



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

**PROPUESTA DE INTEGRACIÓN DE RED WIFI OFFLOAD EN RED MÓVIL HETEROGÉNEA**

**Carlos Enrique Vielman Velásquez**

Asesorado por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, septiembre de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**PROPUESTA DE INTEGRACIÓN DE RED WIFI OFFLOAD EN RED MÓVIL HETEROGÉNEA**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA  
FACULTAD DE INGENIERÍA

POR

**CARLOS ENRIQUE VIELMAN VELÁSQUEZ**

ASESORADO POR LA INGA. INGRID SALOMÉ RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

**INGENIERO EN ELECTRÓNICA**

GUATEMALA, SEPTIEMBRE DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA  
FACULTAD DE INGENIERÍA



**NÓMINA DE JUNTA DIRECTIVA**

DECANO	Ing. Pedro Antonio Aguilar Polanco
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
SECRETARIA	Inga. Lesbia Magalí Herrera López

**TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO**

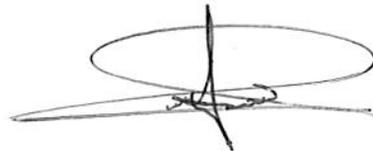
DECANO	Ing. Murphy Olympto Paiz Recinos
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
EXAMINADOR	Ing. Julio Rolando Barrios Archila
EXAMINADOR	Ing. Julio César Solares Peñate
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

## **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 INTEGRACIÓN DE RED WIFI OFFLOAD EN RED MÓVIL HETEROGÉNEA**

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 4 de noviembre de 2013.



**Carlos Enrique Vielman Velásquez**

Guatemala 29 de mayo de 2015

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 INTEGRACIÓN DE RED WIFI OFFLOAD EN RED MÓVIL HETEROGENEA**, del señor **Carlos Enrique Vielman Velásquez**, 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



Ref. EIME 40. 2015

Guatemala, 18 de JUNIO 2015.

Señor Director  
Ing. Guillermo Antonio Puente Romero  
Escuela de Ingeniería Mecánica Eléctrica  
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado:  
PROPUESTA DE INTEGRACIÓN DE RED WIFI OFFLOAD  
EN RED MÓVIL HETEROGÉNEA, del estudiante Carlos  
Enrique Vielman Velásquez que cumple con los requisitos  
establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,  
D Y ENSEÑAD A TODOS

Ing. Carlos Eduardo Guzmán Salazar  
Coordinador Área Electrónica



SFO



FACULTAD DE INGENIERIA

REF. EIME 45. 2015.

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; **CARLOS ENRIQUE VIELMAN VELÁSQUEZ** titulado: **PROPUESTA DE INTEGRACIÓN DE RED WIFI OFFLOAD EN RED MÓVIL HETEROGÉNEA**, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romo



GUATEMALA, 22 DE JULIO 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 INTEGRACIÓN DE RED WIFI OFFLOAD EN RED MÓVIL HETEROGÉNEA**, presentado por el estudiante universitario: **Carlos Enrique Vielman Velásquez**, y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco  
Decano



Guatemala, septiembre de 2015

/cc

## **ACTO QUE DEDICO A:**

<b>Dios</b>	Por darme fe, esperanza y fortaleza en la vida.
<b>Mis padres</b>	José Vielman y María Velásquez, por brindarme amor, disciplina y educación.
<b>Mi esposa</b>	Ozni Morales, por su apoyo y respeto incondicional de mis sueños, anhelos y propósitos.
<b>Mi hija</b>	Ozny Vielman, por ser la razón más grande de lucha en mi vida.
<b>Mis tíos</b>	Por apoyarme en muchos pasajes de mi vida, en especial por motivarme a seguir mi educación.
<b>Mis compañeros</b>	Por el apoyo mutuo de continuar hacia adelante en toda la carrera.

## **AGRADECIMIENTOS A:**

<b>Universidad de San Carlos de Guatemala</b>	Por darme la oportunidad de crecer como profesional.
<b>Facultad de Ingeniería</b>	Por la enseñanza académica inculcada a lo largo de la carrera.
<b>Escuela de Mecánica Eléctrica</b>	Por la experiencia profesional que entregan hacia todos los alumnos.
<b>Francisco Contreras</b>	Por su amistad, apoyo y palabras de aliento en la realización de este documento.
<b>Otto Escobar</b>	Porque, aún lejos, tuve su apoyo incondicional en toda mi carrera.
<b>Julio Cahueque</b>	Por apoyarme en el trabajo y en la realización de mis prácticas.
<b>Ingrid Rodriguez</b>	Por su apoyo, tanto en el examen privado, como en la realización de este documento.

## ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES.....	VII
LISTA DE SÍMBOLOS .....	IX
GLOSARIO .....	XI
RESUMEN.....	XIX
OBJETIVOS.....	XXI
INTRODUCCIÓN.....	XXIII
1. TEORÍA DE LA RADIOFRECUENCIA Y ANTENAS.....	1
1.1. Campo magnético .....	1
1.2. Radiación electromagnética .....	2
1.3. Espectro electromagnético .....	3
1.4. Propagación de las ondas electromagnéticas .....	4
1.5. Propagación terrestre de las ondas electromagnéticas.....	5
1.5.1. Onda terrestre.....	5
1.5.2. Ondas espaciales .....	6
1.6. La antena.....	7
1.6.1. Antenas direccionales.....	8
1.6.2. Antenas omnidireccionales .....	9
1.7. Diagrama de radiación de una antena.....	10
1.8. Parámetros de una antena .....	11
1.8.1. Ancho de banda.....	11
1.8.2. Directividad .....	11
1.8.3. Ganancia .....	12
1.8.4. Eficiencia .....	12
1.8.5. Impedancia de entrada .....	13

1.8.6.	Ancho de haz .....	13
1.8.7.	Resistencia de radiación .....	13
1.9.	Tipos de modulación para transmisión RF .....	14
1.9.1.	Modulación por desplazamiento de amplitud (ASK).....	14
1.9.2.	Modulación por desplazamiento de frecuencia (FSK).....	16
1.9.3.	Modulación por desplazamiento de fase (PSK).....	17
1.9.4.	Modulación de espectro expandido.....	18
1.9.5.	Modulación wifi.....	19
2.	REDES WIFI.....	21
2.1.	Arquitectura de redes wifi.....	21
2.1.1.	Elementos de una red wifi .....	22
2.1.1.1.	Punto de acceso (AP) .....	22
2.1.1.2.	Antena.....	22
2.1.1.3.	Tarjeta wifi.....	23
2.2.	Topología de una red wifi .....	23
2.2.1.	Redes sin infraestructura.....	24
2.2.2.	Redes en modo de infraestructura .....	24
2.3.	Estándares wifi.....	25
2.3.1.	Estándar 802.11b.....	26
2.3.2.	Estándar 802.11a .....	26
2.3.3.	Estándar 802.11g.....	27
2.3.4.	Estándar 802.11n .....	27
2.3.5.	Estándar 802.11i .....	28
2.3.5.1.	Autenticación.....	28
2.3.5.1.1.	Autenticación abierta.....	28

	2.3.5.1.2.	Autenticación de clave compartida.....	29
	2.3.5.1.3.	Autenticación por dirección mac .....	30
	2.3.5.2.	Confidencialidad .....	31
	2.3.5.3.	Integridad.....	32
	2.3.5.4.	Disponibilidad .....	32
2.4.		Limitaciones tecnológicas de la familia 802.11 .....	32
	2.4.1.	Alcance .....	32
	2.4.2.	Ancho de banda.....	33
	2.4.3.	Calidad de servicio .....	33
	2.4.4.	Seguridad .....	33
	2.4.5.	Movilidad.....	34
2.5.		Itinerancia en redes wifi.....	34
	2.5.1.	Estándar 802.11p .....	35
2.6.		Futuras evoluciones de la tecnología wifi .....	35
	2.6.1.	Estándar 802.11r .....	35
	2.6.2.	Estándar 802.11u .....	37
	2.6.3.	Estándar 802.11s.....	37
3.		ARQUITECTURA DE RED MÓVIL PARA DESCARGA DE DATOS ATRAVÉS DE REDES DE ACCESO WIFI.....	39
	3.1.	3GPP versión R99.....	39
	3.2.	Arquitectura de red R99.....	39
		3.2.1. Nodo B.....	39
		3.2.2. RNC.....	40
	3.3.	3GPP versión 4 .....	42
		3.3.1. <i>Media gateway</i> .....	42
	3.4.	3GPP versión 5 .....	43

3.4.1.	HSDPA .....	44
3.4.2.	Iu-flex.....	44
3.4.3.	Pre IMS .....	44
3.5.	Información general de la arquitectura wifi offload .....	45
3.5.1.	Despliegues existentes.....	46
3.5.2.	Disponibilidad de dispositivos que soportan la arquitectura .....	46
3.5.3.	Rentabilidad .....	46
3.5.4.	Capacidad de espectro disponible .....	47
3.6.	Arquitectura wifi offload .....	47
3.6.1.	Autenticación.....	48
3.6.1.1.	Autenticación basada en un portal .....	48
3.6.1.2.	Autenticación basada en EAP .....	51
3.7.	Estrategia y carga de control.....	53
3.7.1.	Arquitectura de PCEF independiente .....	53
3.7.2.	Arquitectura tradicional del GGSN .....	56
3.7.3.	<i>Handover</i> de radio interno .....	57
3.7.3.1.	<i>Handover</i> con dirección IP no persistente.....	58
3.7.3.2.	<i>Handover</i> con dirección IP persistente.....	58
3.7.3.3.	<i>Handover</i> de sesión .....	58
3.7.3.4.	<i>Handover</i> basado en S2A .....	59
4.	PROPUESTA DE INTEGRACIÓN ENTRE RED MÓVIL Y WIFI .....	61
4.1.	Controles wifi.....	61
4.2.	Recientes habilitadores wifi.....	62
4.2.1.	Normas en evolución.....	62
4.2.2.	Evolución en las capacidades de dispositivo.....	64

4.2.3.	Evolución de modelos con interfuncionamiento 3GPP y wifi .....	65
4.2.3.1.	Redes de acoplamiento flexible .....	66
4.2.3.2.	Redes de estructura rígida.....	66
4.3.	Desafíos en el interfuncionamiento celular de 3GPP y wifi .....	67
4.3.1.	Prematura selección de wifi.....	67
4.3.2.	Opciones no saludables .....	67
4.3.3.	Capacidades inferiores .....	68
4.3.4.	Intercambio entre tecnologías.....	68
4.4.	Estado actual de la integración y los retos existentes .....	69
4.4.1.	Continuidad de servicio entre 3GPP y wifi.....	69
4.4.2.	Continuidad de servicio en sesión .....	71
4.5.	Métodos 3GPP para movilidad entre redes .....	72
4.5.1.	Movilidad no continua de todas las conexiones de paquetes .....	72
4.5.2.	Movilidad sin fisuras de todas las conexiones de paquetes.....	73
4.5.3.	Movilidad sin fisuras de las conexiones individuales PDN .....	73
4.5.4.	Movilidad ininterrumpida de IP individual en conexiones específicas de PDN .....	74
4.6.	Servicios en tiempo real sobre QoS de confianza wifi .....	74
4.6.1.	Características necesarias para apoyar los servicios en tiempo real .....	74
4.6.1.1.	Acceso de UE simultáneo a IMS .....	75
4.6.1.2.	Señalización IMS .....	75
4.6.1.3.	Servicios QoS .....	75
4.6.1.4.	Carga y ubicación .....	75
4.6.2.	Habilitación QoS extremo a extremo .....	76

4.6.2.1.	Interfaz S2A entre el P-GW y la WLAN <i>access gateway</i> .....	76
4.6.2.2.	Habilitación entre TWAG y UE para el enlace descendente .....	76
4.6.2.3.	Habilitación entre TWAG y UE para el enlace ascendente .....	77
4.7.	Seguridad y autenticación .....	77
4.7.1.	Autenticación.....	77
4.7.2.	<i>Airlink</i> cifrado.....	79
4.8.	Selección de red inteligente .....	80
4.8.1.	Aspectos de selección de red.....	81
CONCLUSIONES.....		83
RECOMENDACIONES .....		85
BIBLIOGRAFÍA.....		87

# ÍNDICE DE ILUSTRACIONES

## FIGURAS

1.	Gráfica de líneas de campo de una barra magnética.....	1
2.	Onda de radiación plana en dirección z .....	2
3.	División de frecuencias del espectro electromagnético.....	3
4.	Sistema de transmisión con ondas espaciales.....	6
5.	Diagrama de antena dipolo de media onda.....	7
6.	Diagrama tridimensional de campo lejano de antena Yagi. ....	8
7.	Diagrama tridimensional de campo lejano de antena omni. ....	9
8.	Diagrama de propagación de RF en red de telefonía celular .....	10
9.	Fórmula para calcular directividad .....	11
10.	Fórmula para calcular ganancia .....	12
11.	Fórmula para calcular eficiencia.....	13
12.	Fórmula para calcular resistencia de radiación .....	14
13.	Representación gráfica de la modulación ASK .....	15
14.	Representación gráfica de la modulación FSK .....	16
15.	Representación gráfica de la modulación PSK .....	17
16.	Densidad espectral de una señal <i>spread spectrum</i> .....	18
17.	Diagrama de bloques de técnica de modulación DSSS .....	19
18.	Diagrama de arquitectura red wifi. ....	21
19.	Imagen de los elementos de una red wifi.....	23
20.	Diagrama de red wifi AD HOC .....	24
21.	Diagrama de red en modo infraestructura.....	25
22.	Diagrama de autenticación abierta.....	29
23.	Diagrama de autenticación de clave compartida.....	30

24.	Diagrama de autenticación por dirección MAC .....	31
25.	Esquema de itinerancia en red GSM. ....	36
26.	Imagen de la arquitectura del estándar 802.11s.....	38
27.	Nodo B en servicio.....	40
28.	RNC en servicio .....	41
29.	Arquitectura de red 3GPP R99 .....	42
30.	Arquitectura de red BICC .....	43
31.	Arquitectura de red 3GPP R5 .....	45
32.	Arquitectura basada en portal de autenticación .....	49
33.	Inicio de sesión automática de llamadas .....	50
34.	Arquitectura de autenticación basada en EAP .....	51
35.	Flujo de llamada con autenticación EAP.....	52
36.	Arquitectura de PCEF independiente.....	54
37.	Flujo de llamada típica de autenticación PCEF .....	55
38.	Arquitectura tradicional del GGSN .....	56
39.	Flujo de llamada para arquitectura tradicional GGSN.....	57
40.	Flujo de llamada para <i>handover</i> basado en S2A .....	60
41.	Principales retos de la integración entre tecnologías.....	68
42.	Visión general de interfuncionamiento entre 3GPP y wifi .....	70
43.	Aspectos de alto nivel de una red de selección inteligente.....	81

## TABLAS

I.	Canales de frecuencia utilizado en wifi banda 2,4 Ghz.....	34
----	--	----

## LISTA DE SÍMBOLOS

<b>Simbolo</b>	<b>Significado</b>
<b>Bps</b>	Bits por segundo
<b>dB</b>	Decibelio
<b>dBd</b>	Decibelios medidos con respecto a una antena dipolo.
<b>dBi</b>	Decibelios medidos con respecto a una antena isotrópica.
<b>Ghz</b>	Gigahertz
<b>Khz</b>	Kilohertz
<b>Km</b>	Kilómetro
<b>Mbps</b>	Mega bits por segundo
<b>Mhz</b>	Megahertz
<b>ms</b>	Milisegundo



## GLOSARIO

<b>AAA</b>	<i>Authentication, authorization and accounting;</i> autenticación, autorización y contabilización.
<b>Adimensional</b>	Que no tiene dimensiones como el número pi.
<b>ADSL</b>	<i>Asymmetric digital subscriber;</i> línea de abonado digital.
<b>AM</b>	Amplitud modulada.
<b>AP</b>	<i>Access point;</i> punto de acceso inalámbrico.
<b>APN</b>	<i>Access point name;</i> nombre del punto de acceso para GPRS.
<b>ASK</b>	<i>Amplitude-shift keying;</i> modulación por desplazamiento de amplitud.
<b>Azimet</b>	Ángulo que con el meridiano forma el círculo vertical que pasa por un punto de la esfera celeste o del globo terráqueo.
<b>BSC</b>	<i>Base station controller;</i> modulación controlador de estaciones base.

<b>Conductividad</b>	Propiedad que tienen los cuerpos de transmitir el calor o la electricidad.
<b>Convolución</b>	Es un operador matemático que transforma dos funciones, f y g, en una tercera función.
<b>Core</b>	Núcleo de red telefónica celular, es decir, el cerebro de la red de telecomunicaciones.
<b>CS</b>	<i>Circuit switched</i> ; conmutador de circuitos.
<b>Densidad</b>	Magnitud que expresa la relación entre la masa y volumen de un cuerpo.
<b>Discretos</b>	Números en contraposición a continuos, sí son divisibles un número finito de veces.
<b>DSSS</b>	<i>Direct sequence spread spectrum</i> ; espectro ensanchado por secuencia directa.
<b>Espectro</b>	Distribución de la intensidad de una radiación en función de una magnitud.
<b>Ethernet</b>	Estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora.
<b>Exor</b>	Disyunción exclusiva también llamado exclusivo, simbolizado como XOR.

<b>FSK</b>	<i>Frequency shift keying</i> ; modulación por desplazamiento de frecuencia.
<b>Gateway</b>	Dispositivo digital lógico cuyo propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.
<b>GGSN</b>	<i>GPRS Gateway support node</i> ; nodo de soporte para servicio Gateway.
<b>GSM</b>	<i>Global system for mobile</i> ; sistema global para móviles.
<b>Handover</b>	Sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra, cuando la calidad del enlace es insuficiente en una de las estaciones.
<b>Hardware</b>	Todas las partes físicas de un sistema informático.
<b>HLR</b>	<i>Home local register</i> ; registro local de usuarios.
<b>HSDPA</b>	<i>High speed downlink packet access</i> ; descarga de paquetes con acceso a paquetes de alta velocidad.
<b>HTTP</b>	<i>Hypertext transfer protocol</i> ; protocolo de transferencia de hipertexto.
<b>IEEE</b>	Instituto de Ingeniería Eléctrica y Electrónica.

<b>Ionosféricas</b>	Conjunto de capas de la atmósfera que están por encima de los 80 km. Presentan fuerte ionización causada por la radiación solar y afectan de modo importante a la propagación de las ondas radioeléctricas.
<b>Isotrópica</b>	Característica de algunos cuerpos cuyas propiedades físicas no dependen de la dirección en que son examinadas.
<b>Itinerancia</b>	Capacidad de enviar y recibir llamadas en redes móviles fuera del área de servicio local.
<b>Iub</b>	Interfaz entre la RNC y un nodoB.
<b>Láser</b>	Dispositivo electrónico que, basado en la emisión inducida, amplifica de manera extraordinaria un haz de luz monocromático y coherente.
<b>Led</b>	<i>Light-emitting diode</i> ; diodo emisor de luz.
<b>LTE</b>	<i>Long term evolution</i> ; evolución largo plazo.
<b>MGW</b>	<i>Media Gateway</i> ; puente multimedia de datos.
<b>MIMO</b>	<i>Multiple-input, multiple-output</i> ; múltiple entrada, múltiple salida.

