Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

PROPUESTA DE LIBERACIÓN DE CONGESTIÓN DE REDES MÓVILES UTILIZANDO EL WIFI COMO ACCESO ALTERNO PARA DATOS

German Estuardo Jerez Ochoa

Asesorado por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, febrero de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PROPUESTA DE LIBERACIÓN DE CONGESTIÓN DE REDES MÓVILES UTILIZANDO EL WIFI COMO ACCESO ALTERNO PARA DATOS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

GERMAN ESTUARDO JEREZ OCHOA
ASESORADO POR LA INGA. INGRID SALOMÉ RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, FEBRERO DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Narda Lucía Pacay Barrientos
VOCAL V	Br. Walter Rafael Véliz Muñoz
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
EXAMINADOR	Ing. Luis Fernando García Cienfuegos
EXAMINADOR	Ing. Julio Rolando Barrios Archila
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA DE LIBERACIÓN DE CONGESTIÓN DE REDES MÓVILES UTILIZANDO EL WIFI COMO ACCESO ALTERNO PARA DATOS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 11 de febrero del 2014.

German Estuardo Jerez Ochoa

Guatemala 3 de Agosto de 2014

Ingeniero
Carlos Eduardo Guzmán Salazar
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Estimado Ingeniero Guzmán.

Me permito dar aprobación al trabajo de graduación titulado: **PROPUESTA DE LIBERACIÓN DE CONGESTIÓN DE REDES MÓVILES UTILIZANDO EL WIFI COMO ACCESO ALTERNO PARA DATOS**, del señor **German Estuardo Jerez Ochoa**, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

Ingrid Rodríguez de Loukota
Ingeniera en Electrónica
colegiado 5356

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Ref. EIME 51. 2014
Guatemala, 22 de SEPTIEMBRE 2014.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: PROPUESTA DE LIBERACIÓN DE CONGESTIÓN DE REDES MÓVILES UTILIZANDO EL WIFI COMO ACCESO ALTERNO PARA DATOS, del estudiante German Estuardo Jerez Ochoa, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica

SIO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 51. 2014.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; GERMAN ESTUARDO JERÉZ OCHOA titulado: PROPUESTA DE LIBERACIÓN DE CONGESTIÓN DE REDES MÓVILES UTILIZANDO EL WIFI COMO ACCESO ALTERNO PARA DATOS, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 11 DE NOVIEMBRE 2,014.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

DTG. 051.2015

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **PROPUESTA DE LIBERACIÓN DE CONGESTIÓN DE REDES MÓVILES UTILIZANDO EL WIFI COMO ACCESO ALTERNO PARA DATOS,** presentado por el estudiante universitario **German Estuardo Jerez Ochoa,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, 9 de febrero de 2015

/gdech

ACTO QUE DEDICO A:

Dios	Por darme una oportunidad de vida cada día.
Mis padres	German Jerez Juárez y Gudelia Ochoa, por ser mi fortaleza cuando más la he necesitado.
Mis hermanas	Rosita, Gloria e Ingrid Jerez Ochoa, por contar con su apoyo incondicional siempre.
Mi sobrino	Carlos Andrés Jerez, por ser mi inspiración y demostrarte lo grande que es alcanzar las metas.
Mi esposa	Andrea Mejía, por su amor, paciencia y confianza.
Mi hijo	Mateo Estuardo Jerez Mejía, por ser el motor de voluntad que me hace querer ser más y mejor.
Mis amigos	Por ser la familia que he podido elegir y por estar siempre en cada etapa de mi vida.

AGRADECIMIENTOS A:

Facultad de Ingeniería	Por enseñarme que hay que trabajar duro para cumplir los objetivos.
Ingeniera Ingrid de Loukota	Por su valiosa ayuda y apoyo en el último obstáculo del objetivo.
Claro Guatemala	Por brindarme la oportunidad del desarrollo profesional.
Compañeros de trabajo	Por enseñarme a valorar el trabajo en equipo y por impulsar que siempre se puede dar más para alcanzar los objetivos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTADO DE SIMBOLOS

Simbolo	Significado
1G	Primera generación de la telefonía móvil.
2G	Segunda generación de la telefonía móvil.
3G	Tercera generación de la telefonía móvil.
4G	**C**uarta generación de la telefonía móvil.

GLOSARIO

3GPP Asociación que se encarga de definir estándares para que la integración de la tecnología móvil sea eficiente.

AAA Authentication, Authorization and Accounting, por sus siglas en inglés, equipo que se encarga de validar el acceso de un usuario a una red de datos.

AC Access Controller, por sus siglas en inglés, equipo encargado de administrar los puntos de acceso wifi.

AMPS Advanced Mobile Phone System, por sus siglas en inglés, modelo análogo de transmisión de datos utilizada en la primera generación de la telefonía móvil.

AP Access Point, equipo que se encarga de dar el acceso de un usuario a la red de datos wifi.

APN Access Point Name, por sus siglas en inglés, hace referencia a un nombre de dominio que resuelve una IP lo que permite la conexión hacia la salida a internet de un usuario.

BSC	Base Station Controller*,* estación base que controla a varias BTS de una red 2G
BTS	Base Transceiver Station, por sus siglas en inglés, es el equipo que se utiliza para la comunicación bidireccional entre uno o varias terminales móviles.
CDMA	Code Division Multiple Access*,* tecnología que permite la transmisión de paquetes simultáneos utilizando un mismo canal.
CDR	Call Detail Record*,* registros donde quedan almacenadas todas las llamadas de voz y datos.
Contexto PDP	Sesión de usuario establecida entre el equipo solicitante, la terminal de usuario y el GGSN.
CORBA	Common Objetc Request Broker Arquitecture**,** por sus siglas en inglés, en telecomunicaciones es una interfaz de cobro hacia el sistema de cobro en línea.
DCCA	Diameter Credit Control Application, protocolo de Diameter utilizado para el control de crédito en tiempo real.
DHCP	Dynamic Host Configuration Protocol, protocolo que distribuye dinámicamente una dirección IP a los dispositivos de red que la soliciten.

DIAMETER	Protocolo de autenticación y autorización confiable en los protocolos de transporte *TCP* y *UDP*
EAP	Extensible Authentication Protocol, por sus siglas en inglés, protocolo de comunicación utilizado en conexiones inalámbricas y de punto a punto.
EAP-AKA	Extensión del protocolo EAP y se utiliza para la autenticación de usuarios UMTS o 3G.
EAP-SIM	Extensión del protocolo EAP y se utiliza para la autenticación de usuarios GSM o 2G.
EDGE	Enhanced Data rates for GSM Evolution por sus siglas en inglés, tecnología celular que permite improvisar velocidades de datos mayores y compatibles con GSM.
FDMA	Frequency Division Multiple Access, tecnología basada en división de canales por frecuencia.
FTP	File Transfer Protocol¸ protocolo utilizado para transferir archivos desde un host hacia otro.
GERAN	GSM EDGE Radio Access Network, por sus siglas en inglés, nombre dado a la red de acceso para 2G.

GGSN	GPRS Gateway Support Node, equipo que brinda la salida de internet para el servicio de datos dentro de una red móvil.
GPRS	General Packet Radio Service, por sus siglas en inglés, sistema utilizado para la transmisión de datos mediante la conmutación de paquetes.
GRE	Generic Routing Encapsulation, protocolo de túnel que puede encapsular una gran variedad de protocolos de capa de red dentro de enlaces punto a punto.
GSM	Global System for Mobile Communications, estándar desarrollado para describir protocolos de segunda generación.
GTP	GPRS Tunnelling Protocol, por sus siglas en inglés, protocolo que se encarga de encapsular los mensajes *GPRS* entre el *SGSN* y el *GGSN.*
GTP-C	Encapsula los mensajes de control del protocolo *GTP.*
GTP-U	Encapsula los mensajes de navegación hacia la red de internet que viajan por el protocolo *GTP.*

Handover	En telecomunicaciones, transferencia de la responsabilidad de una llamada o una sesión de datos activa y establecida en una radio base hacia otra sin tener una caída del servicio.
HLR	Home Location Register, por sus siglas en inglés, equipo que almacena toda la información de los usuarios de una red.
Hotspot	Dispositivo que ofrece acceso inalámbrico a una red de área local.
HTTP	Hypertext Transfer Protocol, por sus siglas en inglés, protocolo de aplicación que se utiliza para la distribución de sistemas de información de hipermedia.
ID	Número de identificación que se les da a los equipos dentro de una red.
IP	Internet Protocol, protocolo de transporte encargado de entregar paquetes desde un equipo origen hacia un equipo destino utilizando solamente las direcciones P que están en el encabezado.
LTE	Long Term Evolution, nombre con el que se le conoce a la red de datos 4G y está basado en un estándar para comunicación de alta velocidad en redes inalámbricas.

MAP	Mobile Application Part, por sus siglas en inglés, es un protocolo de señalización que permite interconectar varios elementos dentro de una red móvil, el principal es el HLR.
MPLS	Multiprotocol Lable Switching, por sus siglas en inglés, red de alto rendimiento que se encarga de enviar paquetes entre redes utilizando etiquetas de rutas más cortas.
MSC	Mobile Switching Centre, equipo que se encarga de controlar la movilidad de la red y de direccionar las llamadas de voz y mensajería de texto de los usuarios.
MSISDN	Mobile Station Integrated Service Digital Network, por sus siglas en inglés, nombre que se le da al compuesto del código de país más el número móvil del usuario.
OCS	Online Charging System, equipo que se encarga de hacer el cobro en línea de usuarios prepago del operador.
Paging	Mensaje de ubicación al usuario que existe entre la red de datos y la red de acceso.

PCRF	Policy and Charging Rules Function, por sus siglas en inglés, equipo que se encarga de administrar políticas y reglas de navegación para determinados perfiles de usuario.
PMM-IDLE	Modo de estado del usuario y cuando a nivel de red está reportado como *PMM-IDLE* el *paging* es necesario para localizarlo.
P-TMSI	Número de identidad temporal que se le asigna al usuario en el inicio de una sesión de datos, este valor será utilizado en cada actualización de red que haga el subscriptor.
QoS	Quality of Service, por sus siglas en inglés, hace referencia al rendimiento de una red de telefonía visto desde el punto de vista del usuario.
RAB	Radio Access Bearer, proceso en el que se reservan recursos en la terminal del usuario y en la red de acceso para establecer sesiones de datos.
RADIUS	Remote Authentication Dial In User Service, por sus siglas en inglés, protocolo centralizado de autenticación, autorización y cobro que es parte de la capa de aplicación y utiliza el protocolo UDP como transporte.

RAN	Radio Access Network, red encargada de proveer acceso a los servicios de telefonía móvil.
SGSN	Serving GPRS Support Node, nodo encargado de la señalización del servicio de datos y de la movilidad del usuario.
SIGTRAN	Signaling Transfer Network, por sus siglas en inglés, protocolo encargado de transferir señalización SS7 sobre la red IP del operador.
SIM	Subscriber Identification Module, circuito integrado que guarda la identidad de un suscriptor móvil, este circuito es insertado en la terminal para tener servicio de la red del operador.
SMS	Short Message Service por sus siglas en inglés, acrónimo que hace referencia al servicio de mensajería corta.
SS7	Signaling System No.7, por sus siglas en inglés, conjunto de protocolos de señalización que son utilizados en la mayoría de redes de conmutación para establecer las llamadas de voz.
SSID	Service Set Identification, nombre público de una red inalámbrica.

TCP	Transmission Control Protocol, se utiliza junto con el protocolo IP para el envío y rastreo de paquetes a través de una red de transporte.
TDMA	Time Division Multiple Access por sus siglas en inglés, en telecomunicaciones, permite a los usuarios compartir el mismo canal de frecuencia dividiendo la señal en distintos espacios de tiempo.
UDP	User Datagram Protocol, parte del protocolo IP y al igual que TCP funciona sobre la capa de transporte.
UMTS	Universal Mobile Telecommunications System, por sus siglas en inglés, sistema basado en el estándar GSM y está orientado a la tecnología 3G de la telefonía móvil.
USIM	Universal Subscriber Identity Module, aplicación de software para la telefonía UMTS análogo a lo que SIM es para 2G.
UTRAN	UMTS Terrestrial Radio Access Network, denominación de la red de acceso para 3G.
VLR	Visitor Location Register, base de datos que contiene la información de suscriptores *roaming*.
VPN	Virtual Private Network, por sus siglas en inglés, permite extender una red privada a través de una red de acceso público como el internet.

WAG	Wireless Access Gateway, equipo que controla el acceso de la red WiFi y que brinda la conexión GTP hacia el GGSN para la salida de datos hacia internet.
WAP	Wireless Application Protocol, estándar de acceso a información en una red móvil inalámbrica.
WCDMA	Wideband Code Division Multiple Access, por sus siglas en inglés, interfaz de aire estándar para 3G que permite la transmisión de paquetes de datos a una velocidad superior a la normal.
WiFi	Tecnología de conexión inalámbrica hacia una red de área local.

RESUMEN

En el presente trabajo de graduación se explica un diseño distinto y alterno para el acceso en las redes de telefonía móvil, se plantea la división en el ingreso de los servicios de datos y voz a la red de los operadores móviles, logrando así disminuir la utilización de los canales comunes de las antenas que actualmente se utilizan.

En el primer capítulo se explican los fundamentos básicos de las redes de voz y datos, dando a entender en primera instancia, cómo fue la evolución de la telefonía móvil hasta lo que se conoce actualmente, se explica la arquitectura general de una red móvil, dividiéndola en 4 subredes y describiendo sus componentes y tarea que cada elemento ejerce en el funcionamiento de la red general.

En el segundo capítulo se detalla la nueva arquitectura basada en acceso wifi que estará soportando el servicio de datos móviles, se detalla cómo debe ser la autenticación del usuarios, ya que por el modo de acceso, la información del suscriptor debe ser completada para poder registrase a la red y hacer uso del servicio, el equipo AAA será clave en este diseño.

En el tercer capítulo se muestran los diferentes diseños propuestos de integración de la solución wifi a la red y equipos existentes del operador móvil.

En el cuarto capítulo se describen los casos de uso de la solución wifi y ejemplos de cómo lograr una monetización combinando escenarios corporativos con las necesidades técnicas de la red móvil en sí.

OBJETIVOS

General

Realizar una propuesta que logre la liberación de congestión de redes móviles utilizando el wifi como acceso alterno para datos.

Específicos

1. Presentar los fundamentos de una red de voz y datos.

2. Mostrar la arquitectura de la red wifi para la descarga de datos móviles.

3. Detallar la integración de la solución de utilización de datos móviles con acceso por wifi.

4. Presentar los casos de uso de la solución wifi.

INTRODUCCIÓN

La congestión en el acceso de una red de telefonía móvil se da cuando los canales de comunicación de una antena son ocupados en su totalidad, esto ocasiona perder nuevas conexiones que, desde otro punto de vista son en realidad usuarios intentando conectarse a la red del operador sin éxito.

Las redes móviles brindan dos grandes servicios actualmente, voz y datos, y a pesar de las evoluciones de la telefonía celular el acceso para estos dos servicios continúa siendo el mismo, situación que conlleva a la saturación del ancho de banda utilizado en horas de alto tráfico o en lugares donde hay mucha afluencia de personas. El tráfico de datos ha ganado protagonismo en los últimos años, siendo este el servicio más utilizado actualmente por los usuarios de telefonía móvil, encontrando así que en la distribución de canales a nivel de radio de las antenas los recursos asignados para datos son más que los de voz.

De este problema surge la necesidad de encontrar vías alternas para el uso de los servicios de telefonía móvil a un nivel óptimo y de alta disponibilidad. La propuesta de este trabajo de graduación consiste en habilitar un acceso alterno para el tráfico de datos, que es actualmente el más utilizado por los usuarios móviles y es el servicio que tiende a crear la saturación en los accesos principales. La idea de este acceso alterno es brindar únicamente servicios de datos con el objetivo de controlar el tráfico que está de más en el sector; esto permitirá liberar canales de radio para el tráfico de voz y mantener siempre disponibles los recursos de datos en las antenas principales, evitando así congestión y pérdida de servicio para el operador móvil.

La solución planteada está basada en puntos de acceso wifi que serán desplegados en sitios estratégicos y que presenten síntomas de saturación, siendo así una alternativa al servicio de internet móvil brindando soluciones corporativas y una descarga del tráfico general de datos de la red principal.

Una ventaja de la red wifi es que el tráfico que ingrese por este medio puede ser integrado al equipo que maneja el servicio de datos móviles actual, lo que implicaría mantener las reglas de cobro y las políticas de servicio sin cambio alguno y sin integración adicional. Esto dependerá del diseño y de las necesidades del operador.

1. CONCEPTOS FUNDAMENTALES DE UNA RED DE VOZ Y DATOS

1.1. Telefonía móvil

Se basa en dos elementos: la red de comunicaciones y las terminales (dispositivos móviles).

La red de comunicaciones se compone de varios elementos que permiten el acceso a la red de voz y datos, a la validación del usuario, a los cobros en tiempo real y cobros fuera de línea, y lo más importante, a los elementos que permiten una calidad de servicio óptimo. Las terminales son los dispositivos con los que cuenta el usuario, con base al modelo con el que el cliente tenga podrá adquirir una mejor experiencia de los servicios móviles que las operadoras brindan actualmente.

1.1.1. Historia

Es indiscutible que la telefonía móvil (también llamada telefonía celular) constituye un proceso de evolución constante desde sus inicios en 1979, año en que la compañía NTT realizó los primeros diseños comerciales en Japón, específicamente Tokio. Partiendo de este punto, la tecnología tuvo una gran aceptación y ha tenido su desarrollo en la búsqueda de diversas formas de acceso y topologías de red para voz, que fue el primer objetivo que se tuvo con la telefonía celular. Posteriormente se cambiaron los sistemas análogos por digitales con intención de brindar los servicios a más usuarios, con el tiempo han ido surgiendo más necesidades de parte de los usuarios. Paralelamente

con el internet, se dio paso a los datos móviles, y a nuevos estándares, topologías, elementos de red y nuevas demandas del consumidor final.

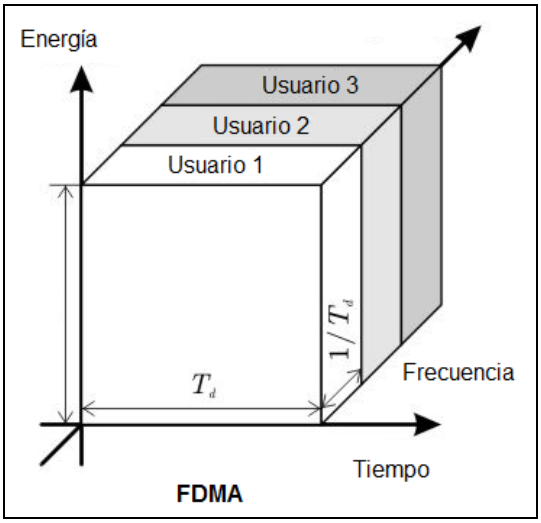
Como consecuencia de la constante evolución, la telefonía celular divide su evolución, hasta este momento, en generaciones, siendo estas llamadas 1G, 2G, 2.5G, 3G y la más reciente 4G o LTE (por sus siglas en inglés, Long Therm Evolution).

1.1.1.1. Primera generación (1G)

Esta se caracterizó por ser análoga y exclusiva para voz. Surgió en 1979 y la tecnología utilizada era conocida como AMPS (Advanced Mobile Phone System*)* la cual estaba basada sobre FDMA (Frequency-division multiple access) que básicamente utilizaba frecuencias separadas o canales para cada conversación.

AMPS era demasiada susceptible a la estática y al ruido e incluso era muy vulnerable a las intercepciones ilegales, ya que carecía de protocolos de encriptación y seguridad.

Figura 1. **Utilización de canales por usuario con FDMA**



Fuente: http://blog.oureducation.in/wp-content/uploads/2013/05/FDMA_TDMA_CDMA.jpg.Consulta: 15 de junio de 2014.

1.1.1.2. Segunda generación (2G)

La generación 2G surgió de la necesidad de atender un número mayor de llamadas sobre un mismo espectro de radiofrecuencia, para lograrlo, se dio el cambio de los sistemas análogos a los digitales, que ya tenían protocolos, que permitían la optimización del uso de ancho de banda y sobre el cual fue posible la implementación de servicios, que antes eran independientes, y que ahora podían ser integrados dentro de la misma señal; estos servicios son los de SMS (Short Messages Services) y servicios de datos como fax y el uso de módems.

2G surgió a principios de 1990, sin embargo, tenía la debilidad que varios protocolos fueron desarrollados por compañías distintas que al final resultaron ser incompatibles. A pesar de estas dificultades, esta generación logró dar una gran mejora en la calidad de voz y permitió que el mercado de las

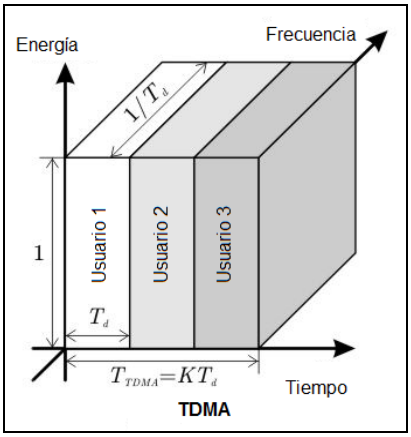
telecomunicaciones se ampliara, dándole paso a varias operadoras de telefonía y otras compañías proveedoras de dispositivo y elementos de red.

