN3 a través de FAT AP.

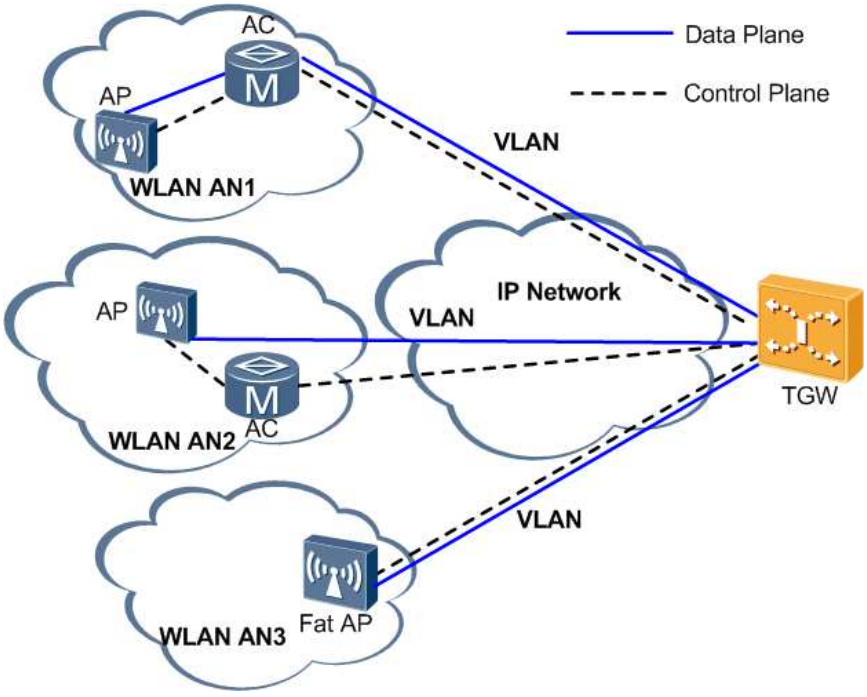


Figura 3-8: SoftGRE networkin mode

Fuente: (Huawei, WLAN Trusted Access, 2015)

3.9 Interfaces lógicas y protocolos para la solución Wifi Offload

Las principales interfaces que intervienen en la solución WiFi offload las podemos ver en la figura 3.8:

- **STa** interfaz que conecta el TGW y el Servidor AAA 3GPP es usada para transmitir autenticación de acceso, la autorización, parámetros de movilidad y la información relacionada con la carga en forma segura, es basado en Radius.
- **Wa** interfaz lógica que permite introducir el AC/BRAS al dominio PS a través de un camino o path lógico hasta el TGW
- **SWx** interfaz que conecta el servidor AAA 3GPP con el HSS y es utilizada para transporte de datos de autenticación, información del subscriptor y datos relacionados a las conexiones PDN es basado en el protocolo MAP. Para el proceso de autenticación Non-3GPP.
- **S2a** interfaz que conecta el TGW con el GGSN/PGW, encargada del plano de usuario relacionado con el control y soporte de movilidad está basado en el protocolo GTP o PMIP.
- **S2c** interfaz del túnel directo entre el GGSN/PGW y el UE para la transmisión de datos de usuario.
- **S6b** interfaz entre el GGSN/PGW y el servidor AAA es utilizada para movilidad relacionada con autenticación y autorización. También se puede utilizar para recuperar y solicitar parámetros de almacenamiento de movilidad

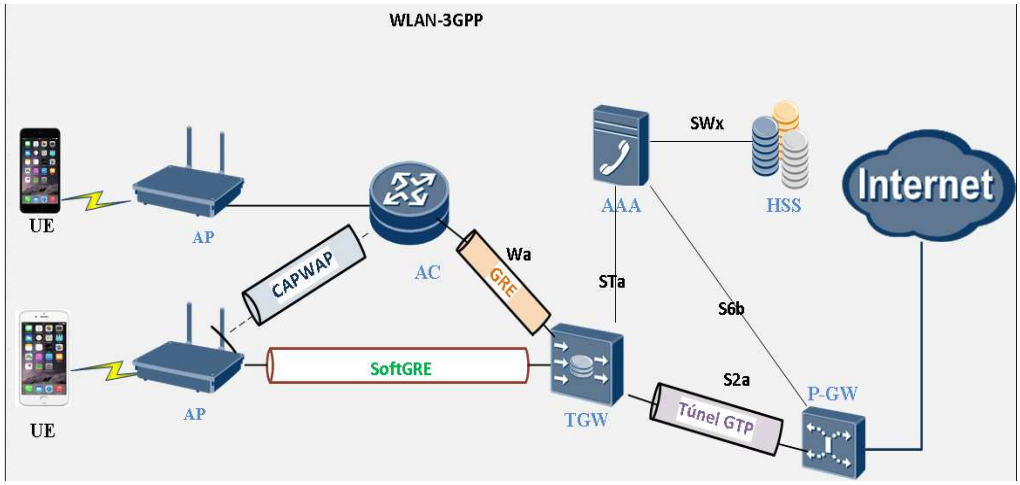


Figura 3-9 Principales interfaces solución WiFi Offload

Elaborado por: Autor

3.10 Autenticación EAP-AKA

Las características de EAP-AKA es permitir al Servidor AAA proveer acceso a los servicios del dominio PS del EPC a través de una red de acceso WLAN a los usuarios no 3GPP que utilizan USIMs, mejorando la seguridad de la red y previniendo ataques de redes no autorizadas, los equipos involucrados en el proceso de autenticación serian el UE, AC/BRAS, TGW, servidor AAA 3GPP y HSS. El AC/BRAS funciona como un cliente Radius, el TGW funciona como un proxy radius para retransmitir los paquetes radius de autenticación entre el AC y el Servidor AAA, el servidor AAA es el encargado de autenticar a los usuarios obteniendo la información de autenticación del subscriptor desde el HSS. Al utilizar este tipo de autenticación las llaves de encripción de cada usuario son aprovisionadas en las USIM y en el HSS para ser requeridas en el proceso de autenticación.