<b>MSC</b>	<i>Mobile switching center</i> ; centro de conmutación de circuitos.
<b>Omni</b>	Radián o captán por igual en todas direcciones.
<b>Onda</b>	Forma de propagarse, a través del espacio, de los campos eléctricos y magnéticos.
<b>Plasma</b>	Materia gaseosa fuertemente ionizada, con igual número de cargas libres positivas y negativas. Es el estado de la materia más abundante en el universo.
<b>Polarización</b>	Proceso por el cual en un conjunto originariamente indiferenciado se establecen características o rasgos distintivos que determinan la aparición en él de dos o más zonas mutuamente cargadas.
<b>PS</b>	<i>Packet switched</i> ; conmutador de paquetes.
<b>PSK</b>	<i>Phase shift keying</i> ; modulación por desplazamiento de fase.
<b>RAN</b>	<i>Radio access network</i> ; acceso a red de radio.
<b>Receptor</b>	Aparato que sirve para recibir las señales eléctricas, telegráficas o telefónicas.
<b>RF</b>	Radiofrecuencia.

<b>RNC</b>	<i>Radio network controller</i> ; controlador de la red radio.
<b>Senoidal</b>	Curva que representa gráficamente la función seno y también a dicha función en sí.
<b>SGSN</b>	<i>GPRS gateway support node</i> ; nodo de soporte para servicio gateway.
<b>SIM</b>	<i>Subscriber identity module</i> ; módulo de identificador de suscriptores.
<b>Software</b>	Conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.
<b>Superposición</b>	Acción y efecto de superponer una función con el fin de simplificar la forma de resolver un problema.
<b>Switch</b>	Dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.
<b>Tablet</b>	Computadora portátil de mayor tamaño que un teléfono inteligente o un PDA.
<b>TCP</b>	<i>Transmission control protocol</i> ; protocolo para control de transmisión.

<b>Topología</b>	Rama de las matemáticas que trata especialmente de la continuidad y de otros conceptos más generales originados de ella, como las propiedades de las figuras con independencia de su tamaño o forma.
<b>UDP</b>	<i>User datagram protocol</i> ; protocolo para uso de diagrama de datos.
<b>USB</b>	<i>Universal serial bus</i> ; protocolo de <i>bus</i> universal en serie.
<b>VCO</b>	Oscilador controlado por tensión.
<b>VoIP</b>	Voz sobre IP.
<b>WCDMA</b>	<i>Wideband code division multiple access</i> ; acceso múltiple por división de código de banda ancha.
<b>WEP</b>	<i>Wired equivalent privacy</i> ; privacidad equivalente a cableado.
<b>wifi</b>	<i>Wireless fidelity</i> ; fidelidad inalámbrica.



## RESUMEN

Este trabajo de graduación propone una solución eficaz a los problemas de capacidad en las redes de telecomunicaciones combinando tecnologías de radiofrecuencia (RF) diferentes, estas tecnologías son: wifi, 3G y LTE. En el primer capítulo se hace un resumen del principio de la RF, iniciando con la teoría electromagnética y la teoría de las antenas, recordando los principios, fortalezas y debilidades de la RF.

En el segundo capítulo, se hace el análisis de la tecnología wifi, de la tecnología 3G y de la combinación de ambas para la solución de problemas por capacidad, se describen las dos tecnologías, empezando en los equipos RF y profundizando en las plataformas del *core* y sus protocolos.

En el tercer capítulo se describe la solución integral y desarrollada por una operadora de telefonía del wifi offload, se presentan por lo menos dos soluciones para la fusión de la tecnología wifi y la tecnología 3G, describiendo los protocolos, plataformas y equipos RF a utilizar, se explica también el desarrollo de las llamadas y de los *handover* internos y externos tanto en el *core* como en RF.

En el último capítulo, se detallan las nuevas tendencias en telefonía y descarga de datos, las evoluciones en la rama de la telecomunicación; también se presentan mejoras a la solución del wifi offload para que la convivencia de las dos tecnologías sea cada vez mejor y menos impactante para el usuario.



# OBJETIVOS

## General

Realizar una propuesta de integración de redes wifi offload en redes móviles heterogéneas.

## Específicos

1. Exponer la teoría de la radiofrecuencia y las antenas.
2. Describir los estándares y arquitecturas de la tecnología wifi.
3. Presentar la arquitectura de red móvil y wifi offload, utilizada para descarga de datos.
4. Presentar una propuesta del método de unificación de tecnología wifi y 3G.



## INTRODUCCIÓN

Este trabajo de graduación se basa en proponer soluciones a los problemas de capacidad de una red 3G activa. Cuando la celda es insuficiente para satisfacer la demanda de datos, se debe recurrir a nuevas soluciones que van más allá de la red de telefonía móvil, ya que deben ser soluciones más enfocadas y puntuales en áreas demandantes de datos. Un ejemplo es cuando una celda macro cubre desde fuera un centro comercial abarrotado de personas un fin de semana específico, en este caso, se debe pensar en introducir soluciones efectivas y poco invasivas a la visión de los usuarios.

De estas soluciones, existen muchas, como femtoceldas, microceldas, DAS, entre otras. Este documento se enfocará en una solución efectiva en descarga masiva de datos llamada wifi offload, que no es más que la fusión de la red móvil 3G o LTE con una solución wifi convencional, utilizando plataformas que fusionan protocolos distintos para que ambas tecnologías se entiendan y puedan convivir, además, que el cambio sea imperceptible para el usuario.

Uno de los puntos clave de la fusión es la seguridad para conectarse del lado wifi, ya que, en la mayoría de casos, las redes wifi son libres de acceso o tienen claves muy sencillas de desbloquear, algo que al operador no le conviene porque el acceso a internet tiene un costo. Entonces, se debe poder bloquear a las personas que no son clientes del operador, para esto, existe un protocolo de autenticación de SIM del dispositivo móvil.



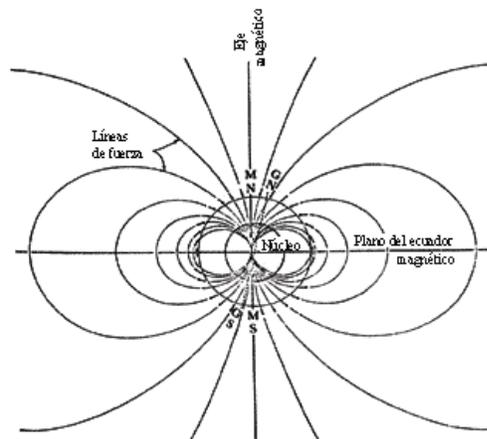
# 1. TEORÍA DE LA RADIOFRECUENCIA Y ANTENAS

## 1.1. Campo magnético

Es una descripción matemática de la influencia magnética, que contienen intrínsecamente los materiales magnéticos. Este, en cualquier punto, se compone de dos valores: la dirección y la magnitud, estos dos valores son producidos por cualquier carga eléctrica en movimiento.

Cuando se estudian campos magnéticos, se analizan las líneas de campo que lo componen, estas describen la intensidad y dirección de campo magnético.

Figura 1. Gráfica de líneas de campo de una barra magnética



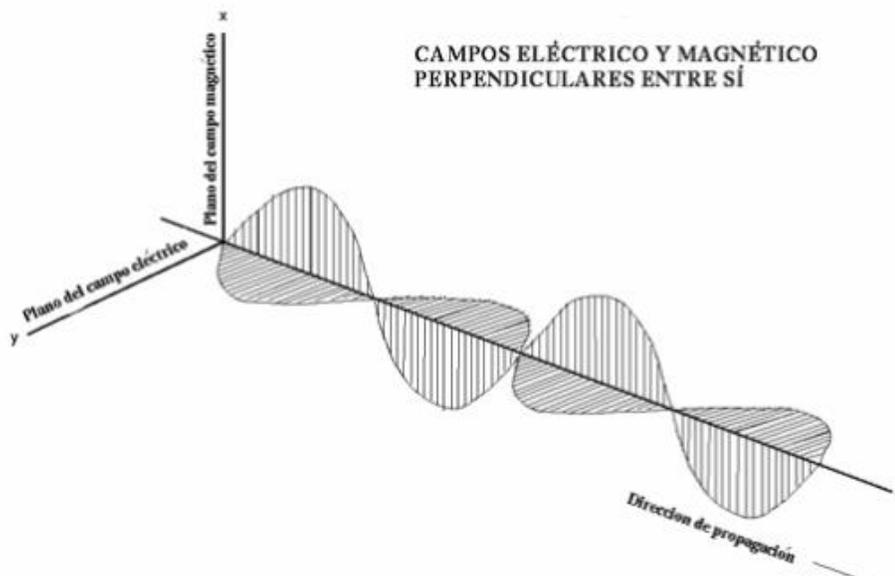
Fuente: Biblioteca digital. *El sol y la tierra, una relación tormentosa*. Capítulo 4.

## 1.2. Radiación electromagnética

Es una combinación de campos eléctricos y magnéticos, estos campos oscilan y se propagan a través del espacio transportando energía de un lugar a otro. La distancia a la que la radiación es percibida depende de las pérdidas en el medio que se transmite, si se trata del espacio vacío, las pérdidas son relativamente nulas.

Uno de los fenómenos visibles de la radiación electromagnética es la luz. Una propiedad de la radiación es su dualidad, el comportamiento de este fenómeno es que algunas veces la radiación se comporta como una onda electromagnética y otras se encuentra como fotones.

Figura 2. Onda de radiación plana en dirección z



Fuente: Centro de astrobiología. [http://www.partner.cab.inta-csic.es/index.php?Section=Curso\\_Fundamentos\\_Capitulo\\_1](http://www.partner.cab.inta-csic.es/index.php?Section=Curso_Fundamentos_Capitulo_1). Consulta: mayo 2014.

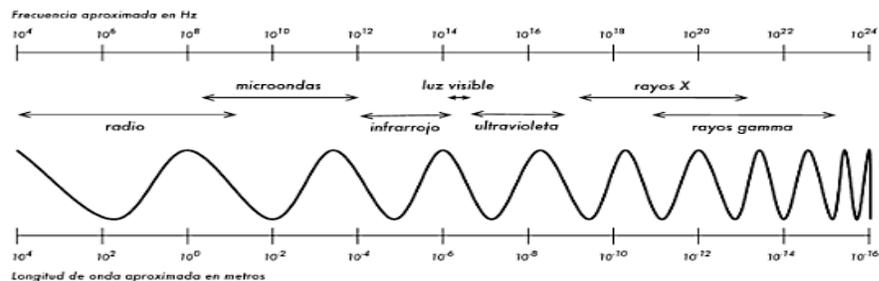
### 1.3. Espectro electromagnético

La energía electromagnética se puede propagar en forma de voltaje y corriente a través de un conductor, también en forma de ondas de radio emitidas hacia el espacio libre, o bien, en forma de luz a través de fibra óptica. La energía electromagnética se distribuye en un intervalo casi infinito de frecuencias.

La frecuencia es la cantidad de veces que sucede un movimiento periódico, un ejemplo de frecuencias puede ser una onda senoidal de voltaje o corriente durante determinado período y cada inversión de la onda se llama ciclo.

La unidad básica de la frecuencia se llama hertz, que equivale a un ciclo por segundo. En electrónica, se acostumbra a utilizar prefijos cuando las frecuencias son muy altas, por ejemplo el Khz y el Mhz los cuales son nombrados kilohertz y megahertz, en la figura 3 se observa la división del espectro de frecuencias.

Figura 3. División de frecuencias del espectro electromagnético



Fuente: *Redes inalámbricas en los países en desarrollo*. <http://wndw.net/pdf/wndw3-es/wndw3-es-ebook.pdf>. Consulta: mayo 2014.

Se denomina espectro electromagnético a la distribución energética del conjunto de las ondas electromagnéticas. Los espectros se pueden observar mediante espectroscopios, que además de permitir ver el espectro permiten realizar medidas como: longitud de onda, frecuencia e intensidad de radiación.

#### **1.4. Propagación de las ondas electromagnéticas**

A la propagación de las ondas electromagnéticas en el espacio vacío se le ha llamado propagación de radiofrecuencia (RF). Las ondas de radio son ondas electromagnéticas, como la luz, viajan en línea recta, con una velocidad de 300 000 km/s en el espacio libre.

Para propagar ondas electromagnéticas en la atmósfera se debe tener una fuente de energía que irradie y un receptor que capture esta energía, para este trabajo existe un dispositivo que captura y a la vez irradia energía, al cual se le ha llamado antena.

En el caso de las ondas sonoras y de luz, se acostumbra analizar a una onda como la suma de ondas sinusoidales simples, este es el principio de superposición lineal. Este principio no aplica a todos los casos ondulatorios, existen algunos casos, como los haces de láseres en la óptica no lineal y las ondas en gases de plasma, cuyo comportamiento no es lineal, este comportamiento es considerado como entidad fundamental en los ondulatorios.

## **1.5. Propagación terrestre de las ondas electromagnéticas**

Las ondas de radio que viajan dentro de la atmósfera terrestre son llamadas ondas terrestres y las comunicaciones entre dos o más puntos de la tierra se llaman radiocomunicaciones terrestres. Las ondas terrestres son influidas por la atmósfera y por el planeta Tierra. En esencia, hay tres formas de propagación de las ondas electromagnéticas dentro de la atmósfera terrestre: ondas terrestres, onda espacial y ondas ionosféricas.

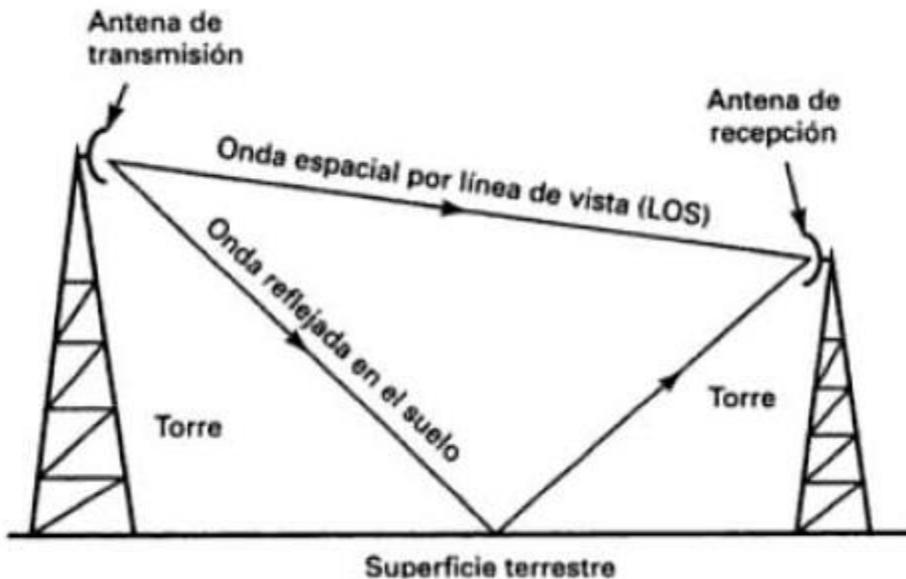
### **1.5.1. Onda terrestre**

Es una onda electromagnética que viaja por la superficie de la tierra, es por eso que son llamadas ondas superficiales. Las ondas terrestres deben estar en polarización vertical, esto se debe a que el campo eléctrico polarizado horizontalmente sería paralelo a la superficie de la Tierra y estas ondas se pondrían en corto por la conductividad del suelo. El fenómeno que ocurre con este tipo de onda, el cual es el causante de limitar su uso, es que el campo eléctrico variable induce voltajes en la superficie terrestre que hace circular corrientes muy parecidas a las de una línea de transmisión, es por eso que las pérdidas en las ondas terrestres aumentan rápidamente conforme aumenta la frecuencia, por consecuencia, su propagación se limita a frecuencias menores a 2 Mhz.

### 1.5.2. Ondas espaciales

La propagación de la energía electromagnética en forma de ondas espaciales, incluye a la energía irradiada que viaja en los kilómetros inferiores de la atmósfera terrestre. Las ondas espaciales incluyen a las ondas directas y a las reflejadas, las ondas directas viajan esencialmente en línea recta entre las antenas de transmisión y recepción. La propagación de las líneas espaciales directas es llamada transmisión por línea vista, esta transmisión está limitada por la curvatura de la tierra y los obstáculos que se interpongan en la línea vista. En la figura 4 se muestran los dos tipos de ondas espaciales.

Figura 4. Sistema de transmisión con ondas espaciales

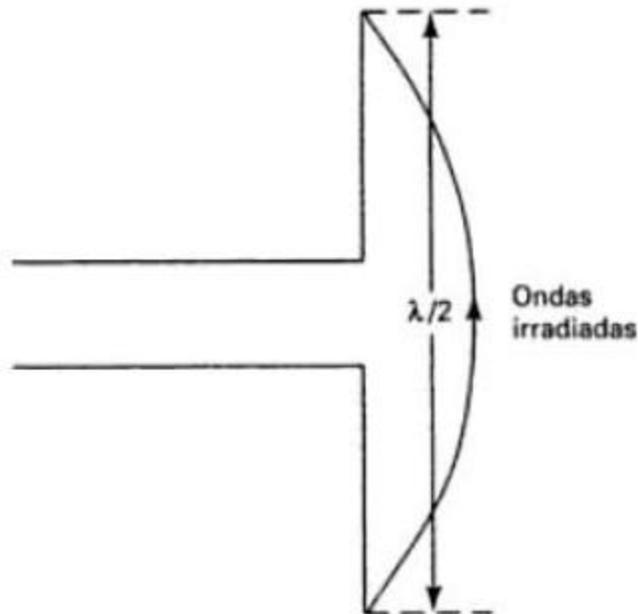


Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 361.

## 1.6. La antena

Es un material conductor metálico capaz de emitir y recibir ondas electromagnéticas hacia y desde el espacio libre; por supuesto que las antenas utilizadas en telecomunicaciones no son solo un simple conductor, estas ya son arreglos de material conductor, los cuales pueden emitir y recibir ciertas frecuencias. Una antena transmisora transforma voltajes en ondas electromagnéticas y una antena receptora realiza la función inversa. En la figura 5 se muestra el diagrama de una antena dipolo.

Figura 5. **Diagrama de antena dipolo de media onda**



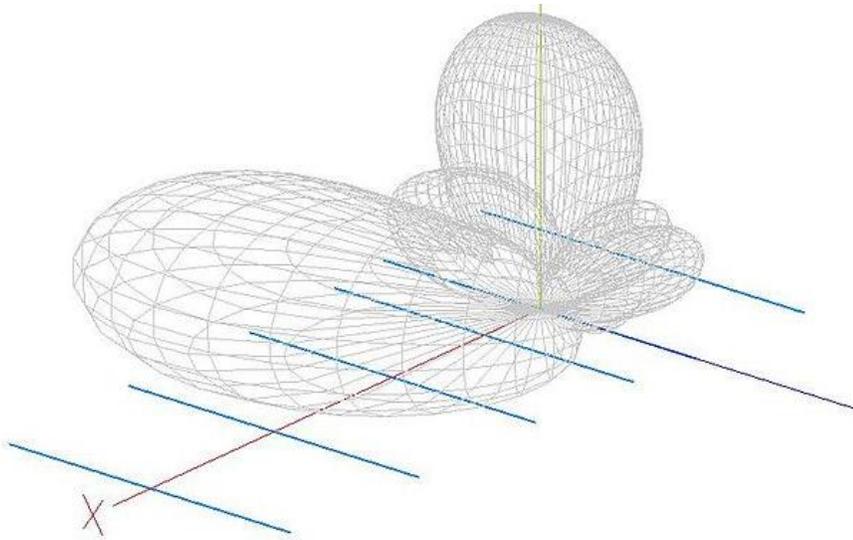
Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 372.