2G fue la que abrió paso a lo que se tiene actualmente, y se utilizaron varias tecnologías, siendo estas:

- GSM (Global System for Mobile Communications), es la más importante y sobre la cual se han ido desarrollando los estándares siguientes.
- PCS/IS-136, basado en TDMA.
- IS-95/*CDMA*ONE, basado en CDMA.
- D-AMPS
- PHS

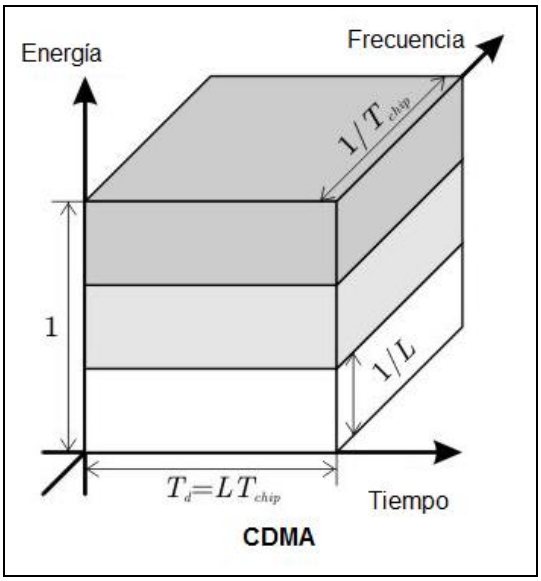
Este último fue utilizado en Japón, enfocado más a la transferencia de datos.

Figura 2. **Utilización de canales por usuario con TDMA**



Fuente: http://blog.oureducation.in/wp-content/uploads/2013/05/*FDMA_TDMA_CDMA*.jpg. Consulta: 15 de junio de 2014.

Figura 3. **Utilización de canales por usuario con *CDMA***



Fuente: http://blog.oureducation.in/wp-content/uploads/2013/05/*FDMA_TDMA_CDMA*.jpg. Consulta: 15 de junio de 2014.

1.1.1.3. Generación 2.5 / 2.75

Esta es una generación de transición, muchos operadores no fueron de 2G a 3G directo, pasaron por una etapa de adaptación con esta, tanto a nivel de infraestructura como de comercialización.

En ella se incorporan funcionalidades del estándar 3G, aunque sin llegar a la capacidad de esta generación como tal; dichas funcionalidades son el GPRS y EDGE.

1.1.1.4. Tercera generación (3G)

Esta constituye un gran salto en las comunicaciones móviles. Bajo este estándar surgen nuevos modelos y tecnologías que permiten una transferencia de datos más veloz y eficiente.

Basada en la tecnología UMTS, el 3G provee una gran capacidad multimedia, un rápido acceso a internet desde los dispositivos móviles y una calidad de voz que se asemeja a la de una llamada de línea fija. Bajo estos tres estatutos se puede decir que, las comunicaciones móviles evolucionaron de una forma más orientada al uso de aplicaciones multimedia que requieren de un fácil acceso a internet, que hoy en día, es utilizado de una gran forma por los usuarios del servicio móvil.

El UMTS en sí, está basado en la tecnología WCDMA que hace referencia al acceso múltiple por separación de código de banda ancha que permite decir en términos simples que para el caso del acceso móvil, es posible soportar varias llamadas al mismo tiempo sin importar el tiempo de duración de las mismas; ya que en sí, el WCDMA aprovecha de una mejor forma el espectro de la comunicación móvil, lo cual da una mejor eficiencia al momento de la transferencia de datos (acceso a internet, es el gran aporte del UMTS en el estándar 3G.

Además del aporte en velocidad de acceso a datos, el 3G también tiene una mejora en los protocolos de seguridad y autenticación de los usuarios en una red móvil, es decir, que se puede tener la certeza que el dispositivo móvil está conectado en la red propia del operador y no en una imitación. En el caso de la autenticación, permite hacer una revisión en los equipos de red si el usuario tiene permitido o no el servicio que está solicitando.

1.1.1.5. Cuarta generación (4G)

En la actualidad, el 3G ha alcanzado un estado de madurez del cual no es posible seguir evolucionando en la telefonía móvil, es por eso que se está a las puertas de un nuevo cambio de generación para que su principal objetivo sea brindar unas velocidades de transferencias de datos y acceso mucho mayores a su predecesor.

El 4G está basado en la tecnología LTE, cuya principal función es separar los canales de autenticación y transferencia de datos en toda la red de acceso logrando mejorar la eficiencia de autenticación y seguridad *versus* la transferencia de voz y datos. Esta generación ya está en operación comercial en algunos países de Asia, Europa y América, para este último caso, Estados Unidos ha sido el primer país que posee una red LTE pura, aunque ya hay varias operaciones en América Latina que tiene planeado lanzar el LTE para el 2014.

1.1.2. Funcionamiento general de una red móvil

La telefonía móvil consiste básicamente en la combinación de una red de acceso, una red de conmutación (red de core), una red de datos y una red IP. La combinación de todos estos elementos logra lo que actualmente se conoce como servicios móviles, estos incluyen mensajería de texto y llamadas de voz y datos, entre otros .

La red de acceso es la entrada a la red de servicios, la red de core conmuta hacia los equipos que direccionan el tráfico según la solicitud inicial del acceso y, también brinda la confirmación si un usuario puede utilizar un servicio o no; la red de datos brinda el medio para la validación del usuario y la salida a

internet que la terminal solicita, utilizando un determinado APN y la red IP brinda la comunicación interna de todos los equipos requeridos, para que se cumplan todos los flujos de los servicios.

En la red de acceso se encuentran estaciones transmisoras o receptoras de radio que, dependiendo la tecnología que se tenga, se le llamará estaciones base o BTS para 2G y nodos B para 3G. Esta red es llamada GERAN para GSM (2G) y UTRAN para UMTS (3G).

La red de conmutación consiste en centrales de conmutaciones móviles que no variarán según sea la tecnología utilizada, sin embargo, por la evolución de las redes móviles, si han ido aumentando su capacidad y modelos más robustos han surgido.

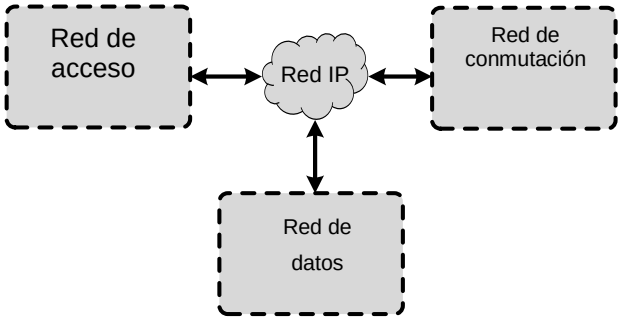
Una función principal del core es posibilitar la comunicación entre terminales móviles y terminales fijas tradicionales.

En general, su funcionamiento se basa en un teléfono móvil, estableciendo comunicación con una estación base y esta a su vez crea la llamada con la red de conmutación que localiza el destino y une a ambos usuarios para el servicio de voz.

Para el caso de una llamada de datos, el teléfono móvil establece comunicación con una BTS o nodo B, que a su vez está asociado con una BSC o RNC, y cada una de estas controladoras está conectada hacia la red de datos que hace las validaciones del usuario con la red de conmutación y finalmente le brinda salida de internet.

La red IP brinda las conexiones a nivel de transporte entre todas las redes de la operación.

Figura 4. **Diagrama de bloques de una red móvil básica**



Fuente: elaboración propia.

1.2. Elementos de una red móvil

Una red móvil se puede dividir en distintas áreas, cada una con una función específica con elementos propios. De acuerdo al objetivo de la investigación, las áreas importantes son:

- Red de acceso
- Red de conmutación
- Red de datos
- Red IP
- Red de cobro

1.2.1. Elementos de la red de acceso

A continuación se presentan los elementos básicos de una red de acceso.

1.2.1.1. BTS

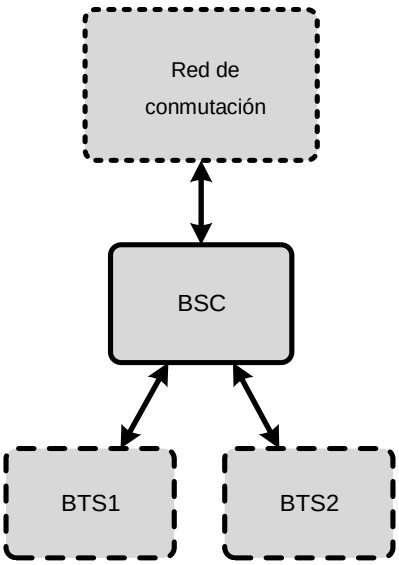
Tienen la función de facilitar la comunicación por la interfaz de aire entre las terminales móviles y la red del operador. Es el primer equipo de la red móvil 2G al cual el usuario se conecta y el que brinda el acceso a la red completa.

1.2.1.2. BSC

Son las controladoras de las BTS, su función principal es el control de uso de los canales de radio y el control del intercambio de usuarios entre BTS (handover), es decir que, si un usuario pierde cobertura de la BTS1, la BTS2 podrá continuar con la llamada sin perder conexión de servicio.

Dependiendo del proveedor una BSC puede tener distinto número de *BTS* bajo su control.

Figura 5. **Red de acceso 2G**



Fuente: elaboración propia.

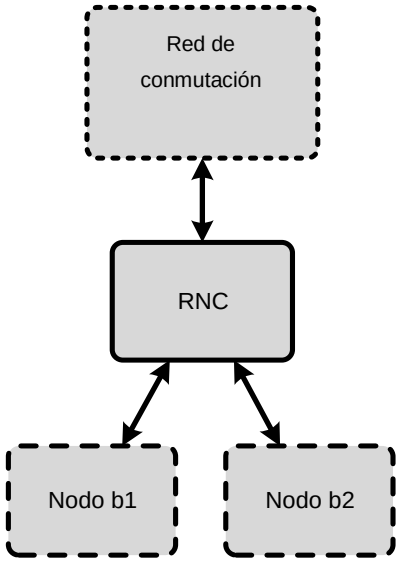
1.2.1.3. Nodos B

Son el equivalente a las BTS en la red 3G y de igual forma su función es facilitar la comunicación por la interfaz de aire entre las terminales y la red del operador. A diferencia de la tecnología GSM, los nodos B utilizan el WCDMA como la tecnología de interfaz de radio

1.2.1.4. RNC

Es el elemento gobernante en la red UMTS y su función principal es el controlar a todos los nodos B conectados a este elemento. Las RNC´s, al igual que las BSC´s, llevan el manejo de los recursos de radio y el control de movilidad o handover.

Figura 6. **Red de acceso *3G***



Fuente: elaboración propia.

1.2.2. Elementos de la red de conmutación

Una red sencilla de conmutación cuenta con elementos como: MSC, HLR, VLR, los cuales son de vital importancia para el funcionamiento de la misma.

1.2.2.1. MSC

Es la responsable de direccionar todas las llamadas de voz y mensajes de texto de una red móvil, además de controlar la movilidad y los requerimientos de handover durante llamadas, y realiza los cobros en tiempo real hacia el sistema de prepago del operador.

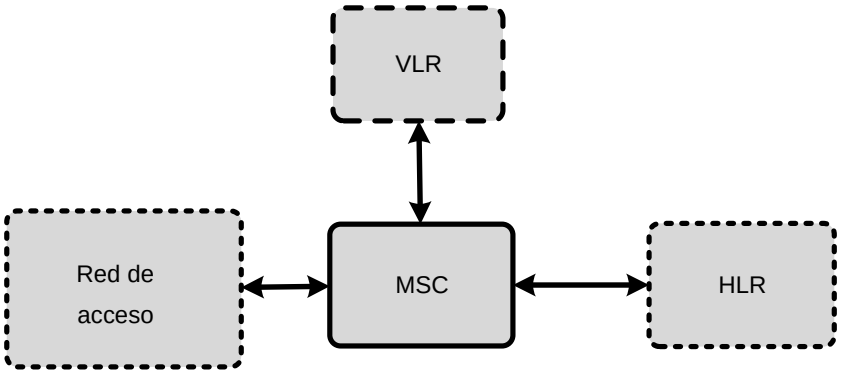
1.2.2.2. HLR

Es una base de datos que almacena la posición del subscriptor dentro de la red, su perfil de usuario, los servicios que tiene disponibles o bloqueados, si está conectado o no, básicamente, contiene toda la información de los usuarios de red móvil.

1.2.2.3. VLR

Es una base de datos volátil, esto quiere decir que, almacena la información de los usuarios que se encuentran activos en ese momento y mantiene una actualización y conexión hacia el HLR de forma constante.

Figura 7. **Red de conmutación móvil**



Fuente: elaboración propia.

1.2.3. Elementos de la red de datos

Esta a diferencia de la red de conmutación cuenta con más elementos ya que es más compleja por el tipo datos que maneja y transmite.

1.2.3.1. SGSN

Es el responsable de la entrega y recepción de los paquetes desde y hacia la terminal móvil, además, en este equipo ocurre la etapa de autenticación y autorización del usuario hacia la red de datos. Una de sus principales funciones es el control de la movilidad o handover de la terminal, esto quiere decir que cada vez que un usuario se conecta a la red de datos, el SGSN obtiene la información de la celda y código de área en donde se encuentra el subscriptor, para que cada vez que hace una actualización de área el equipo pueda encargarse de hacer un handover suave.

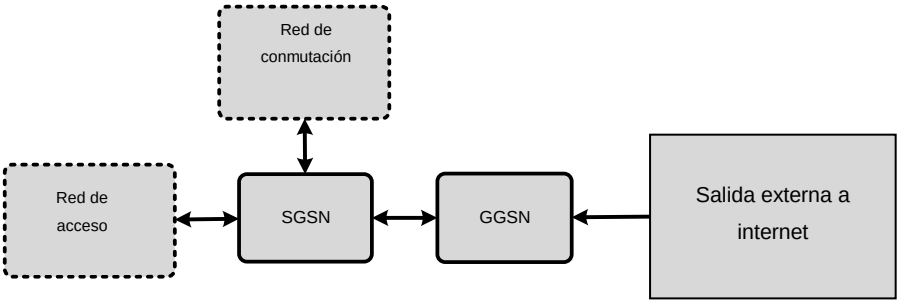
1.2.3.2. GGSN

Es el responsable de encaminar los servicios de datos hacia la red de internet que es una red externa a la red móvil. Básicamente, detecta qué servicio de datos se está solicitando, esto se realiza mediante la detección del APN con el cual llega la solicitud desde la terminal y finalmente asocia este APN con un segmento IP el cual lo envía con destino hacia la red externa de internet o hacia una red interna de WAP.

Otra actividad principal del GGSN es la funcionalidad de túnel directo con la RNC, esto quiere decir que la señalización (autenticación de usuario) es enviada hacia el SGSN, y la transmisión de datos como tal lo hace directo hacia el GGSN, ahorrando de este modo un tiempo de latencia que repercute en una velocidad de transmisión más rápida y que resulta en una mejor experiencia de usuario.

Una gran característica de este equipo es que, además de las funciones de transmisión de datos, también posee funciones de cobro en tiempo real y conexiones hacia equipos de políticas de usuario.

Figura 8. **Red de datos**



Fuente: elaboración propia.

1.2.4. Elementos de una red de cobro

En los siguientes incisos se describen las partes de una red de cobros.

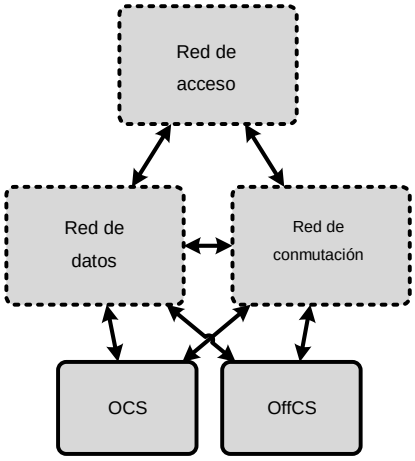
1.2.4.1. OCS

Es el equipo encargado de realizar el cobro en línea, es decir, que cada vez que un usuario de este perfil realiza una llamada de voz, datos o servicios de valor agregado, primero se hace la consulta al OCS y se confirma si posee saldo, si no rechaza el servicio, si posee se debita el costo del balance y se permite completar la llamada.

1.2.4.2. Cobro fuera de línea

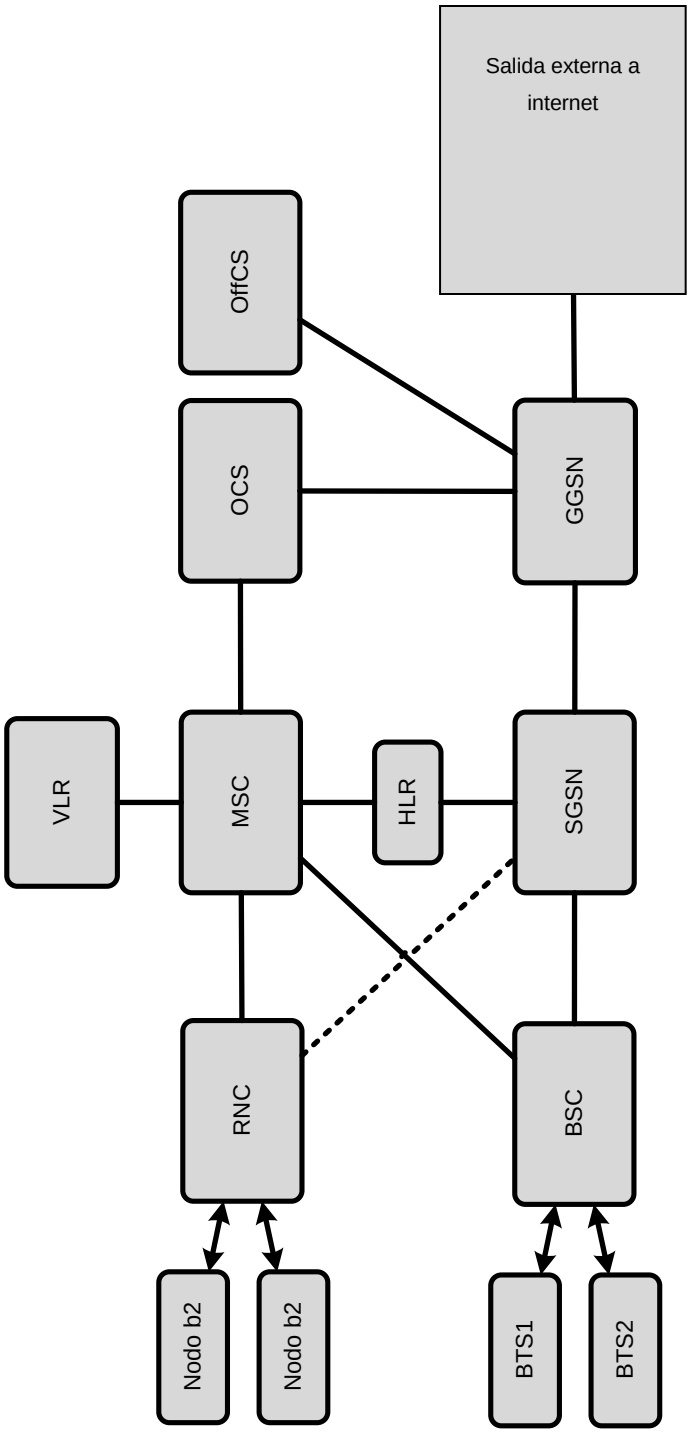
Este equipo se encarga de colectar todos los registros de las llamadas de voz, datos o servicios de valor agregado de tal modo que el cobro se genere al cliente en una factura después de un ciclo de cuenta.

Figura 9. **Red de cobro**



Fuente: elaboración propia.