A continuación basada en la figura 3.10 se detalla el proceso de autenticación ya unificada para un usuario WLAN:

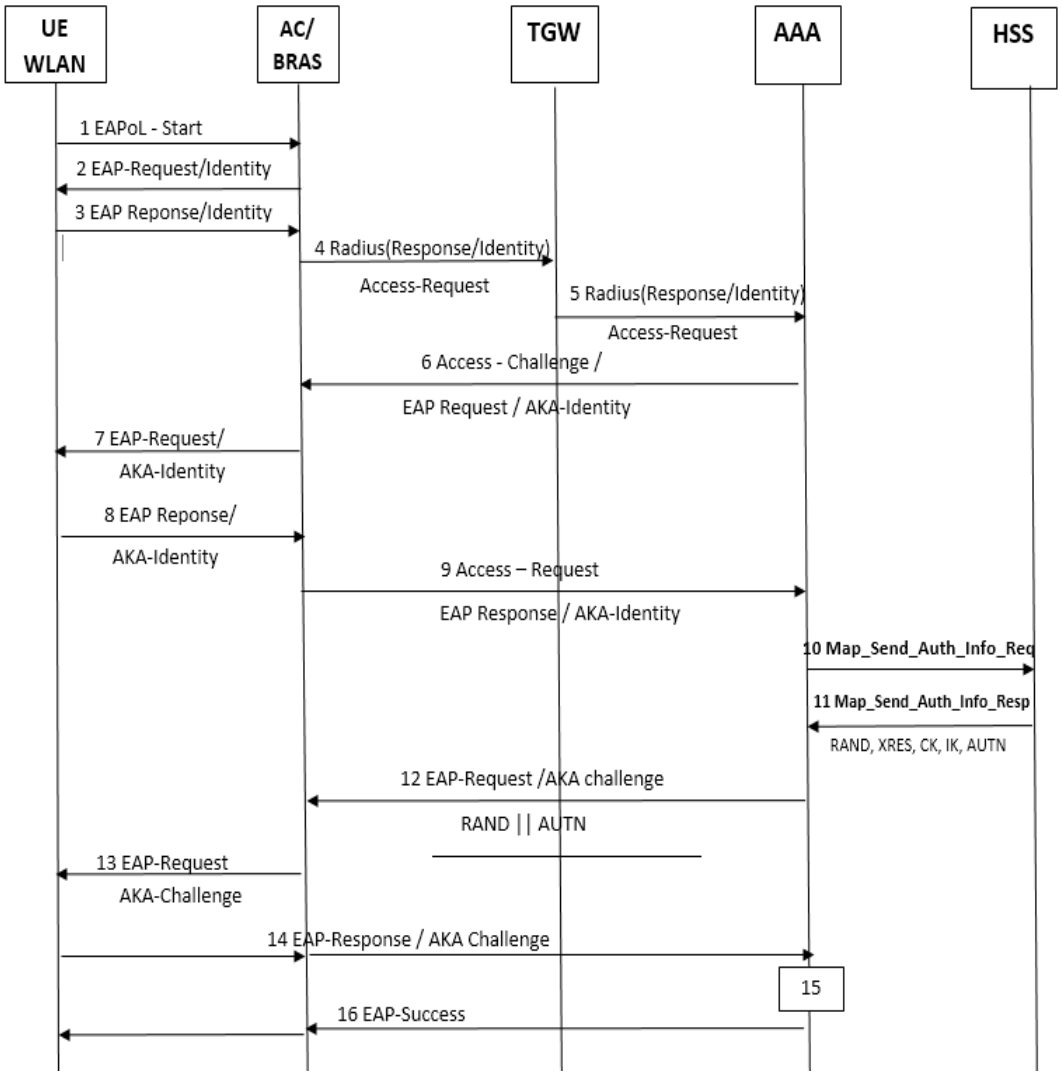


Figura 3-10 Procedimiento de autenticación EAP-AKA para usuarios WLAN

Elaborado por: Autor

1. Luego que el usuario establece una asociación con una red de acceso WLAN, el usuario WLAN envía al AC/BRAS un mensaje de requerimiento de autenticación EAPol-Start (Extensible Authentication Protocol over LAN) para poder acceder a la red EPC.
2. El AC/BRAS envía un mensaje EAP-Request/Identity al UE WLAN solicitando el identificador de acceso a la red NAI (Network Access Identifier)
3. EL UE lee el NAI de la USIM y envía un mensaje EAP Response/Identity al AC/BRAS, el mensaje lleva el NAI el cual puede ser seudónimo o un

permanente NAI. Si el usuario es autenticado por primera vez lleva el IMSI como NAI en el mensaje y el formato es 0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org, donde 0 indica autenticación EAP.

4. EL AC/BRAS encapsula el mensaje EAP Response/Identity en un mensaje Radius Access-Request, ubicando el NAI en el campo de nombre de usuario del mensaje radius con el formato NAI@domain, para luego ser entregado al TGW.
5. El TGW a través de función de Radius Proxy retransmite el mensaje al servidor 3GPP AAA.
6. EL AAA selecciona la Autenticación EAP-AKA, luego envía un mensaje Access-Challenge/EAP-Request/AKA-identinty hacia el AC/BRAS a través del TGW, solicitando identificación del subscriptor. El AAA verifica que el identificador del subscriptor es un NAI seudónimo e investiga en su base de datos para relacionarlo con el IMSI del usuario en caso que no logre relacionarlo será necesario enviar un mensaje EAP-Request/AKA-Identity para que el TGW lo encapsule en un mensaje radius Access Request y lo envíe al AC/BRAS requiriendo el *permanent* NAI, caso contrario si pudo ser relacionado va directo al punto 10.
7. El AC/BRAS envía el mensaje EAP-Request/AKA-Identity al UE WLAN.
8. EL UE envía un mensaje EAP-Response/AKA-Identity al AC/BRAS.
9. EL AC/BRAS envía el mensaje Access-Request/EAP-Response/AKA-identity hacia el servidor AAA a través del TGW.
10. EL servidor AAA identifica el Home HSS usando el IMSI y envía un mensaje MAP_SEND_AUTHENTICATION_INFO_Req solicitando al HSS los vectores de autenticación (Quintupletas).
11. EL HSS responde con un mensaje MAP_SEND_AUTH_INFO_Resp que incluyen los vectores de autenticación (RAND, XRES, CK, IK y AUTN) como se lo indico en el capítulo 2 según la figura 2.15.
12. El servidor AAA envía el mensaje EAP-Request/AKA Challenge que incluyen los parámetros RAND y AUTN hacia el AC/BRAS a través del TGW.