Existe una gran diversidad de tipos de antenas, debido a que las necesidades son muchas, las más utilizadas en telefonía son:

### 1.6.1. Antenas direccionales

Concentran un buen porcentaje de la energía radiada en una o varias direcciones, con el fin de tener el control de la zona en la cual se quiere radiar. En la figura 6 se muestra el diagrama de campo de una antena Yagi.

Figura 6. **Diagrama tridimensional de campo lejano de antena Yagi**

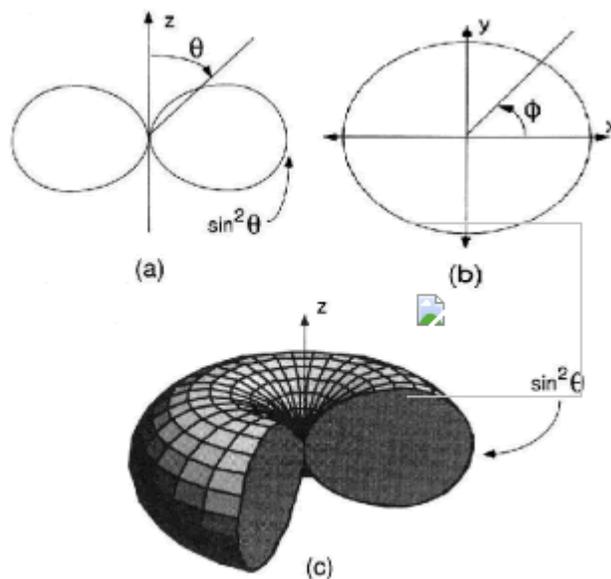


Fuente: *Antena Yagi*. [https://es.wikipedia.org/wiki/Antena\\_Yagi](https://es.wikipedia.org/wiki/Antena_Yagi). Consulta: mayo 2014.

### 1.6.2. Antenas omnidireccionales

Son las antenas más parecidas a la antena isotrópica, la diferencia es que la antena omnidireccional tiene un patrón de radiación con forma de una dona. Este tipo de antenas se utilizan cuando se necesita cubrir una zona reducida y radial, los *access point* utilizan estos tipos de antena. En la figura 7 se muestra el diagrama de campo de una antena omni.

Figura 7. Diagrama tridimensional de campo lejano de antena omni



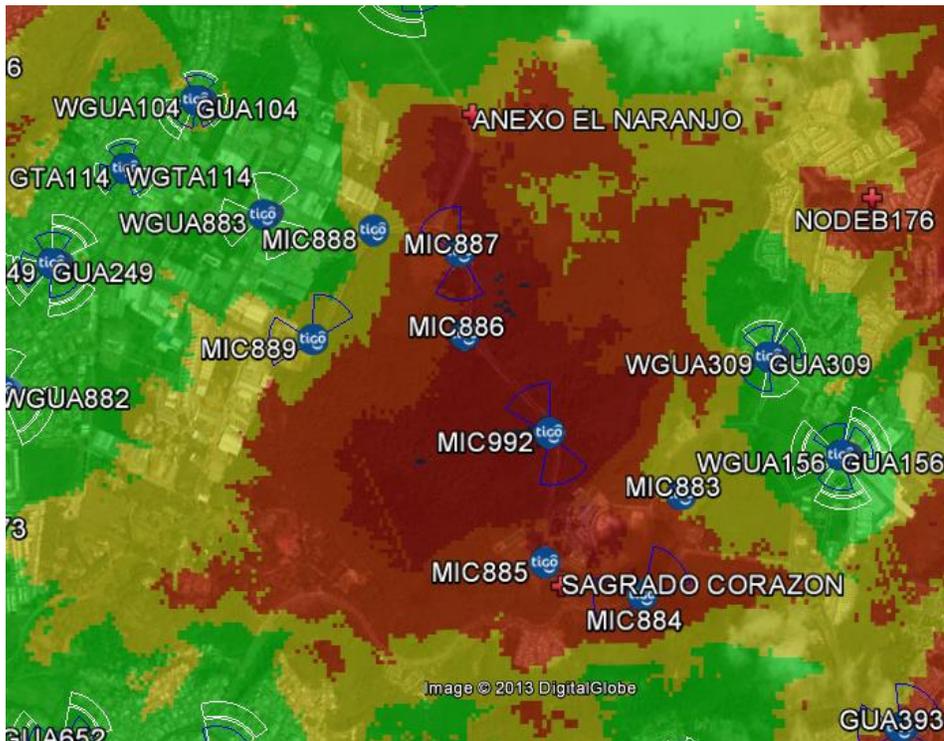
Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 386.

## 1.7. Diagrama de radiación de una antena

Es la representación gráfica de la radiación de la antena, los parámetros usados en la lectura de la misma son: coordenadas, azimut y elevación, estos parámetros sirven como guía para el diseño de coberturas de la antena.

Por supuesto que hay herramientas que dan estas coberturas, una de ellas es el ASSET; utilizando cálculos estadísticos se puede predecir con qué niveles de potencia radiará y a qué distancia lo hará una antena. En la figura 8 se muestra el cálculo de cobertura de sitio en herramienta ASSET.

Figura 8. Diagrama de propagación de RF en red de telefonía celular



Fuente: elaboración propia, con programa Asset.

## 1.8. Parámetros de una antena

Estos parámetros son utilizados para clasificar el tipo de antena y el uso que se le dará. Los parámetros fundamentales de la antena son los siguientes:

### 1.8.1. Ancho de banda

Rango de frecuencias en el cual la antena es óptima y sus parámetros cumplen con determinadas características que hacen que la misma trabaje efectivamente.

### 1.8.2. Directividad

Relación que existe al comparar la intensidad de radiación de una antena direccional entre la intensidad de radiación de una antena isotrópica, las dos radiando a una misma potencia total, la directividad se expresa en decibelios medidos con respecto a una antena isotrópica (dBi). En la figura 9 se detalla la fórmula para el cálculo de directividad.

Figura 9. **Fórmula para calcular directividad**

$$D = 10 \cdot \log(E(\text{max})/E(\text{iso})) \text{ dBi}$$

Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 377.

### 1.8.3. Ganancia

Es la ganancia de potencia en la dirección de máxima radiación, se produce cuando se concentra la potencia en zonas específicas del diagrama de radiación. Este parámetro se produce cuando se tiene un efecto de directividad de la antena, las dimensionales de ganancia dependen respecto a qué se le comparó, si es una antena isotrópica se habla de decibelios medidos con respecto a una antena isotrópica (dBi) y si se trata de una antena direccional decibelios medidos con respecto a una antena dipolo (dBd). En la figura 10 se detalla fórmula para el cálculo de ganancia.

Figura 10. **Fórmula para calcular ganancia**

$$G = 10\log[4\pi \cdot E(\max)/P(\text{in})]$$

Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 377.

### 1.8.4. Eficiencia

Relación que compara la potencia radiada y la potencia entregada a la antena, también se puede definir como la relación ganancia/directividad. Prácticamente este dato indica qué tan buena es la antena para radiar, mientras más se acerca a la unidad será más eficiente la antena, este parámetro es adimensional. En la figura 11, se detalla la fórmula para el cálculo de eficiencia.

Figura 11. **Fórmula para calcular eficiencia**

$$E = P(r)/P(in) = G/D$$

Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 377.

### **1.8.5. Impedancia de entrada**

La impedancia de entrada de una antena se mide en sus terminales. Es la relación entre tensión y corriente, se compone de una parte real y una imaginaria, la parte real se denomina resistencia de antena y la parte imaginaria reactancia. Cuando se realiza una conexión de antena-*feeder*, lo que se busca en el conector es la máxima transferencia de potencia y esto se logra anulando la reactancia de la impedancia de entrada.

### **1.8.6. Ancho de haz**

Es un parámetro de radiación que se calcula con el diagrama de radiación, se puede definir el ancho de haz a -3 dB que es el intervalo del ángulo en el que la densidad de potencia radiada es la mitad de la potencia máxima en la dirección principal de radiación.

### **1.8.7. Resistencia de radiación**

Cuando se habla de resistencia de radiación, se hace teniendo en cuenta que no se puede medir de forma directa. Es igual a la relación de la potencia radiada por la antena entre el cuadrado de la corriente en el punto de alimentación. En la figura 12 se detalla fórmula para cálculo de resistencia de radiación.

Figura 12. **Fórmula para calcular resistencia de radiación**

$$R_r = P / i^2$$

Siendo:

$R_r$  = resistencia de radiación (ohms)

$P$  = potencia radiada por la antena (watts)

$i$  = corriente de la antena en el punto de alimentación (amperes)

Fuente: WAYNE, Tomasi. *Sistema de Comunicaciones Electrónicas*. p. 376.

## **1.9. Tipos de modulación para transmisión RF**

Las modulaciones de información por medio de señales de radiofrecuencia son utilizadas con el fin de que los datos transmitidos sean más inmunes al ruido electromagnético.

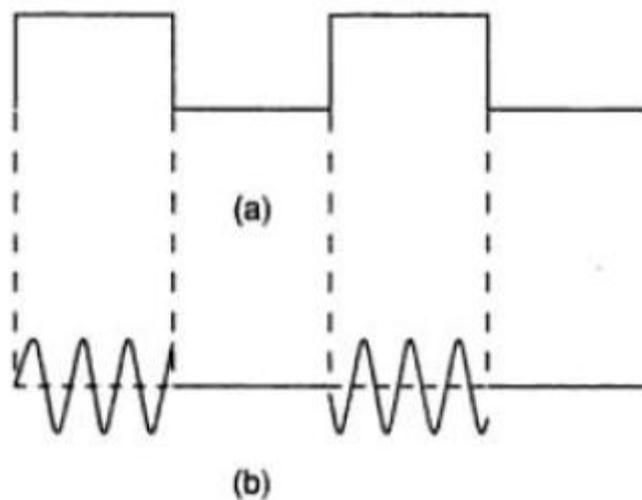
### **1.9.1. Modulación por desplazamiento de amplitud (ASK)**

En este tipo de modulación se representan los datos digitales como variaciones de amplitud de la onda portadora en función de los datos a enviar, explicando, de manera concisa, que la amplitud de una señal portadora análoga varía conforme a la corriente de bit modulando la señal, manteniendo la frecuencia y la fase constante. El nivel de amplitud puede ser usado para representar los valores binarios 1 y 0, se puede pensar en la señal portadora como un interruptor encendido/apagado.

En la señal modulada, el valor lógico 0 es representado por la ausencia de una portadora y el 1 es representado por la presencia de una portadora.

Al igual que la modulación AM, ASK es también susceptible al ruido atmosférico, distorsiones y condiciones de propagación. Esto requiere una amplitud de banda excesiva, lo que significa un gasto de energía; ahora, los procesos de modulación y demodulación son más económicos. La técnica de modulación ASK es también utilizada comúnmente para transmitir datos digitales sobre fibra óptica, para los transmisores led, el valor binario 1 es representado por un pulso corto de luz y el valor binario 0 por la ausencia de luz. En la figura 13, se muestra gráfica de modulación ASK.

Figura 13. **Representación gráfica de la modulación ASK**



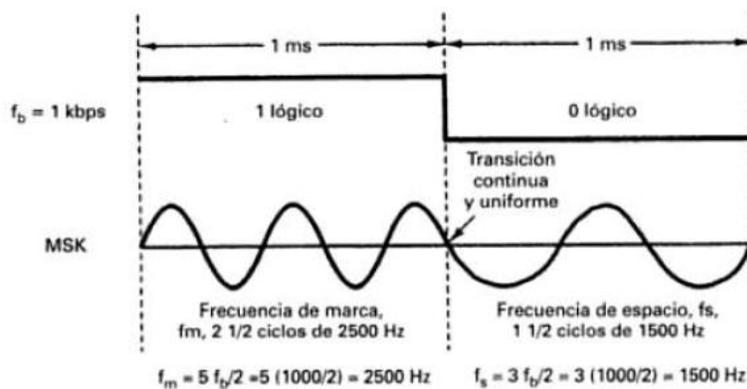
Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 471.

### 1.9.2. Modulación por desplazamiento de frecuencia (FSK)

La técnica de modulación por desplazamiento de frecuencia (FSK) se basa en la transmisión de información digital binaria utilizando dos frecuencias diferentes, la moduladora solo varía entre dos valores de tensión discretos formando un tren de impulsos de valor 1 o 0. Esta señal es la información que se desea enviar; la relación de cambio a la entrada del modulador se le llama *bitrate* y tiene como unidad el bit por segundo (bps), y a la relación de cambio a la salida del modulador se le llama *baudrate*, que es la velocidad o cantidad de símbolos por segundo.

En FSK el *bitrate* es igual al *baudrate*, es por eso que un 0 se representa con una frecuencia  $f_1$  y el 1 se representa con una frecuencia  $f_2$ . El dispositivo modulador usa un VCO, que es un oscilador cuya frecuencia varía en función del voltaje aplicado. En la figura 14, se muestra la gráfica de modulación FSK.

Figura 14. Representación gráfica de la modulación FSK



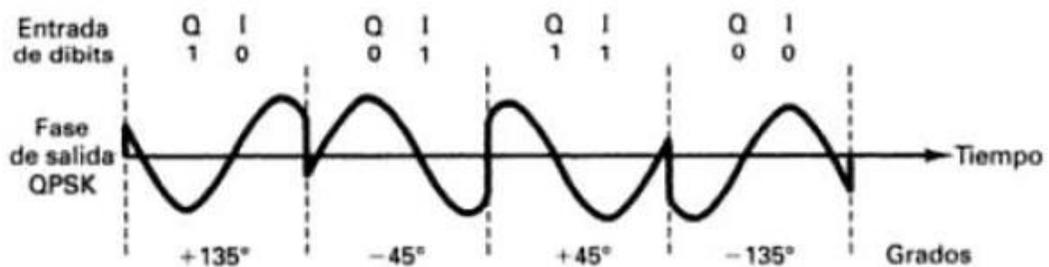
Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 477.

### 1.9.3. Modulación por desplazamiento de fase (PSK)

Es una modulación angular que consiste en hacer variar la fase de la portadora entre un número de valores discretos, ya que la señal moduladora es digital y consta de dos estados, los desplazamientos se harán en solo dos fases.

En la modulación PSK, la fase de la señal portadora representa cada símbolo de información de la señal moduladora, con un valor angular que el modulador elige entre un conjunto discreto de  $n$  valores posibles. Un modulador (PSK) representa la información mediante el valor absoluto de la fase de la señal modulada, este valor se obtiene al comparar la fase de la señal modulada con la fase de la señal sin modular. En la figura 15 se muestra la gráfica de modulación PSK.

Figura 15. Representación gráfica de la modulación PSK



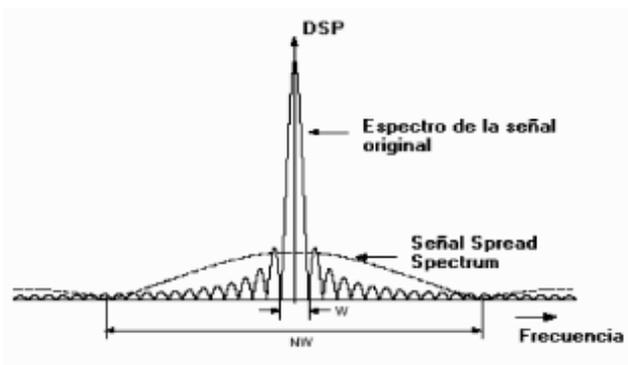
Fuente: WAYNE, Tomasi. *Sistema de comunicaciones electrónicas*. p. 486.

#### 1.9.4. Modulación de espectro expandido

Consiste en expandir la información por una banda de frecuencia más ancha que una banda necesaria para dicha información, con el propósito de contrarrestar el ruido externo y distorsiones que se tienen en la propagación. El método consiste en codificar la señal por separado, asignando un código a cada usuario, luego se decodifica cuando este llega a su destino. La expansión se garantiza aplicando señales pseudoaleatorias, esto es denominado código expensor.

En la recepción de la señal, la señal de información se ve como un ruido si el receptor no conoce el código que se aplicó. Debido a los niveles bajos de potencia a la que se transmite la señal de información el ancho de banda es bajo. De esta manera, la modulación de espectro expandido se optimiza para contrarrestar el ruido, reduciendo los efectos producidos por el mismo. En la figura 16, se muestra gráfica de la densidad espectral de una señal *spread spectrum*.

Figura 16. Densidad espectral de una señal *spread spectrum*

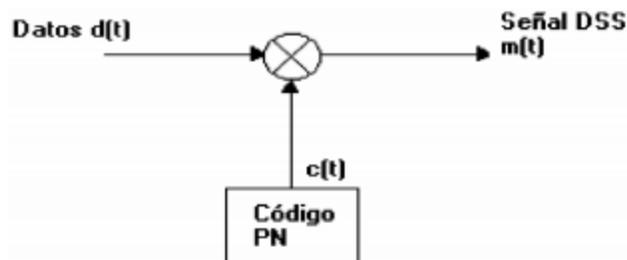


Fuente: Universidad Tecnológica de Pereira. *Repositorio núm. 41*. p. 304.

### 1.9.5. Modulación wifi

Las modulaciones más utilizadas cuando se trata de señal wifi son: DBPSK Y DQPSK, para velocidades de transmisión de 1 y 2 Mbps respectivamente. La técnica DSSS (secuencia directa de espectro extendido) también es utilizada en wifi y usa una secuencia chip de 11 bits, llamada también secuencia *barker*, esta ensancha el espectro 11 veces su tamaño original, pero hay una reducción de potencia RF debido al tamaño del espectro utilizado. En la figura 17, se muestra la técnica de modulación DSSS.

Figura 17. Diagrama de bloques de técnica de modulación DSSS



Fuente: Universidad Tecnológica de Pereira. *Repositorio núm. 41*. p. 304.

Todas las estaciones en una red wifi 802.11 utilizan la misma secuencia de 11 bits, en el transmisor del sistema, una función *exor* combina la trama con la secuencia *barker*, con el fin de que toda la trama se combine con la secuencia de 11 bits. En el receptor está la convolución de la señal emitida y procesada con la secuencia *barker*, luego se corre para recuperar la trama y evitar interferencias.

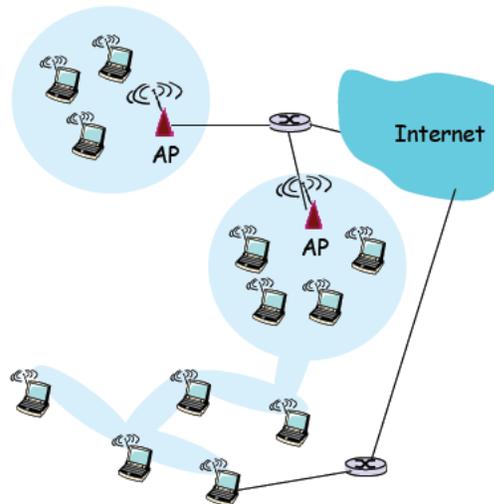


## 2. REDES WIFI

### 2.1. Arquitectura de redes wifi

La tecnología wifi fue concebida con el objetivo de hacer pequeñas redes inalámbricas en empresas de todo tipo, con esta tecnología se lograba utilizar menos cable, haciendo más fácil, algunas veces, económica la construcción de redes locales. Su arquitectura está basada en diseños mucho más sencillos que los que se hacían con cable, pero, a pesar de su sencillez, son redes muy estables en espacios reducidos. El uso de esta tecnología ha evolucionado utilizando la misma estructura hacia redes de área extendida, principalmente en lugares urbanos. En la figura 18, se muestra un tipo de arquitectura wifi.