Figura 10. **Red móvil completa**

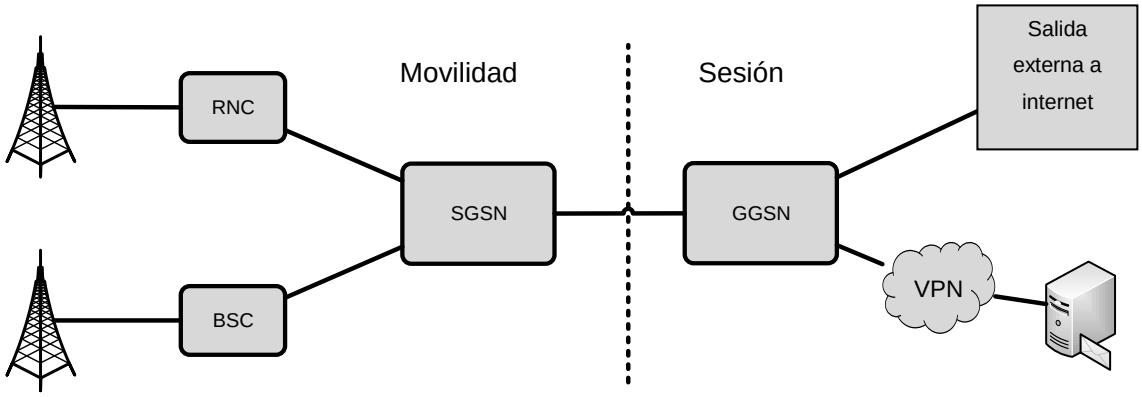


Fuente: elaboración propia.

1.3. Funcionamiento de una red de datos

Para completar una llamada de datos, se requieren de cada etapa y cada componente visto en las secciones anteriores, en sí las redes GSM están compuestas de 2 núcleos (también conocidos como core's); uno para voz y otro para datos, para el caso de los datos, la funcionalidad del core se divide en movilidad y sesión.

Figura 11. **Funcionalidades core de datos**



Fuente: elaboración propia.

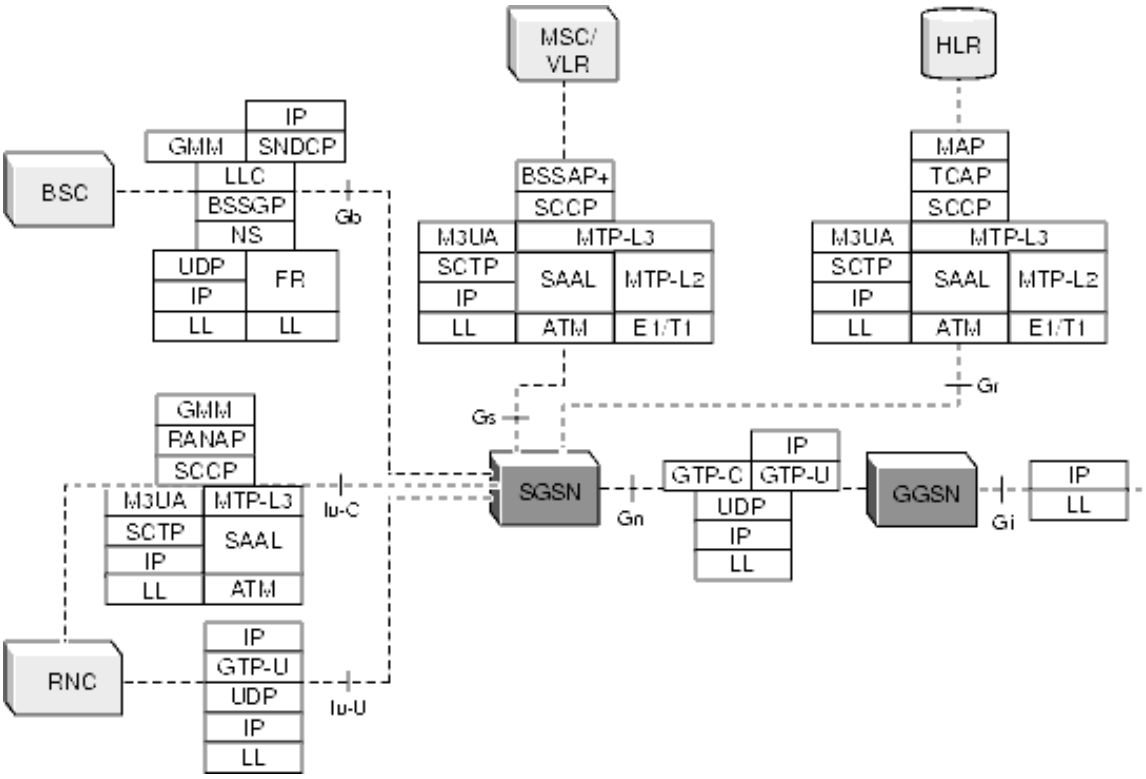
La movilidad corresponde a ubicar físicamente al usuario dentro de la red móvil, recibiendo información exacta del sitio donde se encuentra de parte de la BSC para 2G y RNC para 3G. En esta etapa, también resalta la parte de seguridad, ya que toda la información del usuario se intercambia de forma encriptada manteniendo en confidencia la data del usuario.

La sesión corresponde a la comunicación IP entre el usuario y el destino final, que puede ser la red de internet propiamente o un servidor empresarial alcanzable mediante una VPN o enlace dedicado.

En general, la red de datos debe hacer que tanto la movilidad y la sesión converjan para brindar un servicio estable al usuario final.

En una red de datos, todas las interfaces cumplen distintas funciones por lo que utilizan diferentes protocolos de comunicación y transporte, en sí, estas son las interfaces que están estandarizadas por la 3GPP y que interconectan los equipos de una red de datos:

Figura 12. **Interfaces en una red de datos**



Fuente: curso NOS Cisco Systems.

Para comprender cómo opera una red móvil de datos, es necesario conocer los procesos de señalización que se ejecutan entre la red y las terminales de usuario, ya que con estos se obtiene, almacena y actualiza la

información necesaria para darles acceso a los servicios que los subscriptores requieren. Estos procesos existen tanto en la parte de movilidad como en la de sesión.

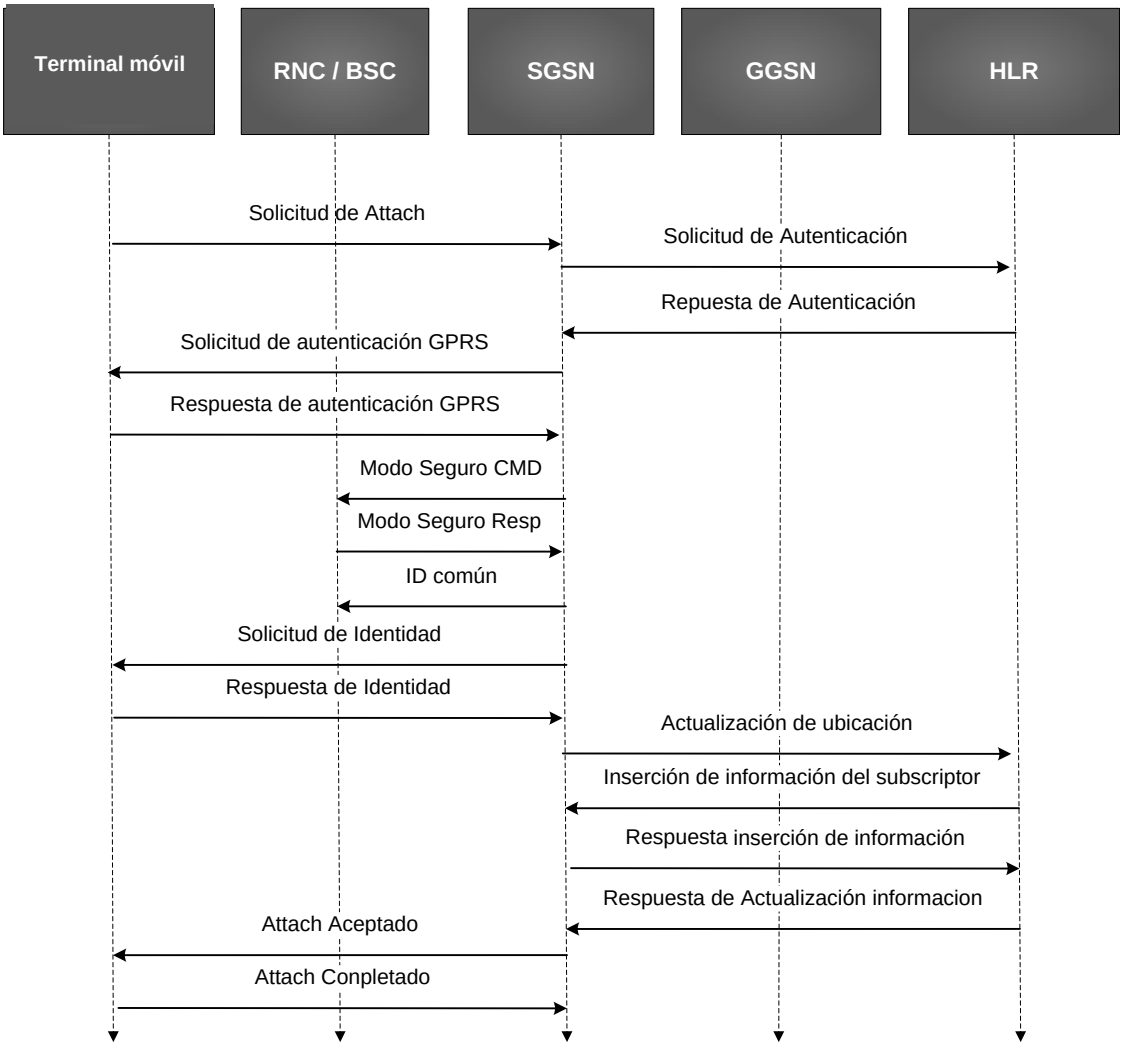
1.3.1. Movilidad

Las redes deben ser versátiles ya que los usuarios que manejan dichas redes deben entenderlas de una manera sencilla y comprensiva.

1.3.1.1. Attach

Es la solicitud que la terminal de usuario envía a la red para su registro en el SGSN, esta comunicación se establece por medio de la interfaz Gr hacia el HLR donde se solicita el perfil de usuario y con base a este el SGSN valida con el usuario, por medio de mensajes encriptados, su identidad. En este proceso se le asigna un ID temporal al usuario (P-TMSI), para que en toda la comunicación los datos puros del subscriptor no sean expuestos en los mensajes de señalización.

Figura 13. **Diagrama de flujo de Attach**



Fuente: elaboración propia.

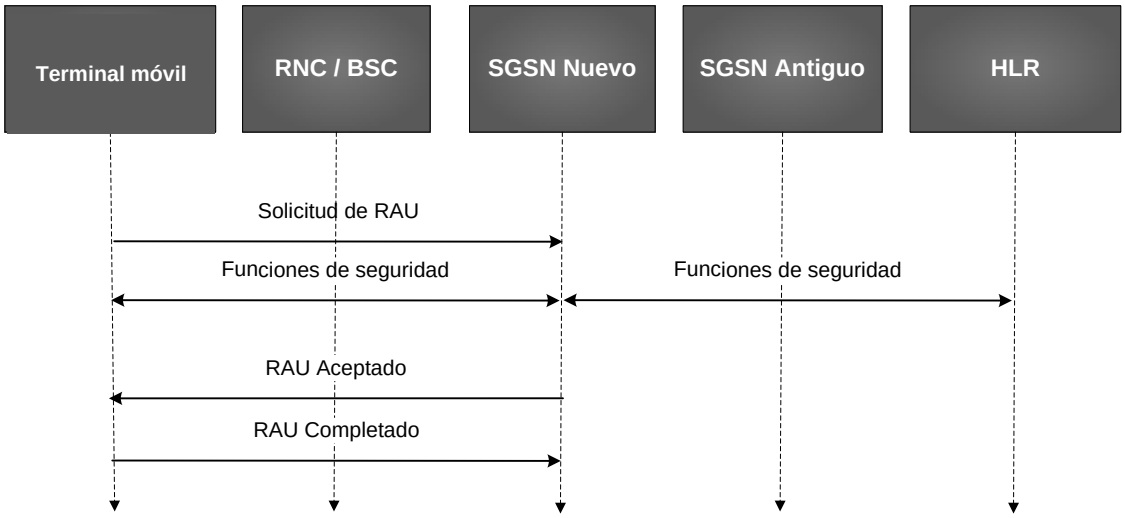
1.3.1.2. Routing Área Update

Cuando el usuario ya está registrado en la red, es necesario mantener su localización geográfica actualizada. Mientras el móvil esté transmitiendo o recibiendo datos, el SGSN sabrá su localización al nivel de celda y bajo este

concepto existen dos escenarios en los cuales esta actualización de área se pueda realizar:

- Cuando el dispositivo móvil detecta un cambio de cobertura, este se mueve a otra celda e inicia el proceso de normal RAU.
- Cuando el dispositivo móvil se encuentra registrado sin hacer un cambio de zona geográfica o sin recibir datos, para este caso el móvil hace una actualización cada cierto tiempo a manera de reportar que se encuentra activo y funcionando, este tiempo lo define el SGSN cuando envía el Attach Accept.

Figura 14. **Diagrama de flujo RAU**



Fuente: elaboración propia.

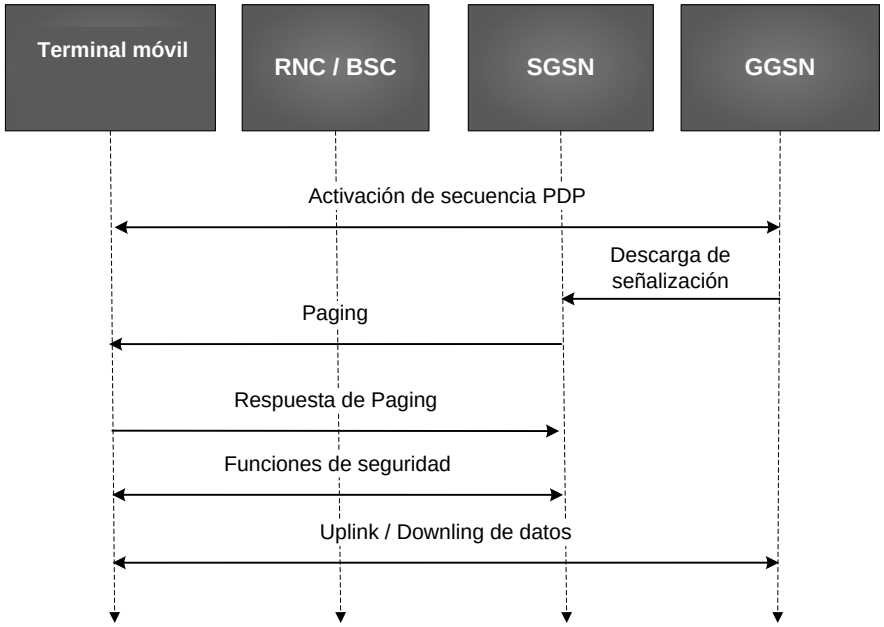
1.3.1.3. PAGING

Este mensaje es utilizado para saber dónde se encuentra el dispositivo móvil y lo envía el SGSN hacia la BSC o RNC utilizando el P-TMSI como

identificador. Este estado es llamado “Standby_Reachable” en GSM y en UMTS es conocido como PMM-IDLE

.

Figura 15. **Diagrama de flujo de Paging**



Fuente: elaboración propia.

1.3.2. Sesión

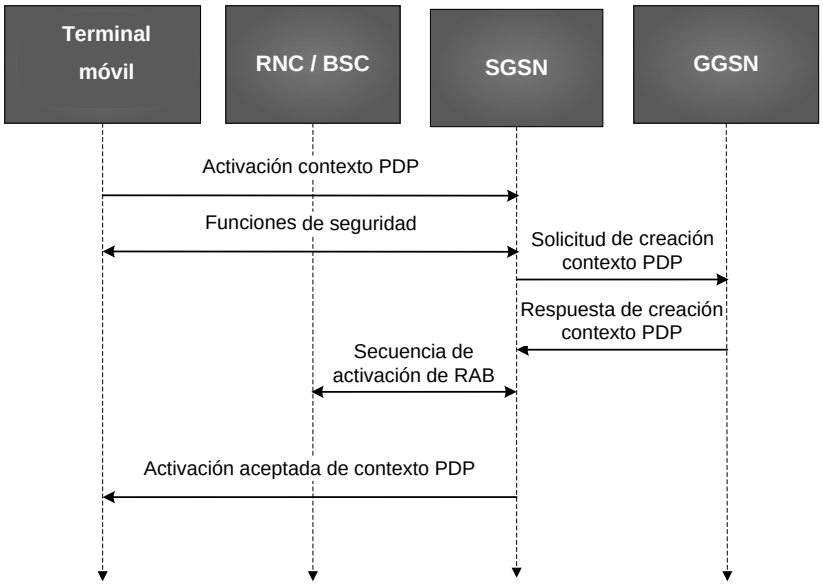
Es la apertura que cuenta con un usuario y una contraseña en la red.

1.3.2.1. Activación de contexto PDP

Este mensaje tiene como finalidad asignarle una dirección IP al dispositivo móvil y lo hace el GGSN. La solicitud de creación de contexto PDP la realiza el SGSN que negocia el QoS con base a los datos obtenidos del perfil de usuario

del HLR y toma en cuenta los recursos disponibles de todos los nodos del core de datos.

Figura 16. **Diagrama de flujo de la creación del contexto PDP**



Fuente: elaboración propia

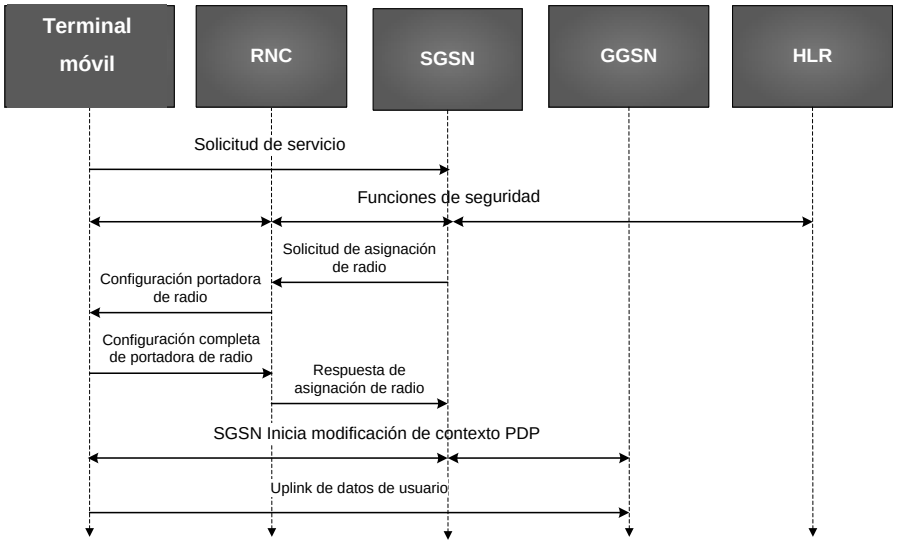
1.3.2.2. Solicitud de servicio

Es un proceso utilizado por las terminales móviles para solicitar recursos de radio y es propio del UMTS.

Este mensaje de señalización se realiza en los siguientes casos:

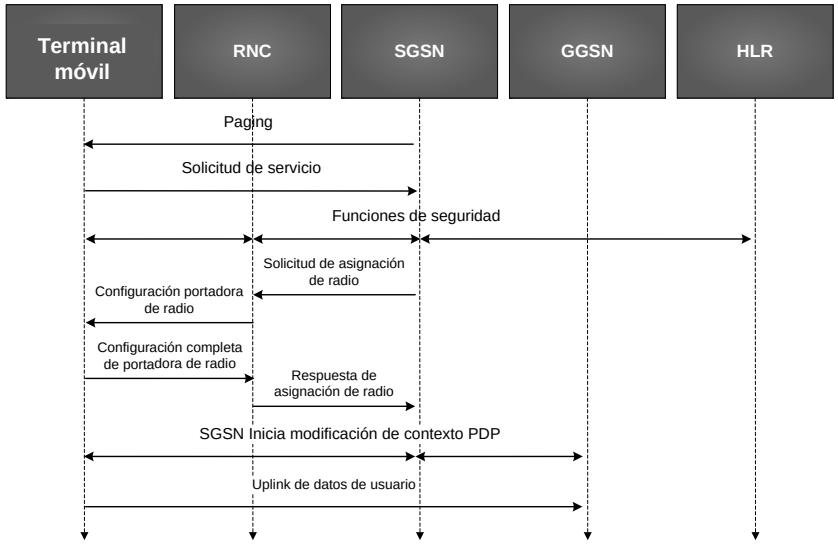
- Cuando el móvil envía datos en uplink sin tener un RAB asignado.
- Cuando un usuario está en estado PMM-IDLE y quiere crear un contexto PDP.
- Cuando el móvil envía una respuesta a un paging recibido.

Figura 17. **Diagrama de flujo solicitud de servicio originado por el móvil**



Fuente: elaboración propia.