13. El AC/BRAS reenvía el mensaje EAP-Request/AKA Challenge al UE para iniciar el proceso de autenticación.
14. El UE calcula el parámetro RES basado en los valores recibidos de RAND y AUTN y luego lo envía al AC/BRAS para que lo encapsule y lo envíe al servidor AAA a través del mensaje EAP-Response/ AKA Challenge.
15. El Servidor AAA compara el valor de RES recibido del UE con el valor de XRES calculado en el HSS.
    - Si los valores de RES y XRES no son los mismos el servidor AAA envía un mensaje al UE indicando que la autenticación fue rechazada, después de recibir el mensaje de rechazo el UE considera que el usuario no está autorizado y la autenticación es fallida.
    - Si los valores de RES y XRES si son los mismos indica que el UE si paso la autenticación. El servidor AAA encapsula un mensaje de acceso aceptado en un mensaje Access-Accepted/EAP-Success enviado al AC/BRAS.
16. EL AC/BRAS envía un mensaje EAP-Success al UE indicando que la autenticación fue exitosa. A partir de ese momento el TGW puede iniciar el proceso de activar los contextos con el GGSN/PGW

3.11 Funciones elementales TGW

Dentro de las funciones elementales y básicas que realiza el TGW podemos mencionar la gestión de una sesión de usuario, la asignación de dirección IP al usuario

3.11.1 Gestión de sesiones

Esta característica del TGW permite establecer la conexión entre un usuario WLAN cuando quiere acceder a un PDN o internet y crear, actualizar y eliminar contextos PDP para los UEs WLAN.

Una sesión puede ser una conexión lógica usada para intercambiar datos entre dos nodos de la red, es usada para simplificar el tiempo de conexión. Los contextos PDP son habilitados sobre el TGW estos contextos almacenan información requerida para la transmisión de datos de usuario incluyendo direcciones de UE, TEIDs y

parámetros QoS. Los siguientes procesos de gestión de sesiones son usados para gestionar contextos PDP:

- Activación de contexto PDP, cuando un UE WLAN accede a la red EPS a través del TGW, este inicia el proceso de activación de PDP context estableciendo un canal virtual de datos entre el TGW y el GGSN/PGW. Durante este procedimiento se le asigna una IP al UE y se negocia el QoS basado en los datos del subscriptor, luego que la activación es exitosa el UE puede acceder a la PDN a través de una red de acceso WLAN.
- Desactivación de contexto PDP, este procedimiento puede ser iniciado por el UE, el TGW o el GGSN/PGW, durante este procedimiento de desactivación la dirección IP del UE es removida y el contexto asociado al GGSN/PGW es eliminado. Luego que el procedimiento de desactivación es exitoso el usuario ya no puede acceder a la PDN.
- Modificación de contexto PDP, el GGSN/PGW inicia el procedimiento de modificación de contexto PDP como por ejemplo el QoS.

3.11.2 Asignación de IP

El UE debe obtener al menos una IP privada para acceder a los servicios de datos, existen 2 maneras de asignarle una IP al usuario, una forma es implementando un servidor DHCP, otra forma es configurando Pools de IPs en el TGW o en el GGSN/PGW. En esta tesis implementaremos la función de DHCP al GGSN/PGW que serán encargado de entregar la IP al usuario basado en el pool de IPs de un APN especifico. Para conseguirlo el UE debe cumplir funciones de cliente DHCP, el TGW permitir la transferencia de la dirección IP al UE y el GGSN/PGW asignar la dirección IP al UE.

En la figura 3.11 se muestra el intercambio de mensajes para que el GGSN/PGW le asigne la dirección IP al UE.