Figura 18. Diagrama de arquitectura red wifi



Fuente: Unavarra. *Arquitectura de redes y sistemas ingeniería telemática*. p. 6.

## **2.1.1. Elementos de una red wifi**

Los elementos que conforman una red wifi son los siguientes:

### **2.1.1.1. Punto de acceso (AP)**

Este dispositivo es la unión entre la red fija y la red wifi. Se encarga de gestionar la información recibida de la red fija y la hace llegar a los dispositivos de forma inalámbrica, esto lo puede hacer con varios dispositivos a la vez, ya que en una sola sala se pueden encontrar varios AP, dependiendo de la demanda de conexiones wifi en la sala y del ancho de banda que se desee proporcionar. La zona de cobertura dependerá de la ganancia de las antenas, pero aproximadamente es de 20 metros cuadrados (m<sup>2</sup>).

### **2.1.1.2. Antena**

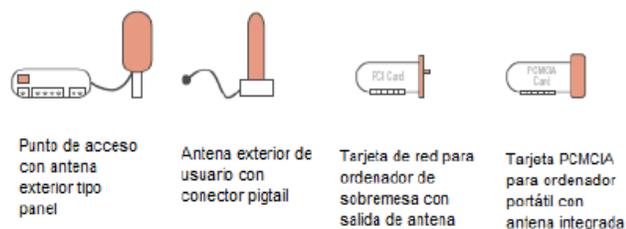
Encargada de radiar en forma de energía electromagnética la señal que el AP está entregando, de igual manera, capta la energía y la transforma en señal proveniente de los dispositivos. En este caso se tiene una antena receptora y otra transmisora en el mismo punto.

El ancho de banda de las antenas está en el rango de los 2,4 Ghz a los 5 Ghz y son de tipo omnidireccionales.

### 2.1.1.3. Tarjeta wifi

Es una tarjeta que controla una red de área local y cumple con la certificación wifi, por lo tanto, permite la conexión de un terminal de usuario en una red 802.11. Existen diferentes modelos de tarjetas dependiendo del subestándar a, b o g, también hay tarjetas mixtas. Estos dispositivos externos se conectan a las ranuras PCI, PCMCIA, o bien, al puerto USB. Las tarjetas se diferencian de una tarjeta *ethernet* en el cifrado de datos, el identificador ESSID, el canal y el ajuste de velocidad. En la figura 19 se muestran los elementos de una red wifi.

Figura 19. Imagen de los elementos de una red wifi



Fuente: *Las tecnologías wifi y Wimax*. [http://www.dip-badajoz.es/agenda/tablon/jornadaWIFI/doc/tecnologias\\_wifi\\_wmax.pdf](http://www.dip-badajoz.es/agenda/tablon/jornadaWIFI/doc/tecnologias_wifi_wmax.pdf). Consulta: junio 2014.

## 2.2. Topología de una red wifi

En las redes wifi se pueden encontrar dos tipos de escenarios, las redes sin infraestructura y redes en modo de infraestructura.

### 2.2.1. Redes sin infraestructura

Topología poco utilizada debido a que no tiene un punto de acceso común para las terminales, la conexión entre terminales se hace punto a punto, tal como un radioenlace convencional. En la figura 20 se puede observar el diagrama este tipo de conexión al cual se le ha llamado AD HOC, un ejemplo de ello es la conexión entre dos computadoras utilizando wifi.

Figura 20. Diagrama de red wifi AD HOC

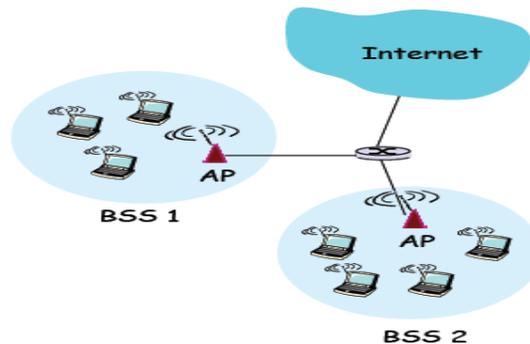


Fuente: Unavarra. *Arquitectura de redes y sistemas ingeniería telemática*. p. 6.

### 2.2.2. Redes en modo de infraestructura

Este modo gestiona y transporta cada paquete a su destino desde un punto de acceso AP, lo cual mejora la velocidad de conjunto cuando están conectados varios dispositivos a la vez. Para esta topología, la tarjeta de red se configura automáticamente para utilizar el mismo canal que del punto de acceso más próximo. En esta infraestructura existen dos tipos de conexiones, uno es la interconexión, una red wifi con una red sobre cables que bien puede ser una red local o un acceso ADSL, y la otra es la interconexión de dos usuarios wifi que pueden o no estar en el mismo lugar, un ejemplo de esta topología puede ser la red wifi de un campus universitario (ver figura 21).

Figura 21. **Diagrama de red en modo infraestructura**



Fuente: Unavarra. *Arquitectura de redes y sistemas ingeniería telemática*. p. 7.

### 2.3. Estándares wifi

La creación de los estándares que dieron vida a wifi fue un trabajo llevado a cabo por la Asociación Internacional de Ingenieros Electrónicos y de Telecomunicaciones, conocido por las siglas IEEE, esta asociación se encarga de realizar conferencias y redacción de estándares como el *ethernet*.

La IEEE dispone de una extensa línea de estándares de área local, el 802, dentro de esta familia existen diferentes subfamilias, todas dependen del alcance que se quiere dar con el estándar. Ejemplos de ello son el estándar 802.15.4, más conocido como zigBee, este es dedicado a las redes de sensores donde se necesita poca corriente pero diversidad de topología. El 802.15.1, más conocido como Bluetooth, es utilizado en dispositivos móviles para transferencia de datos a alta velocidad pero a corta distancia, aproximadamente 10 a 20 metros. Si se requiere de alta velocidad pero distancia de cobertura de kilómetros, se tiene el estándar 802.16, más conocido como Wimax.

Entre los tres estándares existe otro que, se podría decir, está a la mitad entre distancia y capacidad, no es ni muy reducido ni muy extendido, se trata del estándar 802.11, más conocido como wifi. Estos protocolos nunca se realizan cerrados, siempre se dejan abiertos a mejoras para hacer más eficiente el desempeño, cuando estos van cambiando se les agrega una letra minúscula seguido del nombre que tiene. Los subestándares que se han trabajado tienen los cambios en los 2 parámetros principales, los cuales son la velocidad de transmisión de datos y la banda de frecuencia de uso. Con base en estos se han definido hasta ahora los estándares siguientes:

### **2.3.1. Estándar 802.11b**

Define la creación de redes inalámbricas con frecuencia 2,4 Ghz con una modulación que permite alcanzar velocidades de hasta 11 Mbps, esto da una velocidad efectiva para los usuarios de la mitad de la velocidad pico 5,5 Mbps. Hasta hace poco era el estándar utilizado en las redes wifi, pero ahora ha sido sustituido por el estándar 802.11g.

### **2.3.2. Estándar 802.11a**

Define la creación de redes inalámbricas con frecuencia de 5 Ghz. La información de cada usuario se transmite modulando esta frecuencia digitalmente. La modulación utilizada en este estándar es menos susceptible a la interferencia y a las velocidades altas de movimiento, por ejemplo el movimiento dentro de un metro. Las velocidades de transmisión de datos pueden alcanzar los 54 Mbps, teniendo una velocidad efectiva de 36 Mbps, mucho más alta que el estándar 802.11b.

### **2.3.3. Estándar 802.11g**

Este estándar mejora al 802.11b, siempre trabajando a la frecuencia 2,4 Ghz, pero con una variación en la modulación, ya que esta es idéntica a la del estándar 802.11a, alcanzando una máxima velocidad de transmisión de 54 Mbps, una velocidad efectiva de 36 Mbps. Uno de sus beneficios es que su capacidad de trabajar con el mismo equipo que el 802.11b, hace que la migración al nuevo estándar pueda ser más lenta y mantener el equipo anterior en funcionamiento.

### **2.3.4. Estándar 802.11n**

Su objetivo es mejorar el alcance, en gran parte, el ancho de banda de la red wifi, de manera que este sea comparado con una red de área local fija, la velocidad de transmisión de datos es de aproximadamente 100 Mbps.

La solución que se está utilizando en este estándar tiene como fin reducir las ineficiencias de los otros estándares, se trata de aprovechar lo que en un principio es una desventaja para los sistemas inalámbricos. Estas desventajas son las interferencias provocadas por el eco que genera la misma señal en paredes y objetos, lo que hace que se repitan las señales ligeramente distorsionadas y que la información, al llegar al objetivo, sea por lo menos duplicada.

La innovación más importante de este estándar es la utilización de más de una antena en el AP y en cada terminal. Esto hace que cada una de las antenas extras obtengan los rebotes, con toda esa información se utiliza el principio de superposición y se genera una sola señal de información relativamente sin errores. Al mismo tiempo, se puede enviar más de una señal a

la vez por la diversidad de las antenas, así, combinando ambos efectos, se consigue una transmisión más eficaz y robusta contra el ruido, esta técnica es llamada MIMO (múltiple entrada, múltiple salida).

### **2.3.5. Estándar 802.11i**

Este estándar contiene aspectos muy importantes para la popularización de las redes wifi. Todas las tecnologías de radio son vulnerables por el hecho de utilizar el aire como medio de transporte, así que la transmisión es accesible a todo el mundo que tenga cobertura del servicio, por eso se tienen que incluir medidas de seguridad muy estrictas a la hora de implementar una red wifi. En términos generales los requerimientos de seguridad de una red de radio son:

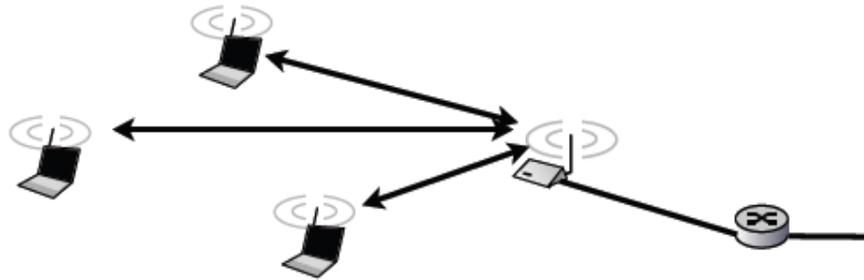
#### **2.3.5.1. Autenticación**

Este requerimiento es una garantía que da la confianza de que los que están conectados a la red wifi han pasado por el proceso de autenticación para utilizar la red y también a los usuarios les da la confianza de que el proveedor del servicio es ser quien dice ser. Esto asegura que la red no sea utilizada por personas que no son miembros de ella. Existen diferentes tipos de autenticación, a continuación algunos de ellos:

##### **2.3.5.1.1. Autenticación abierta**

Viene por defecto en los dispositivos y permite que cualquier dispositivo se conecte, la transmisión de información no lleva ningún tipo de cifrado. En la figura 22 se puede observar el diagrama de autenticación abierta.

Figura 22. **Diagrama de autenticación abierta**

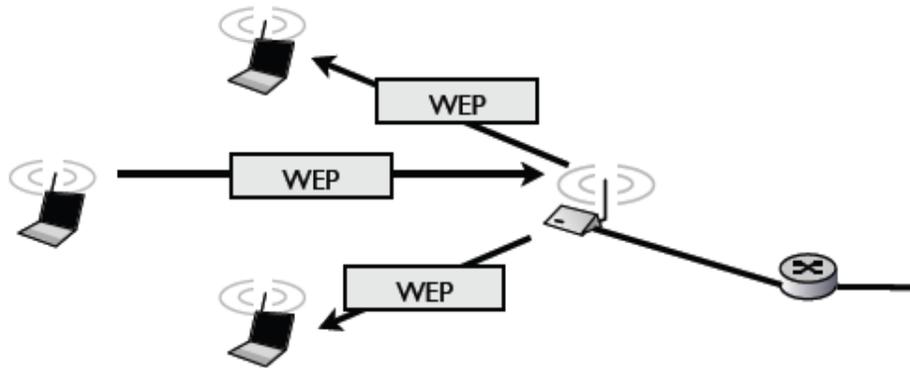


Fuente: Unavarra. *Arquitectura de redes y sistemas ingeniería telemática*. p. 33.

#### **2.3.5.1.2. Autenticación de clave compartida**

Utiliza la clave WEP para autenticar a un usuario, consiste en el envío de un mensaje por parte del AP al cliente, el cual debe responder con la clave WEP cifrada; si el proceso es exitoso se hace de igual forma desde el cliente al AP y así se produce una autenticación mutua. Este tipo de cifrado es muy vulnerable, ya que la clave es fácil de conseguir y por ende no se le considera seguro (ver figura 23).

Figura 23. **Diagrama de autenticación de clave compartida**

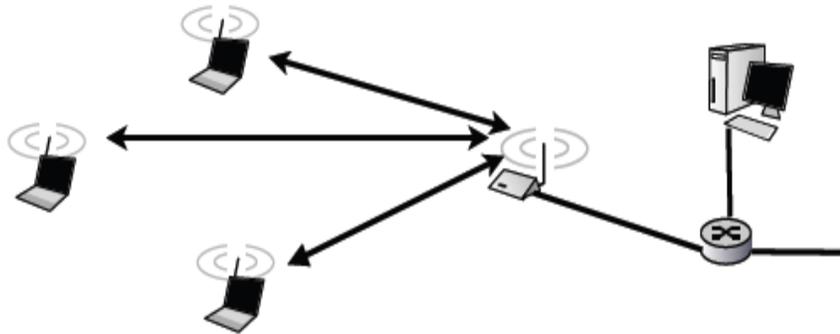


Fuente: Unavarra. *Arquitectura de redes y sistemas ingeniería telemática*. p. 31.

#### **2.3.5.1.3. Autenticación por dirección mac**

Consiste en tener un listado de direcciones MAC de los clientes que van a estar autorizados a entrar a la red, este listado se debe encontrar en cualquier AP de la red. También es vulnerable ya que es fácil de obtener las listas MAC de los clientes desde un AP específico.

Figura 24. **Diagrama de autenticación por dirección MAC**



Fuente: Unavarra. *Arquitectura de redes y sistemas ingeniería telemática*. p. 35.

### **2.3.5.2. Confidencialidad**

Garantía que permite estar la seguridad y confiabilidad de que los usuarios que han sido autenticados para estar en la red sean personas con permiso para estar en la misma. Para obtener esta confidencialidad, se utiliza un tipo de cifrado en la transmisión de datos, de tal manera que estos vayan protegidos y no sean robados por personas ajenas a la red.

Un sistema utilizado para el cifrado de la información es el WEP. Este sistema fue propuesto por el Comité 802.11, comprime y cifra los datos que se van a transmitir a través de ondas de radio, es vulnerable ya que es sencillo obtener el cifrado de los datos. La clave es fija para todos los usuarios y nunca cambia, este cifrado es soportado por la mayoría de los productos wifi.

### **2.3.5.3. Integridad**

Da la confianza de que los datos recibidos por una terminal son los datos reales enviados y que no fueron alterados o cambiados mientras estuvieron en el medio de transmisión, o bien, sufrir un robo de la información por usos inadecuados.

### **2.3.5.4. Disponibilidad**

Tiene como propósito mantener el acceso en cualquier momento a los usuarios autorizados, además, esta información debe ser sencilla de obtener, todo esto en el área de cobertura de los AP.

## **2.4. Limitaciones tecnológicas de la familia 802.11**

Toda la familia del estándar 802.11 tiene limitaciones, por lo que es conveniente conocerlas antes de tomar una decisión con respecto a cobertura, alcance y velocidades. A continuación se nombran los limitantes:

### **2.4.1. Alcance**

Aunque comercialmente se habla de un promedio de alcance de 100 metros, todo va a depender del escenario en el cual se presente la solución. Existen muchas variables que pueden influir, como obstáculos cercanos, clima e interferencias cercanas. Esto es al aire libre, pero de igual forma, dentro de un edificio las mismas paredes u otras redes wifi pueden influir en el alcance.

#### **2.4.2. Ancho de banda**

En teoría, los estándares nombrados pueden alcanzar velocidades altas. Sin embargo, esto es sin incluir la ineficiencia en los protocolos de transmisión, ni las interferencias, que son muy comunes en sistemas RF. Estos problemas hacen que el sistema vaya utilizando codificaciones más robustas para disminuir la pérdida de información, lo cual impacta en la disminución drástica de la velocidad de transmisión, por eso se encuentran algunas veces AP con velocidades de descarga de 5 Mbps, 2 Mbps o hasta 1 Mbps.

#### **2.4.3. Calidad de servicio**

Desde el punto de vista de los usuarios, no todo el tráfico tiene la misma importancia, una llamada VoIP no tiene la misma prioridad que el envío de ficheros, por lo que se debe priorizar una llamada. Pero en una red wifi, no existe ningún mecanismo que pueda discernir entre un servicio con más importancia que otro. Por lo tanto, se puede decir que wifi es poco eficiente cuando se le pide entregar tráfico con altos niveles de calidad, ya que no va a priorizar un servicio de otro, dando una mala calidad al servicio más exigente.

#### **2.4.4. Seguridad**

En un principio la tecnología inalámbrica era muy vulnerable en el sentido de seguridad, ya que se habían enfocado todos los recursos en transmitir vía RF datos a alta velocidad y no en resguardar estos datos. Pero, conforme se dio la necesidad de que estos datos fueran confidenciales, se empezaron a hacer mejoras; el estándar 802.11i tiene fuerte sistema de seguridad casi comparado con el de una red fija.

### 2.4.5. Movilidad

Popularmente se considera a una red wifi móvil, debido a que no se necesita ningún tipo de alambre para conectarse y que, al cambiar de ubicación, se puede seguir conectado, toda vez se esté bajo cobertura del AP. Pero, las limitaciones de movilidad se dan, si se quiere utilizarla moviéndose en un vehículo o incluso caminando hacia una zona de no cobertura. Esta es una ineficiencia del estándar que no se puede modificar.

### 2.5. Itinerancia en redes wifi

Es una característica de las redes wifi que permite cambiar de islas wifi sin necesidad de configuración de la PC o del móvil. Para que se permita la itinerancia entre los diferentes puntos de acceso de una red wifi, se debe configurar cada uno de los AP con canales de frecuencias distintos, de manera que cuando se crucen las coberturas de los AP no se tenga inconsistencia en el salto de un AP a otro.

Tabla I. **Canales de frecuencia utilizado en wifi banda 2,4 Ghz**

Canal	Frecuencia	Canal	Frecuencia
1	2 412 Mhz	8	2 447 Mhz
2	2 417 Mhz	9	2 452 Mhz
3	2 422 Mhz	10	2 457 Mhz
4	2 427 Mhz	11	2 462 Mhz
5	2 432 Mhz	12	2 467 Mhz
6	2 437 Mhz	13	2 472 Mhz
7	2 442 Mhz	14	2 484 Mhz

Fuente: elaboración propia.

La movilidad en una red wifi aún está en constante evolución, debido a que no se ha logrado tener saltos de AP a altas velocidades, tampoco se ha podido estandarizar todas las marcas de proveedores de AP para que se tenga movilidad entre AP sin discriminar marca o modelos. Un ejemplo de itinerancia entre tecnologías se verá en el capítulo 3 con el wifi offload. Para resolver estos problemas se está trabajando en un nuevo estándar dedicado a la movilidad, este es el estándar 802.11p.