Figura 18. **Diagrama de flujo solicitud de servicio originado por la red**

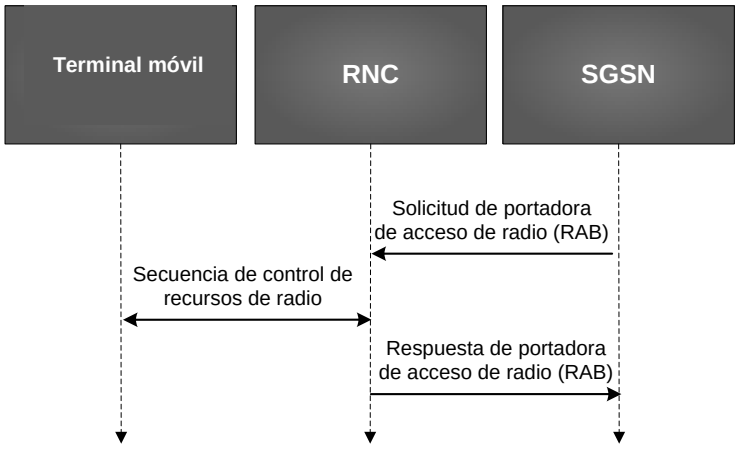


Fuente: elaboración propia.

1.3.2.3. Solicitud de asignación RAB

Es en este proceso donde se reservan todos los recursos necesarios en los dispositivos e interfaces de la RAN para la transferencia de datos y señalización del terminal móvil del usuario.

Figura 19. **Diagrama de flujo de la asignación de recursos de radio RAB**



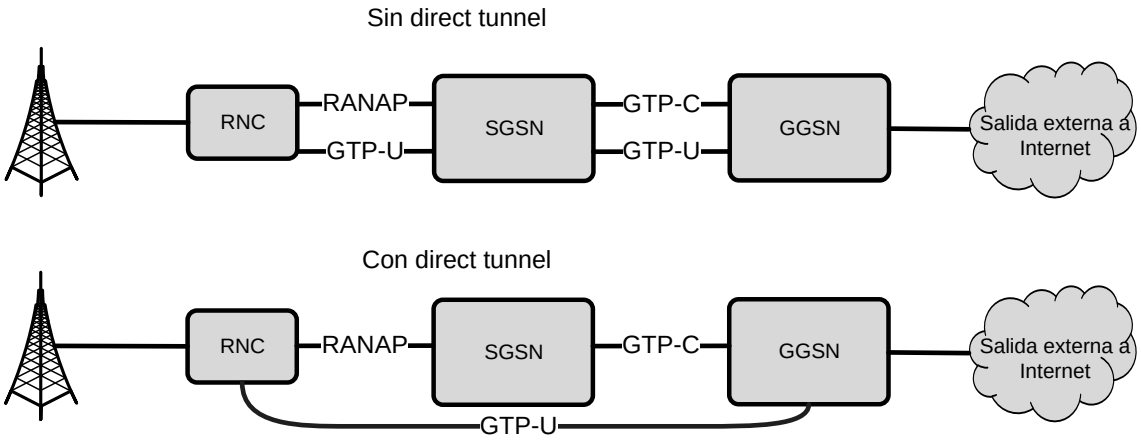
Fuente: elaboración propia.

1.3.3. Direct Tunnel

Esta funcionalidad permite separar el tráfico de señalización y data de los usuarios móviles de 3G únicamente.

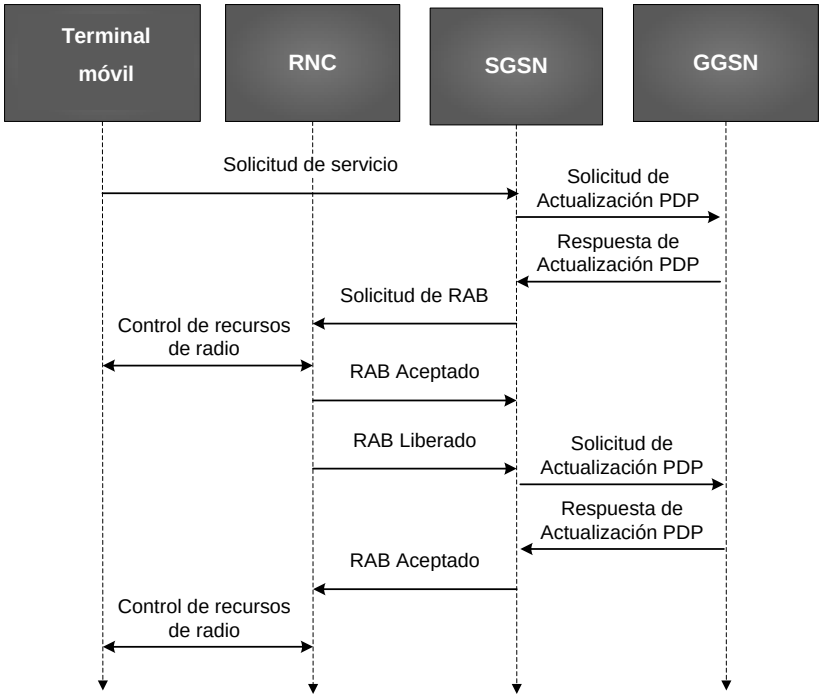
Dado que en las arquitecturas móviles actuales la RNC y GGSN hablan el mismo protocolo, GTP-U, este proceso consiste en crear un túnel desde la RNC hacia el GGSN de forma directa y aun cuando esto está establecido, el control de la señalización, GTP-C, siempre lo mantiene el SGSN.

Figura 20. **Comparación funcionalidad Direct Tunnel**



Fuente: elaboración propia.

Figura 21. **Diagrama de flujo Direct Tunnel**



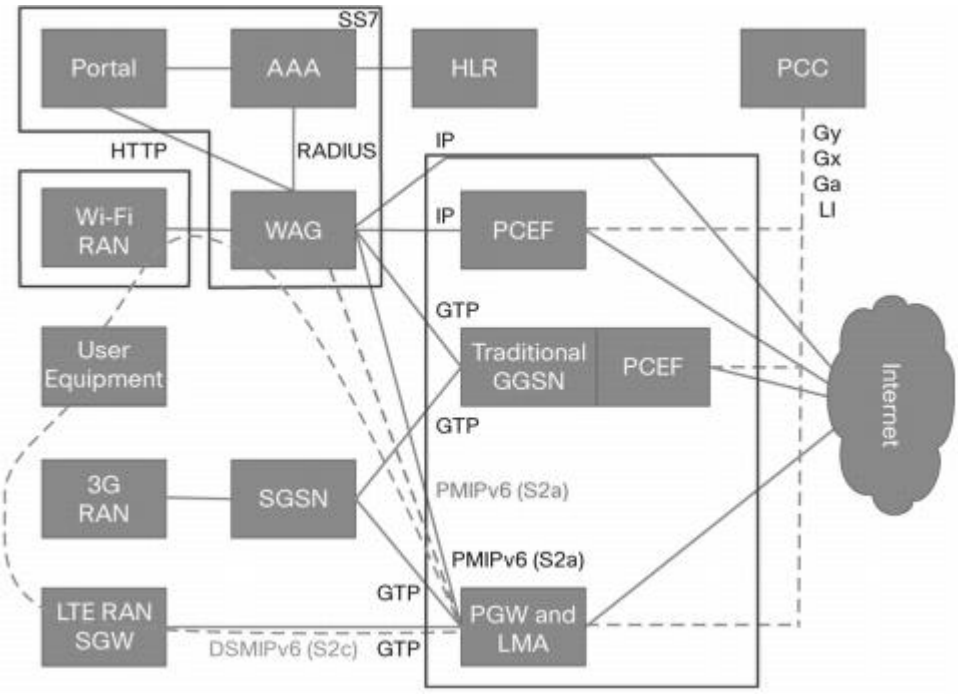
Fuente: elaboración propia.

2. ARQUITECTURA DE RED WIFI PARA DESCARGA DE DATOS MÓVILES

El modelo de descarga wifi, básicamente consiste de tres puntos:

- Acceso
- Autenticación
- Servicio

Figura 22. **Estructura general de una red wifi en 3G y LTE**



Fuente: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white_paper_c11-701018.html. Consulta: 08 de marzo de 2014.

2.1. Acceso

Según la 3GPP se reconocen dos modos de acceso únicamente y dependerá del servicio a brindar, cuál es el que se tiene que utilizar:

- Sin confianza: se refiere a un Hotspot abierto en el cual el operador no tiene el control de las conexiones o brindan un nivel de seguridad bajo.
- De confianza: se refiere a utilizar un modo de autenticación por el aire más seguro y encriptado.

Evidentemente por los niveles de seguridad que ofrece y el modo de confianza, es el más seleccionado para los despliegues de la solución.

La red de acceso está conformada por los dispositivos AP y AC, que haciendo una analogía, serían lo que en 3G son los nodos B y las RNC. Para uno su función es brindar el acceso como tal y el segundo es el controlador de recursos y configuraciones.

2.1.1. Punto de acceso

Es el encargado de radiar el SSID de la red de APs y de establecer comunicación por medio de un túnel GRE hacia el WAG, cuando un usuario está tratando de identificarse en una red wifi o inalámbrica.

El AP, únicamente necesita saber la IP del WAG para establecer el túnel GRE que es un túnel general entre el WAG y toda la red de acceso de APs

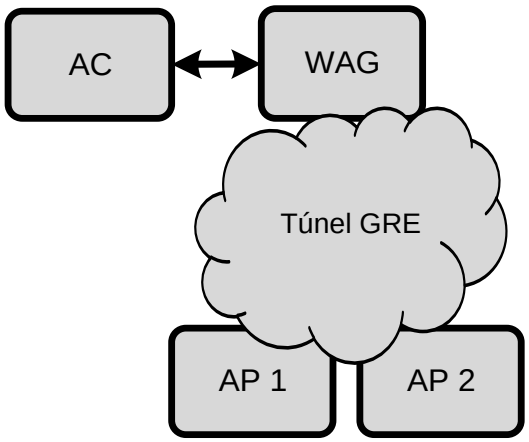
2.1.2. Control de acceso

Conocido como AC, se utiliza para administrar toda la red AP, es decir, por este medio se envían todas las configuraciones a toda la red de APs.

Dependiendo del modelo de AC, este equipo puede segmentar la red completa de AP dividiéndola por zonas, esto facilitaría el poder configurar por sección y no de forma global.

Al igual que una RNC, el AC posee una limitante de cuántos AP puede controlar, esto dependerá también del modelo y del diseño de red que se utilice.

Figura 23. **Diagrama de conexión AC y AP**



Fuente: elaboración propia.

2.1.3. Movilidad

Como en toda red de acceso, una de las funcionalidades más importantes es la movilidad que también es conocida como *handover*, que es cuando un

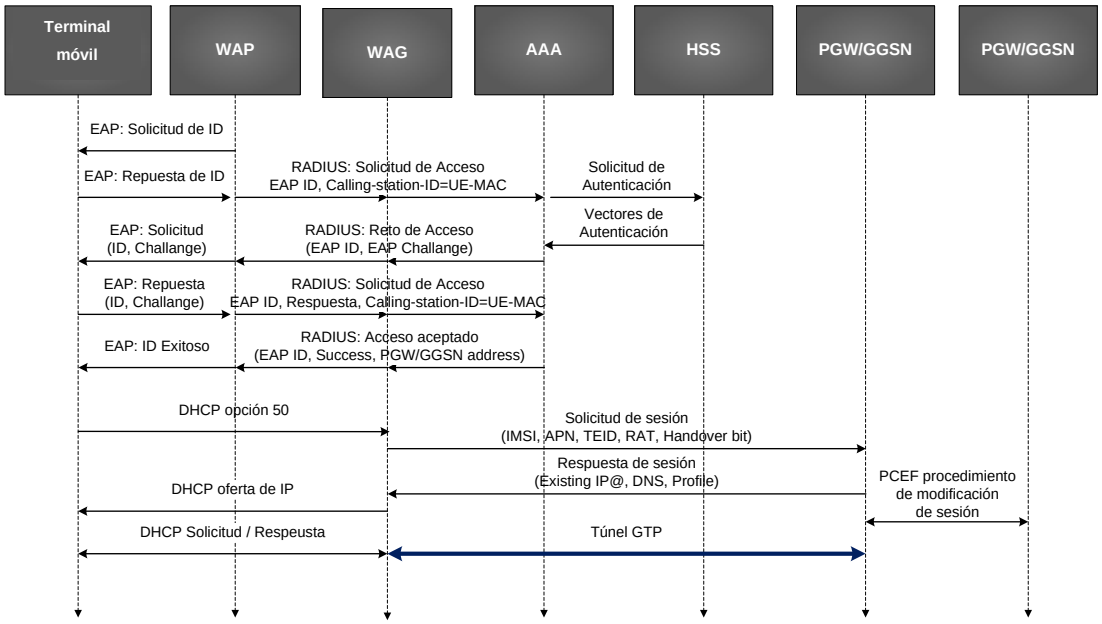
usuario se mueve de una estación de radio hacia otra, en este caso de un AP hacia otro.

Para una red wifi los tipos de handover que se puede encontrar son los siguientes:

- Sin dirección IP persistente: se refiere cuando un usuario se autentica en la red wifi y es esta misma red la que le asigna una dirección IP, la cual se utilizará como origen en la comunicación hacia una red externa. Sin embargo, todas las conexiones TCP o UDP que se establezcan, también pueden seguir siendo utilizadas sobre la red 3G, siempre y cuando este permanezca habilitado en el dispositivo, pero, si el dispositivo deshabilita el 3G estas conexiones tendrán que ser reestablecidas nuevamente desde la red wifi.
- Con dirección IP persistente: es cuando un usuario se conecta en la red wifi y se le asigna la misma dirección IP que tenía previamente en una red 3G o LTE, sin embargo, si las conexiones TCP y UDP están asociadas a una interfaz física tendrán que ser reestablecidas utilizando la nueva interfaz de wifi, sin importar que tengan la misma IP.
- De sesión: se refiere cuando el usuario está utilizando datos en tiempo real como Skype, videos en línea, entre otros y se debe de hacer un cambio de tecnologías de 3G a wifi o viceversa. Para este caso particular no existe un estándar definido, por lo que cuando se da este escenario la sesión se pierde y es necesario iniciar una nueva, esto a nivel de experiencia de usuario no es lo ideal, ya que siempre se buscan los escenarios de handover más transparentes posibles.
- Para LTE: en referencia a este escenario, la 3GPP versión 12 ha definido que el handover de sesión en el escenario de movilidad de wifi a 4G y viceversa, ya sea soportado de tal forma que no importa si se tiene

habilitada una sesión de datos esta no se perderá, independientemente de la red en la que el usuario se encuentre.

Figura 24. **Handover 4G y wifi**



Fuente: elaboración propia.

2.2. Autenticación

Dado que en el sistema wifi no se tiene un método de autenticación de usuarios hacia la red móvil, es importante contar con los elementos necesarios y establecer un diseño óptimo de solución que sí pueda permitir esta acción, certificando de esta forma que son usuarios permitidos únicamente los que hacen uso de un servicio de datos utilizando el acceso wifi.

Se puede utilizar múltiples modos de autenticación para tener el control de conexión del usuario, sin embargo, es importante definir qué método se estará

utilizando, ya que mientras más transparente sea para el cliente, más probabilidades hay de que la red wifi sea utilizada.

El método de autenticación, también puede determinar hacia qué red debe de ser direccionado el subscriptor, en este caso si se le da servicio a visitantes de otros países o usuarios sin una SIM.

Para lograr la funcionalidad de autenticación se debe tomar en cuenta que se puede hacer de dos formas.

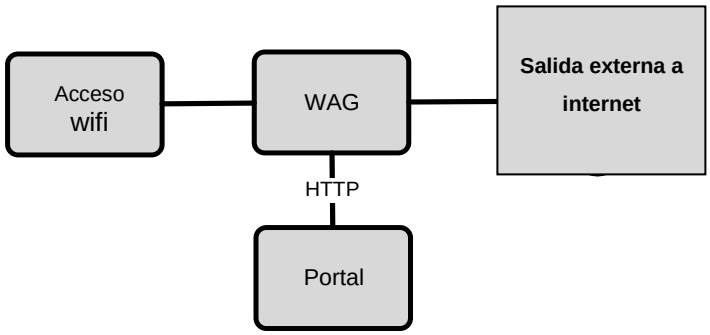
- Autenticación basada en portal: esta es para usuarios que no posean un contrato permanente con el operador.
- Autenticación EAP: esta permite transparencia de conexión de los usuarios hacia la red wifi.

2.2.1. Autenticación basada en portal

Este método está previsto para usuarios que no pertenezcan a la red del operador o que sean visitantes de otros países.

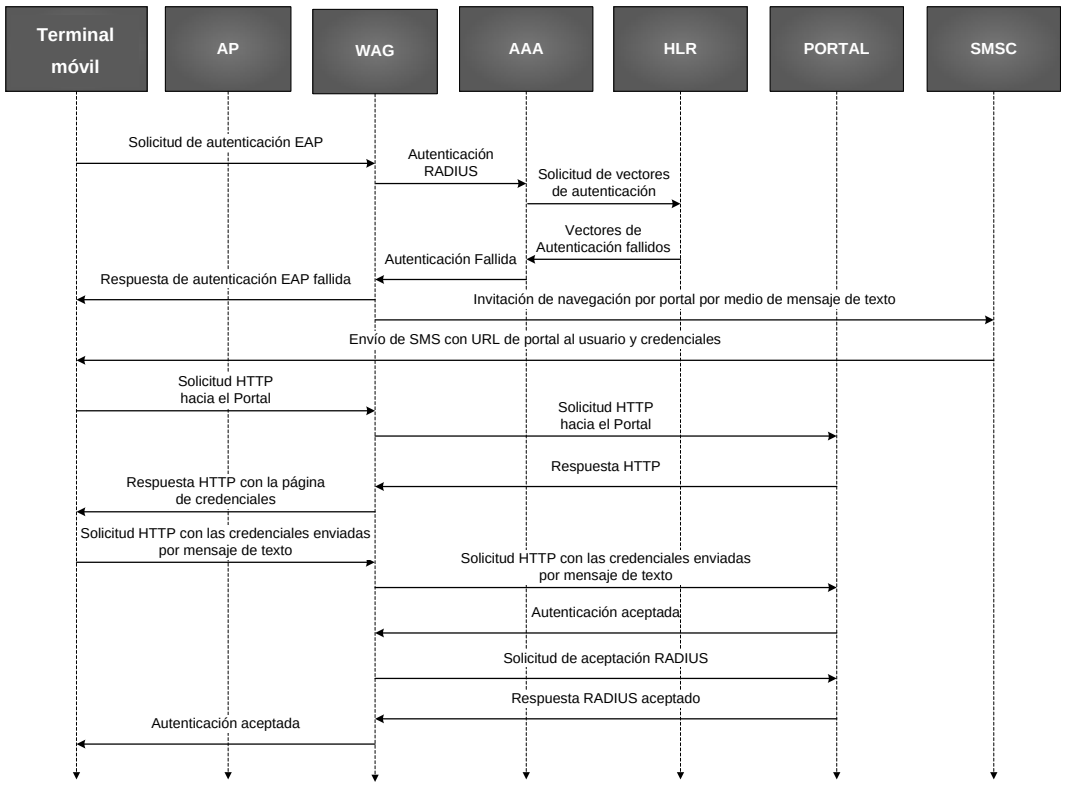
La autenticación basada en portal consiste en tener conexión HTTP hacia un servidor externo que garantice el acceso al servicio para los usuarios visitantes.

Figura 25. **Diagrama general de la autenticación basada en portal**



Fuente: elaboración propia.

Figura 26. **Diagrama de flujo de autenticación basada en portal**



Fuente: elaboración propia.

El método funciona de la siguiente forma: el WAG bloquea toda comunicación IP de un usuario desconocido o nuevo y lo direcciona hacia un portal cautivo, este portal requiere que se ingresen las credenciales enviadas previamente, y una vez validadas las mismas devuelve un disparo de autenticación correcta hacia el WAG que se encarga de completar la llamada de datos.