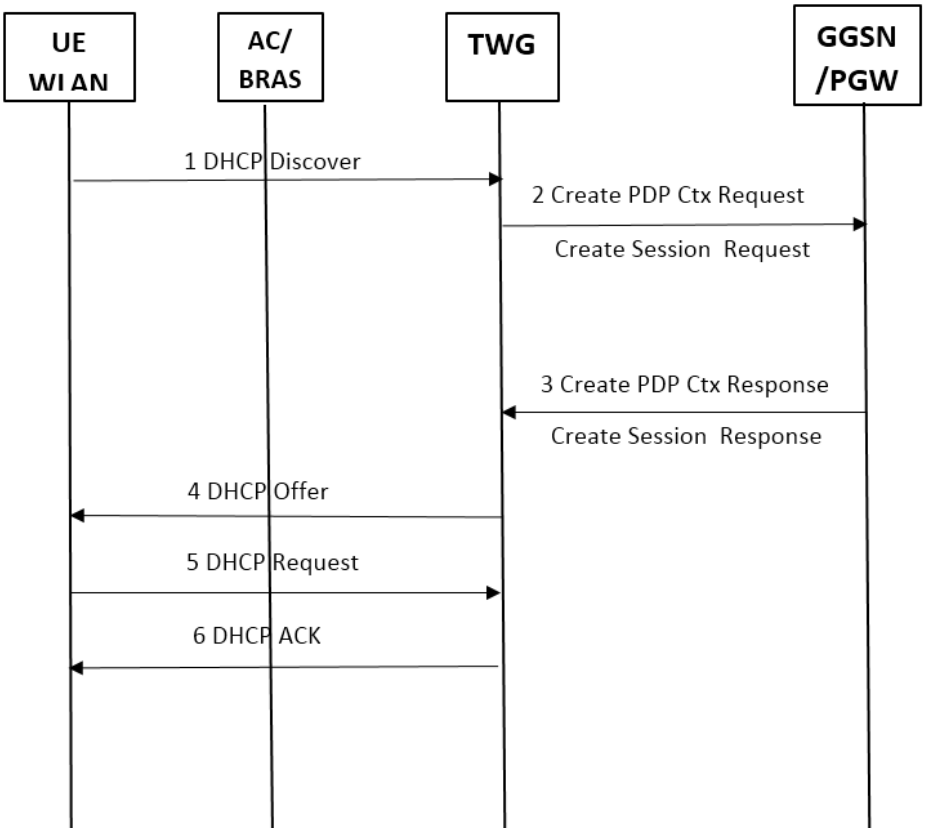


Figura 3-11 Proceso de asignación de IP desde el GGSN/PGW al UE

Elaborado por: Autor

1. El UE envía un mensaje DHCP Discover al TGW para aplicar a una dirección IP.
2. El TGW envía un mensaje créate PDP Context Request si es al GGSN o Create Session Request si es para el PGW. Para poder alcanzar al GGSN/PGW correcto si en el cache de la autenticación no viene incluida la IP del GGSN/PGW es necesario el proceso de resolución de APN a través de un DNS para poder recibir la dirección IP del GGSN/PGW al que debe enviarle el requerimiento de contexto.
3. El GGSN/PGW establece un túnel GTP, asigna una dirección IP al UE basado en el APN y la envía en el mensaje Create PDP Context Response o Create Session Response al TGW.
4. El TGW obtiene la dirección IP asignada por el GGSN/PGW y envía un mensaje DHCP Offer llevando la dirección IP al UE.
5. El UE envía un mensaje DHCP Request al TGW confirmando si esa dirección IP puede ser utilizada por el UE.

6. El TGW le envía un mensaje de reconocimiento DHCP ACK al UE confirmando que puede usar esa IP.

3.12 Diseño de una solución WiFi offload complementaria a la red UMTS y LTE

En la figura 3.12 se plantea la red final de datos UMTS y LTE complementada con la solución WiFi offload:

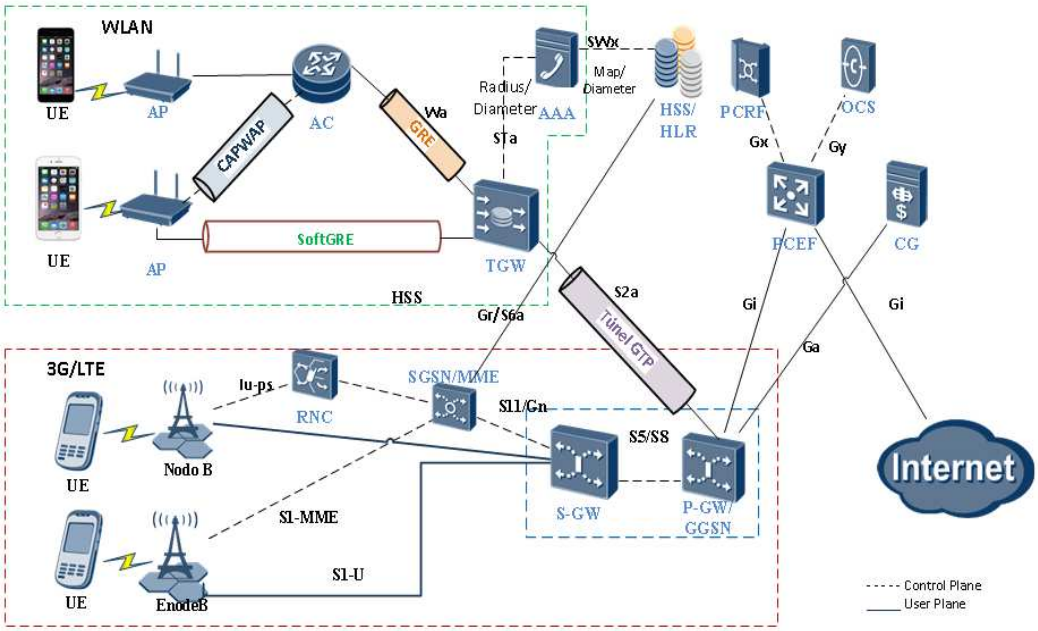


Figura 3-12 Topología de Red para la solución WiFi Offload

Elaborado por: Autor

3.1 Flujo de Señalización

En la figura 3.13 se muestra el flujo final de señalización para que un usuario pueda a acceder a internet a través de una red de acceso no 3GPP como se describe a continuación:

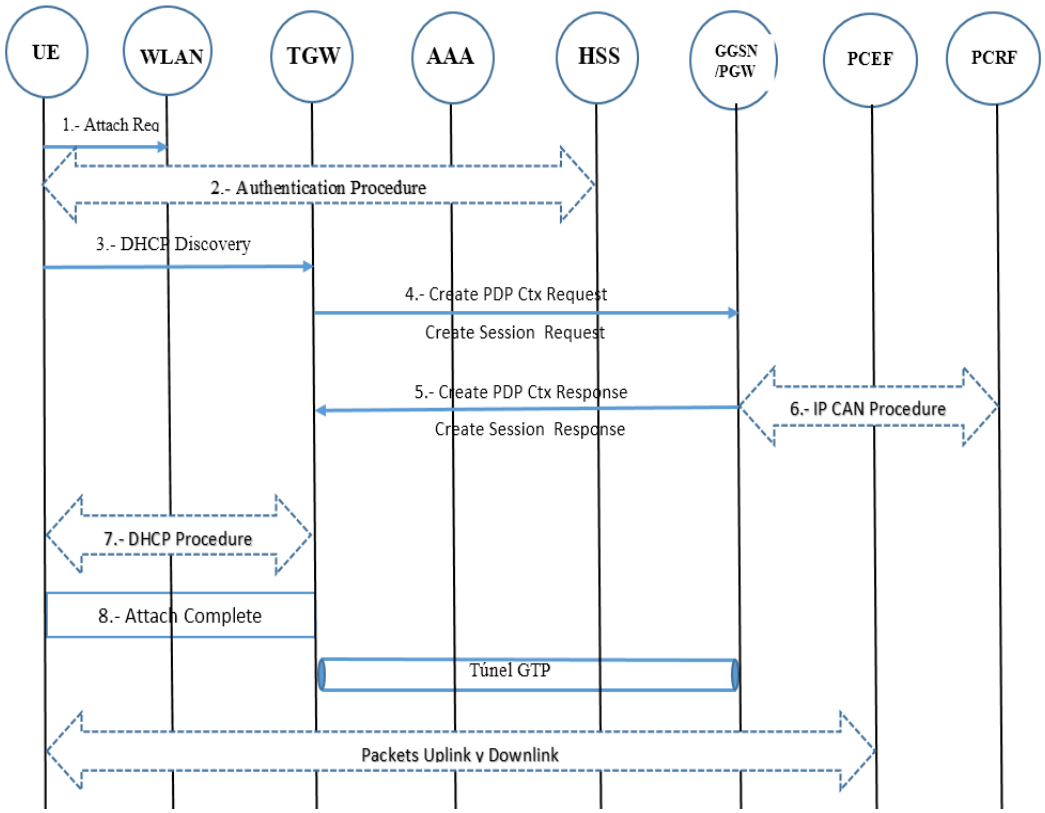


Figura 3-13 Flujo de señalización de la solución WiFi Offload

Elaborado por: Autor

El flujo de señalización que se plantea es el proceso inicial cuando un usuario enciende el dispositivo móvil y comienza por escanear de manera automática todas las redes de acceso habilitadas una vez que reconoce una red de acceso WLAN inicia el proceso que se detalla a continuación:

1. EL UE envía un requerimiento para engancharse a la red de acceso WiFi a través del mensaje *Attach Request*.
2. Después de recibir un requerimiento para poder hacer uso de la red es necesario iniciar el proceso de autenticación detallado en el literal 3.10 y figura 3.10. Si el proceso de autenticación es exitoso el HSS le envía al servidor AAA la información de suscripción como por ejemplo el IMSI, MSISDN y APN.
3. Luego que la autenticación es exitosa el UE envía un requerimiento de dirección Ip como se lo detallo en el literal 3.11.2 y figura 3.11.

4. El TGW envía un mensaje créate PDP Context Request si es al GGSN o Create Session Request si es para el PGW para que le asigne una dirección IP al usuario según el Pool de IPs que tienen para cada APN.
5. La dirección IP del usuario va incluido en el mensaje de respuesta Create PDP Context Response o Create Session Response al TGW.
6. Una vez que se recibe el mensaje de creación de Contextos el GGSN/PGW inicia el proceso de establecer la sesión IP CAN o *accounting start* entre el GGSN/PGW y el PCEF para poder poner al UE en estado online como se lo detalla en el literal 3.6.3 y la figura 3-4.
7. Finaliza el proceso de asignación de una dirección IP privada al UE con la cual podrá acceder a una red pública o privada.
8. Luego de recibir la dirección IP privada finaliza el proceso de engancharse en la red y se forma el túnel GTP para que el UE pueda hacer uso de la red pública como internet o una red privada como intranet enviando paquetes UL y recibiendo paquetes DL, cuando el usuario ya no desee hacer uno de la red pública o privada cambia a estado offline enviando un mensaje PDP deactivate request al GGSN/PGW o *accounting stop.*

Conclusiones

- Se facilita al usuario móvil acceder a ambas tecnologías celular y WiFi al unificar las políticas de seguridad con el proceso de autenticación EAP-AKA para todos los dispositivos que utilizan USIMs. El proceso de autenticación y encriptación es el mismo tanto para un usuario que accede a los servicios de internet móvil a través de una red de acceso 3GPP o no 3GPP.
- Se detalló paso a paso todo el proceso desde que un usuario enciende el dispositivo móvil para engancharse a la red de acceso no 3GPP hasta que está habilitado para poder interactuar con una red pública ya sea navegando en internet o en una red privada con una conexión intranet a través del core móvil.
- La solución propuesta ofrece una integración total con la red móvil 3GPP, permitiendo brindar un modo de acceso convergente con handover sin desconexión entre tecnologías de acceso como (Celular a WiFi y viceversa) o entre una misma red (WiFi a WiFi) manteniendo la misma IP. Diferentes proveedores a nivel mundial incluyen soluciones WiFi Offload propias maximizando los beneficios y costos de operación.
- Al cumplir los objetivos específicos se cumple el objetivo general al proponer el diseño de una red de datos móviles con la solución Wi-Fi Offload complementaria a las redes de datos UMTS y LTE que permita descongestionar el tráfico generado por los usuarios de telefonía celular redireccionando la descarga de datos móviles a través de una red de acceso WiFi.