### **2.5.1. Estándar 802.11p**

Este estándar opera en el espectro de frecuencias 5,9 Ghz y el de 6,2 Ghz, diseñado especialmente para automóviles. Este será la base de las comunicaciones dedicadas de corto alcance y permitirá la comunicación entre vehículos en movimiento y carreteras inteligentes.

## **2.6. Futuras evoluciones de la tecnología wifi**

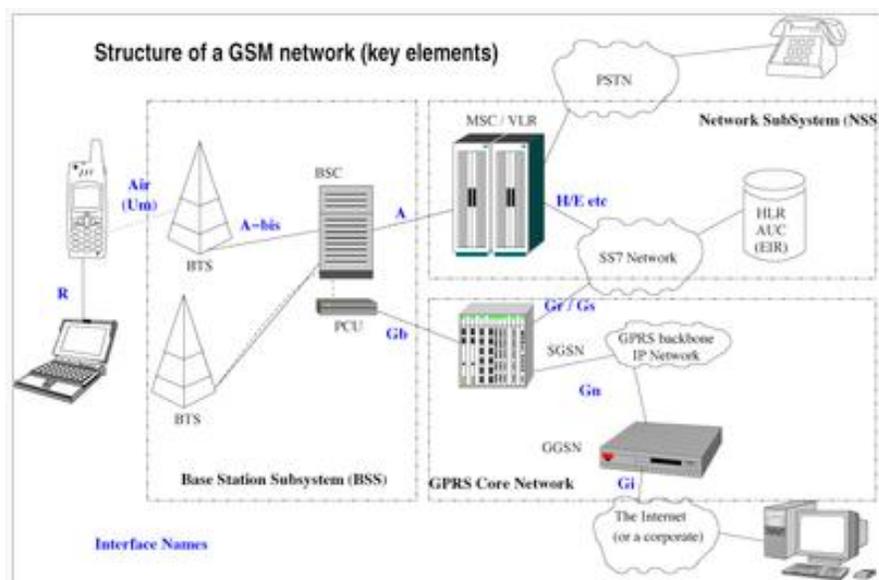
La evolución es constante en cualquier tipo de tecnología y prácticamente van todas de la mano, la tecnología wifi no es la excepción con los nuevos estándares.

### **2.6.1. Estándar 802.11r**

La principal característica es que permite a la red establecer protocolos de seguridad que se encargan de identificar a un dispositivo en el nuevo punto de acceso, antes de que abandone el actual y salte a él. Esta función permite que la transición entre nodos demore menos de 50 milisegundos, un lapso tan pequeño como este permite mantener una comunicación vía VoIP sin que existan cortes perceptibles por el usuario.

Esta función es de suma importancia en sistemas de comunicación inalámbricos tal y como ocurre en una red móvil 2G, 3G o 4G. En estas, la función es denominada *handover*, consiste en mantener una comunicación sin cortes mientras el usuario se mueve de una celda a otra, no importando si es celda hermana o vecina, ni si es de la misma tecnología o no.

Figura 25. Esquema de itinerancia en red GSM



Fuente: *Sistema global de comunicaciones.*

[http://es.wikipedia.org/wiki/Sistema\\_global\\_para\\_las\\_comunicaciones\\_m%C3%B3viles](http://es.wikipedia.org/wiki/Sistema_global_para_las_comunicaciones_m%C3%B3viles).

Consulta: junio 2014.

### **2.6.2. Estándar 802.11u**

Con este estándar, una red será capaz de permitir el acceso de un dispositivo en relación con una red externa de telecomunicaciones, como sucede con el *roaming*, incluso estos accesos pueden ser limitados en servicios.

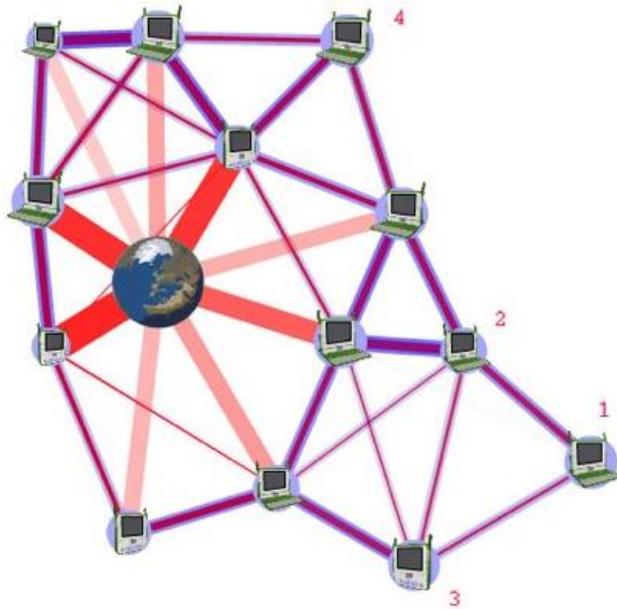
Viendo el lado del usuario, lo que se busca es mejorar su experiencia al momento de movilizarse largas distancias ya que no utilizará una larga fila de SSID, solo tendría que conectarse al AP de servicio wifi del hotel y podría hacer llamadas VoIP a larga distancia sin tanto protocolo.

### **2.6.3. Estándar 802.11s**

Su objetivo es crear una red inalámbrica mundial, entre sus principales armas para lograrlo están el bajo costo de del hardware y el software libre, con lo cual podrían salir beneficiados más de 1 billón de personas en el mundo.

Se trata de una serie de protocolos con el objetivo de crear redes malladas y autogestionables. Los dispositivos que se deben usar en este protocolo deben ser capaces de crear, de forma dinámica, rutas para la optimización del tráfico de información, así, cuando se tengan dispositivos defectuosos, se conseguirá mantener la cobertura por medio de otra ruta.

Figura 26. **Imagen de la arquitectura del estándar 802.11s**



Fuente: *Arquitectura de red estándar*. <http://wiki.laptop.org/go/Image>. Consulta: junio 2014.

### **3. ARQUITECTURA DE RED MÓVIL PARA DESCARGA DE DATOS ATRAVÉS DE REDES DE ACCESO WIFI**

#### **3.1. 3GPP versión R99**

Esta fue la primera versión UMTS, como sistema de acceso utilizó el WCDMA, que permite múltiples accesos por división de códigos y está soportado por un subsistema llamado red de radios. Este subsistema convive y es controlado por la MSC, elemento del *core* de GSM que controla las BSC como un gran *switch* de llamadas, todo esto para llamadas de voz. Cuando se trata de la conmutación de paquetes de datos, los elementos a controlar son la RNC y el SGSN.

#### **3.2. Arquitectura de red R99**

En este subsistema se encuentra la red de acceso UMTS que es una red de radio terrestre de acceso. Está compuesta por 2 elementos principales para su funcionamiento.

##### **3.2.1. Nodo B**

Este elemento tiene capacidad para controlar desde una hasta seis celdas físicas. Es el responsable de controlar los radios, los cuales son la interface que convierte la energía electromagnética de una señal proveniente de una terminal o celular a óptica. Esta señal es procesada en la BBU, la cual se encarga de empaquetarla y enviarla a través de la interface *Iub* hacia la RNC, que, simplificando su función, es como un *switch* que administra las rutas de

llamadas o de servicios adicionales de la red de telefonía 3G. En la figura 27 se presenta un nodo B en servicio.

Figura 27. **Nodo B en servicio**



Fuente: zona 1, ciudad de Guatemala.

### 3.2.2. RNC

Se encarga de controlar el nodo B, específicamente el control de recursos de radio y *handover* entre nodos. Se conecta hacia el *core* por medio de interface IU. Existen dos tipos de aplicaciones en el *core* una es la aplicación CS (*circuit switched*) la cual utiliza interface IU-C, y la otra es la aplicación PS (*packet switched*) esta utiliza una IU-P. En la figura 28 se presenta una RNC en servicio.

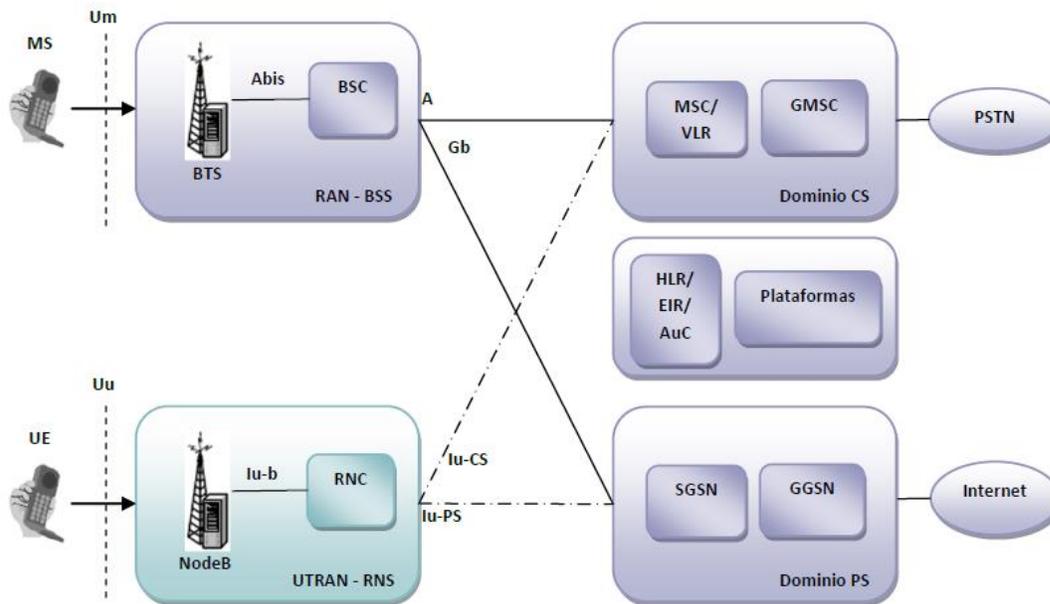
Figura 28. **RNC en servicio**



Fuente: municipio de Fraijanes, Guatemala.

En la figura 29 se muestra el modelo de la arquitectura R99, junto con la interacción entre UMTS y GSM, en el cual se especifica los dominios de CS y PS de la tecnología UMTS y la combinación de las dos tecnologías cuando se vuelve necesario cambiar de una tecnología a otra.

Figura 29. **Arquitectura de red 3GPP R99**



Fuente: Interactiv. *Documentos técnicos No.2.* p. 2.

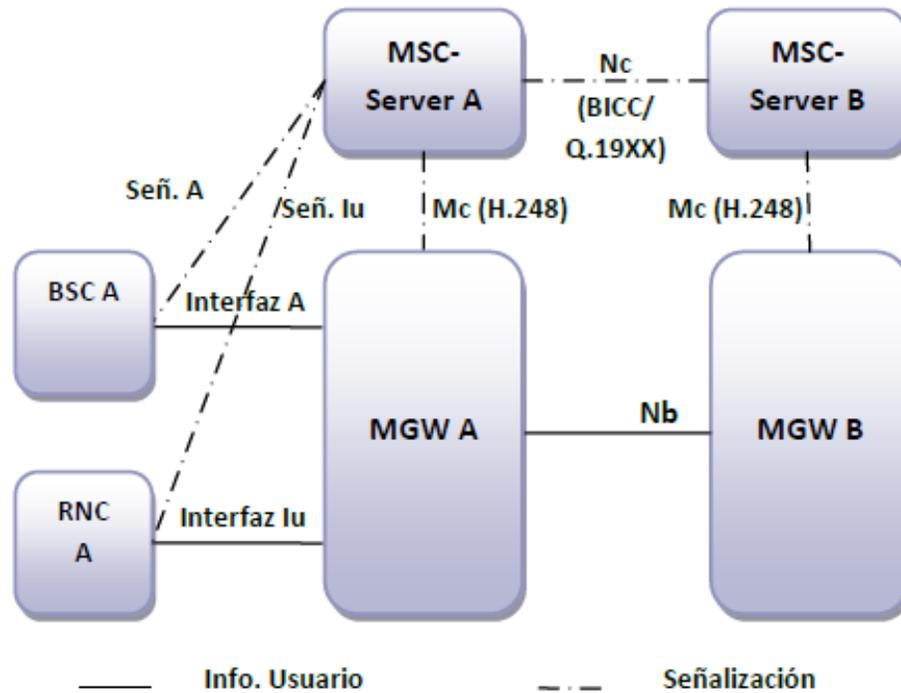
### 3.3. 3GPP versión 4

La modificación principal en esta arquitectura fue que se agregó el control independiente de la portadora, así, las principales funciones de la MSC del sistema R99 o GSM se reparten entre un nuevo elemento de red el MGW.

#### 3.3.1. *Media gateway*

Encargado de la función de transporte de flujos de información y control de recursos de información. En la figura 30 se detalla la arquitectura de esta nueva versión de 3GPP.

Figura 30. **Arquitectura de red BICC**



Fuente: Interactiv. *Documentos técnicos. No.2. p. 3.*

### 3.4. 3GPP versión 5

Versión que introduce HSDPA, el cual disminuye la latencia y eleva la tasa de mega bits por segundo. También en el *core* se implementa una versión preliminar del IMS, el cual se encarga de las sesiones multimedia que demande la terminal.

### **3.4.1. HSDPA**

Este concepto reduce la latencia y aumenta la tasa de transmisión a 14 Mbps en el enlace de descarga hacia el móvil, se basa en un esquema de modulación y codificación adaptivo.

En términos de arquitectura, la inclusión de HSDPA no altera la estructura lógica de la red de acceso, lo único que se requiere es la actualización de hardware y software en los nodos, ya que estos tendrán la función de control de paquetes para reducir la latencia.

### **3.4.2. Iuflex**

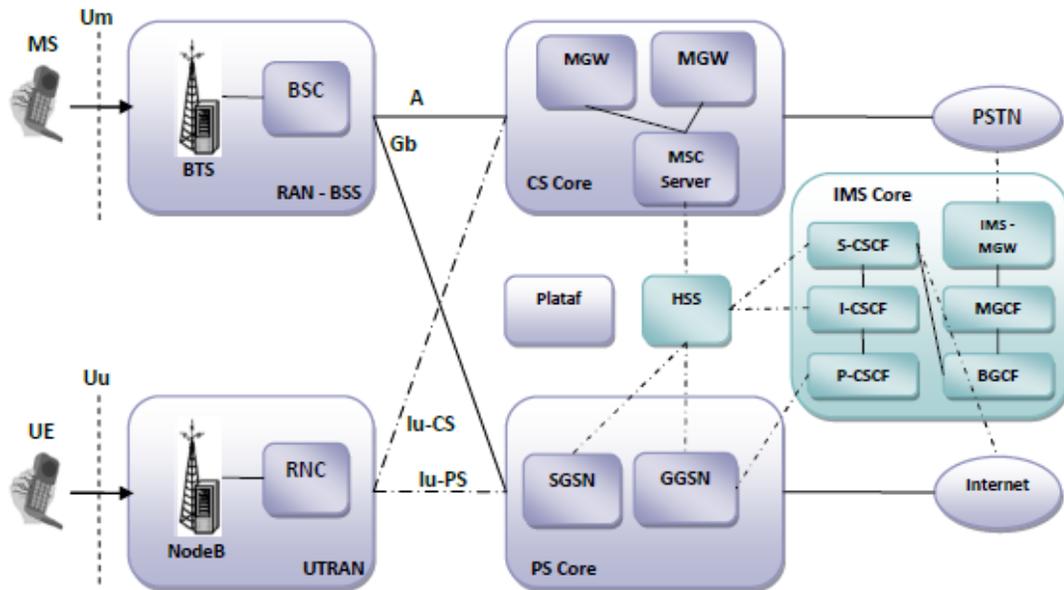
A nivel de radio, la IU proporciona un subsistema RAN a más de una MSC o SGSN. La ventaja de conectar varias MSC o SGSN es que permite tener redundancia para cuando uno de los elementos quede fuera de servicio. También ayuda con el balance de carga entre elementos y así tener una mejor utilización del recurso.

### **3.4.3. Pre IMS**

Manteniendo la tendencia de la convergencia a redes puramente IP, la red *core* evoluciona al nuevo subsistema IP multimedia (IMS), en la figura 29 se observa la integración al *core* que se tenía con anterioridad, en la cual la IMS no está integrada. Este subsistema utiliza un protocolo de inicialización de sesión y se encarga de abrir sesiones multimedia entre los distintos dispositivos de usuario.

En la figura 31 se presenta el diagrama de arquitectura de una red 3GPP R5, en la cual integra el IMS al core estándar de UMTS.

Figura 31. **Arquitectura de red 3GPP R5**



Fuente: Interactiv. Documentos técnicos No.2. p. 5.

### 3.5. Información general de la arquitectura wifi offload

El tráfico de la red móvil está creciendo exponencialmente, una tendencia global muy marcada, esto hace que los proveedores de servicios gestionen de manera eficiente su red para satisfacer la demanda de sus abonados. Uno de los problemas en la evolución es que, a nivel de radio, las leyes de la física limitan el crecimiento, el acceso a radio está llegando a los límites de la ley de Shannon, debido a que el espectro disponible para las aplicaciones de datos móviles es limitado.

Por lo tanto, se tiene un despliegue de tecnologías de celdas pequeñas, con el fin de poder focalizar el tráfico en zonas densas y de gran demanda de datos, como centros comerciales, estadios, estaciones de metro y campus universitarios. Una de las soluciones que las compañías de telefonía están implementando es el de wifi offload, a cual, además de ser rentable, ofrece una amplia gama de servicios. La solución cuenta con algunas características importantes a favor:

### **3.5.1. Despliegues existentes**

Reutilización de redes wifi de alguna empresa que quiera adquirir un servicio especial o velocidades altas de descarga de datos, o también en redes gubernamentales que quieran tener un servicio de datos robusto.

### **3.5.2. Disponibilidad de dispositivos que soportan la arquitectura**

En general, los dispositivos soportan casi cualquier tecnología, pasando por HSDPA, LTE y wifi así que es casi imposible de que al implementar wifi offload estos dispositivos no funcionen, si ese fuera el caso se trataría de un dispositivo obsoleto.

### **3.5.3. Rentabilidad**

En cualquier tecnología se debe hacer una inversión inicial fuerte, pero, en este caso, la inversión es menor e incluso es solo de complementar el *core* existente con la parte de wifi. A la vez, los AP y *switch* son sumamente más baratos que un nodo B y una RNC.

A la hora de estar implementado es más eficiente un AP que un nodo B en descarga de datos. Sin embargo, el tráfico está bien focalizado, porque de eso trata esta tecnología, no es para coberturas amplias sino para demanda de capacidad.

#### **3.5.4. Capacidad de espectro disponible**

A nivel mundial existe un buen trecho de espectro a utilizar en wifi, las dos bandas de trabajo más comunes son 2,4 Ghz y de 5 Ghz, un espectro más limpio y amplio que los utilizados en HSDPA y LTE. Estas características son las de mayor peso en la solución.

#### **3.6. Arquitectura wifi offload**

Dado que la mayoría de las empresas de telecomunicaciones tienen una red 3G desplegada, se describirá el método de acceso integrado de confianza 3GPP no IP al *core* 3G de paquetes MPC, en conjunto con la política asociada y la carga de control PCC.

La infraestructura de la red wifi para descarga de datos móviles consta de tres partes: la red de acceso de radio wifi, *gateway* wifi y los elementos de integración del *core* de paquetes. Estos elementos son fundamentales en la red wifi para que esta se encargue de la descarga masiva de datos, así como de la gestión de otra tarea muy importante que es la autenticación.