2.2.2. Autenticación EAP

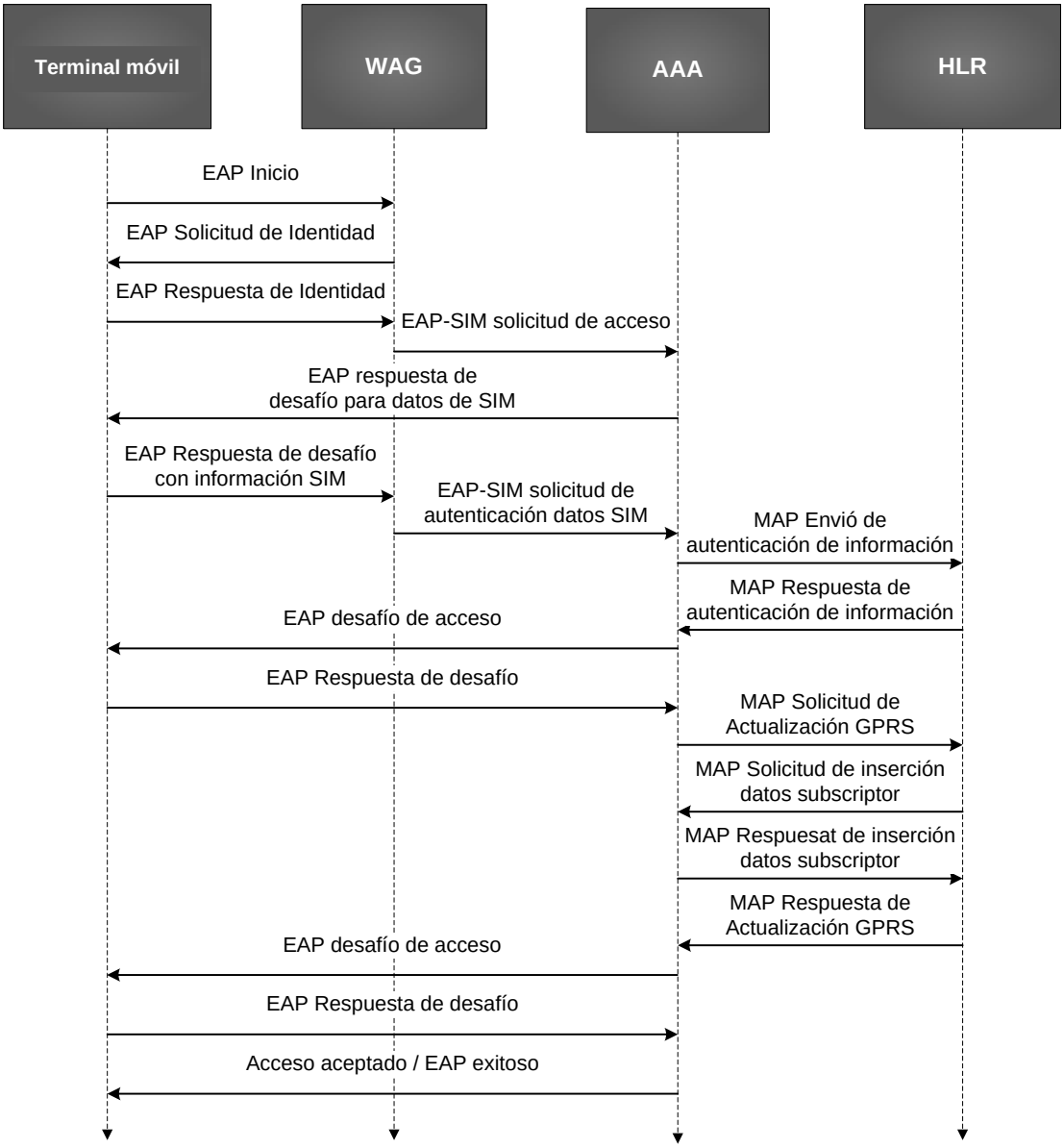
El protocolo de autenticación extensible está definido en la RFC3748 y lo que hace es proveer validación en capa 2 y es utilizado, comúnmente para validaciones de conexiones inalámbricas.

El encapsulamiento de información dependerá del método de EAP a utilizar y para fines de este diseño se estará utilizando 2 únicamente:
EAP-SIM y EAP-AKA

2.2.2.1. EAP-SIM

Modo de autenticación definido para GSM en la RFC4186 y su función es tomar la información de la tarjeta SIM, encapsulándolo dentro del mensaje EAP, enviándolo hacia un servidor de autenticación llamado AAA, ver figura 25.

Figura 27. **Flujo de mensajes de autenticación EAP-SIM**

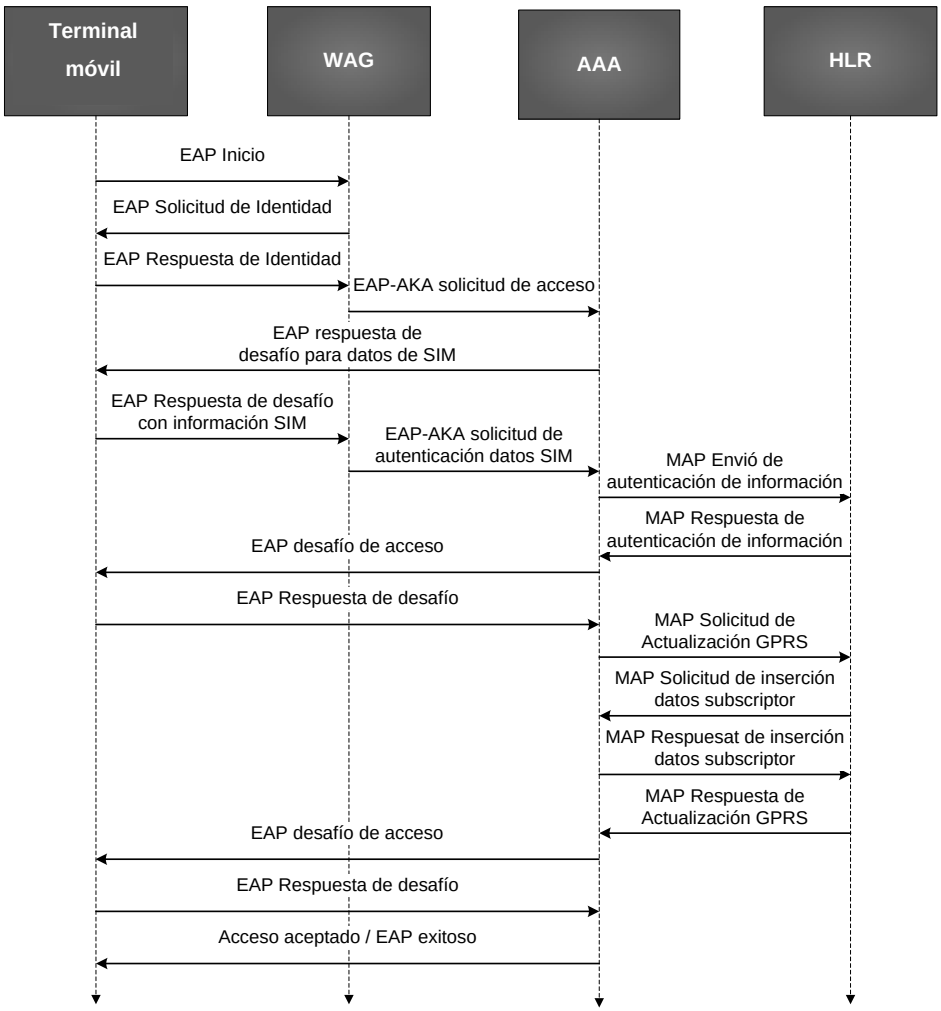


Fuente: elaboración propia.

2.2.2.2. EAP-AKA

El EAP-AKA está definido para UMTS en la RFC4187 y sucede exactamente lo mismo que en el EAP-SIM, envía los mensajes de la USIM encapsulados en los mensajes EAP, ver figura 26.

Figura 28. **Flujo de mensajes de autenticación EAP-AKA**



Fuente: elaboración propia.

2.2.3. Autenticación, autorización y administración de cuentas

Es el equipo encargado de hacer la validación del usuario hacia el HLR por medio del protocolo MAP, en el caso de las redes 3G y en caso que sea una red LTE lo hace vía Diameter con el HSS. Hacia el WAG utiliza una conexión radius.

El AAA, como comúnmente es llamado el equipo, complementa los mensajes EAP-SIM o EAP-AKA que la terminal envía desde el punto de acceso wifi. El EAP envía únicamente el número o MSISDN que tiene la SIM en ese momento y el AAA complementa la acción agregando valores de autenticación propios de la red móvil y envía la solicitud de autenticación hacia el HLR del operador, si el usuario existe le permite el servicio y si no lo deniega, ver figuras 25 y 26,

También existe un método que limita el servicio a usuarios que tengan ciertas características específicas en el HLR y no solo validar si el usuario existe o no en la red del operador. Este método consiste en obtener del HLR toda la información del perfil de usuario que posee y evalúa si el subscriptor que está atendiendo tiene o no aprovisionado un APN específico que hace referencia al servicio wifi; si lo tiene confirma la autenticación del usuario y sino la deniega, esto sirve al operador para vender planes adicionales de wifi y obtener una mejor ganancia del servicio, ver figuras 27 y 28.

2.2.3.1. Protocolo Radius

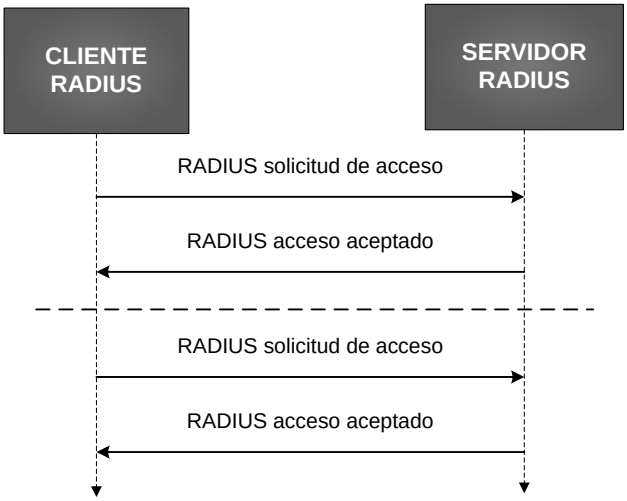
Su principal función es establecer una conexión segura desde accesos inalámbricos por medio de mensajes de autenticación, autorización y administración de cobro hacia los equipos remotos de una red inalámbrica.

Los mensajes de autenticación y autorización están definidos en la RFC2865 en donde se estipula que, para la comunicación se utiliza el protocolo UDP debido a que el algoritmo de retransmisión y los tiempos de respuesta del protocolo TCP no son funcionales a nivel experiencia de usuario.

Para Radius, la RFC2865 define los siguientes tipos de mensajes:

- Solicitud de acceso: primer mensaje enviado desde el usuario hacia un servidor Radius.
- Aceptación de acceso: mensaje del servidor hacia el usuario garantizando la autorización y autenticación
- Rechazo de acceso: negación del servicio de autorización y autenticación al usuario. Pudiéndose dar por fallas en la conexión o simplemente no estaba autorizado su acceso.
- Desafío de acceso: mensaje que se da cuando el servidor Radius solicita una segunda confirmación de acceso al usuario, por ejemplo, cuando le solicita una segunda contraseña o PIN.

Figura 29. **Mensajes de la RFC2865 para autenticación y autorización**



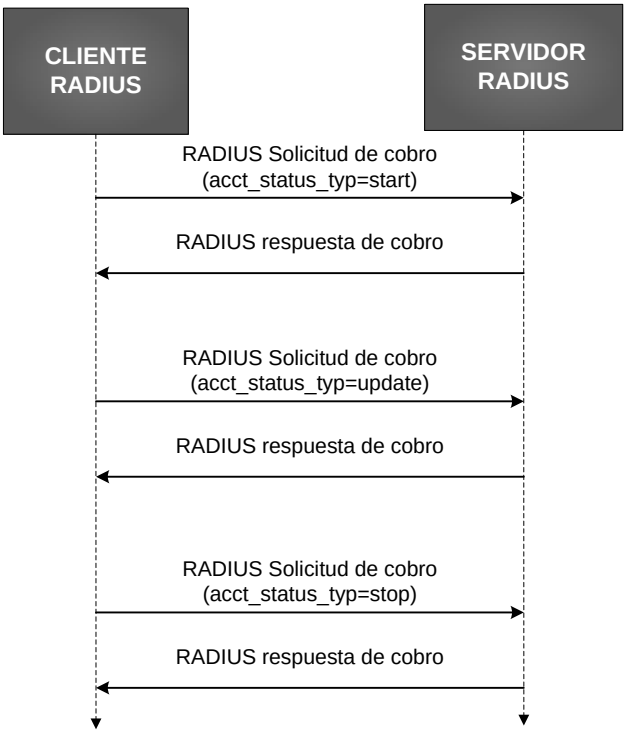
Fuente: http://en.wikipedia.org/wiki/File:Drawing_RADIUS_1812.svg. Consulta: 15 de marzo de 2024.

El mensaje de administración de cobro se define en la RFC2866, se toma como una RFC distinta, ya que son mensajes completamente distintos que los de autenticación y autorización.

Para administración de cobro, la RFC2866 define los siguientes mensajes:

- Solicitud de administración de cobro: se utiliza para el envío de información desde los usuarios hacia el servidor Radius.
- Respuesta de cobro: es la respuesta al mensaje de solicitud iniciado por el usuario.

Figura 30. **Mensaje de la RFC2866 para administración de cobro**



Fuente: http://en.wikipedia.org/wiki/File:Drawing_RADIUS_1813.svg. Consulta 15 de marzo de 2014.

2.2.3.2. Protocolo MAP

Es parte del conjunto de protocolos que se utiliza para señalización SS7 o SIGTRAN.

Su función principal es comunicar el estatus de un usuario dentro de una red móvil, es decir, valída los mensajes de autenticación, autorización y localización de un subscriptor en la base de datos del equipo que soporta este protocolo, que por lo general, son equipos con vastas bases de datos como el HLR.

Autentica y autoriza, tomando en cuenta si el usuario existe y qué perfil posee dentro de la base de datos que tiene cargada el HLR.

La localización del usuario dentro de la red es muy importante por el concepto de movilidad, que sirve para no perder una llamada de voz o datos en la transferencia de cobertura de la red de acceso.

Para una referencia, el protocolo MAP está definido según se utilice para GSM o UMTS de la siguiente forma:

- MAP para GSM, 3GPP TS 09.02
- MAP Para UMTS, 3GPP TS 29.002

2.3. Servicio

Un punto importante a tomar en cuenta es el método de cobro del servicio. Evidentemente al ser un acceso distinto, la red no podrá hacer el cobro al usuario como lo hace actualmente, y nuevas integraciones serían necesarias, sin embargo, existe un método con el cual se puede reutilizar las conexiones existentes de cobro en y fuera de línea que hace la integración más simple y efectiva.

La salida de servicio puede ser de dos formas:

- Salida directa a internet
- Salida por medio del core de datos

2.3.1. Salida directa a internet

Este esquema brinda liberación de carga en el core de datos, especialmente en el GGSN, sin embargo, no posee un control propio de las políticas de navegación de usuario ni respeta la calidad de servicio que el subscriptor ha contratado en su plan de navegación y la responsabilidad del cobro en y fuera de línea recae sobre el equipo AAA, que además de autenticar también llevaría el control de saldo del usuario.

La forma en la que el AAA lleve el control de saldo del subscriptor es por medio de una interfaz diameter o corba hacia el equipo de cobro en línea con el cual intercambiaría el flujo de mensajes de administración de cobro

Para el cobro fuera de línea de este esquema, la plataforma AAA estaría llevando el control de saldo almacenando CDRs que guardan los consumos de los usuarios del servicio, para este control una interfaz FTP deberá ser habilitada hacia los servidores de mediación y facturación que procesen toda la información y gestionen las cuentas de los usuarios.

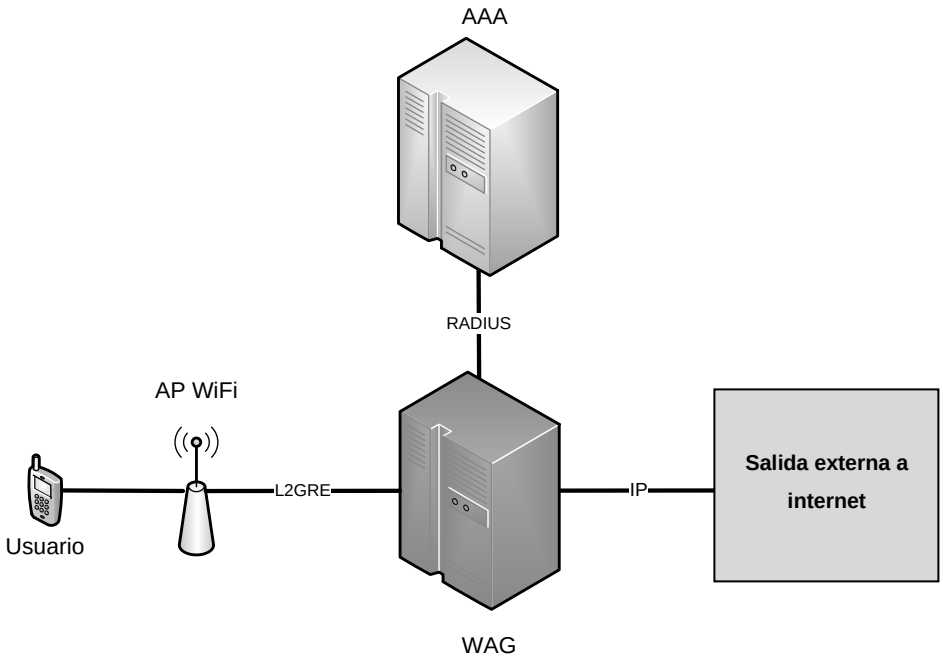
Una vez definido el esquema de cobro, la salida a internet se daría por medio del WAG que llevaría a cabo las siguientes funciones:

- Validar contra el AAA al usuario
- Dar salida a internet por una conexión directa
- Llevar el control de la asignación IP utilizando un proceso DHCP interno

En este último punto, el protocolo DHCP se utiliza para la asignación dinámica de la dirección IP que se le asigna al usuario y, que es necesaria para la comunicación hacia cualquier destino de internet.

La solución con salida a internet directa es simple y efectiva, pero no óptima en relación a lo que una red de telefonía móvil ya posee por lo que es una solución ideal como primera fase de proyecto.

Figura 31. **Esquema de solución con salida directa a internet**



Fuente: elaboración propia.

2.3.2. Salida por medio del core de datos

Este es el método más óptimo y efectivo de la solución total de descarga de datos, este esquema utiliza las conexiones ya existentes que posee la red de datos móvil como lo son el control de políticas de usuario, el cobro en y fuera de línea y la salida de internet que garantiza la calidad de servicio que un usuario adquiere en un plan de datos.

Este diseño está basado en la conexión del WAG, que actúa como SGSN para este caso y el GGSN estableciendo así túneles de transporte GTP para cada usuario, lo que permite establecer una conexión y flujo de datos en el GGSN, independiente para cada subscriptor por medio de una interfaz Gn.

2.3.2.1. Protocolo GTP

Está basado en IP y tiene como función encapsular los mensajes GPRS entre los nodos SGSN y GGSN, tanto de señalización como de usuario utilizando como medios de transporte los protocolos UDP o TCP.

El protocolo GTP, dependiendo qué mensajes transmite, se desglosa de la siguiente forma:

- GTP-C: protocolo por el que viajan los mensajes de señalización que establece una sesión PDP entre el SGSN y GGSN, constituye los parámetros de calidad de servicio y actualiza la información de movilidad de los usuarios, es decir, si un usuario cambia de cobertura, o si acaba de arribar a un SGSN proveniente de otro.
- GTP-U: protocolo por el que viajan los mensajes de servicio como tal, es decir, los datos de navegación de usuarios hacia la red de internet.
- GTP': puede ser utilizado para envíos de cobro.

2.3.2.2. Interfaz Gn

Es la encargada de comunicar el GGSN y SGSN (el WAG en este caso), utilizando el protocolo de transporte GTP, el cual permite establecer túneles independientes por cada usuario asignándole un identificador de túnel (TunnelID) para señalización y otro para tráfico de usuario. Estos identificadores

serán en lo de adelante el único modo de diferenciar los paquetes pertenecientes a cada usuario en la comunicación que se dé entre los equipos mencionados, WAG y GGSN.

Los túneles GTP se establecen durante la activación de la sesión PDP y en este punto no hay discriminación de tecnología, es decir que no importa si el usuario está en cobertura GSM o UMTS, el trato será siempre el mismo.

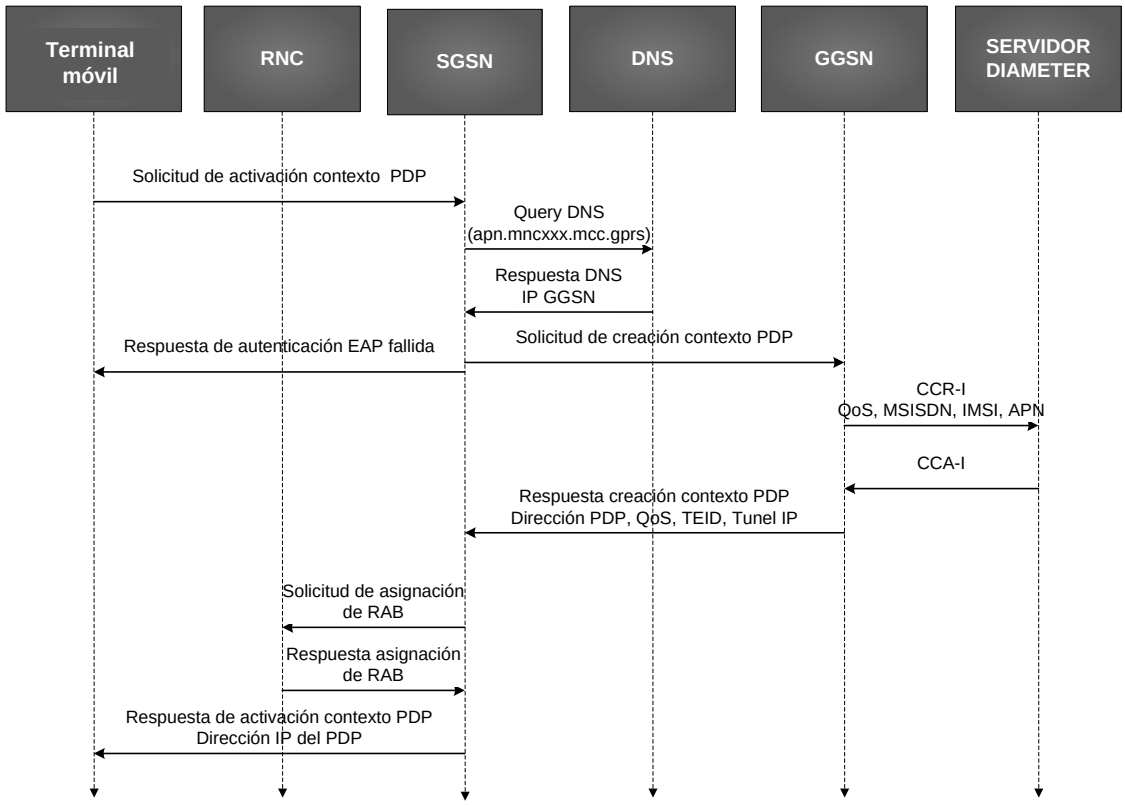
Teniendo claro el modo de transporte y comunicación entre el WAG y el GGSN, este esquema requiere, como último paso, la asignación de una IP por medio de un APN y poder así establecer el servicio de navegación.