Recomendaciones

- La implementación de WiFi Offload como complemento de las redes de datos ya existentes UMTS y LTE en las operadoras móviles del país es una solución costo-efectivo que permite incrementar la capacidad de navegación e incluir mayor cantidad de usuarios en zonas de alto tráfico o mejorar la intensidad de la señal en interiores a un costo menor el Mbps, esto será una ventaja competitiva para mejorar la experiencia del usuario creando lealtad de los clientes existentes y atraer nuevos usuarios.
- Otra tecnología complementaria para analizar es la solución de Voz sobre WiFi o mejor conocida como VoWiFi, actualmente varios operadores moviles en el mundo ya ofrecen dentro de sus servicios esta tecnología para mejorar la cobertura en sitios como los trenes subterráneos garantizando continuidad en el servicio de voz e igualando la calidad en servicio de otras soluciones como lo es Voz sobre LTE VoLTE, para VoWiFi no se necesitan de aplicaciones como Line, Whatsapp o Skype para poder tener una llamada de voz y la mayoría de proveedores de dispositivos móviles como Apple, Samsung, LG y Nokia soportan están tecnología.

Glosario de términos

2G (Second Generation, Segunda Generación)

3G (Third Generation, tercera Generación)

3GPP (3rd Generation Partnership Project)

AAA (Authentication, Authorization, Accounting, Autenticación, Autorización y Contabilización)

AC/ BRAS (Access Controller / broadband remote access server, Controlador de Acceso)

AK (Anonymity Key, Clave Anónima)

AMF (Authentication and key Management Field, Campo de Gestión de clave y Autenticación)

AN (Access network, Red de Acceso)

ANDSF (Access Network Discovery and Selection Function, Descubrir Redes de Acceso y Función de Selección)

AP (Access Point, Punto de Acceso)

APN (Access Point Name, Nombre de Punto de Acceso)

ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones

BBAI (Broadband Forum Access Interworking)

BT (Bit Torrent, Flujo de Bits)

CC (Country Code, Código de País)

CCAI (Credit Control Answer Initial, Respuesta Inicial de Control de Crédito)

CCRI (Credit Control Request Initial, Requerimiento Inicial de Control de Crédito)

CCRT (Credit Control Request Terminate, Requerimiento de Terminación de Control de Crédito)

CCRU (Credit Control Request Update, Requerimiento de Actualizar Control de Crédito)

CDR (Charging Data Record, Registro de Datos de Facturación)

CG (Charging Gateway, Enlace de Facturación)

CK (Ciphering Key, Cifrado de Clave)

CN (Core Network, Núcleo de la Red)

CONECEL (Consorcio Ecuatoriano de Telecomunicaciones)

CS (Circuit Switched, Circuitos Conmutados)

CSFB (Circuit Switched Fallback)

DHCP (Dynamic Host Configuration Protocol, Protocolo de configuración Dinámica de Host)

DL (Downlink, Descarga)

DNS (Domain Name System, Sistema de Dominio de Nombres)

DPI (Deep Packet Inspection, Inspección de Paquetes Profunda)

DRB (Data Radio Bearer)

DSCP (Differentiated Services Code Point, Punto de Código de Servicio Diferenciado)

DSMIP (Dual Stack Mobile IPv6)

DSSS (Direct Sequence Spread Spectrum**)**

EAP (Extensible Authentication Protocol, Protocolo de Autenticación Extensible)

EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement)

EAP-AKA´ (EAP-AKA enhancement, EAP-AKA Mejorado)

EAPol (Extensible Authentication Protocol over LAN)

EDGE (Enhanced Data Rates for GSM Evolution, Tasa de Datos Mejorada para la evolución de GSM)

EIR (Equipment Identity Register, Registro de Identidad de Equipos)

EMM (EPS Mobility Management, Gestión de Movilidad EPS)

EPC (Evolved Packet Core, Evolución del Núcleo de Paquetes)

EPS (Evolved Packet System, Evolución del Sistema de Paquetes)

E-RAB (E-UTRAN Radio Access Bearer, Portadora de Radio Acceso E-UTRAN)

E-UTRAN (Evolved Universal Terrestrial Radio Access Network)

EV-DO/CDMA2000 (Evolution – Data Optimized / Code Division Multiple Access, Acceso Múltiple por División de Código)

FAC (Final Assemble Code, Código Ensamblado Final)

FMC (Fixed Mobile Convergence)

FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos)

FUP (Fair Use Policy):

GGSN (Gateway GPRS Support Node)

GPRS (General Packet Radio Service, Servicio General de Paquetes de Radio)

GRE (Generic Routing Encapsulation)

GSM (Global System for Mobile communications, Sistema Global para Comunicaciones Mobiles)

GTP-U (GPRS Tunneling Protocol – User plane, Protocolo de Túnel GPRS- Plano de Usuario)

GUTI (Globally Unique Temporary Identity, Único Identicador Global Temporal)

H-ANDSF (Home Access Network Discovery and Selection Function, ANDSF Local)

HBM (Host Based Mobility, Movilidad Basada en Host)

HLR/ AuC (Home Location Register / Authentication Center, Ubicación de Registro Local/ Centro de Autenticación)

HSPA (High Speed Packet Access, Acceso de Paquetes de Alta Velocidad)

HTTP (Hypertext Transfer Protocol, Protocolo de transferencia Hipertexto)

IFOM (IP Flow Mobility and Seamless WLAN offload)

IK (Integrity Key, Clave de integridad)

IMEI (International Mobile Station Equipment Identities, Estación de Identificación Internacional de Equipos Móviles)

IMSI (International Mobile Station Identity, Estación de Identidad Internacional Móvil)

IP-CAN (IP Connectivity Access Network)

IPoGRE (IP over GRE, IP sobre GRE)

IPSEC (Internet Protocol Security, Protocolo de Seguridad IP)

ISMP (Inter-System Mobility Policy, Políticas de Movilidad entre Sistemas)

ISRP (Inter-System Routing Policy, Políticas de Enrutamiento entre Sistemas)

ITU (Internationational Telecommunication Union, Unión Internacional de Telecomunicaciones)

I-WLAN (Interworking WLAN, Interacción WLAN)

LMA (Local Mobility Anchor)

LOBSTER (Location-Based Selection of gateways for WLAN)

LTE (Long Term Evolution)

MAA (Multimedia Authentication Answer, Respuesta de Autenticación Multimedia)