### **3.6.1. Autenticación**

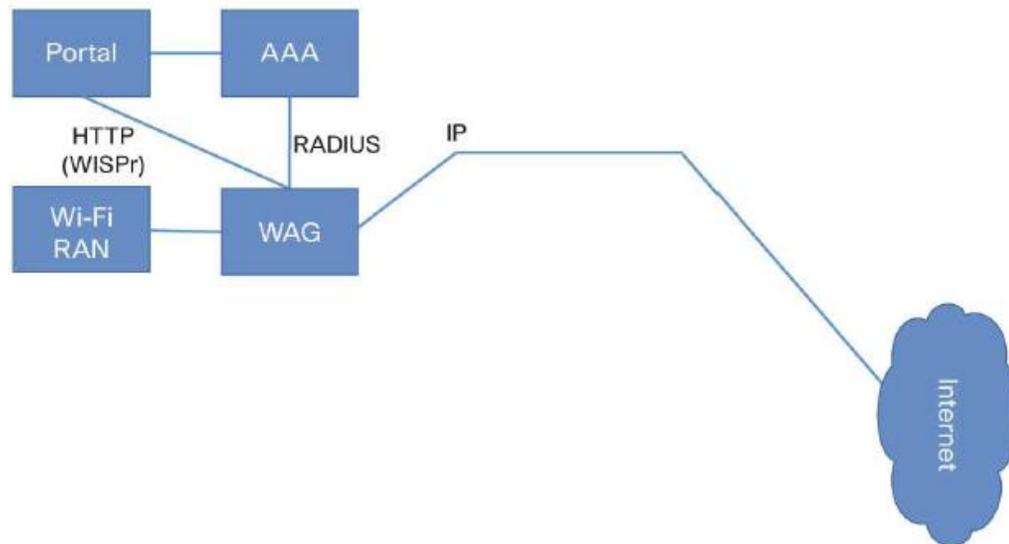
Existen varios métodos para controlar el acceso de los abonados a una red wifi. La elección del tipo de autenticación es esencial para que sea sencillo el uso de la red para el abonado, mientras más sencillo es el acceso, la probabilidad de que el usuario lo utilice es más alta. Lo que se trata es que no sea una pérdida de tiempo o algo complicado de configurar para el usuario, evitando que no lo utilice y se mantenga en la red 3G, sin aprovechar la descarga masiva de datos.

También determina el tipo de abonado o suscriptor que va a conectarse a la red, los tipos de abonado pueden ser dispositivos con o sin tarjeta SIM o dispositivos visitantes. En una red wifi típica moderna existen dos tipos de autenticación que soportan todos los tipos de abonados y que también facilitan el acceso de los abonados existentes a la red wifi.

#### **3.6.1.1. Autenticación basada en un portal**

La autenticación por medio de un portal depende de la conectividad de capa tres a la red y de la comunicación por medio de una HTTP hacia el dispositivo del abonado antes de que obtenga acceso a internet (ver figura 32).

Figura 32. **Arquitectura basada en portal de autenticación**



Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p. 4.

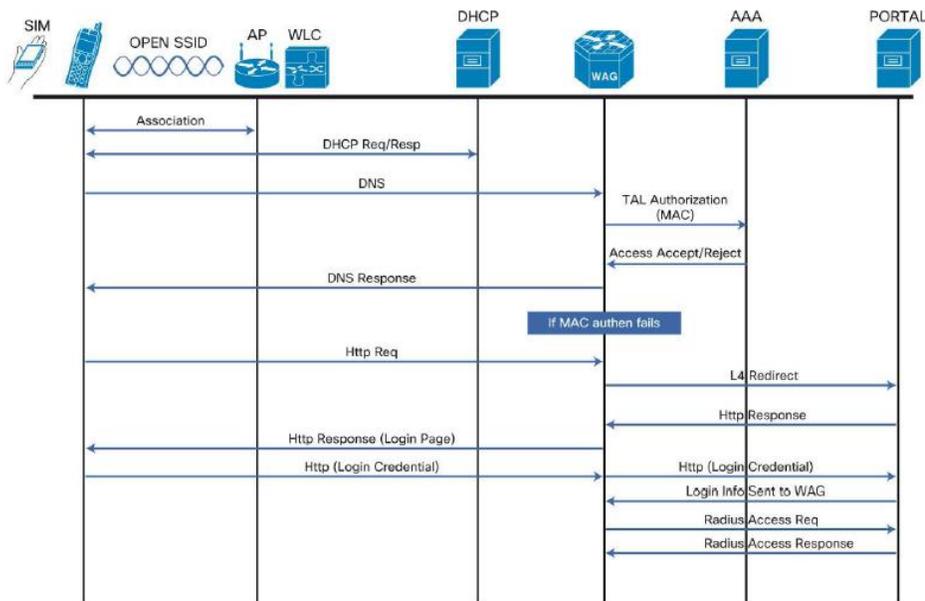
Este método de autenticación consiste en bloquear toda comunicación IP para un dispositivo nuevo. El encargado de bloquearlo es el WAG *switch* de última generación, el cual tiene la capacidad de discernir entre usuarios nuevos y usuarios ya registrados. Si se tratara de un dispositivo nuevo, este redirige la conexión HTTP hacia un portal cautivo responsable de solicitar credenciales al abonado, autenticación, autorización y contabilidad.

Luego de abrir sesión registrándose en el portal, el WAG y el AAA estarán en comunicación continua, ya que la información del abonado quedará guardada en la memoria caché de AAA así como la contabilidad de gasto del abonado, mientras que el encargado del acceso a internet del abonado seguirá siendo el WAG.

En el caso en que el abonado ya se registró a la red wifi, abandona la cobertura de la misma y luego regresa, ya no deberá registrarse de nuevo, será reconocido por el WAG por medio de la dirección MAC del dispositivo. Esto hace que el abonado no pase por el portal en repetidas ocasiones sino que automáticamente se registre y su información se tenga en la memoria caché del AAA.

En la figura 33 se describe el flujo de una llamada e inicio de sesión y acceso a red wifi, según la arquitectura basada en portal de autenticación de CISCO.

Figura 33. Inicio de sesión automática de llamadas



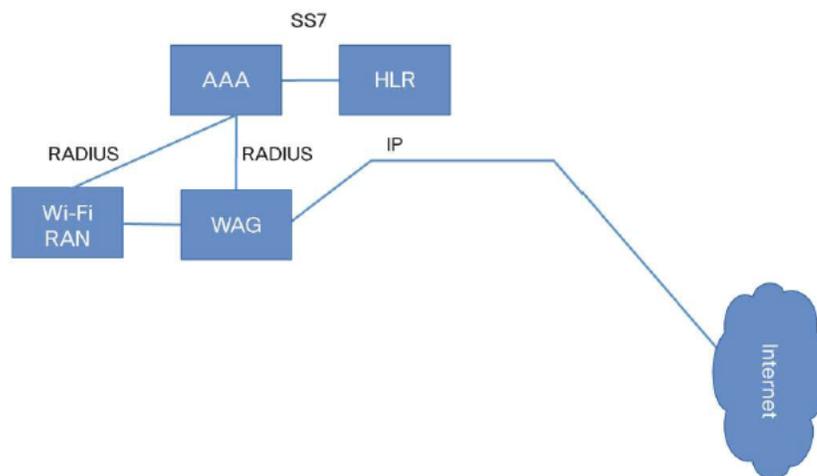
Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p. 5.

### 3.6.1.2. Autenticación basada en EAP

La autenticación basada en EAP utiliza IEEE 802.1X y EAP para proporcionar, por medio de capa 2, el acceso a la autenticación de los abonados. En este caso existen múltiples credenciales para autenticación, todo dependiendo del tipo de dispositivo y su capacidad de soportar EAP.

El método para la autenticación empieza en el dispositivo, el cual toma la información de la SIM, la encapsula en el mensaje EAP y lo envía. Luego, el servidor de autenticación AAA toma el mensaje, envía la información hacia el HLR donde se encuentra el abonado apegado, lo compara, autentica que sea de la red y que tenga saldo para navegar. La arquitectura de este método se muestra en la figura 34.

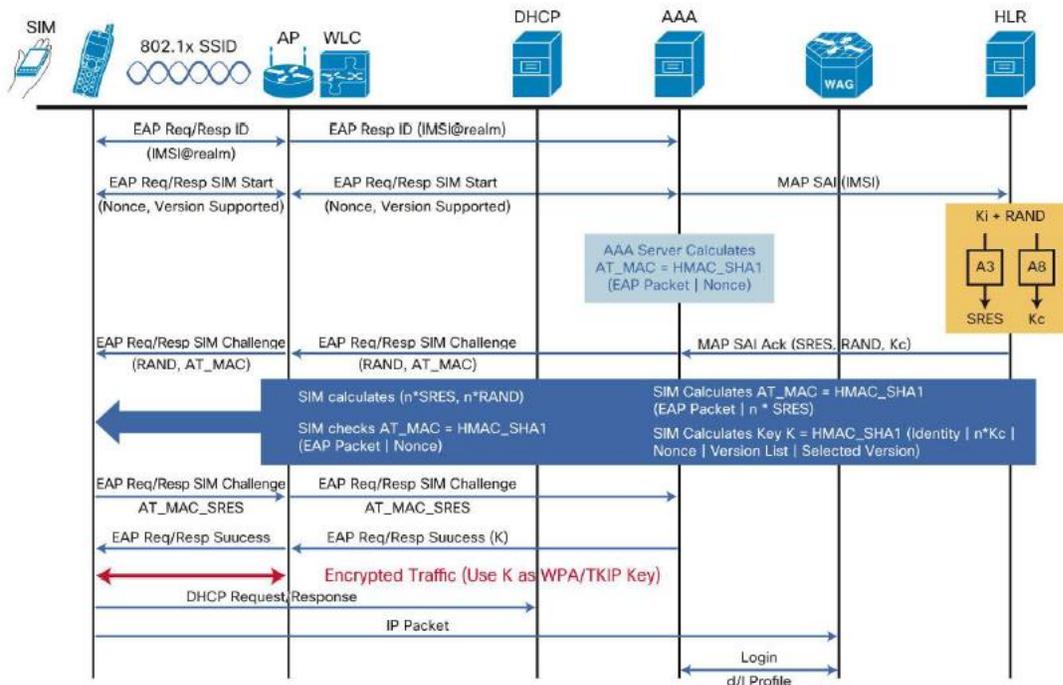
Figura 34. **Arquitectura de autenticación basada en EAP**



Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p. 6.

Para los abonados que tienen dispositivos sin SIM, el operador puede distribuir certificados EAP-TLS o una versión similar, el flujo de llamada típico para la autenticación con EAP se muestra en la figura 35.

Figura 35. Flujo de llamada con autenticación EAP



Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p. 7.

La autenticación basada en mensajes EAP ofrece la seguridad de radio como ventaja, debido a que la autenticación la maneja en capa 2. Los mensajes EAP se utilizan para negociar claves de cifrado con base en IEEE802.11i de la interfaz de radio. Este enfoque proporciona más seguridad para la comunicación de radio en comparación con la interfaz de radio no cifrado de autenticación basada en portal y es el único capaz de evitar los ataques de suplantación de direcciones MAC.

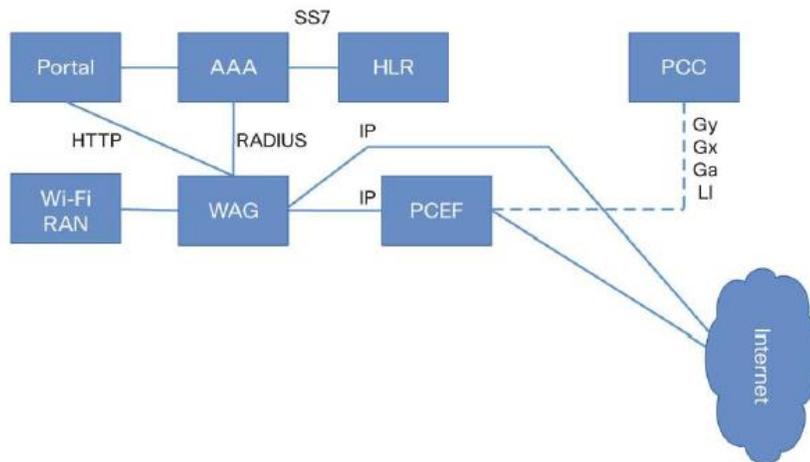
### **3.7. Estrategia y cargo de control**

Una de las preocupaciones más importantes de los operadores de telefonía es la disponibilidad de poder aplicar políticas similares o idénticas y reglas de cargo para el abonado, esto independiente de la RAN que se utilice. Por lo tanto, la integración del PCC es crucial en el wifi offload.

#### **3.7.1. Arquitectura de PCEF independiente**

En este caso, el WAG está configurado para enviar tráfico a través del PCEF, que a su vez tiene señalización con el PCC para el control de políticas de usuario. El PCEF sirve de portal antes de que el abonado pueda tener acceso a internet, pero, si el abonado que intenta tener acceso es un abonado visitante o mayorista, este tiene acceso directo a internet, tal y como se ve en la configuración, en la figura 36.

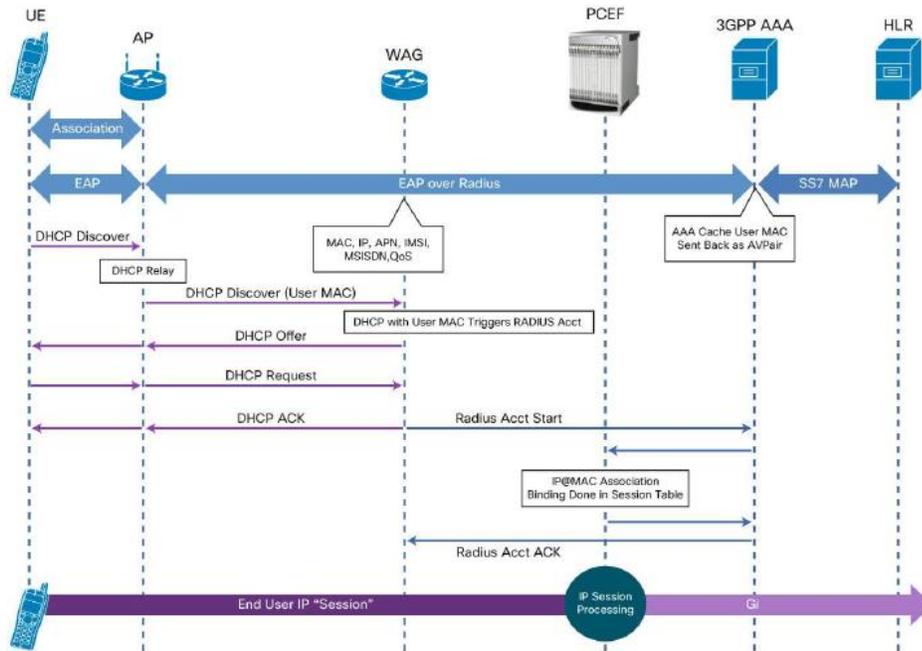
Figura 36. **Arquitectura de PCEF independiente**



Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p. 8.

La PCEF debe ser capaz de correlacionar la identidad del usuario con el flujo de datos del mismo. Para esto se utiliza un mecanismo capaz de sincronizar tanto la identidad del usuario con su dirección IP, de este modo, los paquetes de datos individuales de cada usuario pueden ser procesados, comúnmente para este trabajo se utiliza la función *proxy*, llamada RADIUS en la PCEF. En la figura 37 se muestra el flujo de llamada típica para esta arquitectura.

Figura 37. Flujo de llamada típica de autenticación PCEF



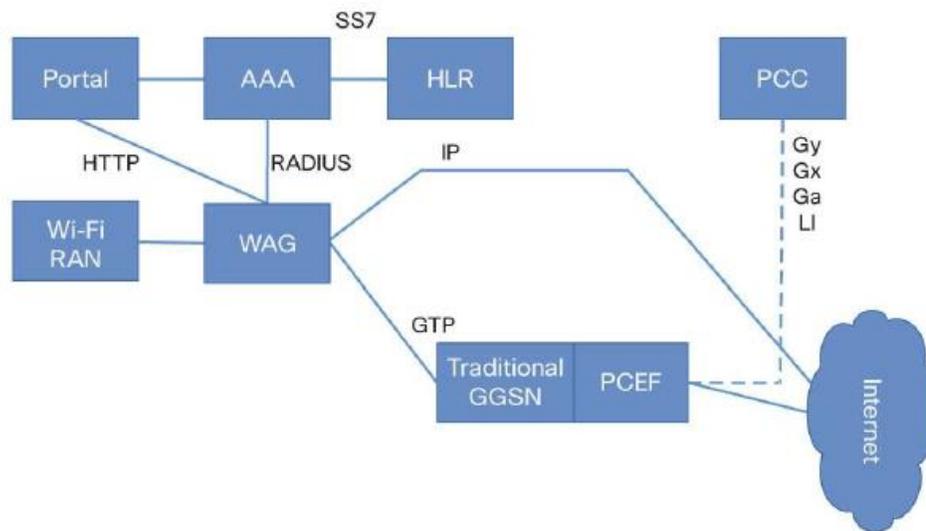
Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p. 9.

Para la implementación de este modelo, el operador necesita garantizar toda la información obligatoria que necesita el PCEF. Esta información es la dirección IP de la sesión del suscriptor, la información sobre la identidad del abonado móvil internacional, número de la guía internacional del abonado de la estación móvil y el nombre del punto de acceso APN.

### 3.7.2. Arquitectura tradicional del GGSN

Si el PCEF está integrado al GGSN directamente, se toma como mejor opción forzar las sesiones wifi a través de un túnel GTP, que no es más que un protocolo de paquetes de datos, esta es la mejor solución para la integración del PCC. El tráfico que no pertenece a los abonados móviles se remite directamente a internet. En la figura 38 se expone el diagrama de esta arquitectura.

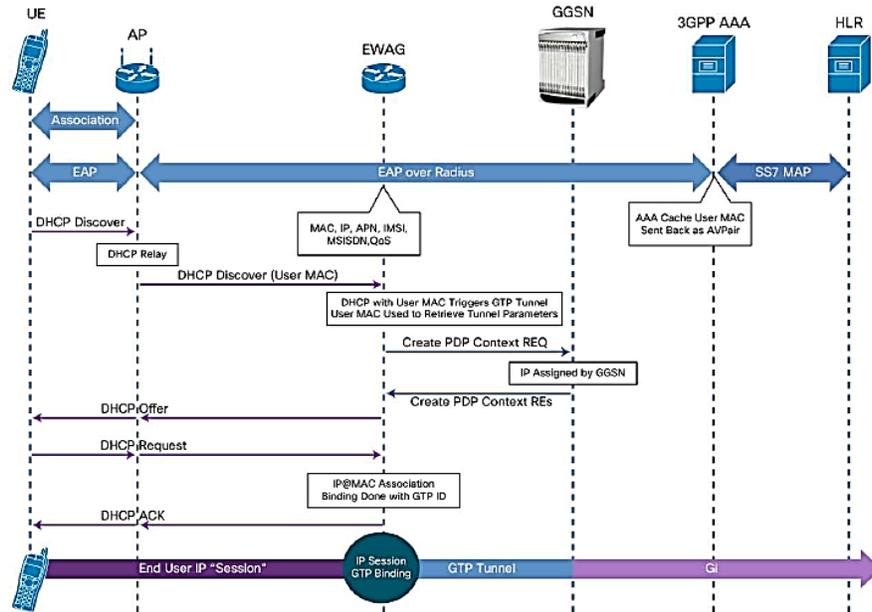
Figura 38. **Arquitectura tradicional del GGSN**



Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p. 10.