2.3.2.3. APN

Se utiliza en el GGSN y hace referencia a un nombre de dominio para resolución de un segmento de IP´s de las cuales se asigna una por usuario. Permitiendo establecer la conexión hacia una red destino que puede ser interna o externa y en este caso internet.

El APN puede ser un diferenciador de servicios, lo cual permite configurar protocolos de encriptación o de autenticación y cobro distintos para cada uno.

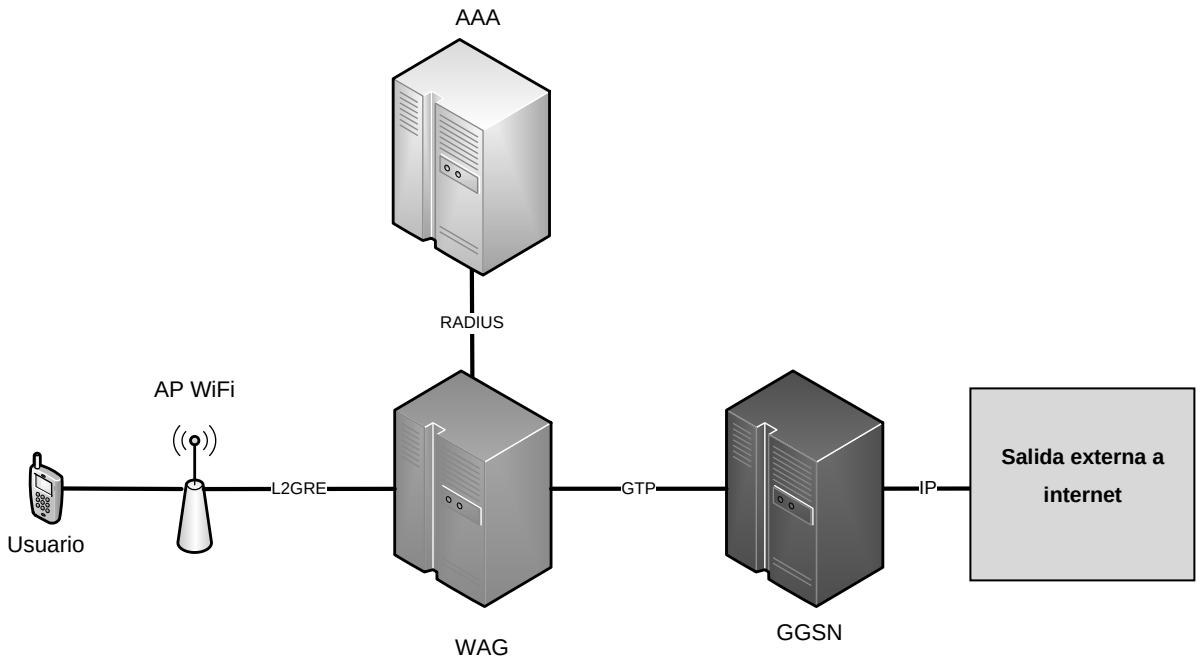
Figura 32. **Flujo de activación APN**



Fuente: elaboración propia.

El máximo logro de este esquema es utilizar las políticas de control de datos y las interfaces de cobro en línea que ya posee el GGSN, esto hace más corto el tiempo de ejecución del proyecto y permite mantener el control de los ingresos del servicio. Es importante mencionar que para estas conexiones se utiliza el protocolo diameter en las interfaces Gy y Gx

Figura 33. **Esquema solución con salida por medio del core de datos**



Fuente: elaboración propia.

2.3.2.4. Protocolo Diameter

Está definido en la RFC6733 y es la versión mejorada de Radius que al igual que este, Diameter también tiene como función autenticar, autorizar y administrar el cobro de los usuarios, sin embargo, a diferencia de su antecesor, Diameter está basado en protocolos de transporte más confiables como TCP o SCTP y no UDP, por lo que en este protocolo ya existen las retransmisiones a nivel de transporte.

En la tabla I se enumeran los mensajes que existen a nivel de protocolo:

Tabla I. **Listado de mensajes en Diameter**

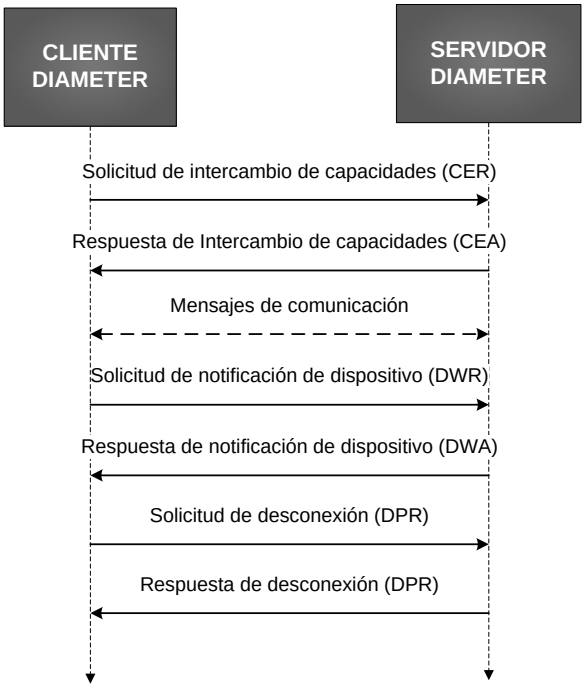
Nombre del mensaje	Abreviación	Código
AA-Request	AAR	265
AA-Answer	AAA	265
Diameter-EAP-Request	DER	268
Diameter-EAP-Answer	DEA	268
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Credit-Control-Request	CCR	272
Credit-Control-Answer	CCA	272
Capabilities-Exchange-Request	CER	257
Capabilities-Exchange-Answer	CEA	257
Device-Watchdog-Request	DWR	280
Device-Watchdog-Answer	DWA	280
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	275
User-Authorization-Request	UAR	300
User-Authorization-Answer	UAA	300
Server-Assignment-Request	SAR	301
Server-Assignment-Answer	SAA	301
Location-Info-Request	LIR	302
Location-Info-Answer	LIA	302
Multimedia-Auth-Request	MAR	303
Multimedia-Auth-Answer	MAA	303
Registration-Termination-Request	RTR	304
Registration-Termination-Answer	RTA	304
Push-Profile-Request	PPR	305

Continuación de la tabla I.

Push-Profile-Answer	PPA	305
User-Data-Request	UDR	306
User-Data-Answer	UDA	306
Profile-Update-Request	PUR	307
Profile-Update-Answer	PUA	307
Subscribe-Notifications-Request	SNR	308
Subscribe-Notifications-Answer	SNA	308
Push-Notification-Request	PNR	309
Push-Notification-Answer	PNA	309
Bootstrapping-Info-Request	BIR	310
Bootstrapping-Info-Answer	BIA	310
Message-Process-Request	MPR	311
Message-Process-Answer	MPA	311
Update-Location-Request	ULR	316
Update-Location-Answer	ULA	316
Authentication-Information-Request	AIR	318
Authentication-Information-Answer	AIA	318
Notify-Request	NR	323
Notify-Answer	NA	323

Fuente: http://en.wikipedia.org/wiki/Diameter_(protocol). Consulta: 01 de abril de 2014.

Figura 34. **Diagrama de flujo de mensajes Diameter**



Fuente: elaboración propia.

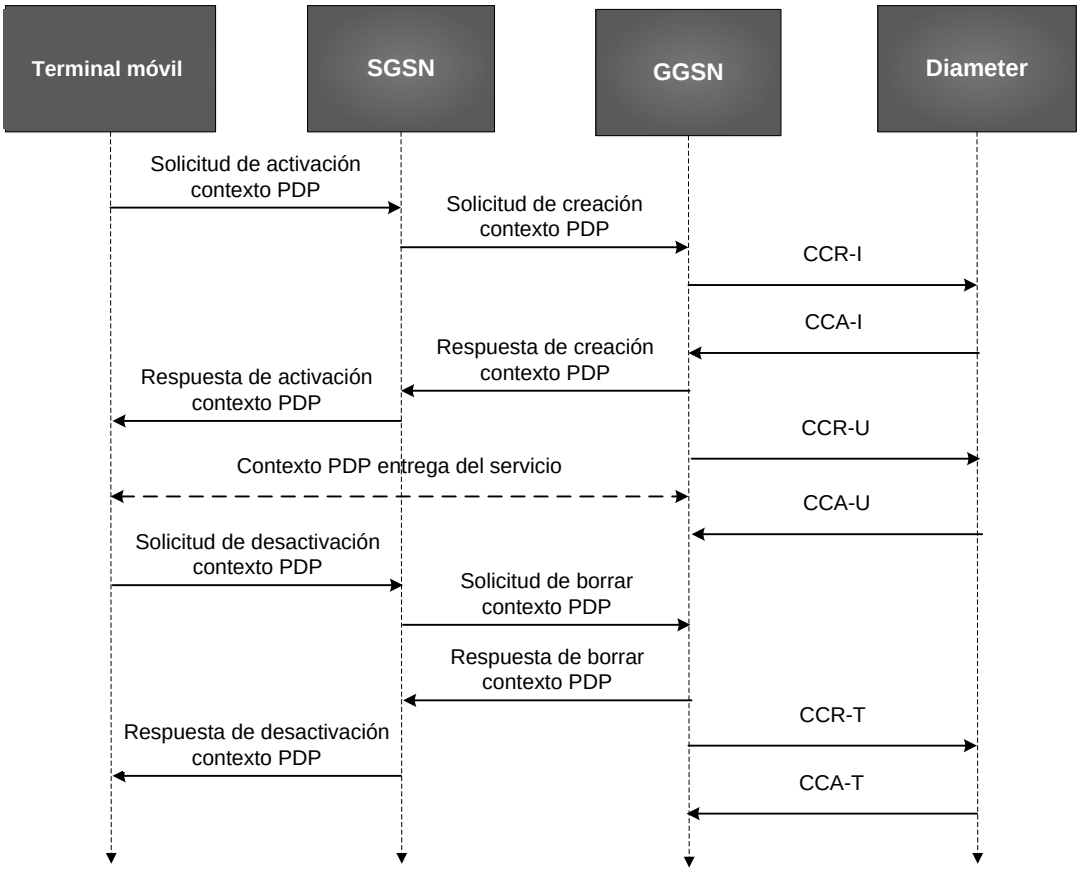
2.3.2.5. Interfaz Gy

Está basada en el estándar 3GPP TS32.299 y sirve para la interacción en tiempo real entre el GGSN y el OCS por medio del protocolo DCCA sobre diameter, lo que permite realizar cobro, ya sea por volumen o tiempo, esto se define por medio de configuración en ambos equipos.

La interfaz Gy utiliza el sistema de cobro diferenciado para la clasificación del tráfico y basa su funcionamiento en la utilización de cuotas parciales que pueden ser de la siguiente forma:

- Unidades de débito: GGSN solicita una cantidad de unidades de cuota que puede o no ser asociada a un grupo de cobro en específico.
- Unidades de reserva: GGSN solicita un crédito al OCS y en ambos equipos este crédito se asocia con un grupo de cobro en específico

Figura 35. **Diagrama de flujo interfaz Gy**



Fuente: elaboración propia.

2.3.2.6. Interfaz Gx

Se utiliza para la comunicación por medio de diameter entre el GGSN y el equipo que controla las reglas de datos o PCRF, básicamente se utiliza para aprovisionar o eliminar las reglas de datos a cada usuario de acuerdo a los planes de cobro establecidos y qué plan tenga contratado el subscriptor.

GGSN se encarga de aplicar las políticas que envía el PCRF para cada usuario y su función principal en esta comunicación es el siguiente:

- Aplicar la calidad de servicio (QoS) correspondiente sobre el tráfico de cada subscriptor.
- Detección de los diferentes flujos de tráfico y las interacciones necesarias para su cobro.
- Bloquear el tráfico de acuerdo a las políticas instaladas por el PCRF y clasificar el tráfico con base a ellas.
- Reportar los eventos de movilidad asociados al tráfico de los usuarios.

La función principal del PCRF es enviarle las políticas de cómo va a controlar el tráfico de cada usuario al GGSN, estas se dividen de la siguiente forma:

- Aplicar las políticas que corresponden a cada tráfico de cada usuario
- Permitir o no un flujo de datos específicos
- Reportar cada evento que pasa con cada subscritor
- Aplicar la calidad de servicio a cada usuario
- Asignar las reglas de cobro diferenciado

3. INTEGRACIÓN DE LA SOLUCIÓN DE UTILIZACIÓN DE DATOS MÓVILES CON ACCESO POR WIFI

El alcance del proyecto está dado para implementar una solución de tipo interior, esto quiere decir que los sitios para desplegar infraestructura serán de tipo cerrados y dependiendo el caso puede considerarse algún despliegue de tipo exterior.

Para lograr la integración del proyecto es necesario considerar separar en dos partes la implementación del mismo:

- Despliegue de acceso
- Integración del core wifi a la red del operador

3.1. Despliegue de acceso

En esta etapa ya es necesario evaluar y tomar en consideración toda información necesaria dentro de la red, para decidir qué dispositivos colocar y la ubicación geográfica de los mismos.

Dentro de la información que puede ser evaluada se sugiere la siguiente:

- Cantidad de usuarios por zona o por LAC.
- Cantidad de tráfico de datos por LAC, ya sea 2G o 3G.
- Ubicación geográfica de los sitios con más caídas de llamadas.
- Ubicación geográfica de los sitios con más intentos fallidos de conexión.

- De ser posible, tener identificados qué tipo de dispositivos se encuentran activos en la red móvil.
- Identificar en qué zonas se concentra la mayor cantidad de dispositivos inteligentes.

De lo anterior es preferible contar con la información de los dos primeros puntos, por sector de la radio base o nodo B y así tener una mejor idea de la orientación hacia la que será necesario el despliegue de los AP.

La idea de saber qué tipo de terminales están activos en la red y de saber en qué zona geográfica se concentra la mayor cantidad de dispositivos inteligentes, es porque no todos los teléfonos celulares soportan la autenticación por EAP-SIM o EAP-AKA, por esta razón es muy importante conocer el comportamiento de la red y sus usuarios para que con base a eso se pueda realizar la mejor inversión de soluciones móviles.

Tabla II. **Lista de dispositivos móviles que soportan EAP-SIM**

Marca	**Modelo**	**EAP**	**EAP a partir de SO**
Alcatel	6030 Idol	EAP-SIM	Android (4.1.1 Jelly bean)
Apple	Iphone *4G*	EAP-SIM	i-OS (6.1.3)
Apple	Iphone 4S	EAP-SIM	i-OS (6.1.3)
Apple	Ipad mini	EAP-SIM	i-OS (6.1.3)
Apple	Ipad 3	EAP-SIM	i-OS (6.1.3)
Apple	Ipad 4	EAP-SIM	i-OS (6.1.3)
Apple	Iphone *3G*	EAP-SIM	i-OS (6.1.3)
Apple	Iphone *3G* S	EAP-SIM	i-OS (6.1.3)
Blackberry	8220	EAP-SIM	Blackberry(5)
Blackberry	8320	EAP-SIM	Blackberry(5)
Blackberry	8900	EAP-SIM	Blackberry(5)
Blackberry	9000	EAP-SIM	Blackberry(5)

Continuación de la tabla II.

Blackberry	9300	EAP-SIM	Blackberry(6)
Blackberry	9320	EAP-SIM	Blackberry(7.1)
Blackberry	9360	EAP-SIM	Blackberry(6)
Blackberry	9500	EAP-SIM	Blackberry(5)
Blackberry	9700	EAP-SIM	Blackberry(6)
Blackberry	9780	EAP-SIM	Blackberry(6)
Blackberry	9800	EAP-SIM	Blackberry(6)
Blackberry	9860	EAP-SIM	Blackberry(7)
Blackberry	9790	EAP-SIM	Blackberry(7)
Blackberry	9900	EAP-SIM	Blackberry(7)
Blackberry	8520	EAP-SIM	Blackberry(5)
Blackberry	Z10	EAP-SIM	BB10
Huawei	Y210	EAP-SIM	Android (2.3 Gingerbread)
Huawei	Y300	EAP-SIM	Android (4.1.1 Jelly bean)
LG	Optimus G	EAP-SIM	Android (4.1.2 Jelly bean)
LG	Optimus L1 II	EAP-SIM	Android (4.1.2 Jelly bean)
LG	Optimus L3 II	EAP-SIM	Android (4.0.1 Ice Cream Sandwich)
LG	Optimus L5 II	EAP-SIM	Android (4.0.1 Ice Cream Sandwich)
LG	Optimus L7 II	EAP-SIM	Android (4.0.1 Ice Cream Sandwich)
LG	Optimus G2	EAP-SIM	Android (4.1.2 Jelly bean)
LG	Optimus L9	EAP-SIM	Android (4.0.1 Ice Cream Sandwich)
Motorola	Moto G	EAP-SIM	Android (4.3.3 Jelly bean)
Motorola	Moto X	EAP-SIM	Android (4.2.2 Jelly bean)
Motorola	Razr D3	EAP-SIM	Android (4.1.2 Jelly bean)
Motorola	Razr Hd	EAP-SIM	Android (4.1.2 Jelly bean)
Motorola	Razr I	EAP-SIM	Android (4.1.2 Jelly bean)
Nokia	Lumia 620	EAP-SIM	Windows 8 AMBER
Nokia	Lumia 720	EAP-SIM	Windows 8 AMBER
Nokia	Lumia 1020	EAP-SIM	Windows 8 AMBER
Nokia	Lumia 920	EAP-SIM	Windows 8 AMBER

Continuación de la tabla II.

Nokia	Lumia 520	EAP-SIM	Windows 8 AMBER
Samsung	Galaxy Core	EAP-SIM	Android (4.1.2 Jelly bean)
Samsung	Galaxy Fame	EAP-SIM	Android (4.1.2 Jelly bean)
Samsung	Galaxy Note	EAP-SIM	Android (4.1.2 Jelly bean)
Samsung	Galaxy Note 2	EAP-SIM	Android (4.0.1 Ice Cream Sandwich)
Samsung	Galaxy Note 3	EAP-SIM	Android (4.3.3 Jelly bean)
Samsung	Galaxy S Advance	EAP-SIM	Android (4.1.2 Jelly bean)
Samsung	Galaxy S2	EAP-SIM	Android (4.1.2 Jelly bean)
Samsung	Galaxy S3	EAP-SIM	Android (4.0.1 Ice Cream Sandwich)
Samsung	Galaxy S3 Mini	EAP-SIM	Android (4.1 Jelly bean)
Samsung	Galaxy S4	EAP-SIM	Android (4.2.2 Jelly bean)
Samsung	Galaxy S4 mini	EAP-SIM	Android (4.2.2 Jelly bean)
Samsung	Galaxy Tab2 7	EAP-SIM	Android (4.1.2 Jelly bean)
Samsung	Galaxy Tab10.1	EAP-SIM	Android (4.1.2 Jelly bean)
Sony Ericsson	Xperia L	EAP-SIM	Android (4.1.2 Jelly bean)
Sony Ericsson	Xperia S	EAP-SIM	Android (4.1.2 Jelly bean)
Sony Ericsson	Xperia ZL	EAP-SIM	Android (4.1.2 Jelly bean)

Fuente: elaboración propia.

http://www.personal.com.ar/AdManager/carpeta_iframes/nuevo_site/individuos/servicios/personal_*WiFi*/terminales_eap_*WiFi*.pdf. Consulta: 26 de abril de 2014.