MAC (Message Authentication Code, Código de Autenticación Multimedia)

MAG (Mobile Access Gateway, Puerta de Enlace de Acceso Móvil)

MAP (Mobile Application Part)

MAPCON (Multi Access PDN Connectivity, Conectividad de Multi Acceso PDN)

MAR (Multimedia-Authentication-Request, Requerimiento de Autenticación Multimedia)

MCC (Mobile Country Code, Código Móvil del País)

ME (Mobile Equipment, Equipo Móvil)

MIMO (Multiple Input Multiple Output, Multiples Entradas Multiples Salidas**)**

MIP (Mobile IP, IP Móvil)

MM (Mobility Management, Gestión de Movilidad)

MME (Mobility Management Entity, Entidad de Gestión de Movilidad)

MMS (Multimedia Messaging Service, Servicio de Mensajes Multimedia)

MSC (Mobile Switching Center, Centro de Conmutación Móvil)

MSIN (Mobile Subscription Identification Number, Número de Identificación del Suscriptor Móvil)

MSISDN (Mobile Station International Subscriber Directory Number, Número de Directorio del Suscriptor de Estación Móvil Internacional)

MT (Mobile Termination, Terminal Móvil)

NAS (Non-access Stratum)

NAT (Network Address Translation, Traducción de Direcciones de Red)

NBAP (Node B Application Part)

NBM (Netrwork Base Movility, Movilidad Basada en Redes)

NDC (Network Destination Code, Código de Destino de Red)

NI (Network ID, Identificador de la Red)

OCS (Online Charging System, Sistema de Facturación en Línea)

OFDM (Orthogonal Frequency Division Multiplexing, Multiplexación por División de Frecuencia Ortogonal)

OI (Operator ID, Identificación del Operador)

OTECEL (Operadora de Telefonía Celular Sociedad Anónima)

PCC (Policy & Charging Control, Políticas de control y Facturación)

PCEF (Policy and Charging Enforcement Function, Función de Aplicación de Políticas de Control y Facturación)

PCRF (Policy and Charging Rules Function, Función Reglas de Políticas de Control y Facturación)

PDN (Public Data Network, Red de Datos Pública)

PDP (Packet Data Protocol, Protocolo de Paquetes de Datos)

PEAP (Protected Extensible Authentication Protocol)

P-GW (PDN Gateway, Puerta de Enlace al PDN)

PMIP (Proxy Mobile IP)

PMIPv6 (Proxy Mobile IPv6)

PMM (Packet Mobility Management, Gestión de Movilidad de Paquetes)

PS (Packet Switched, Conmutación de Paquetes)

P-TIMSI (PS Temporary IMSI, IMSI Temporal para PS)

QCI (QoS class Identifier, Identificador de Clase de QoS)

QoE (Quality of Experience, Calidad de Experiencia)

QoS (Quality of Service, Calidad de Servicio)

RAB (Radio Access Bearer, Portadora de Radio Acceso)

Radius (Remote Authentication Dial In User Service)

RANAP (Radio Access Network Aplication Protocol, Protocolo de Aplicación de RAN)

RAU (Routing Area Update, Actualización de Área de Enrutamiento)

RNC (Radio Network Controler, Controlador de Radio de Red)

RNS (Radio Network System, Sistema de Red de Radio)

S1-AP (S1 Aplication Protocol, Protocolo de Aplicación de S1)

SA (Service Awareness, Garantías de Servicio)

SaMOG (S2a Mobility based On GTP, Movilidad S2a basada en GTP)

SCTP (Stream Control Transmission Protocol)

SGSN (Serving GPRS Support Node)

S-GW (Serving Gateway)

SIM (Subscriber Identity Module, Módulo de Identificación de Suscriptor)

SM (Session Managemente, Gestion de Sesiones)

SMS (Short Message Service, Servicio de Mensajes Cortos)

SN (Subscriber Number, Número de Suscriptor)

SRN (Serial Number, Número de Serie)

SSID (Service Set Identifier, Identificador de Conjunto de Servicios)

TA (Terminal Adapter, Adaptador de terminal)

TA (Tracking Area, Área de Seguimiento)

TAC (Type Authorization Code, Tipo de Código de Autenticación)

TAU (Tracking Area Update, Actualización de TA)

TCP (Transmission Control Protocol, Protocolo de Control de Transmisión)

TE (Terminal Equipment, Equipo Terminal)

TGW (Trusted Gateway)

TWAG (Trusted WLAN access gateway)

TWAP (Trusted WLAN AAA Peer)

UDP (User Datagram Protocol)

UE (User Equipment, Equipo de Usuario)

UL (Uplink, Carga)

ULI (User Location Information, Información de Localización de Usuario)

UMTS (Universal Mobile Telecommunications System, Sistema Móvil Universal de Telecomunicaciones)

URL (Uniform Resource Identifier)

USIM (Universal Subscriber Identity Module, Modulo de Identificación de Suscriptor Universal)

UTRAN (UMTS Terrestrial Radio Access Network, Red de Acceso de Radio Terrestre UMTS)

VLAN (Virtual Local Area Network, Virtual LAN)

VNI (Visual Networking Index, Índice de Redes Visuales)

WAP (Wireless Application Protocol, Protocolo de Aplicación Inalámbrico)

WCDMA/UMTS (Wideband Code Division Multiple Access / Universal Mobile Telecommunication System, Sistema Móvil Universal de Telecomunicaciones)

WLAN (Wireless Local Area Network, Red de Área Local Inalámbrica)

WMM (Wi-Fi Multimedia)

Referencias Bibliográficas

3GPP R8 - TS 23.401, 2007 Evolved Universal Terrestrial Radio Access Network. http://www.qtc.jp/3GPP/Specs/23401-800.pdf.

3GPP R11 - TS 23.402, 2012, Architecture enhancements for non-3GPP accesses. http://www.etsi.org/deliver/etsi_ts/123400_123499/123402/11.04.00_60/ts_123402v110400p.pdf.