Para este modelo de implementación se requiere el apoyo de GTP en el WAG, también es necesaria la información de usuario requerida en la arquitectura anterior. En la figura 39 se expone el flujo de llamada para esta arquitectura.

Figura 39. Flujo de llamada para arquitectura tradicional GGSN



Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p. 10.

### 3.7.3. Handover de radio interno

Antes de analizar los métodos de *handover*, es necesario conocer los conceptos de sesión, traspaso y el tipo de entrega a utilizar en función de los requisitos del operador. En las redes de datos móviles, uno de los procedimientos más importantes es el *handover*, término utilizado para describir la entrega y recepción de una conexión en proceso cuando el móvil cambia de cobertura entre radio bases. Este mismo proceso se lleva a cabo cuando se está utilizando wifi offload el móvil cambia de una cobertura 3G a wifi o viceversa. Entre estos tipos de *handover* se encuentra los siguientes.

### **3.7.3.1. *Handover* con dirección IP no persistente**

Cuando un usuario se conecta a la red wifi, proveniente de una red móvil, pasa por el proceso de autenticación antes analizado. Luego de ser autenticado, se le asigna una nueva dirección IP de la red wifi, todas las nuevas comunicaciones pueden utilizar la nueva IP como fuente. Sin embargo, las redes TCP y UDP siguen establecidas en la red móvil hasta que se pierda conexión con ella y cuando esto sucede se restablecen en la red wifi.

### **3.7.3.2. *Handover* con dirección IP persistente**

Cuando un usuario se conecta a la red wifi proveniente de una red móvil, pasa por el proceso de autenticación y luego se le asigna la misma dirección IP de la red móvil a la red wifi a la que está ingresando, redes TCP y UDP están obligadas a restablecerse en la red wifi automáticamente, en este caso no permanecen en la red móvil.

### **3.7.3.3. *Handover* de sesión**

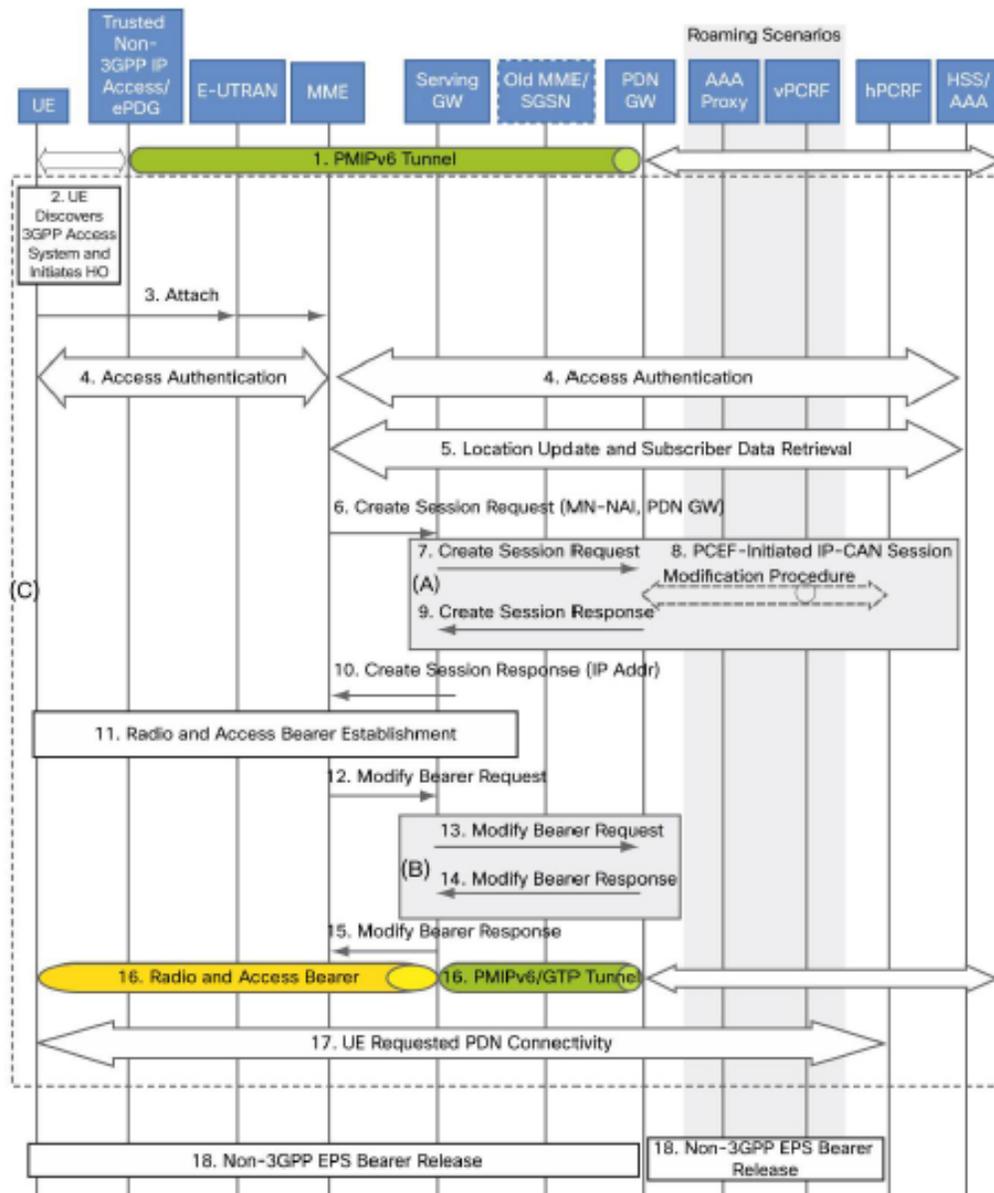
Similar al *handover* con dirección IP persistente, lo único que los diferencia son los tiempos de entrega, ya que para este *handover* la entrega de sesión debe ser imperceptible para el usuario. Todas las aplicaciones en tiempo real no deben ser afectadas al pasar de la red móvil a la red wifi, es por eso que el tiempo debe de ser muy corto.

#### **3.7.3.4. Handover basado en S2A**

Este no necesita la participación del abonado para mantener la movilidad debido a la utilización del PIMIPv6. Este protocolo está construido basado en la red de movilidad IP, facilitando la entrega de direcciones IP para diferentes accesos sin la participación del cliente.

En este diseño, el responsable del anclaje de la sesión y asignación de las direcciones IP es el P-GW. Este enlace también se encarga de la conmutación de túneles por medio del protocolo PIMP-v6, tal y como se observa en la figura 40.

Figura 40. Flujo de llamada para *handover* basado en S2A



Fuente: Cisco. *Architecture for mobile data offload over wifi access networks*. p.18.

## 4. PROPUESTA DE INTEGRACIÓN ENTRE RED MÓVIL Y WIFI

### 4.1. Controles wifi

El incremento en la demanda de tráfico de datos a través de redes inalámbricas está creciendo rápidamente debido al enorme desarrollo de las aplicaciones multimedia, como: música, video, videoconferencias y redes sociales. Aplicaciones de alta tasa de bits hacen que el recurso de las frecuencias en una red móvil sea sobreutilizado, y además, la existencia de limitaciones de licencias de espectro para uso celular, obliga a que se utilice cada vez más redes wifi con el fin de liberar recursos celulares en la red móvil.

El crecimiento exponencial del tráfico de datos en la red celular en los últimos años ha sido superado por un aumento mayor en el tráfico wifi proveniente de *smartphone* y *tablets*. De acuerdo con la Wireless Broadband Alliance, las cifras para el año 2011 indican que el número total de usuarios de *hotspots* wifi públicos en el mundo haciende a 1,3 millones. Este número se prevé que crecerá en un 350 %, lo que equivale a 5,8 millones en el año 2015.

Además del crecimiento en el consumo de datos, los abonados están siendo más exigentes cada día, ellos esperan que en cualquier lugar donde se encuentren sus dispositivos no experimenten ningún tipo de disminución en la calidad de señal, velocidad de descarga entre otros.

Otro punto por el cual wifi es una opción fuerte es que cuando la red móvil tiene algún tipo de limitación interinstitucional o de tecnologías incompatibles, estas limitaciones son transparentes cuando se habla de una conexión wifi, debido a que su protocolo y espectro de frecuencias es equivalente en todo el mundo.

La disponibilidad de explotar el espectro sin licencia, mientras se está proporcionando una experiencia al abonado sin fisuras, tiene un atractivo para todos los proveedores de servicios de telefonía celular. Los proveedores están empezando a ver la tecnología wifi como otra tecnología inalámbrica con la que pueden aumentar su red macro con redes micro. En particular, los proveedores pueden aprovechar wifi para ofrecer un acceso inalámbrico de banda ancha rápida, fiable y rentable.

## **4.2. Recientes habilitadores wifi**

Recientemente se han producido avances en la tecnología wifi que facilitan la interacción con redes celulares por medio del denominado wifi offload, estos se describen a continuación.

### **4.2.1. Normas en evolución**

Los esfuerzos realizados por IEEE, Wifi Alliance (WFA) y Banda Ancha Inalámbrica Alliance (WBA) para estandarizar características de portadoras da como fruto el Hotspot 2.0 y el Next Generation Hotspot, también hay esfuerzos de 3GPP para estandarizar aún más el *handover* entre wifi y 3GPP son parte de las evoluciones de las dos tecnologías, tanto wifi como celular.

Hotspot 2.0 está orientado a facilitar y automatizar una conexión segura y confiable a wifi, con la capacidad de utilizar una variedad de credenciales del usuario, o de los dispositivos utilizados por ellos. Además, promete mejorar la detección y selección de redes wifi, al suministrar nuevos métodos de transmisión de información para los puntos de acceso sin haber asociado un dispositivo; todo esto con el fin de mejorar el método de wifi offload.

En paralelo, la industria celular ha convergido en un único estándar de banda ancha móvil, que ha facilitado la integración wifi/celular. Históricamente, las tecnologías 2G y 3G han estado separadas, TDMA basada en TIA EIA y el acceso CDMA, para Norte América, y 3GPP en gran parte del resto del mundo. En la actualidad, la opción de evolución en todos los operadores ha sido LTE para 4G, la gravitación de normas basadas en 3GPP para 4G facilita la integración con wifi. Como es más económico y facilita la inclusión de socios de operador diferente, se incrementa el incentivo para que los operadores inviertan en wifi offload. Esto ha hecho que los operadores piensen estratégicamente en la inversión de las dos tecnologías tanto LTE como wifi offload.

Entre los trabajos de 3GPP está la mejora del *interhandover* wifi/celular, incluyendo las formas de mejorar la selección de las redes wifi de dispositivos y las opciones de integración de las redes wifi en el *core* de la red celular.

Autenticación basada en EAP-AKA/SIM, movilidad basada en S2a sobre GTP(SaMOG) y acceso de confianza para el *core* de 3GPP a través de wifi, permitirá a los abonados moverse sin problemas entre redes wifi/celular. Además, con el fin de optimizar los recursos de la RAN y entregar una mejor experiencia al abonado, 3GPP está trabajando en la integración de wifi en el *radio access technology* (RAT), esto entrega selección dirigida por usuario y decisiones basadas en tiempo real. 3GPP también pasó tiempo estandarizando

ANDSF, este proporciona una herramienta más para que los operadores puedan personalizar las políticas de dirección de red y distribuir esas políticas a los dispositivos.

En la versión 11 de las normas 3GPP, el trabajo se centró en el acceso no 3GPP para el *evolved packet core* (EPC), que se basa en SaMOG. Este enfoque aprovecha la mejora de WLAN y la gestión de túnel seguro más eficiente, estos túneles se abren entre puntos de acceso wifi y la puerta de acceso WLAN. Este enfoque da como resultado la capacidad para proporcionar la descarga de internet directamente desde la puerta de acceso WLAN de confianza a través del *packet core*. También hay esfuerzos para proporcionar la movilidad con la preservación de la dirección IP y el apoyo a la PDN de múltiple conectividad a través de wifi, así como una integración más estrecha de la RAN, con el fin de proporcionar tráfico de dirección y movilidad entre 3GPP y wifi, para así mantener una buena experiencia del usuario QoE siempre optimizando el recurso de red.

#### **4.2.2. Evolución en las capacidades de dispositivo**

La mayoría de los dispositivos móviles a la venta en el mercado actualmente son de radio dual, es decir, manejan red móvil celular y wifi; además, son capaces de utilizar las dos tecnologías al mismo tiempo. Esta característica de acceso simultáneo a wifi y 3GPP significa que existe la oportunidad de dividir entre las dos tecnologías los servicios que el proveedor entrega. Sin embargo, con el crecimiento de estos dispositivos y de la variedad de tecnología, se va haciendo más importante la selección inteligente de la dirección del tráfico a utilizar.

Para ir de la mano con la evolución de los dispositivos, los operadores están interesados en utilizar clientes ANDSF en los dispositivos, quienes se comunican con un servidor ANDSF en la red, el cual suministra la política ANDSF al dispositivo para que este sea el encargado de la selección de red y las decisiones de direccionamiento de tráfico. Todo esto, con el fin de que el abonado obtenga una buena experiencia y se mejore la utilización de los recursos de red y radio.

Los dispositivos móviles se han vuelto más inteligentes y son la entidad que está más consciente de las condiciones de la conectividad a la red en tiempo real. Con la combinación de la política del operador y la inteligencia de red/dispositivo, es el dispositivo el que se encuentra en una posición única para tomar la mejor determinación de por qué tipo de acceso será transportado el tráfico.

#### **4.2.3. Evolución de modelos con interfuncionamiento 3GPP y wifi**

Debido a que las redes wifi de acceso público operan en el espectro sin licencia, los operadores pierden visibilidad del cliente cuando este se mueve de la red celular a una red wifi, debido a que el cliente atraviesa infraestructuras de red alternativas que no siempre pertenecen al operador. Sin embargo, la situación está cambiando con la evolución de los estándares compatibles.

#### **4.2.3.1. Redes de acoplamiento flexible**

En este tipo de solución, el rendimiento de la red wifi por lo general no está dentro del control del operador, lo cual influye en la experiencia del usuario porque se pierde la continuidad de la sesión IP, ocasionando que se rompa el flujo de datos hasta que se abra una nueva sesión IP. Para este problema, los operadores están utilizando ANDSF para distribuir las políticas que guían las decisiones de direccionamiento del tráfico y así maximizar la experiencia del usuario.

#### **4.2.3.2. Redes de estructura rígida**

En esta solución, el rendimiento de la red wifi está bajo el control del operador. Como solución de la red, se realiza la integración de la red 3GPP con la red wifi de redes RAN y se diseña de manera que se pueda proporcionar continuidad de la sesión IP, haciendo que la experiencia del usuario final sea óptima.

En este tipo de solución, la sección de la red del operador de control inteligente jugará un papel vital, ya que se debe asegurar de que la decisión de mover el tráfico hacia o desde la red wifi se haga de manera que se maximice el QoE.

### **4.3. Desafíos en el interfuncionamiento celular de 3GPP y wifi**

En particular, los desafíos que enfrenta la integración de la red de telefonía y la red wifi consisten en la realización de una solución completa de selección de red inteligente que permitirá a los operadores dirigir el tráfico de forma que se maximice la experiencia del usuario y que se pueda hacer en todos los RAT, los cuales son 2G, 3G, LTE y wifi. Entre los retos principales que tiene la integración de las dos tecnologías se encuentran:

#### **4.3.1. Prematura selección de wifi**

Este fenómeno ocurre cuando el dispositivo hace el cambio de una red 3G a wifi sin hacer previo una comparación de la demanda de datos que tenía en 3G, provocando que la velocidad de transferencia de datos caiga de una manera abrupta, lo cual deja una mala percepción al usuario. Tener el rendimiento en tiempo real del tráfico demandado puede ser utilizado para mitigar esto.

#### **4.3.2. Opciones no saludables**

En una red inalámbrica mixta LTE, HSPA y wifi, se puede dar el escenario de traslado de la red móvil sin mucha carga a una red wifi que está bajo carga pesada. El resultado de esto sería la degradación de la experiencia del usuario, debido a que el rendimiento en el borde de una celda de red móvil con poca carga puede ser superior al rendimiento de una red wifi muy cercano al AP pero con mucha demanda de datos.

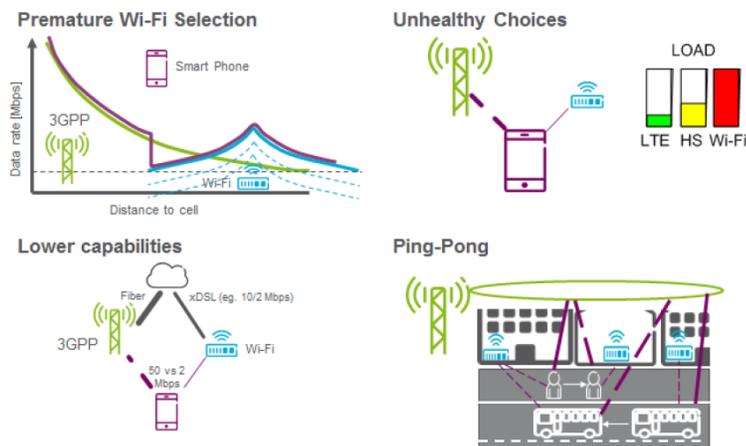
### 4.3.3. Capacidades inferiores

En algunos casos, se puede tener un traslado de un robusto AP wifi hacia una red móvil con un ancho de banda en el *backhaul* mucho más pequeño que el que se tiene para el AP, esto produce una reducción abrupta de capacidad y, por ende, de velocidad para el usuario.

### 4.3.4. Intercambio entre tecnologías

Cuando en una misma zona se tienen muchas buenas servidoras, se genera un fenómeno llamado *ping-pong*, debido a que el dispositivo en uso se conecta y desconecta entre las redes que le sirven en intervalos de tiempo muy cortos. En la figura 41 se muestran los 4 principales retos de la integración entre tecnologías.

Figura 41. Principales retos de la integración entre tecnologías



Fuente: 4G Americas. *Integration of cellular and wifi networks*. p. 10.

#### **4.4. Estado actual de la integración y los retos existentes**

Debido al crecimiento exponencial del consumo de datos, wifi se ha colocado en una posición única para apoyar con la expansión de datos, esto se ve como el complemento ideal para estabilizar las tecnologías 3G y LTE.