En paralelo al análisis se pueden iniciar a considerar los proveedores de la solución para la parte de acceso, algo muy importante es que tanto el AP como el AC sean del mismo proveedor, la razón de esto es para no tener conflictos a nivel de equipo durante las configuraciones, actualizaciones y tareas de

operación y mantenimiento de los AP. Dentro de los proveedores más destacados en el ambiente de telecomunicaciones y redes inalámbricas se pueden considerar: Cisco, Ruckus, Huawei, Meraki y Ericsson.

Otro punto importante a considerar es el modo de conexión entre los AP, el AC y el core wifi. Esta conexión dependerá mucho de la ubicación geográfica en la que se hará el despliegue de los nuevos equipos inalámbricos. Ahora bien, tomando de referencia lo anterior, la comunicación entre los equipos de acceso y el core pueden ser divididos de acuerdo al medio: RAN y MPLS.

3.1.1. Despliegue utilizando la RAN del operador

El fin del proyecto es descargar la parte de datos de la red del operador, por lo que realmente es indiferente si un usuario se encuentra en cobertura 2G, 3G o incluso en algunos países 4G.

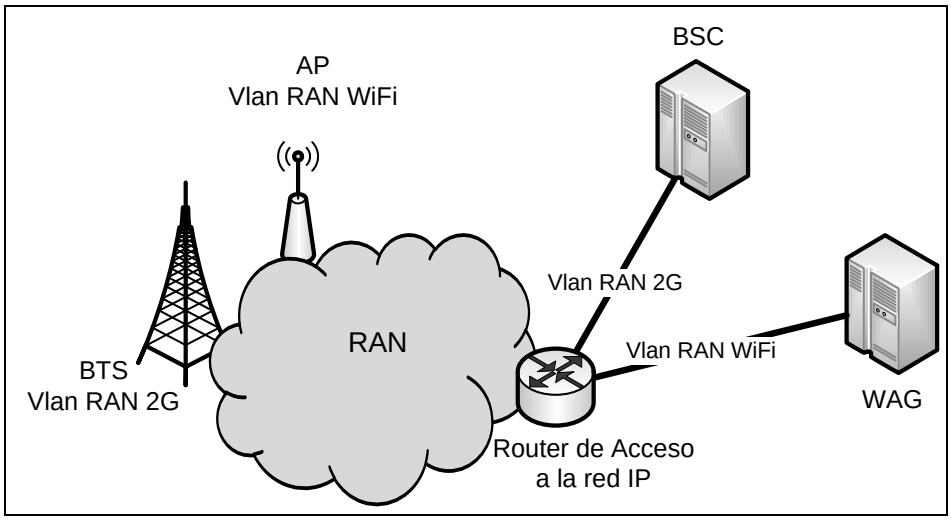
Partiendo de esto, se puede aprovechar el despliegue RAN de cualquier tecnología con la que ya cuente el operador y conectar el AP en los equipos de transporte a los que está conectada la radio base, permitiendo a que la red de acceso wifi sea instalada de una forma inmediata y ahorraría costos en adquirir equipos de transmisión para esta nueva RAN.

Las redes de acceso de 2G y 3G tienen, básicamente la misma estructura la red de 4G sí varia de las dos anteriores.

3.1.1.1. GERAN

Es como se define la red de acceso para 2G y los elementos de red que la conforman son las BSC y BTS. El propósito principal es controlar el radio *link* entre las terminales móviles y la red de core del operador.

Figura 36. **Diagrama de conexión AP red GERAN**

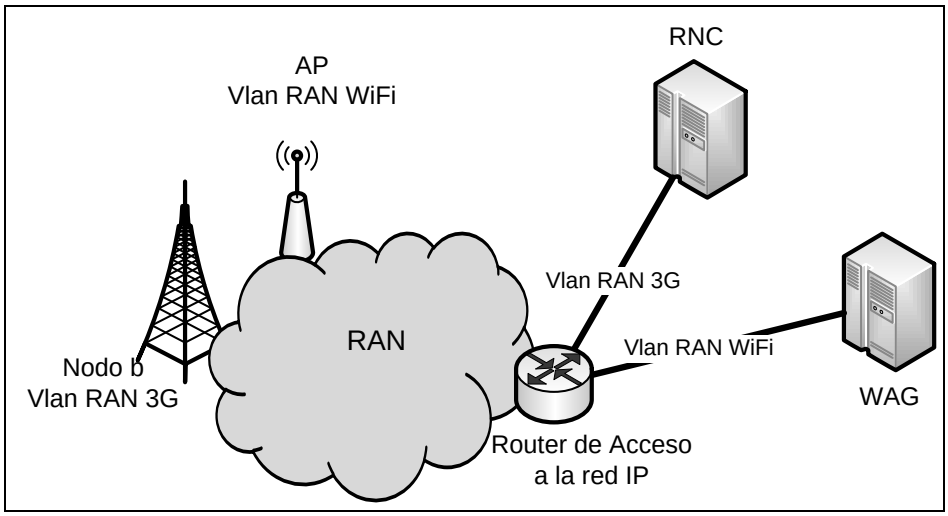


Fuente: elaboración propia.

3.1.1.2. UTRAN

Es como se define la red de acceso 3G y consta de RNC y nodos B, los cuales llevan el control de movilidad del usuario y proveen funcionalidades a nivel de datos que ayudan a una transmisión más rápida y eficiente.

Figura 37. **Diagrama de conexión AP red UTRAN**



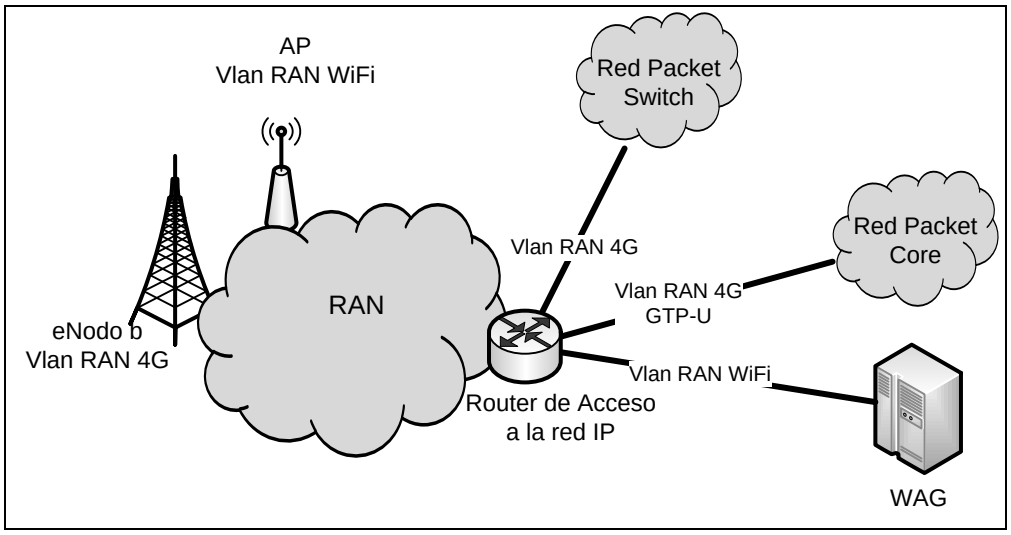
Fuente: elaboración propia.

3.1.1.3. eUTRAN

Es como se define la red 4G y está conformada por los enodos B únicamente. La diferencia de esta red de acceso es que no existe un controlador que centralice todos los enodos B como lo hace la RNC para 3G y la BSC para 2G.

Todos los enodos B llegan directo hacia el *packet switch* y *packet* core del operador.

Figura 38. **Diagrama de conexión AP red eUTRAN**



Fuente: elaboración propia

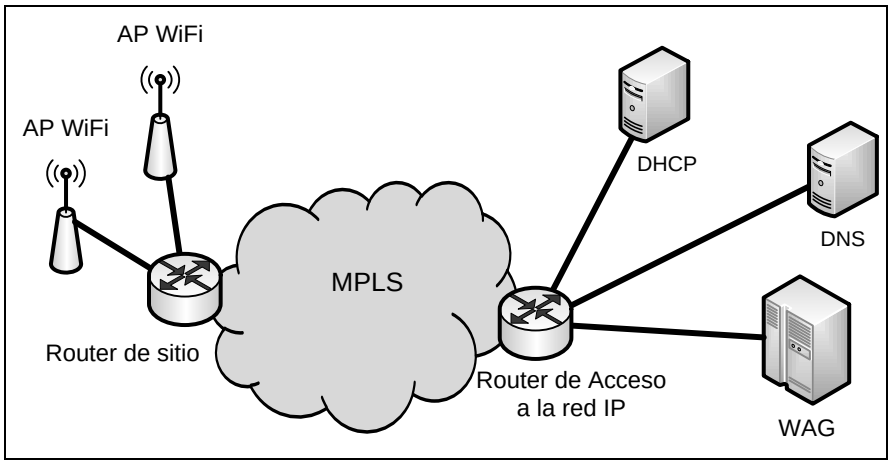
3.1.2. Despliegue utilizando la MPLS del operador

Una segunda opción de conexión es integrar la RAN de wifi directamente hacia la red MPLS del operador, sin embargo, esto dependerá de los sitios que tengan equipos de transmisión que lo permita, por ejemplo, sitios con enlaces empresariales.

3.1.2.1. Red MPLS

Está definida en la RFC3031 y su principal objetivo es unificar las redes de circuitos y paquetes y además, centralizar el tráfico IP y de voz.

Figura 39. **Diagrama de conexión AP red MPLS**



Fuente: elaboración propia

La desventaja de esta opción es que si el *router* del sitio donde se está planeando instalar los AP no posee más interfaces físicas, será necesaria la instalación de más equipo, ya sea con un *router* nuevo o con alguna tarjeta de expansión para el *router* actual. Dependiendo de cuál sea la situación puede implicar un despliegue más tardado y costoso.

Un adicional en esta opción es necesario contar con un servidor DHCP y un servidor DNS, que en caso de no contar con estos equipos será necesario adquirirlos.

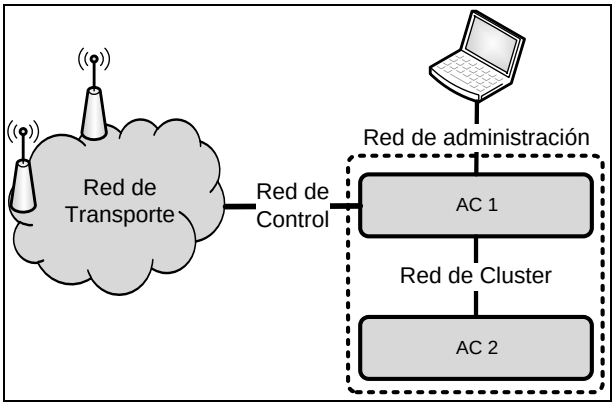
Independientemente de ambos casos, es importante notar que para establecer la comunicación entre los AP y el core de wifi, a nivel de IP se hará por medio de una VRF nueva que aislará y separará el tráfico wifi del resto que puede ser de voz o datos de la red macro 2G o 3G y de los paquetes de datos IP de la red MPLS.

Una vez se haya definido el despliegue de los equipos AP, es necesario considerar los requerimientos para que los AC pueden aplicar su función de control y administración de la RAN de wifi, tomando en cuenta lo anterior lo que el o los AC necesitan en primera instancia es la asignación IP de los equipos y su integración a la red del operador. Como mínimo los recursos necesarios son 3 redes divididas de la siguiente forma:

- Red de control: esta red será necesaria para la configuración de la RAN de WiFi.
- Red de clúster: es necesaria para la redundancia de los AC.
- Red de administración: esta red se utilizará para la operación y mantenimiento de todos los AP desplegados, es decir toda la RAN de WiFi del operador.

Lo anterior mencionado es lo necesario para implementar la parte de acceso para la red wifi, al menos en una fase inicial.

Figura 40. **Diagrama de conexión AC**



Fuente: elaboración propia

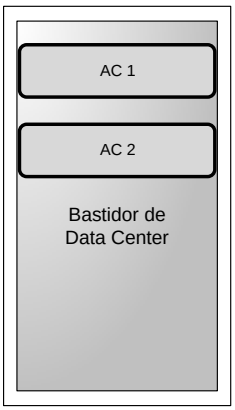
3.1.3. Instalación física del equipo

El equipo debe ser ubicado en un lugar que posea una temperatura ambiente ya que este tiene a generar calor superior de los 60 centígrados.

3.1.3.1. Equipo de control de acceso, AC

Son básicamente dos servidores robustos, las características de energía e infraestructura dependerán en mucho del proveedor con el que se esté trabajando pero en cualquier caso serán instalados en la sala de equipos (Data Center) del operador.

Figura 41. **Diagrama de instalación física en bastidor de los *AC***



Fuente: elaboración propia.

3.1.3.2. Equipo de puntos de acceso, AP

La elección de los AP dependerá si serán instalados en interiores o exteriores y para cada caso existen diversos modelos y proveedores con especificaciones similares y algunas funcionalidades propias de cada uno.

Para instalar los AP ya sea interior o exterior es necesario hacer un análisis de las condiciones del sitio y específicamente para los exteriores es necesario tomar en cuenta las condiciones climáticas bajo las que pueden ser expuestos de tal forma que las puedan soportar. Todos estos análisis deben hacerse junto con el proveedor elegido ya que al final, ellos son los expertos por ser los dueños del producto.

Dentro del análisis que se debe de realizar es necesario tomar en consideración la cantidad de usuarios o tráfico que estaría cursando el equipo, la distancia en cobertura que puedan llegar a alcanzar, la sensibilidad a la polarización de onda, si soportan la energización por Ethernet (POE), por mencionar algunas. Al día de hoy, los AP poseen una tecnología inteligente que permite ser flexibles en cuanto al lugar físico de instalación por lo que es necesario evaluarlos a nivel funcionalidades.

3.2. Integración del core wifi a la red del operador

La integración hacia la red del operador del core wifi ya es menos complejo que el análisis del acceso por la simple razón de que son equipos que se encuentran en un data center fijo que ya posee equipos de transmisión que brindan la integración a la red del operador.

La integración de esta etapa consta de los equipos WAG, AAA y GGSN/PGW, se toma en cuenta el equipo del core de datos dado que es necesaria la integración hacia él a pesar de que ya se encuentre instalado en la red del operador.

3.2.1. Integración AAA

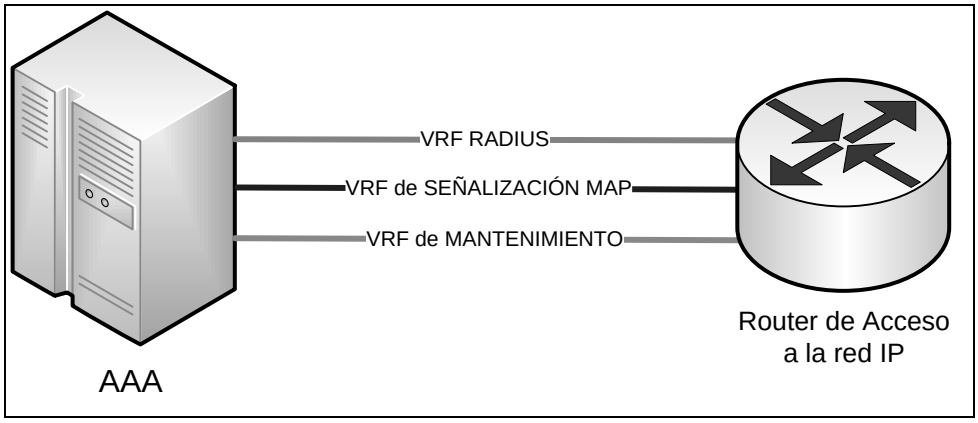
Los requisitos de integración del AAA a la red del operador deben contener como mínimo la asignación de tres redes IP que se dividen de la siguiente forma:

- Red de Radius: utilizada para la comunicación de autenticación y autorización del usuario entre el WAG y el AAA.
- Red de señalización: necesaria para la comunicación MAP entre el AAA y el HLR. Sobre esta interfaz se autentica si un usuario puede utilizar o no el servicio.
- Red de mantenimiento: utilizada para los procesos de operación y mantenimiento sobre la plataforma de AAA.

Con base en esta información se puede definir que la integración hacia los equipos de red del operador puede ser sobre una sola interfaz y cada tráfico de las redes mencionadas se pueden separar lógicamente por medio de capa 3 del modelo OSI, sin embargo, lo recomendable es separarlo físicamente en interfaces independientes y aprovechar de esta forma las capacidades de la plataforma. Esta separación es por capa 2 del mismo modelo.

Estos son los requisitos mínimos para que la solución funcione, existen varios proveedores con diferentes modelos que pueden variar la solución agregando otras funcionalidades pero siempre mantendrán los requisitos mencionadas anteriormente.

Figura 42. **Diagrama de conexión plataforma AAA**



Fuente: elaboración propia.

3.2.2. Integración WAG

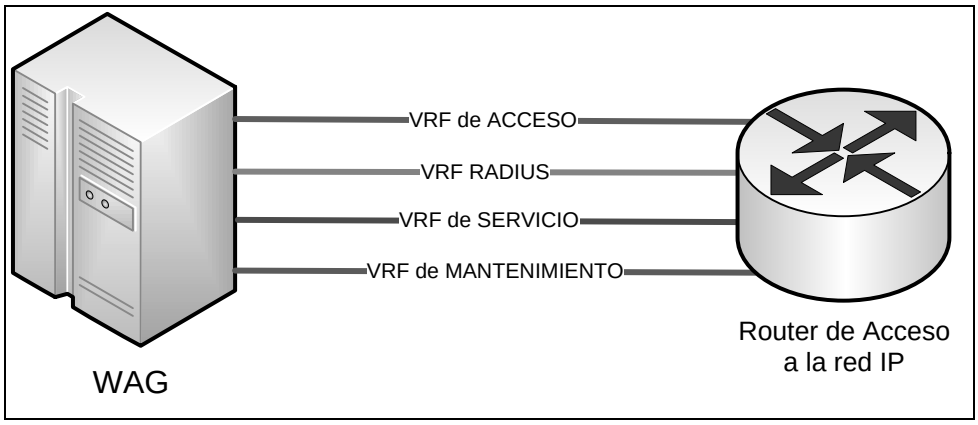
La integración de esta plataforma es crucial para el proyecto completo, es sobre el cual pasará todo el tráfico de autenticación y datos del usuario, además de brindar la conexión de capa 2 del AC de la parte de acceso.

Evidentemente el WAG estará concentrando todas las comunicaciones entre los equipos del core de wifi, por tal razón requiere más recursos que los otros equipos, como mínimo las redes que necesita el WAG son las siguientes:

- Red de acceso: brinda la comunicación que establece el AP hacia el WAG creando el túnel GRE para la transferencia de datos.
- Red de RADIUS: se utiliza para el tráfico de autenticación del usuario hacia el AAA.

- Red de servicio: interfaz que comunica el WAG con el GGSN estableciendo el túnel GTP sobre el cual se transfiere el tráfico de datos de la RAN de wifi.
- Red de mantenimiento: interfaz, por la cual se administra el equipo y se atiende en caso de una falla con el servicio.

Figura 43. **Diagrama de conexión plataforma WAG**



Fuente: elaboración propia.

Un punto a considerar son los siguientes parámetros que son indispensables en la comunicación entre el AAA y el WAG:

- Alc-Subsc-ID-Str: parámetro identificador de una sesión activa.
- Alc-SLA-Prof-Str: perfil existente en el WAG, el cual incluye la calidad de servicio, políticas y el filtro IP que pueda tener un usuario.
- Alc-Subsc-Prof-Str: subperfil configurado en el WAG, que incluye políticas de NAT y cobro por radius.
- VSA 3GPP: parámetros de protocolo necesarios para confirmar la autorización y autenticación por medio de los paquetes de AAA hacia el WAG:

- IMSI [1]
- GGSN ADDRESS [7]
- APN-NAME

Estos requisitos son los indispensables para que la solución funcione, sin embargo, siempre existen varios proveedores con diversas funcionalidades en sus equipos, los cuales no son indispensables, pero sí brindan diversas opciones para la administración del tráfico de datos.

Un último punto importante a considerar es, si en dado caso los proveedores de AAA y de WAG son diferentes, es indispensable el intercambio de diccionario radius entre ambos equipos, en caso contrario la integración será demasiado complicada.