3GPP R.99, 2010 Overview of 3GPP Release 1999. http://www.3gpp.org/specifications/releases/77-release-1999.

3GPP R8 -TS 36.300, 2009 LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2. http://www.etsi.org/deliver/etsi_ts/136300_136399/136300/08.09.00_60/ts_136300v080900p.pdf.

3GPP R13 - TS 33.105, 2016 Characteristics of the Universal Subscribe Module (USIM) application. http://www.etsi.org/deliver/etsi_ts/133100_133199/133105/13.00.00_60/ts_133105v130000p.pdf.

ARCOTEL, Agencia de Regulación y Control de las Telecomunicaciones | 2016 Agencia de Regulación Y Control de Las Telecomunicaciones | Ecuador » Servicio de Acceso a Internet (SAI). Agencia de Regulación Y Control de Las Telecomunicaciones | Ecuador. http://www.arcotel.gob.ec/servicio-acceso-internet/, accessed August 21, 2016.

Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020, 1 Febrero 2016 Cisco. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, accessed July 30, 2016.

Ericsson-Mobility-Report-Nov-2015.pdf https://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf, accessed August 11, 2016.

3g4g. (24 de Noviembre de 2010). IP Flow Mobility and Seamless Offload (IFOM). Obtenido de 3g4g.blogspot.com: http://blog.3g4g.co.uk/2010/11/ip-flow-mobility-and-seamless-offload.html

Guidelines, V. S. (07 de 10 de 2014). GSMA. Obtenido de VoLTE Service Description and Implementation Guidelines 2.0:

http://www.gsma.com/network2020/wp-content/uploads/2014/10/FCM.01-VoLTE-Service-Description-and-Implementation-Guidelines-Version-2.0.pdf

Huawei. (2015). WLAN Trusted Access. Obtenido de Huawei Solution: http://support.huawei.com/hdx/hdx.do?docid=DOC1000059770&lang=en&clientWidth=1904&browseTime=1497365032164

Huawei. (2016). Service Awareness. Obtenido de Huawei System: http://support.huawei.com/carrier/en/esb/index.html

Lucent, A. (12 de 11 de 2015). Voice over LTE the new mobile voice . Obtenido de http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2013/6685-voice-over-lte-new-mobile-voice-inspire-new.pdf

Rumney, M. (01 de 01 de 2008). 3GPP LTE Introducing Single Carrier FDMA. Recuperado el 16 de 09 de 2016, de http://cp.literature.agilent.com/litweb/pdf/5989-7898EN.pdf

Sandvine. (2015). Voice over LTE Challenges and opportunities. Recuperado el 16 de 09 de 2016, de An Industry Whitepaper.

Vargas, D. F. (2012). Calidad de Servicio en Redes LTE Advanced. Colombia. de http://cintel.co/wp-content/uploads/2013/05/02.Calidad_de_Servicio_en_Redes.pdf

VoipForo. (s.f.). Sip Session Iniation Protocol. http://www.voipforo.com/SIP/SIParquitectura.php

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Christian Xavier Ferigra Orellana**, con C.C: # **0922475736** autor/a del trabajo de titulación: **Propuesta de diseño de una red de datos móviles con la solución WiFi Offload complementaria a las redes UMTS y LTE, que permita brindar servicio de internet a usuarios móviles a través de un acceso WiFi,** previo a la obtención del título de **Magister en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 21 de junio de 2017

f. _____

Nombre: Christian Xavier Ferigra Orellana

C.C: 0922475736

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Propuesta de diseño de una red de datos móviles con la solución WiFi Offload complementaria a las redes UMTS y LTE, que permita brindar servicio de internet a usuarios móviles a través de un acceso WiFi		
AUTOR(ES)	Christian Xavier Ferigra Orellana		
REVISOR(ES)/TUTOR(ES)	MSc. Orlando Philco Asqui / MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
CARRERA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	21 de junio de 2017	**No. DE PÁGINAS:**	101
ÁREAS TEMÁTICAS:	Estructura de red de datos 3G UMTS, Interfaces lógicas y protocolos de la arquitectura UMTS, Arquitectura de red LTE, Interfaces lógicas y protocolos EPS, WiFi Offloading		
PALABRAS CLAVES/ KEYWORDS:	UMTS, LTE, WLAN, WiFi Offload, SaMOG.		
RESUMEN/ABSTRACT (150-250 palabras): Este proyecto de tesis consiste en proponer el diseño de una red móvil de datos con la solución WiFi Offload para poder proporcionar el servicio de datos móviles a través de una red de acceso no 3GPP como WiFi como una alternativa tecnológica para mejorar el rendimiento general de la red, solventar los problemas de cobertura indoor y mejorar la experiencia de navegación del usuario con velocidades y calidad de servicio que superan a 3G e igualan y mejoran 4G a menor precio el Mbps. Se analizó la mejor propuesta basado en los últimos estándares propuestos por 3GPP y basados en la tecnología de un proveedor de telecomunicación como Huawei. Se describe las arquitecturas existentes UMTS/LTE y la arquitectura final luego de la implementación de la solución con sus respectivos protocolos e interfaces lógicas, así como el detalle del flujo de señalización que debe seguir un usuario para poder acceder al servicio de datos móviles a través de una red de acceso WiFi con un servicio continuo permitiendo handover entre diferentes tecnologías de acceso (WiFi a Celular y viceversa) y entre las mismas tecnologías como (WiFi a WiFi).			
ADJUNTO PDF:	☒ SI	☐ NO	
CONTACTO CON AUTOR/ES:	**Teléfono:** 0999626449	E-mail: cferigra89@gmail.com	
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Manuel de Jesús Romero Paz		
	Teléfono: +593-4-2202935 /0994606932		
	E-mail: manuel.romero@cu.ucsg.edu.ec / mromeropaz@yahoo.com		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			