##### **4.4.1. Continuidad de servicio entre 3GPP y wifi**

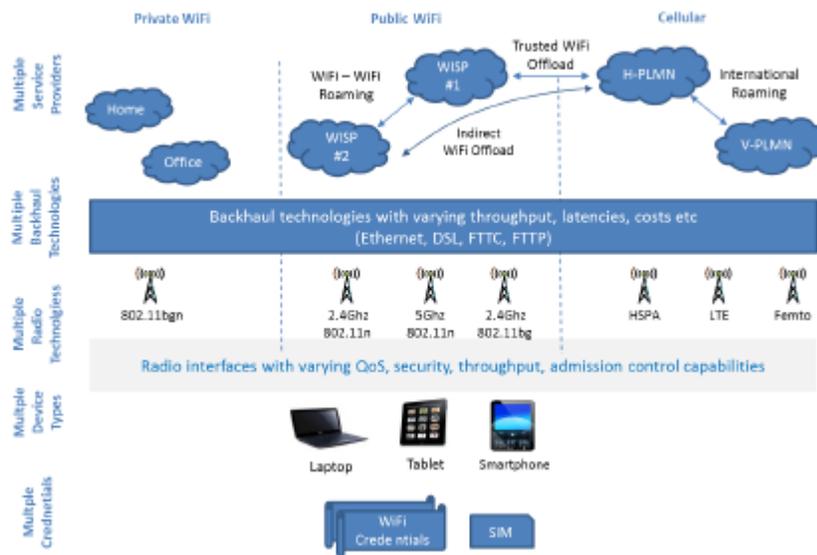
La movilidad entre wifi y redes celulares conservando las direcciones IP ha sido la visión deseada por muchos años, debido a la demanda de datos en las redes móviles, esto se ha venido acelerando para que la solución sea posible. Es conveniente para el proveedor que el usuario final tenga la capacidad de moverse sin problemas con la misma IP en diferentes redes wifi, esta función permite movilidad de servicios más sofisticados como IP *flow mobility* (IFOM) y multiacceso PDN (MAPCON) definidos para 3GPP.

Cuando se analiza a detalle la fusión de las dos redes, se llega a la conclusión de que el acceso WLAN puede ser usado por el operador para ofrecer acceso a la red móvil, permitiendo que un usuario final utilice la red WLAN gratuita en el celular y, al estar utilizándola, un administrador de conexiones enlace el tráfico de vuelta a la red central de paquetes del operador móvil y por lo tanto obtener acceso a internet a través del operador móvil.

El papel del operador móvil implica el plan de enrutamiento del usuario incluyendo el *back end* para la autenticación, autorización y contabilidad (AAA), para proporcionar control de acceso y facturación de servicios WLAN. En este caso, al dispositivo del usuario se le asigna una dirección IP por el operador móvil y cualquier requisito para la interceptación legal del tráfico de usuarios caería sobre el operador de telefonía móvil. En la figura 42 se presenta una

visión general de las opciones de servicio y las interacciones entre la red móvil y las redes wifi.

Figura 42. **Visión general de interfuncionamiento entre 3GPP y wifi**



Fuente: 4G Americas. *Integration of cellular and wifi networks*. p. 15.

#### **4.4.2. Continuidad de servicio en sesión**

Se refiere a la solución en la que la aplicación garantiza la continuidad del servicio a pesar de que la dirección IP utilizada para acceder sea modificada debido a la movilidad entre redes. A continuación se describe un escenario en donde sucede una discontinuidad de servicio, la cual debe evitarse: un cliente está utilizando una aplicación de servicios HTTPS y al mismo tiempo ocurre un evento de movilidad de red, si el cambio de la conexión TCP ocurre mientras el usuario está llenando un formulario o datos privados, se daría el problema de que el usuario tendría que volver a empezar a llenar el formulario.

Describiendo otro caso en que el dispositivo demanda un servicio de calidad, como por ejemplo VoIP, la continuidad se vuelve más problemática ya que el receptor tiene que ser consciente de los cambios de IP. La solución proporcionada por el IMS resulta en una gran cantidad de señalización de intercambios entre el dispositivo y la red. A continuación, se describen los pasos que el IMS genera para la continuidad del servicio: primero debe registrarse en la capa de IMS con su nueva dirección IP, luego tiene que permitir la señalización relacionada con la sesión a la SCC AS, que se produce al cambiar de dirección IP en una sesión de VoIP, por último, se deberá hacer una renegociación entre los medios de comunicación en cuestión; en este proceso se reinicia la comunicación.

En conclusión, mientras que algunos de los servicios pueden convivir con un cambio de dirección IP, otros son susceptibles de ser impactados; la experiencia del usuario dependerá del tipo de servicio y confiando en la capa de sesión de continuidad que no es una solución genérica.

#### **4.5. Métodos 3GPP para movilidad entre redes**

La arquitectura del EPC, que no es más que el *core* de paquetes que fue diseñada para proporcionar apoyo al legado 2G/3G, LTE y acceso no-3GPP como el wifi, este se utiliza para el método de movilidad entre redes.

El soporte de acceso no-3GPP se describe en la especificación internacional 3GPP TS 23.402. Hay dos tipos de redes de acceso no-3GPP a EPC y son definidos por 3GPP TS 33.402: un-confianza y trusted4. Tal como se define en la cláusula 4.3.1.2 de TS 23.402, es la decisión política del operador de origen si una red de acceso no-3GPP se trata de una red de confianza.

Cuando se requiere la preservación de la dirección IP durante la movilidad entre 3GPP y el acceso no-3GPP, el EPC se basa en el P-GW que actúa como punto de anclaje entre estos dos tipos de acceso y oculta la movilidad a las entidades de la red de paquetes de datos. Dependiendo de la naturaleza de la interconexión se tienen las siguientes opciones de movilidad.

##### **4.5.1. Movilidad no continua de todas las conexiones de paquetes**

La UE pone diferentes direcciones IP y posiblemente diferentes servicios a través de wifi por el acceso normal a través de la red móvil, esta característica se ha definido en 3GPP Release 6 como I-WLAN/3GPP IP *access*.

#### **4.5.2. Movilidad sin fisuras de todas las conexiones de paquetes**

Se tiene que, en la movilidad entre 3GPP y wifi, todas las conexiones PDN son *handover* y se conserva la dirección IP. Esta característica se ha definido en 3GPP Release 8 como acceso no confiable no-3GPP.

#### **4.5.3. Movilidad sin fisuras de las conexiones individuales PDN**

En este caso, la UE determina que en la red pública de datos PDN las conexiones son entregadas con conservación de dirección IP, como ejemplo se tiene un punto de acceso APN para mejores movimientos entre el acceso celular y la WLAN wifi, mientras un segundo APN para servicio IMS permanece en el acceso celular, esta característica se ha definido en el 3GPP Release 10 como MAPCON.

#### **4.5.4. Movilidad ininterrumpida de IP individual en conexiones específicas de PDN**

En la movilidad entre 3GPP y la conexión a la UE se determina que se entrega sobre los flujos IP de una conexión PDN, se debe recordar que todas las conexiones PDN tienen su dirección IP conservada, un ejemplo de esta movilidad es cuando el mejor tráfico de internet esta sobre un APN determinado y este se mueve entre la red 3GPP y la WLAN, mientras que un *streaming* de vídeo dedicado en un segundo APN para IMS permanece en el acceso celular. Esta característica se ha definido en 3GPP Release 10 como protocolo de flujo de internet en movimiento y transparente a la WLAN *offload* (IFOM).

#### **4.6. Servicios en tiempo real sobre QoS de confianza wifi**

Para tener un servicio en tiempo real de muy buena calidad se deben de cumplir una serie de características.

##### **4.6.1. Características necesarias para apoyar los servicios en tiempo real**

Un requisito de servicio clave es ser capaz de llevar servicios de tiempo real como VoIP o vídeo de dos vías sobre una red WLAN segura S2a, para dicho requisito se necesita tener las siguientes características.

#### **4.6.1.1. Acceso de UE simultáneo a IMS**

Para el acceso simultáneo a internet de la UE a través del IMS, este requiere de una conexión dedicada PDN por GSMA IR92, por lo tanto la WLAN de confianza requiere capacidad de *multihoming* interpuesto por fase SaMOG 2, que se puede encontrar en 3GPP Release 12.

#### **4.6.1.2. Señalización IMS**

En la movilidad entre 3GPP y cobertura wifi, se desea que la UE no tenga que volverse a registrar. La preservación de la dirección IP del UE después de la movilidad entre las dos redes y la capacidad de manejar la función *proxy* de sesión de control de llamada P-CSFCF, son requisitos para utilizar servicios de tiempo real.

#### **4.6.1.3. Servicios QoS**

Se debe asegurar que en la red WLAN con acceso de confianza se ofrezcan los paquetes que llevan VoIP con la calidad de servicio pertinente en ambas direcciones.

#### **4.6.1.4. Carga y ubicación**

Se debe asegurar que en la puesta a punto y liberación de una llamada VoIP, el IMS pueda proporcionar información de la ubicación de la celda, también proporcionar el CELLID y el PLMNID, que es similar a la información que un acceso 3GPP puede proporcionar.

#### **4.6.2. Habilitación QoS extremo a extremo**

Para flujo IP que requiere QoS y se envían por WLAN hacia internet de una manera confiable, la integración wifi/celular estrecho ofrece tratar de extremo a extremo prioridades que no es posible de otro modo. Esto se logra mediante el aprovechamiento y la coordinación de los mecanismos de QoS disponibles en los diversos segmentos de la red, a continuación se describe este proceso.

##### **4.6.2.1. Interfaz S2A entre el P-GW y la WLAN access gateway**

Para los caudales que requieren QoS se tienen portadores S2a dedicados que se asocian con parámetros QoS como asignación y prioridad de retención, tasa de bits garantizada, máxima tasa de bits y plantilla de flujo de tráfico en el *uplink*. En el ámbito de transporte, la GSMA IR 34 describe la asignación por defecto de los parámetros de calidad de servicio QCI para ser utilizados en la capa de transporte.

##### **4.6.2.2. Habilitación entre TWAG y UE para el enlace descendente**

Cuando se recibe más de un portador dedicado S2a, debe referirse un valor por defecto sobre GSMA IR 34, luego, para el tráfico recibido del TWAG, se hace un mapeo QoS en el AP a los mecanismos de QoS 802.11, para posteriormente seguir las reglas definidas por el estándar. Esto implica la coordinación con la función HCF, que es un híbrido basado en la contención de acceso al canal para proporcionar QoS adecuado sobre el radio WLAN.

#### **4.6.2.3. Habilitación entre TWAG y UE para el enlace ascendente**

Se necesita el mapeo del UE para asociar un flujo de enlace ascendente IP con un nivel de QoS adecuado. La definición de esta asignación puede requerir un mayor estudio que se basa en los principios de SaMOG, que permiten al TWAG enviar un nuevo mensaje de señalización de QoS para el enlace ascendente a la UE.

#### **4.7. Seguridad y autenticación**

Hacer una conectividad segura a las redes de acceso wifi transparentes para el usuario final es un requisito de servicio. Un obstáculo clave para la experiencia del usuario de una conectividad sin fisuras a través de wifi ha sido la falta de mecanismos adecuados de seguridad y autenticación de acceso *airlink*. A continuación se describe el método de autenticación más reciente que está ayudando a superar el obstáculo.

##### **4.7.1. Autenticación**

Para facilitar el acceso a la red de suscriptores de una red celular wifi primero se tiene que ser identificado y autenticado por la red de forma única. Un entorno de red integrado basado en 3GPP en el EPC podrán manejar dispositivos de modo dual de apoyo, tanto wifi como red celular, estos dispositivos incluyen un módulo con USIM. Esta contiene información de suscripciones de usuario y autenticación de credenciales almacenada, de alguna manera, a prueba de manipulaciones. Estas credenciales basadas en USIM se utilizan en la autenticación con la red celular, pero su existencia en dispositivos de modo dual hace que sea más fácil de reutilizar para la

autenticación a través de accesos wifi que se integran con las redes celulares EAP-SIM Y EAP AKA, que son mecanismos wifi de autenticación y hacen uso de la USIM.

EAP-SIM es el mecanismo basado en EAP definido para la autenticación basada en credenciales SIM. EAP-AKA es una mejora respecto a la anterior versión y se basa en claves simétricas USIM que permiten la autenticación mutua, la protección de la integridad y protección de repetición EAP-AKA' es una revisión menor al método EAP-AKA con una nueva función de derivación de claves. Cabe señalar que, mientras los tres mecanismos hacen uso de credenciales USIM basadas en 3GPP, solo las últimas dos pueden proporcionar acceso al EPC a través de no-3GPP Access 6. Es por ello que estas últimas dos se recomiendan como apoyo en la autenticación de una red integrada. Todos estos métodos requieren el soporte IEEE 802.1X, usarlos se ha hecho más fácil debido a que IEEE 802.11i y IEEE802.1X ahora son parte de Hotspot versión 2.0 y por lo tanto son parte de la certificación Passpoint de WFA.

La mayoría de las redes wifi implementan técnicas manuales de inicio de sesión en la que se presta nombre de usuario y sesión a través de una sesión de HTTPS. El uso de esta técnica, llamada portal cautivo, puede resultar en robo de identidad o robo de servicio, y tampoco permite acceso a la EPC, por lo tanto la integración con redes celulares no es posible. En términos de seguridad wifi y la autenticación en un entorno de red integrado, se recomienda el uso de WPA2-Enterprise en conjunto con EAP-AKA y EAP-AKA'.

#### **4.7.2. *Airlink cifrado***

Las redes celulares proporcionan una interfaz de aire segura para fines de autenticación y acceso a la red. A diferencia de estas, las redes wifi pueden tener distintos niveles de seguridad de un enlace aéreo, estos pueden ir desde sin seguridad, es decir que todo el tráfico es transmitido en claro, a la seguridad que puede compararse a la de redes celulares. Cuando wifi y una red celular están integrados, se tiene la expectativa de que la red combinada proporcione el mismo nivel de seguridad en las dos redes.

Con el fin de lograr dicha expectativa Hotspot 2.0 incluye un mecanismo de seguridad basado en WPA2-Enterprise para redes wifi. WPA2 proporciona cifrado de enlace aéreo basado en AES mediante el estándar IEEE 802.11i, el cual tiene certificación de los dispositivos wifi que son capaces de soportar el mecanismo. Este mecanismo proporciona seguridad adicional mediante el aprovechamiento de 802.1x y el uso del servidor AAA para la distribución de claves de sesión.

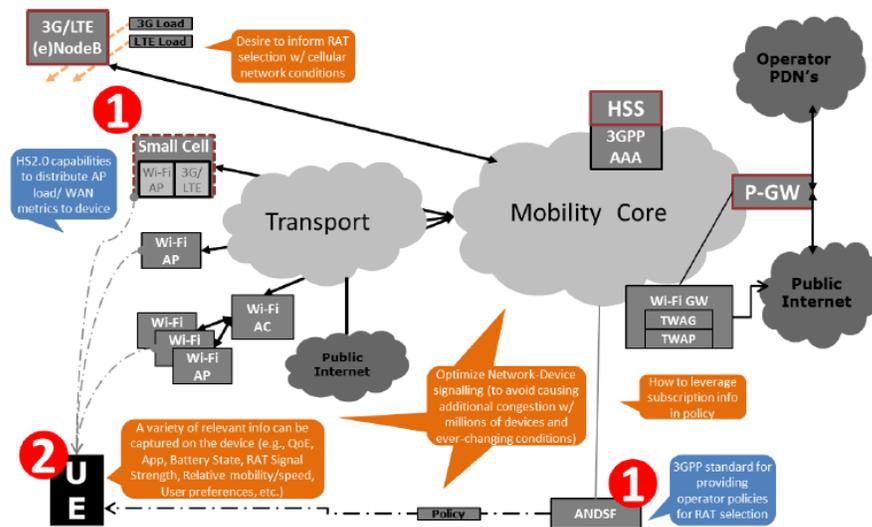
El uso de la seguridad en un enlace aéreo puede ayudar a aliviar las preocupaciones relacionadas con el espionaje, además, una vez que el enlace aéreo está asegurado de manera adecuada, es más probable que el operador de red considere el wifi como acceso confiable. En particular, esto ayudará con la implementación de arquitecturas de tipo SaMOG para proporcionar movilidad entre wifi y red celular con la preservación de la dirección IP.

#### **4.8. Selección de red inteligente**

Las redes inalámbricas son cada vez más heterogéneas y a menudo están compuestas por diferentes capas celulares y múltiples tecnologías de acceso. Con la evolución de las redes heterogéneas, es posible que un UE específico se encuentre en un rango de varias redes de diferentes tecnologías, tanto como redes celulares tradicionales 3G, 2G y LTE como celdas pequeñas integradas con las tres tecnologías descritas y además wifi, así como una variedad de AP de consumo privado o en su defecto que se integran a la red móvil. Ante esta realidad, la selección de la red para un usuario determinado en un lugar determinado es críticamente importante para la optimización de la experiencia del usuario.

Existen varios aspectos a considerar para la selección de red inteligente, en la figura 43 se describe la información de red que se puede aprovechar para ayudar a tomar decisiones de selección de red y de direccionamiento de tráfico, y un número de maneras para distribuir el tráfico.

Figura 43. Aspectos de alto nivel de una red de selección inteligente



Fuente: 4G Americas. *Integration of cellular and wifi networks*. p. 25.

#### 4.8.1. Aspectos de selección de red

La detección de redes de acceso y función de selección son habilitadores de selección de red inteligente entre 3GPP y redes de acceso no-3GPP. ANDSF es un elemento de red opcional en el EPC, el propósito es orientar a las UE con información útil y políticas definidas con el operador para orientar decisiones de selección de red.



## CONCLUSIONES

1. El software ASSET, como herramienta sofisticada, permite nuevos métodos de medición de antenas y de cálculo de cobertura de radiofrecuencia.
2. La tecnología wifi ha estado en constante evolución, lo que permite desarrollar nuevos proyectos, que aportan beneficios como la descarga masiva de datos y soluciones especiales en eventos sociales.
3. Los diferentes estándares de la tecnología wifi proponen diversas soluciones aplicadas a la necesidad del contexto.
4. Las redes móviles 3G, utilizadas para descarga de datos, se han estado sobrecargando de usuarios, por lo que es imprescindible la utilización de métodos de liberación de carga de datos.
5. Wifi offload es el mejor método de unificación entre las tecnologías wifi y 3G, ya que fusiona, de forma integral, la transmisión de datos.
6. La calidad de la experiencia del usuario es un logro que se obtiene implementando wifi offload en centros muy concurridos como estadios, centros comerciales y centros de convenciones.



## RECOMENDACIONES

1. Las empresas de telecomunicaciones pueden integrar la dinámica de la investigación para desarrollar los nuevos avances en la teoría de la radiofrecuencia, sobre las dos tecnologías utilizadas en esta propuesta.
2. Los estudiantes y trabajadores especializados en telecomunicaciones móviles pueden incluir en sus prácticas el desarrollo de proyectos utilizando arquitecturas y estándares wifi.
3. Es importante que los ingenieros de radiofrecuencia analicen constantemente el desarrollo de la telefonía móvil y las tendencias del consumidor.
4. Considerar que el implementar la tecnología wifi offload en las empresas de telefonía móvil permitirá mejorar la calidad del servicio.



## BIBLIOGRAFÍA

1. *Architecture for mobile data offload over wifi access networks*. [en línea]. <<http://www.cisco.com>>. [Consulta: mayo de 2014].
2. *Centro de astrobiología*. [en línea]. <[http://www.partner.cab.intacsic.es/index.php?Section=Curso\\_Fundamentos\\_Capitulo\\_1](http://www.partner.cab.intacsic.es/index.php?Section=Curso_Fundamentos_Capitulo_1)>. [Consulta: mayo de 2014].
3. SMITH, Raymond. *Wifi home networking*. India: McGraw-Hill Education, 2003. 370 p.
4. TAUB, Herbert. *Principles of communication system*. India: McGraw-Hill Education, 2008. 884 p. ISBN: 0070648115.
5. TOMASI, Wayne. *Sistema de comunicaciones electrónicas*. 3a. ed. México: Pearson Educación, 2003. 704 p. ISBN: 970-26-0316-1.
6. \_\_\_\_\_. *Electromagnetic spectrum*. 3a. ed. Estados Unidos: Prentice Hall Career & Technology, 1994. 1408 p. ISBN: 107505376306.