3.2.3. Integración GGSN

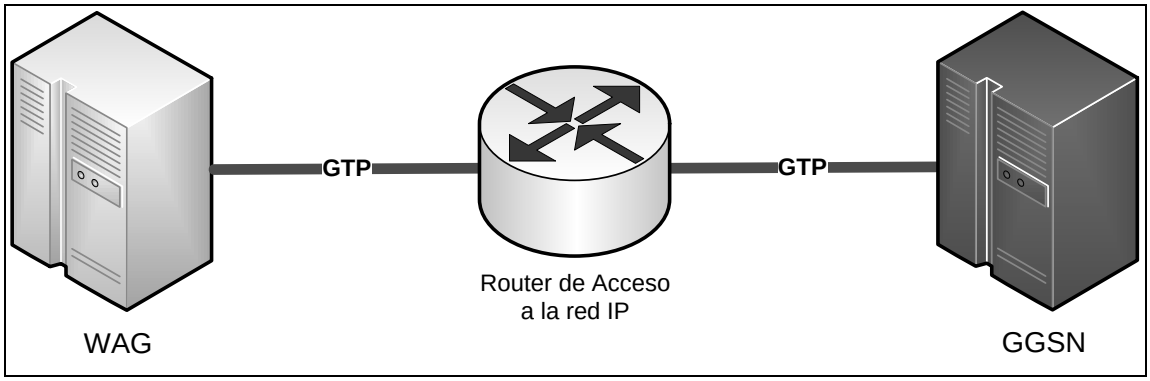
Desde el punto de vista del GGSN, el WAG estará actuando como un SGSN cuya función es validar al usuario y establecer el túnel GT*P* para el uso del servicio de datos de los subscriptores.

Partiendo de la premisa anterior, a nivel de configuración en el GGSN será necesario dar de alta la IP del WAG, de tal forma que el GGSN lo reconozca como un nodo capaz de establecer túneles GTP y de solicitar sesiones PDP para el uso de servicio de navegación.

Algo muy importante de definir, es que el GGSN ya se encuentra integrado en la red del operador, por tal razón, en la capa física de conexión no es necesario realizar ninguna variante, todo el trabajo de infraestructura es realizado en los nodos anteriores y lo que sí es necesario es establecer

conexión desde la IP de servicio del WAG hacia la IP de servicio del GGSN donde se le dará de alta al WAG como si fuese un SGSN local por medio de una configuración bastante básica y sencilla, también dependerá de la marca del GGSN.

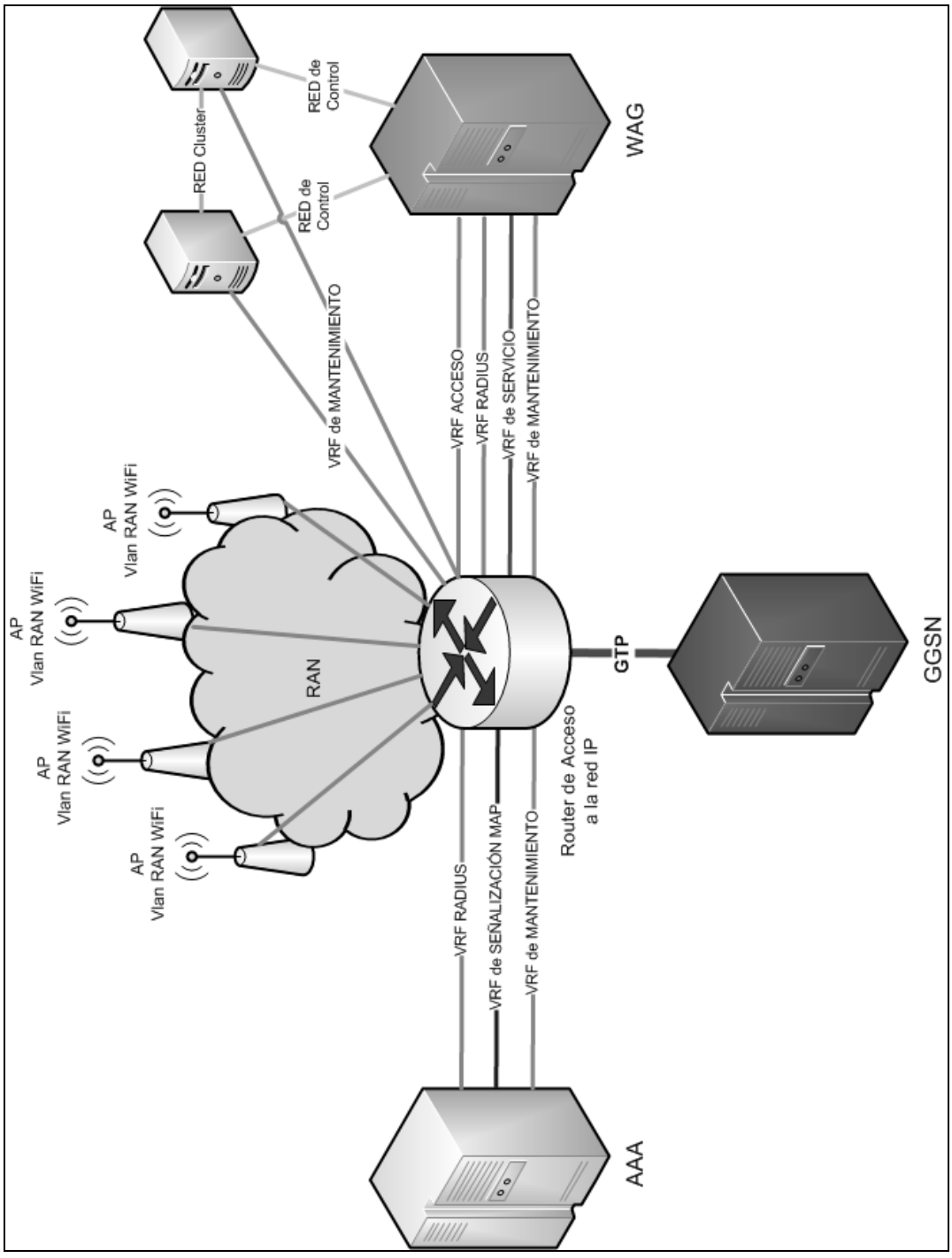
Figura 44. **Diagrama conexión GTP GGSN**



Fuente: elaboración propia.

Hay que considerar además, que como se ha mencionado en la solución propuesta el GGSN, tiene conexión directa hacia el sistema de cobro prepago y hacia el equipo que controla las políticas de navegación llamado PCRF, de esta forma se optimiza el uso de recursos y minimiza el impacto en el servicio.

Figura 45. **Diagrama del proyecto completo**



Fuente: elaboración propia.

3.3. Posibles lugares de despliegue

Como fase inicial, la recomendación es hacer un despliegue en sitios amplios, controlados y concurrentes que permitirá definir un patrón de comportamiento de los usuarios y del servicio, estos sitios deberán de ser analizados tomando en consideración, independientemente la tecnología (2G o 3G) la cantidad de usuarios por zona, cantidad de caídas de llamadas, intentos fallidos de conexión y tipo de terminales utilizadas en el lugar, esto último no es importante, pero valdrá la pena tener el dato con el objetivo de comprobar si el mercado permite el uso de autenticación automática por medio del EAP-SIM.

Teniendo definidos los puntos anteriores se puede tomar como referencias los siguientes lugares para iniciar con un despliegue WiFi:

- Universidades
- Centros comerciales
- Plazas
- Torres empresariales
- Centros de servicio
- Zonas hoteleras

La idea principal es lograr la descongestión de las redes macro 2G y 3G de los sitios que dan cobertura a los lugares mencionados, el acceso WiFi puede proveer de una mejor experiencia, tanto para los usuarios enganchados en las radio bases móviles a nivel de voz y datos como en los APs de WiFi a nivel de datos.

El despliegue anterior puede ser tomado como una fase inicial, para una segunda fase ya pueden ser tomados en cuenta sitios mucho más abiertos como: carreteras y áreas residenciales, por mencionar algunos.

4. CASOS DE USO SOLUCIÓN WIFI

Los casos de uso para este proyecto son más comerciales que aplicaciones técnicas, el diseño final permite una única función la cual es descargar las redes macro 2G y 3G a nivel de datos.

4.1. Servicios empresariales

Las operadoras móviles siempre deben mantener la imagen de alta disponibilidad y la mejor calidad del servicio brindado. La solución wifi puede ser la mejor opción para mantener esta imagen a nivel empresarial.

La solución de este servicio consiste en colocar AP dentro de las instalaciones físicas de la organización y enviar el tráfico de datos mediante un enlace corporativo vía MPLS hacia el core wifi que hará todo el proceso de autenticación y autorización, para finalmente brindar la salida del servicio de datos demandada por la institución.

La parte comercial es muy importante en la solución, ya que es necesario montar una propuesta sólida y que justifique la inversión del cliente dándole la certeza y garantía de una buena calidad de servicio

4.2. Soluciones exteriores

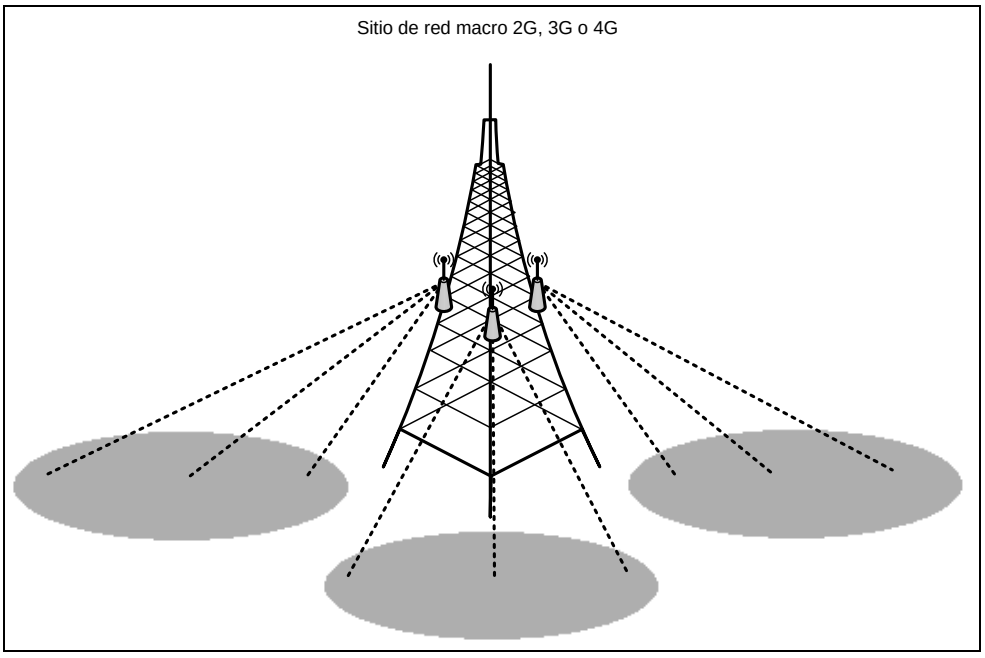
El escenario en sitios de alto congestionamiento vehicular y que la mayor parte del tiempo los usuarios se mantienen sin movilidad. Este escenario supone una alta carga para los sitios macro de cualquier tecnología, pero

además de ser una alta carga es una oportunidad para descargar todo el tráfico de datos de los sitios macro utilizando la RAN de wifi.

Lo que se considera para esta solución es adquirir equipo AP especial para exteriores que, comparándolo con el de interiores tiene una mejor ganancia y potencia más elevada para cubrir los espacios abiertos.

Del lado del core wifi no es requerido ningún cambio, ya que es transparente qué tipo de AP se utilice siempre y cuando cumpla con los estándares ya definidos previamente en la solución general.

Figura 46. **Montaje de AP en sitios de redes macro**



Fuente: elaboración propia.

4.3. Soluciones exteriores específicas

La mayoría de usuarios han tenido la experiencia de haber estado en conciertos, estadios de futbol llenos y han querido compartir esos momentos a través de las redes sociales pero no han tenido éxito, esto se debe a la sobrecarga de usuarios conectados al mismo tiempo que existen en las redes macros y por tal razón todos los servicios resultan imposibles de utilizar en esos momentos específicos.

La solución planteada para este caso es colocar una RAN wifi en lugares donde se realicen estos eventos de forma seguida y/o esporádicamente, y que además se puede calcular la cantidad de usuarios que pueden estar en estas instalaciones, logrando evitar así una saturación en todas las redes brindando un mejor servicio y dando una mejor imagen a nivel de empresa de telefonía con alta disponibilidad real en el servicio.

Para que esta solución funcione es necesario hacer un estudio del sitio de instalación, y tomar en cuenta todos los escenarios posibles en el lugar los cuales pueden ser interiores como exteriores.

Una vez más el acceso no impacta en temas de core wifi, que siempre mantendrá la postura de alta disponibilidad del servicio para los usuarios que conecten por medio de la solución.

4.4. Servicio wifi abierto a todo público

Este caso es totalmente comercial y válido, consiste en tener un SSID abierto a todo el público sin importar que sean usuarios de otras compañías de telefonía local. En primera instancia se hace la autenticación normal del usuario

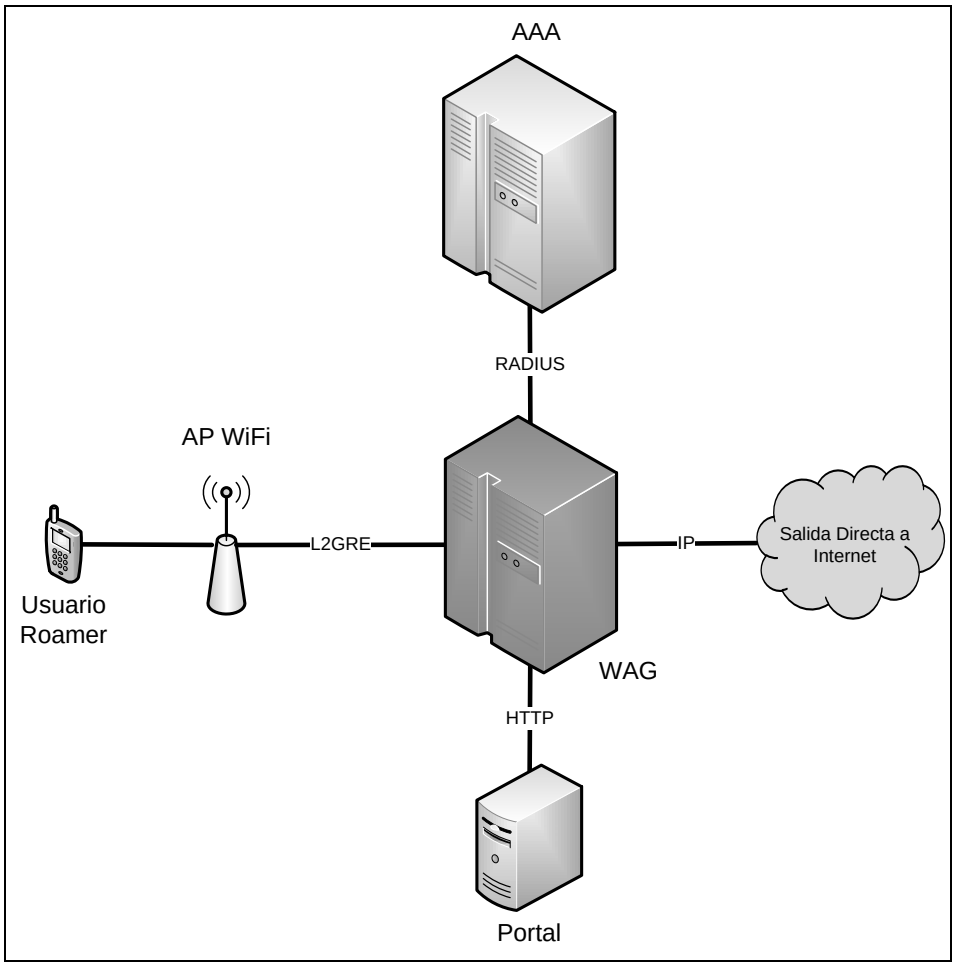
hacia el AAA, como no es un usuario propio de la red dueña de la RAN de wifi se le redirecciona hacia un portal de compra de servicio por medio de tarjeta de crédito donde podrán aplicar a una velocidad y cantidad de datos específica, después de la confirmación de compra y habiendo enviado las credenciales de acceso a la red al móvil mediante mensaje de texto se establece la conexión del servicio y el usuario puede utilizar la red del operador al que no pertenece para el servicio.

La solución, también aplica para usuarios de otros países que necesiten utilizar un paquete de datos local y el precio que se le estaría aplicando sería el uso de la red de acceso wifi. La idea de validación sería la misma que en el caso de usuarios de telefonías competencia local. ¿Cómo harían para navegar? ¿Se unen a la red en donde están conectados al roaming?R/ ¿Confundir diagramas?, la idea es monetizar por el cobro del acceso con salida directa a internet, sin necesidad de ir al GGSN local, por lo que la navegación tendría salida directa por los equipos de la operadora dueña de la RAN.

Estos casos de uso colocan a la empresa que brinda el servicio como una empresa de alta disponibilidad y con opciones viables para todo público.

La monetización, es decir cobro de este servicio, también puede darse mediante tarjetas de prepago con usuarios y pines previamente asignados y validados en la solución lo que permitirá que una tarjeta de crédito no sea indispensable para el uso del servicio.

Figura 47. **Diagrama conexión abierta todo público**



Fuente: elaboración propia.

CONCLUSIONES

1. A pesar de tener equipos robustos y con altas capacidades de manejo de tráfico en las redes de conmutación y de datos móviles, el cuello de botella es la red de acceso actual.

2. La división del tráfico de voz y datos permite liberar recursos de los canales de acceso actuales, aprovechando de mejor manera la red general del operador.

3. Dada la nueva arquitectura de acceso al servicio de datos móviles, nuevos métodos de autenticación serán requeridos para completar la información del suscriptor y validar así la utilización de los recursos de la red.

4. La red de acceso wifi es estratégica y no implica hacer un despliegue general de puntos de acceso tratando de igualar una cobertura de nodos b.

5. Es necesario determinar sectores específicos de saturación y evaluar la cantidad de puntos de acceso necesarios para satisfacer la demanda del servicio.

6. La red wifi es complementaria a una red macro, por lo que no debe de tomarse como acceso principal debido a que el ancho de banda y el número de suscriptores no alcanzan los valores de las redes de acceso actual.

7. La red wifi puede ser utilizada para brindar opciones de servicios administrados para el mercado corporativo, aprovechando los clientes con enlaces dedicados que el operador pueda tener.

RECOMENDACIONES

1. Antes de realizar expansiones dentro de la red general de telefonía, considerar hacer un estudio y determinar si los problemas de capacidades son por la red de acceso actual.

2. Considerar que la operadora que tenga la iniciativa de colocar una red wifi, haga un estudio a nivel de radio frecuencia para determinar la necesidad de la ubicación de los puntos de acceso.

3. Es importante realizar la integración de la red wifi con los equipos de datos móviles actuales, ahorrará inversión y tiempos de integración.

4. Hacer un estudio de mercado sobre la tendencia de uso de los datos móviles para explotar las funcionalidades de forma masiva y formar alianzas con diversas empresas para explotar el mercado corporativo.

5. Es conveniente invertir sobre el acceso wifi, dado que implica una inversión menor y su instalación es más sencilla y efectiva.

BIBLIOGRAFÍA

6. ANAYA MARTÍN, Marco Antonio. *Dimensionamiento y optimización de red GPRS para ofrecer servicios de banda ancha y prepago* [en línea].http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/859/Reporte_Experiencia_Profesional_Marco_Anaya.pdf?sequence= [Consulta: 17 de febrero de 2014].

7. CISCO.COM. *Architecture for Mobile Data Offload over Wi-Fi Access Networks* [en línea] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white_paper_c11-701018.pdf]. [Consulta: 4 de febrero de 2014].

8. INTERNET ENGINEERING TASK FORCE (IETF). *RFC 2865: Remote Authentication Dial In User Service (RADIUS)* [en línea]. Edited by W. Simpson. http://www.ietf.org/rfc/rfc2865. [Consulta: 8 de marzo de 2014].

9. _____. *RFC 2866: RADIUS Accounting* [en línea]. Edited by C. Rigney. http://www.ietf.org/rfc/rfc2866. [Consulta: 8 de marzo de 2014].

10. _____. *RFC 3748: Extensible Authentication Protocol (EAP)* [en línea]. Edited by H. Levkowetz. http://www.ietf.org/rfc/rfc3748. Consulta: 15 de marzo de 2014].

11. _____. *RFC 4186: Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)* [en línea]. Edited by Cisco Systems. Enero http://www.ietf.org/rfc/rfc4186. [Consulta: 15 de marzo de 2014].

12. _____. *RFC 4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)* [en línea]. Edited by Nokia.: http://www.ietf.org/rfc/rfc4187. [Consulta: 15 de marzo de 2014].

13. INTERNET ENGINEERING TASK FORCE (IETF). *RFC 6733: Diameter Base Protocol* [en línea]. Edited by Network Zen. Octubre 2006 http://www.ietf.org/rfc/rfc6733.txt. [Consulta: 16 de marzo de 2014].

14. _____. *RFC 3031: Multiprotocol Label Switching Architecture* [en línea]. Edited by Juniper Networks, Inc. http://www.ietf.org/rfc/rfc3031. [Consulta: 18 de marzo de 2014].

15. _____. *RFC 3031: Multiprotocol Label Switching Architecture* [en línea]. Edited by Juniper Networks, Inc. http://www.ietf.org/rfc/rfc3031. [Consulta: 19 de marzo de 2014].